Protecting Yourself Against Identity Theft and Scams

SERGEANT MATT KUETHER

DETECTIVE

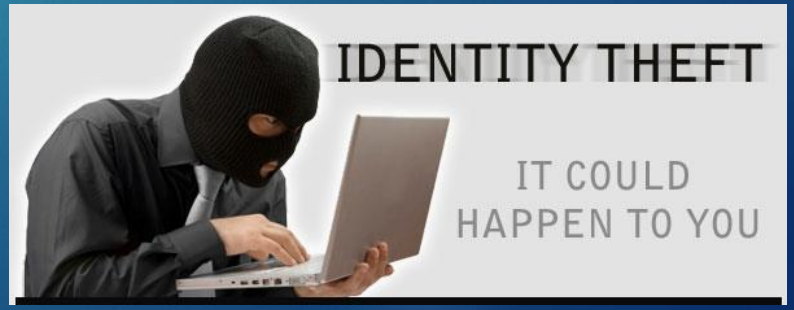
APPLETON POLICE DEPARTMENT

Identity Theft

- unauthorized use or attempted use of an existing account
- unauthorized use or attempted use of personal information to open a new account
- misuse of personal information for a fraudulent purpose.

The 2017 **Identity Fraud Study**, released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion and 13.1 million victims a year earlier. In the past six years identity thieves have stolen over $107 billion.

- Approx. 60% of victims are 50 or older.



Stealing Your Identity

Thieves are getting smarter. With technology advancing it's becoming easier to steal your identity.

- Phishing- the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
- Theft- Wallet, purses, mail, phone
- Going through your trash
- Skimming devices
- Data Breach
- Finding your personal info. laying around/overhearing conversations/looking over your shoulder.

Top Financial Scams Targeting Seniors

According to the National Council on Aging

- Medicare/Health Insurance Scams
  - Perpetrators may pose as a Medicare representative to get older people to give them their personal information.
  - Perpetrators may provide bogus services for elderly people at makeshift mobile clinics, they use personal information provided to bill Medicare and pocket the money.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- Counterfeit Prescription Drugs
  - Most commonly operated on the Internet. Besides paying money for something that will not help a person's medical condition, victims may purchase unsafe substances that can inflict even more harm.
- Funeral and Cemetery Scams
  - Scammers read obituaries and then call or attend funeral services to approach widow or widower (or other family) about fictitious, unsettled debt with the deceased
  - Disreputable funeral homes may take advantage of unfamiliarity with funeral costs and add unnecessary charges to the bill.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- Fraudulent Anti-Aging Products
  - Scammers may offer fake treatments, which could be harmful to victims, or completely bogus homeopathic remedies that do absolutely nothing.
- Investment Schemes
  - Pyramid or inheritance schemes targeted towards seniors looking to safeguard their cash for their later years.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- Telemarketing/Phone Scams
  - Very common – Very difficult to trace
    - Scammer will tell the victim they have a large sum of money and will share it if the person makes a "good faith" payment by withdrawing funds from their own account. Can involve second person furthering the scheme by posing as a trusted individual like a lawyer, banker, etc.
    - Scammer may get the victim to wire or send money on the pretext the person's child, grandchild, or other relative is in the hospital or jail and needs money.
    - Scammers may solicit money for fake charities. This often occurs after natural disasters.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- Internet Fraud
  - Pop-up browser windows can simulate virus-scanning software and fool victims into either downloading a fake anti-virus program, at a substantial cost, or an actual virus that will open up whatever information is on the user's computer to scammers.

- Email/Phishing Scams
  - A senior may receive email messages appearing to be from a legitimate company or institution, asking them to update or verify their personal information. Another example is a senior receiving an email appearing to be from the IRS about a tax refund.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- Homeowner/Reverse Mortgage Scams
  - Seniors targeted because many of them own their homes outright, which is a very valuable asset
  - Fake letters sent out, appearing to be from the local assessor's office, and offering to arrange a reassessment, for a fee, to lower the homeowner's tax burden.
  - Scammers can take advantage of older adults who have recently unlocked equity in their homes. Those considering reverse mortgages should be cognizant of people in their lives pressuring them to obtain a reverse mortgage, or those that stand to benefit from the borrowing accessing equity, such as home repair companies who approach the older adult directly.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- Sweepstakes and Lottery Scams
  - Scammers inform the victim they have won a lottery or sweepstakes of some kind and need to make a payment to unlock the prize money. Often, seniors will be sent a check they can deposit in their bank account, knowing that while it shows up in their account immediately, it will take a few days before the fake check is rejected. The perpetrator will collect supposed fees or taxes prior to the bank removing the "prize money" from the victim's account as soon as the check bounces.

Scams Targeting Seniors Cont'd

According to the National Council on Aging

- The Grandparent Scam
  - Scammers will place a call to an older person and when the person picks up, the scammer will say something along the lines of: "Hi Grandma, do you know who this is?" When the unsuspecting grandparent guesses the name of the grandchild the scammer most sounds like, the scammer has established a fake identity without any background research.
  - The scammer will then ask for money to solve some unexpected financial problem, to be paid via Western Union or MoneyGram, which don't always require ID to collect. Scammers will often beg the grandparent, "Please don't tell my parents, they would kill me!"

Scams

FRAUD ALERT

"IRS SUING YOU?"

"WON THE LOTTERY?"

"MICROSOFT" CALLING?

"FAMILY MEMBER IN JAIL?"

HANG UP!

IF IT SOUNDS TOO GOOD TO BE TRUE, IT PROBABLY IS.
NEVER PROVIDE SENSITIVE PERSONAL INFORMATION OVER THE TELEPHONE.

What Can You Do To Protect Yourself?

- Be mindful about who you give your personal information to.

Phone

Mail

Internet

What Can You Do To Protect Yourself?

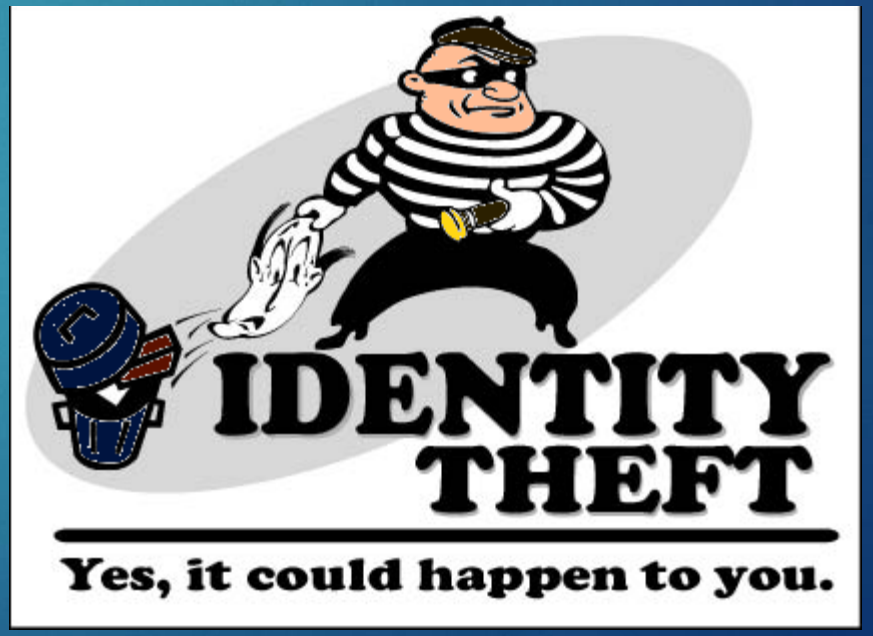
- Don't carry unnecessary personal information on your person, in your wallet/purse, in your vehicle.

Social Security Card

Passport

PIN #'S or Passports

Checks



What Can You Do To Protect Yourself?

- Don't leave personal or financial information in the open. 20% of victims know the suspect.

Family members

Friends

Neighbors

Co-workers

Caregiver/Housekeeper (including hotels)

- Mailbox Considerations- Outgoing Mail.
  - Theft of mail on the rise. Go to Post Office.
- Public use computers

What Can You Do To Protect Yourself?

- Properly destroy personal documents before throwing them out.
- Shred financial statements, bank statements, credit card apps, old credit cards, etc.
- Use a shredder that shreds in pieces rather than strips (strips can be re-constructed).

Things to Watch Out For

- A phone call or email from someone asking you for money or personal information.
- An offer in an email that sounds ‘too good to be true.’
- An email or call from someone you do not know, about a product you have never heard of or from a company you have never dealt with.
- An email or text message that asks you to click a link or download software.
- An email or text message from someone or a company that is unlikely to make personal contact. For example, a company like Microsoft is unlikely to call everyone who uses Windows to tell them about a problem.
- An email that contains a suspicious attachment.

Be Proactive and Not Reactive

- Use creative passwords for online accounts. Change if needed.
- Make a photocopy of important docs- SSC, CC's, DL, etc. Keep this in a safe place.
- Consider online banking for more effective monitoring of bank statements.
- Check your credit report annually.

www.annualcreditreport.com

1-877-322-8228

One from each company, so check a different one every four months.

I'm A Victim…Now What?

- Don't be afraid or embarrassed to talk about it with someone you trust.
- You are not alone, and there are people who can help.
- Keep handy the phone numbers and resources you can turn to, including the local police, your bank, and Adult Protective Services.

I'm A Victim…Now What?

- ID Theft- Place a fraud alert on your credit reports (90 days). It makes creditors verify your identity before making any changes.
- When you place a fraud alert you're entitled to a copy of your credit report. Check for unauthorized accounts.
- Close accounts that have suspicious activity or were opened without your permission. May require completion of affidavit of fraud/forgery.
- FREEZE your credit!!! (Must freeze with each company)

- Unlawful use of credit card/unauthorized charges to bank account- Notify your CC company or bank immediately to cancel the card or put a hold on the account.

- Contact your local law enforcement agency if necessary. Some financial institutions will require a police report. Local police department SHALL take a report. WI Statute 943.201(4)

Credit Card vs Debit Card Which is Safer?

The key difference: With a credit card, the card issuer must fight to get *its* money back. With a debit card, you must fight to get *your* money back.

When a fraudulent transaction occurs on your credit card, you have lost no money. You can report the fraud, get a credit on your statement, and the issue will never affect your bank account.

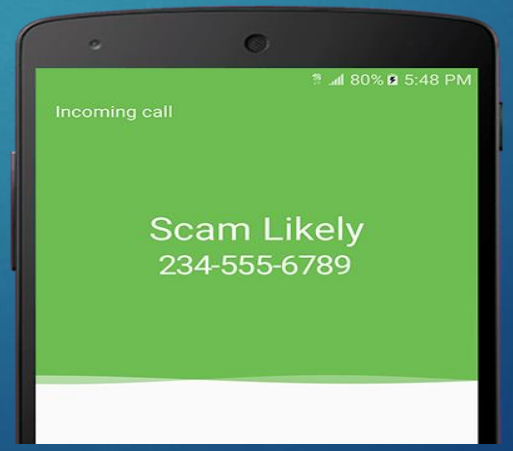
With a debit card, your bank account balance is affected from the moment the fraudulent transaction takes place. If the transactions are significant, you could experience a domino effect of financial headaches. Fraudulent charges can tie up funds so that legitimate charges are declined or cause overdrafts.

10 Things You Can Do to Avoid Fraud

Spot imposters- Scammers often pretend to be someone you trust, like a government official, charity or a company you do business with. Don't send money or give out personal information in response to an unexpected request — whether it comes as a text, a phone call, or an email.

Do online searches- Type a company or product name followed by "scam." Search phone numbers.

Don't believe your caller ID



Avoiding Fraud

Don't pay upfront for a promise- Don't pay in advance for things like debt relief, credit and loan offers, mortgage assistance or job. They might even say you've won a prize, but first you have to pay taxes or fees. If you do, they will probably take the money and disappear.

Consider how you pay. Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through Western Union or MoneyGram is **risky** because it's nearly impossible to get your money back. Government offices and honest companies won't require you to use these payment methods or ask for gift cards.

Avoiding Fraud

- **Talk to someone.** Before you give up your money or personal information talk to someone. Ask questions. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, do an online search, or consult an expert

- **Hang up on robocalls-** Don't call them back. This could lead to more calls.

- **Don't deposit a check and wire money back.** By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If a check you deposit turns out to be a fake, you're responsible for repaying the bank.

Avoiding Fraud

- NEVER PAY FOR ANYTHING VIA GIFT CARDS!!!!
- EVER… NEVER EVER!
- SERIOUSLY, DON'T DO IT.

Resources

- Request a FREE Credit report annually
  - Call (877)322-8228
  - Online at www.annualcreditreport.com
- NO CALL Program
  - National Do Not Call Registry
  - Online www.donotcall.gov
- Opt Out of credit card offers
  - Call (888)567-8688 or
  - Online at www.optoutprescreen.com

Appleton Police Dept. 920-832-5500