



THINK SECURITY FIRST!

PROTECTING YOUR **IDENTITY** IN AN AGE
OF **CYBERCRIME**

NEAL O'FARRELL

2019 EDITION

“ If every consumer read and used this guide, life would have been a lot harder for people like me

Brett Johnson, AKA “Gollumfun”

Founder of the Shadowcrew hacker network and original Dark Web, first FBI's Most Wanted Cybercriminal, and the original Internet Godfather

”

Compliments of



Right Networks®

Copyright © by Neal O'Farrell

All rights reserved. This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the author except for the use of brief quotations in a book or other similar review.

The information provided within this book is for general informational purposes only. While we try to keep the information up-to-date and correct, there are no representations or warranties, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the information, products, services, or related graphics contained in this book for any purpose. Any use of this information is at your own risk.

For more information about this book or the author, please visit www.nealofarrell.com or email Neal O'Farrell at emailme@nealofarrell.com.



CPA FMA — CPA FIRM MANAGEMENT ASSOCIATION

The CPA Firm Management Association is excited to partner with a world class expert like Neal O'Farrell and to bring this important information to our members.

As an organization representing more than 1,200 CPA firm managers responsible for the management of accounting practices throughout the United States and Canada, fraud prevention and cybersecurity are always a top concern for us.

We work tirelessly to make sure our members are aware of the latest threats and risks, and have partnered with vendors with the best tools available to protect themselves, their firms, and their clients.

We strongly encourage you to share this expert resource with everyone you know. The smarter and stronger we are as a community, the more difficult it becomes for crooks and identity thieves to find and exploit weak links.

And remember, as a member, you can always turn to CPAFMA and our members with questions, issues or concerns.

Kim Fantaci
President
CPA Firm Management Association

Learn more about us at www.cpaafma.org



Expanding
Knowledge



Sharing
Experiences



Influencing
Leadership



Envisioning
Possibilities



Achieving Through
Collaboration

CPA FMA

CPA FIRM MANAGEMENT ASSOCIATION

*Leading CPA firm practice
management while empowering
all CPA firms to thrive.*

10 REASONS TO JOIN

Be a part of a one-of-a-kind organization. As the world's premier CPA firm practice management association, CPAFMA connects you with professionals from all firm sizes with experience ranging from those new to firm management to those with more than thirty years of experience – giving you and your firm unparalleled networking opportunities.

1

2 Stay current with trends in the CPA firm practice management arena with educational offerings including MAPCasts, local networking opportunities, our regular news feed and CPAFMA Partnerships with Alliances, CPA firm associations, the AICPA-PCPS and state societies.

2



3 Grow your network and increase your visibility by attending local and national events and conferences and MAPCasts that connect you to key influencers in the accounting profession.

3

4 Demonstrate your experience. CPAFMA's Public Accounting Firm Manager (PAFM) credential provides the opportunity for those managing accounting practices to demonstrate their experience with the knowledge, leadership, skills and abilities to operate at a high level of expertise in the field of accounting firm management.

4



5 Learn from experts in the area of CPA firm management and keep ahead of the competition with fresh ideas and high-quality information through CPAFMA's innovative programs, communications, surveys, and best practices.

5

6 Join a local or regional chapter of CPAFMA. Chapter participation enables members to network with firm managers in their geographic area.

6

7 Advance your professional development and earn CPE through many of CPAFMA's offerings to keep your credentials current.

7

8 Access CONNECT the Association's online community where members can share and exchange resources and experiences.

8

9 Get exclusive access to CPAFMA's Member Directory that connects you with more than 1,000 professionals throughout North America – the most complete address book at your fingertips. The Association's Job Market assists firms making human capital decisions with position and resume postings available.

9

To join, visit
www.cpaafma.org

10 Receive member discounts through the Association's Group Purchasing Program – save on software, services, publications and more.

10

The leading cloud hosting provider for accounting professionals

Right Networks gets all your critical accounting and business applications into the cloud so you and your team can be more productive, collaborate more effectively, and scale with ease.

Our cloud-connected ecosystem of 250+ best-in-class accounting applications features:

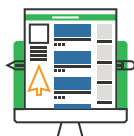
- QuickBooks Desktop hosted in the cloud
- Anytime, anywhere access
- Automatic updates and backups
- Enterprise-class security
- Unparalleled support, 24/7

Ready to get started?

866-228-5809
rightnetworks.com



100%
Accounting
Focused



250+
Best-in-Class
Applications



50,000+
Accounting
Firms & SMBs



THINK SECURITY FIRST!



The Association
Accountants &
Financial Prof
in Business

MEET THE AUTHOR

NEAL O'FARRELL IS EXACTLY THE KIND OF SECURITY EXPERT YOU WANT ON YOUR SIDE. BEFORE A SECURITY INCIDENT HAPPENS, OR AFTER.

THE STRAIGHT-TALKING, NO-NONSENSE IRISHMAN HAS BEEN FIGHTING CYBERCRIME AND IDENTITY THEFT AROUND THE WORLD FOR MORE THAN 35 YEARS, WHICH MAKES HIM ONE OF THE MOST EXPERIENCED SECURITY EXPERTS ON THE PLANET. AND WHICH IS WHY GOVERNMENTS, INTELLIGENCE AGENCIES, FORTUNE 500 COMPANIES AND CONSUMERS HAVE TURNED TO HIM FOR ADVICE.

Like so many experts, Neal started his career in the deep end, protecting the networks and secrets of the highest value targets - banks, governments, and the intelligence community. He was also one of the first generation of security entrepreneurs to take on the NSA, an experience chronicled in his upcoming book *The Man from Intrepid*.

TRUSTED ADVISOR

Over his 35 year career Neal has worked with governments, the intelligence community, the financial community, Fortune 500 companies, thousands of small businesses and millions of end users and consumers. He was a member of the Federal Communications Commission's Cybersecurity Roundtable, where he helped develop one of the first online security planning tools for small firms.

He was also the only security expert invited to advise the Congressionally-mandated [Stock Act panel](#) in 2013, empanelled to study the security and privacy implications of greater financial transparency by members of Congress and senior federal employees.

Neal started his career in security protecting European banks and governments from the first generation of hackers, including winning the first ever contract to encrypt Ireland's entire national ATM network in 1988, and co-hosting with IBM one of Europe's first network security conferences in 1989.

PASSIONATE EDUCATOR

Neal is passionate about the importance of educating users to defeat cyber threats, and was a co-founder of the Center for Information Security Awareness, a partnership with FBI/InfraGard to provide free employee security awareness training for individuals and small businesses. Neal created the entire course, test, and certification, and that course has since been accessed by thousands of organizations. In 2002 he launched Hackademia, one of the first companies to offer cybersecurity courses online. Hackademia is now part of the University of Washington.

Neal currently heads [Schooled In Security](#), a non-profit Silicon Valley initiative to bring cybersecurity education to every high school and encourage students to pursue careers in cybersecurity to help address the critical national shortage of cybersecurity professionals.

He also leads a program called Foster Warriors, to help foster youth and graduates pursue studies and careers in the world of cybersecurity.

IDENTITY THEFT EXPERT

In 2004 Neal was the first expert to train an entire police department in identity theft awareness. He went on to lead the Identity Theft Council, an award-winning non-profit that has assisted thousands of victims of identity theft. Through his work with the Council, Neal has helped set new standards in the way victims of identity theft are treated and supported, and in how law enforcement is trained.

He works with hundreds of police departments, Neighborhood Watch groups and community action organizations. He also takes on complex cases referred to him by the FBI and U.S. Secret Service. In 2011 the Council was honored with the 2011 Editors Choice Award from SC Magazine, one of the cyber security industry's most prestigious awards. Previous winners include the NSA.

Neal also leads [Operation Stop IT! – Stop Identity Theft](#)—the biggest push back against identity theft in law enforcement history. Partners in the initiative include the international Association of Chiefs of Police, the American Bankers Association, the Credit Union National Association,

and Transunion. He has also been called on as an expert witness and as an advisor on data breach response.

His book on identity theft has been used by three of the top five U.S. banks to educate their customers on identity theft prevention. Neal is also the Executive Producer of the documentary series *In the Company of Thieves* that goes inside the world of professional identity thieves, and has appeared on the Discovery Channel's *Investigation Discovery* series.

SECURITY ADVOCATE

Neal is a member of the Online Trust Alliance IoT working group, and in 2015 he was honored as the first ever recipient of the Eigen Award, presented by the International Association of Certified Fraud Examiners at the headquarters of Wells Fargo Bank in San Francisco. He's also a member of the National Initiative for Cybersecurity Education (NICE) K12 Committee. He was also an advisor to Civic, a Silicon Valley startup that is changing the fight against identity theft for consumers, lenders, and merchants.

Neal has acted as advisor to numerous security firms including ZoneAlarm (now Check Point), Surf Control (now Websense), Ntru Cryptosystems, Securify, and SiteLock, and identity protection firms like PrivacyMatters, EZ Shield, IdentityGuard, and Credit Sesame. He is currently advisor to Civic, a Silicon Valley startup that is changing the fight against identity theft for consumers, lenders, and merchants.

In 2003 Neal launched the nation's very first Cyber Secure City, a unique experiment to train an entire city – residents, businesses, schools, even the Mayor and city council – in cybersecurity and identity theft awareness. Partners in the yearlong initiative included Microsoft, Cisco, McAfee, and AT&T, and received the endorsement of the US Chamber of Commerce, the Department of Homeland Security, and the International Information Systems Security Certification Consortium, Inc. (ISC)².

SPEAKER AND TRAINER

Neal has taught security to numerous audiences including Morgan Stanley Smith Barney, Ameriprise, Stifel Nicolaus, US Bank, US Trust, BKR International, the Credit Union National

Association (CUNA), and the National Association of Secretaries of State, as well as the Association of Certified Fraud Examiners, the High Tech Crimes Investigators Association (HTCIA), the California Financial Crimes Investigators Association (CFCIA), the California High Technology Crime Advisory Committee (HTCAC), and the International Association of Financial Crimes Investigators.

Neal has authored more than a thousand blogs and articles on security and privacy and has been quoted in numerous publications around the world including the New York Times, Forbes, Inc., the Wall St. Journal, the Huffington Post, CNN Money, BusinessWeek, USA Today, SmartMoney, CNET, Information Week, the National Law Journal, Today.com, NBC, CBS, CNBC, Fox Business, and the South China Morning Post.

A DEEP BACKGROUND IN SECURITY

In the 1980s, at the birth of the cybersecurity industry, Neal was helping governments, banks, and intelligence agencies protect their most sensitive communications. In the mid-1980s, after a phone tapping scandal, he developed a telephone privacy system for the Irish government, and later went on to work with Nokia to incorporate privacy and security into their first generation of cell phones.

In 1988 Neal won the first contract to encrypt Ireland's entire national ATM network, the same year he installed the first two-factor authentication system in an Irish bank. He also co-hosted with IBM one of Europe's first network security conferences.

In 1989 he started the Intrepid project, a government supported program to develop a European rival for the NSA's Secure Telephone System (STU3), considered the world's most secure, secure telephone system. The result of the project was the launch of Milcode, widely considered the most secure secure telephone of its time. That project brought Neal into direct conflict with the NSA and that story is chronicled in his upcoming book *The Man from Intrepid*.

Neal also developed Faxcode, the world's first fully encrypting fax machine, and resulted in his selection as the first Irish entrepreneur to be invited to participate in the Export to Japan study program hosted by the Japanese government.

Neal later went on to work with a number of British defense companies to develop a new generation of telephone privacy and encryption systems, and was the first Irishman invited to visit GCHQ, Britain's ultra secretive spy center. He also worked with Britain's largest bank to develop the first generation of voice verification biometrics for the bank's telephone banking system.

ON A LESS SERIOUS NOTE

- Neal expected to be a dress maker and not a code maker, and the third generation to take over a famous Irish family weaving business whose clients included Yves St Laurent, Coco Chanel, the Duchess of Westminster, and the Queen of Siam.
- Neal's family (his grand uncle and grand aunt) made Maureen O'Hara's first ever movie, in 1934.
- Neal's second cousin, Michelle Dockery, played Lady Mary Crawley in the PBS television series Downton Abbey.
- In the true spirit of the Irish Immigrant, Neal came to America by boat – delivering a brand new yacht from the shipyard in France, stopping on the west coast of Africa, and across the mid Atlantic to the Caribbean. In the middle of winter.

ABOUT THINK SECURITY FIRST!

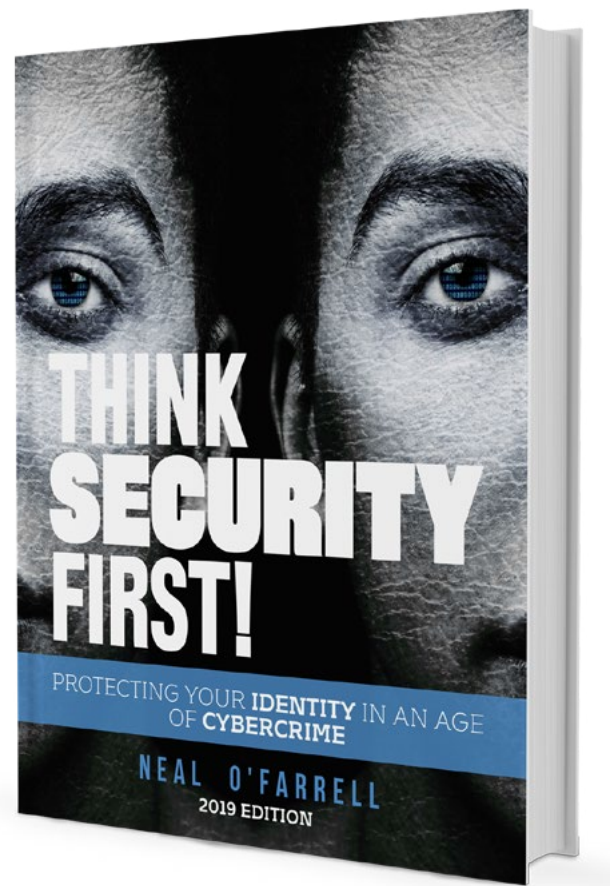
Identity theft is the crime of this century, affecting every business, workplace and consumer in some way, directly or indirectly. It has a thousand different faces – family and friends, mail thieves and burglars, lone wolves and professional teams, street gangs and organized crime, hacker collectives and state sponsored actors – not to mention the more than 50 million victims it's already claimed in the U.S. just in the last few years.

And after two decades of fighting this crime, the crime appears to be winning with more than 1 million new victims

every 30 days. And a big part of the winning strategy is the collusion of identity theft with cybercrime. Identity theft and cybercrime are two sides of the same coin, equal partners in the same crime spree, and it's hard to fight one without understanding its connections to the other.

This book lays out those connections, and provides every consumer and small business owner with one of most detailed and easy-to-read insights into these crimes and the people behind them.

Think Security First! condenses more than 30 years of security experience into more than 30 chapters of straight-talking, no-nonsense advice from one of the world's most experienced consumer security experts.



No more confusing advice, no more pointless recommendations – just straight-to-the-point wisdom from a highly respected and straight-talking expert who's been fighting these crimes and criminals for longer than almost any other expert alive today.

The book includes:

- More than 30 chapters and 270 pages of easy-to-use advice.
- Covers identity theft, malware, hacking and hackers, organized cybercrime, tax fraud, ransomware, passwords, data breaches and everything in between.
- Interviews with some of the most notorious identity thieves and cyber crooks.
- Real life stories of cases, victims, and criminal schemes.
- A list of more than 50 great security and privacy products that are absolutely free.
- A Personal Security Checklist
- A Small Business Security and Privacy Checklist

CONTENTS

Chapter 1

"America Was Made For Identity Theft"

The words of "Ray," described by law enforcement as the most dangerous identity thief in America.

Chapter 2

The Different Types of Identity Theft

And What You Can Do About Them

Chapter 3

Why So Much Identity Theft?

Blame it on.... Everything

Chapter 4

12 Myths About Identity Theft

And Why It's Important To Debunk Them

Chapter 5

Why Are We Losing the Battle Against Identity Theft?

10 Good Reasons

Chapter 6

Know Your Enemy

12 Traits Of Highly Successful Identity Thieves

Chapter 7

Data Breaches and Identity Theft

Close Cousins and Dangerous Liaisons

Chapter 8

The Fake, Fake You

The Growing Problem Of Synthetic Identity Theft

Chapter 9

Invasion of the Body Snatchers

The Growing Menace of Medical Identity Theft

Chapter 10

The Tax Thief Cometh

Protecting Your Identity at Tax Time

Chapter 11

The Most Vulnerable Identity

Protecting the Elderly from Identity Theft

Chapter 12

Keeping Your Kids Safe

From Identity Thieves, Data Stealers, Predators, and Themselves

Chapter 13

Small Is Beautiful – to Identity Thieves

Protecting Your Business From Identity Theft

Chapter 14

An Inside Job

Protecting Your Identity In The Workplace

Chapter 15

Home Sweet Home

Protecting Your Home From Identity Theft

Chapter 16

Grinch This!

Avoiding Identity Theft During the Holidays

Chapter 17

From Princes To Skimmers

Avoiding Common Scams And Frauds

Chapter 18

On The Road Again

Avoiding Identity Theft When Traveling

Chapter 19

You Click. Therefore You Lose

The Menace Of Phishing Attacks

Chapter 20

Credit Monitoring, Freezes, And Alerts

Similar, Different, Important

Chapter 21

Hackers And Hacking

A Brief History

Chapter 22

The Hacker's Favorite Tool

Understanding The Scourge Of Malware

Chapter 23

We've Got Your Data. We Want Your Money

The Growing Threat of Ransomware

Chapter 24

Preventing Identity Theft

21 Simple Choices

Chapter 25

Dawn of the Zombie Refrigerator Apocalypse

Protecting Your World From The Internet Of Things

Chapter 26

Hackers In Your Pocket

Why The Smallest Devices Are The Biggest Target

Chapter 27

PSST! What's Your Password?

The Good, Bad, And Ugly Of The Still Essential Password

Chapter 28

Guarding The Candy Store

Hackers and The Wealthy

Chapter 29

Do What We \$@Y!

The Growing Threat Of Cyber Extortion

Chapter 30

We Are At War

The Global Cyber War And Your Role In It

Chapter 31

50 Free Security Tools

Keeping Your World Safe, Secure, And Secret

Chapter 32

Helpful Resources

Chapter 33

Personal Security checklist

Chapter 34

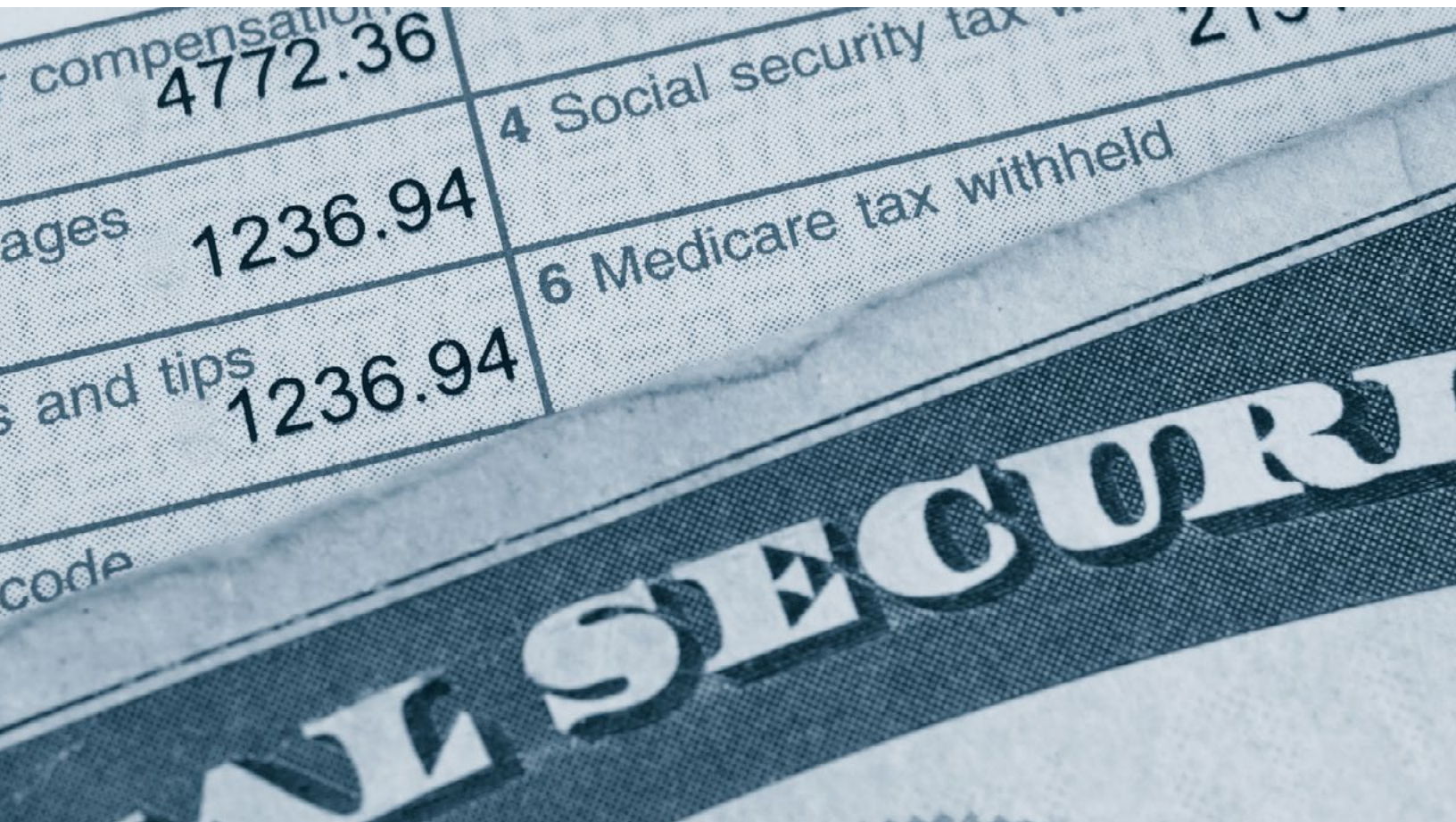
Small Business Security and Privacy Checklist

Chapter 35

Business Travel Security Checklist



THINK SECURITY FIRST!



“AMERICA WAS MADE FOR IDENTITY THEFT”

THE WORDS OF “RAY,” DESCRIBED BY LAW
ENFORCEMENT AS THE MOST DANGEROUS IDENTITY
THIEF IN AMERICA.

Chapter 1

CHAPTER 1

I don't know if Ray is the most dangerous identity thief in America. But he's certainly the most dangerous I've come across in my 30 plus years in cybercrime and identity theft. Dangerous because he's smart, incredibly smart. Smart enough to never have been arrested in a twenty-year crime spree.

Ray used mail theft as a simple example of his theory. Mail theft is still one of the most popular first steps for many identity thieves, because mail provides an interrupted daily stream of priceless information just lying around on public streets and in quiet neighborhoods.

In most American cities, this mail, which is essentially like cash, is not delivered to the home but instead left in an open box by the curb. Even better than that, said Ray, the mailbox at the side of the street is usually conveniently located at exactly the right height to simply drive up, roll down a car window, and drive away with the treasure. Without ever having to leave your vehicle.

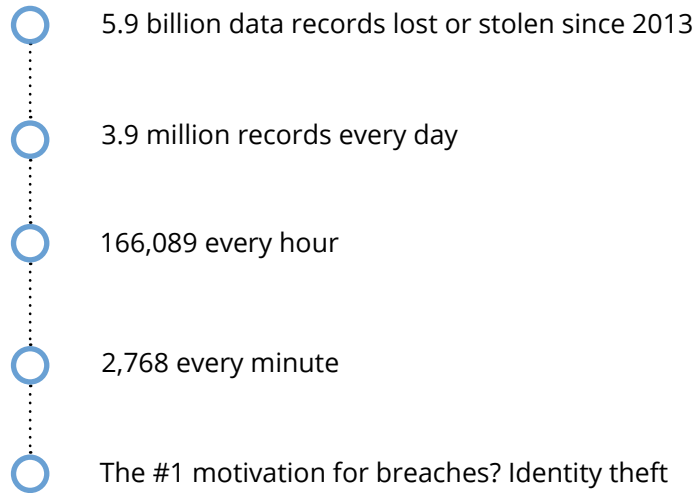
And as if that wasn't tempting enough, if you choose to leave outgoing mail to be collected (like bills with checks included) you even have the option of raising a big red flag on the top of your mail box to let everyone on that street know there's money in that mailbox just waiting to be collected.

It's as though the mailbox is waving, screaming "pick me, pick me" to every passing thief. And the thieves usually oblige. Which is just one of the reasons that the United States is impacted most by this crime.

Identity theft, in its most common financial form, has been around for more than 25 years. And it's been the top consumer complaint to the Federal Trade Commission every year for more than a decade.

But perhaps the one incident that alerted most consumers to the crime happened in 2001. That's when a dishwasher at a New York diner was arrested for stealing the identities of more than 200 celebrities, including Oprah Winfrey, Steven Spielberg and tycoon Warren Buffet. He was only caught when he tried to withdraw \$10 million from the account of a well-known billionaire.

Say What?



Gemalto Data Breach Index 2017

What really caught the attention of both law enforcement and the media at the time was how easy the crime appeared to be. The thief, described as “not very smart,” had used nothing more than a computer at a public library, and a phone book, to find and target his victims.

Today's thieves, like Ray, are much smarter. Since those early days the crime has not slowed for a second, with some studies suggesting that between 7% and 10% of American households have been affected by identity theft. Other reports have pegged the number as high as one in every four households.

And one of the greatest drivers of identity theft is cybercrime. Hackers are daily targeting all kinds of businesses in search of personal, financial, and medical data that they can turn into money, and usually through identity theft. And they have a stunning array of tools to choose from, from malware and phishing emails to a simple phone call.

Because of that collision, between cybercrime and identity theft, and the fact that there is now so much private information in the hands of criminals, most experts agree that at some point every American will eventually be a victim – who amongst us has not had a credit card cancelled because of a data breach?

The Statistics Are Sobering

- In 2018 there were an estimated 14.4 million victims of identity theft in the U.S.
- Identity theft has claimed more than 60 million victims over the last five years¹.
- Identity theft currently claims about 1.2 million new victims every 30 days or one every two seconds¹.
- Identity theft is the single biggest crime in America, claiming more victims than murder and attempted murder, assault, burglary, vehicle theft, arson, check fraud, shoplifting, purse snatching, and pick pocketing – combined.
- Identity theft has cost businesses and consumers an average of \$35,000 every sixty seconds over the last 5 years¹.
- In just the first half of 2018, nearly 1,000 data breaches exposed more than 3 billion more personal records.
- According to Gemalto, more than 13.5 billion data records have been exposed or stolen since 2013 with identity theft being the leading type of data breach².

“ A Gallup poll from 2016 found that the biggest worry for consumers, more even than Ebola and terrorism, was identity theft, causing concern for nearly 70% of respondents. That was followed by fear of hackers using stolen credit cards (69%), which is also identity theft. And those were the only two crimes in the poll that worried the majority of Americans. ”

According to Gallup, more than a quarter of Americans say they or another household member had a credit card stolen by hackers in the last year, which made it the most frequently experienced crime on a list of nine crimes. More than one in ten also said they or a household member have had their computer or smartphone hacked in the last year.

And while the majority of victims of other crimes, like burglary and muggings, say they reported the crime to the police, less than half of identity theft victims and a quarter of hacking victims say they went to the police. And if you've ever been a victim of identity theft and tried to report it to the police, you'll understand why many never bother.

In a completely separate study the same year, the Chapman University Survey on American Fears interviewed 1,500 participants from across the nation and from all walks of life. According to their study, the #1 fear in America today is walking alone at night. Which is understandable, and probably a fear that has been with most humans since sabre tooth tigers roamed the neighborhood.

But the survey also found that hot on the heels of nightwalking fears, identity theft and Internet safety were ranked 2 and 3. Pretty scary stuff when you consider all the possible risks, threats, and fears most of us face every single day. And when the Chapman study moved away from fears and on to concerns, worries over what lurked in the darkness were banished from the throne. When asked about their top concerns (as opposed to fears) identity theft came in at number 1 while internet surveillance by businesses was number 2.

By the end of 2016, fears over identity theft seemed to have dissipated a little, with the Chapman study finding it had dropped to #8 on the list. Which didn't surprise too many experts, given the concern that with so much identity theft news every day, consumers have started to become complacent.

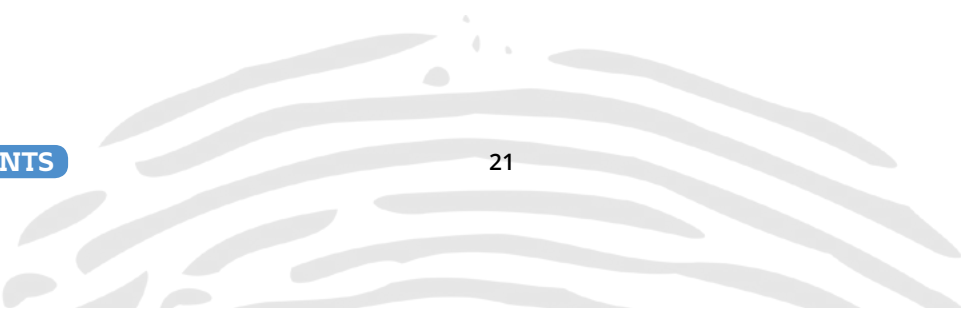
And chew on this. In America we're becoming immune to many types of fraud because we don't really feel the direct pain. Zero liability zeros out the losses for many victims. In most other countries there's no such thing as zero liability. Consumers are on the hook for all the losses they incur. What if things were to change and that became our new normal?

In the meantime, identity theft fears appear to be on the rise again. A study released by insurance company Assurant in January 2017 found that as the lives of consumers become more connected through technology, from phones to the Internet of Things, the top fear this interconnection has brought is – you guessed it – identity theft. But perhaps the most troubling statistic of all is that most victims never see justice, never see the thief prosecuted, and usually never even know who the thief is or how the crime happened.

The Bottom Line?

Identity theft is one of the few crimes in recent history that has changed America. It has changed the way people trust – businesses, their neighbors, each other. It has changed the financial industry, the way Social Security Numbers are used, the postal system. It has changed consumer confidence in the ways businesses collect and protect personal information.

There is some good news though, at least for now. The majority of victims of identity theft lose little if any money. They're protected by zero liability and a variety of consumer protection laws, and can quickly fix the problem and move on. And new security technologies are making it easier to prevent many breaches in the first place, and allowing consumers to gain great control over their identity.



But for a growing number of victims, the crime can be very costly, time consuming and life changing. And for most victims, even those who don't lose any money, the fear and worry that come with identity theft can remain forever.

And I mean no offense when I suggest that one of you is enough. If you agree, use this book to help keep it that way.

1 Javelin Strategy and Research

2 Gemalto Data Breach Index 2018



A VICTIM'S TALE

The Case of the mistaken DUI

Identity theft victims aren't really victims at all. I hear that often, way too often. Or worse, that identity theft is a victimless crime. As if no one has to bear any of the billions of dollars in annual losses.

And while most victims of identity theft end up losing nothing financially, someone is always picking up the tab. And whether it's a bank, a credit card company, or a retailer, those losses ultimately filter their way down to the consumer anyway.

But in many cases, victims pay an unimaginable price. In the case of the first victim (we'll call her Melanie), her nightmare began when she visited the DMV in southern California to routinely renew her driver's license. That's when she got her first surprise. The DMV refused to renew Melanie's license because, according to their records, she had at least two outstanding DUI cases she needed to take care of first.

Melanie was 23 years old and had a perfect driving record with no DUIs. To add insult, citing California privacy laws the DMV refused to provide Melanie with any information about the two cases. Without a driver's license, Melanie wouldn't be able to renew her car insurance. Which meant she wouldn't be able to get to work. Which in turn meant she might lose her job and her apartment. She was at her wits end.

Melanie had nowhere to turn, in part because the system is designed to provide less information and not more, less assistance and not more. Melanie even talked to a couple of lawyers about getting legal help but none seemed interested. There was no windfall to win.

Melanie finally got a break a few weeks later when a District Attorney in northern California sent her instructions for installing an ignition interlock device – a breathalyzer ignition - in her vehicle, something that was mandatory for DUI cases and which could cost Melanie up to \$3,000.

But at least now she knew a little more about who had been using her identity and leaving her with a criminal record. I advised Melanie that her first step would be to obtain a police report from her local law enforcement agency.

As a courtesy, I contacted her local police department, briefed them on the case, and advised them that the victim would be making arrangements to obtain a police report. She was free to do that, replied the detective, but because she had warrants for multiple DUIs (even though they weren't hers), she would be arrested as soon as she showed up to file her police report. Even when we offered to show up, with another police officer, the detective said his hands were tied.

If she was arrested, she would likely have to remain in jail for some time until arrangements could be made to move her to a jail in Northern California where she would likely remain even longer until the case was resolved.

So how was the case resolved? We may never know. I started down the long and winding resolution path, initially contacting the arresting officer. He said because there were no photos or fingerprints taken at the time, he couldn't say for sure who he really arrested. I contacted the local DA to see if their office would take a look at the case and provide us with a letter to the judge to overturn the false conviction. Their response was that they were also helpless unless the arresting officer would admit to the mistake.

Even if the DA or judge agreed to re-hear the case, Melanie would likely have to travel to Northern California, perhaps a number of times, to appear in person. That would mean at least six hours driving, each way, each time. Made even more difficult because she no longer had a driver's license and probably no insurance either because of the DUI.

Shortly after that, while I was trying to find a cooperative judge, Melanie disappeared and her phone was disconnected. In spite of efforts to contact her, we never heard from her again. But Melanie's case is a great example of the thousands, maybe millions of cases of identity theft that can turn a victim's life upside down, are almost impossible to resolve, and even if the initial crime didn't involve any financial losses.



THINK SECURITY FIRST!

THE DIFFERENT TYPES OF IDENTITY THEFT

AND WHAT YOU CAN DO ABOUT THEM

Chapter 2

CHAPTER 2

Blink. Slowly. Now do it again. That's how long it takes for identity theft to claim another victim in the U.S. Nearly 17 million new victims in 2017 alone, more than a million every 30 days, one every two seconds.

There are many reasons why identity theft is the biggest single crime epidemic in history. It's very easy to commit, very easy to make a lot of money, and very easy to get away with. As one notorious thief observed "If I can make \$10,000 in a morning without even getting out of bed, why wouldn't I?"

And with more than 1 billion personal records exposed in data breaches last year alone, thieves have no shortage of stolen identities to exploit. But perhaps the biggest reason behind the biggest crime spree are the endless options thieves have when it comes to exploiting your stolen information.

Thieves have all the advantage. There are dozens of different ways they can get their hands on the information they need – from credit cards and Social Security Numbers, to dates of birth and the answers to all those supposedly secret questions. And as financial institutions now demand things like utility bills as extra proof you really are who you say you are, hackers are now offering to steal those too, on request, for as little as a few dollars.

And armed with all that highly accurate but very stolen information, thieves can use it to commit all kinds of identity crimes.

A World of Fraud

Here's a rundown of just some of the more common types of identity theft, how you can minimize the chances that you'll fall victim, and what you may need to do to deal with the aftermath.

EXISTING ACCOUNT FRAUD

This is one of the most common types of identity theft and really nothing more than credit or debit card fraud. That means that the thieves don't steal or clone your entire identity and pretend to be you, but simply get their hands on a copy of a credit or debit card number and go on the spending spree.

How Can You Prevent It? The easiest way to prevent this type of identity theft is to simply be very careful where you use your credit card, where you shop, and making sure you use a credit card and not a debit card.

How Do You Detect It? The easiest way, and perhaps the only way, is to check your credit card and bank account statements very carefully and very often. Check if your bank or credit card provider will send you alerts for every transaction. And never ignore small charges that you don't recognize. It could simply be identity thieves testing the card or its security to make sure that it works.

“Credit and debit card fraud costs worldwide are expected to exceed \$35 billion worldwide, with nearly half of that in the U.S.”

NEW ACCOUNT CREATION

This is a more serious type of identity theft because it usually means the thieves have your Social Security Number and perhaps other highly sensitive or personal information. Armed with enough information, thieves are usually able to convince credit card companies and other lenders that they are in fact the real and only you and so are able to open up multiple credit cards in your name and begin the spending spree.

But it's not just credit cards. Thieves can apply for mortgages, phone service, cable service, rent an apartment, buy or lease a car, and lots of other types of credit.

How Do You Prevent It? This type of identity theft may also be very difficult to prevent, because so many organizations that may have collected your personal information, like your Social Security Number, may not be very good at protecting it.

One of the few failsafe ways to prevent new account creation is to freeze your credit reports. It's quick, it's easy, and in most states it's cheap and sometimes even free. But you need to give it some thought, because freezing your credit will also mean that not even you can apply for new credit - you'll have to go through the process of unfreezing your credit before you can do that.

So if you plan on applying for new credit any time soon, or if you apply for a lot of credit, a credit freeze may not be ideal. Your next best option is to monitor your credit reports around the clock so you'll get early warning if thieves are trying to open new credit accounts in your name. My chapter on freezes and alerts explains more.

How Can You Detect It? There are really only three ways to detect that someone has opened new accounts in your name, or at least is trying.

1. You'll be notified by your credit monitoring service that someone is trying to apply for credit using some or all of your information.
2. You may get an inquiry from the lender wanting to confirm that you did indeed apply for credit.
3. Or unfortunately for most victims, the first time you learn about the application is either because it appears as a bad or unpaid debt on your credit report, or because a debt collector comes calling and maybe even threatening.

“ Account takeover attacks surged in 2017, as criminals appeared to have figured out ways around security measures, according to the 2018 Identity Fraud Study from Javelin Strategy and Research ”

TAX IDENTITY THEFT

This growing type of very costly identity theft happens when thieves use your information to file fraudulent tax returns with the IRS and make off with a sizeable refund. A refund that might have been meant for you.

It's proven so lucrative for identity thieves, the IRS admits that it may be losing billions of dollars to this type of crime every year. The IRS even had to hire and train thousands of extra employees just to detect this kind of fraud.

Later in the book I'll discuss Operation Rainmaker, about how a gang of street-level drug dealers in Florida managed to file more than \$100 million in fraudulent tax returns.

How Can You Prevent It? There really are only two good ways to prevent this kind of identity theft. Either file your taxes as early as possible every year so that you beat the thief to the punch.

Or if you think that you may be a victim of tax identity theft or that a thief has your Social Security Number, you can apply to the IRS for unique PIN or number that must be used any time you file a tax return. If thieves don't have the PIN, they can't file for a refund using your information.

However, there are now indications that thieves have even figured out how to get their hands on these PINs too. And the PIN is still not available nationally. So check with the IRS at www.irs.gov.

How Can You Detect It? The only real way you can detect this type of identity theft is when you try to file your own tax return and the submission is rejected because someone has already filed using that Social Security Number.

“ The IRS admits that in spite of an increase in security and vigilance, they expect to pay out close to \$5 billion of taxpayer money *every year* for the next couple of years to identity thieves. ”

CRIMINAL IMPERSONATION OR CRIMINAL IDENTITY THEFT

Okay, so all identity theft is criminal. But criminal identity theft usually refers to a criminal using your identity to hide theirs. For example, someone is arrested and gives your personal information, or has a DUI and provides a fraudulent driver's license created using your information. When this happens, you may end up with that person's criminal record. You could be refused a driver's license because of a false DUI, or even be arrested because of the crimes of someone else.

I've come across many victims of this kind of identity theft and it's not pretty. But worst of all, it can be very difficult to undo. It can be a very lengthy process, usually through the courts, to get a false criminal record expunged. And those courts can be on the other side of the country and unwilling to cooperate.

And it may never be resolved if fingerprints or photographs of the criminal who used your identity were never taken in the first place.

So How Can You Detect It? Usually the only way victims learn about this crime is the hard way. They're either refused a driver's license, they're turned down for a job because a background check turns up a criminal record in their name, or they're arrested because of someone else's warrants.

How Can You Prevent It? Again, it's almost impossible to stop. You'll never know when or how thieves get your personal information or how they use it - until it's too late. This is one of the many nightmare challenges of dealing with identity theft. In many cases, there are no fixes. There is no way to prevent it, and your only option might be to engage in a very protracted fight with the legal and court systems.

“ According to the Federal Trade Commission, identity theft using Government documents and records accounted for more than 1 in every 3 cases of identity theft last year.

”

MEDICAL IDENTITY THEFT

Medical identity theft is one of the most frightening forms of identity theft, and for good reasons:

- It can be very hard to undo the crime, especially when dealing with hospitals, insurance companies, and strict privacy laws.
- It can cost tens of thousands of dollars (we all know how costly healthcare can be), and the crime can go on for many years.
- It can mess up your health and insurance records when treatments and conditions that are associated with you are not actually yours.
- It can impact your job if you get a poor health grade because of someone else's medical treatments.

“ According to the Medical Identity Fraud Alliance, around 20% of victims say they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to identity theft. ”

My chapter on medical identity theft has more information on this topic.

SYNTHETIC IDENTITY THEFT

Synthetic identity theft is one of the fastest-growing types of fraud, and expected to grow even more because of the amount of information being exposed daily in data breaches.

Synthetic identity theft uses various pieces of unconnected information to create a fake but still viable identity. That means using one person's Social Security number, another person's date of birth, and yet another person's address.

And because so many organizations still don't join the dots and make sure all the pieces add up to a real person, it makes fraud easy.

So How Do You Detect It? No different to any other kind of identity theft. If you're monitoring your credit, that's likely the first place you'll see signs of synthetic identity theft. And not just because there are new accounts appearing in your name, but maybe new addresses, dates of birth and other incorrect information suddenly appearing on your credit reports.

How Do You Prevent It? Again, like any other type of identity theft. Monitoring or freezing your credit is a great way to detect that something's wrong so you can quickly react, or shut down new credit applications completely.

And if it's allowed in your state, consider freezing or locking the credit reports of your kids too so that their Social Security Numbers are not hijacked at an early age.

“ According to InformationWeek, synthetic ID fraud accounts for 80% of all credit card fraud losses, and nearly 20% of credit card charge-offs ”

EMPLOYMENT/BENEFIT FRAUD

If someone is using your identity to apply for benefits or to work, it could end up being very costly for you. It could result in a denial of legitimate payments, claims, or benefits, or the IRS demanding more from you in taxes or penalties for failing to declare income that wasn't actually yours.

And employment-related identity theft can get especially tricky because if your Social Security Number makes it into the wrong hands, it may end up being used and shared by many different people.

So How Can You Detect It? The best way to check if your identity is being used to commit benefit or employment fraud is to regularly request your Social Security Benefits Statement, and perhaps even create a Social Security Account, with the Social Security Administration at www.ssa.gov. That can help raise red flags if there are claims that are not yours.

You should also consider doing occasional background checks on yourself, just to see if there are any unusual names or addresses associated with your identity.

How Can You Prevent It? Guard your Social Security Number, and those of all family members, and especially your Social Security cards. Never carry Social Security card with you, and hide them some place in your home where burglars or visitors can't easily find them.

BUSINESS IDENTITY THEFT

Later in the book I'll talk about the growing problem of business identity theft, where thieves clone the identity of an entire small business. The goal of the thieves is usually to obtain some kind of credit or loan in the name of the business, and then disappear. Leaving the real owners of the business to deal with the fallout.

And it's much easier to commit than personal identity theft because most of the information needed to clone a business identity is easily available in the public domain.

So How Can You Detect It? It's very hard to detect because it's not like monitoring your personal credit. But the main credit bureaus, and companies like Dunn and Bradstreet do have similar services that will monitor the reputation and financial health of your business.

Regularly Google or search your business name, and set up alerts for it and any variations. That might warn you of any lookalike businesses emerging that are too alike for comfort. And regularly checking the business filings in your state to make sure everything is accurate and up-to-date can help too.

How Can You Prevent It? You can reduce the risk by protecting business information, like tax returns, EINs, and registration documents. And don't share your business EIN (Employer Identification Number) or corporation number unless you really have to.

Throughout this book you'll find plenty of simple advice on how to avoid all kinds of identity theft and recover from them. Until you get there, always keep these simple observations in mind:

- Don't panic. Identity theft is not the end of the world and you won't be required by law to prove you didn't do it.
- Check your credit reports no matter what kind of identity theft it is, just to make sure there's no unusual activity there.
- Keep a record - of what steps you take, who you talk to, and what they tell you. Not necessarily for any legal reasons or action, but just so you don't forget to do something important.
- Get free advice, from sites like the FTC identity theft website (www.identitytheft.gov), Operation Stop IT (www.operationstopit.org) or talk to a free counselor at the Identity Theft Resource Center (www.idtheftcenter.org)
- Use the experience as a reminder to conduct a complete personal audit of your life and your credit. Hackers exploit gaps and it's amazing how many you'll find if you just look. Do it before hackers do.



THINK SECURITY FIRST!

WHY SO MUCH IDENTITY THEFT?

BLAME IT ON... EVERYTHING

Chapter 3

CHAPTER 3

Identity theft is a crime committed with data. Data is everywhere. Therefore, so is identity theft. The #1 reason identity theft is the nation's #1 crime and consumer concern is that you can lose your identity in so many ways and to so many different types of crooks.

And the #2 reason is simply because there is so much data everywhere. Data is the fuel of identity theft. A study a few years ago suggested that if data were water, it would cover the entire planet to a level equal to ten times the height of Mount Everest. We're literally drowning in data.

Because data is everywhere, identity theft can happen just about anywhere – online, in public, in the workplace, and even in your own home. Which is why it's so important to always be vigilant and aware that you can be victimized just about anywhere.

All identity theft begins with data theft, and the thieves use the stolen information to pretend to be another person – like you.

“ A Harvard paper in 2014 suggested that by the year 2020 there will be an estimated 40,000 exabytes of data in existence on planet Earth. One Exabyte is the equivalent of 3,000 times the entire contents of the Library of Congress ”

So Where Can Thieves Get All This Information?

FROM YOUR COMPUTER AND MOBILE DEVICES

According to AV Test, one of the leading independent labs that studies malware, there are now more than 600 million different types of computer viruses, spyware, Trojans, bots, keyloggers and other malware in circulation. Another 400,000 are discovered every 24 hours, and most designed to steal your personal information and your identity.

Much of this malicious software, or malware, is delivered by email – either hidden in or attached to the email, or using links in the email to trick you into downloading something nasty on to your computer.

“ More than 13 billion records have been exposed in data breaches since 2013. Those records include personal, financial, and medical records, dates of birth, credit and debit cards, passwords, and Social Security Numbers. ”

Gemalto 2017 Data Breach Index

ONLINE

There are more than a dozen ways you can lose your identity online, some easy to spot, some not so easy:

- Drive-by downloads or watering holes are web sites that have been infected with malicious code that can automatically infect your computer if you simply visit that website.
- Phishing uses bogus emails and web sites pretending to be your bank, a credit card company, the IRS, a customer, a close friend or a thousand other variations. The goal is usually to trick you into revealing a password, downloading or clicking on something malicious, or revealing something else you shouldn't.
- Social networks are a haven for identity thieves, with many thieves targeting gullible teens or not-so-savvy seniors who might more easily be tricked into revealing personal or family information.
- Bogus web sites offering fake deals or products but which exist only to trick you into providing a credit card number or other personal information.

DATA BREACHES

Thousands of companies every year lose millions of customer records to data breaches. According to the most recent study by security firm Gemalto, there were nearly 1,000 publicized data breaches in the U.S. in the first half of 2018 that exposed billions of personal records, including financial and medical. That's a steady increase over previous years, which suggests that businesses are not getting much better at protecting your personal data.

PETTY CRIMINALS

The thief who used to break into a home or business through a window or skylight armed with a crowbar can now break into the same place through a network, and armed with nothing more than a laptop. And maybe a coffee.

Petty criminals were very quick to realize the money to be made in identity theft, and the very low risk of ever being caught or prosecuted. That's why burglars, car thieves, pickpockets, mail thieves, and drug addicts have turned to identity theft in their droves to make some very easy money.

“ In just one small case in California, an identity thief was found with nearly 250,000 stolen identities in his hotel room. That's close to the entire population of Orlando Florida. At his trial, a major retailer claimed that this one thief, acting alone, cost them more than \$1 million in just one of their stores he targeted. ”

ON THE MOVE

Identity theft is usually a crime of opportunity. Thieves rarely come looking for you, but instead either stumble across you or you simply do something, make a mistake, that they can immediately take advantage of.

Identity theft can happen so easily when you're traveling or simply out in public:

- Travel much? In one scam, hotel guests received calls from the hotel reception apologizing for a computer error with credit card processing and requesting that the guest re-confirm their credit card information. The calls actually came from outside the hotel.
- In another hotel scam, thieves slipped a flier for a local pizzeria under the doors of hotel guests offering irresistible deals and online ordering. The pizzeria didn't exist - the thieves were just collecting credit card numbers.
- Pickpockets around the world have found a ready market for anything stolen from a wallet or purse – credit cards, store cards, id cards, driver's licenses, Social Security cards, even work IDs.
- Skimming is a very common and relatively easy way for thieves to make an unauthorized copy of your credit or ATM card – by placing a bogus card reader inside an ATM machine, waiters at a restaurant using pocket-sized card copiers, and even entire card readers at supermarkets being compromised by dishonest insiders.
- State sponsored hackers are constantly targeting corporate employees on the move. These hackers are usually looking for sensitive data or an unprotected backdoor to the employee's workplace.

“ In one skimming case, thieves made more than \$13 million by paying waiters in restaurants to covertly swipe or skim customer credit cards. The gang then created new cards with the skimmed information, hired a team of shoppers to go on high-end shopping sprees with the stolen cards, then split the proceeds. ”

FAMILY AND FRIENDS

Perhaps the worst kind of identity theft is the one committed by family, friends, or neighbors – the people we usually trust the most. But people close to the victim, people with insider knowledge, familiarity with the victim, and easy access to personal data, commit a large percentage of identity thefts.

Especially vulnerable are kids and the elderly, not just because they never expect to be victimized by family members, but also because the thieves often expect to be able to repay the money before ever being discovered.

IN THE WORKPLACE

Many identity thefts begin in the workplace, either by employee errors that result in personal or customer data being exposed, or deliberate thefts by employees and other insiders.

Your greatest risk in the workplace could be from an insider who grabs an opportunity to copy your credit card number, steal a check from your checkbook, or access payroll files to steal your Social Security Number. And then there are the walk-ins – thieves who simply walk into an office posing as someone who doesn't raise any suspicions.


MAIL THEFT

For many professional identity theft gangs and rings, stealing mail from homes or office buildings provides an endless supply of valuable data. While thieves are always on the lookout for Social Security Numbers, most agree that any data is valuable, because it can either fill in a missing piece of an identity or lead the thieves to more valuable information.

And mail is now such a hot commodity, there have been reports of thieves stealing mail vans and even assaulting mail carriers just to get their hands on all that information.

How Else Can Your Identity Be Compromised?

- Dumpster diving and searching through your trash
- Public records are a great and often free source
- Finding data on used electronics like an old computer
- Burglary, and purse and wallet theft
- Shoulder surfing at places like ATMs
- Figuring out answers to those all-too-easy secret questions. How hard is it to find the name of your high school?
- Credit and debit card skimming, at ATMs, gas stations, and checkouts
- Stealing unprotected data from websites
- Bogus job offers
- Buying stolen data from others
- Attacking payment processing companies
- Dishonest insiders and employees
- Targeting third parties and company vendors, and especially their untrained employees
- Exploiting weak passwords

- 
- Forging personal documents
 - Spoofing and phishing
 - Data stolen in state sponsored attacks and getting into the hands of criminals
 - Tapping into what you say and share on social networks
 - Social engineering – that convincing call claiming to be from the IRS or your credit card company
 - Purchasing Social Security Numbers
 - Stealing and forging checks
 - Accessing credit reports
 - Family and friends

Identity theft can appear to be overwhelming, which is why so many consumers simply throw up their hands in defeat. But I'm hoping that the clearest message you get, especially from this chapter, is that the best defense is a constant one. Always be vigilant, even beyond the point of paranoia, and you'll have the best chance of avoiding the most common traps.



INTERVIEW WITH A THIEF

THIS WAS THE FIRST TIME I INTERVIEWED RAY, SITTING IN A JAIL IN NORTHERN CALIFORNIA WHERE HE WAS SERVING OUT A FEW MORE YEARS OF A LENGTHY SENTENCE FOR IDENTITY THEFT.

Ray should have been serving his time at the much tougher San Quentin Prison just a few miles away. After all, he'd just been convicted of more than 70 felonies, and the judge described him as a menace and a sociopath.

But even in prison Ray was a menace. He'd been caught committing tax fraud during his stay at San Quentin, using Social Security Numbers he purchased or traded from other inmates. So to restore the peace, and for his own safety, Ray was transferred to a less dangerous jail to serve out his remaining years.

Just as the interview got underway, a very strange thing happened. In one quick clean movement, Ray stood up very suddenly and lurched towards me asking if I had a cigarette he could bum as he quickly patted down my shirt pockets as if to see if I managed to sneak a pack past the guards.

I didn't have any cigarettes. And I didn't have any shirt pockets either. Ray wasn't looking for a cigarette – there was a guard posted outside the door and a cop sitting right next to me. Ray was just checking to see if I was wearing a wire.

This was my first meeting, in a California jail, with Ray. He had been described as America's most dangerous identity thief and his luck had run out. He had never been arrested once in twenty years as he stole millions of dollars from victims across the country.

Never arrested until that one unlucky day when he was spotted by a curious wine cop. It was a Friday afternoon and it was that cop's very last day on patrol. If Ray just hadn't been there, had

left just seconds before, or had parked his car anywhere else but there, Ray would still be free and I wouldn't be interviewing him.

That one meeting with the wine cop led to Ray's first arrest, 77 felony charges, and the beginning of a long series of jail and prison sentences that included a few years in California's notorious San Quentin. Where he continued to make thousands of dollars running identity theft scams.

And Ray wanted to talk. He wanted to spill all, or at least as much as he felt safe to. If the other inmates found out he was sharing insider secrets, especially to a cop, Ray could be in even bigger trouble. But he was curiously proud of his life of identity crime and his reputation as the best of the best. And he wanted his story told.

"The thrill, the excitement of committing crimes was always the attraction for me, you know what I mean? It was never about the money. When I think about when I get out of here in the future, I would say 60% of the time I think that I want to go straight, you know what I mean?"

His only guilt was what he was doing to his family. *"I have three daughters. I have a lot of things to stay out of jail for, but to be honest with you, it's an addiction. Forty percent of the time I'm thinking about other things that I want to try, other financial crimes that I have a pretty good idea would work."*

Prosecutors described Ray as a sociopath, and Ray agreed without reservation. *"I think I am a sociopath. There must be something wrong with me, you know, to keep wanting to do this."* It wasn't about the money, he really wanted us to know. *"I want to test my theories to see if they do work. And when I think about that, I get excited, it's got to be some kind of medical thing wrong with me, but I do, I get excited about it."*

He had no hard feelings about the cop who arrested him either, although he was caught hacking into a jail computer to do some background investigating on the cop and his family.

"Even with the police officer that arrested me, I joke with him and I say yeah, you know, I'd like to retire from this crime, but there's just a few more things that I really know will work and I want to try and see if they do. Not so much for the money, just to see if they will work."

I'll be sharing more of my discussions with Ray in later chapters. Ray called me a while after our interviews. He'd been released early and was trying to go straight. I hope he does but I doubt he will. Not because he's a bad guy. But because I think he's addicted to the life of an identity thief.



THINK SECURITY FIRST!

12 MYTHS ABOUT IDENTITY THEFT

AND WHY IT'S IMPORTANT TO DEBUNK
THEM

Chapter 4

CHAPTER 4

Ever get the sense that there are just too many experts churning out the same advice and tips about identity theft, and yet, identity theft keeps getting worse?

Maybe it's because some of those experts are not so expert after all, and don't fully understand the reality of America's biggest crime epidemic.

So to add a little reality check to the discussion, I thought it might help to expose just some of the myths that can lead to consumer confusion about identity theft. Call them Identity theft's *Dirty Dozen*, but if I can help you to better understand the reality of identity theft, you might better appreciate these tips and apply them more often.

SO HERE GOES.

Myth #1

"IDENTITY THEFT IS MORE HYPE THAN REAL"

Truth

Identity theft may be the single greatest crime epidemic in the history of America. According to research firm Javelin Strategy and Research, identity theft claimed an average of more than 1.3 million victims every single month just in 2018. That's no myth.

If you look at the FBI's national crime statistics, that means there were probably more victims of identity theft last year than there were burglaries, attempted burglaries, assaults, robberies, arsons, vehicles thefts, purse snatchings, pick pocketings, check fraud, and shoplifting - combined.

Myth #2

"IDENTITY THEFT VICTIMS ARE NOT REALLY VICTIMS BECAUSE THEY GET THEIR MONEY BACK, SO IT'S NO BIG DEAL"

Truth

The biggest cost for victims of identity theft is usually the long-term emotional harm. If a thief has your Social Security Number, or a grudge, as a victim you can be fighting for your identity for years. Victims often talk about the emotional harm being the worst – the worry, the damage to their credit, their loss of trust, their feelings of betrayal, wondering when the next shoe will drop, if it will impact their credit worthiness, their job prospects and many other worries.

Myth #3

“ZERO LIABILITY MEANS I HAVE NOTHING TO LOSE EVEN IF I AM A VICTIM”

Truth

If you lose a small amount to an identity thief, say a few hundred dollars, chances are high that your bank, credit union, or credit card company will reimburse you quickly. But if the amount is higher than that, or if you can't explain how the money was removed from your bank account, banks will often either deny your claim outright or tell you they will need to launch an investigation into the incident. Something that could take months. Which can hurt even more if the thieves stole money you need for urgent bills.

And you may be in even bigger trouble if your debit card is copied through skimming. The thieves will likely have your card *and* your PIN, without your knowledge, and banks will often use that as an excuse to pin the blame on you, the victim.

Myth #4

“I FROZE MY CREDIT SO MY IDENTITY IS SAFE.”

Truth

A credit or security freeze is a very useful tool but only protects against new account creation, meaning that it stops thieves from opening new credit accounts in your name. But it doesn't stop a thief from misusing an existing account or credit card, prevent skimming, emptying a bank account, check fraud, using your identity to file fraudulent tax returns, Social Security

fraud, employment fraud and many other types of identity theft. And in a troubling trend, identity thieves are turning to payday lenders as a way to get around freezes, fraud alerts, and monitoring, because payday lenders often don't run credit checks.

Myth #5

"I SHOULD BE MORE WORRIED ABOUT MORE COMMON CRIMES LIKE BURGLARY, PURSE SNATCHING, AND PICK POCKETS"

Truth

You are 6 times more likely to be a victim of identity theft than burglary, and 500 times more likely to be a victim of identity theft than purse snatching. Nuff said?

Myth#6

"I CAN JUST GET A POLICE REPORT TO PROVE I'M A VICTIM."

Truth

A police report may be vital if you need to defend yourself against claims from debt collectors or victimized businesses. But they're not always easy to get, in spite of the fact that victims are entitled by Federal law to a police report. Law enforcement is often overstretched and doesn't have the manpower to have someone sit down and help victims complete often complex reports. Reports that most in law enforcement already know will probably not result in any investigation.

The most common excuses victims report receiving when they try to file a police report include *"You need to file the report in the jurisdiction where the crime was committed"* and *"You'll need hard evidence before a police report can be filed."* Neither is true but you may still have to be patient when trying to get a police report. The worst advice I heard a victim get from a local police department when trying to get a report was to "pray on it."

Myth #7

"I TEND TO SHOP ON SMALL BUSINESS WEBSITES BECAUSE THEY'RE TOO SMALL FOR HACKERS."

Truth

Most security experts believe that small businesses are now the number one target for hackers, mainly because of lax security. Web security firm SiteLock has reported finding up to 5,000 new small business websites every single day that have already been comprised or infected with malware waiting to infect visitors and shoppers.

Myth #8

“I USUALLY USE A DEBIT CARD BECAUSE IT’S MUCH SAFER.”

Truth

A credit card is a much safer option than a debit card. A debit card connects directly to your bank account. If it’s compromised, the thief is stealing your money. If your credit card is compromised, the thief is stealing the bank’s money. Which would you prefer?

Myth #9

“I HAVE GOOD ANTIVIRUS SOFTWARE THAT’S ALWAYS UPDATED, SO I DON’T HAVE TO WORRY ABOUT CYBER THREATS.”

Truth

Antivirus software is very important but it’s only one layer of protection. And not necessarily as effective as you might think. A study a few years ago by the University of Alabama found that most of the popular antivirus programs in use at the time only caught about 25% of malware. A test by security firm OPSWAT around the same time found that out of 44 of the most popular antivirus products on the market, only one was able to detect a very simple keylogger.

And there’s growing evidence that hackers have tools that allow them to test their malware against all the most popular antivirus software on the market so the malware is almost certain to bypass security when launched into the wild.

Myth #10

“I GUARD MY PERSONAL DATA BETTER THAN FORT KNOX ”

Truth

It's not you, it's them. No matter how well you guard your personal information, others will betray you. For example, there have been an average of two reported data breaches in the U.S. every single day for the last five years, and more than 5 billion personal records exposed in data breaches in just the last three years. Many of those records may have included Social Security Numbers. Could yours have been one of them?

Myth #11

“PHEW, AT LEAST I'M SAFE AT HOME”

Truth

Don't be so sure. Identity theft is the new burglary. Burglars are much more interested in your personal information, financial statements, tax returns, and Social Security cards than a room full of big screen TVs and high tech gadgets. Social Security Numbers are easy to walk down the street with, don't leave fingerprints, and can be resold many times over.

Myth #12

“WE'RE WINNING THE BATTLE AND PRETTY SOON IDENTITY THEFT WILL BE HISTORY”

Truth

Yes and no. Or to be more accurate, no and yes. No, we're not winning the battle. Far from it. 2016 had the highest number of identity theft victims on record. Will we beat identity theft? Eventually, probably. Until eventually happens, shield's up!



THINK SECURITY FIRST!

WHY ARE WE LOSING THE BATTLE AGAINST IDENTITY THEFT?

10 GOOD REASONS

Chapter 5

CHAPTER 5

Blaming victims of any crime is never a smart thing to do. But the contrarian view is that if you're not honest with consumers, brutally honest, then they're even more likely to become victims.

And because we know that so many cyber and identity crimes happen only because of bad decisions by consumers, a little tough talking might not be a bad thing.

I've identified ten clear reasons why after so much progress in the fight against identity theft, that fight is still steeply uphill.

Reason #1

ZERO LIABILITY HAS MADE CONSUMERS FEEL THEY HAVE NOTHING TO LOSE

The notion of zero liability came from a blend of federal law (the FACT Act or FACTA) and marketing savvy by financial institutions, to shift losses to identity theft from consumers and victims to the financial industry and to merchants.

The financial industry often absorbs identity theft and fraud losses as the cost of doing business and keeping customers happy, but that comes with an unfortunate side effect. Many consumers have fallen into the trap of believing that *zero liability* means *zero responsibility* or loss. In reality, many victims face months or even years of emotional and financial costs, and often with no help.

And remember - the estimated \$36,000 lost every sixty seconds to identity theft usually trickles its way down to consumers, so we all end up paying for it anyway.

Reason #2

LAW ENFORCEMENT LACK RESOURCES TO HANDLE ID THEFT CASES

The number one complaint I hear from victims is the seeming indifference of law enforcement to identity theft and its victims. And most police departments I work with admit that at best they investigate less than one percent of identity theft cases. As one Chief once said to me, if he assigned every single officer in his department to just investigating identity theft, it probably still wouldn't make even a dent in the crime.

To be fair to law enforcement, most police departments simply don't have the resources to investigate identity theft. But many others simply don't understand that they really need to be more sympathetic to victims who arrive on their doorstep desperately looking for help.

Reason #3

CONSUMERS THINK WE'RE WINNING THE BATTLE

Consumers have become increasingly apathetic to identity theft in the last few years, either because they believe they have little to lose (zero liability will take care of everything) or because they think the enemy is on the retreat. This increase in apathy has led to a decrease in vigilance as consumers continue to leave their guard down.

Reason #4

ORGANIZED CRIME HAS GIVEN CYBERCRIME AND IDENTITY THEFT A WHOLE NEW LEASE ON LIFE

Sophisticated criminal gangs, lone-wolf hackers, and even state sponsored groups have been constantly and heavily investing in well-organized scams and attacks, hiring some of the most talented hackers and thieves in the world, creating some of the most sophisticated new kinds of malware, and operating in regions where law enforcement can't, or won't, reach them.

These groups have upped the stakes, turning identity theft into a global business that they have no intention of abandoning any time soon. According to the annual data breach survey from security firm Gemalto, the #1 motivation for the 1,000+ data breaches annually is identity theft.

Reason #5

MOST FINANCIAL INSTITUTIONS STILL DON'T TALK TO THEIR CUSTOMERS ABOUT IDENTITY THEFT

Even today I still hear it whispered by banks, credit unions and credit card companies – if you talk to your customers about identity theft, they'll worry unnecessarily. Silence is a better strategy. Of course the exact opposite is true. If your bank or credit union is not regularly reminding you about the reality of identity theft, that's when you should worry. Financial Institutions need to educate their customers about identity theft and other security risks because it's simply good for business.

Not occasionally, but relentlessly. Just like they should be educating their own employees about security risks and the need for constant vigilance. Constant reminders fuel greater vigilance. And if done right, talking to customers *more* often about identity theft can also present a powerful marketing and brand-building opportunity.

Reason #6

SMALL BUSINESS OWNERS ARE STILL IN DENIAL

I'm a small business owner and have worked with small businesses and Chambers of Commerce for years. The small business community represents a major vulnerability both to identity theft and national cyber security, yet most small business owners still don't consider data and customer protection a priority.

Small businesses in America employ an estimated 130 million workers, many of them daily using computers and mobile devices to work and to access customer data. That means tens of millions of Internet-connected devices with little security are being used by employees with little security awareness or training.

Those unprotected devices and employees are not just an easy target for the spread of malware and phishing emails, they're also very vulnerable to bots that can enlist those devices in attacks on other computers and networks – even targets of national security importance.

Reason #7

THIEVES ARE EMBOLDENED BECAUSE THEY KNOW THEY'RE UNLIKELY TO BE CAUGHT

Some studies have suggested that only one in every 700 cases of identity theft is ever prosecuted. While the punishments for identity theft can now be very severe, with stiff prison sentences for the worst offenders, the vast majority of identity theft cases go uninvestigated, unprosecuted, and unpunished. So even the most inexperienced thieves know this is a criminal career worth pursuing.

And that's given rise to a generation of Super Thieves - thieves who start out very small, maybe cashing fake or stolen checks. But when they realize how easy it is to make a few hundred dollars, with little risk, they up the ante. And keep upping it. Within a few years they know so much about the crime and how to avoid being caught, their crimes become far more costly. And they rarely even make it on to the radar of law enforcement.

Reason #8

CONSUMERS ARE STILL NOT CHANGING THEIR HABITS

In spite of repeated advice and warnings, most consumers are still not checking their credit reports often enough, not changing their passwords often enough, and not updating their software and devices often enough. And they're still nowhere near as cautious and vigilant as they should be, especially with their online habits. Bad habits create the biggest risks.

Reason #9

CONSUMERS ARE GIVING AWAY TOO MUCH PERSONAL INFORMATION ON SOCIAL NETWORKS

Study after study has shown that consumers are literally giving their information away to thieves, especially on sites like Facebook and Twitter. Information like birthdays, employers, family names and photos, friend connections, interests and hobbies are all immensely

valuable to identity thieves who need this information to successfully assemble a viable cloned identity.

Reason #10

BUSINESSES AND CONSUMERS ARE BECOMING IMMUNE TO DATA BREACHES

There are now so many publicized data breaches - an average of two every day according to the Identity Theft Resource Center - that consumers are becoming indifferent to them. But that's nothing new. The highly publicized data breach at retail giant TJX in early 2007 was one of the worst on record at the time, affecting more than 45 million customers and threatening the financial future of a chain of stores that includes TJ Maxx, Marshalls, and Home Goods.

Many experts, myself included, speculated that TJX would pay dearly for the incident. Customers would abandon the stores for fear their personal information could be exposed, and investors would avoid the brand because of the crippling fines and costs faced by the company. Yet in the 12 months immediately following the announcement of the breach, TJX never looked better. Revenues increased, profits increased, and their share price increased.

It seems like customers and investors were at least forgiving, but more likely just indifferent. And it was a clear message to TJX and other businesses that not only is a data breach no big deal any more, it may, like its close cousin identity theft, just be another acceptable cost of doing business.



INTERVIEW WITH A THIEF

Part 2 - "Check Fraud is easy for me"

THIS IS TAKEN FROM THE TRANSCRIPT OF AN INTERVIEW WITH IDENTITY THIEF "RAY" IN A CALIFORNIA JAIL IN 2014.

"If you take someone like me who makes it their business to know how checks are processed, how checks are made, how to obtain credit cards, how credit cards are used, how credit cards are paid off, you can exploit just about every facet of the process to make money.

Check fraud is easy for me. This is like Disneyland for me. I mean I can't believe how people readily accept checks. And it's simple if you know what you're doing. You're just going to use a valid ABA routing number, you're going to use a valid account number and you get these numbers in abundance in mailboxes every day.

I can go out and in 20 minutes get 10 personal checking account numbers. And 95% of the time, they're going to be good, so I just make a copy, use that same check number and go into Macy's with a driver's license and the machine is going to accept it every time.

I'll do probably two checks the first day. I may be able to get a third one. I may be able to get two the first day and then one the second day, but then they won't go anymore, so I just do two or three for each account. Like I said, I can get 10 accounts in 20 minutes.

How big a check would I write? For a store, \$500, \$600, \$700. And a store like Home Depot, you just go in

and you buy a \$500 Home Depot gift card. Write them a check for \$500. Some stores have better limits than others and you get to know the stores, you know. Target I don't like to go over \$350. Home Depot, I'll go \$600 on a check, and with a business check, \$700 or \$800.

Personal checks at stores is like just for fun, you know what I mean? It's hard to make real money doing it because you're just going to get a \$400-\$500 check. So if I were to go shopping at Safeway, I would never use cash, you know. If I had to go get socks and underwear, I'd never use cash. I'd just always use a check. If I needed a TV for the house, I'd never use cash. I would never even use a credit card, I'd always just use a check that I made.

Check fraud with the banks is even easier. Once you open that bank account, you're now their customer, right? I've seen some people, that are in this jail even, that find a check and they take it to a bank and they want to try and cash it, and they don't even have an ID or anything.

And you know the bank is really not going to want to cash that check. They usually end up calling the police because they can tell the person is not a real customer. But when you walk into a bank to open up an account, I'd walk in there and I give them \$100 for checking and \$100 for savings, and I give them a driver's license, they're so happy to open this account and their guard is down because they don't think that I'm in there to take their money. I'm giving them my money.

So you know they're happy to open this account. And then as soon as I get the ATM debit card - it goes to the PO Box in 5, 6, 7 days - now that bank's mine. Now I just start getting checks that have been stolen out of the mail, remaking them for \$10,00, \$20,000, \$30,000 sometimes.

The way it works, Company A sends an invoice to Company B for \$27,000 for goods or services that they ordered. And Company B sends Company A back a check for \$27,000.

Well, if I can get that check out of the mail or someone else can get that out of the mail and get it to me, I can make a copy of that, change the payee to the fake bank account that I opened up, and just deposit it.

Now, this Company A, they're not checking their mail every day for that check. So when the \$27,000 comes out of Company B's bank account, they're not tripping either because they wrote the check for \$27,000

but they just don't realize that somebody like me has diverted it. And usually, it takes about six weeks for these two companies to realize that the company they sent the money to didn't get the money and that someone else got it.

And by that time, you've already put in another couple of checks maybe for \$5,000, \$6,000, \$7,000 or even \$10,000, and that's it. I'm sure there's a reason for this, but I've never seen an instance in doing this for a lot of years, I've never seen an instance where the bank will set a trap for me.

Okay, eventually they know this is a fraudulent account and somebody's remaking these checks and depositing them, but when they do find out, the first thing they do is close the account. So as a precaution I would always first check the ATM machine before I walked into the bank.

If there was supposed to be \$12,000 in there and it said available balance was zero, I knew that account had closed and then I don't go in the bank. So very easy.

And if you know the equipment that you need to make checks, you can get it at Staples or Office Depot. They sell blank check stock and they sell magnetic ink. You can buy magnetic ink cartridges on eBay for 50 bucks.

Check writing software, you can get free demos online, and it doesn't cost you anything. You can steal the CD from Staples, you don't even have to buy it. You can buy it for \$29 or you can just steal it if you want. It's very easy.

I would sometimes go to casinos and print checks right in the parking lot of the casino. I'd run out of money, I'd come out, print a check, take it into the casino and cash it, you know. It's called riding dirty, an id factory in my car.

Sometimes I go to the same teller like three times with three different driver licenses, three different checks, and they just cash them. That happens a lot."



THINK SECURITY FIRST!

KNOW YOUR ENEMY

12 TRAITS OF HIGHLY SUCCESSFUL IDENTITY
THIEVES

Chapter 6

CHAPTER 6

Sometimes I keep questionable company for noble reasons. I've developed trusting, almost friendly relationships with some very accomplished and dangerous identity thieves. Even had them over to my home. And it's not because I get some kind of thrill from being so close to a strange kind of criminal underworld.

It's because I'm wired to be insatiably curious. I don't like identity thieves, and the havoc they can wreak on the lives of their victims. But in some cases I have found myself admiring their tenacity, ingenuity, and even work ethic.

So I figured that by hanging around some of them I might learn something valuable from them that could help others. From the thieves, investigators, and prosecutors I've met over the years, I've assembled what I think are some of the most surprising traits of the most successful identity thieves. The kind you really don't want picking through your mail or your garbage.

“ Yes, I am a criminal. My crime is that of curiosity. ”
Mentor, The Hacker Manifesto, 1986

1. They Work Hard

Contrary to the assumption that most thieves choose their career path simply because they don't want to get a proper job, successful identity thieves actually work harder than most of us. Sixteen-hour days are not unusual, especially if the thief is close to cracking a vulnerability, exploiting a security weakness, or about to snare a really lucrative victim.

And when drugs are involved, especially meth, a typical day can actually become two or three days with no sleep. Many of the most successful thieves use drugs like

meth, not for the high or for recreation, but often for the clarity, energy, creativity, and focus they unleash.

2. They're Very Patient

One thief explained how he would work a stolen identity for a couple of years. He'd apply for numerous credit cards with low credit limits, and very responsibly and diligently pay those cards off every month (using a phony address for the statements so the victim was never alerted). He would use that good credit management strategy to steadily increase the credit limits on the cards until they were perfectly ripe for a big hit. Then he'd max out the cards, often making \$20,000 or more, and abandon that identity for the next one.

3. They're Big Into Big Data But In A Smaller Way

The best thieves know that much of their crime is about the quality of the data they can get their hands on. Not just data about victims and targets, but information on vulnerabilities and weaknesses in financial systems that they can exploit before being discovered. So they're constantly gathering data from all kinds of sources – from other crooks, from professionals like forgers, from insiders and from hacker forums, even from fellow inmates – and then joining all the often very tiny dots to create the most accurate picture of their challenge.

“ I always think hacking is a little bit of a superpower. ... You can see through everyone's personal lives. ... The fact you can manipulate people because you can hack them and learn everything about their personal lives — that's an immense amount of power. ”

Sam Esmail, creator of Mr. Robot

4. They're Loners Who Tend To Play Well With Others

While many successful identity thieves choose to be loners in order to insulate themselves from others who might betray them, they're not antisocial. The best thieves are usually very charming, friendly, and charismatic. They interact well with other people, especially crooks, who can help them. They develop relationships with experts who can teach them. They use social engineering to find and flip insiders. And they can charm their way into and out of all kinds of situations.

5. They See Victims Differently

Many identity thieves get upset when they're forced to think about the innocent victims whose lives they've harmed. So to avoid their own guilt, they often shift the blame and responsibility to others.

One thief claimed that victims really should blame the system that makes their personal information so vulnerable, and makes it so easy for people like him to steal or spoof an identity. He also believed that he was doing victims, and society, a great big favor because he was exposing weaknesses and even lies that the public otherwise would never be aware of.

6. It's Not Just A Job Or A Profession But A Passion And Addiction

Successful thieves agree that while identity theft can be a full-time job, it works because it's more than that. In order to take the risks they do (getting caught in the big league can mean twenty years or more in prison), they need to be passionate about what they do. And that passion can often lead to addiction – to the thrill and the danger, or to the realization that even when a bank invests millions in security,

a kid who never finished high school can figure out in just a couple of weeks of late nights and creative thinking how to completely undermine that investment.

And many get addicted to the lifestyle – staying at the best hotels, driving luxury cars, gambling at the biggest casinos, and being treated like a high roller – and all at someone else's expense. One thief recounted how he and some friends spent more than a week at a luxury suite at the Ritz Carlton at California's Half Moon Bay, and on his way out convinced the valet to bring round an expensive Lexus he had spotted earlier in the parking lot.

7. They Make A Ton Of Money But Rarely Get Rich

The thieves I've spoken to have been very comfortable admitting that over their careers they've stolen millions of dollars. But most of that money simply flows away through the same fingers that steal it. Many successful thieves can be very generous, especially with family and friends. They can also be generous with those whose help they need – one thief told about how he would offer a brand new car to a complete stranger in exchange for a bag of stolen mail. The car was one of half a dozen the thief had rented using a stolen identity and had simply never returned.

8. There's No Mold To Break

Identity thieves don't follow a pattern, at least initially. In my experience they come from all walks of life, and depending on circumstances can be opportunists who stumble upon a quick way to scam a few bucks, will do it occasionally because they know they're not going to get caught, or they become professional and make a good living from it.

And maybe that's another reason identity theft is so hard to fight. There's really no usual suspect to pick out of a lineup.

9. They're Constantly Learning

Like most criminals, identity thieves understand that the more they know, the more they make. Not just knowing how to commit the dozens of different types of scams and frauds they have to choose from, but how not to get caught.

And prison isn't a deterrent either. In fact, it's a University and sometimes even a vacation. One thief I interviewed said he felt he needed a short dose of jail every now and then just to keep going. It was an opportunity to get his head clear, and get a break from the constant stress of staying a step ahead of the law. But most important, at least for this thief, jail was an opportunity to sharpen his skills by learning the latest tricks and scams from all the other incarcerated scammers.

10. They're Relentlessly Curious

Much like their close cousins the hackers, many identity thieves are relentlessly curious and driven to simply learn more – about the scams they're already pulling and scams they've never actually tried. One identity thief I spoke to said he would stay up for days at a time driven by the excitement of proving that a security system a bank had spent millions of dollars developing could be broken by someone like him.

11. They Enjoy The Power And Control They Exert

Another common driver for both identity thieves and hackers is the sense of power they feel being able to peer deep inside the lives of others, complete strangers, learn their most secret of secrets, and exert enormous control if they choose.

“ I had memos Hillary Clinton got as a State Secretary, with CIA briefings. These were being read by her, two other people from the US Government, and Guccifer. I used to read her memos for six-seven hours and then I’d get up and do the gardening in the yard.”

Guccifer, hacker

12. They’re More About Personality Traits Than Skills

The most successful (and dangerous) identity thieves I’ve come across stand out because of their personalities rather than any particular set of skills. Not that they don’t have some wicked skills – some have evolved from simple fraudsters to accomplished and very technical hackers.

But the key to their success is rooted in their psychological makeup, their wiring. Whether it’s their tenacity, their people (social engineering) skills, their analytical skills, or simply because they’re sociopaths, the most successful identity thieves are the ones who are simply wired for the job.

Know your enemy. That’s always the key to any defense. Knowing how the most dangerous identity thieves are wired might help you take the risk more seriously, and understand that while many identity thefts might be crimes or opportunity, many others are well and carefully planned. Think about that the next time someone tells you that identity theft is really no big deal.



THINK SECURITY FIRST!



DATA BREACHES AND IDENTITY THEFT

CLOSE COUSINS AND DANGEROUS LIAISONS

Chapter 7

CHAPTER 7

The leading cause of data breaches is mistakes by people. And the #1 motivation for data breaches is personal identity theft. Are you seeing the connection? It's all about people, people.

There's a well-known saying in security, attributed to many different sources but the same sobering message: *"There are two types of businesses in America – those that have had a data breach, and those that just don't know they have."*

Which might help explain why it seems like hardly a day goes by when there isn't another data breach in the news. That's because it's true. There have been an average of 2 reported data breaches every single day for the past five years. And that's just the reported ones. If you include all the other data breaches that are discovered but not reported, or simply never discovered at all, we could be looking at ten or even twenty times that number.

And there are no signs that data breaches are abating:

- According to the non-profit Identity Theft Resource Center, which has been tracking data breaches for years, there were more than 1,000 reported data breaches just in the first 9 months of 2018. That works out to an average of more than four every 24 hours. Think your data hasn't been exposed yet?
- In August 2017, security firm lookout published its own research on the latest data breaches, reporting that in just the first six months of 2017 more than 1.7 billion records were exposed in data breaches.
- And what kinds of records? According to Lookout, email addresses (in 39% of breaches), financial information (in 31% of breaches), phone numbers (in 26% of breaches), Social Security Numbers (in 24% of breaches), dates of birth (in 22% of breaches) and passwords (in 19% of breaches).

“ According to the Annual Data Breach Report from security firm Gemalto, which has been tracking data breaches for years, more than 13 billion data records have been exposed since 2013 with identity theft being the leading type of data breach accounting for 64% of all data breaches. And 75% of those breaches were in the U.S. ”

Some of the breaches have been massive and scary:

- In 2013, a data breach at Target Stores exposed the personal information, including email addresses and credit card numbers, of more than 70 million people. And it was all triggered by just one employee clicking on an email that hid some malware allegedly created by a teenager. Ouch!
- Data breaches at just two healthcare companies in March of 2015 exposed the Social Security Numbers of one in every two adults in America.
- Between 2003 and 2006, hackers stole more than 200 million credit card numbers by hacking into companies like TJ Maxx, Dave and Busters, and Heartland Payment Systems. All they did was cruise by their offices at night looking for networks that had no passwords. In many ways, not much has changed.
- In September 2017 Equifax announced one of the biggest data breaches in history, exposing detailed personal and financial records of nearly 150 million people.

So Why Should You Care?

- Each data breach helps hackers join the dots, and create a more complete and financially useful version of your identity.
- Even something like an email address can be of value to criminals, because if they can associate you with a company you already do business with, they can easily trick you into falling for a scam like phishing.
- Some reports in recent years from the non-profit Identity Theft Resource Center have found that close to 40% of exposed records have included Social Security Numbers.
- If hackers get a password for one account, they can easily find if you're using the same password for other accounts. And I know you are!
- Hackers are increasingly targeting healthcare companies and medical clinics in search of medical identities. And medical identity theft can be much harder to fight than other forms of identity theft.

If Data Breaches Make You Yawn, You May be Suffering From Breach Fatigue

It's been more than four years since I first used the term breach fatigue. It was in an interview with a bank security publication and hot on the heels of the massive Epsilon data breach. What's an Epsilon, I hear you scream? Exactly my point. Even though the Epsilon breach was considered absolutely massive at the time, losing 60 million customer email addresses doesn't seem like such a big deal anymore. Which might explain why so few consumers even recall the name Epsilon any more.

Since that interview I've watched the term breach fatigue used with increasing frequency. And despondency. So much so that it now looks like it's actually a thing, a phenomenon, and a real worry about the future of data security and privacy.

The idea behind breach fatigue was simple. The more breaches consumers go through, without experiencing any direct and tangible financial consequences, the less likely they are to care or worry about the next breach. And the next one. And the one after that. To the point that data breaches won't even be news to anyone any more. And that could result in huge risks all round.

“ According to insurance firm HSB, a third of Americans have reported receiving a data breach notification

”

Back in 2014, a company called Software Advice conducted a study of more than 4,000 U.S. adults to try to measure their awareness and recall of major data breaches, and the news didn't really surprise many. For example, the study found that only two of the top breaches that year actually registered higher than 23% awareness. And a whopping 77% of those interviewed were completely unaware that eBay had just had a massive data breach about a week before. Even though it affected nearly 150 million individuals.

The report also found that less than 15% of consumers surveyed were actually aware of that year's other highly publicized breaches at Michaels Stores, PF Changs, Neiman Marcus and even JP Morgan Chase. If such a lack of awareness existed then, imagine how bad it must be all these data breaches later?

The Consequences of Breach Fatigue

For the consumer, breach fatigue is likely to only increase complacency and apathy, and at the same time reduce concern and vigilance. Consumers are already beginning to tune out news of even massive data breaches, especially as they look down each time and realized they're not injured. They're less likely to respond, to beef up their vigilance, and equally less likely to alter their behavior or change their habits.

Consumers are also more likely to ignore any alarms, alerts, or notifications, and less likely to demand or accept offers of free credit monitoring or identity protection. A number of studies have indicated that in the aftermath of a data breach only between 5% and 8% of affected customers accept offers of free credit monitoring.

After all, if they're not hurt, they don't need first aid, right? Most importantly, they'll be too tired and cynical to be outraged anymore. They're more likely to believe and forgive – that data breaches are inevitable no matter how much money is invested in security. And without that rage, nothing has even a chance of changing.

And what if the sense of fatigue infects other security challenges, like identity theft and bank fraud? It's already a challenge to get consumers to take these risks seriously enough – getting consumers to take even basic precautions like passwords seriously is a perfect example. Will the cynicism of fatigue result in consumers not caring as much about their passwords as they should, not checking their statements as often or as carefully, not being as vigilant or hygienic when it comes to malware?

“ Who hacked my Honda? A 2016 survey by KPMG found that the majority of car companies, 85%, had experienced some kind of cyber attack in the previous 24 months. ”

Your Very Own Personal Data Breach?

As increasingly powerful malware plunders and pillages its way through the checkouts and databases of businesses across the land, there could be a very vicious version of the same plundering coming to a village near you.

How worried are you about malware? I mean really worried? It's not quite the same as identity theft, right? I mean, it can be a real pain and disruption, but it's not going to change your life in the same way as a bad case of identity theft.

If that's your position, like it is for most consumers, permission to change your mind. Because malware is changing. And if you're not ready for it, it will change your life.

Banking Trojans are a great example. They first emerged a few years ago and within months had managed to siphon hundreds of millions of dollars from consumer bank accounts.

Banking Trojans are a very nasty type of malware because if created properly they're usually able to bypass your antivirus software. Worse than that, once installed on your computer they can then mimic your current antivirus software and pretend that everything's OK. They can even block any attempts by your computer or antivirus software to update their security. Once on your computer, the more advanced banking Trojans will grab your bank login and password, and then log in to that account at the same time you do. Which means that when your account has been emptied, all your bank sees is the exact dates and times you logged in, and no one else.

And that can often leave victims with a big fight on their hands. And if you're a small business owner, it's a double whammy. That's because zero liability and other consumer fraud protections don't usually extend to small business accounts. If a hacker takes everything you have, chances are you're never getting it back.

And that can be devastating. The security landscape is now littered with small businesses, non-profits, and local governments that have lost hundreds of thousands and even millions of dollars to banking Trojans, and never got it back. For some businesses, it's a death knell.

And while banks have no choice but to make their personal customers whole, they're often not as worried about their small business customers. Many banks are not warning their small business customers that their bank is not liable for any losses through malware or other frauds. But they're also not warning their small business customers that the risks even exist, and most banks are not giving their small business customers the tools to defend against these threats.

In a recent study of the Russian cybercrime underworld, at least five major criminal gangs were identified as specializing in banking Trojans, and more specifically in the creation and distribution of mobile banking Trojans.

So there you have it. Highly sophisticated malware that can easily sneak on to your computer, circumvent security, and steal everything you have. And maybe leave you with little recourse. Still not worried?

“ Research firm Javelin Strategy and Research estimated that as far back as 2012, U.S. consumers saw nearly \$5 billion stolen from their bank accounts by malware. In a world of big numbers, even \$5 billion is not small. Things haven’t improved much since. ”

So What Should You Do About Breaches?

If you were actually an affected customer:

- If your credit card or debit card were exposed, keep an eye on your statements. You won’t be liable for any fraudulent charges so don’t panic if they pop up.
- If you used a debit card, keep an eye on your bank statements and change your PIN. And try not to use debit cards in the future. They create a bigger risk than credit cards.
- If you have or had an online account with the breached business, change the password and be on the alert for any suspicious emails.
- If your email address was exposed, be very vigilant for any emails, and especially emails claiming to be from the breached business and offering some kind of assistance. If you get an offer of free monitoring, for example, don’t click but go directly to the website instead.

- If your Social Security Number was exposed, freeze your credit reports immediately. That's the easiest way to close down the biggest immediate risk. My chapter on freezes and alerts will explain the process.

Even if you're not directly affected by the breach:

- Be suspicious of any emails in the following days and months that claim to be from that business or about that breach. Hackers and spammers are going to have a field day with all the media coverage.
- Don't wait to be offered credit monitoring or identity protection. A growing number of firms now offer free basic monitoring and protection, including Civic, Credit Karma, Credit Sesame, and Transunion. So get proactive and get protected before something bad happens.
- Use every data breach as a reminder to catch up on all those security housekeeping chores that we all now have to live with – change your passwords even if they weren't affected or you're not a victim; check your credit card and bank statements thoroughly for any unusual charges; be vigilant for suspicious emails; and keep a very close eye on your credit.
- Don't stop shopping at the breached business. All you're doing is hurting the thousands of employees who had nothing to do with the breach, and playing into the hands of the hackers.

By doing all these simple things, you're actually making things harder for the thieves. Because the more locked-down and vigilant you are, the harder it becomes for these thieves to use the breached information against you.



THE BREACH FILES

Did the Chinese Breach the Government's HR Department?

IN 2015, THE OFFICE OF PERSONNEL MANAGEMENT, OR OPM, REPORTED PUBLICLY THAT IT HAD BEEN VICTIM OF A DATA BREACH THAT MAY HAVE IMPACTED THE PERSONAL INFORMATION OF APPROXIMATELY 4 MILLION CURRENT AND FORMER EMPLOYEES. PRETTY SOON THAT NUMBER JUMPED TO 18 MILLION, AND A FEW WEEKS LATER TO 21 MILLION.

But it wasn't just the number of records but the types of data and employees. OPM is essentially the HR department for the Government, including many sensitive hires, and its personnel records are amongst the most coveted.

The hacker haul was both massive and troubling:



It included the names, addresses, dates of birth, and Social Security Numbers of possibly every current and former Federal employee, as well as prospective federal government employees, and U.S. military personnel.



The haul included background checks and security clearance information. Because of the depth of some background checks, the hack also included information on family members, college roommates, foreign contacts, and psychological information and evaluations.

- The breach may also have exposed military records, veteran information, addresses, job and pay history, health insurance and life insurance information, pension information, and data on age, gender, and race.
- 5.6 millions sets of fingerprints were stolen.

Numerous investigations have suggested that the culprit behind the attack was the Chinese government. If that turns out to be accurate, it raises many tricky questions, not least of which is why the government of China would be interested in stealing the Social Security Numbers of so many Americans. Does it plan to clone a few million credit cards and go on a spending spree? Buy an aircraft carrier? Perhaps start applying for fraudulent tax refunds?

What we may be seeing instead is a troubling pattern, and a new focus in hacking, espionage, and sabotage. As one expert put it, China wants to be everywhere, and is aggressively using hacking and data theft to gain social, economic, and political superiority.

Armed with SSNs and other employment information, the Chinese would be in a much better position to obtain detailed financial records which they could then use to identify government employees they might be able to exploit. For example, they could target employees who might have financial or health issues, or embarrassing spending habits, that could be exploited through entrapment and blackmail.

Or they may use that information to identify family members who could be exploited in the same way. And it's far from the first time. The hack attack against the U.S. Post Office last year that exposed the personal information of more than 800,000 postal employees was believed to originate in China too and part of an intelligence gathering campaign.

The Chinese have always used hacking as a propaganda weapon, to embarrass the United States and expose its security weaknesses. And major public hacks like this can also be used to create worry and turmoil that can chip away at consumer confidence and cause economic damage.

Many experts believe the same hackers were responsible for the massive attack on Anthem Healthcare just a couple of months earlier that exposed the Social Security Numbers of nearly one in two adults in America.

The fears appear real and justified. A couple of years ago I served as security advisor to a Congressionally-mandated panel tasked with investigating the potential privacy and security risks of making the personal financial information of thousands of senior government employees available to the public.

The goal was to deter fraud and financial abuse by creating greater financial transparency. As part of the process we interviewed representatives of nearly 60 different organizations and agencies, including the intelligence community. The biggest fear was that foreign governments and criminal groups could use this financial information to identify and target vulnerable government employees.

As a result of our report, the idea was shelved, but it was a close call. And even if the Chinese government didn't use the information for direct financial gain, they would most likely turn a blind eye if one of their quasi-official hacking groups did so as a reward.

And if it turns out not to be the Chinese government, or the information was passed to cyber crooks, what then? It's very possible that this information might have been offered for sale on black market forums, added to other personal information to make the information of more value, given to other nations, or even laundered and sold back to legitimate marketing and research companies.



THINK SECURITY FIRST!



Fraud

THE FAKE, FAKE YOU

THE GROWING PROBLEM OF
SYNTHETIC IDENTITY THEFT

Chapter 8

CHAPTER 8

This Chapter was contributed by Brett Johnson – a leading fraud expert, speaker, writer, convicted felon, and a co-founder of Shawdocrew, the first major criminal forum where hackers and fraudsters could buy, sell, share, and learn.

Synthetic identity theft could be the most common type of identity theft around, costing businesses \$6 billion every year in losses, and yet you've probably never heard of it. A Synthetic Identity, or CPN (Credit Profile or Credit Privacy Number) is a form of fraud, typically using elements of identity theft, used to create "ghost" credit profiles among the three major credit bureaus, Equifax, Experian, and TransUnion.

How Synthetic Identity Theft Typically Works

A cyber criminal goes to one of the many online criminal bazaars and finds a vendor who traffics in the stolen identities of children. These identities typically sell for \$1-\$3 each, depending on the time of year they're purchased. For that price, the criminal can get the child's name, Social Security Number, and date of birth. Typically, criminals are looking for very young children, the younger the better, because that increases the fraud possibilities.

Specifically, what the criminal needs most is the Social Security Number or SSN. This is the main piece of data used to create the synthetic ID. This is where the synthetic part comes in – the criminal will use the real SSN but a completely different name and date of birth. It's like they've created an entirely new and fictitious person. Now, it's important to note that this isn't the only way synthetic IDs are created. Other methods include using ITINs, or Individual Taxpayer Identification Numbers, and also using completely generated numbers that match the SSA issuing structure. But using the identity of a child is most successful and popular.

Let's Discuss How Credit Profiles Work

When you're born, the three major credit bureaus don't know you exist. In fact, they don't know you at all until you do something in your life that triggers a credit query with one of the credit bureaus. Typically, when an individual starts entering adulthood, they apply for a credit card, utilities, a smartphone, or similar, in their own name and Social Security Number. The first time the person applies for credit, a request is sent to one of the three credit bureaus for

a credit check. If this is the individual's first time ever applying for credit, the return response is "No Record Found."

This means that the individual, as far as the credit bureau is concerned, has never had any credit in their life. So the credit bureau reports this. But in doing so, the credit bureau now triggers a new credit profile in the name of that person. Simply by applying for credit for the first time, even if it's rejected, automatically creates a credit file.

And criminals can use this loophole to their advantage. If completely new data is presented to a credit bureau, including name Social Security Number, and date of birth - it creates a brand new credit profile that an experienced criminal can exploit.

One of the major problems here is that credit bureaus and credit issuers don't automatically verify the SSN against the Social Security Administration database. It is an easy fix, but something that hasn't been implemented and isn't even on the horizon to implement. Because of this, the credit bureaus simply don't know if the information submitted to them about the individual is accurate or not. The bureaus make the profile only with the information presented as long as the information isn't already in their system.

Using a child's SSN ensures that no one is likely to complain. At least not for many years. If the criminal uses the SSN of a 2-year-old, for example, it could be 15 years before anyone knows a crime was ever committed. By that time, the trail will have grown cold and there's probably nothing to investigate. Law enforcement likely won't follow up on it because there's nothing to follow. The crook has gotten away. The result? The kid who is now an adult is likely saddled with the disastrous consequences of massive debt and delinquencies that could take a LONG time to fix.

Which brings us to another problem. Currently there are no nationwide mechanisms to protect children from identity theft. It isn't a difficult problem to solve. A credit freeze can be placed on a child's identity as easily as on an adult's. Currently this requires the actions of a parent. A growing number of states have passed measures that make it easier to freeze the credit files of a child, but for a parent to do it on their own can be a chore.

Which Brings Us To The Next Level Of This Crime

So the criminal now has a ghost in the system. He has created a fictitious person using some real elements and posted it with at least one of the credit bureaus. The problem for the criminal is the ghost credit profile has absolutely no credit or credit history. As such, it isn't really worth much to someone trying to commit fraud. The criminal needs to do a number of things at this point for the intended fraud to ultimately be successful.

Here is where I decline to state what some of those "things" specifically are. It is not my intention to walk would-be criminals through the process of committing synthetic fraud. I simply want to illustrate how easy this fraud is to perpetrate and how easy it is stop, given proper legislation and security. And that part of the story is for another day.

But the payoff for the crook? Anywhere from a few grand to many thousands of dollars. It all depends on the patience of the criminal. If the criminal takes his time, obtains real credit cards, pays off those credit cards over a few months and builds a detailed credit history, then the criminal may ultimately walk off with well over \$50k from just one profile. A professional could be building and grooming dozens of similar profiles at the same time. All they need is the right data, and the thousands of data breaches annually generate an endless supply of cheap data.

This type of crime is ideal for fraudsters. The fraudster controls everything about the profile because he created the profile. He can answer all security questions. And no one EVER complains. At least not for many years. This is the reason that Synthetic Identity Theft may now account for over 80% of all ID Theft. It is extremely effective."



THINK SECURITY FIRST!

INVASION OF THE BODY SNATCHERS

THE GROWING MENACE OF MEDICAL
IDENTITY THEFT

Chapter 9

CHAPTER 9

Of all the forms of identity theft your body can be exposed to, medical identity theft will make you sickest of all. That's because medical identity theft can be very costly, very time consuming to fix, and have a very detrimental affect on your healthcare and coverage.

While the average cost of identity theft to the victim is just a few hundred dollars, the average cost of medical identity theft is more than \$13,000, according to a Ponemon study in 2015. And instead of just a phone call to a credit card company to make it all go away, resolving medical identity theft can take months if not years.

And it's only going to get worse, as medical records have become the most valuable commodity on the hacker black market often selling for 10 or even 100 times what a credit card number might fetch.

“ Chances are, your medical records are already in the hands of criminals. A study by global consulting firm Accenture in February 2017 found that a staggering 1 in every 4 U.S. consumers have had their medical records exposed or stolen in breaches. ”

And as if medical identity theft wasn't creepy enough, imagine if the thief were a foreign government. In March of 2015, two data breaches alone exposed the Social Security Numbers of one in every two adults in America. One of those breaches was at healthcare giant Anthem, where personal, financial, and medical records of more than 80 million Americans were stolen by hackers. That information also included names, social security numbers, e-mail addresses, birthdays, street addresses, member IDs, and employment information.

A two-year investigation concluded that the likely culprit was a foreign government. And while China appears to be the prime suspect, no one seems to know for sure. But it's certainly a

scary notion that some foreign government would go to such lengths to find out the medical histories of so many Americans. And how did the attack happen? A single employee clicked on a single email that opened their computer to malware, and that's all she wrote.

Medical identity theft may be set to explode in coming years as more criminals get their hands on more medical data, and start using it to defraud a healthcare industry that seems to have no clue how to respond. And as that stolen data filters its way through the criminal underworld, it may soon surface at a healthcare facility somewhere in America and pretending to be you.

“ In the first half of 2018 there were at least 351 reported healthcare data breaches in the U.S, according to Government records, affecting 6 million patients. Medical data breaches have grown...”

So why do people commit medical identity theft? It's not like opening a fraudulent BestBuy account and buying a bunch of high-end electronics, or walking away with thousands of dollars in a fraudulent tax refund courtesy of the IRS.

There are three main drivers behind medical identity theft:

1. To get coverage for care or procedures the thieves can't afford to pay for themselves.
2. To fraudulently obtain prescription pharmaceuticals, and especially highly protected prescription medications like painkillers and anti depressants.
3. To commit billing fraud by billing Medicare and other insurance programs using phony identities.

So What Can Happen If You're A Victim Of Medical Identity Theft?

- A complete stranger could end up getting medical treatment or having a medical procedure in your name. Think of what that could do to your medical history and credit.
- It could take years for you to resolve the case – there's no 800 number you can dial to undo medical identity theft and the healthcare community has no simplified process in place to assist victims.
- Your own medical and healthcare records can become contaminated with those of the thief, which can lead to all kinds of health, financial, legal and insurance complications.
- You could be denied urgent treatment when you need it most, see your premiums go up because of the risk you appear to pose, or be denied coverage altogether.

Unlike other forms of identity theft, the out-of-pocket expenses for victims of medical identity theft can be very high, and with very little resolution. According to the Fifth Annual Study on Medical Identity Theft, released by the Medical Identity Theft Alliance, more than 65% of medical identity theft victims had to pay an average of \$13,500 to resolve the crime. Most victims of non-medical identity theft pay little if anything out of pocket.

“ While most non-medical identity thefts can be cleaned up quickly and without any lasting damage, only around 10% of victims of medical identity theft report a satisfactory outcome.

The Medical Identity Theft Alliance

”

But it's not just global cybercriminal empires we have to worry about peering into our most private parts. I came across a case where one lone and low level identity thief was found with more than half a million stolen identities in his hotel room. That's more than the entire population of the city of Miami.

And where did he get this treasure trove? Apparently the non-hacker found it surprisingly easy to hack into the networks of a local group of small healthcare providers. By the time he was caught he had already used that information to rack up more than \$1.5 million in fraud charges.

So What's A Body To Do?

Sadly, the news gets worse. In the good old days, it was usually easy to round off an identity theft story with *"here are five great tips that will protect you."* Unfortunately, there's not a lot you can realistically do to prevent medical identity theft. You can't refuse to provide the information that the healthcare industry demands from you because they'll simply refuse you care.

You could ask your healthcare provider how they protect your information but in response they'll probably quote all kinds of security and privacy regulations to tell you to mind your own business. You could check your health records and explanation of benefits, but that will only tell you that your horse has already bolted and welcome to the world of victims.

You should be checking your credit reports regularly anyway, but if the fraudulent care or procedure has been paid for by insurance, it's only likely to appear in your credit reports after it's gone into collections.

One of the best and most effective prescriptions is to **freeze your credit**. It's not a cure, but it could close down many of the simplest forms of medical identity theft.

And What Can You Do If You're A Victim?

- Ask the provider, the organization claiming you received treatment, for all the files they have. By law you're entitled to the information, but the healthcare industry can have some stifling privacy rules. Be pushy.
- Try to figure out exactly what kind of information the thief used. Did they have your Social Security Number, date of birth, maybe your insurance and family information?
- Collect all your information, get a police report, complete an identity theft affidavit, then contact whatever company is making the claim and start the dispute process.
- Keep a copy of everything, and a record of every response, conversation, email etc.
- Contact your insurance provider and ask them to remove any records or treatments associated with the identity thief.
- Freeze your credit reports to prevent the thief from doing it all over again.



A VICTIM'S TALE

Who Swatted Ashton Kutcher?

"Sarah" is a hard working young woman in her early twenties with a good credit history and no criminal record. She found out she was a victim of identity theft while she was in the middle of a deployment to the middle east as part of her young military career. Her family had been contacting her about a growing number of calls from debt collectors over debts she knew nothing about.

Fighting identity theft from a faraway land while on military service is no easy challenge, but Sarah had little idea how much more challenging her case was about to become. Google your name, was all her friends said. When she did, the very first search results were a list of hacker forums containing detailed dossiers on Sarah and every member of her family.

Someone had gone to great lengths to research and document vast amounts of detailed personal information. And once posted in public forums, identity thieves didn't hesitate in exploiting that

- information. The files included
- Detailed personal and financial information on at least six family members.
- Full dates of birth for all and Social Security Numbers for three.
- All home addresses for the last 20 years.

- Multiple email addresses and accounts including passwords.
- Multiple bank accounts including routing numbers and passwords.
Multiple credit card accounts.
- Account numbers and passwords for FasTrak, PayPal, Comcast (even the router serial number) and Verizon.
- Detailed vehicle and driver information, including driver's licenses (with photocopies) as well as make, model, year and registration for three family vehicles.
- 10+ phone numbers and 20+ email addresses.

As a result of those postings:

- Every single family member has been a victim of multiple identity thefts.
- More than 100 fraudulent accounts were opened in Sarah's name.
- Her old address was swatted by a SWAT team looking for her.

She and her new husband were not only turned down for their first mortgage, they were told they would likely never qualify for a mortgage because of the high risk she presented to lenders.

And forget zero liability. The thieves went on a spending spree at one well-known jewelry chain, making purchases of more than \$120,000 using Sarah's identity. And in spite of a mountain of evidence that she was the victim, the jewelry chain ignored those claims and vigorously pursued her for payment.

Sarah has been fighting her case for more than six years now. So who would go to such lengths to try to destroy an entire family? My digging pointed to a 12-year-old wannabe hacker who had a childish online beef with one of Sarah's siblings. The same 12-year-old who may have also "swatted" the homes of Ashton Kutcher and Justin Bieber.

And maybe that's the scariest part. That a 12-year-old had the skills, patience, and determination to gather so much supposedly private and even secret information from so many supposedly hard-to-crack places. Or maybe such things are now so easy, a pre-teen could pull it off. But the next time someone tells you that victims of identity theft are not really victims, I have a 12-year-old who would like to disabuse them of that notion.



THINK SECURITY FIRST!

TAXES

THE TAX THIEF COMETH

PROTECTING YOUR IDENTITY AT TAX TIME

Chapter 10

CHAPTER 10

Tax season is identity theft season. For most thieves, tax time is harvest time. It's like Black Friday and the Christmas Holidays are to retailers, and where many thieves make the bulk of their yearly earnings. In fact, it may even be the single biggest source of profits for many identity thieves.

A couple of years ago the IRS admitted in testimony before Congress that in spite of all its precautions it would likely pay out close to \$5 billion every year for the next few years because of tax related identity theft.

And why is that? Blame it on a badly broken system. Identity thieves figured out a long time ago that all the IRS needed to process a tax return and pay a refund was a name and matching Social Security Number. For whatever reasons, the IRS never bothered to look out for red flags that might suggest a tax return was really just a fraud.

Living at different address this year? No problem, the IRS didn't notice or care. 500 refunds being sent to the same address? Nope, no alarm bells at the IRS. Worked at the same job for the last thirty years, yet last year you completely changed your career path, doubled your deductions, attended college, and went from zero kids to a gaggle of six or seven. And all in less than a year. Think the IRS could tell something about that sudden and dramatic change in lifestyle warranted a second look? Well, apparently not.

In fact the IRS has been so overwhelmed (and probably underfunded) that the agency admitted that in spite of increased vigilance it would still lose billions of taxpayer dollars to identity theft.

And the thieves are taking full advantage of even the slightest weaknesses. In just one of thousands of cases, prosecutors charged at least sixteen people from the New York area with running a massive identity theft ring that made its money from filing fraudulent tax returns.

Prosecutors claimed that the gang had stolen the identities of more than 11,000 people, opening up 3,500 bank accounts in more than 400 financial institutions. The thieves used that elaborate network to file fraudulent tax returns for close to \$38 million, of which more than \$10 million was actually paid out. The scheme only unraveled after a vigilant employee at a small credit union spotted an anomaly and reported it to the FBI.

“ In January 2017 the IRS announced that it would have to delay refunds to around 40 million families so it could better weed out identity theft. ”

But that case is small fry. Check out my chapter on Operation Rainmaker where a gang in Florida filed fraudulent tax returns amounting to more than \$120 million. Police only got suspicious when they noticed that small-time drug dealers were disappearing from street corners. Turns out the drug dealers had gone back to school. They were busy attending seminars at local hotels that were hosted by other drug-dealers-turned-identity-thieves who were teaching their criminal audience how to use tax filing software like Turbo Tax to file for millions of dollars in bogus refunds using stolen personal information.

And where are the thieves getting all the information to file so many fraudulent returns? Think data breaches. Like 1,000+ data breaches every year that expose millions of records to hackers. In the first six months of 2017 there were already more than 800 reported data breaches, exposing millions of personal records. And the #1 motivation for the attacks? Identity theft.

“ We did a lot of tax fraud in San Quentin. We lived pretty well in prison by just doing the IRS tax fraud. My girlfriend would go to Office Depot to get packs of W-2 forms, and bring them into prison hidden in paperwork, pretending to be an attorney. We would recruit other inmates, get their Social Security Numbers, give them \$500-\$600. We would file each return and get \$4,000, sometimes \$5,000 each. They’d never know how much we were making. ”

Ray, convicted identity thief.

But it's not just data breaches you have to worry about, because many data thefts that lead to identity theft happen much closer to home. When I spoke to a notorious identity thief who was nearly finished serving a lengthy sentence in Northern California, he said that tax time makes people like him giddy, even itchy.

He talked about hiring strangers to spend tax season wandering through neighborhoods stealing mail and checking trash. Once he found a good target (and he said he could find upwards of twenty on a good weekend), he would eventually be able to piece together enough information to start filing bogus returns.

And the news is not good for victims who find that the IRS has rejected their tax return. Only a couple of years ago, victims of tax refund identity theft could still expect to get their refund within a month or two. Today, victims can expect to wait a year or more for the IRS to investigate the fraud and issue a new refund.

And as if the news couldn't get any worse, the IRS recently announced that as a result of budget problems, it expected more cases of identity theft, less help for victims, and an even slower response to claims of identity theft. The average time to resolve an identity theft claim with the IRS is now estimated at 278 days, according to USA Today.

So What Do You Need To Watch Out For?

Each year we see thieves become more creative and sophisticated, with scams that could fool the most cynical and vigilant consumer. Here's just a selection of the most common:

Bogus IRS Calls

These can come in the form of either live (a real person) or automated phone calls purporting to be from the IRS and accusing you of something you didn't do, or asking for clarification for something they claim you did.

For example, some scams will claim that someone else has already filed tax returns in your name or Social Security number. Or that the IRS has multiple addresses for you, you're not listed with the employer you claim, or your taxes are being withheld because of unpaid

child support. The scam is usually focused on tricking you into revealing your Social Security Number in order to clear up the matter.

Bogus Refunds

These scams take the same format as the one mentioned above - usually a phone call or an email - but instead focus on reasons why you won't be receiving your refund until certain discrepancies have been cleared up. Like your full name, spouse's name, Social Security Number etc. A variation of this scam requests bank account information in order to direct deposit your refund (and threats of long delays if you choose not to direct deposit), or that a random review has found that you were underpaid in your last refund.

Dishonest Tax Preparers

Your choice of tax preparer could get you in trouble too. It might surprise you but if you have your taxes prepared by one of the large tax preparation services there's a good chance that your returns will be completed in Mumbai or Bangalore.

India is one of the world's top locations for outsourcing everything from customer support to telemarketing, and it's now also popular for outsourcing tax return preparation. And despite the security precautions your tax firm may take, they may have little control over the security and privacy of your data in a country that has very different privacy laws.

You also need to be wary of dishonest tax preparers much closer to home. In one incident a woman left her tax preparer's office only to find out when she got home that she had left her documents with the tax preparer, including her Social Security card, driver's license, and bank documents.

But when she returned to collect the documents the preparer denied any knowledge of them. The tax preparer was later charged with identity theft when he used the stolen documents to withdraw \$2,500 from the victim's bank account.

“ In February 2017, investigators uncovered a hacker website with a special section devoted to selling stolen W-2 tax forms. The data for sale included taxpayer’s employer name, employer ID and work address, taxpayer address, Social Security Number and information about 2016 wages and taxes withheld. ”

Mail Theft

Another common tax scam focuses on your mail. In one scam, a thief created a company called “MRS” and at tax time spent her time raiding mailboxes in numerous neighborhoods. Wherever she found checks made out to the “IRS” she simply changed the “I” to an “M” and lodged the checks in her own bank account.

In total the thief netted around \$500,000 and by the time the IRS notified the victims months later that they had not received their tax returns, the thief and her company were long gone.

Phishing

Phishing schemes abound around tax time, as consumers are bombarded with all kinds of emails offering free tax preparation, faster refunds, requests for donations from bogus charities, threats from the IRS and so on.

You should even expect bogus emails purporting to be from your bank or credit union notifying you of anything from *"Your refund has arrived early...Please click here to view it."* (they're after your bank account information and password), to *"Your refund check from the IRS has been rejected by your bank because of an accounting error. Please confirm your bank account number."*

So What Can You Do To Protect Yourself?

- Be suspicious of any calls or emails purporting to be from the IRS, no matter what the issue. The IRS will always write to you first and will never call or email you.
- Never give your Social Security Number or bank account details by email or over the phone unless you're absolutely certain about who you're talking to.
- Be wary of any calls asking that you confirm your tax information or employment status and especially if either your bank or employer have recently been acquired.
- Guard your mail, because it's especially attractive at tax time. Ideally have your mail delivered to your front door and not to a curbside mailbox. Collect your mail as soon as you can and avoid putting your returns in a curbside mailbox for collection - take them to the post office instead.
- If you plan to use an online tax preparation service, make sure you stick with a reputable one that has adequate security measures in place. Be wary of emails offering such services because they're often bogus, and be careful when typing in the URL or web address of an online service in case you misspell the name and end up on a fraudulent site that looks like the real one.
- Make sure your computer is free of malware that can steal a copy of your Social Security Number, bank account password, or previous returns.
- Choose your tax preparer carefully, and don't be afraid to ask them important security questions - like how your information is protected in their offices during and after preparation, how long they keep a copy of your tax return, if they outsource any of their services, and whether they conduct background checks on their employees.

- If you plan to pay the IRS by check, spell out the name Internal Revenue Service because it's harder to forge than the letters IRS. And don't drop the check in a mailbox - take it to the post office. It's only once a year and is worth the extra effort.
- Avoid emailing tax information or returns to your accountant. Email is not a secure way to send any document.
- If you make copies of your return on a photocopier, be aware that many machines keep a copy of your pages in short term memory. Not so good if you use a photocopier in a public location.
- Don't forget to shred any unnecessary documents or copies when tax season is over.
- If you plan to keep a copy of your tax return on your computer, make sure it's password protected and encrypted to protect it from prying eyes and malware.
- And check your credit report immediately after tax time and a few months later too, to make sure that if your personal information was stolen it's not being used against you.



THINK SECURITY FIRST!

THE MOST VULNERABLE IDENTITY

PROTECTING THE ELDERLY FROM
IDENTITY THEFT

Chapter 11

CHAPTER 11

When I started the Identity Theft Council in 2009, one of the first cases I investigated involved a frail woman in her late 80s who had been a victim of a massive fraud totaling nearly \$250,000. Multiple accounts had been opened in her name, her Social Security benefits had been diverted and stolen, her bank accounts emptied, two vehicles were purchased using her identity, and the home she hoped to retire to had been sold without her knowledge. She was now penniless and having trouble paying for some essential medications.

We were alerted by one of the victim's six children, who told me that the police were of little help. Investigators had suggested that rather than a crime, the entire issue was either a civil matter or that the victim was simply confused.

In a way they were sadly right. After a few months investigation we discovered that the culprits were actually her own kids, all at different times plundering their mother's funds, income, and retirement to pay their own bills and support their lifestyles.

Identity theft against the elderly has been called the silent epidemic because often the victims are too ashamed or confused to come forward. The elderly have always been a target for scams, but the growth of identity theft has only made the elderly even more vulnerable to all kinds of criminals with endless ideas for conning people most likely to trust them. And the emotional impact on victims can be devastating.

“ The True Link Report on Elder Financial Abuse in 2015 revealed that seniors lose \$36.48 billion each year to financial abuse ”

If you have elderly parents or care for the elderly, especially if they live alone, you need to play close attention to their vulnerability to identity theft. As far back as 2014, studies from both the Federal Trade Commission and the Bureau of Justice found that the elderly could represent as much as 10% of all identity theft victims.

Whatever the true number is, there's little doubt that the elderly are particularly vulnerable to identity theft and are likely to continue to be targeted by thieves. The cases I've come across are many and often tragic:

- A thief swindled two elderly women in North Carolina out of an estimated \$100,000 by simply calling the victims, claiming to be a representative of their bank, and persuading them to reveal their bank account numbers and passwords.
- An elderly couple had to spend nearly seven years recovering from an identity theft involving dozens of fraudulent accounts opened in their names at a cost of more than \$100,000.
- The frauds have not been confined to money, and there are a growing number of cases of food stamp id theft. Which can have a significant impact on the victim's health.
- In one case an elderly woman reported that her entire monthly food stamp allotment had been wiped out by a con man who called her on the phone and claimed to need her personal details to "re-certify" her in the food stamp program.
- Scammers are also posing as police officers or representatives of police charities to trick thousands of victims into handing over their personal information.
- The elderly are often victimized by people they know and trust, such as neighbors, friends, caregivers, and even family.

“ An employee at a Georgia nursing home was charged with stealing the identities of dozens of elderly victims, going on a spending spree and only getting caught more than a year after an alert family member got involved. ”

Targeting the Elderly

There are a number of reasons these heartless scammers target the elderly:

- They're more trusting, and less likely to be immediately suspicious of strangers.
- Many live alone, have no family to protect them, and are unable to resist high pressure tactics.
- Loneliness may make them more likely to welcome a stranger into their home.
- They often have great credit, a paid-off home, and plenty of equity for a thief to tap. And many elderly also keep large amounts of cash in their home.
- They're not naturally security savvy - they're less likely to lock away their financial information, shred credit card offers, protect their mail.
- They're more gullible to technology-based scams, like phishing, charity and lottery scams, and phone-based scams.

While the elderly are vulnerable to all types of identity theft and fraud, there are some scams more commonly targeted at this group, including:

- **Loan frauds** - where the thief takes out new loans in the victim's name. Many victims have found their homes have been re-mortgaged, or new home equity loans taken out, often by family members.
- **Utility fraud** - where the thief uses the victim's personal information to pay for utilities like phone service. For whatever reason, one of the first things id thieves do with stolen information is to apply for new cell phone service in the victim's name.

- **Theft of services** - where the victim's information is used to steal medical services, Social Security services, and even food stamps.
- **Account dripping** - where the thief takes just a little money from bank accounts and credit cards over an extended period - thefts that usually go undetected.
- **Account hijacking** - when a thief, family member, or caregiver gains control of the victim's bank and credit card accounts, pensions, and Social Security payments.

So How Can You Help?

If you're taking care of an elderly family member or friend there are many easy ways you can help reduce their vulnerability to identity theft and other scams:

- The best thing you can do is to be around and in touch. Scammers are less likely to focus on an elderly victim if they know a family member is close by and vigilant.
- If you know and trust their neighbors, ask them to get more involved and keep an eye open.
- If the individual is in a nursing home or retirement community, do your homework on the community, talk to the operators or managers about security, and encourage the individual to keep as little personal or financial information with them as possible.
- If the individual is in a nursing home, suggest that all mail be forwarded to you.
- Talk to them about the risks, give them a simple checklist of warning signs to watch out for, and encourage them to always call you before they buy something new, sign any legal or loan documents, or are pressured or harassed by any stranger.

“ My wife had a heart attack during that same time, so the stress factor was much more severe than normal. I had to take care of her, and I had to try to work all this other stuff in on top of that...and these guys that do that, they couldn't care less, you know. I can't understand how people can be so heartless. It's one of the worst nightmares I've ever been through in my entire life. ”

Elderly victim of identity theft in his own words

- Conduct a regular home audit, making sure that all financial documentation is safely locked away, and that any computers have adequate security in place and working.
- If home help or caregivers are involved, let them know that you're watching out for that individual and will encourage the prosecution of any crime. Run a criminal background check on any caregivers, home help, or anyone else that might have regular access to the home.
- If appropriate, offer to handle all financial transactions and account management for the individual, and have them refer any financial enquiries, proposals, or problems directly to you.
- Work with their bank and credit card providers so that they are also alert to any unusual activities or transactions on their accounts.
- Offer to check their incoming mail for suspicious offers, and to check their monthly bank and credit card statements to ensure there are no fraudulent charges or suspicious “drip” payments.

- Regularly check that the individual is receiving any Social Security benefits, pension payments, and health care they're entitled to, and that these entitlements or payments are not being diverted or misused.
- Remove them from direct mailing lists to reduce the amount of junk mail they receive.
- Encourage them to make payments for things like utility bills online so that checks are not stolen in the mail. But make sure you set up the payments so they don't make any costly mistakes.
- Consider placing a freeze on their credit reports to prevent any unauthorized credit. This freeze can easily be lifted if the individual wants to take out new credit.
- Check for any financial or utility accounts that are no longer used or needed and close them if possible.
- Help them to regularly check their credit reports and if possible set them up with a credit monitoring service with alerts sent directly to you.



INTERVIEW WITH A THIEF

Part 3 - *"I Really Destroyed This Guy's Credit"*

THIS IS TAKEN FROM THE TRANSCRIPT OF AN INTERVIEW WITH IDENTITY THIEF "RAY" IN A CALIFORNIA JAIL IN 2014.

"I came across this credit profile in a storage unit, a box of papers that had the gentleman's name and it was a very foreign sounding name...and his Social Security Number, date of birth, previous addresses.

Also in this box were financial documents that told me right away this guy probably had sufficient amounts of money in the bank and definitely had good credit. Which turned out to be the case.

From just using the Internet I was able to get some more information - previous addresses, his wife's name, mother's maiden name, whether or not he had kid, whether or not he had other family. You know, some websites will show you someone lived in this house, everybody else that lived in that house and how they're connected.

When I applied for the Visa card in his name, it asked me three questions like which one of these people is related to you and through those other social media sites and stuff, you can get the answers to those questions. So just be prepared.

So I ordered a Visa card in his name and I got a card with a \$7,000 limit. With that card, I made a driver's license. This was back when I started making driver's licenses. The reason I started

making driver's licenses was using these credit cards, for big purchases, people started more and more asking for a driver's license to go with the credit card and it got to be a real pain.

So I thought well, if the state and some civil servants can make a driver's license, why can't I? So I did some research, found out what equipment they used to make the driver's licenses, and found out that it's readily available if you know where to look. You can buy the same equipment that the state of California or the state of Texas can buy to make licenses.

It was very easy to make a driver's license to go with this gentleman's name. And I went down to Best Buy and got instant credit for I think another \$8,000. I then opened up three or four bank accounts in his name that I proceeded to run stolen business checks through. The biggest check that I ran through one of these accounts was about \$32,000. And that's just one account, one check.

I also ran other checks through that account, so on that one bank account that I got in his name, I probably did about \$45,000. The other three would've been less, but they were at least \$10,000 or \$12,000 in each one of those other three accounts.

The credit cards, the original Visa, I ran up the \$7,000 limit. It was a Target Visa, and then I took a check down to Target customer service, paid the \$8,000 bill off after I charged the card to the limit in four days. Paid the \$8,000 with a bad check. Got a fresh \$8,000 on the card, spent that, and then took another check down to Target customer service...paid that \$8,000 and was able to get another \$4,000 on that card before they shut it off. So that's \$20,000 just on that one Visa.

And then the Best Buy card, I spent all the same day that I got it. I bought a couple of big screens for friends of mine and I gave all that Best Buy stuff away.

I know there were more credit cards that I got in his name because I really destroyed this guy's credit, you know. And afterwards I thought about it because I had never gotten so much credit from one profile, and I was like, I felt bad and I didn't usually feel bad, I was sorry to say. You know, I didn't really think about the damage, the headaches it caused people.

I don't remember the exact cards I got, but it was like four or five credit cards, all with big limits and it was like man, they're going to make it hard for this guy to get his credit straight, you know.

But so in one profile almost \$100,000."



THINK SECURITY FIRST!



KEEPING YOUR KIDS SAFE

FROM IDENTITY THIEVES, DATA STEALERS,
PREDATORS, AND THEMSELVES

Chapter 12

CHAPTER 12

Youth might be wasted on the young, but Social Security Numbers are not. Kids and teens are a growing target for identity thieves and in large part because of the early creation of Social Security Numbers that can remain largely unprotected for years.

This single circumstance gives thieves plenty of time to get away with the crime – teens usually don't even check their credit until they're in their late teens – and it's still very difficult to monitor the identity of a child.

And in most cases, the thieves won't even know the identity belongs to a child. Many Social Security Numbers are stolen through burglaries and purse snatchings, but the thieves will have no way to telling who that SSN belongs to.

Which is why so often the thieves end up creating a synthetic identity – the Social Security Number of one of your kids combined with someone else's date of birth, address, and so on. And those identities will often work when the thieves use them to scam banks or credit card companies. And for most victims, they only find out when it's much too late, discovering years of fraud and debt the first time they apply for credit in their own name.

“ More than 1 million children were victims of identity theft in 2018, and two thirds of them were under the age of eight ”

The results of this kind of identify theft can be frightening:

- A 3-year-old whose very first piece of mail was a letter from a prosecutor informing him that his identity had been stolen.
- A 12-year-old girl who not only discovered that a bank account had been opened in her name, and in turn used to open numerous credit card accounts, but the culprit also declared bankruptcy leaving the girl and her parents with a legal nightmare.
- A 3-week-old whose stolen identity was used to purchase prescription drugs, leaving his parents to foot the bill.
- A 17-year-old Colorado college student who found out how bad his credit was when he applied for his first job, discovering that 10 years earlier someone had stolen his identity and purchased a \$40,000 boat.

Kids Are Great Targets For Many Reasons:

Parents don't always think to protect their kids' Social Security Numbers and cards and especially in the home.

- Parents don't think to check if there are credit reports in their kids' names.
- Kids can be gullible and easily fooled into revealing sensitive personal information.
- Kids can be careless with personal information online.
- The theft of personal information can go undetected for years -plenty of time for the thief to make a leisurely escape.

Do Your Kids Know What Their Digital Footprint Looks Like?

It's now more important than ever to focus on instilling in your kids what things like privacy, security, and sensitive personal information are and why they needed to be protected.

Kids of all ages must be programmed as early as possible to understand what a digital footprint is, how to hide their tracks, and how to make safe and sensible choices.

What can happen if they don't?

- Unscrupulous marketers can start grooming them early on to be obedient consumers of the future.
- Hackers can use them as a back door into the home and all its valuables.
- Perverts using tools created by hackers can infect computers and use webcams to spy on your kids and even bully or extort them.
- Social media can be used to spread scams and malware and infect others, and over-sharing of personal information could expose everyone in the family.
- What your kids say and do online now, what they search for and enquire about today, could be used against them for years to come. One single juvenile rant could ruin a college application or job opportunity.

Why Share So Much? Because They Can

The biggest risk for kids and teens sharing is simply because they can. According to a study from Pew Research Center in February 2015:

- Nearly three quarters of teens age 13 to 17 either have a smartphone or access to one.
- 91% of teens go online from a mobile device.

- 92% of teens report going online daily — including 24% who say they go online “almost constantly,”
- More than half (56%) of teens go online several times a day.
- 87% of American teens have or have access to a desktop or laptop computer, and 58% of teens have or have access to a tablet.
- 71% of teens are daily on more than one social media site, with nearly three quarters of all teens using Facebook regularly and nearly half using Instagram. And while more teens are beginning to embrace privacy and anonymity tools like Wickr, SnapChat, and YikYak, it's probably for all the wrong reasons. They don't realize that it's not their parents' scrutiny and surveillance they have to be worried about.

How Can You Tell?

There are a handful of ways to tell if your kids' identities have already been compromised:

- The IRS or Social Security Administration inform you of some discrepancies because someone else is working or claiming benefits using your kids' Social Security Numbers.
- You notice an uptick in mail addressed to your kids.
- Or in the worst case, debt collectors come calling and wondering why your 3-year-old skipped out on his massive phone bill or the apartment he'd been renting.

Early Intervention Is Key

- Get them used to the lingo and concepts like privacy, secrecy, anonymity and digital footprint. And sometimes the easiest concepts are best – bad people are watching and listening and snooping and so you have to hide to stay safe.

- Before you can teach, you have to learn. And ideally practice. How likely are your kids to wear seatbelts when they're adults if their parents never led by example?
- Security and privacy should be their default instinct. They have to be made to understand that it only has to be said once, texted once, or posted once to live forever.
- Introduce them to the Paranoid Consumer's Privacy and Anonymity Toolkit (hint: you're reading it). There are now dozens of free tools that will protect the security, privacy, and anonymity of every family member, on every device, every second of the day. And they do so automatically, by default, in the background. So make some introductions. There's a chapter on those tools in this book.
- Teach your kids and all family members about responsible passwording. That means creating passwords that are difficult to guess or crack, and making sure they don't get password lazy and use the same password for just about everything. Like maybe you do?
- Set rules and enforce them. It's like running a business. If you don't have a security policy, you have no guidance for employees to follow. Find a good balance both sides can work with.
- Teach them the mantra "Kick The Click." So many of today's threats rely on users, and especially kids and teens, just clicking on something they simply shouldn't have. If you don't click, you win.
- Remind your kids early of the connection between all these risks and their personal finances. With so many crimes focused on identity theft, identity protection has to be constantly on their minds. And money might just be the incentive they need.

- College-age teens should be warned about the dangers of leaving personal financial information around their dorm or on their computers.
- Watch where your kids go and what they do online so they're not duped into revealing personal information that can be used to steal their identity theft.
- Check that your kids don't have credit reports. If you don't check, years may pass before you and they discover the crime.
Check to see if your state allows you to freeze your kids' credit reports. More than half of all U.S. states now allow you to freeze the credit reports of your kids and my chapter on credit freezes will explain more.
- Place a fraud alert on your kids' Social Security Numbers. A number of identity protection vendors now provide this.
- Make sure your kids' school is not using Social Security numbers as student IDs. Many schools still do even though they know they're not supposed to.
- If your kids are active on social networks make sure you warn them to be suspicious about any requests, no matter where they come from, for personal or financial information. Theirs or yours!



THINK SECURITY FIRST!

SMALL IS BEAUTIFUL - TO IDENTITY THIEVES

PROTECTING YOUR BUSINESS FROM
IDENTITY THEFT

Chapter 13

CHAPTER 13

If you've ever dreamed of having the global media focused on your business, camped on your doorstep, scrambling for an interview, and hanging on your every word, then you might want to be careful what you wish for.

Most small business owners like to be in the news, but when the global media descended on the owners of a small Hauppauge New York software business one morning, it was for all the wrong reasons. The Feds had just announced to the national media that the biggest case of identity theft in American history had been traced to information stolen from that small business.

But as journalists and news reporters swamped the company with cameras and questions, the worst news was yet to come. More than 30,000 victims had their identity compromised as a result of personal credit information pilfered from the business, and the FBI identified the mastermind behind the crime as one of the company's own 65 employees.

The 34-year-old former employee was alleged to have used an old password to steal customer account data and then sold the information to street-corner criminals one account at a time. Losses were estimated at more than \$100 million but expected to increase significantly, as were the number of victims. According to Manhattan U.S. Attorney James Comey *"With a few keystrokes, these men essentially picked the pockets of tens of thousands of Americans and, in the process, took their identities, stole their money and swiped their security."*

“ Nearly 80,000 businesses, mainly small firms, lost an estimated \$12 billion to email fraud between June 2016 and July 2018, according to the FBI ”

The New York incident was a wake-up call for those business owners who believed that they had little to worry from the threat of cybercrime and identity theft. Many other business owners have learned the hard way. And according to the Ponemon Institute, small businesses will pay an average of \$690,000 to clean up after a hack¹. Do you have the budget for that? Probably not, which means you may end up in the 60% Club.

Security experts have been warning for years that the small business could be the biggest target for cybercrooks, and that the threats could come from anywhere. Even your own employees. There are so many different ways identity theft can happen in your business, whether it's the theft of employee information by insiders or outsiders, the accidental exposure of client data that makes it into the hands of identity thieves, or by hacking or an external breach.

Employees can play a key role in preventing most of these threats. Your business stands a much better chance of avoiding all kinds of identity theft if your employees understand what the risks are and how to avoid them. That means understanding how identity theft happens, what kind of information you and your employees need to focus on protecting, your access rules, and best practices to follow in order to protect that information.

So What Are Your Options?

As a small business owner there are many things you can do to minimize the risk of facilitating an identity theft crime, and to minimize the loss if your security precautions fail.

LEARN TO THINK SECURITY FIRST!

Recognize the risk, and prioritize your protection. Given all the focus on cybercrime in the last few years it's easy to become complacent and fatigued every time a new story hits the headlines. But cybercrime is not going away any time soon, and identity theft is likely to become the single biggest threat to your business.

Business owners need to start developing and implementing a security strategy today to ensure that they're not tomorrow's headline. Key to good security is learning to Think Security First! so that security awareness is as second-nature as being polite to customers, and kicks in automatically into every business decision and action.

HAVE A CLEAR SECURITY POLICY AND STRATEGY

Every business has to have a company-wide security policy that clearly states what the company security rules are, and the consequences for failing to obey them. This helps deter

would-be thieves, alerts all employees to the need for security, and can offer some protection in case of any legal action.

Your business also needs a clear security strategy for protecting the data that identity thieves are after. A basic security strategy should include setting access rules and controls, the use of security technologies, regular security testing and assessment, employee training, employee background checks, and incident response.

CONTROL ACCESS AND KEEP LOGS

The fewer employees with access to sensitive files, the lower the risk of security abuse. So restrict access to sensitive data strictly to those who need it by creating access lists that state clearly who has access to what data, and under what circumstances. For example, there are technologies today that can restrict what an employee can do with a computer record, prohibiting them from opening it or saving it to another drive, making a copy, printing it, or emailing it.

“ Did You Know? Zero liability does not apply to commercial or business accounts. Which means if a thief or hacker empties your business accounts, don't expect to be reimbursed by your bank. You're probably on the hook for all of the losses. ”

Access logs are also a great deterrent, as well as powerful evidence if a crime is committed. When employees know that their access to certain files is being recorded, they may be less inclined to misuse that access.

That's why it's important to keep logs of access to all sensitive files, make sure all employees know that the logs are in use, and make sure that employees cannot interfere with or circumvent those logs. It's also important to keep secure back-ups of all logs in case they need to be referred to months or even years later.

Train, Train, Train

Your employees can either be sentries or vulnerabilities. It's entirely up to you. Your employees are your first line of defense against external and internal crimes. The more they know about security, about the signs of a crime, and of how to respond, the less vulnerable your business will be. So introduce regular security training to teach employees about their roles and keep security fresh in their minds.

Training shouldn't be annual or even monthly but daily, constantly. Find creative ways to constantly remind employees to *Think Security First*, to think "before" they click on something because the opposite is too late.

And test the training by testing your employees. A growing number of companies will send your employees phishing emails to see how many will fall for them. A great way to tell, before it's too late, how well your employees are getting the message.

Focus on Phishing

One of the biggest and most dangerous threats to all businesses is the phishing email. It's a spoof email, often well researched and well written, designed to either trick an employee into revealing sensitive information like a password, or clicking on a link or attachment that triggers the launch of some nasty malware into the business.




That malware could be ransomware designed to lock or hijack every file in the company and hold it for ransom, or gain access to bank accounts and start moving money around. Or maybe it will target credit cards or customer data. Employee vigilance is your best defense and that comes from both constant awareness training and building a culture of security throughout your business. My chapter on phishing explains this threat in greater detail.

“ 43% of businesses targeted by phishing attacks were small businesses ”

Symantec Internet Security Threat Report

Protect Your Website

Website security firm SiteLock has estimated that anywhere between 5,000 and 10,000 websites are discovered every single day to either have malware planted on them or vulnerable to hacking. If your website is hacked, or even just detected to have a vulnerability, the consequences can be severe:

-  Your client data can be stolen.
-  Your website could infect the computers of your customers.
-  Your site could be blacklisted by search engines or blocked by ISPs.

Hackers use automated tools to scour millions of websites that might have even the smallest vulnerability. It often takes just a few seconds to find and hack a site, and if you don't have even basic security in place, you might never know you've been hacked. Until it's too late. There are a growing number of companies that protect small business websites, like Securi and SiteLock, often for less than \$10 a month.

Encourage Reporting By Fellow Employees

The best sentries against a crime by an employee are fellow employees. And while many employees might be reluctant to think of themselves as spies or snitches, they must be made aware of the risk to their workplace and to their jobs from insider crimes, and of how important it is to report suspicious behavior by fellow employees.

To help ensure that employees take security seriously, it's always helpful to make a personal connection - that cybercrime costs money and threatens jobs. If an employee suspects a co-worker is engaging in risky or criminal behavior, he or she is more likely to report that worker if they believe that behavior may have an impact on their own job security.

Focus Your Security On Id Theft Targets

ID thieves need very specific information in order to launch an effective ID theft. The most valuable information is a Social Security number - yours, your customers' and your employees'. Other target information includes credit card data, bank accounts, and family information.

That's why it's so important to identify the type of information thieves target, and where you store it, so you can focus most of your security on it.

These records should ideally be:

- Stored on a secure computer that is not connected to the Internet.
- Kept in a room that is secure.
- Protected by strong passwords.
- Encrypted.
- Available only to those who absolutely need access and who have been approved.

“ According to a study by Osterman Research in June 2017, one in five small businesses have suffered a ransomware attack and the average loss was \$100,000. ”

It's also important to keep accurate records of who accesses the information, when, and for what purpose. And printed records also need strong physical security, including theft-proof data safes (and don't hide the key in a nearby drawer.)

Use All The Available Technologies

Security is about creating layers, concentric rings of security that slow down, frustrate, or completely stop attackers. Most security technologies for the small business are affordable or even free and should include antivirus software on every computer and laptop, mobile security, intrusion prevention and firewalls, website security, encryption, password managers, backup and so on. And it's also important that all employees have similar layers of security on their personal computers and mobile devices, especially if they use their personal devices at work. Which most do.

Don't Forget About Privacy

Just as identity theft and cybercrime are equal partners in crime, security and privacy also go hand in hand. An understanding of and commitment to privacy, and especially to keeping customer and employee information private, is the foundation of good security. Many of today's security breaches occur because data collection didn't start with privacy. If you don't respect and live privacy, your data will be plundered.

Beware of Fake CEO Emails

This scam is growing so fast, and is so easy to pull off, the FBI issued a major warning to businesses in 2018. The FBI estimates that U.S. businesses, mainly small businesses, have lost close to \$12 billion in just the last three years to this scam.

Here's how it works – the scammers, with a little research, find the name and email address of the CEO or other executive and send an email from that address to an employee at the company instructing them to pay a certain bill or make an urgent transfer. Because the scammers have done their homework, the emails can be very convincing, using the type of language, jargon, and even nicknames an employee would recognize, and targeting an employee who would usually make such transfers.

There's always a sense of urgency, and that's to reduce the likelihood of the employee double-checking with the boss before following the instructions. In one recent case I worked on, scammers persuaded a bookkeeper to transfer more than \$170,000 before she realized it was a scam. In another case, an employee called me before she made a transfer, asking me for my advice because her boss was out of the country and unreachable. That call, and more important, her vigilance, saved her boss at least \$15,000 and possibly more. Two very different outcomes, and all determined by the level of vigilance of an employee.

Have An Incident Response Plan

The worst case is that despite all your security precautions a determined thief or dishonest employee manages to steal confidential information and launch an identity theft. How much the incident will ultimately cost your business will depend largely on how well you respond.

That response should include how any digital forensic evidence is preserved, including log files and emails; informing the appropriate authorities, including the FBI; how you deal with the suspected or accused employee (make sure you have good legal advice); responding to worried customers; and dealing with the media.

Don't Ignore Legal And Compliance Issues

The surge in data breaches in the last five years has resulted in a wave of federal, state, and industry regulations designed to force businesses of all sizes to better protect their data and their customers.

Compliance requirements may also apply to your business, even if it's a very small business. Not only can these regulations be costly to implement, they may cost even more if you don't comply. Or worse, if you have a security incident or data breach. And of course, apart from the Federal data protection laws, most states now have their own data protection and identity theft laws to protect consumers.

1 Ponemon Institute, LLC, 2015 Cost of Data Breach Study



THINK SECURITY FIRST!



**SCAM
ALERT**

AN INSIDE JOB

PROTECTING YOUR IDENTITY IN THE
WORKPLACE

CHAPTER 14

It's been about a decade since a University of Michigan study found that as many as 75% of all identity thefts originate in workplaces across America.

There have been no major studies on the topic since so it's hard to tell if it's still true. But if you consider that most data breaches start in somebody's workplace, and the majority of those breaches are focused on identity theft, in a sense the claim is still valid.

And there's not shortage of bad actors to choose from:

- The FBI arrested a former senior financial analyst at Countrywide Financial Corp. employee who later admitted to stealing up to 20,000 customer records a week which he then sold for approximately \$500 each. In total he stole the personal information of more than 2 million customers.
- A former Texas Lottery Commission computer analyst was arrested for copying the personal data of Texas lottery winners. He downloaded his own work files off his computer and took them to his next job. The names and Social Security numbers of 27,075 mid-level lottery winners - people who have won prizes from \$600 up to around \$1 million - were on the employee's hard drive.
- A former programmer at Birmingham, AL bank stole a hard drive containing 1 million customer records and used some of that information to commit debit card fraud. The thief had used the information stolen from the bank to create about 250 counterfeit debit cards. He was able to use about 45 of those cards to access and withdraw cash from customer accounts at the bank before he was arrested.
- A former employee at one of the subsidiaries of Fidelity National Information Services pleaded guilty to stealing and trying to sell the personal financial records of 8.5 million customers, including credit cards, bank accounts and other personal information.

Careless employees can also be a threat. A laptop computer containing limited health information on 100,000 patients was stolen after an employee left the laptop in his car. Included were 7,400 patients whose Social Security numbers were stored on the computer.

“ Employees are not the only threat, and many data breaches and identity thefts have been committed by third parties and contractors. For example, a laptop stolen from a third-party vendor that managed job applications for the Gap group of stores contained the personal data, including Social Security numbers, of approximately 800,000 people who had applied for jobs at the Gap. ”

One of the biggest data breaches in Britain was traced to a government employee who lost a set of computer tapes containing the personal information of almost every taxpayer in the country.

Typical Workplace Threats Include:

- Stealing a check from the back of your checkbook in the hope that it will be weeks or months before you notice the check missing.
- Copying credit card numbers from your purse or wallet when you're away from your desk.
- Accessing other personal information in your purse or around your workspace.
- Stealing your Social Security number and other information from your personnel file.

- Stealing your password and using it to access and download customer information without permission.
- Breaking or ignoring security rules that accidentally expose your personal information to others.

So How Can You Protect Yourself?

There are many things you can do to protect yourself, your co-workers, and your employer from identity theft in the workplace, and most simply require a little extra vigilance:

- Rule #1 – if your employer has data and identity protection policies, understand and follow them. If you follow the rules and there's still an incident, you can't be blamed. Hopefully.
- Take personal responsibility. Whatever precautions your employer takes to protect your information and identity, you should also take your own precautions for that extra layer of security.
- Protect your computer and mobile devices. If your employer doesn't already protect your devices and the information on them, ask if you can install approved security to help protect any sensitive information on the device.
- Protect your passwords. Your passwords can be vulnerable not only to hackers and other external threats, but also to insiders including fellow employees, contractors, maintenance staff and even visitors. So keep them safe and confidential and don't be tempted to keep them written down and stored near your workspace.
- Don't store personal information like tax returns or financial statements on a work computer. In most organizations this would be against company policy anyway but don't be tempted to take personal information to work for any reason.

- Protect your laptop and tablet, whether it's your personal laptop or a company computer, and especially if it contains any sensitive personal or company information. And don't leave it lying around the office - many of the data thefts and security breaches reported in the last few years have resulted from the theft of employee laptops from the workplace.
- Avoid accessing personal accounts from work. Even if you know your work computers have security installed, it's still not a good idea to access personal financial accounts from work because it could expose your login and password details to hackers or even other employees.
- Protect your purse or wallet. Many identity thefts have been traced to the theft of checks, credit cards, and credit card numbers from employee desks. So remove the temptation by always protecting your wallet or purse while at work and especially during lunch and other breaks.
- Avoid using personal passwords at work, either to access personal accounts from work computers, or using the same passwords for work and personal use. Any security breach at your workplace could end up exposing your personal accounts.
- Be alert for social engineering attempts. Social engineering is used by hackers to trick employees into revealing sensitive information like passwords, often by simply placing phone calls or sending emails to employees and posing as an IT administrator resetting employee passwords.
- Watch out for walk-ins - visitors, contractors, or anyone else who walks into your office. Many id thefts are walk-ins - a thief walking into an office posing as a visitor, contractor, computer technician or even delivery driver and walking out with a laptop, server or unattended purse.

- Be careful with new employers and job interviews. In one case the CEO of a New York computer company used the Social Security numbers of his employees to obtain new credit and obtain more than \$1 million in fraudulent loans.
- Be wary of email requests and workplace phishing schemes. Identity thieves are increasingly using "spear phishing" schemes that target specific organizations using emails, logos, and language to mimic the organization and trick recipients into revealing sensitive information.
- If you receive such emails, check with a supervisor or manager first, or simply ignore. The worst that can happen is you'll be applauded for your vigilance (I hope).



IDENTITY THIEVES MAKE IT RAIN MONEY IN FLORIDA

IT WAS ADDICTIVE. JUST LIKE THE DOPE THEY ONCE SOLD ON THE STREETS, IF NOT MORE, ACCORDING TO THE STORY IN THE SEMINOLE HEIGHTS NEWSPAPER. "A HIGHLY LUCRATIVE BUSINESS TAKING PLACE IN FRONT OF A LAPTOP IN THE PRIVACY AND COMFORT OF HOME. A BUSINESS AMOUNTING TO \$130 MILLION IN TAX FRAUD, COSTING TAMPA TAXPAYERS AN ESTIMATED \$15 MILLION A DAY."

They were talking about Operation Rainmaker, an identity theft scheme that was so easy and so lucrative it persuaded drug dealers to abandon their trade and turn to identity theft instead. The operation got its name from law enforcement simply because of the vast amounts of money thieves were able to rain down on themselves – about \$130 million at the final tally.

Authorities were only tipped off to the scheme when numerous Florida taxpayers began to file complaints that when they went to file their own taxes, they found someone else had filed using their name. And that was the core of the scam.

Here's what law enforcement eventually discovered. The thieves were using public websites like Ancestry.com to assemble the identities of the living and the dead, and were also buying complete identities on the black market – something that's surprisingly easy for anyone to do.

Once the thieves had assembled enough information about a victim, they used off-the-shelf tax return software like Turbo Tax to file fraudulent tax returns. By the thousands. And that

was probably the easiest part of the entire scam. At the time, the IRS was unable to thoroughly review or cross-reference every single tax return they received, or spot any red flags like a sudden change of a taxpayer's address. And if the amount of the refund was under \$10,000, it rarely faced scrutiny.

So naturally the thieves kept their returns under the \$10,000 threshold and then sat back and watched the IRS rain money down on them. That money often came in debit cards or "Green Dot Cards" issued by the Treasury and sent to a variety of homes, some of them vacant, or deposited electronically into bogus accounts. According to some reports, members of the gang attended seminars on preparing and filing tax returns, and even rented hotel rooms to host their own tax filing parties.

Once they had their hands on the funds, the thieves would go on spending sprees. The scheme was so lucrative and widespread, authorities in the area said they noticed a significant reduction in street-level drug dealing. According to a number of sources, informants told police that local drug dealers quickly realized that identity theft was a much more lucrative and safe line of business.

As soon as authorities learned of the scheme, they assembled a task force that included police and Sheriff's departments, the United States Secret Service, the United States Postal Inspection Service, the State Attorney's Office, and the United States Attorney's Office.

But in spite of all the evidence they had gathered, authorities had trouble in filing charges of tax fraud because initially the IRS refused to share the records they had – apparently the IRS protects the personal information of thieves who are caught committing tax fraud.

How To Make The IRS Rain

Nearly fifty people were eventually arrested as part of Operation Rainmaker, and here's exactly how law enforcement laid out the multiple steps in this bizarre criminal enterprise:



Create Fake Identities



Suspects search the web to find identities of deceased or living victims.



Defendants buy large volume of identities from suspects who are stealing names and Social Security Numbers from businesses, medical facilities, and even prisons.



File Fraudulent Tax Returns Online



Suspects use multiple electronic filing programs including Turbo Tax, Tax Hawk and Tax Slayer. Turbo Tax is the most commonly used.



Suspects refer to this tax scam as “doing drops.”



Request Refund on Green Dot Card, Treasury Check or Direct Deposit



Suspects have refunds sent to vacant homes, another suspect’s home or an innocent bystander’s home and then intercept the mail.



Defendants open fraudulent bank accounts to receive direct deposits.



Cash in the Refund



Suspects withdraw money from ATM’s.

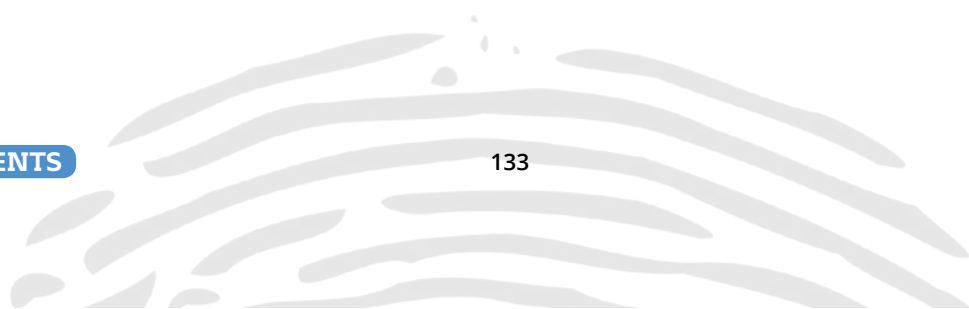


Buy large ticket items or money orders at legitimate businesses.



Suspects launder the money through illegal businesses.

And apart from how easy it was to pull off the scam – if they’d stuck to victimizing dead people they might never have been caught – the most worrying part of the story is how drug dealers and other criminals are turning away from traditional crimes and towards identity theft. And with so few investigations, arrests and prosecutions for identity theft, what do these crooks have to worry about?



Off With Her Head! The Takedown Of The Queen Of Tax Fraud

One of the leaders of the Operation Rainmaker crew was eventually taken down because she just wouldn't shut up. In a series of postings on her own Facebook page, ringleader Rashia Wilson not only boasted of her role in the crime, she also taunted authorities with a series of "catch me if you can" messages. In one posting, surrounded by some of the piles of cash she claimed she stole from the IRS, she boasted:

"I'M RASHIA, THE QUEEN OF IRS TAX FRAUD... I'm a millionaire for the record, so if U think indicting me will B easy it won't, I promise you! U need more than black and white to hold me down N that's to da rat who went N told, as if 1st lady don't have da TPD under her spell. I run Tampa right now."

First rule of crime – don't use Facebook to tell everyone that you did it. Second rule – don't taunt the people who can take you down. Even though Her Majesty already had more than 40 convictions for fraud and other crimes, and in spite of her own boasts and utterings, it still took law enforcement a few years to build a case against her.

But there was nowhere to hide and no royal immunity. Three years after Operation Rainmaker was exposed, Her Majesty the Queen of Tax Fraud, still in her twenties, swapped her swanky robes for prison scrubs as a judge sentenced her to 21 years in prison. But although convicted of making at least \$3 million from her role in the crime spree, her conviction was overturned on appeal because of what were described as "procedural errors" in her sentencing.

In short, her defense team believed the sentence of 21 years in prison was way too harsh. But while justice might be slow, she's usually reliable. A short time later the Queen faced the very same judge that had overseen her previous sentencing, and he gave her exactly the same sentence all over again – 21 years in state prison. With good behavior, she could be out in 2031.



THINK SECURITY FIRST!

HOME SWEET HOME

PROTECTING YOUR HOME FROM IDENTITY
THEFT

Chapter 15

CHAPTER 15

Wherever your identity goes, so does the risk. And that includes your own home. One of the reasons identity theft is such a pervasive crime is that it can happen anywhere, even in your own home, and committed by those you least expect.

Like the young couple from Philadelphia who earned notoriety around the world when their identity theft spree earned them the title of a modern Bonnie and Clyde. Before being caught and sentenced to more than four years in prison, the pair went on a global jet setting spending spree blowing more than \$120,000 in stolen funds. To fund their spree they simply stole the identities of their friends and neighbors by burglarizing their homes.

A reporter for a newspaper in Silicon Valley spent years chasing down an identity thief who burglarized his home one afternoon and stole some personal financial documents. That one crime of opportunity led to an exhaustive cat-and-mouse game with the thief as the victim's information was sold and resold on the global black market for stolen information.

The theft also resulted in a number of different thieves showing up at numerous banks with the victim's Social Security Number, bank account numbers and even real drivers' licenses in the victim's name.

“Oops! A victim of identity theft was arrested two years after a burglar stole his birth certificate and created a new identity. When the victim showed up at a police department to complain about a new bank account opened in his name, he was promptly arrested because his identity was now in a database of other crimes committed by his new clone.”

Identity theft has quickly become the crime of choice for burglars. As one expert said, it's much easier for a thief to walk down the street with your Social Security number written on his hand than your brand new 55" TV tucked under his arm.

Not only will your Social Security Number fetch more than your TV, the thief can sell the information over and over again. And once your personal information is on the black market, it will be there forever, forcing you to fight the same battle month after month and perhaps even year after year.

But these incidents and many more like them serve as a powerful lesson that while we often worry too much about hackers stealing our personal information from private databases at the other side of the world, we have as much if not more to fear from the thieves in our own backyard.

So What Can You Do?



Think like a thief: Do a security survey of your home from the perspective of a thief, focusing on the easiest ways into your home, the places a thief could enter your home without being seen, and where you keep personal information in your home.



Create a set of house security rules: This is a simple checklist of things that you and any family members should be aware of and rules that should be followed. Those rules should include things like how mail is handled, internet and email use, how to deal with spam, how to recognize scams, how to manage financial paperwork etc.



Lock down your computer: Your computer will always be a target for hackers, spammers, and identity thieves so it's important that you devote the time and resources to make sure all computers in your home are as hack-proof as you can make them.

Every computer should have the latest in anti-virus software, and if you know where to look it can cost you nothing. My chapter on free security tools explains. Just as important as having the right software is making sure it's always up to date. Identity thieves and malware authors are always changing their tactics and codes, and up-to-date security software is the best way to stay ahead of them.

- **Protect your financial information:** Whether thieves come into your home through the internet or through a back window, chances are they're after the same thing – your personal financial information.

So do your best to frustrate them. Hide your most sensitive financial information, and especially anything with your Social Security Number, in a place that's almost impossible for a thief to find. If that data is on a computer, make sure it's protected with strong passwords and a good encryption program.

And don't leave financial information lying around the home in plain sight, especially things like bank and credit card statements, tax returns, paylips, checkbooks and credit cards, and any other sensitive financial correspondence.

Create security zones: A typical security zone might be a place you do your bookkeeping, store your financial information, or a home office. If you have a lot of sensitive information in these locations, then keep them off limits to as many people as possible.

“ Did You Know? According to the insurance industry, there's a burglary every 15 seconds in America, or more than 5,700 every single day. And the #1 motivation? Identity theft. ”

- **Get physical with security:** If burglary is a big risk in your neighborhood, you can bet those thieves are after your Social Security Number. So think about creating layers of security defenses around your home to deter burglars.

These layers could include a burglar alarm (even a fake one if it's all you can afford), good security lighting that senses movement close to the house, and good window and door locks.

If you can afford it, a simple video surveillance system can be a great deterrent and the sight of a surveillance camera is often enough to persuade a burglar to pass your home by and look for an easier target. Make sure you take a close look at every entry point to your home and that these doors and windows are all as secure as possible.

And finally, it's time to get rid of that old habit of hiding house keys in secret places that you think a burglar would never dream of looking. Believe me, they know exactly where to look.



Be wary of visitors: Identity theft is often a very personal crime, very close to home, and committed by people you least expect. Those people can include family members, friends, neighbors, and even occasional visitors. So to avoid the risk that someone you trust betrays that trust, don't leave any temptations lying around.

If you have cleaners, contractors, or service people coming to your home, make sure you supervise them as much as possible and keep all financial information out of sight.



Shred it! It's a sad fact that every home today should have a personal shredder, because throwing out sensitive financial documents these days is no longer a safe thing to do.

Thieves will often go through garbage in search of any information that they use to create new credit accounts in your name. A decent personal shredder can cost as little as \$50 and can be a very worthwhile investment. But only if you use it!



THINK SECURITY FIRST!



GRINCH THIS!

AVOIDING IDENTITY THEFT DURING THE
HOLIDAYS

Chapter 16

CHAPTER 16

Of all the things you might want for Christmas, a clone is probably not one of them. But if statistics are true to form, in the month of December more than a million Americans will lose something that Santa won't be able to replace – their identity.

With identity thefts occurring at the rate of an average of 42,000 every day the Christmas holiday season is just as big a business opportunity for identity thieves as it is for retailers.

So to help you keep your good cheer and your identity, I've taken a look at some of the most common ways your identity could disappear during any Christmas holiday period and what you can do to prevent it.

Phishing

Phishing has become one of the costliest and most lucrative forms of identity theft, increasingly being run by organized crime gangs, carefully designed and well funded to dupe even the most cautious user.

Phishing uses convincing-looking but bogus emails and web sites to trick you into revealing confidential financial or other information that can be used to steal your identity. The messages will often take the form of a warning that you that you need to update your account or confirm your account information to avoid having your account frozen.

This kind of scam is particularly successful around Christmas, a time when no user wants their bank accounts or credit cards frozen. And you might be amazed at how many consumers still fall for this scam.

How Can You Grinch This? Pretty easy - if you're paying attention. Make it a rule to never, ever give any personal, financial, or security (like a password) information to any email request or phone call.

If you get such an email or call and you have an account with that company, go directly to the web site of the company named, call the customer support number on the web site, and ask for more information. Don't ever click on a link in the email because the sender can easily spoof the web site they link you to, or launch malware. And don't call any numbers offered in the email.

Bogus Receipts By Email

These are typically very convincing looking emails, often with attachments claiming to be receipts for goods you never ordered. The behavioral exploit is (1) around Christmas most people are dealing with a surge in receipts and therefore expecting them, and (2) the scammer is hoping to panic you into opening an email attachment you normally might be suspicious about.

The goal of the email is usually to trick you into installing malware on your computer when you open the attachment, which will then steal passwords and other information and gift them to an identity thief.

How Can You Grinch This? Don't open email attachments unless you're expecting them, even if you recognize the sender. And make sure you have good antivirus software with up-to-date definitions on every computer and mobile device you use. If you're still curious about the email, call the customer support number for that company, as listed on their web site, and inquire from there. Don't click on any link, or trust any information offered in the email.

The "Hard-to-find" Deal

Every year thousands of online shoppers are bilked out of millions of dollars by bogus web sites offering that year's "must have" gift. Every year we expect to see variations on that theme where identity theft, rather than simple fraud, is the primary motive.

For example, when you try to order that last minute gift at a too-good-to-be-true price, after entering all your credit card details you may receive a message that goes something like *"Sorry but our servers are busy and we are unable to process your order at this time. Please try again later."*

What you don't realize is that the thieves may have just grabbed a copy of your credit card number, address, and verification number. And what's more, you're unlikely to be suspicious because you believe the transaction never actually occurred.

How Can You Grinch This? Only purchase from web sites that you know and trust. And make sure it's the real site and not a spoofed or lookalike site. Don't visit the web site through a link in an unsolicited email or from another web site – instead enter the web site address directly (and carefully) into your browser.

Mail Theft

Mail theft has always been a favorite for identity thieves, and this year you can expect your mail to get plenty of attention from petty thieves, opportunists, and organized crimes gangs.

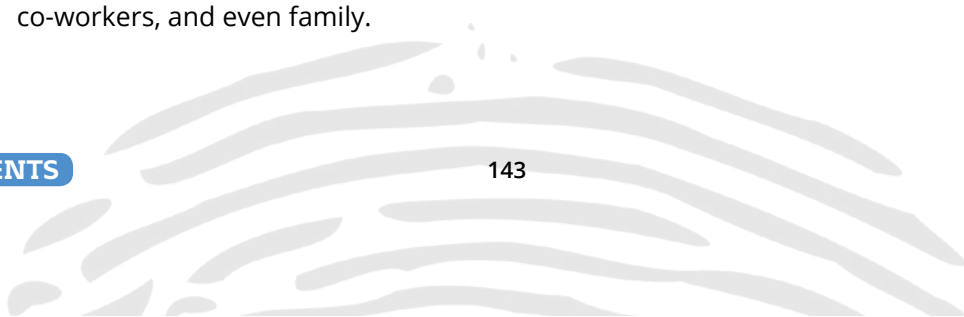
They're after anything that can be used to clone your identity or simply enrich their bank accounts – things like incoming and outgoing checks (as you pay off those big credit card bills), bank statements, credit card statements, credit card offers, gift cards and certificates, and even cash.

How Can You Grinch This? Be very careful with your incoming and outgoing mail during the holidays. If possible, have your mail delivered to your front door and not to a mailbox at the end of your driveway.

Deliver mail to the Post Office instead of leaving it in a curbside mailbox to be collected. Try paying as many bills online as you can, and give as many cash/check gifts as you can in person. Don't print your full address on checks either, and only have your first initial and last name printed – that way a thief will have great difficulty signing your name if they steal your checks.

Nearest and Dearest

One of the saddest facts about identity theft, according to a number of studies, is that many of these crimes are committed by people known to the victim, including friends, neighbors, co-workers, and even family.



The holidays often put great pressure on consumers to buy more, and for those who can't afford to out of their own resources, they may be tempted to turn to yours instead. And studies have shown that identity theft committed by family members and friends can cost more and last longer, because the culprits are usually able to hide the crime for longer. And as if it wasn't already creepy enough, there have been thousands of cases of family members stealing the identities of deceased family members.

How Can You Grinch This? Remove the temptation. Don't leave personal information, including bank statements, credit cards, checkbooks, and mail lying around your home or workplace where they can alert and tempt someone you trust. Keep your key identity documents well hidden too – things like Social Security cards, birth certificates, passports, and tax returns.

And instead of giving a check as a gift, consider instead a gift card - something that can't be used to clone your identity if stolen. And if you have older family member who may be living alone or has caregivers dropping in, make sure to read my chapter on protecting the elderly from identity theft and other scams.

Electronic Greeting Cards

At the risk of offending the entire online greeting card industry, I personally recommend never opening electronic greeting cards because they can very easily be used to hide malware that can target your identity.

While these cards can often be funny, cute, cheap (even free) and very convenient for those last minute procrastinators, if not legitimate they can bear an unwanted gift that will just keep on giving, and costing the victim for many Christmases to come. And I don't think you want to be remembered that way.

How Can You Grinch This? Make the effort and send a real card by mail or in person. If you have to send a last minute electronic greeting, a personal email with no attachments is just as good and perhaps even more appreciated. If you receive such a card, check with the sender before you open it (by calling and thanking them – if they don't know what you're talking about, you know you're being scammed).

And be careful about web sites that ask you to sign up to send unlimited electronic or printed cards to all your friends free of charge. Many of these scams trick you into downloading malware that can be very difficult to remove. Or to upload your entire contacts list as a gift to the crooks.

Pickpockets

Just like their close cousins, the burglars, pickpockets see the holidays as their biggest and best revenue opportunity, and your gift to them this year could be your wallet or purse. The holidays are an exciting time for pickpockets because of big crowds, big spending, and hassled shoppers too busy to notice that they're being, well, noticed.

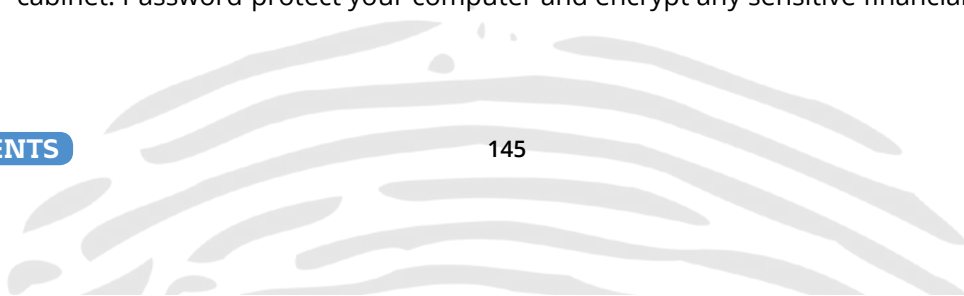
How Can You Grinch This? If shopping online doesn't satisfy all your gift giving (even if it's to yourself), think about shopping as a covert mission, and as with any such important missions always travel light. The most you're likely to need at the mall this year is a credit card (yes, just one) and a driver's license. So slip them into an inside pocket and leave bulky big targets at home.

But if you feel you must go shopping with absolutely every credit card you possess, make sure before you go that you make a photocopy of everything in your wallet or purse, and both sides, so that if you do fall victim to a pickpocket you'll know what they've got and what you have to cancel quickly. And always keep wallets in pockets that are not easy to access, and keep purses tucked in close to the front of your body.

Burglary

Identity theft may be the burglary of the future. Burglars know that they'll look much less suspicious walking through your neighborhood with your Social Security number written on their hand than if they have your brand new 65-inch TV tucked under their arm. The payoff from your stolen Social Security number or tax return will buy a dozen flat screen TVs, and without leaving as much as a fingerprint.

How Can You Grinch This? When you're going shopping this Christmas, go in shifts so your home is never empty. Hide your financial records or place them in safe or locked filing cabinet. Password-protect your computer and encrypt any sensitive financial data on it. And



hide your laptop. Burglars tend not to stay in a home for too long so the harder you make it for them to find your information, the greater the chance they'll just leave with less. And you'll be thankful for that mercy!

Charity Scams

'Tis the season of taking as much as giving, and there's always an increase in the number of bogus charities asking for credit card donations throughout Christmas. This could be by phone, mail, and increasingly by email. And many of these scams will either spoof well-known charity organizations, or use similar-sounding names, to trick you into giving what is definitely not deserved.

How Can You Grinch This? Give only to charities you know and trust, and preferably through their web site rather than in response to a phone call or email solicitation.

Hard Drive Rebuilding

Planning to treat yourself to a new computer or tablet this Christmas? What are your plans for the old one? Before you retire your old devices to the recycle scrap heap or the auction block, make sure that you do a complete wipe of the hard drive so that you don't leave any extra gifts for the new owner.

In an exercise by students at MIT a few years ago, researchers who purchased 158 used hard drives at places like eBay found that 128 had usable information still on them, including medical records, personal email, pornography, and more than 5,000 credit card numbers.

How Can You Grinch This? Deleting files from a computer, tablet, or even phone does not erase them. Consider using one of the many professional and often free data erasing programs, like Darik's Boot And Nuke, that will completely erase all data, forever. And check with the manufacturer of your phone for their guidelines on fully wiping your phone before your sell, trade, or donate it.

Alternatively, take any hard drives to one of the many shredding events that take place every day around the country. Or easiest of all, take the drive outside and destroy it with a hammer (please wear goggles).



THINK SECURITY FIRST!

FROM PRINCES TO SKIMMERS

AVOIDING COMMON SCAMS
AND FRAUDS

Chapter 17

CHAPTER 17

Every year millions of Americans lose hundreds of millions of dollars to scams, cons, and frauds – some so clever it's easy to understand why victims could fall for them, and some so obviously and even hilariously fraudulent it's hard to understand who in their right mind would even give them a second look.

The world is now awash with scams and frauds of all kinds, offline and online, and whose sole purpose is the redistribution of wealth. Yours to the scammers. And you don't have to be wealthy to be a target. In fact most scams don't target the wealthy because it's easier to commit a massive fraud involving millions of users and only small amounts of money. These frauds are often easier to hide from the victim and rarely attract the interest of law enforcement.

So why do all these scams work? There are two main reasons:

- Because the scammers are often clever, well funded and well organized, and simply smarter than their victims.
- Because busy victims don't slow down enough to read the warning signs.

Federal Trade Commission

The FTC keeps a running record of the number of complaints it receives from consumers. And while the list is very informative, it may not tell the complete story simply because most consumers and victims never actually file a complaint with the FTC. And as you can tell, the list is very broad and each category can include many different types of crimes.

So with that caveat, here's the FTC's list of the top 10 consumer complaints from 2018 (expect 2019 to be about the same):

- 1 Debt Collection
- 2 Identity Theft
- 3 Imposter Scams

- 4 Telephone and Mobile Services
- 5 Banks and Lenders
- 6 Prizes, Sweepstakes and Lotteries
- 7 Shop-At-Home and Catalog Sales
- 8 Auto-Related Complaints
- 9 Credit Bureaus, Information Furnishers and Report Users
- 10 Television and Electronic Media

Common Scams To Watch Out For

Phishing scams are probably the most common scams and therefore something to always be vigilant for. Phishing is simply the use of bogus emails, web sites, and even phone calls designed to trick users into believing the communication is from a bank, credit card company, the IRS, your boss, or other legitimate organization.

The goal is usually to trick the victim into either handing over a password or other sensitive information, or clicking on a link that will download or activate some malicious software. Most of the scams want either your money or your personal information so they can clone your identity and steal someone else's money, or both.

But increasingly, these phishing emails also hide sophisticated malware capable of bypassing your antivirus software and wreaking havoc on your life and finances. And in the world of hacking, phishing emails are the weapon of choice when targeting employees and businesses as a first step to a security or data breach. Numerous reports have suggested that more than 90% of all security and data breaches start with someone opening a phishing email. Could your clicking habits be costing you money?

Phishing is such an important topic its earned its own chapter in this book.

Tech support calls. The bogus tech support call has been around for years and is only increasing in popularity – at least with thieves. And the elderly are the most vulnerable because they tend to be more trusting and can easily be snared by a threatening stranger.

The call is simple – it will often claim to be from a well-known tech company, like Microsoft, and alerting you that their regular scans have discovered malware on your computer. They will then either ask for remote access to your computer (which they can use to steal information on the computer), or ask for a credit card payment to fix the problem. Or in another version, a popup warning will suddenly appear on your screen, with a similar message, and urging you to call an 800 number for a quick and easy fix.

“ Over just a four-month period in 2017, the FBI received more than 11,000 tech support scam complaints with victims reporting combined losses of \$15 million. ”

In March 2017, a group of researchers from the State University of New York investigating tech support scams quickly discovered more than 22,000 tech support scam web pages spread across 8,700 domains, and with each of those domains earning around \$2,000 a day in fraudulent fees. They also found that while 85% of the scam operators were based in India, 10% were in the U.S.

And in May 2017, the Federal Trade Commission (FTC) launched Operation Tech Trap, a coordinated national campaign to crack down on these scams. The FTC announced that it had opened nearly 30 legal actions against these operators, obtaining a \$27 million settlement in just one case alone.

Fake Boss Emails. This scam has surged in recent years, and according to the FBI has cost businesses and individuals billions of dollars in losses. The scam is pretty easy – the scammers will do some basic research on the target company, like finding the names and email addresses for the boss and some key employees, then send a very convincing email from the boss's real email address to someone in accounting and demanding that they pay some urgent invoices that he or she, the boss, forgot to pay.

If done right, the emails can look very legitimate. In one case I worked on, a bookkeeper was tricked into transferring hundreds of thousands of dollars to the scammers because the email from her boss used a nickname that only he and a few others even knew about.

Charity and Catastrophe Scams. These will typically appear around the Christmas holidays or major natural disasters like floods and hurricanes. They're usually begging emails or phone calls from fake charities looking for donations. Whenever there's a natural catastrophe, like an earthquake or hurricane, the event is often followed by spam emails claiming to contain links to graphic videos or photos of the event but instead contain links to malicious web sites or downloads.

Nigerian 419 Scams. You're probably one of the millions of internet users to receive one of those often-comical pleas from Nigeria and other faraway countries offering you a share of the vast fortune of some recently deceased diplomat, government official, or businessman. All you have to do is either pretend to be a long lost relative or allow the sender to deposit their money in your back account for a generous share or fee.

Oh and you'll also have to pay some paltry "advance fees" like taxes, bribes, paperwork, or legal costs. This scam is commonly called the Nigerian 419 scam, named after the Nigerian penal code that covers this criminal activity that has turned many poor Nigerians into instant millionaires. In one recent prosecution, a Nigerian con man made more than \$1.4 million in less than a year simply by spamming millions of users around the world with his crudely worded begging letters.

A study in 2013 by a group of scam investigators estimated that victims of the scam lost a combined \$12.7 billion in that year alone.

“ Personally I know of an elderly gentleman who lost more than \$1 million of his life savings to a Nigerian 419 fraud, and despite warnings continued to hand over money to the scammers in the belief that eventually he would hit the jackpot. ”

Lottery Scams. You get that surprise email telling you that your email address has been plucked randomly from some state or national lottery, and asks you to either provide identification information in order to process your winnings, or requests an upfront payment for taxes in order to send you your jackpot. In 2007 a Chinese student killed herself after learning that the lottery she thought she'd won was just a hoax.

Work-At-Home Scams. These scams vary from high-priced kits to help you make or sell goods that no-one really wants, to offers to make \$1,500 a week processing payments or accepting deliveries, part time, at home. In the latter scam, the thieves will simply be using you and your home address to ship goods bought with stolen credit cards. Or they'll use your bank account to process payments for stolen goods or other illegal activities. Not the kind of work experience you want on your resume! And more recently, hackers are hiring U.S. residents as "payment processors" and using their U.S. bank accounts to transfer or hide funds stolen from bank accounts by malware.

IRS Scams. These usually appear at tax time, either in the form of emails or phone calls, asking for personal information in order to release or speed up a tax repayment. But they can also come in the form of requests to verify your Social Security Number because your last tax return was not received, or that a check sent to you was returned to the IRS.

And of course all these scams come with different labels, including stock scams, foreclosure assistance, credit repair, package forwarding, auctions, and political donations. They all use the same tactics and usually amount to the same thing. So unless you're absolutely certain you can trust the originator, steer clear. My chapter on IRS fraud and identity theft goes into this challenge in more detail.

Skimming and Skimmers

Skimming is probably one of the most dangerous scams you'll face, because it involves everyday transactions with people and places you trust – or just don't think about. And because it's completely invisible – until you check your bank account. Skimming uses card swiping technology to make unauthorized copies of your credit or ATM cards, and the most common places they're used are in restaurants, stores, ATM machines and gas stations.

In restaurant skimming, a waiter uses a miniature hand-held credit card reader to make a quick copy of your credit card information when you're not looking. The stolen information is then sold to others or used to make purchases using your card information.

“ In one high profile case, a network of dishonest waiters in restaurants around New York were paid to skim credit card numbers from restaurant patrons and sell them to a crime gang. That gang then purchased more than \$3 million worth of goods across ten states. ”

In store skimming, the card reader at the checkout is simply replaced with a reader the thieves have control of. So not only are you paying for your groceries, you're also handing your card information to thieves. If you used your debit or ATM card to pay for those groceries, then the thieves will probably have your PIN too and will quickly empty your bank account.

In 2011 I worked with a supermarket group in California after it found that crooks had installed skimmers at checkouts in at least 24 of its stores. It was believed that the crooks had visited each of the stores individually and managed to replace at least one card reader in each store with a rigged one, and all in broad daylight.

One of the victims of that scam that I worked with afterwards was suicidal when she realized she couldn't afford to pay for essential medications after the crooks stole more than \$1,000 from her skimmed account, and her bank was refusing to refund her losses until after a lengthy investigation. Yet another reminder that the cost of these scams reaches far beyond the obvious financial losses.

What To Do To Avoid Skimming

Skimming is one of those crimes that's very hard to avoid, but there are some precautions you can take:

- Pay cash when you're in strange places. I know it can be awkward but paying cash is the easiest way to avoid identity theft.
- Use a credit card instead of a debit card. A skimmed debit card could give thieves instant access to your bank account.
- Be vigilant, especially in restaurants, stores, and gas stations. Always take a close look at any card reader first and don't use your card if the reader looks unusual, out of place, or damaged.
- Check your credit card and bank statements regularly and carefully. Skimming often goes undetected because the thieves make numerous but small payments on your card in the hope of avoiding detection.


How To Avoid Being Scammed

- Verify first - if it looks too good to be true, it probably is. So just ignore. If it looks legitimate, double-check before you respond or make any commitments.
- Never pay any fees in advance, based on a promise that once the fee is paid some kind of payment will be released to you.
- Ignore "you won the lottery" emails. Sorry to break it to you but you probably didn't. Lottery operators won't confirm a win by email anyway.
- If the offer is obviously a scam and you think you can either outsmart the scammers or make money by joining in, forget it. You're just wasting your time, your money, and possibly your freedom.

- Don't submit your password, username, Social Security Number, or any other personal information in response to an email or phone call. Especially if the caller claims to be from your bank or credit card company.
- If you get a call from the courts claiming you missed jury duty and are going to be arrested, or from the government claiming you're not registered to vote, just hang up.
- Ignore offers to participate in secret shopping, paid surveys, or free trials. Most are scams that start by enlisting your trust as a first step to your wallet.
- Avoid work-at-home offers because most are scams, and you'll either end up with worthless sales kits that won't make you a dime, or the scammers will get their hands on your personal information or credit card number they can then sell to others.
- The IRS will never call or email you looking for personal information or to confirm your Social Security Number.
- Don't download free security software or conduct security scans from security companies you don't recognize.
- You're probably not related to a dead diplomat from Nigeria.
- Don't assume that just because the person sending the email or making the phone call knows something about you (like your name, address, or employment) means that they're legitimate. Research is easy and free.



THINK SECURITY FIRST!



ON THE ROAD AGAIN

AVOIDING IDENTITY THEFT
WHEN TRAVELING

Chapter 18

CHAPTER 18

Your identity is a loyal creature. Whenever you travel, whether for business or pleasure, your identity travels with you. That's why you want to make sure that you protect it at all times and that when you arrive home your identity also arrives intact. But easier said than done.

Identity theft is a universal crime, and almost every nation has its own set of traps and techniques for depriving travelers of their identity. And one of the reasons your identity is increasingly vulnerable when traveling is that you're probably busier and more distracted than usual – hurrying to catch a plane or train, trying to make a meeting, or figuring out your bar tab in a foreign currency.

Identity thieves know and recognize these opportunities and won't waste a moment in exploiting them.

How Are You Vulnerable?

Laptops, tablets, and phones – Your devices are like a universal currency. Thieves in every part of the nation and around the world recognize laptops, tablets, and phones for both their value as a product and for the value of the data on them. Device theft is now at epidemic levels and organized gangs even offer bounties based on the type of device (or owner) and the amount of information on it.

“ Chinese intelligence agents have long been suspected of infiltrating high tech conferences around the world with instructions to steal the laptops of specific CEOs known to be working on breakthrough technologies. ”

Hotels – There have been numerous reports of employees at hotels colluding with each other or with organized crime gangs to steal the identities of guests. The techniques range from stealing the credit card information you use to book your room, to staff providing

master keys for thieves to access your room when you're not there. A well-known identity thief confirmed to me in an interview that he's never visited a hotel where he couldn't find at least one dishonest employee he could flip.

In one case, staff, managers, and even the owners of a chain of motels were accused of working together to steal millions of dollars from their guests, simply by copying customer credit card numbers and selling them to others.

An increasingly common scam is the call from reception informing you that there's a problem with your credit card and requesting confirmation of the card number. The call usually comes from the hotel reception, which is enough to convince most guests that the call is genuine. But it's a simple scam. The thief simply calls the hotel and asks for a random room number. When the call is passed through to the guest room it appears to be coming from the hotel.

And guest computers at hotels should also be avoided as they're often infected with malware that can steal personal information and logins.

Airports - Identity theft scams abound at airports for a few obvious reasons. There are thousands of people at any airport at any one time, many of them travelers with laptops and luggage. And chaos usually reigns, making travelers more hurried and hassled, and less cautious and aware.

Common identity thefts at airports include the theft of luggage, the theft of a laptop or tablet when the owner is not looking, travelers leaving their devices at a terminal, a bar, or a bathroom, pickpockets, thieves pretending to be luggage attendants or assistants, and high tech thieves eavesdropping on your Wi-Fi connection. According to security firm Kensington, of all the laptops stolen in 2016, one in every ten were stolen at airports and hotels, and one in every four from cars.

“ In a twist on the hotel attack, in February 2017 guests at a hotel in Austria were locked out of their rooms by hackers because the hotel refused to meet the demands of a ransomware attack. ”

Pickpockets – Pickpockets are everywhere but are especially common wherever there are travelers, including airports, hotels, tourist destinations, and popular vacation spots. They know that people drop their guard when they're traveling, either because they're in too much of a hurry, or have wound down into vacation mode and are thinking of everything else but personal security.

And pickpockets know that credit cards and personal identifying information in your wallet or purse are a universal currency. A single successful theft by a pickpocket can generate thousands of dollars in a matter of hours, as the thief goes on a well-planned spending spree before you even know your credit cards are gone.

Burglars at home - When the homeowner's away the burglars will play. You may not realize it but when you leave your home for an extended period you may also be leaving plenty of vacancy signs for burglars. Mail left uncollected in your hallway, newspapers left uncollected on your driveway, and no sign of life in your home day or night are instant alerts for burglars who have a sharpened sense for these kinds of signs.

Foreign ATMs – If you've ever tried to use an ATM in another country, you'll realize how foreign they really can appear. Not just the language but the instructions. And many of these ATMs are in places that have little security, making it much easier for hackers to rig them to steal your card information and money.

So What Can You Do to Protect Yourself?

- Guard your devices. Keep them with you at all times, don't leave them down, even for a moment, at an airport or in a taxi. Consider installing device recovery software, like Lookout (www.lookout.com) that can help track down a stolen or lost device.
- Avoid storing any personal and confidential information on your devices, and especially financial information and passwords.
- If you have to store sensitive information on your device, make sure it's encrypted. Encryption software locks your data so a thief can't access it without the code. Good encryption software can cost less than \$50 and some of the best is free.

- Keep your luggage with you at all times, and keep your devices and other valuable personal items with you too.
- Make photocopies of everything in your wallet or purse, especially credit cards, ATM cards, store cards, and your driver's license. This will make it easier to remember what you have to cancel if your wallet is stolen.
- Keep credit cards to a minimum when you travel, and bring only one or two credit cards if you can, ideally with the lowest spending limit possible.
- When staying at a hotel, bring your own luggage up to your room and don't leave it unattended in the lobby. If you get a call from reception about any credit card or financial issue, hang up and go down to the reception.
- Keep as little personal information in your room as possible, or keep it in the safe. And when you get home, check your credit card statements immediately for any unusual charges or activities.
- Be wary of surprising last minute changes. If you get a call from your airline or travel agent telling you there's an issue with a credit card, payment, or schedule, and they ask you to confirm any personal information, offer to call them back on the number you have on record for them.
- Carry traveler's checks or even cash, and when paying a restaurant bill, use cash. A dishonest waiter can easily make a copy of your credit card and make it a much more expensive meal than you expected.
- Avoid using ATMs and debit cards in foreign countries. Apart from the risk of high hidden fees, you may be exposing your card and PIN to thieves in a country that provides little recourse for victims or tourists.
- Try not to bring personal financial information with you, like bank or credit card statements. You might plan to use some down time to catch up on your finances, but it's not worth the risk.
- Be careful using free or even paid Wi-Fi services at airports, coffee shops or other public places. Most of these networks are unprotected and make it very easy for hackers to eavesdrop on your devices. Especially if you're using them to access an online bank account or pay a bill.



THINK SECURITY FIRST!

YOU CLICK. THEREFORE YOU LOSE.

THE MENACE OF PHISHING
ATTACKS

Chapter 19

CHAPTER 19

Did you know that 91% of all cyber attacks are believed to start with a phishing email? That's according to a 2017 report from security awareness company PhishMe. If they're right, it means that the vast majority of cyber attacks only happen because people (like you) click on stuff they shouldn't. Imagine how few cyber attacks might actually succeed if people (like you) just stopped clicking on stuff?

Think for a moment about all the biggest and most notorious data breaches of the last few years:

- Target Stores – 70 million records.
- Equifax – 147 million records.
- JP Morgan Chase – 76 million records.
- Anthem healthcare – 80 million records.
- eBay – 145 million records.
- Yahoo! – More than 1 billion records.

One of the things that these massive and costly data breaches have in common is that they probably all started with nothing more than a trick email sent to employees.

Phishing has emerged as one of the most potent forms of mass identity theft, and has proven to be a very effective way to trick millions of users at a time into revealing confidential information that can then be used to steal their identities.

“ Different reports over the last few years have suggested that more than 150 million phishing emails are churned out each year, and that more than 90% of these emails are used to hide and deliver malware. ”

Phishing attacks usually start as an email from what appears to be a legitimate and well-known organization, often a bank or credit card company. Or it can appear to come from a customer, a colleague, or even an insider. The email could claim that the sender is either verifying or updating account information, or conducting a security exercise, and in order to do so requires you to verify your username and password information to keep your account up-to-date. Or it could be more subtle, asking you to verify some internal workplace information, identify an attached document, or view a resume.

The email often includes a veiled threat – for example, if you don't respond immediately your account will be closed in 24 hours, or you'll get into trouble with the IRS, your boss, or a customer. The email will usually contain one or all three of the following traps – a request that you reveal some sensitive information (like a password), an attachment loaded with malware that will infect your computer or device once clicked on, or a link to a fake website that will do both.

So Why Go Phishing?

Why would professional hackers and crime gangs invest so much effort in swamping consumers with so many bogus emails? Because it works.

An annual study by Verizon found that:

- Two-thirds of electronic espionage cases can be traced back to phishing.
- 23 % of recipients open phishing messages.
- 11% open attachments in phishing emails.
- It takes an average of 82 seconds from the time a phishing campaign is launched until the first victim clicks on one.

Of course, when the first phishing expeditions appeared they were very easy to spot. For one thing the emails were fairly crude, and the very poor spelling and grammar were usually enough to expose the fraudulent emails.

But today the emails and web sites are much more sophisticated, using realistic graphics, logos, and marketing language you'd expect from a professional company. And the more targeted phishing emails will be based on research into your employer and executives that's going to make these attacks increasingly hard to detect and prevent.

What we have learned from these kinds of attacks is that crooks are constantly adjusting and improving their attacks, and always with the focus on getting into our comfort zone where we trust the party sending us the email because we think we know them. It's just another example of getting inside the minds of victims and luring them into familiar territory where a theft is easiest.

“ *Did you know?* The massive Target Stores data breach in 2013, that snagged more than 70 million credit and debit cards for hackers, all started when an employee at a small Target HVAC vendor simply clicked on a phishing email. That email contained undetectable malware that unleashed one of the biggest data breaches in history. ”

So Why Does Phishing Work?

Mainly because of poor consumer education and lack of awareness. In a study a few years ago by Harvard University and UC Berkeley called “Why Phishing Works,” 90% of subjects in the study were unable to pick out a highly effective phishing email when simply judging whether or not it was genuine.

Using a spoofed Bank Of the West email with a phishing Web site www.bankofthevest.com (with a double “v” instead of “w”), a padlock in the content, spoofed VeriSign logo, a bogus certificate validation seal, and a pop-up consumer security alert, 91% of participants guessed it was legitimate.

And when presented with a genuine E*Trade email that directed recipients to a legitimate secure site with a simple, graphic-free design optimized for mobile browsers, 77% of participants guessed it to be a fake. And nearly a quarter of participants in the research study didn't look at the address bar, status bar or security indicators on the phishing sites.

“ *Phishing from the Crypt*

With so many phishing emails now containing malware, hackers have a new tool to help make sure the malware gets through undetected. It's called “crypting,” a service provided by hackers to hackers that for just a few hundred dollars will test the malware against dozens of the most popular antivirus software programs and tweaked until it can't be detected by any of them.

”

How One Phish Destroyed a Small Business

In a previous chapter, I spoke about how a phishing email closed down a small business. When an employee at a small escrow firm in Southern California did something that millions of employees do around the world every day, he or she had little idea of the enormity of that mistake. The employee clicked on an email they shouldn't have. But they had no idea at the time that single and simple mistake would cost them their job. And costs the entire business too.

That phishing email contained one very nasty type of malware known as a banking Trojan, and that single click allowed the Trojan to sneak past security, hide on the employee's computer, and just wait. As soon as that employee accessed the company bank account, the Trojan was able to steal the login and password, take over the account, and start transferring money out of the account.

By the time the attack was discovered, more than \$1.5 million had been looted and transferred to accounts in Russia and China. And while some of the money was recovered, \$1.1 million was not. And because the money was in escrow, it didn't actually belong to the business but to its clients.

More than 20 clients were out their money, the small business had to borrow at a very high interest rate to cover losses, and regulators give the business very few options. And when the

escrow company's bank denied any liability and even suggested it was an inside job, it was more than the business could bear. Within weeks, the company was forced by the State of California to close its doors and lay off all 9 employees.

So How Can You Avoid Being Phished?

- Just say no! Phishing is probably unique amongst crimes because of one major difference. In order to be successful phishing requires the victim to be a willing, albeit unwitting participant. You, the target, need to respond to the phisher's request to hand over your personal information, through an email, a web site, or a phone call. If you don't cooperate, the crime can't happen.
- Kick the Click! If the phishing email isn't asking you to share confidential information, it's probably instead (or also) hiding some kind of malware that's just begging you to click on it. If you resist the urge to click, the attack fails, and you save the day.
- Never provide confidential, personal, or security information in response to any email. If the email claims to be from a financial institution you have an account with, call the institution directly using the customer service number listed on their web site.
- Teach all family members to be wary of such emails - it only takes one unsuspecting user.
- Be very careful when typing in the url or web address of important web sites like your bank or credit card company. Many bogus phishing or "pharming" web sites lie in wait for users to make the mistake of mistyping a web address and revealing sensitive information to what they think is their bank or ISP.
- Don't reveal any confidential information to phone callers, even if they claim to be from your bank, the IRS, some kind of tech support company, or any other organization. No such organization would ever request such information without first proving that they are legitimate.

- Minimize the amount of personal information you make available, especially in online communities like LinkedIn, Facebook, and Twitter, as well as job-hunting resume sites. Thieves can steal this information to create very personal and targeted emails that can be very convincing.
- Be extra vigilant for phishing emails around major events, like elections and natural tragedies. Phishers can exploit the media attention to create very real looking pleas for help or support.



INTERVIEW WITH A THIEF

Part 4 - There's A Million Ways To Get Your Social Security Number

THIS IS TAKEN FROM THE TRANSCRIPT OF AN INTERVIEW WITH IDENTITY THIEF "RAY" IN A CALIFORNIA JAIL IN 2014.

"There are always ways to get them {Social Security Numbers}. Personally, I still have a membership as a private investigator on a website where if I need your Social Security Number, all I need is your first, middle, last name and an address where you previously lived within like the last 10 years. If I give them \$57 or \$58, they'll give me your Social Security Number within 24 hours.

There are other little tricks where I can get it, without just getting it from your mailbox. There's one internet site that's an electronic check-processing site. And if I just give them any check number, ABA routing number and account number and a check number, they then ask me what's my name.

And if I put your name in there and your address, it'll pop up with four different possible Social Security numbers for you, and the last four digits are x'd out, but the first five numbers of the Social Security number are right there. And if you know anything about Social Security Numbers, they start on the east coast with 0 up in Maine, and they go to the west coast, they issue 6s.

There's a million ways to get your Social Security number without you actually telling it to me. It's easier to get the credit report once you have the Social Security Number. It's very easy. A few years back the government made the credit reporting agencies give you a free credit report every year. And then you had all these websites pop up, myfreecreditscore.com and a lot of others.

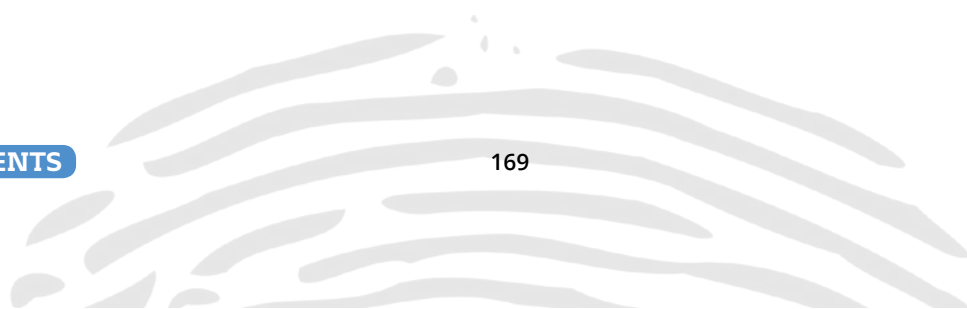
And I'll log on and say I want to check my credit and give them your birthdate, which is very easy to get, especially with social media today, ancestry.com etc. The birthdates take a second to find. I have your Social Security Number, I put that in there and I put your name in there. Then it's going to ask me a few qualifying questions about you, which are very easy to guess, they're multiple choice.

“

That's just one way to game the system that's out there. If I try to get 10 credit reports having the date of birth, Social Security Number, I'll probably get 6 or 7 just by guessing the combination because you use common sense and most people, their answers fit into a certain category, you know what I mean?

”

Or I'd just buy it from the Internet and like I said, \$29 and I'll get it, I have it in three minutes. It's very easy. And it costs me \$29. That \$29 investment, once I get your credit report, if you have good credit, I can make thousands."





THINK SECURITY FIRST!



CREDIT MONITORING, FREEZES, AND ALERTS

SIMILAR, DIFFERENT, IMPORTANT

CHAPTER 20

As a consumer, you have plenty of tools to help you create those critical layers of protection around your identity. But none of those defenses are perfect, and even less so if you don't know what to expect from them.

When it comes to protecting your identity, three essential tools are available to most consumers. At least the adult kind. They are:

- Credit monitoring.
- Fraud alerts.
- A credit or security freeze.

Credit Monitoring

In the early days of identity theft, subscribing to a credit monitoring service was the only real option most consumers had to protect their identity. When the first monitoring services were launched, they were very bare and rudimentary. The first one I ever used monitored (really just checked) one of my three credit reports once every three months.

Not very comprehensive or effective and plenty of time in between checks for thieves to do a lot of damage. Luckily for consumers, and dozens of companies making money from them, credit or identity monitoring services have come a long way and today usually include:

- Round-the-clock monitoring of one or all three credit reports.
- Monitoring of all kinds of places, from public websites to the dark web, for any hint that your information is exposed, for sale, or being used.
- Personal guarantees of up to \$1 million if you ever do fall victim.

- Access to experts 24/7 to help you resolve an issue.
- All kinds of additional security bundled in, like antivirus, password managers, and lost wallet protection.

The problem for consumers is that most of these features may just be a waste of time, and therefore the services a waste of money.

For example, credit monitoring doesn't actually prevent identity theft, but instead just alerts you that it's either happening or about to happen. Some services that have partnerships with networks of companies can actually use monitoring to instantly alert of any attempt to use your personal information, but they're far from perfect too. A credit or security freeze will do a much better job of preventing identity theft without any intervention from you and without the hefty monthly fees.

Dark web monitoring is a stretch at best, and at worst, simply deceptive. Your personal information is probably already out there, in all corners of the web, and mainly because of the thousands of data breaches in just the last few years. So you shouldn't need to pay a monthly fee to be told what you should already know.

And most of these services are very vague about the true meaning of deep – where on the dark web do they check, how many sites do they check, how deeply do they check, and how often? The really bad guys, and the ones you really need to worry about, are not hosting your personal information on sites where these services will ever find them.

“ In 2015 identity protection firm LifeLock paid more than \$100 million to settle charges that included deceptive marketing practices. It was the second time in its history Lifelock agreed to such settlements. ”

A much better option to deep or dark web monitoring is to just accept the reality that your information is already out there, someone's going to use it eventually (if they aren't already), and the time to protect yourself from that eventuality is now. And that approach is free.

And what about those \$1 million guarantees? Most of them are just standard insurance policies with lots of clauses that actually limit the payout to cover things (like lawyers and lost wages) that most victims will never actually need. In short, it's very easy to offer a massive and media-friendly prize when you're certain no one will ever claim it. So far, no one has.

Credit Freezes

A credit or security freeze allows you to freeze your credit reports for a specified period. The idea is that when your credit reports are frozen, no enquiries can be made about your credit. And that means a thief should not be able to apply for new credit in your name.

In spite of millions of dollars spent by the credit bureaus to lobby against freezes, they're now available in all states. And thanks to a new law that came into effect in September 2018, credit freezes are now free in every state, even for children. A freeze usually remains in place for as long as you request, but you can temporarily or permanently lift it at any time.

You'll need to place a freeze with each of the three main credit reporting agencies - Experian, Equifax, and Transunion. In order to lift the freeze you'll be asked to provide a unique PIN you were given when you placed the freeze - so don't lose it!

The credit bureaus typically don't like credit freezes because it limits their ability to sell your credit reports, but if you don't actively apply for new credit it might be worth considering. But bear in mind that if you have a credit freeze in place it could cause some temporary problems. A freeze will prevent you from applying for new credit. So if you apply for credit pretty often, or you have some big credit events coming up (like a mortgage) you might at least want to consider the timing of a freeze.

And don't worry about some of the scare tactics often used to spook consumers away from a credit freeze:

- A freeze does not hurt your credit score.
- A freeze does not stop you checking your own credit.
- A freeze does not affect your existing credit accounts.

- A freeze does not stop you from using your credit cards.
- A freeze does not mean you're forever condemned to paying cash for everything.

But one word of caution. The biggest downside I've seen to credit freezes is complacency. Many consumers mistakenly believe that a credit freeze stops all kinds of identity theft. So once they have one in place, they drop their guard. So it's worth the reminder. A credit freeze only prevents one type of identity theft – new account creation. And nothing else.

And another cautionary note. Some lenders, like payday lenders, don't always run credit checks, so in such cases freezes, monitoring, and fraud alerts are of no value.

Fraud Alerts

A fraud alert is a free service provided by the credit bureaus to alert you if an application is made for credit using your information. An alert is only supposed to be used if you suspect or detect a suspicious incident or transaction, but in reality you can place a fraud alert at any time.

Unlike a credit freeze, which requires notifying each of the three credit bureaus separately, when you place a fraud alert on one credit report that credit bureau is required by law to notify the other two main credit bureaus, so you shouldn't have to. And whenever you place a fraud alert you're also entitled to a free credit report so you can look for any suspicious activity.

But you should be checking your credit reports regularly anyway, and if you're not using a credit monitoring service you can check each of your three credit reports once a year free of charge at www.annualcreditreport.com.

A fraud alert can be put in place for 90 days. In some circumstances, you can place an extended alert that lasts for up to seven years, but I wouldn't recommend this. Apart from hampering your ability to get credit you really want, it could lead to complacency. And of course you can remove an alert any time you want.

But a quick word of caution about fraud alerts too. Fraud alerts have been so over-used, and in many cases misused over the past few years they may not work as you expect. While a fraud alert is a valuable tool if you suspect you have been a victim of fraud or identity theft, the alert is only of value if the bank, credit card company, or credit bureau responds quickly and appropriately. I've worked many cases where credit has been granted to a thief even with a fraud alert in place. Often the problem is poorly trained or new staff that don't know what a fraud alert on a credit report is, or how it should work.

So What Are Your Best Options:

- If you can, and it suits your needs, freeze your credit instead of monitoring your credit reports.
- If freezing your credit is not a good option, consider using one of the growing number of free identity monitoring and protection services that are available from companies like Civic (www.civic.com), Transunion/TrueIdentity (www.trueidentity.com), Credit Sesame (www.creditsesame.com), Credit Karma (www.creditkarma.com) and many others.
- If in doubt, freeze two of your credit reports and monitor the third. If thieves are stalking your identity, the monitored bureau should at least alert you that you have a problem.
- If you're just interested in checking or monitoring your credit reports, try Civic (www.civic.com), Credit Sesame and Credit Karma, or check your credit reports once a year free of charge at www.annualcreditreport.com. Other companies that offer free credit monitoring include WalletHub, Mint, Bankrate, Quizzle, Lending Tree and many others.
- Be vigilant to the point of paranoia. And beyond if it suits. The more vigilant and cynical you are, and the most basic precautions you take, the less vulnerable you'll be.
- But remember, there's nothing in the world that can prevent all identity theft. If anyone tries to sell you that, move on.



INTERVIEW WITH A THIEF

Part 5 - *“The First Time I Committed Identity Theft”*

THIS IS TAKEN FROM THE TRANSCRIPT OF AN INTERVIEW WITH IDENTITY THIEF “RAY” IN A CALIFORNIA JAIL IN 2014.

"The first time I committed identity theft, I remember specifically. I had a cousin who was in the army and he had passed away, from natural causes. This would have been around 1984 or '85. And for some reason I was wondering.

I had just gotten my first credit card. I think it was a \$300 Sears card. I applied for it and I got it, and it was so easy. I think I was 19 at the time. And I wondered, for some reason I wondered about, if this would work for somebody who had passed away. I had my cousin's information so I sent away for a card in his name, the same card that I had just applied for in my own name, and I got it in the mail. It was so easy.

So from there I proceeded to build that credit profile up for about a year and a half. I got a Visa, a MasterCard, Discover card, a couple of department store cards and then I just blew them out. I'd get like a \$1,000 limit on each card and then just spend it all and never pay the bills. And I always used a PO Box for the address, so I could just walk away from the PO Box, not pay it and that's where the bills would go. And it worked.

That was the first time I ever committed identity theft and from there on it was a pretty regular thing for me to do. Back then it was never a full time occupation. It was always a side occupation. I worked for the phone company, Bell Atlantic, and then I worked for an alarm and telephone company.

Later on I went to work for AT&T, got a top-level security clearance and went to work for the National Reconnaissance Office, NRO, and that's how I got out to California. And the whole time, identity theft and fraud were my passion. I went to work eight hours a day, but at night and on the weekends I was on the computer and mostly just doing not identity theft but what I would call identity creation.

I noticed when I was younger that my sister and I both got our Social Security cards at the same time. And this was when we were around 14 years old. And they came in the mail because my parents had gotten divorced and for some reason my dad had to get us Social Security Numbers.

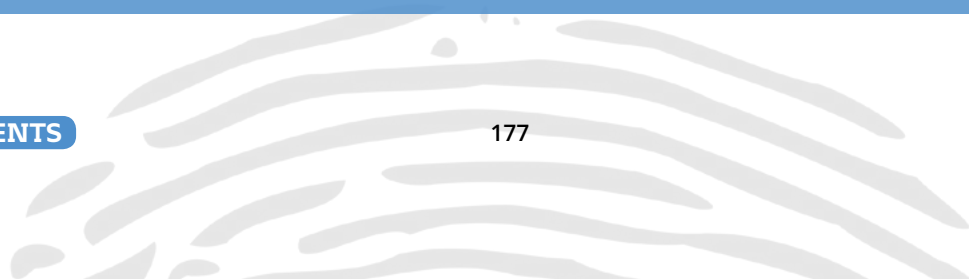
They both came at the same time and her and my Social Security numbers were only three digits apart. And I remember noticing that they must issue these numbers in sequence. So it stayed in my mind and when I was older, in my early 20s and I started to focus on identity creation, I asked somebody else who had a child, I said did you get your kid a Social Security Number yet, and what is it?

So I took that number and I just added four or five numbers to it, and this is before I knew how Social Security Numbers were area indexed, how they were distributed, what form they took, what all the rules were for Social Security and how they issued numbers.

“

I was constantly playing with the numbers. And I figured this would be a new number that the Social Security Administration had issued to a minor, someone who's 2, 3, 4 years old, and they wouldn't be using it for credit purposes until they were 18 or 19.

”



So I also did some research and found out that when the Social Security Administration issues these numbers, they don't really share anything with the credit reporting companies like TransUnion, Equifax, or TRW back in the day. And so I started playing with that and I would just make up an identity.

There would be no file under that Social Security Number with those credit reporting agencies until I presented them with a number and applied for credit. And even in most cases, the first time you do that it's turned down for lack of credit. But just because of that application, a file has now been created with those companies.

So the next time you do it, you have a much better chance of getting that \$200-\$300 card back then. And then a few years later they came out with secured credit cards, where you would pay a \$75 initiation fee and give them \$300. And they would give you \$300 in credit as long as they held \$300 of your money.

When they started doing that, and that was in the late '80s, every credit instance, as long as I had a Social Security Number that was recently issued, wasn't an adult and they hadn't created a credit record yet, I knew it would work. When I would present that number to the credit reporting agencies, and it was a virgin number, 100% of the time I would be able to get a \$300 secured Visa card. And once I got that, I knew that profile was gonna be good.

Sometimes I would make five identities in a month. And this is when I was working regular jobs and doing different things, going to night school. Once I got that card, I knew within 18 months I would have maybe \$12,000 in credit between the Visa, MasterCard, Discover card, a couple of store credit cards, because once I had that card, within 2-3 months, they started sending me pre-approved applications and now I just have to send them back.

And within eighteen months I would have enough money where it would make it worthwhile to blow that identity out - use the cards to buy some big ticket items, get big cash advances, expensive merchandise from stores, and then just walk away from that account, that identity."



THINK SECURITY FIRST!

HACKERS AND HACKING

A BRIEF HISTORY

Chapter 21

CHAPTER 21

Cyber crime is the greatest threat to every company in the world. So said Ginni Rometty, Chairman, President and CEO of IBM. She added “We believe that data is the phenomenon of our time. It is the world’s new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world.”

Hackers are nothing new, and have been around since before the birth of the personal computer. But like everything else, it’s the arrival of the Internet that gave them the power to create chaos.

So what created the hacker in the first place? According to an article in 2015 by CNN called *The Evolution of Hacking*, “Curiosity created the hacker. Hacking became the art of figuring out unique solutions. It takes an insatiable curiosity about how things work; hackers wanted to make technology work better, or differently. They were not inherently good or bad, just clever.”

The first hackers, in the early 1970’s focused their skills on hacking public telephone systems as a way to pay for long distance calls. Some of the earliest hackers grew up to become some of the greatest entrepreneurs.

“ In 1984 a young Russian hacker figured out a way to eavesdrop on the phones of Citibank and simply use a tape recorder to record the tones of account numbers and PINs as they were being entered. He stole \$10 million. ”

Talk About A Growth Industry

- In 2013, The Wall Street Journal estimated that the global cybercrime would soon cost \$100 billion annually.

- In 2015, Cybersecurity Ventures suggested that we were already at \$3 trillion annually and the cost could reach \$6 trillion by 2021
- To counter this crimewave, businesses will soon be spending more than \$200 billion on cybersecurity, and another \$20 billion on cyber insurance.
- Some types of attacks, like ransomware, have grown at more than 1,000% in a single year.

So What Is A Hacker Anyway?

There are now so many types of hackers and hacking groups, with different motivations, it might help explain why hacking is so hard to fight:

- Organized crime – typically well established and more traditional criminal groups that have turned to hacking and other cybercrimes as a way to make money from data.
- Organized groups – loosely organized and smaller groups who hack for a variety of reasons, usually financial, but only focused on hacking.
- Hacktivists like Anonymous and Lulz – expect these groups to grow as a highly effective way to protest all kinds of issues.
- Lone wolves – these individuals prefer to work alone, either because it suits their personality or because there's less risk of getting caught. Their motive is usually more financial than protest, and they often work as hired guns for others in search of data or vulnerabilities.

“ I always think hacking is a little bit of a superpower. ... You can see through everyone's personal lives. ... The fact you can manipulate people because you can hack them and learn everything about their personal lives — that's an immense amount of power. ”

Sam Esmail, creator of Mr. Robot

- Novices – everyone starts here, and this pool of would-be hackers is growing rapidly as part of the allure of the counter culture.
- State sponsored – safe to assume that every government on this planet is engaged in some form of hacking, either as a form of intelligence gathering or espionage, or a covert act of war. These organizations usually use a mixture of their own personnel and outside parties that are well paid and protected or sympathetic to the cause.
- The service providers – in the middle of this industry is a group of middlemen who profit by providing tools and services to make hacking easier and more profitable. Services like testing malware so that it can't be detected by antivirus software, renting out bot networks, developing malware and phishing kits, and churning out millions of infected emails.

Not All Hackers Turn Out Bad

Some of the most successful entrepreneurs on the planet started out as hackers, including:

- Mark Zuckerberg of Facebook.
- Jack Dorsey of Twitter
- Steve Jobs and Steve Wozniak of Apple
- Jan Koum of WhatsApp
- Bills Gates and Paul Allen of Microsoft
- Napster co-founders Shawn Fanning and Sean Parker

For example, Bill Gates, Paul Allen, and two other school friends were caught using an exploit to get free computer time at a company that had to agreed to provide a limited amount of time to students at their school.

Gates and Allen would have been around 13 or 14 at the time. They were allowed back on the computer when they agreed to find and report more bugs in return for free computer time. A year later, Gates and Allen started their first computer company and a couple of years after that, Microsoft was born.

“ Steve Wozniak and Steve Jobs started out by making and selling little blue boxes that allowed people to make free long distance calls. It was hacking to commit fraud and Jobs had often said that if not for those blue boxes, there would have been no Apple. And Steve Wozniak was kicked out of his first year in college when caught hacking at age 18 or 19. ”

Then there's Sean Parker. He got his first computer at age nine, was arrested for hacking military networks by sixteen, and later went on to launch Napster and appointed the first President of Facebook at age twenty four.

What Motivates Hackers?

It all depends on the hackers, but it's usually one, some, or all of the following:

- Steal information to use it for leverage, extortion, or commercial advantage.
- State sponsored intelligence gathering and espionage.
- Commit identity theft and other fraud.
- Protest and publicize.
- Expose and embarrass.
- Disrupt and disable.

- An act of aggression or war.
- Satisfy personal curiosity or test and improve hacking skills.

The Hacker Black Market

The industry of cybercrime has created incredibly detailed price lists outlining what one group of hackers will charge another for the essential services of hacking. In 2016, security magazine Dark Reading assembled a list of the latest fees, as an example of just how easy and cheap it is to build a business from hacking.

For example:

- A network of bots, which can be used to attack other computers and websites, or infect millions of computers, can be rented for around \$60 a day or \$400 a week.
- To rent a complete ransomware kit will cost about \$1,000 a month, with a piece of quality malware costing \$10.
- A compromised website or server, ready to be accessed and exploited, costs less than \$5.
- A bullet-proof server able to resist takedown by investigators or law enforcement costs just \$3.
- Fraud tutorials, like how to steal and exploit credit cards, costs as little as 35 cents.
- A fullz, or complete file including card numbers, security code, name, date of birth etc., costs up to \$30.
- A bank account with a balance of \$5000-\$8000 can cost \$200-\$300.

- Bank account logins can be purchased at a rate of between 1% and 5% of the account balance.
- Skimming devices, to steal card and Pin information from ATMs and gas pumps, can cost less than \$400. Not much when you consider one skimming operation can easily make \$250,000 for more for crooks.

“ When banks started to request things like utility bills as an extra layer of identification, hackers were on it. You can now “order” a very specific utility bill from hacker forums for as little as \$10. ”

And in January 2017 investigators discovered one of the first “Yelp for Cybercrime” web sites where hackers and cybercrooks could rate other cybercrooks on their honesty, and whether the stolen accounts and data they were selling were genuine.

What Can Hackers Do With Your Data?

If we assume that hackers are in possession of terabytes of stolen information, exactly what do they plan to do with it?

- If they have just email addresses, they'll use them to send spam emails to users around the world. That spam can be used to promote everything from counterfeit goods and costly scams to dangerous fake pharmaceuticals.
- Also just armed with email addresses, they can spread increasingly dangerous malware, hidden in links and attachments. That malware can break into your bank account, steal your personal information, or turn your computer into a remote controlled zombie.
- They can also use email addresses for convincing phishing schemes, pretending to be anything from your bank or credit card company to the IRS or Social Security Administration and hoping to trick you into divulging some sensitive information or paying for something you shouldn't.

- If the hackers have more than your email address, they can sell it to other hackers who might have some matching missing pieces, like a Social Security Number or credit card.
- They could sell your identity to criminals who want to use you to avoid detection or arrest.
- They could match some of your identity with someone else's information to create a synthetic or hybrid identity.
- They could use your identity to pay for costly and complex medical procedures. That not only potentially leaves you with a huge financial mess to clean up, it could also deny you access to critical health care, deny you health insurance, and attach your name to a procedure, illness, or disease that you never actually had.
- They could try to launder your information, passing it through seemingly legitimate data brokers who then sell the stolen data to marketers and researchers around the world.
- If the hackers manage to get your Social Security Number, they can turn your life upside down. They can open new lines of credit, commit tax and mortgage fraud, commit Social Security and employment fraud, help others get a job in your name, give your identity when arrested (leaving you with a criminal record), and impersonate you in all kinds of frightening ways.
- If the hackers get their hands on your email password, they can also get access to possibly years of information about your life, work, friends, and finances. They can also start targeting scams at everyone in your contacts, leaving the finger of blame pointing right back at you. And they can add a forwarding address to your account so that even if you change your password, they can still read your emails.

White, Black, or Grey Hat

The term hacker has evolved just as much as the industry of cybercrime and the role of the hacker. To the point that the word “hacker” is not necessarily a bad thing. Many experts argue that the word hacker never actually started out as something bad, but simply referred to curious explorers of technology frontiers more interested in figuring out how things really work. And often just to make them better rather than to commit a crime.

And in popular culture, just about everything is now being “hacked” – from cupcake recipes to raising families. But in the world of security, colors do matter a little, if only to help define the role of a hacker. For example, a black hat hacker generally refers to a criminal or malicious hacker, someone who hacks mainly for criminal purposes – to steal, break, maliciously disrupt.

White hat generally refers to professionals who hack as part of their security role, perhaps to test their own defenses, find flaws before the bad guys do, or develop new and better security tools. Grey hat hackers, as the term implies, float somewhere between the two worlds of good and over the line.

For experts like me, the main differentiator is intent, and to a lesser extent permission. If your motives are bad, there’s generally little to defend your methods. And even if your goals are noble, hacking into my computer without my permission if only to prove a point is no less an unacceptable intrusion.

Some Hacks Are Personal

In one case I worked on, a prominent plastic surgeon in Florida found out the hard way that a hacker had cracked his email password – even though he was paranoid about security and made the password every long and random.

But still they managed to steal or crack it. And the first thing the hacker did was use the victim’s email to identify at least two of his financial advisors. The hacker then requested one financial advisor to mail a check for \$50,000 to a person in Oregon.

Because everything in the email looked legitimate the financial advisor initially fell for the scam and started the payment process. The financial advisor only became suspicious when the hackers changed the recipient's name and address not once but twice.

And while the second financial advisor didn't move any money either, he did hand the hacker personal financial documents that included the victim's Social Security Number.

But the real fear for the victim was now the hackers knew who hundreds of his patients were, what procedures they had done, and all kinds of juicy information that could absolutely ruin the victim's reputation and business.

And a couple of weeks after I started working with the victim, he called me to say that out of 27 medical professionals in his group, at least 8 reported having their email accounts hacked in a similar way.



THINK SECURITY FIRST!

malware

THE HACKER'S FAVORITE TOOL

UNDERSTANDING THE SCOURGE OF
MALWARE

Chapter 22

CHAPTER 22

Of all of the tools in all of the land that hackers love most and consumers should fear most, it's got to be malware. Malware is the evil minion of the hacker underworld, created and raised to do whatever its creator bids, and without pause or question.

And with possibly millions of new malware variants detected *every month*, you can bet some of it is coming soon to a computer or device near you. If it hasn't already arrived. Malware stands for **malicious software** and is an increasingly broad catchall for all kinds of criminal software that includes viruses, Trojans, ransomware, spyware, key loggers, root kits, bots, and zombies, and many many others.

“

According to AV Test, one of the most respected labs dedicated to the world of malware, there were more than 850 million different types of malware in circulation by the end of 2018. Nearly 400,000 new types of malware are being detected daily.

”

And while malware was for a long time seen as a threat mainly to PCs, now there's some kind of malware for just about every kind of technology, device, and platform you can think of.

10 Reasons You Should Be Afraid of Malware

- 1 There are hundreds of millions of different types of malware and getting increasingly sophisticated every day.
- 2 There's increasing concern that much of this malware can easily evade the most common antivirus programs. A bad infection with questionable cures.
- 3 Much of this malware can be remotely controlled, constantly chatting with its creator, digging through your computer or bank account, and getting to know you uncomfortably well.

- ④ Malware has been behind some of the biggest data breaches in history, including Target Stores, Home Depot, and JP Morgan.
- ⑤ Ransomware has emerged as the scariest type of malware, especially for consumers, because it can be devastating for victims and gives an instant payoff for criminals.
- ⑥ Wherever there's technology there's malware. Not just on computers and mobile devices but infiltrating IoT and home automation, smart cities, power systems, transportation, military networks.
- ⑦ Malware is the favorite tool of virtually all hackers, because it works so well and so easy.
- ⑧ Malware is now considered a weapon of war by most nations and will increasingly be used as such.
- ⑨ There's so much malware, hiding in so many places, there's virtually no way to completely avoid it.
- ⑩ It's cheap and easy. A single piece of malware can be purchased in the hacker underground for as little as \$10, and is almost always delivered by email.

Today's malware is also smart. It's able, because it's programmed, to learn about your system, your behavior, and your habits. The goal is to learn as much as possible about the types of computers and devices you're using and how you use them. And when it learns that information, it's able to change, to morph, and to adapt to suit the environment it's now in - the host, that it's infected, which is you.

And in the case of some malware, like a banking Trojan, this software has been programmed to immediately identify where your bank accounts are, how and when you access them, and more specifically, what your username and passwords are. And once it has all that information, it makes it very easy for the malware to break into those accounts, bypass any additional security, and start moving money to other accounts.

“

Once upon a time, an employee at a small HVAC company clicked on an email he shouldn't have. That email hid some malware, allegedly created by a 16-year-old, that was able to bypass the employee's antivirus software and break into the network of one of the HVAC company's clients.

That client was Target Stores, and by the time the malware was detected it had stolen more than 70 million credit and debit cards and resulted in one of the biggest and most embarrassing data breaches in history.

”

How Malware Wiped Out A Business

One day, an employee at a small, 9-person escrow firm in Southern California clicked on an email they shouldn't. They had no idea that the email was infected with a nasty piece of malware, that the malware was able to sniff out their bank account passwords and access their accounts, and pretty soon the malware would wipe out the entire business.

The type of malware used is known as a banking Trojan. It's designed to bypass traditional security like antivirus software, identify and steal banking logins and passwords, and access and empty those accounts.

And this piece of malware did just that. Its first move was to transfer more than \$432,000 to a bank in Russia. The company's bank never caught or flagged the highly unusual transaction. The second move was to make another two transfers, this time to accounts in China, totaling \$1.1 million. And once again, their bank noticed nothing.

Because the money was escrow funds - meaning it belonged to the firm's clients and not to the firm - and because the firm was tightly regulated, it was given just three days to recover the funds.

Unable to do so, the firm had no choice but to close down. One click, one piece of malware, was all it took to ruin a business and destroy a dozen jobs. And was the bank liable? The bank said no, initially claiming the fraud was committed by one of the firms' own employees, and later claiming that it had no obligation to warn its customers of such risks or transactions.

How Malware Is Used By Crooks

In February 2016, one member of a gang of cybercrooks pleaded guilty in a scheme that used malware to steal \$1.2 million from 30 victims. It could have been worse. They nearly got their hands on \$6 million, and this is how it worked:

- The crooks sent malware-laden emails to their victims. When the victims fell for the email and clicked on the attachment, malware was launched on their computers.
- That malware was then able to access the victims' bank accounts when they logged in.
- Money was transferred from those infected accounts to "money mule" accounts in the U.S. Money mules are people who have been recruited to either let the crooks use their accounts to deposit money, or open up new accounts. Sometimes the mules don't know what they're getting into, but most times they do. Transferring money to U.S. bank accounts bypasses the red flags most banks have for money transferred to banks outside the country.
- Once the money was in the accounts of the mules, the owners of the accounts would send cashiers checks to a phony business owned by the crooks and from there the money was transferred through other businesses to banks in other countries.

Simple but highly effective. Commenting on the case, the FBI said *"Modern-day bank robbers no longer need a gunman and a getaway driver. Today, they just need a malware operator and money mules to carry out their crime from anywhere in the world."*

Infected Websites, Watering Holes, and Drive By Downloads

Malware isn't just focused on infecting computers or laptops or smart phones or tablets. In order to increase the spread of malware, hackers are turning to poorly protected websites. An estimated 5,000 to 10,000 new websites are discovered every single day, every 24 hours, that are either vulnerable to malware or that have already been infected with malware².

These infected websites are referred to as drive-by downloads or watering holes, and the goal is not necessarily to damage the website but instead to infect any visitors to that website. It's just another example of how creative and flexible hackers have become in making sure their malware infects as many victims in as many ways as possible.

And the most recent types of malware being discovered go one step further because they're able to encrypt themselves and their communications so that even when discovered it can be very difficult for security or forensics teams to figure out exactly what kind of malware it is and what it's been programmed to do.

And that same malware, once installed, is able to download and install more and often more dangerous malware, update itself, add additional tools and functionality, and live and survive and function undetected for months or even years.

“ Never underestimate how creative and determined hackers can be in targeting unprotected websites. In one case, hackers tried to target energy companies around the world with malware, and figured out that a number of employees of one of the target companies spent a lot of time at a local Chinese restaurant.

So what do you think the hackers did? They targeted the restaurant instead, discovered a vulnerability in the website of the restaurant, uploaded infected copies of the restaurant's menus, then simply waited for employees of the target company to go to the website, download the infected menus, and bring the malware right into their own company.

”

Phishing and Malware

As if bad malware wasn't scary enough, the delivery system is so easy it's just as frightening. It's as simple as email. A phishing email is a carefully, or sometimes badly crafted email

designed to trick the recipient into either clicking on an infected attachment or clicking on a link that downloads malware or takes them to an infected website.

And as I've mentioned before, phishing emails laden with malware have been used with devastating effect in some of the biggest breaches of the last few years. In fact, hackers and security experts cite malware-laden phishing emails as the favorite type of attack, the most effective and easy type, and the most difficult to stop.

The only thing that protects most users from this type of attack is a click-happy finger. And consumers seem to have plenty of those.

So What Can Malware Do?

- It can steal personal information on your computer.
- It can access your bank accounts and transfer every dime.
- It can hold your files for ransom.
- It can use your computer to attack other computers.
- It can use your computer to hide other stolen data or even porn.
- It can take control of your webcam and allow the hackers to watch you and your family.
- It can take control of home automation systems.
- It can crash your computer and make it unusable.
- It can use your computer or mobile device as a backdoor to your workplace, business, or clients.

The Growing Threat of Ransomware

Ransomware is such a major threat to every consumer and business, it's the only type of malware to earn its own chapter in this book. Ransomware is a type of malware that has surged in the last few years. Once this type of malware infects a computer, the first thing it does is encrypt every single file that it can find and then pops up a message to the user of that computer demanding a ransom for the safe return of those files.

That ransom can be anywhere from \$300-\$500, but it can be as high as \$3000. Failure to pay the ransom to the hacker, which is usually demanded in the form of untraceable bitcoin, usually means that your files are gone forever.

And even paying the ransom is no guarantee that you'll get your files back. In one case, a small law firm lost nearly 15 years of files thanks to ransomware. And the reason ransomware has become so popular amongst hackers is because it's so lucrative. In one case a gang made an estimated \$34 million from one ransomware campaign, and even smaller gangs can make more than \$30,000 a day just pumping out ransomware.

How Infected Is Your City?

A study of malware infections by software firm Enigma found that the cities with the greatest number of malware infections in the first half of 2018 were:

1. Atlanta
2. Orlando
3. Denver
4. St. Louis
5. Tampa
6. Newark
7. Washington
8. Cleveland
9. Madison
10. Cincinnati

How To Keep Malware Out Of Your Life

- First and foremost, and the golden rule for all consumers and even businesses, is constant vigilance. Most malware relies on mistakes, or carelessness, or lack of vigilance, to infect a computer. That's why the first and best line of defense is the constant vigilance of every family member.
- Golden Rule#2 – just stop clicking on stuff. Smart as malware is, most of it still depends on people like you clicking on stuff. If you don't click, malware loses.
- You've also got to pay very close attention to phishing emails, and learn to kick that click habit when it comes to invitations to click on links and attachments in emails you're not expecting.
- Make sure that you have the best antivirus software on every computer and device you use, but make sure you reinforce it with constant vigilance, good encryption, mobile security, constant patching and so on.
- Every family member has to be careful with and vigilant about what they download. It's still a very popular delivery mechanism for hackers, because it still works very well.
- Speaking of downloads, you've also got to be very vigilant about where you surf and what websites you visit, so that you can avoid those popular drive-by infections.
- And don't forget to patch. So many of today's attacks do nothing more than take advantage of known holes, or vulnerabilities, in popular software. Your best defense is to make sure that every computer and device you have is set to automatically download and install any updates and patches.
- I also spoke earlier about the risk of cross-contamination, meaning you and family members or employees downloading stuff to their personal computers or devices and then bringing those devices into work. And piggy backing on those devices is any malware that infected them somewhere else.
- Don't overlook any devices – computers, laptops, tablets, phones, Android and Apple. There are families of malware for every type of device so treat everything to an equally high level of security.

1 Symantec 2016 Internet Security Threat Report



THINK SECURITY FIRST!

WE'VE GOT YOUR DATA. WE WANT YOUR MONEY

THE GROWING THREAT OF RANSOMWARE

Chapter 23

CHAPTER 23

Talk about a growth industry. Over the last few years, a type of attack known as ransomware has emerged as one of the most dangerous and popular cyber attacks in the entire history of cybercrime. And it's probably coming soon to a computer near you.

Ransomware is so dangerous because once this type of malware makes it on to your computer, it can encrypt or lock every file it finds and hold it hostage until a ransom is paid. There's usually no way around it, no quick fix. You either pay up or lose everything. Yet even paying up is no guarantee.

Ransomware is popular with cyber crooks because it's profitable. Immensely profitable:

- The FBI estimated that criminal gangs made around \$24 million in 2015 from ransoms paid. By 2016, just 12 months later, that number had jumped to more than \$1 billion. That's right. I said one billion dollars (as I raise my pinkie finger to the side of my mouth).
- According to an article in Network World in January 2016 "ransomware is an easy business to get into, the payout is immediate, and it offers an ongoing revenue stream." According to one expert interviewed in the article, the \$1 billion number could actually be too low, and according to another, every security expert he has spoken to says that ransomware is their number one concern.
- According to The Ransomware Damage Report, published by Cybersecurity Ventures, global ransomware costs exceeded \$8 billion in 2018.
- Research firm Gartner says that there were between 2 million and 3 million successful ransomware attacks in 2018, and that the frequency will double year over year through 2019.
- And in 2016, security training firm PhishMe released a report which found that 93% of all phishing emails contained encrypting ransomware.

- The problem has become so serious, law enforcement and security experts from dozens of countries even created a group called No More Ransom to find ways to fight back.

“

In January 2017, Los Angeles Valley College admitted that it paid \$28,000 to hackers to get back files hijacked by ransomware.

”

Ransomware is not particularly new, but if it continues on its current trajectory it could be just as big a threat to consumers as it is to businesses. And if it ever achieves the greatness it seeks it could create a panic amongst consumers that no other security threat, even identity theft, has ever done.

And while much of the ransomware to date has been pretty predictable – mass spamming with canned phishing lures to trick users – ransomware authors are switching to more focused attacks. That includes more sophisticated ransomware, more spear phishing used to direct it, and targeting industries like financial services and healthcare where denying access to critical and time-sensitive data can hurt the most. And therefore pay the most.

And Hollywood Presbyterian Medical Center in Los Angeles has unhappily testified to that truth, recently forced to fork over more than \$17,000 to get its files back from a Locky ransomware attack.

“

Think your computer won't be infected? At its height, the Locky ransomware was infecting computers at the rate of 90,000 a day, and in one 72-hour spell had infected more than a quarter of a million computers.

”

If properly deployed, such ransomware can have near 100% effectiveness. Unlike most other malware, a deep computer sweep won't solve the problem, nor will a complete hard drive

wipe or rebuild, or even a brand new computer. If you're infected, the only cure is to pay up. Even the FBI admitted as much in a conference in 2015, although it later backtracked.

For criminals, encrypting a victim's data and holding it for ransom is a much less complicated business model than breaking in, searching for and stealing vast amounts of data, and then trying to either find buyers for it or monetize it in other ways. Encrypt it, and they will come, begging for a swift release. And the growth in ransomware-as-a-service is only likely to fuel growth.

So How Could Ransomware Be Different For Consumers?

- It can touch and impact them directly and personally, and in ways no other cyber or financial crime ever has. The notion that years of personal information, perhaps even very sensitive information, is now under the control of some very bad people could have a profound emotional effect on victims. And victims will likely have to fight the kidnapping and negotiate the ransom on their own. No 1-800 hotlines to help bail them out.
- Victims of ransomware will likely pay full price. In crimes like identity theft, while the losses per victim can range from a few hundred to a few thousand dollars, various forms of zero liability make sure that while most victims may lose some sleep, they don't lose a dime. With ransomware, victims will be on the hook for every dollar demanded by the kidnappers.
- It's almost impossible for consumers to stop ransomware. Like any other malware, attackers can easily "crypt" the malware to make sure that before it's dispatched it's successfully tested on all the most commonly used antivirus software. Which means once it arrives in a victim's neighborhood, it will slip; as the guards unchallenged.

○ Ransomware can come from anywhere. It can be delivered like any other malware – in infected emails, USB drives, drive-by downloads and malvertising. For most consumers it's going to be impossible to avoid contact.

○ The news for small firms is very troubling too. According to the 2nd Annual State of Ransomware Report, published by security firm Malwarebytes in July 2017, the impact of ransomware on SMBs can be devastating with 22 percent reporting that they had to cease business operations immediately after a ransomware attack.

“

FedEx attributed a \$300 million loss in 2017 to the NotPetya ransomware attack. The company reportedly did not have cybersecurity insurance.

”

○ It exploits the easiest vulnerability – lack of vigilance. Most malware succeeds because the victims fail. They fail to be aware and vigilant, to avoid clicking on stuff, opening attachments, updating software, visiting iffy websites. Just as phishing has become one of the most unstoppable threats to the enterprise, ransomware will easily exploit the biggest weakness of all – human nature.

○ It's almost entirely risk free for the attacker, which will only attract more attackers. Ransomware attacks are rarely targeted, but instead broadcast out by the millions and often using third party spammers. The ransomware will be on autopilot once it accesses a computer, and payment by bitcoin is still a very safe way to get paid anonymously.

○ And as word spreads from other victims, new victims will be more willing to fork over a modest ransom rather than face the prospect of losing every shred of data they've ever possessed. And that's the business model. A modest amount of pain to make an even bigger pain simply go away.

Of course this is all speculation, and I hope ransomware never lives up to its full potential. But as my grandmother was so fond of saying, *"If a cybercrime makes sense, it's already happening."*

There is some hope though. A growing number of security firms, including Malwarebytes, ZoneAlarm, BitDefender and many others now offer a variety of software tools that can help prevent, detect, and neutralize ransomware, and in some cases recover files that have been encrypted. Some of these programs are free, others cost a couple of dollars a month. A good investment either way.

So How Can You Avoid The Menace Of Ransomware?

- Like so many other threats, be very careful what you click on, and especially when it comes to emails and attachments.
- Be equally careful what websites you visit. Most malware is delivered either by email or through compromised and infected websites.
- Back up your data constantly so you still have a copy of whatever's been hijacked.
- Don't just back up online. As an additional defense, back up at least once a week to a hard drive and then unplug it from your computer. That can help stop the ransomware from encrypting the backup too.
- Keep all your devices, computers, and software constantly patched with the latest updates. Like most malware, the biggest weakness is often something you forgot to patch.
- Back up up precious and one-time files, like family photos, legal and financial files, and home videos, to an external drive or USB and leave them untouched so that at least they're safe if the worst happens.
- Use good antivirus and anti ransomware software on every computer and on your mobile devices too.
- Spread the word to stop the spread of the infection. That means speaking to family members or employees about the risks and the need for everyone to be vigilant.



THINK SECURITY FIRST!

PREVENTING IDENTITY THEFT

21 SIMPLE CHOICES

Chapter 24

CHAPTER 24

Identity theft is far too complicated to be solved by something as simple as a list of Top Tips. But these habits are a very good place to start.

One of the biggest challenges in preventing identity theft is that you as a consumer have little control over how others manage and protect your personal information. But that doesn't mean you should be helpless or hopeless. Make these simple suggestions part of your everyday routines and you should be able to minimize your exposure.

☐ Take It Seriously

Hiding in the herd or relying on zero liability are not good defense strategies. You can't completely avoid identity theft, but there are plenty of ways to minimize the risk, the eventual cost, and the worry.

☐ Monitor Or Freeze Your Credit

Most thieves head straight for your credit, and usually to open new lines of credit or apply for loans. Monitoring your credit reports will give you early warning. Freezing your credit reports will stop them in their tracks.

☐ Guard Your Mail

Collect it as soon as it arrives each day. Take your mail to the Post Office instead of leaving it out to be collected. Switch to online accounts to reduce the amount of mail you receive. And watch out for strangers in your neighborhood.

☐ Stop Clicking On Stuff

Resist the temptation to click on links in emails or attachments to emails. Way too often those links are used to hide malware that can quickly take over your computer.

☐ **Keep Your Computers And Devices Updated**

Much of today's malware works by simply taking advantage of vulnerabilities in common software, like browsers, that should have been updated. Setting your devices to update all software automatically can stop most of those attacks.

☐ **Be Careful Where You Surf And What You Download**

Hackers now hide their malware in compromised websites, and all you have to do to be infected is to visit those websites. So stay away!

☐ **Check Your Statements**

The more diligent you are about checking your bank and credit card statements, the more likely you are to discover if someone has your account information and is committing fraud.

☐ **Use Credit Cards, Not Debit Cards**

If thieves compromise your debit or ATM card, and especially with your PIN too, they can quickly empty your bank account. And while you should get your money back, it could take a while. Credit cards carry far less risk.

☐ **Be Miserly With Your Information**

The less you share about yourself, the less information others will have that can be compromised. So the next time someone asks you for a Social Security Number, date of birth, or email address, ask them if they really need it.

☐ **Talk To Other Family Members**

It only takes one weak link. So make sure you educate all family members about the risks of identity theft, how it can happen, and the good habits they need to practice.

☐ Be Careful On Social Networks

Social networks are a favorite haunt for hackers and scammers who can use them to find incredibly detailed information about you, your family and friends, your work and social life and so on. So mind what you say and share, and make sure your privacy and security settings are set to the max.

☐ Protect Your Home

Identity theft is the new burglary. Burglars know that information like Social Security Numbers, birth certificates, and tax returns are far more valuable than your brand new 60" TV. And a lot easier to haul away. Burglars also don't like to spend a lot of time in a home so hide your personal information where it's not easy for them to find.

☐ Be Careful When You're Traveling

Like I said earlier, thieves and scammers are everywhere, and identity theft is not just a U.S. problem. When you travel, bring as little personal information as possible, guard your wallet or purse, and avoid using guest computers at hotels – they can often be infested with nasty malware.

☐ Get Serious About Passwords

Your password may still be your only defense, and especially for things like email and bank accounts. So get serious about them. Make them long and complicated, unique to each site or account, and guarded at all times.

☐ Watch Out For Free Wi-Fi

There's so much free Wi-Fi available, from coffee shops to hotels, we often take it for granted. But Wi-Fi that's open to the public is also open to hackers, who can easily hang out nearby and eavesdrop on everything you're

☐ Move Away From Checks

Try using credit cards instead of checks to pay for things. Checks mean more documents to intercept, steal, and exploit, and could provide thieves with access to your bank account.

☐ If You Have To Use Checks

Don't include your address on the check. You don't need to, and if the check is stolen, the thieves have some extra personal information to work with.

☐ Make A Copy Of Your Wallet Contents

Take every card and document you keep in your wallet or purse – credit cards, store cards, ID cards, driver's license, medical cards, debit cards – and take a photo or make a photocopy of all of them. If your wallet or purse are ever stolen, you'll know what they have and what to cancel. To make it easy, put them all together in a grid, take a photo of the front and back, so just two photos should do the trick.

☐ Pay Your Bills Online

Paying online also removes two temptations from thieves – incoming bills and outgoing checks. Paying your bills online can help avoid those risks. Many online bill-paying services are packed with extra features, like regular reminders so you don't miss a payment. And most are free.

☐ Pick The Right Credit Cards

Some credit card companies offer a variety of extra consumer protection, like free credit monitoring, extra liability protection, and fraud assistance. So see if your credit card providers offer any extra security features and if you've activated them.

☐ Turn Your Alerts On

Most banks and credit unions offer a variety of alerts to protect your accounts and funds, including notifying you of any lodgments, transfers, or withdrawals, someone using an ATM with your card, low balances, attempts to change a phone number, email address, or physical address, accessing your account from another country or a different computer and so on. So make sure the ones you want are enabled.



THINK SECURITY FIRST!

DAWN OF THE ZOMBIE REFRIGERATOR APOCALYPSE

PROTECTING YOUR WORLD FROM THE
INTERNET OF THINGS

Chapter 25

CHAPTER 25

In 2016, a hacking group calling itself NewWorld Hackers claimed responsibility for a type of hack attack that most consumers would find, at the least, weird. The attack successfully took down or slowed down some of the best-known and most trafficked websites including PayPal, Netflix, and Twitter. But it's "what" the attackers were that might surprise most consumers.

To carry out the attack, hackers used malware to infect and hijack tens of millions of Internet connected devices like webcams and thermostats, in homes just like yours, and used those devices to both launch their attack and hide their tracks. Your home electronics were infected and turned into minions. Welcome to the dark side of IoT, the Internet of Dangerous Things.

It's not just homes that are being targeted. In January 2017, hackers managed to breach the networks of a hotel in Austria, hack the systems that managed the door locks on all the guest rooms, and instantly locked more than 100 guests either in or out of their rooms. The hackers only agreed to unlock the doors after the hotel paid a ransom.

And as more homes, businesses, and entire cities become connected and automated, hackers will increasingly target these home devices, and not just to enlist them as zombie attackers against big name brands. Hackers also want to use these devices to eavesdrop on you, steal your information, or even just mess with you a little.

Imagine a hacker with either a grudge or just a twisted sense of humor able to turn off your fridge or your heat, open your garage door, or spy on you and your kids using any webcams in the home?

The same applies to home assistants like Google Home and Amazon Alexa, and even toys that can electronically interact with your kids. All are fundamentally vulnerable to being remotely and maliciously controlled.

“

According to Cisco, by the year 2020 there could be around 50 billion IoT devices installed across the globe, or about seven devices for every person on the planet.

”

But of all the statistics and projections swirling around the world of IoT, one of the most troubling I've come across in the last few years came from research firm Gartner. Gartner estimates that by 2018, more than half of all the IoT solutions in use were created by startups that are less than 3 years old. Why is that so frightening?

Because those of us even remotely familiar with tech startups understand that in the almighty rush – to get the product to market, build the brand, win market share, get to profitability, gain followers and fans, manage endless funding rounds – security and privacy often get left behind, left sitting by the curb like overlooked children.

At least consumers seem to be aware that they should be worried, even if they don't plan to do much about it. A recent survey of 6,000 consumers in the UK by security firm BullGuard found that:

- More than a quarter of respondents said they are planning to buy IoT devices in the next 12 months.
- 66% of them are concerned about attacks against their devices.
- 57% are worried about privacy breaches.

The two biggest risks in the world of IoT are connectivity and complexity. While most consumers understand that these connected devices can collect and share significant amounts of personal information, most consumers will admit that they're nowhere near tech savvy enough to confidently check and adjust the security and privacy settings of their devices. Assuming that they're even able to do so.

“

The parents of a 10-month-old were awakened in the middle of the night by the sound of a stranger shouting at their baby. A hacker had broken into their internet-connected baby monitor and was yelling obscenities at the baby.

”

That same report from BullGuard found that 72% of consumers do not know how to configure a wireless router to protect a home network, and 22% of consumers who say they have advanced technical skills are not confident that they have the ability to keep their connected devices secure.

It's not just your home. Smart cities are quickly emerging around the world, creating opportunities for hackers to wreak havoc with street lighting, traffic lights, emergency services, and, yes, even parking meters. Can you imagine the chaos and potential risk if in the middle of rush hour hackers turned every traffic light permanently green? And by 2020, 90% of cars will be online according to Spanish telecom provider Telefonica.

So What Kinds Of Risks Are We Talking About?

- Cars that can be hacked to hit the brakes, make a sharp unexpected turn, accelerate without explanation, or simply die in rush hour traffic.
- Smart televisions that work by voice commands but in doing so can listen in to everything you say.
- Fitness bands that can record your vitals and share the info with complete strangers or insurance companies.
- Climate control systems and garage doors that can be hijacked remotely.
- A refrigerator that can churn out millions of spam emails.
- Webcams that can monitor and record everything you say and do.

There are growing industry efforts to do something that's rarely been done in the past when it comes to new technologies – bake security and privacy in early. For example, the Online Trust Alliance launched an IoT working group in 2015 (of which I'm a member) and over the last year has been working on what it calls its IoT Framework - a collection of 30 privacy, security, and sustainability principles targeted at connected home devices and health and fitness wearables.

Amongst those principles:

- All personally identifiable data in transit and in storage must be encrypted. This is including but not limited to wired, WI-FI and Bluetooth connections.
- Ensure all IoT devices and associated software have been subjected to a rigorous, standardized software development lifecycle process including unit, system, acceptance, regression testing and threat modeling.
- Enact a breach response and consumer notification plan to be reevaluated, tested and updated at least annually or after significant internal system, technical and/or operational changes.
- Ensure privacy, security and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download or enrollment.
- Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data that is reasonably useful for the functionality and purpose for which it is being collected.
- Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the “factory default.” [You can read the full list here.](#)

“

Is your wrist the snitch? There will be an estimated 173 million wearable devices in use by consumers by 2019, most capable of monitoring your vitals and reporting back over the Internet. ”

So what can we all do to make the evolution of IoT a pleasant and trustworthy experience?



Companies making and marketing IoT devices should at the very least adopt the OTA's 30 principles. They're simple, common sense and while not perfect are a very good starting point.



Those companies must make security and privacy a priority, baked in, and fully transparent.



Consumer education and participation are key. Consumers must be educated about both the potential and risks of IoT and the roles they have to play in protecting themselves. For example, the OTA and National Association of Realtors have created a [SmartHome checklist](#) that all consumers should be familiar with.



IoT device manufacturers must make it as easy as possible for consumers to program and reset their devices so they have greater control over their own security and privacy.

“

A disgruntled ex-husband took revenge on his former wife -- and her new live-in boyfriend -- by remotely messing with the thermostat in his previous home: *“When they are away on their weekend getaways, I crank the heat up to 80 degrees and back down to 40 before they arrive home. I can only imagine what their electricity bills might be.”* InfoWorld

”

Manufacturers and vendors should make it very clear, at point of purchase, exactly what kind of personal information is collected, how it's protected, and how it's used and shared. That's the only way to allow consumers to make informed decisions.

And what will I be doing to protect myself? I can tell you what I won't be doing. No more naked yoga in the kitchen. At least for now.

One of the greatest defenses every consumer should have when it comes to security and privacy is a healthy dose of paranoia, and especially when it comes to the surge of Internet connected devices living (and listening) amongst us in our homes, offices, and cities. We know these devices increasingly have the ability to listen to us and communicate with each other. What we're not certain about is what that will all mean.

So How Can You Protect Yourself From Your "Stuff"?

Think about what you're installing, what it's capable of, and if you're capable of effectively managing it.

- Check and if necessary reset the password on any device you install in your home and any home network they connect to.
- Read the fine print. The terms and conditions often hide small print allowing the manufacturers to monitor and collect data.
- Research the manufacturer, and especially their experience and trust reputation.
- Keep all devices constantly updated, because many attacks will come in the form of exploits of older and more vulnerable software.
- Check the app. Many IoT devices come with apps for easier control but many of these apps have security and privacy flaws. Read the reviews first.
- Protect your network. Your home network is the gateway and the gate works both ways. So control what the devices are sending out and who they might be letting in.



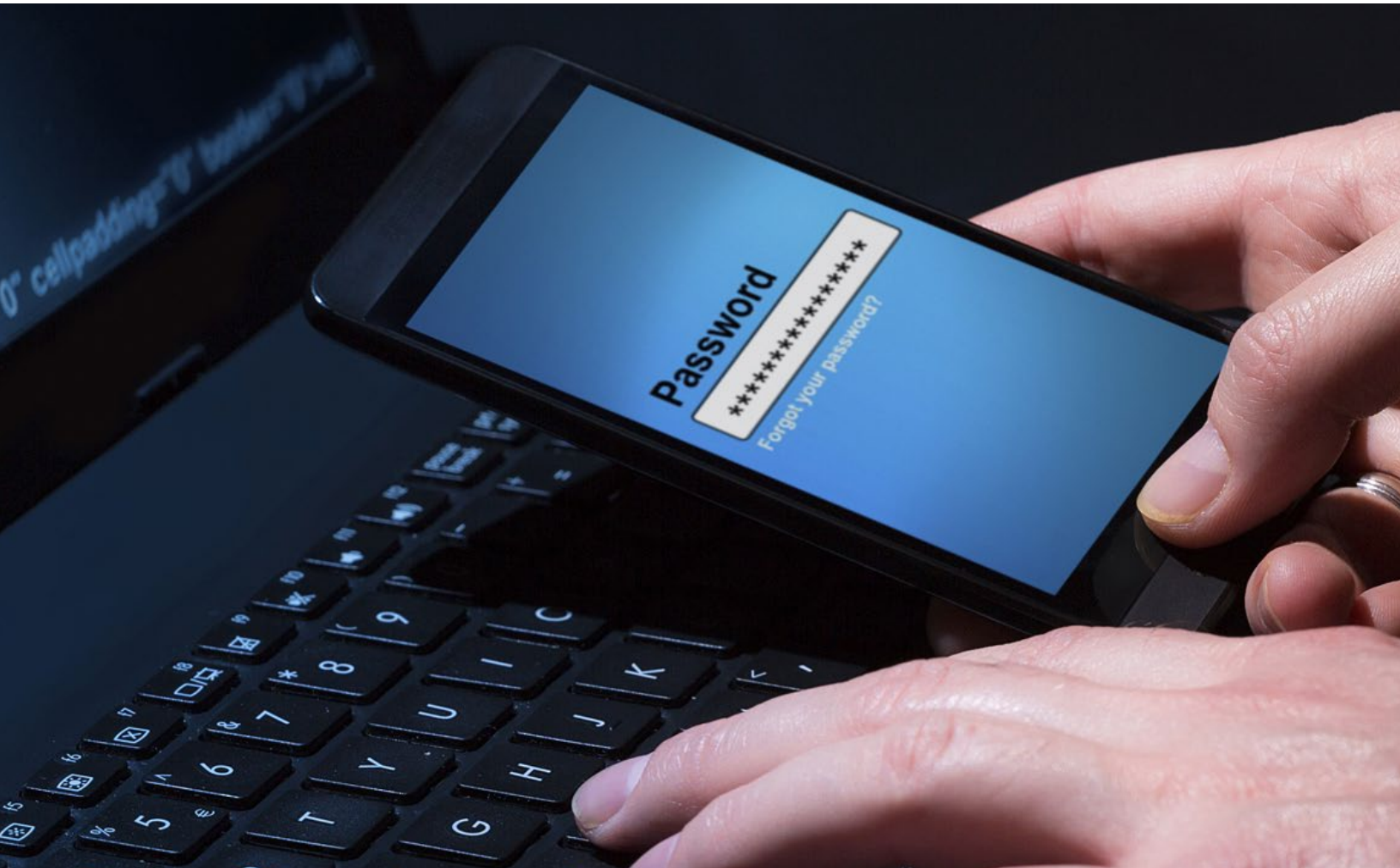
Explore the growing number of security options, like emerging IoT security systems that will help you set up and secure all your devices from one simple console.



If you don't need it, just don't do it. No matter how cool they appear, or how uncool you might look, don't install home connection or automation devices that you don't need. Or at the very least, just don't connect them to the Internet.



THINK SECURITY FIRST!



HACKERS IN YOUR POCKET

WHY THE SMALLEST DEVICES ARE THE
BIGGEST TARGET

CHAPTER 26

Do you remember your first mobile phone? Not the first one you owned but the first one you ever set eyes on? Mine was in the mid 70's. It wasn't exactly a mobile phone but a car phone, which was really the first generation of mobile phone because it wasn't attached to a building.

It was on Dawson Street in Dublin, right around the corner from Trinity College. Built in to the center console of a beige Roll Royce Silver Shadow was a matching plastic phone complete with curly cord and flashing red light. Things have changed a little.

There are now more mobile devices in the world than there are humans, and pretty soon there will be an average of two mobile devices for every biped with a soul. And the rate of adoption and growth of mobile is even more startling. According to Cisco, by 2020 there will be 5.5 billion mobile users, representing 70 percent of the global population. And many of those mobile users will have more than one mobile device. Like the hundreds of millions of wearable devices with functionality similar to many phones.

“

Current industry estimates put the number of Internet-connected wearables around 780 million, which works out to a wearable device on one of every 10 people on Earth.

”

What's not so surprising are all the security risks that the surge in mobile use and dependence has created. Until the Government introduced a “kill switch” in the U.S. a few years ago that allowed an owner to remotely disable a stolen phone, more than 1 million smartphones were being stolen every year. But even with that risk reducing, others are rising. The biggest risks may now come in all the apps these devices are running – neatly 4 billion in total just between the Google Play Store and Apple's App Store.

And with so many people now living and working on their phones and tablets, hackers are there too. Security firm Trend McAfee claims that there were more than 20 million different types of mobile malware by the end of 2017.

The Risks of Mobile

The risks created by mobile are many and scary, and especially as more users co-mingle business and personal tasks on the same devices.

Those risks include:

- Data leakage
- Users installing unapproved or vulnerable apps
- Holes created when accessing corporate or personal networks
- Failure to update apps and operating systems
- Forgetting to wipe phones properly before disposal
- The growth in mobile malware
- Privacy issues
- Jailbreaking devices
- Careless Wi-Fi use
- Device loss or theft

Apart from the value of your devices, your phone or tablet could be a treasure-trove of information that thieves can use to piece together your identity, including:

- Personal and family information, including names and addresses, contained in email and texts
- Personal, family, and work phone numbers
- Work information including computer logins and passwords
- Financial information and financial apps

A six-month study by McAfee of 190 million apps found 37 million instances of malware.

- Location information that can tell the thief where you go and where you hang out
- Downloaded books and music that clues the thief into your personal tastes
- Photos of you, your friends and family that can help the thief identify you or impersonate you

Lookout Mobile Security

There are lots of great and often free apps that will not only protect your phone and tablet and their contents, but also use your phone as a warning beacon in case of a security event.

One of my favorites is Lookout, one of the first and probably the best apps. And the basic version is absolutely free. Lookout has something called a Mobile Threat Network that's built upon the world's largest app database, which includes millions of mobile applications and grows daily as more applications are added to app stores around the world.

When it comes to mobile infections – the number of mobile devices infected with malware – the U.S. ranks #2 in the world after India. When a threat is positively identified, the Mobile Threat Network automatically updates the Lookout Mobile Security app to instantly protect millions of users worldwide.

In order to prevent identity theft, financial fraud and the loss of your most personal data, Lookout can help you avoid risky behavior, like connecting to an unsecured Wi-Fi network, downloading a malicious app, postponing security updates or clicking on a fraudulent link. Lookout can even show you which apps can access your location and personal data.

Even if your phone is on silent, activate a loud alarm to find it nearby. Lookout helps you find your phone if it's lost or stolen, quickly and easily, even if it is out of your hands.

If you don't want to gift your favorite phone to a complete stranger, here are a few tips to keep in mind:

- Less is more. If you don't really need to use your device in a public place, keep it in your pocket and find some other way to distract yourself.
- Eyes up. If you're using a phone or tablet on a train, a bus, subway, park bench, keep an eye on the people around you so you're not surprised by a quick grab-and-dash.
- Be especially vigilant if you're on your phone on a busy street. It's not uncommon for a thief to emerge from a crowd, snatch a phone from the hands of a victim, and just disappear back into the same crowd.
- Keep as little personal information as possible on your phone. Here's a revolutionary idea – use the phone as a phone, and not a portable data locker. If your phone is stolen, your life doesn't go along with it.
- Consider using one of the growing number of free apps that will back up and restore your phone's contents, disable your phone, and even help locate it if it's stolen.
- Always use a password to protect your device, whether it's a PIN, pattern or some kind of biometric like a fingerprint.
- Be very careful about what apps you download, where you download them from (stick to the Google Play Store, the Apple App Store, or a company-approved source), and the permissions you allow them.

10 Ways To Protect Your Laptop And Tablet

One thing we know about hackers and identity thieves is that they always follow the crowds and the data, and as more people use laptops and tablets to run the personal and professional lives, the more attractive these devices become.

Laptop theft and loss are far more common than you might think. Mobile security company Kensington has estimated that a laptop is stolen every 53 seconds and most are never recovered.

And the loss of a laptop or tablet can be devastating for your employer and your workplace too. According to Data Loss DB, a research project aimed at documenting known and reported data loss incidents and data breaches world-wide, more than 30% of data breaches were the result of a lost or stolen laptop, mobile phone, or other portable media device.

So here are some simple reminders of the steps you can take to protect your device from theft and its consequences:

- **Encrypt it!** This should be the fundamental rule for every laptop, and many experts argue that all laptops should be encrypted by default. Encryption locks either the entire hard drive or specific folders with an unbreakable code. So if the laptop is lost, the data is safe.
- **Use strong passwords.** The next best layer of security after encryption is the password, and while a determined thief might be able to get past your password, it's still a powerful defense. So make sure that your laptop is set to request a password every time you want start or use it, and make sure it's a very strong password.
- **Don't use a laptop case** – it's a bright red flag to thieves that you're carrying a laptop. Most laptops and tablets are small enough to carry in a briefcase or backpack.
- **Be careful using Wi-Fi** – because they're supposed to be accessible to the public, Wi-Fi networks are also easily accessible to hackers and eavesdroppers. So if you have to use a Wi-Fi network in a public place like a coffee shop or hotel, don't use it to access anything sensitive like your bank account.
- **Don't use your laptop to store or move sensitive information.** If you lose it, you only have to worry about the value of the device itself and not the harm the thief can do with it.
- **Treat it like a desktop computer.** Make sure you always have layers of up-to-date security, including firewall, virus protection, browser security, and all the other security software that you would expect on a desktop.



Don't forget tablet security. I'm amazed to see how many people are still not aware that there are anti-virus programs available for Android and Apple tablets. Or that they even need them.



Use a tracking and recovery service – services like LoJack, Lookout, Prey, and YouGetItBack.com will help you track and recover your laptop, tablet, or smartphone, often for just a couple of bucks a month and sometimes free.



Spare the apps – don't download endless apps just because they're cool or free. Only download apps you really need and make sure they're from trusted sources.



Most important of all, be **careful where you leave your devices**. Laptops and tablets have become such a familiar accessory, often times they get left behind – at hotels and bars, in taxis, at airports. Just because they're portable doesn't mean they should be forgettable.



THINK SECURITY FIRST!

PASSWORD
●●●●●●●●

PSST! WHAT'S YOUR P@\$\$WORD?

THE GOOD, BAD, AND UGLY OF
THE STILL ESSENTIAL P@\$\$WORD

Chapter 27

CHAPTER 27

Remember all that advice that experts like me have been beating into you for years – about making up long strings of garbage-like passwords by using a random mixture of upper case, lower case, numbers, letters, symbols, a pint of your own blood etc.?

Well, apparently time and research appear to have schooled us that all that well-meant advice was probably not the best and probably didn't do much to make you any more secure. Frustrated maybe, but not secure. But more on that later.

A hacker's favorite word is password because in spite of all the sophisticated malware tools and tricks available to most hackers, most have to do nothing more sophisticated than try a few of the common and predictable passwords and they'll probably get in.

And while you've probably heard for years that a reasonably complex 8-character password is more than enough to frustrate the intruders, forget that advice too. It's now widely accepted that hackers can crack a complex 8-character password in the blink of an eye. Literally. About a second is all it takes.

So you can understand how easy it must be for hackers to crack obviously dumb password choices like password123, admin, and letmein, right? And yet, we know that these are still some of the most popular passwords in use today.

And the winner is? The most common password in use in 2018 was....123456.

Every year, a company called Keeper Security crunches the millions of passwords exposed in data breaches to get a better idea of what passwords are used the most often. And the news is downright frightening.

According to Keeper, the top 10 most commonly used passwords in 2018 were:

- 1 123456
- 2 123456789
- 3 qwerty

- 4 12345678
- 5 111111
- 6 1234567890
- 7 1234567
- 8 password
- 9 123123
- 10 987654321

And even worse, 4 of the top 10 passwords contain six characters or less. Which makes them just as easy to crack as no password at all. Seems like most consumers are still not getting the message.

Is Conventional Advice Just Plain Wrong?

Much of the conventional wisdom about password strength and effectiveness is rooted in documents authored years ago. One such document quickly became the de facto authority on the subject, and was published by the National Institute for Standards and Technology (NIST), more than a decade ago.

But in a series of interviews in August 2017, the author of that guide admits that he, and countless experts since, might have been plain wrong. He now says that creating random passwords from a mixture of everything on your keyboard, and then changing all those passwords every three months or so, has proven so difficult in real life that most users default to their old and easier ways – one easy-to-remember password for everything. Hardly the best fall back.

“ It takes hackers only .29 milliseconds to crack a 7-character password consisting of all lowercase letters. ”

So instead of a password like P@ssW0rd123!, experts are now suggesting that a sequence of random words that don't make any sense together or which don't follow a pattern are a much better bet. Better because they're still very hard for hackers and their technology to crack, but will also be easier for users to remember and change.

In other words, the password "telephone orbital march tyrant" could be much harder to defeat than "Th!\$!\$MyP@\$s\$wrđ"

So Just How Easy Is It To Crack A Typical Password?

A lot easier than you might think. In an article in March 2017 by security website Web Of Trust (WoT), it takes hackers only .29 milliseconds to crack a 7-character password consisting of all lowercase letters.

According to the article:

- 1 8-character passwords take a few hours to crack.
- 2 9-character passwords take about a week to crack.
- 3 10-character passwords take months to crack.
- 4 11-character passwords take about a decade to crack.
- 5 It would take nearly 200 years to crack a 12-character password of mixed lower case letters!

An article on the topic by The Verge in 2017 suggested that *"the password 'Tr0ub4dor&3' could be cracked in about three days with standard techniques, due to its predictable capitalization, numeric substitutions, and special character use. The password 'correct horse battery staple,' written as a single phrase, would take 550 years."*

Bad, Bad Habits

But that's not the worst news. A Telesign study found that on top of really, really poor password choices, users were also doing very bad things with those passwords:

- 1 21% of those surveyed said they have been using the same passwords for more than a decade.
- 2 47% said they've been using passwords that they haven't changed in five years.
- 3 Not surprising, 73% say they regularly use duplicate passwords for online accounts.
- 4 More than half of those surveyed said they use five or fewer passwords for everything.
- 5 And on average most people say they use just six passwords to guard an average of 24 online accounts.

And in another study, more than half of all adults surveyed admit to using exactly the same single password for most of all the websites they have accounts with.

“ One forgotten password. In 2004, the owners of a small software company in New York forgot to cancel the password of an employee they had just fired. Using that password, the employee, or now former employee, was able to access the company's networks, and through them access thousands of customer accounts. The resulting crimes cost more than \$100 million. ”

Users now face a real problem. Free password cracking tools, like Cain and Abel and John the Ripper, claim to be able to test more than 6 million different passwords every second. And professional hackers can create their own customized password cracking dictionaries that can contain upwards of 60 million of the most common words used in passwords. Even those using punctuation and numbers.

Look At Your Phone For The Answer

It's not like we haven't tried to fix the password problem. We've tried things like pass phrases and password managers, which both work fine if properly implemented. We're still trying biometrics, including fingerprints, voice recognition, and iris scanning, but too many consumers still seem to resist these approaches. There's that human problem again. We're just not that good at implementing things correctly. In the early 1990s I was working on a voice verification-based access control system for telephone banking for Britain's largest bank. It worked, it was affordable, it was easy to use, it had a very low failure rate but eventually the bank said no. It was just too much of a switch for consumers to handle.

But the security world still sees biometrics as the replacement for passwords. The solution, and the presumptive heir to the throne of the password, might be on the end of your nose. Both ends, in fact. Remember when I said "If I just look at my phone..."? There's the clue. Welcome to your PassFace.

Facial recognition is now emerging as the most likely heir to the password. Your finger might still do all the walking, but now your face can do the paying. And accessing and logging in, and confirming and authenticating and all those other things the stinking rotten corpse of a password (we miss you dearly) used to do.

So why does your face stand a better chance of doing what your brain couldn't? I guess the answer is also in the sentence. Because your brain may now and finally be out of the equation. Amazon recently revealed that it has filed for a patent that replaces a password with facial recognition. Not that the idea is entirely original. A number of banks and credit card companies have been offering this option for some time. And it works. Which is why we're here.

The idea is simple. If you can do all the things that a password used to allow you to do, but with nothing more than smiling into your phone, all those password mistakes go away. Nothing to remember, no easy peasy passwords, nothing to write down, no cheating and duplicating, no breached or phished passwords to exploit, no reminders to dispose and refresh.

Your face can now do, and do so much better, what your brain never could. And apart from the potential rivalry between the two, there's a lot to be said for it.

So Why Faces And Why Now?

- 1 The algorithms used for facial recognition, verification and authentication have gotten so much better, leading to the Holy Grails of biometrics – fewer false positives, fewer false negatives, and instant gratification.
- 2 Phones have more powerful processors and better Internet connections that make it easier for the exchange of vitals – the challenge and response – to take place.
- 3 Personal cameras, especially those in phones, are powerful enough to solve most image processing issues. Better processors and sensors, better (and often dual) lenses, better image stabilization and anti shake, adaptable to all kinds of conditions, movements, backgrounds, lighting.
- 4 Cameras are everywhere because personal devices are. And longer battery life means your key to every door will be ready every time you need it.
- 5 Facial recognition keeps the good side of users (their face) involved while shutting out the bad parts – user mistakes, short cuts, sloppiness, forgetfulness.
- 6 The system is hard to fool. Simply placing a still image of the user in front of the camera is nowhere near enough to fool the system.

Passphrases Instead?

Until some solution, biometric, emerges as the clear alternative to the passwords, then it's passwords we're stuck with. And if a random collection of unconnected words is not yet your thing, maybe a passphrase is. A pass phrase is a line or statement about you that's easy for you to remember but almost impossible for a hacker to crack or guess.

Take the simple phrase ***"I got married in Hellhole Palms California on August 25th 1990."***

Now take the first letter and all the numbers and put them together to make a password IgmiHPCoA25th1990. That's a massive 17-character password that's got upper case, lower case, and numbers, and which should be easy for you to remember but almost impossible for a hacker to guess.

You can even write it down, maybe in something like a diary. What are the chances that a hacker will break into your home, stumble across that statement, and realize it's the secret code generator for a password?

And yes, Hellhole Palms is a real place.

Password Managers

Password managers are small tools, little helpers, that allow you to store all your passwords, tens of thousands of them if you want, on one single program that's protected by one master password.

And that program can either be installed on your computer (in the browser), on to your tablet or phone, or it can be in the cloud so that you can access your passwords no matter where you are. But they go far beyond simply storing your passwords. They can eliminate many of the shortcuts and mistakes most users make that can create vulnerabilities with their passwords.

For example, they can automatically generate unique and complex passwords that include all the basics like upper and lowercase letters, numbers, symbols, and anything else you want to include. They can make sure that you don't duplicate passwords or use the same weak passwords for multiple sites.

They can also auto fill password forms or any other forms, and even auto fill credit card forms. And while a number of these firms have had some security scares recently, because hackers know that between them they contain the passwords of millions of users, they still have proven themselves to be pretty robust in defending against hackers.

Probably the best-known password managers out there, especially with free versions, include LastPass, Dashlane, One Password, KeyPass, and Robo form. Probably the most popular are DashLane, and last pass, and I have used both.

So if you're serious about managing the password challenge and you're willing to try these products, I strongly suggest you do. They'll make your life much easier, and as long as they can keep hackers out they will make their lives much harder. Just be smart about the way you use them.

Avoiding Password Pain

So to avoid all the pain, as well as all kinds of risks ranging from identity theft to hackers owning your Facebook or email account, here are some of the key things you should and shouldn't be doing with your passwords:

DO:

- 1 Make all your passwords at least 12 characters long.
- 2 Consider following the latest thinking, of using a series of unconnected words instead of gibberish that you can never remember.
- 3 Use different passwords for all your important sites and accounts.
- 4 Change your passwords as often as you can. It's a pain, but also a simple defense.
- 5 Think about using a pass phrase instead of a password. The pass phrase idea is described below.
- 6 Consider using a good password manager. Although it's always risky storing all your passwords in the same place, it's better the most of the options.
- 7 Write down complex passwords, especially if you're keeping them at home. If hidden in the right place, little chance that a hacker, burglar, or malware will find them.

DON'T:

- 1 Use obvious words that can be easily guessed or found in a dictionary.
- 2 Assume that adding a few random numbers to the end of a word will do you any good. It won't.
- 3 Store passwords in a Word or Excel file on your computer.
- 4 Fall for phishing emails claiming to be from your IT department, bank, or Facebook and asking you to confirm your password.
- 5 Forget about malware. Today's malware can easily infect your computer or phone and grab your passwords.
- 6 Just rely on passwords for protection. Always use two-factor authentication whenever it's offered.



SAY WHAT?

How Thieves Stole An Entire Business

If you've never heard of business or corporate identity theft, expect to hear a lot about it in the future. Corporate identity theft is where the thieves clone an entire business, usually a smaller one, instead of an individual. Then they pretend to be that business and obtain credit using the victim company's credit history or order goods only to disappear into the night leaving the real business to face the often-devastating consequences.

These cases are on the rise for two reasons – they make a heck of a lot of money for the crooks, sometimes \$1 million or more. And they're very easy to pull off because most of the information the thieves need to clone a business identity is already freely available – the victim company's own web site is often where the thieves start. Some of the gangs involved can spend a year or more researching their victims, and are usually long gone before the victim company finds out anything's wrong.

The threat is so real, the National Association of Secretaries of State launched a task force to educate business owners and look for ways they could make it harder for criminals. And it seems pretty easy for these scammers to fool even the most careful of banks. In February 2017, a scammer from Naples Florida was sentenced to 11 years in prison after he was convicted of stealing \$2.2 million from a number of different banks simply by pretending he was the CEO or other executive from a variety of real companies across Florida.

I first got my first case a few years ago and the victim was a small electronics firm in the San Francisco bay area that was fielding calls from angry vendors wanting to know why some very big bills had not been paid. Problem was, the company had not placed any orders. Not so, said the vendors who received the orders by email and showed them to the victim.

Those orders came in very convincing emails using the victim company's correct email address. The email order included an 800 number and that number directed the caller to the company's real employees. Or at least voice mail boxes in the names of the real company's executives. They really had done their homework.

But it was all a scam. And not only a live one but a dangerous one. The crooks had spent a lot of time researching the company. They set up their own web site and email addresses, even using the company's web address. Except they were using the .net version instead of the .com address, which the company had failed to register. They even had the company's bank account information and trade references. Enough information for even the most careful customer to fall for.

The first thing the victim did was contact their local police department, although they expected very little to come from it. Most police departments wouldn't even consider this a crime, and certainly would have no idea where or how to investigate it. A typical victim in this type of case would be on their own and largely helpless.

Their only option would be to try to find out the name of the domain registrar that the crooks used to register the domain and ask them to take some action. But that could take months, or might never happen at all. Many registrars, often based in countries with few laws on this topic, simply ignore such requests. Or maybe legal action, a court judgment, or a search warrant are required first. But with no police department ready to even investigate, there's absolutely no chance of any of these happening.

I tried to help the owner of the business by contacting multiple domain registers in Canada and Switzerland, imploring them to recognize the domains as fraudulent and take them down. Some cooperated, others didn't, and yet others wanted detailed evidence before they could act.

But the deeper we dug, the more we realized that the crooks had registered dozens of similar-looking domains, and every time we took one down the crooks were quickly back up with another. Leaving us playing a time-consuming and often-pointless game of whack-a-mole.

To this day we have no idea who did it or why they picked on this small business. But it caused the business owner months of stress and distress as he watched his suppliers lose faith in his business, his credit worthiness, and his word. The business closed a couple of months later.

Courtesy of



GUARDING THE CANDY STORE

HACKERS AND THE WEALTHY

By Neal O'Farrell, Think Security First!

WHY HIGH NET WORTH ! = HIGH NET RISK

As the harsh lessons of life have probably taught you, not all consumers are created equal. And certainly not in the eyes of hackers, identity thieves, and other crooks. Today's professional, highly skilled, and resourceful cybercrooks are now focusing their attention on the targets that provide the biggest payoff with the lowest risk. And crooks call these targets "Candy Stores."

Candy Stores are the most affluent personal targets – that means higher net worth individuals and families, professional advisors, and successful small business owners who not only offer the best payoff to hackers and identity thieves but also provide a potential gateway to countless and maybe even priceless other assets.

And most important, the crooks are after much more than money. Data is the currency of cybercrime, and Candy Stores provide access to a wealth of often invaluable information that includes personal and corporate secrets, business and social contacts, customer and employee files, financial and investment information – the list is endless.

“ Insider Threat? In February 2017, a former Morgan Stanley wealth advisor was charged with stealing \$5 million from his clients and spending it on private jets, luxury cars, and expensive club memberships. ”

And for the affluent consumer the worry is also about things like reputation, interruption of their retirement, the impact of their family, and the potential to be a massive and unpleasant waste of time. And there's also the worry about the potential for public embarrassment, the risks that could create for relationships with business partners and associates, maybe the exposure of sensitive private secrets, and even the jeopardy to business deals.

And while the business of cybercrime is evolving rapidly, I mean daily, even hourly, for the last decade consumer security has actually changed very little. For most consumers, options are still limited to maybe a cookie-cutter identity protection service and some

antivirus software. And that's it. For the more affluent consumers, who are targeted by the more sophisticated attackers, those defenses offer little resistance.

What Makes A Candy Store?

- First, they have to be either wealthy or at least more affluent than the average consumer.
- They should ideally have information and connections that they wouldn't want exposed or others to have access to.
- They should have substantial bank account balances, ideally personal, investment and business.
- And they should be connected to other similar individuals, through business dealings, through their friends, neighbors, work, charities, political activities and so on.

So by that definition, you can see why candy Stores can include successful small business owners and professionals, physicians, lawyers and law firms, financial advisors, wealth managers, brokers, insurance agents and many other professions. In other words, people who by themselves are more affluent, but also by their profession or success have access to lots of other people, whether that's friends, colleagues, clients, or even patients.

So Why Target The Affluent?

Targeting the affluent is more complex than it might appear. And it's not just because they might have more money or better credit than the average consumer. Higher net worth individuals certainly have more to steal from. But they also present a much bigger payoff for thieves, in a very different way, and with a much lower risk:

- The affluent often have more accounts and with higher deposits, making it much harder for them to protect themselves. While the average consumer might have as few as one or two bank accounts (a checking and savings), a higher net worth target may have as many as twenty different accounts - business accounts, brokerage and investment accounts, and even trust accounts.
- Protecting so many accounts is like spinning plates. With so little security spread over so many accounts, it's easy to understand why some plates might come crashing down.
- These targets have more than money to steal and to worry about. They're equally worried about their privacy, their reputation, the protection of the family, their standing in business and social circles, their access to the right people, their business deals and investments, their access to funds and liquid assets, and the need to protect multiple accounts.
- The crooks that target them are usually very sophisticated and persistent, making them much harder to defend against. And those crooks increasingly want access to things like personal secrets and communications, corporate secrets and business transactions, conversations with advisers and partners, social and business connections, and especially peccadillos, infidelities and transgressions.
- It's relatively easy to steal the personal information of these victims and clone their identity because there is much more information about them in the public domain. Information that can be very difficult to remove or to bury.
- They're often too busy to think about protecting themselves. And maybe they're also falsely confident (or perhaps just arrogant) that either no one would dare try to snatch their beloved identity away from them, or they'll just be able to make it go away if it does happen.

- Often the focus of the attack is simply to find a backdoor into another business, corporate partner, or financial institution, or merely as a backdoor to an even higher net worth target.
- These victims often feel uncomfortable about reporting the crime in case it causes embarrassment or reputation damage. And if the individual runs a business, bad press over a security breach can also be financially costly and especially if it impacts potential future business dealings. And the likelihood of never being caught, prosecuted, punished or even reported can seal the deal for criminals.
- With enough information, thieves can successfully attack the same victim again and again. For the victim it ends up being a high-stakes game of whack-a-mole, never knowing where the thieves can pop up again.
- And finally, affluent consumers typically have more points of access and vulnerability – meaning more people around them, from employees to advisors, who can be exploited for access. Not to mention more accounts, more relationships, more purchases, more credit cards, more spending, more travel – all of which increase exposure and opportunity.

Cybercrime Changed Things for the Wealthy

Who knew that cybercrime would become the great equalizer? It sounds counter intuitive but wealthy neighborhoods are not the preferred pickings of the thieving class, because rich is rarely worth the risk. Wealthier neighborhoods are usually better protected, gated, and guarded. And you're probably not going to blend in very well when you're cruising the neighborhood in that old panel van with the Penske decal still visible under the single coat of emulsion. Even if you're staying under the speed limit.

Then there are all those extra eyes to avoid. Landscapers, perhaps a nanny or two, or maybe a housekeeper. And if you're lucky to slip past all the human surveillance, you're still not home free. The homes of the wealthy tend to be harder to breach: sophisticated intruder alarms with rapid-response remote monitoring; maybe a video surveillance system and

security lights; and almost definitely high quality doors and windows with security locks that don't seem to agree that resistance is futile.

For most crooks, the reward is just not worth the risk. But cybercrime has changed all that. Cybercrime has allowed the most sophisticated crooks to reach out and touch their victims, any victims, from the next neighborhood over or from the other side of the world. They're now free to pick any victims they want, the reward potential has skyrocketed, and the risk is now so low it's barely even a factor. It's like a video game, where the gamer not only has all the control and options, but knows all the cheats needed to guarantee the highest score every time.

The attacks are also far more advanced and persistent than ever before, often making conventional credit monitoring of limited value. Symantec recently told the story of how a CEO was targeted by an endless series of sophisticated hacking attacks that went on for nearly a year. In one month alone the victim was targeted 24 times – that's nearly once a day.

I handled a case of a wealthy family where both parents and both teenage kids were the subject of a persistent and very successful series of identity attacks that also went on for nearly a year. And a Silicon Valley entrepreneur whose personal information was pilfered from a wealth management company had to suffer through more than 300 harassing and threatening phone calls in just one month, often starting at five in the morning, and coming from dozens of payday lenders from the U.S. and beyond and all claiming he owed them money.

“ Cyber criminals are actively seeking out unprepared soft targets, and asset managers' lack of cyber sophistication makes them ideal targets. ”

PriceWaterhouse Coopers

Wealth Can't Strengthen Your Weakest Links

A common ploy by crooks that want to get closer to their chosen target is to exploit one of the many weak links around them. Affluent identities can be much more vulnerable to mistakes by those around them who have may provide easier access – secretaries, admin assistants, portfolio managers, investment managers, financial and legal advisors, and even family and friends.

Thieves often target these individuals with spear phishing and social engineering attacks as a weak link or back door to the real target. One of the ways cyber crooks might try to target your wealth is through your wealth managers or advisors.

- Security firm Kroll has repeatedly issued alerts that it's seeing significant growth in sophisticated attacks against wealth management firms. Attacks that have resulted in millions of dollars in financial losses.
- Celebrity hacker Christopher Chaney managed to break into the email accounts of celebrities like Scarlett Johansson and Mila Kunis by figuring out the answers to the secret questions that protected their email passwords. The only way he was able to find the email addresses of the dozens of stars he targeted was because he focused on the email account of one celebrity hairstylist the victims confided in.
- In the highly publicized attack on Target Stores, that resulted in one of the biggest data breaches in history and exposed more than 70 million customer records, the attack was started by targeting a low-level employee at a Target vendor using nothing more than a phishing email laced with malware.
- Russian hackers targeting energy companies knew they would have difficulty penetrating the security of those corporations. So instead they focused on the favorite restaurants of key employees, hacked those websites, and infected online menus with malware that would be downloaded by employees.

Why Professional Advisors Are A Target Too

Nearly fifteen years ago, speaking at the 25th Annual Conference of the State Bar of California's Intellectual Property Section, I warned of the likelihood that law firms will be targeted as a path to their clients. In recent years the FBI has warned that it is seeing hundreds of law firms fall victim to hackers. And the American Bar Association recently warned its members that "You have been or will be hacked. It's a matter of "when" and not "if".

“ What’s going on in the industry today is full-scale war on financial service companies and institutions all over the world.”

Wealth Management Magazine

Successful professionals who have access to high net worth clients also meet the definition of Candy Stores. Professional cybercrooks now have a vast array of advanced tools they can use to launch remote, automated, and undetectable attacks against these individuals and their firms. Attacks like spear phishing, social engineering, keyloggers, and website exploits are usually undetectable. And a single security failure by an advisory firm can inflict serious damage on its clients.

Such is the concern for the financial sector and particularly for personal advisors that the SEC has introduced cybersecurity as part of its annual testing for broker/dealers.

So Why Target These Firms?

- Their owners and partners are often individually high net worth and worth targeting.
- They provide an often too-easy back door to their clients and accounts.
- They have detailed customer files and sometimes account credentials and other inside information.
- They're susceptible to extortion because of the importance of maintaining absolute client trust and business reputation.

Spear Phishing Is The Most Popular Attack

There are many tricks and tools available to hackers to reach out and infiltrate the world of almost any target. But one of the most popular and effective tactics used against high net worth consumers and their advisors is spear phishing.

An attack will often go something like this:

- One or a small group of professional crooks will identify large groups of potential targets and start doing their research – about their personal lives and family, friends and social networks, charities and causes they're involved in, businesses they're a part of, who their financial and legal advisors are, who their key employees are.
- A target or group of targets will be identified – either the final target or someone close to them.
- The most likely attack will be a spear phishing email – an email based on what the crooks have learned about the target and designed to look like it comes from someone the target knows.
- A common ploy is to impersonate a financial advisor, lawyer or accountant, a family member, an employee, the IRS, or even a personal trainer or hair stylist; sending an email using that person's real email address; and using a topic that won't arouse the suspicions of the target.
- The email is likely to include either an attachment or a link to a website, and clicking on that link or opening that attachment will launch a piece of malware the target's antivirus software can't detect.

So How Can You Protect Yourself?

Above all else, take the threat seriously and personally. Don't assume that it's unlikely to ever happen to you, or if it does, your success or affluence means you can easily make it just go away. One single incident can become a costly distraction that lasts for years.

- Plan your protection just like you would plan your financial and wealth management. Use a professional, understand and weigh the risks, create a personal security plan, and stick to it.

- Think about what the thieves want most or what you can least afford to lose. Is it access to your bank, investment, or brokerage accounts, access to your private discussions and communications, business and investment plans, your reputation? A good defense always begins with knowing what the attacker is after and hardening that target.
- Think about those around you. Many attacks targeting higher net worth victims begin by targeting those around them and especially family, friends, and employees. So make sure you talk to them about the risks so they don't become an embarrassing weak link.
- If you have employees, make security awareness training a regular event so they know what to look for and what to avoid. Good security vigilance is great for them and their families too.
- Protect your accounts in multiple layers of security. That includes strong and frequently changed passwords, account activity alerts, multi-factor authentication, and lots of malware protection on any computers or devices you use to access these accounts.
- Think about using a separate and dedicated computer for access to your most sensitive accounts. Don't use that computer for surfing, email, or anything else that could let in malware. A cheap \$200 computer is a small price to pay for the security and immunity it can bring.
- Be especially vigilant for spear phishing attacks, and make sure family members and employees are aware too. Spear phishing usually manifests as a legitimate and convincing email, from a partner, advisor, friend, or even the IRS, inviting you to click on an urgent link or attachment. It's one of the most effective techniques hackers have and vigilance is your only defense.

- Use encryption. For personal and even small business use, there are a number of free and easy-to-use encryption programs that will protect your most sensitive data from the most determined hacker. You can even protect phone calls, emails, text messages, photos, and videos.
- If your phone calls, text messages, and emails are sensitive, use one of the growing number of free apps, like Signal and Wickr, that will encrypt all these messages to military grade, destroy them after a pre-set time, and hide any trace they were ever even sent.
- If you spend a lot of time online, be extra cautious. A growing amount of malware is now being delivered through compromised websites that in turn infect any computers visiting those sites.
- Focus on your advisors. They can sometimes be the weakest link and the first stop for hackers trying to get to you. Ask them what their security procedures are, what they know about spear phishing, how they protect your information (and especially accounts), how often they train their employees, how they verify requests from their clients. Don't be general, get specific.



THINK SECURITY FIRST!

DO WHAT WE \$@Y!

THE GROWING THREAT OF CYBER EXTORTION

Chapter 29

CHAPTER 29

Remember the huge and very embarrassing hack of online dating company Ashley Madison? Or the equally embarrassing Sony breach? OK, you could be forgiven for not being able to recall specifically why those breaches were any different to the thousands of others in the past decade.

But they were, and for reasons that should really concern you. In the case of Ashley Madison, the breach was all about extortion, with criminals vowing to share highly sensitive information on millions of its cheating members unless the company did just one thing – completely shut down its business.

In the case of Sony, hackers stole and shared very candid and embarrassing email exchanges between senior executives that resulted in resignations, career damage, and long term harm to both Sony and its relationships with many of its top artists.

Both breaches were the first volleys in a new type of cyberwar, targeting businesses and individuals with threats of data exposure and humiliation unless the hackers' demands are met.

And it's not just businesses that are being targeted. In March 2017, numerous media outlets reported that Russian hackers were actively targeting dozens of Democratic lawmakers and organizations, stealing sensitive and potentially embarrassing emails and other communications, and demanding extortions of up to \$150,000 to "make the problem go away."

This growing type of attack could work many different yet very easy ways:

- We have some embarrassing tax documents and we'll send to the IRS if you don't do as we say.
- We have all those secret text messages from your lover.
- We got access to your email account and have years of embarrassing email exchanges.

- We have your sensitive client files and we'll publish unless you pay up.
- We're the ones who took down your website and we'll keep it down until you pay up.

But back to Ashley Madison. The online cheating business was nearly destroyed when hackers accessed the accounts of millions of users, threatened to publish the steamy details if the business didn't shut its doors. And the hackers made good on their promise when the company refused to comply.

The Ashley Madison brand quickly became the subject of massive and embarrassing media coverage, with increased scrutiny on many of its questionable business practices. Clients rushed to close their accounts and try to hide their identities, and a number of users are believed to have committed suicide as a result of the exposure. The founder and CEO was finally forced to step down from the company when it was revealed by hackers that in spite of his claims to the contrary, he may have used his own site to cheat on his wife.

And the intense scrutiny by the security and tech community has even revealed the possibility that the entire business model might have all been a scam to start with, especially after media stories suggesting that the vast majority of messages sent by what appeared to be women using the site were in fact internally generated by bots and not real people.

And with growing reports over attempts to personally extort members unlucky enough to have had their relationship to the site exposed, we shouldn't forget that the attack on Ashley Madison was fundamentally about extortion. The hackers who stole the information and threatened to publish it offered Ashley Madison a simple remedy. If you don't want us to publish all this data, simply close your doors and go away. Simple extortion, even if tinged with some excuse of social nobility.

The Battle Over Bits

Cyber extortion is not new but it is accelerating rapidly. Ransomware is a very simple but effective type of extortion that has surged in the last few years and snared its own fair share of extortion victims. And it's obviously an effective business model for hackers, with Symantec reporting a 4,000% surge in crypto ransom in just one year.

- The FBI has issued a number of warnings about the growth in sextortion, and especially targeting kids, that extorts the victims by threatening to publish revealing or intimate photos or videos.
- Hundreds of companies have reported receiving extortion demands from Denial of Service gangs like DD4BC threatening to launch debilitating Denial of Service attacks unless substantial ransoms are paid.
- In 2014, British plastic surgery group the Harley Medical Group confirmed it had received a ransom demand after hackers stole the personal information of more than half a million customers.
- Security firm BitDefender reported receiving a ransom demand after sensitive customer information was stolen by hackers.
- In January 2017, hackers targeted Lloyds Bank in Great Britain, disrupting their website and demanding a payment of \$94,000 to end the attack.

Higher net worth consumers and their advisors are likely to be the biggest targets of personal extortion. These targets typically have more to protect and more to hide. They're the most likely to pay to make an embarrassing problem go away, and the least likely to report the crime to law enforcement.

Victims Willing To Pay Ransoms

A study published by security firm ThreatTrack found that one in three security professionals admitted they would be willing to consider paying a ransom in order to get back sensitive data from hackers.

The study also found that for those organizations that have already been victim of cyber extortionists, more than half admit they would be willing to meet the demands of extortionists. Which suggests they might have already seen some success in paying a ransom. And more than 80% said they believe that other organizations have negotiated with cyber extortionists.

And the study revealed some additional insight:

- 74% of those interviewed said they believed they were targets for cyber extortion.
- Those in the healthcare and financial sector were the most opposed to paying ransoms, with more than 80% saying it's not something they would consider.
- Yet of those in the healthcare and financial sectors, more than 40% said they would have no problem with their insurance carriers using third parties to negotiate ransoms.

The Response to the Crime Will Fuel the Crime

- As more victims agree to pay extortionists, it will become more acceptable and widespread, and therefore likely only to attract more hackers and extortionists.
- Which might explain why a growing number of companies are now admitting to setting aside "hush" funds to pay extortion demands. That will also only increase the attention of hackers.
- If the insurance industry starts to cover this risk, with affordable premiums and third-party negotiators, that's also likely to drive the crime.
- Paying a ransom after a data breach, to both recover the data and buy the silence of the thieves, is likely to cost the victim a lot less than a publicized data breach. That may be an irresistible proposition for many.
- The growth in undetectable malware and crypting – testing that malware is undetectable before launch – is making targeted attacks much easier.

Cyber extortion checks all the right boxes for crooks of all kinds. It can be very lucrative, very easy to pull off, and there's minimal chance of being caught and punished. The secret to extortion is the need for secrecy. If a victim doesn't want certain data, events, breaches, communications, or personal information exposed, that includes keeping it a secret from law enforcement too. What a recipe!



THINK SECURITY FIRST!

WE ARE ALL AT WAR

THE GLOBAL CYBER WAR AND
YOUR ROLE IN IT

Chapter 30

CHAPTER 30

Einstein was wrong. World War 4 will not be fought with sticks or rocks. It will be fought with bits and bytes, Trojans and bots, APTs and zero-days, it's already started and we're already losing.

I'm not a fan of drama, especially as a tool to herd the masses in a specific direction and even for a good reason. But I'm not a fan of sugar coating either. That's why I think we think we need to speak honestly about war. And the fact that we're in one, right now, and have been for some time. It's just that this war is so very different to every war before, and many of us can't see, hear, smell, or touch it. But it doesn't mean it's not there and it's not urgent.

China has been attacking the U.S. for years- attacking businesses, government, and military, probing networks, planting malware, stealing secrets. It's also believed that China is always looking for catastrophic weaknesses that could be exploited at an appropriate time – in our financial, communications, food supply, and energy systems.

And even our industrial systems are being heavily targeted, often to disrupt. In March 2017 researchers at a security called Drago estimated that around 3,000 industrial sites are infected every year with malware that targets critical control systems – including nuclear facilities - and that could be a conservative estimate.

If it turns out that the Russian government was behind a series of intrusions into U.S. power and nuclear plants in May 2017, as the FBI has indicated, that would be as clear an act of war on American interests as the invasion of Ukraine was to the people of that country.

And speaking of Ukraine, many security observers believe that the regular power outages in Ukraine, and especially around Christmas, are a mixture of psychological and cyber attacks by neighboring Russia intended to intimidate and demoralize the nation. And send a clear message about who's really in charge in that region.

And while America is constantly under cyber attack, it's not sitting on its hands. It's been speculated that the very advanced Stuxnet malware that is believed to have done significant damage to Iran's nuclear program in 2010 was created jointly by Israel and the United States.

“ In Russia’s shadow, the decades-old nightmare of hackers stopping the gears of modern society has become a reality.

Wired, June 2017

”

There are many who think that the notion of cyberwar is simply hype or scaremongering, and others argue that cyberwar can never actually be called a war because it doesn’t fit with traditional definitions or understanding of what a war is:

- In an article from the Council of Foreign Relations in 2013, one noted author argued that “the hype about everything “cyber” has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future.”
- Around the same time, InfoWorld took an opposite position in an article titled “Unseen, all-out cyber war on U.S. has begun” and concluded that “One thing is clear: The era of cyber warfare is here, and it’s happening on the home front.”

How Is This Different To Other Wars?

- There will be no clear and official declaration of the beginning of hostilities (a bit late anyway).
- There will be few decisive battles, no clear winners or losers, and no end. We might therefore want to call this one the Until-the-end-of-the-World War.
- We will never be sure who our friends and allies are, or when they switched sides.
- We are the battlefields too – our computers, our phones, our small businesses, and our internet-connected homes.

- The war won't be fought by professional armies but mainly by mercenaries, home front militias, and civilian volunteers.
- Our traditional armies will be largely relegated to spectators, sitting in frustration on the sidelines as they wait for a call to arms that may never come.
- The battles will be largely stealthy, silent, and bloodless, which will make it very hard to rally national support for or against.
- It will eventually get physical, as one side realizes that while it's been out-coded it's not outgunned, and so as a symbolic gesture will attack some vulnerable overseas target.
- It will be relatively cheap. 5,000 AK47s cost roughly \$3 million, 5,000 mortar rounds cost around \$50 million, 5,000 artillery shells cost around \$500 million, and just ten fighter jets will cost more than \$1 billion before you fuel, arm, man, deliver, and support them. A million bottled and hijacked computers ready to attack on command will cost less than \$50,000.
- The battlefields will be very comfortable. An attacker and his best buddies will be disabling the power station that provides electricity to most of a major U.S. city, while his siblings do their homework in the next room.
- There will be few prisoners of war and our enemies will walk unnoticed amongst us.
- It will be largely economical and psychological, in an attempt to reduce to rubble our economy, our spirit, and our ability and appetite to continue the fight.
- Weapons will eventually attack their masters, as increasingly sophisticated malware unleashed into the wild infect the systems of their creators and benefactors.

- It's a war from which we will all suffer and in which we can all play a role.

Is Ransomware The New Kalashnikov?

If you're not already aware of the threat of ransomware, then I urge you to read my chapter on the topic. Ransomware is a devastating and therefore highly popular type of attack that uses malware to infect computers, lock files, and demand a ransom to release those files.

Imagine a large-scale ransomware attack on hospitals, pharmacies, banks and credit unions, employers, schools? Imagine all those critical and maybe even critically urgent files no longer being accessible? Not even the backups? And still locked and lost forever even if a ransom is paid.

We've seen exactly such attacks, or at least very successful test runs, take place over the last year. More are coming, because they're easy, effective, and cheap.

Why It Could All Be Your Fault

What this war has in common with previous wars is the dependence on infrastructure. Many of these attacks rely on a growing number of compromised and conscripted computers, phones, and websites to spread malware and attacks, probe other computers, infect businesses, attack banks and accounts, steal personal information, and disable our personal technologies.

We're not powerless in our response. We don't have to sign up or show up in order to join up. And there's no need to flee to Canada. This is a war where every man, woman, and child can play a role, and our most powerful weapon is lodged squarely between our ears.

Our own awareness, vigilance, behavior, habits, and choices can disable many of these attacks. If you won't stop clicking on stuff, or creating crappy passwords, for yourself, your family, or your job, then do it for your country. If your lights go out or your Internet goes down because of a cyber attack, wonder if it's because of something you did.



THINK SECURITY FIRST!



50 FREE SECURITY TOOLS

KEEPING YOUR WORLD SAFE,
SECURE, AND SECRET

Chapter 31

CHAPTER 31

Throughout this book, and probably my life, I've talked about the importance of layering security as the best way to stop, or at least slow down, hackers, identity thieves, and snoopers. And with so many great and free security tools now available, here's where you begin to run out of excuses.

By protecting all corners of your life and business with multiple layers of security, you make it infinitely harder for a hacker, identity thief, malware or any of the multitude of other threat to get past the obstacles you created. It's never an absolute guarantee, but it really can improve your odds of avoiding falling victim.

In this chapter you'll come across many products that you've heard about, some that you might have even used, and others that are new. All these products are free, although many have paid or premium versions that offer extra features. The decision whether to stick with free or go for the upgrade is yours, but in my experience the free versions offer solid basic security that works for most users.


Malware Protection

First of all let's talk about the basics, and for every computer and even phones and tablets that's got to be antivirus or AV software. If you've already read my chapters on malware and phishing, then you probably already heard about the growing concerns that antivirus software can have a hard time keeping up with today's sophisticated malware.

But I believe, like most experts, that it's still an essential part of your defense. In case you weren't aware, there are more than 45 different consumer antivirus products on the market. Most has been around for a decade or more, some are very good, some average, and a handful simply downright scary and don't belong on anyone's computer.

Amongst the best out there, at least according to a variety of antivirus testing companies, are the brand names you've probably heard about. Some of the brands that you may be familiar with, like Norton, unfortunately do not have free versions.

But you still have plenty of great and free options. I've included the home page for all these companies because the specific URLs for their free versions often change. So you may have to dig around their websites a little:

- 
- Panda (www.pandasecurity.com)
 - AVG (www.avg.com, now owned by Avast)
 - Avast (www.avast.com)
 - Sophos (www.sophos.com)
 - Bit Defender (www.bitdefender.com)
 - ZoneAlarm (www.zonealarm.com)
 - Malwarebytes (www.malwarebytes.com)
 - Kaspersky (www.kaspersky.com)
 - Avira (www.avira.com)
 - Comodo (www.comodo.com)
 - Adaware (www.adaware.com)
 - McAfee Cloud AV (www.mcafee)

Having trouble choosing? All of these products will provide similar protection, but according to a study in August 2017 by PC Magazine of the Top 10 antivirus products on the market *“Our current Editors’ Choice products for free antivirus utility are **Avast Free Antivirus** and **AVG AntiVirus Free**. Both get very good scores from the independent labs, and in our own tests as well. Both include some useful bonus features. Avast in particular packs a password manager and a network security scanner in its toolkit.”*

How Are Free Versions Different To Paid Or Premium?

Different vendors give their products away for different reasons, but usually either because they're driven by altruistic reasons and believe that free security helps everyone; or they see free as a great way to maximize the use of their products and the awareness of the brand name. Both very good reasons.

Free versions can differ in a number of ways:

- Free versions may include advertising, sometimes irritating, although I've never noticed any with my free products.
- The vendor may be collecting your information and using it for other marketing purposes. This should be a real worry so check their privacy policy first.
- The interface for the free version might be different to the paid version.
- The paid version might have more features, but you'll have to determine if you really need them.
- The free versions usually come with a lot less technical support than the paid versions. And that can be very important if you ever have a malware problem.

These products are all well tested and highly regarded. So if you're using any of these products, either personally or for your business, then you're already off to a good start.

And it's worth remembering that most but not all of the free antivirus software products are only meant for personal use and not for business. But because there's such a grey line between business and personal computing (most people still use their personal laptops, phones, and tablets for work), you may still be able to use the free versions. But just make sure you check the licensing first.

If you're using a Mac, don't make the mistake of assuming you're safe from malware.

Macs were traditionally not a favorite target for malware authors. Not because they were invulnerable or impenetrable, but simply because there weren't enough Mac users in the world to make it worth the investment.

But because that has now changed, there has been a growth in malware targeted specifically at Macs and anything Apple. So while Macs still may have better security than Windows computers, you still need some basic antivirus in place. And fortunately, most of the antivirus companies offer free or low-cost antivirus software specifically for Macs.

And even if you have antivirus software in place, you should always supplement it with additional tools that can scan a little bit deeper into your computer or phone for malware your other antivirus software didn't pick up. So I always recommend regularly testing your computer with products like Malwarebytes and Microsoft's malicious software removal tool. Both are free and both can provide a useful extra layer of defense and detection.

Mobile Security

As I mentioned earlier, antivirus software is no longer just for your computer or your Mac. While malware targeting mobile devices like smart phones and tablets is not anywhere as severe as PC or Mac malware, it's growing rapidly.

So it's vitally important that you're protecting your devices. And luckily, most of the antivirus software companies have good versions for mobile devices and usually free. And most of today's mobile security software goes far beyond simply malware protection. These products can protect you against snooping, they can protect against the loss or theft of a device, some of them can even snap and send a photo of the thief, and they can back up and restore your data so you can move it quickly to another device.

They can wipe the device clean so if thieves gets access to it, they don't have access to any sensitive information. They can also scan apps for security or privacy risks, and they can even help you surf safely.

So even if you're not too worried about the threats of malware to your mobile devices, it's still a good idea to consider using one of these products for all the other great security and privacy features they offer. One of my favorites is **Lookout** and you'll find out at Lookout.com. It's also free (the basic version).

Password Managers

In so many cases, a password is the only thing between you, your bank accounts, your Facebook account, your network, your clients - and hackers and malware. But the arrival of password managers removed many of those problems. The idea of a password manager is pretty simple. It allows you to store all your passwords - tens of thousands of them if you want - on one single program that's protected by one master password.

And that program can either be downloaded onto your computer, phone, or tablet, or it can be in the cloud so that you can access your passwords no matter where you are.

But they go far beyond simply storing your passwords:

- They can eliminate many of the shortcuts and mistakes most users make that create vulnerabilities with their passwords.
- They can automatically generate unique and complex passwords.
- They can make sure that you don't duplicate passwords - using the same weak passwords for multiple sites.

And while a number of these products have had some security scares recently, they still have proven themselves to be pretty robust in defending against hackers.

The best-known password managers, especially the free ones, include:

- LastPass (www.lastpass.com)
- Dashlane (www.dashlane.com)
- 1Password (www.1password.com)
- KeyPass (www.keeppass.info)

- RoboForm (www.roboform.com)
- Zoho Vault (www.zoho.com/vault)

The most popular are probably Dashlane and LastPass, and I have used both. So if you're serious about managing the password challenge and you're willing to try these products I strongly suggest you do. Just make sure you always protect that master password.

Secure Communications

Another growing security topic, in part because of endless spying scandals and NSA disclosures, is secure communications. Hackers know that there's tremendous value in what we say to each other, whether it's by phone, text, or email.

So if you're concerned that your private and confidential communications, especially with clients, could make it into the hands of hackers, spies, competitors, or the NSA, believe me, there's an app for that.


These apps not only encrypt your text messages, but also any images, photos or videos that are included. They can be set up so that only the intended recipient can read or review them, and even better, you can set up a message so that it self-destructs within days, hours, minutes, even seconds after you send it.

And going one better, many of these apps can also hide meta-data. This helps protect not just the information in the message but information about the message, like who sent it, who it was sent to, when it was sent and so on.

You can also encrypt your phone calls in the same way, so that no one except the authorized recipient can participate in the phone call. And you can create secure circles of trusted parties, like family members, friends, co-workers, employees, and even clients.

And you can even protect your address and phone books too, so that if your device is ever lost or stolen, or a spy manages for whatever reason to crack it, your contacts will never make it into the wrong hands.

Some of the more popular security and privacy apps for your mobile world include:

- 
- Wickr (www.wickr.com)
 - Signal (www.whispersystems.org)
 - Telegram (www.telegram.org)
 - WhatsApp (www.whatsapp.com)
 - ChatSecure (www.chatsecure.org)
 - Silence (www.silence.im)
 - Gliph (www.gli.ph)

So I strongly urge you to check them out, try them out, and if you like them, make sure everyone in your network uses them. Remember, it only takes one weak link.

Privacy

Many security breaches start with privacy failures. Which might be the reason behind the surge in privacy tools that are also free and which can protect you against this pervasive, invasive surveillance.

All these products work in different ways to achieve similar outcomes. They can, for example, warn you that a website is dangerous, maybe it's hiding malware, or that it simply exhibits signs that it's not very respectful of your privacy. And when these tools identify such a site, they'll warn you before you click on it, and so allow you to make the right decision. You can also use these tools to hide what websites you visit and hide whatever you download.

They can prevent marketers from gathering information about you, from tracking your movements from one site to another for example, and of course prevent security agencies or anyone else from learning too much about you.

And even if you're not so worried about all these legitimate companies collecting way too much information about you, you have to remember data breaches. One of the reasons there is so much stolen information in circulation is that the companies that collect it can't protect it.

And this has to be a growing concern for consumers who simply wants to make sure that their private information, their interests, their surfing habits, whatever it is they happen to be doing online, doesn't make it into the wrong hands.

There are products like **Duck Duck Go** (www.duckduckgo.com) which has become one of the most popular private surfing tools.

Simply by using Duck Duck Go like you would use, for example. Google or Bing, not only is all your searching hidden and anonymous, but you actually get legitimate results. That's because Duck Duck Go doesn't sell search results to the highest bidder - all results are treated equally.

- The Electronic Frontier Foundation has a privacy product called Privacy Badger which although not a search tool can hide much of what you do online. <https://www.eff.org/privacybadger>
- Companies like AVG and McAfee Site Adviser (www.siteadvisor.com) will tell you if the site you're visiting is safe.
- A free service called Hotspot Shield (www.hotspotshield.com) will allow you to use public Wi-Fi networks securely and anonymously, without having to worry who else might be nearby or eavesdropping.
- A new service called Zenmate (www.zenmate.com) will also allow you to surf the Internet in complete anonymity.
- Products like Ad Block Plus (www.adblockplus.org) will allow you to surf the Internet without the irritation and increasing danger of infected ads.
- Privoxy (www.privoxy.org) will also let you surf anonymously.

Protecting Your Kids

If your kids, or any family members, are like most families, they probably have a phone with them most of the time. Now you can use those phones to apply even more layers of security and privacy around your kids.

For example:

- Life 360 (www.life360.com) helps you stay in touch with your kids, know where they are, and warn you if they venture beyond agreed boundaries – they say they're going to a friend's but instead hit the mall.
- Mama Bear (www.mamabearapp.com) can use your kids' phones to tell you where are your kids are at all times, allows you to monitor their social media accounts, and even warn you if they're speeding when driving.
- A free service called Qustodio (www.qustodio.com) helps you manage and protect your kids' online activities, set rules and time schedules, block questionable sites (like pornography) and view social media activity.
- Kidlogger (www.kidlogger.net) monitors Internet activities, screenshots, webcam use, phone calls and plenty more.

You can also set up geographical zones beyond which your kids are not supposed to travel. If they go beyond those zones, their phone will tell you and your phone will tell you.

You can also set up a number of check-in points. For example, the apps will notify you when your kids have checked into places they're supposed to be. When they arrive at school in the morning, you'll be notified. When they get home from school in the afternoon, you'll be notified again.

If they're not coming straight home, but instead are going to a friend's house, the library, the mall, or maybe some kind of afterschool program, you'll be notified when they show up to that location.

And if your kids are on any kind of social media, and chances are they are, these apps will also notify you about what they're doing on those sites. What they're saying, what hot words they might be using, like drugs or alcohol, what photos or images they're sharing, and even what new people they're connecting with.

Free Identity Protection

Looking for some free identity protection? You now have a growing number of options, although some are pretty limited:

- Civic (www.civic.com) offers \$1 million identity insurance, as well as black market monitoring.
- Credit Sesame (www.creditsesame.com) offers free monitoring of your Transunion credit report.
- CreditKarma (www.crediteitkarma.com) provides free monitoring of your Transunion credit report, as well as a feature to instantly dispute any charges right from your CreditKarma dashboard.
- TrueIdentity (www.trueidentity.com) from Transunion allows you to freeze or lock your Transunion credit report instantly, as well as providing instant alerts.

You should also check with your insurance carrier about whether they offer free identity protection or insurance. Many home, vehicle, and travel insurance policies offer free identity protection as well as a growing number of banks, credit unions, and credit card companies.

In July 2017 Discover Card offered began offering its customers free monitoring of their Experian credit report, free fraud alerts, and monitoring for any misuse of their Social Security Number. So you may be surrounded by free identity protection services and never know it.

Private Form Filler

It seems like no matter what website you visit, they want either an email address or phone number. I have two problems with that. First there's simply the privacy thing, and not wanting to provide any more information that I have to.

The bigger problem though, is that so many companies are so bad at protecting the information they collect. So their sloppy security can cost you dearly if your information gets into the hands of hackers.

Free products like **Blur** from Abine (www.abine.com) can help in situations like this. For example, with Blur installed in your browser, any time you're asked for an email address or phone number, Blur will automatically and instantly generate a fake address or number.

The email address and phone number will still work, because they will be directly connected back to your real email address and phone number. But the website will never know what that real email address and phone number are. They just have the fake ones but the fake ones work, so they are readily accepted by the websites. But if there is a breach at that website, all the hackers get is the fake information that's of absolutely no value to them.

I think these tools are going to become even more commonplace, as more consumers and businesses try to mask their real information with fake or substituted versions.

Honorable Mention

And there are plenty of other free apps out there that can protect you and your business.

For example, a free app called **Eraser** will permanently shred any documents you have so that they can never be recovered. It works by overwriting the documents so thoroughly, to military grade, that they can never ever be recovered. You should always use it instead of just deleting sensitive documents, which doesn't actually delete anything, and especially if you're selling or disposing of a computer.

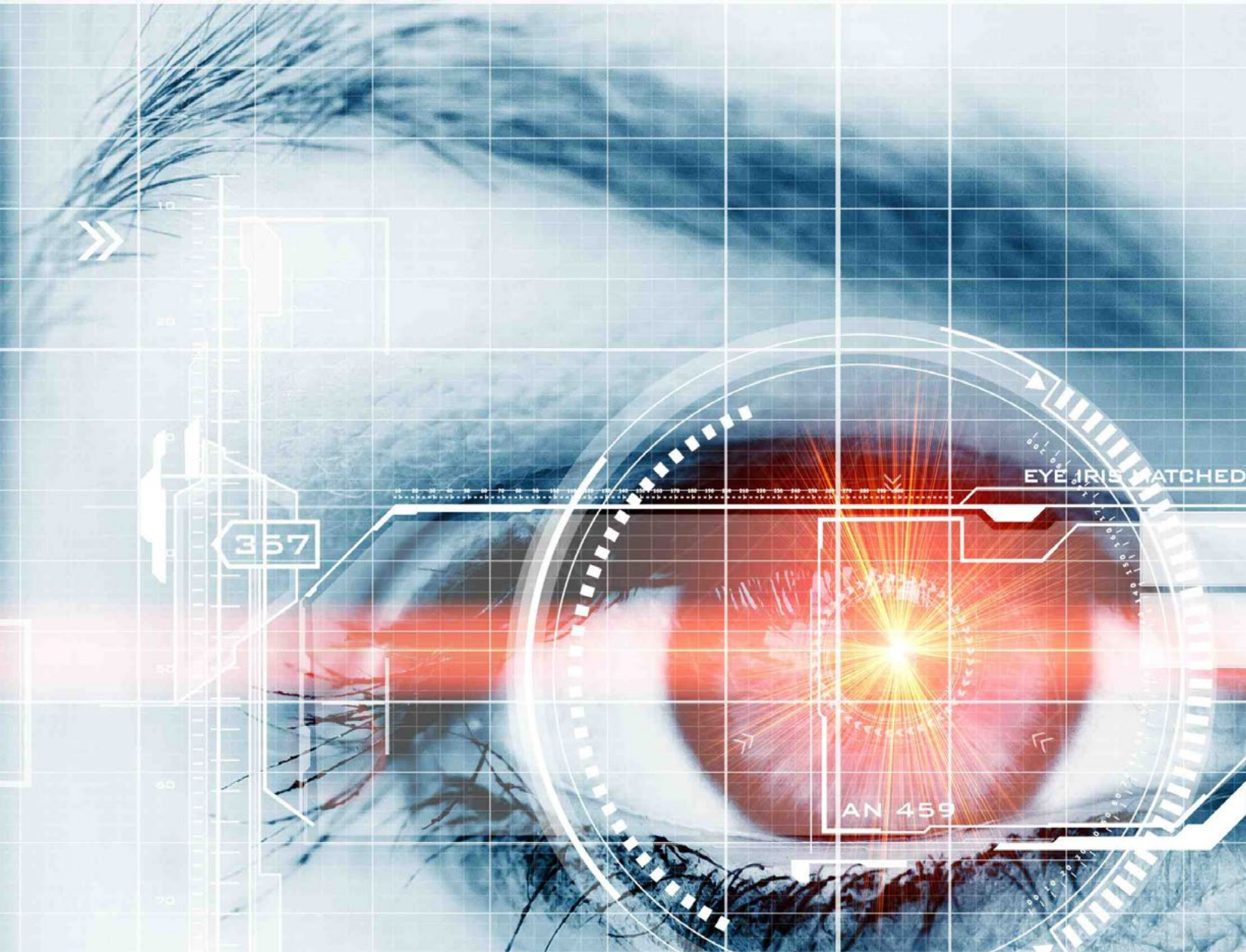
If you use cloud services like Box or Dropbox to store or share sensitive documents, there are a growing number of free encryption services, like an **nCrypted Cloud** (www.ncryptedcloud.com/download) that will make sure this data is well protected.

And with the increasing vulnerability of email communications to snoops and eavesdropping, free tools like **Vertru** (www.vertru.com) and **SendInc** (www.sendinc.com) can protect all your email communications.

If you believe in the power of encryption, and I hope you do, there are a growing number of free tools that will help you keep your privates private. There are lots of free products like **Bit Locker** and **Bit Locker To Go**, **Cloud Fogger**, **GPG**, **Our Secret**, **File Vault**, and many others. These products can encrypt files, folders, entire hard drives, thumb drives, communications, and plenty more.



THINK SECURITY FIRST!



HELPFUL RESOURCES

Chapter 32

CHAPTER 32

There are thousands of websites, bloggers, and commentators offering all kinds of advice on topics like identity theft and fraud, cybersecurity and cybercrime, privacy and a host of connected issues.

Rather than drown you in information, I've highlighted some of the most popular and respected destinations that should be able to answer most of your questions.

If you still can't find answers, just emailme@nealofarrell.com

IdentityTheft.Gov

From the Federal Trade Commission

This is your tax dollars at work, in a very comprehensive resource where you can get some of the best advice and tips on preventing identity theft, and even build and manage a case file if you fall victim. www.identitytheft.gov.

The Identity Theft Resource Center

The longest-running and most respected non-profit devoted to helping victims of identity theft. Their hotline has trained and experienced counselors who can help you navigate through even the most complicated types of identity theft.

Their hotline number is **888.400.5530** and their website is www.idtheftcenter.org.

The Identity Theft Council

Another victim support non-profit, the Identity Theft Council is also behind Operation Stop IT!, a national identity theft prevention initiative in partnership with the nation's police chiefs. Check them out at www.operationstopit.org.

The National Support Network for Victims of Identity Theft

This initiative is part of the non-profit Operation Stop IT! and is an online forum where victims and consumers can learn from experts, get advice from counselors, and share ideas and stories. Visit them at www.operationstopit.org

The National Cyber Security Alliance

The NCSA has been focused on consumer and business security education for a number of years and has some great free educational resources. www.staysafeonline.org.

PERSONAL SECURITY CHECKLIST

The best way to use this checklist is to just print off these few pages, check the boxes that apply, then regularly check back in to remind or improve.

The list isn't designed to be exhaustive, but just to cover some of the most important habits to get into.

IDENTITY THEFT

- ☐ Most important of all, always remain aware, vigilant, and careful of what you click on and the information you share.
- ☐ Never share any personal information, and especially a Social Security Number or date of birth, unless you have absolutely no choice.
- ☐ Protect your credit. Freeze or monitor your credit reports, although a freeze is better.
- ☐ If you have children under the age of 16, freeze their credit reports too.
- ☐ Protect personal information in the home and especially Social Security cards, birth certificates, passports, and tax returns.
- ☐ Never carry any Social Security Card with you.
- ☐ Check credit card and bank statements regularly and challenge any discrepancies.
- ☐ If your bank or credit union offers alerts of any changes or unusual activities on your accounts, enable as many as possible.

- ☐ Shred sensitive documents regularly, at least three or four times each year.
- ☐ Check your credit reports regularly for any inaccuracies or discrepancies.

TAX IDENTITY THEFT

- ☐ File your taxes as early as possible every year, before an identity thief has time to.
- ☐ Keep your tax return copies in a safe place in your home where burglars can't find them.
- ☐ Be careful about how you choose your tax preparer and what information you share with them.
- ☐ Be wary of calls, text messages, and emails, especially around tax time, claiming to be from the IRS.
- ☐ Guard your mail, always, but especially around tax time as thieves target it for tax and financial information.

COMPUTER SECURITY

- ☐ Make sure you have a firewall enabled and up-to-date antivirus software installed on every computer and device.
- ☐ Set your computer to automatically download and install all software updates and especially critical ones.
- ☐ Use a password lock or screensaver to protect access to your computer when you're not there.
- ☐ Back up your data regularly, both online and to a local external drive.
- ☐ When backing up to a local external drive, keep the drive disconnected when not backing up.

- If you have a Wi-Fi router, make sure to change the password from the factory default.
- If you use connected or IoT devices around your home, make their passwords strong and verify what information those devices collect.

PASSWORDS

- Change your important passwords frequently, and especially email, financial accounts, and social media.
- Make all your passwords as long and complicated as possible.
- Don't reuse old passwords, or use the same passwords for multiple accounts or sites.
- Protect your passwords and don't share them with others.
- Consider using a password manager.
- Don't share your passwords in response to a request by phone, text, or email.

ONLINE AND EMAIL

- Stopping clicking on stuff, and especially emails you're not expecting or don't recognize.
- If in doubt, just don't click. Don't give in to your curiosity.
- Stay away from websites you're not familiar with.
- Consider using a safe surfing or web anonymizer tool.

SOCIAL MEDIA

- ☐ Protect all your social media account passwords.
- ☐ Share and post as little as possible on social media.
- ☐ Set all accounts to private, connections or friends only.
- ☐ Beware of unsolicited connection or friend requests.
- ☐ Be careful about sharing messages and good causes on social media. Many are simply fraudulent.
- ☐ Be careful of what you read on social media, and be alert for fake news, fake stories, and fake alerts.

SCAMS AND FRAUDS

- ☐ When shopping, use a credit card instead of a debit or ATM card. Credit cards are safer.
- ☐ When using an ATM, be vigilant for any tampering on or around the ATM, or anyone standing too close to you (shoulder surfing).
- ☐ Avoid using those stand-alone ATMs. Apart from the higher fees you might face, they could also be tampered with.
- ☐ Be careful when pumping gas, as the pump could be compromised by hackers. And use a credit card instead of a debit card to pay.
- ☐ Warn children and the elderly to be vigilant for phone and email scams. Have them report them to you

SMALL BUSINESS SECURITY AND PRIVACY CHECKLIST

This list is by no means exhaustive, as there are so many threats and risks that can impact your business.

Print the list, check the boxes as you go, and refer to the list often as a way to remind yourself. And don't forget to share the list with team members and employees so everyone can play a role in protecting your business.

- ☐ Make security and privacy as important as profit, and integral to every business decision you make.
- ☐ If you have employees, make sure they're constantly trained and reminded about the most important security risks.
- ☐ When it comes to data privacy and security, there's a simple rule - if you can't protect it, don't collect it.
- ☐ Make sure you have a written security plan and policies so you have something clear to follow and share.
- ☐ Make sure every device and computer used by you and any employee has all the latest security software installed.
- ☐ Learn about ransomware, how to spot and avoid it, and make sure all employees are made aware too.
- ☐ Make sure you protect your website, limit admin access, create a strong website password, and use a website security service.

- Understand what Business Email Compromise scams are, and teach employees how to spot them.
- Respect all data, and especially customer, employee, and vendor information; only collect what you need; and protect it with multiple security layers.
- Make sure you have a clear and written password policy with tough rules on the creation, use, protection, and expiration of employee passwords.
- Make sure you have rules about the use of personal devices, like phones and tablets, for business tasks.
- Always be cyber alert when traveling, and especially at airports, hotels, and conferences.
- Have a clearly-written privacy policy on your website, and make sure you always honor it.
- Be constantly vigilant for phishing emails, know how to recognize them, and regularly remind all employees.
- Don't forget physical security. Burglars and intruders understand that the data on a laptop may be far more valuable than the laptop.
- Make sure all data, devices, and networks are protected with multiple layers of security, just in case one fails.
- Control access to sensitive data and resources, and only grant access to those who absolutely need it.
- Get familiar with any of the privacy and security regulations your business needs to comply with - and get compliant.
- Review your security regularly and at least every six months is ideal. Just like business, the security landscape is constantly changing.

- Recognize and remember that the best defenses against most threats are things like vigilance, awareness, education, and decisions. Not technologies.
- Back up all data constantly, and ideally online as well as to a local external drive (to protect against ransomware).
- After you back up to a local external drive, disconnect that drive so it can't be infected with malware like ransomware.
- Make sure all software and hardware are constantly patched and updated, and automatically if possible.
- Be very careful about what you and your employees download and share. Malware can hide anywhere.
- Be very careful with the use of thumb or USB drives, and teach employees to never plug them in unless they know what's on them.
- Use encryption wherever possible, but especially on mobile devices and to protect sensitive data.

BUSINESS TRAVEL SECURITY CHECKLIST

Whether you're an executive or an employee, or simply traveling for fun, you're always at risk to cyber and privacy threats. The threat to executives and employees is now so big, entire security conferences have emerged just focusing on this type of risk, and the Department of Homeland Security regularly issues warnings and tips to business travelers.

Our simple checklist was designed to help you remind yourself of the most common precautions you need to take in order to avoid the most likely risks.

Print it off, check the boxes, then review it regularly.

- ☐ First things first: always refer to this checklist before any business trip, domestic or foreign, to make sure your security and privacy are maximized.
- ☐ Treat travel like it's your workplace, but under attack. Exercise the same precautions and security hygiene as your workplace, but amp them up for extra precaution.
- ☐ To protect against identity theft, if there's no one at home make sure newspapers and mail are collected daily, lights are on at night, and ideally, a vehicle in the driveway.
- ☐ Sanitize your devices before you go, backing up and deleting any sensitive and non-essential data.
- ☐ Harden your devices before you leave. That means good security software, a device password or lock, and any security apps you're going to need.
- ☐ Don't download apps to your devices from foreign countries.
- ☐ Be very careful about using free wi-fi at airports, hotels, coffee shops, and conference centers, as they could be fake or vulnerable.

- If you do plan on using wi-fi when traveling, make sure you install a VPN before you leave.
- Don't use USB charging ports at airports, conference centers, or hotel rooms to charge your devices. They can also steal data.
- Stick to phones and tablets, and don't take a laptop unless you have to. Mobile devices are slightly more secure.
- Make sure all devices are fully patched and updated before you leave.
- Make sure you have a password manager installed on every device you use.
- Thinking about using a separate email address when traveling so that you don't have to log in to a personal or work email account. Simply redirect or forward emails to the temporary email address.
- Take as few documents as you need. Even seemingly innocent information could provide valuable clues if stolen.
- Don't trust a hotel safe for devices or data. Keep them with you at all times.
- Be careful logging in to sensitive accounts at airports. High powered cameras could capture your passwords or keystrokes.
- Disable auto connect on your devices so that they don't automatically connect to the nearest wi-fi network.
- Disable Bluetooth on your devices until you actually need it.
- Encrypt all sensitive data and documents all on all devices. With a laptop, make sure to use whole disk encryption so that everything is protected.

- Be very careful when using ATMs in foreign countries. Local security and consumer protection might be very different.
- Empty your wallet or purse before you leave. Remove all the cards and IDs that you won't need when traveling, and keep credit cards to a minimum.
- Don't use your ATM or debit card when traveling, even domestically. Stick to using a credit card, it's safer and offers better consumer protection.
- As you travel through security checkpoints at airports, don't get distracted and never take your eyes off your devices or laptop.
- If you think you're a high value target, turn off GPS and location tracking until you need it. Better still, power down all devices until you need them.
- Always carry your devices with you, and don't leave them in your luggage.
- Be aware, some countries will demand that you power up and open all devices before entry is granted, or may block the entry of devices containing encrypted information.
- Avoid guest computers and business services at hotels – they're too easy to compromise with malware.
- Be wary of calls purporting to be from the hotel front desk and asking you to verify your credit card number. The call could be coming from outside the hotel.
- Make sure that all accounts you want to access while traveling have 2-factor authentication enabled.
- If you carry an authentication token with you, never keep it with any devices that need authentication.

- If you plan to send sensitive information by email, make sure you're using company-approved encryption.
- If your text or phone conversations are sensitive, consider using one of the many and often free secure apps like Wickr or Signal.
- Be very wary of plugging USB or thumb drives into your devices, especially if you haven't had complete control of them.
- Don't accept promotional or informational USB or thumb drives at conferences or expos.

