Data Security in the Age of COVID-19


Presented by
Wynn J. Salisch
CCM, CHS, ETA CPP, MBKS
Principal, Casablanca Ventures LLC
• Payment processing savings
• Working capital sources
• Cyber security education
• Caring personal concierge service
• Trusted: Better Business Bureau A+ Rated
• Partner: United States Secret Service Electronic Crimes Task Force
Core Beliefs

The Golden Rule: Treat others the way you would want them to treat you.

Life is service - the one who progresses is the one who gives his fellow men a little more - a little better service.
Wynn J. Salisch
CCM, ETA CPP, MBKS

60+ years of show business experience onstage, backstage, in payment processing and cyber security training, and overseeing 1000+ stage & screen commercial and non-profit operations, a 16-000-seat stadium, and Presidential and U.S. Defense and State Department venues across 70 countries and 7 continents plus Oceania and afloat.

The Electronic Transaction Association’s Certified Payments Professional designation is the payments industry’s professional certification awarded for knowledge, professionalism, integrity and excellence in payment processing, earned by less than 1% of the entire payments industry.
Affiliations & Accreditations
How Credit Card Processing Works

1. Card presented by customer
2. Card is inserted into terminal
3. Processor communicates with card networks
4. Card network sends authorization to customer’s bank
5. Sale is complete
6. Processor sends approval to terminal
7. Card network relays approval to processor
8. Bank sends approval to card network
Interchange

1. The process of passing a card payment transaction between the...
   Merchant ⇄ Credit Card Processor ⇄ Payment Brands ⇄ Issuing Bank

2. The universal payments industry schedule of wholesale rates and fees.
Processing Costs: Interchange

• **100% goes to the card issuing banks for issuing and maintaining cardholder accounts.**
• Largest part (78%) of the total processing fees merchants pay.
• Set by the card brands (Visa, etc.) to reimburse issuing banks for the cost of cardholder accounts – underwriting, security, rewards, support, statements, etc.
• Non-negotiable.
• Over 400 rates & fees that vary by type of card used, risk level, industry, transaction size, elapsed time between authorization and settlement, how the transaction is processed (swiped/dipped vs. keyed-in vs. online gateway), and other factors.
• Published at [https://usa.visa.com/](https://usa.visa.com/) and [https://www.mastercard.us/en-us.html](https://www.mastercard.us/en-us.html)
• Interchange fees include:
  • Qualification Rate (a % of the transaction amount + a flat rate per transaction, e.g. 1.75% + $0.10)
  • Foreign Card Fees (around 3.00% Interchange + processor’s markup + 1.45% depending on card brand)
  • Authorization Fees (APF, NABU, Discover authorization fee) – $0.0145-$0.0195 per authorization depending on brand
  • Visa TIF/ZFL/Misuse – Applied to transactions that don’t follow Visa requirements ($0.045 to $0.10 per item)

Copyright © 2020 Casablanca Ventures LLC. All rights reserved.
### Interchange Rates

April 15, 2016

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Interchange Rate</th>
<th>Cap Rate</th>
<th>Ticket Rate I</th>
<th>Ticket Rate II</th>
<th>Ticket Rate III</th>
<th>Ride Rate</th>
<th>Credit Card</th>
<th>Debit Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Call</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Long Distance</td>
<td>1.0% + $0.10</td>
<td>1.75%</td>
<td>2.50%</td>
<td>3.30%</td>
<td>3.45%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Canadian Non-Pin</td>
<td>1.0% + $0.10</td>
<td>1.50%</td>
<td>2.25%</td>
<td>3.05%</td>
<td>3.20%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Canadian PIN</td>
<td>1.0% + $0.10</td>
<td>1.50%</td>
<td>2.25%</td>
<td>3.05%</td>
<td>3.20%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>International</td>
<td>1.25% + $0.10</td>
<td>2.00%</td>
<td>2.80%</td>
<td>3.60%</td>
<td>3.75%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Prepaid</td>
<td>1.0% + $0.10</td>
<td>1.50%</td>
<td>2.25%</td>
<td>3.05%</td>
<td>3.20%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>PIN Debit</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>PIN Credit</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Mobile</td>
<td>0.65% + $0.10</td>
<td>1.30%</td>
<td>1.90%</td>
<td>2.70%</td>
<td>2.85%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Voice over IP</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>VoIP</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>iBridges</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Tap2Pay</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Direct Debit</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>EFT</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Utilities</td>
<td>0.5% + $0.10</td>
<td>1.25%</td>
<td>1.85%</td>
<td>2.65%</td>
<td>2.80%</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### Interchange Rate Details

- **Base Rate**: The minimum rate applied to all transactions.
- **Cap Rate**: The maximum rate that applies to certain transactions.
- **Ticket Rate I**: The rate applied to the first tier of transactions.
- **Ticket Rate II**: The rate applied to the second tier of transactions.
- **Ticket Rate III**: The rate applied to the third tier of transactions.
- **Ride Rate**: The rate applied to ride-related transactions.
- **Credit Card**: The rate applied to credit card transactions.
- **Debit Card**: The rate applied to debit card transactions.

---

**Note**: Rates are subject to change and may vary based on specific terms and conditions.

---

Copyright © 2020 Casablanca Ventures LLC. All rights reserved.
Processing Costs: Network Fees

• **100% goes to the card brands (Visa, etc.) for use of their networks.**
• Average 4% of total fees required for processing a payment.
• Card brands set these fees.
• Not negotiable.
• Network fees include:
  • Assessments (11-15 bps depending on the brand)
  • Network Fees (Visa, MasterCard, Discover) – $0.005 per settled transaction
  • Visa FANF – Monthly cost per merchant based on several factors; ranges from $2.00 to $15.00 or more
Processing Costs: Processor Markups

• **100% goes to your processor for their costs in maintaining merchant account.**
• About 18% of the total fees you pay for your merchant account.
• Based on a business’s risk, size, negotiating power, knowledge, and other factors.
• Somewhat negotiable.

<table>
<thead>
<tr>
<th>Chargeback</th>
<th>Retrieval</th>
<th>Statement</th>
<th>Bank Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Account on File</td>
<td>Regulatory</td>
<td>ACH Reject</td>
</tr>
<tr>
<td>Annual</td>
<td>Early Termination</td>
<td>Transaction</td>
<td>Authorization</td>
</tr>
<tr>
<td>Settlement</td>
<td>Gateway Transaction</td>
<td>Gateway Access</td>
<td>Monthly Minimum</td>
</tr>
<tr>
<td>Return Transaction</td>
<td>Setup</td>
<td>Terminal Warranty</td>
<td>Programming</td>
</tr>
<tr>
<td>EMV Non-Enablement</td>
<td>Discount</td>
<td>Data Protection</td>
<td>Terminal Rental</td>
</tr>
<tr>
<td>PCI Compliance</td>
<td>PCI Non-Compliance</td>
<td>Mobile Access</td>
<td>Help Desk</td>
</tr>
<tr>
<td>Mailing</td>
<td>Supply &amp; Benefits</td>
<td>Address Verification</td>
<td>Per Item</td>
</tr>
<tr>
<td>Voice Authorization</td>
<td>Wireless Monthly</td>
<td>Online Access</td>
<td></td>
</tr>
</tbody>
</table>
Common Merchant Account Pricing Methods

1. INTERCHANGE-PLUS / COST-PLUS
   • A standard processor’s markup (basis points + cents) per transaction is applied to direct pass-through of the wholesale Interchange costs.
   • Caution: some processors pad the Interchange!
   • Yields long, complex statements, but is (sometimes) more cost-efficient.

2. TIERED
   • Simpler, easier-to-read monthly statements.
   • The 400+ wholesale Interchange rates & fees are bundled into 2-3 “buckets” or tiers: Qualified, Mid-Qualified, Non-Qualified
   • Caution: If a statement only shows a base rate followed by many line items of additional fees (EIRF, etc.), those are actually surcharges and your true cost is higher than the rate shown!

3. FLAT RATE
   • Simplest calculation and clearest monthly statements.
If it sounds too good to be true, it probably is!
The payments industry is rife with...

- Fee padding
- Misdirection
- Hidden fees
- Misleading offers like this one...

The itty bitty teeny tiny footnote reveals the big boldface .05% rate is really just for debit card transactions where the PIN is not used (a/k/a check cards), on cards issued by only the largest banks. It reads, *Durbin regulated Check Card percentage rate. A per transaction fee will also apply.*
Dancing the (Hidden) Statement Two-Step
Aggregators, or Payment Facilitators (PayFacs)

• Square, Stripe, PayPal, Braintree, InnPayment, Yapstone, etc.
• Not real processors – a PayFac has one merchant account in their corporate name with a real processor, and their clients simply share in that single account but do not have their own individual accounts.
• Created to simplify processing for micromerchants.
• Sign-up is simple because PayFacs use “progressive underwriting” to constantly monitor the wholesale cost of each client’s transactions.
• As a result, they have a history of selective rate increases by merchant to ensure profitability or even holding back deposits or suspending clients from service without warning if a client costs them too much.
• Square lost $127,000,000 last year and still has never been profitable.
COVID-19-Related Threats in Q1 2020

- **907K**
  Total spam messages related to COVID-19

- **737**
  Detected malware related to COVID-19

- **48K**
  Hits on malicious URLs related to COVID-19

- **220x**
  Increase in spam from Feb to Mar 2020

- **260%**
  Increase in malicious URL hits from Feb to Mar 2020

**United States**
Top location for spam and malware detections, and users accessing malicious URLs

*Detection numbers are based on the coverage of our Smart Protection Network, which has limited global distribution (collection period January 1 to March 31, 2020).*
COVID-19 Exploited by Malicious Cyber Actors

There is a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations. Threats include:

• Phishing, using the subject of coronavirus or COVID-19 as a lure,
• Malware distribution, using coronavirus- or COVID-19- themed lures,
• Registration of new domain names containing wording related to coronavirus or COVID-19, and
• Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

• Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
  • For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install "CovidLock" ransomware on their device.

• Open a file (such as an email attachment) that contains malware.
  • For example, email subject lines contain COVID-19-related phrases such as “Coronavirus Update” or “2019-nCov: Coronavirus outbreak in your city (Emergency)”.

43% of cyber attacks target small businesses.

60% of those hacked close their doors within 6 months.
How They Get In

Your Systems & Information

- Clients
- Vendors
- Suppliers
- Banks
- Telecom Providers
- Payroll Processors
- Cloud Service Providers
- IT Consultants
- Accounting Firms
- Law Firms

Copyright © 2020 Casablanca Ventures LLC. All rights reserved.
Your Digital Voice Assistant is Listening!
Protect Your DVA from Hackers

1. **Watch what you connect** – Since your voice assistant can be a hub for your connected devices — lights, thermostat, TV — be selective about what you connect. It’s smart not to connect security functions, such as a door lock or a surveillance camera. You don’t want a burglar to yell “Unlock the door!” and have your voice assistant oblige. At the same time, you should disable the feature that links your calendar or address book — often rich sources of information.

2. **Delete commands** – Smart speakers allow you to listen to your past commands and to erase some or all of them. This is a good way to wipe any sensitive information that may be stored. It’s true, your device may have to “relearn” a command, but it’s a quick learner.

3. **Be careful what you share** – There’s plenty of information you don’t want your voice assistant to know. That includes your passwords, credit card information, and Social Security number. Remember, it’s possible anyone could access your sensitive personal information just by asking for it.

4. **Turn off the microphone** – Consider muting your device when you’re not using it. That’s the easiest way to get your device to stop listening. Of course, you’ll have to turn it back on next time you want to check the weather. Or you could look outside.

5. **Turn off purchasing** – Smart speakers often can be set to make purchases on command. Anyone with access to the device may be able to make a buy. That could be a problem. The solution? Set up a purchase password and keep it a secret.

6. **Stay on top of notification emails** – What if someone happens to slip in a purchase. You’ll usually receive a notification email. If it’s something you didn’t order — maybe it’s something suspiciously suited to your 12-year-old — you can cancel it.

7. **Turn off “personal results”** - Your voice assistant may help you to pay bills and manage other personal information. That could expose information you’d rather keep private, such as passwords or bank account numbers. One option? Turn it off.

8. **Mind your network** – Use a WPA2 encrypted Wi-Fi network and not an open hotspot at home. Create a guest Wi-Fi network for guests and unsecured IoT devices.

9. **Enable voice recognition** – You may be able to configure your device for voice recognition. This enables your device to tell different voices apart. This can be helpful, but it may not work all the time.

10. **Strengthen your passwords** – Protect the service account linked to your device with a strong password. If it’s available, use two-factor authentication. This can prevent anyone who has access to the account from listening in remotely.
The compromised pump with the hidden camera bar still attached. Newer, more secure pumps have a horizontal card reader and a raised metallic keypad.
The fake panel (horizontal) above the “This Sale” display obscures a tiny hidden camera angled toward the gas pump’s PIN pad.
A front view of the hidden camera panel.
The unauthorized Bluetooth circuit board can be seen at bottom left attached to the pump’s power and card reader.
What’s at Risk

• Account Data – cardholder data, ACH/check info, Bitcoin private key
• Customer Data – PII, PHI, metadata, authentication info
• Corporate Data – sales, revenue, projections, employees
• Competitive Intelligence – pricing/cost, sourcing, new products, new markets
• Intellectual Property – R&D, processes, trade secrets, electronic products
Cybercrime by the Numbers

• EVERY DAY…
  • 80 BILLION malicious scans
  • 300,000 new malware released
  • 33,000 phishing attacks
  • 4,000 ransomware attacks
  • 780,000 records lost due to hacking

• 90% of breaches were caused by phishing
  • 65% growth in phishing attempts in the past year.
  • 30% of phishing messages get opened by targeted users.
    ...12% of targets clicked on the malicious attachment or link
    ...50% of those did so within an hour.
  • 15% of people successfully phished will be targeted at least one more time within a year.

• 72% of breaches involved firewalls not up to security standards or improperly configured.
• 63% of breaches involved weak, default or stolen passwords.
• 61% of breached merchants didn’t have effective antivirus software.
• 60% of hackers compromise an organization within minutes.

**Surface Web**

- Yahoo!
- Google
- CNN
- Bing

**Deep Web**

- Academic databases
- Medical records
- Financial records
- Legal documents
- Some scientific reports
- Some government reports
- Subscription-only information
- Some organization-specific repositories

- 96% of content on the Web (estimated)

**Dark Web**

- TOR
- Political protest
- Drug trafficking and other illegal activities

---

**HOW DO YOU ACCESS THE DARK WEB?**

The dark web can be accessed through specific browsers. The most popular browser is The Onion Router or simply known as TOR. Because the websites in the dark web are not indexed, the use of TOR hides the IP addresses of websites within the dark web to maintain its anonymity. The IP addresses are hidden using the .onion suffix.
For Sale: Everything & Anything

<table>
<thead>
<tr>
<th>Murder Types</th>
<th>Low Rank</th>
<th>Medium Rank</th>
<th>High Rank and Political</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular</td>
<td>$45,000</td>
<td>$90,000</td>
<td>$180,000</td>
</tr>
<tr>
<td>Missing in action</td>
<td>$60,000</td>
<td>$120,000</td>
<td>$240,000</td>
</tr>
<tr>
<td>Death in accident</td>
<td>$75,000</td>
<td>$150,000</td>
<td>$300,000</td>
</tr>
<tr>
<td>Cripple Types</td>
<td>Low Rank</td>
<td>Medium Rank</td>
<td>High Rank and Political</td>
</tr>
<tr>
<td>Regular</td>
<td>$12,000</td>
<td>$24,000</td>
<td>$48,000</td>
</tr>
<tr>
<td>Uglify</td>
<td>$18,000</td>
<td>$36,000</td>
<td>$72,000</td>
</tr>
<tr>
<td>Two Hands</td>
<td>$24,000</td>
<td>$48,000</td>
<td>$96,000</td>
</tr>
<tr>
<td>Paralyse</td>
<td>$30,000</td>
<td>$60,000</td>
<td>$120,000</td>
</tr>
<tr>
<td>Rape</td>
<td>Low Rank</td>
<td>Medium Rank</td>
<td>High Rank and Political</td>
</tr>
<tr>
<td>Regular</td>
<td>$7,000</td>
<td>$14,000</td>
<td>$28,000</td>
</tr>
<tr>
<td>Under age</td>
<td>$21,000</td>
<td>$42,000</td>
<td>$84,000</td>
</tr>
<tr>
<td>Bombing</td>
<td>Low Rank</td>
<td>Medium Rank</td>
<td>High Rank and Political</td>
</tr>
<tr>
<td>Simple</td>
<td>$5,000</td>
<td>$10,000</td>
<td>$20,000</td>
</tr>
<tr>
<td>Complex</td>
<td>$10,000</td>
<td>$20,000</td>
<td>$40,000</td>
</tr>
<tr>
<td>Beating</td>
<td>Low Rank</td>
<td>Medium Rank</td>
<td>High Rank and Political</td>
</tr>
<tr>
<td>Simple</td>
<td>$3,000</td>
<td>$9,000</td>
<td>$18,000</td>
</tr>
</tbody>
</table>

**Dark Web Prices**

- Social Security: $1
- DDOS as a service: ~$7 per hour
- Medical record: $50 and up
- Credit card data: $0.25 to $60
- Bank account info: $1,000 and up depending on the account type and balance
- Mobile malware: $150
- Spam: $50 for ~500,000 emails
- Exploits: $1,000-$300,000
- Malware development: $2,500 (Commercial malware)
- Facebook account: $1 for an account with 15 friends

Source: RSA

Copyright © 2020 Casablanca Ventures LLC. All rights reserved.
Credit Card Dumps

What are the bank logins and credit cards available?

Some Of US \ UK Banks Available Now

For United States Of America Banks

<table>
<thead>
<tr>
<th>Bank Names</th>
<th>Balance</th>
<th>Price</th>
<th>Preview Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank Of America</td>
<td>Between 2k - 50k</td>
<td>$400</td>
<td>Download</td>
</tr>
<tr>
<td>WellsFargo</td>
<td>Between 4k - 40k</td>
<td>$300</td>
<td>Download</td>
</tr>
<tr>
<td>Chase Bank</td>
<td>Between 2k - 30k</td>
<td>$250</td>
<td>Download</td>
</tr>
<tr>
<td>Citibank</td>
<td>Between 0k - 70k</td>
<td>$300</td>
<td>Download</td>
</tr>
<tr>
<td>Wachovia</td>
<td>Between 2k - 18k</td>
<td>$275</td>
<td>Download</td>
</tr>
</tbody>
</table>

For United Kingdom Banks

<table>
<thead>
<tr>
<th>Bank Names</th>
<th>Balance</th>
<th>Price</th>
<th>Preview Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barclays</td>
<td>Any Balance</td>
<td>$400</td>
<td>Download</td>
</tr>
<tr>
<td>HSBBC</td>
<td>Between 30k - 312k</td>
<td>$400 up to 100k=600$</td>
<td>Download</td>
</tr>
<tr>
<td>Halifax</td>
<td>Between 20k - 180k</td>
<td>$450</td>
<td>Download</td>
</tr>
<tr>
<td>Nationwide</td>
<td>Between 15k - 230k</td>
<td>$450</td>
<td>Download</td>
</tr>
<tr>
<td>Lloyds TSB</td>
<td>Between 10k - 400k</td>
<td>$600</td>
<td>Download</td>
</tr>
</tbody>
</table>

If You Are Not Able To Raise The Amount For Any Of The Logins. I Can Make For You Any Transfer To Any Bank Listed With Upfront 250€ And My Shares 20%

Payments With: E-gold, Western Union, Moneygram, Moneybookers.

Copyright © 2020 Casablanca Ventures LLC. All rights reserved.
Valuable Social Media Accounts

$12.99
ACCOUNT HACKING PROGRAM
USED TO HACK SOCIAL MEDIA ACCOUNTS

HACKED ACCOUNTS ARE THEN USED FOR:
Purchasing Products | Broadcasting | Verification | Cashouts and more.

Copyright © 2020 Casablanca Ventures LLC. All rights reserved.
Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so much time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don’t pay in 7 days, you won’t be able to recover your files forever. We will have free events for users who are so poor that they couldn’t pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkhHljcRdfjINXj6LrLn

Copy

Check Payment

Decrypt
THE STATE OF RANSOMWARE AMONG SMBs

In the last 12 months:

- **22%** of organizations had to cease business operations immediately because of ransomware.
- **81%** of businesses have experienced a cyberattack.
- **66%** have suffered a data breach.
- **35%** were victims of ransomware.

Source: Malwarebytes
INFECTION TO ENCRYPTION IN 3 SECONDS

SECOND 0
User clicks on phishing email

SECOND 1.0
User unknowingly downloads ransomware

SECOND 1.5
Ransomware unpacks and executes

SECOND 2.0
Ransomware downloads encryption keys

SECOND 2.5
Scans computer to identify all attached drives

SECOND 3.0
File encryption begins

User gets ransom notification

ENCORPTION COMPLETED
Cyber Attack Stats

- There is a cyber attack every 39 seconds.
- 43% of cyber attacks target small businesses.
- 95% of cybersecurity breaches are due to human error.
- The average cost of a data breach in 2020 will exceed $150 million.
- Total cost for global cybercrimes has added up to over $1 trillion dollars in 2018.
- $6 trillion is expected to be spent globally on cybersecurity by 2021.
Discovering a Breach

Average time it takes a company to detect that they’ve been breached:

250-300 days

Source: 2017 Nuix Black Report
The Target Breach

1. All Target stores used same HVAC contractor.
2. Malware delivered in an email to employees.
3. VPN (Virtual Private Network) credentials used by the contractor to remotely connect to Target’s network were then stolen.
4. That foothold was then used to push malicious software down to all of the case registers at more than 1,800 stores nationwide.
5. DAMAGE:
   • 70 MILLION credit & debit card account numbers stolen.
   • $595,000,000.00 estimated value to the hackers.
   • Total cost to Target: $291,000,000.00 PLUS lost sales and profits due to reduced consumer trust.
The Equifax Breach

How Attackers Exploited Vulnerabilities in the 2017 Breach, Based on Equifax Information

1. Attackers scan the web for vulnerable servers
2. Attackers find a vulnerability within the Equifax dispute portal servers
3. Attackers locate additional servers and login credentials
4. Data extraction extends over 76 days
5. Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559

United States Government Accountability Office
Breaches are Expensive!

Malicious or criminal attacks are the leading root cause of a data breach...and result in the highest cost per record.

- Human error: 29% - $134 per record
- Malicious or criminal attack: 47% - $170 per record
- System glitch: 26% - $142 per record

“65% of all cyber attacks happen on small to medium sized businesses. And 60% of those who have a data breach go bankrupt in 6 months. So a data breach is literally a death sentence for these businesses.”

Source: Small Business Association of America 2013
<table>
<thead>
<tr>
<th>Breach Remediation Item</th>
<th>Approximate Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI Forensic Investigator</td>
<td>$50,000 to $5000,000 +</td>
</tr>
<tr>
<td>Forensic investigation</td>
<td>$12,000 to $100,000 +</td>
</tr>
<tr>
<td>Accelerated Remediation: Short-term - Stop the bleeding Controls (low-hanging fruit) &amp; full PCI gap assessment Long-term processes and procedures, and tactical and strategic fixes</td>
<td>$200,000 to $500,000 + $500,000 to $1,000,000 + $1,000,000 to $10,000,000 +</td>
</tr>
<tr>
<td>Card brand compromise fines</td>
<td>$5,000 to $50,000 +</td>
</tr>
<tr>
<td>QSA assessments</td>
<td>$20,000 to $100,000 +</td>
</tr>
<tr>
<td>Free credit monitoring for affected cardholders</td>
<td>$10 to $30 per card</td>
</tr>
<tr>
<td>Card re-issuance penalties</td>
<td>$3 to $10 per card</td>
</tr>
<tr>
<td>Breach notifications - each affected cardholder must be notified as required by their own (not just your) state’s law, usually within 30 days of when the PFI confirms the breach and notifies you; there are significant fines for violating state deadlines</td>
<td>$2,000 to $5,000 +</td>
</tr>
<tr>
<td>Technology repairs</td>
<td>$2,000 to $10,000 +</td>
</tr>
<tr>
<td>Legal fees</td>
<td>$5,000 to $100,000 +</td>
</tr>
<tr>
<td>Increased card processing fees</td>
<td></td>
</tr>
<tr>
<td>Civil judgments</td>
<td></td>
</tr>
<tr>
<td>Reputational costs - after a breach, many businesses have lost up to 40% of their sales from customers losing confidence in their brand</td>
<td>Up to 40% of sales</td>
</tr>
<tr>
<td>PR &amp; marketing communications firm retainer</td>
<td>Expensive</td>
</tr>
<tr>
<td>Insurance co-pays</td>
<td></td>
</tr>
</tbody>
</table>
A Public Relations Nightmare

76% The percentage of Americans who say they would stop doing business with a company following a data breach.

Source: Ponemon Institute
The problem with passwords

Hackers have more than one way to get in, but passwords are the most common soft spot

- **81%**: Bad/weak passwords
- **51%**: Install malware
- **43%**: Social media scam
- **14%**: Internal mistake
- **14%**: Internal access abuse

Source: Verizon
The 50 Most Used Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon
11. 123123
12. baseball
13. abc123
14. football
15. monkey
16. letmein
17. shadow
18. master
19. 696969
20. michael
21. mustang
22. 666666
23. qwertyuiop
24. 123321
25. 1234...890
26. p*s*y
27. superman
28. 270
29. 654321
30. 1qaz2wsx
31. 7777777
32. f*cky*u
33. qazwsx
34. jordan
35. jennifer
36. 123qwe
37. 121212
38. killer
39. trustno1
40. hunter
41. harley
42. zxcvbnm
43. asdfgh
44. buster
45. andrew
46. batman
47. soccer
48. tigger
49. charlie
50. robert
I changed all my passwords to “incorrect”
So whenever I forget, it will tell me “Your password is incorrect.”
Another Solution...
Password Entropy

**Password entropy** – measurement of a password’s unpredictability based on the character set used (which is expansible by using lowercase, uppercase, numbers, and symbols) and password length.

For example, at 1,000 guesses per second...

- *Tr0ub4dor&3* would take **3 days** to crack.
- *correcthorsebatterystaple* would take **550 years** to crack.
  - Don’t use this specific one because it’s already been widely publicized on the web. Come up with your own.
## How long will it take to crack your password?

<table>
<thead>
<tr>
<th>Length of Password (Chars)</th>
<th>Only Numbers</th>
<th>Mixed Lower and Upper case alphabets</th>
<th>Mixed numbers, Lower and Upper case alphabets</th>
<th>Mixed numbers, Lower and Upper case alphabets, symbols</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>4</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
<td>Instantly</td>
</tr>
<tr>
<td>5</td>
<td>Instantly</td>
<td>3 secs</td>
<td>10 secs</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Instantly</td>
<td>8 secs</td>
<td>13 mins</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Instantly</td>
<td>5 mins</td>
<td>17 hours</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Instantly</td>
<td>3 hours</td>
<td>57 days</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4 secs</td>
<td>4 days</td>
<td>12 years</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>40 secs</td>
<td>169 days</td>
<td>1 year</td>
<td>928 years</td>
</tr>
<tr>
<td>11</td>
<td>6 mins</td>
<td>16 years</td>
<td>71k years</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>1 hour</td>
<td>600 years</td>
<td>5m years</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>11 hours</td>
<td>21k years</td>
<td>423m years</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>4 days</td>
<td>778k years</td>
<td>5bn years</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>46 days</td>
<td>28m years</td>
<td>2tn years</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>1 year</td>
<td>1bn years</td>
<td>193tn years</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>12 years</td>
<td>36bn years</td>
<td>14gd years</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>126 years</td>
<td>1tn years</td>
<td>1qt years</td>
<td></td>
</tr>
</tbody>
</table>
Solution: A Password Manager!

Go to CNET.com or PCMag.com for unbiased reviews and comparisons.
Password Advice

1. Never use the same password twice. (And no, “poodle 3” and “poodle4” don’t count as different passwords.)

2. Use long randomly-generated gibberish passwords, or word strings without spaces.

3. Store them securely in a password manager.
   • Visit www.cnet.com for unbiased reviews of popular password manager apps and software, and then use a very secure password to protect access to the password manager.

4. At the very minimum, use a:
   • Basic password for websites that don’t store or require any of your personal information,
   • Secure password for retailer websites where you enter your credit card information, and a
   • Very secure password for financial, medical and other websites containing your most sensitive information.

5. Change passwords at least annually; quarterly for sensitive sites.

6. Remember: a good password written down and stored in a secure location is much better than a bad password memorized!
Clicking on the Change Password link above is how John Podesta, the chairman of Hillary Clinton’s presidential campaign, had his email account compromised. Logging in via the embedded Change Password button exposed his username and password to the hackers. What he should have done instead was to close the email, open his browser, log into his Gmail account via his known link, and changed his password that way.
Welcome to the LinkedIn Network Security community!

Diane Sibbet <diane.sibbet@smurl.org>

Dear David,

I would like to invite you to come and join the Network Security, Management and Monitoring group on LinkedIn, which was just established as a community for professionals who are interested in keeping up on the latest technologies and strategies for network security.

Meet and share ideas with people who are passionate about creating safe computing environments for their users to get work done without having to worry about security all the time. What are the best technologies to use for firewalls, detection and alerting? How can we avoid creating performance bottlenecks and added complexity that make it harder for users to get things done?

You can join us on LinkedIn now for free:

https://www.linkedin.com/groups/12013406

I will make sure to approve your membership request soon after you submit it.

I look forward to seeing you soon.

Kind regards

Diane Sibbet

If you'd like to unsubscribe and stop receiving these emails click here.

Do you know the sender?

Hold your mouse over a link to show it's REAL web address.

http://smurl.org/AAAAAMlV3qDNBqQAFv=3
Don’t click on links in emails or open attachments unless you recognize the source.

Be cautious and wary, and inspect the email address for strange features like extra digits or characters, misspellings, grammatical or syntax errors, etc.

Even then, be careful. A healthy dose of skepticism is advisable in our online world.

Open your browser and enter the URL for the page from your records, not the email.

Hackers spoof emails to look almost exactly like the page you’re used to seeing.

Turn on your spam filters.

Don’t Get Caught by Phishing Attempts!
1. Freeze (not lock) your credit for free with all four credit reporting agencies to prevent anyone from pulling your records except you and those financial institutions where you already do business:

   - Equifax: https://www.equifaxsecurity2017.com/
   - Experian: https://www.experian.com/freeze/center.html
   - Innovis: https://www.innovis.com/personal/securityFreeze
   - TransUnion: https://www.transunion.com/credit-freeze/place-credit-freeze

2. To allow future lenders to pull your records, you’ll need a PIN that each of the above credit agencies will give you when you freeze your account (keep it somewhere safe!) so you can unfreeze your records either for a few days or permanently.

3. Once your credit has been checked by the lender you’ve authorized, you should re-freeze the records.
This isn’t foolproof.

- Criminals can still use your stolen information to file bogus tax returns for refunds, make bogus medical claims against your medical insurance, etc.
- File your taxes as early as possible.
- Monitor your insurance records to ensure no one else is getting benefits on your plan.
- Request a full copy of your complete medical history file to serve as a benchmark in case someone pulls something in the future.
Credit or Debit?

1. **Always use credit, not debit, cards for purchases.**
2. Debit cards should only be used to withdraw cash at bank ATMs (not ones outside or in stores as these can be tampered with much more easily than those inside banks).
3. Consumer protections are stronger for credit cards (e.g. issuers’ zero-liability policies) than debit cards (no such policies).
4. Card skimming, in which an illegal reader is attached to a payment terminal, is a pervasive financial scam.
5. If a debit card is compromised your entire checking account gets drained and all your outstanding checks will bounce, and banks require a lot of red tape and take a long time to reimburse you. When fraud happens on a credit card, you just contact the issuer and they’ll delete the offending transaction or issue you a new card, and you’re done.
6. Using a debit card for purchases doesn’t help your credit score at all.
7. If there’s a cashier error on a debit card, you have to wait weeks while the bank investigates and then they may or may not reimburse you.
8. Set up fraud alerts for both your credit and debit cards.
Check Your Credit Reports Regularly for Free at www.annualcreditreport.com

You’re allowed one per year for free from each of the big 3 credit bureaus (hopefully newcomer Innovis will soon be included), so spread them across the year (e.g., pull your report from Experian now, Equifax in 4 months, Trans Union in 8 months, and then repeat the cycle with Experian in 12 months – you can do them in any order, but you can only get a free report from each one once every 12 months).
CYBER SAFETY CHECKLIST

- Back up online and offline files regularly and securely
- Strengthen your home network
- Use strong passwords
- Keep your software updated
- Manage social media profiles
- Check privacy and security settings
- Avoid opening and delete suspicious emails or attachments
Solutions

• Cyber (breach) Insurance
  • ~ $1500 per year for $1 million in coverage.
  • Available from a growing number of insurance companies.
  • Should cover as many of the cost elements as possible.
  • Some processors offer it, but review the coverage details.

• Comply with PCI DSS and GDPR security mandates

• Use layered security
  • Tokenization
  • Encryption
  • EMV
  • Smart passwords – no dictionary words, children or pet names, or default passwords), multi-factor authentication (complex passwords + cellular text code or biometric scan

• Segment your network to restrict cross-contamination of systems by hackers...and guests!

• Secure remote access with multiple layers of authenticating security

• Install security systems including multiple robust firewalls and intrusion detection & prevention systems.

• Conduct a thorough risk assessment to identify data targets and the threats against them.

• Monitor your systems: regularly review firewall and intrusion detection & prevention logs to see threats to your systems
Your Takeaways

1. **Layered security**: Passwords, tokenization, encryption, multi-factor authentication, watchfulness, and PCI compliance for all POS, PMS, CRM, and online solutions, system vendors, and data handling procedures (passwords, credit card data, sensitive PII).

2. **Freeze your credit now**.

3. **Latest versions** of your computer’s firewall, antivirus software, programs, and operating system.

4. **Complex passwords** for sensitive websites (financial, etc.) should be complex and not contain any proper nouns, dictionary words, personal information (pet names, digit sequences from your SSN, etc.), or keyboard patterns (QWERTY, etc.); instead, use nonsense phrases strung together without spaces or long words corrupted with numbers, symbols and upper/lower case letters.

5. **Breach insurance**.

6. **Use a Trusted Advisor** like an accredited Certified Payments Professional with decades of hands-on experience as both an innkeeping and payments professional to guide and advise you and help you reduce risk and save money to protect your valuable business!
“...the beginning of a beautiful friendship.”
Thank You!

For a copy of this presentation plus additional data security information, please email me.

Wynn J. Salisch
CCM, ETA CPP, MBKS
203-253-7259
wynn@casablanca-ventures.com