CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

SENIOR CYBERSECURITY CHEAT SHEET

① Senior Scams

Every year, seniors get scammed out of tens of billions of dollars, money they've spent their entire lives saving only to have it stolen. The cybercriminals see the elderly as a prime target for Internet scams because of a perceived vulnerability, and now because Internet use among seniors is on the rise.

② Common Scams

Cybercrime is the fastest growing crime internationally, and current estimates place that cost at $600 billion last year alone. With so many threats, it can be challenging to protect yourself.

Here are only a few of the rampant internet scams to watch out for:

Email Scams - used to steal sensitive information such as usernames, passwords, and credit card details for malicious purposes. These typically involve a scammer pretending to be someone else. The email looks real and will have a company's color scheme, logo, and design style. It may feature an offer that seems too good to be true. However, if you look closely at the domain, you'll notice it isn't real. It may originate from a domain like Ama.zon.com, for example. When you click a link in that email, you will end up on a website that may infect your computer with malicious threats. If you complete a purchase, on this fake website, they will steal your credit card.

Tax Scams and Banking Scams - Scammers send out emails that appear to be from your bank or other financial institution.

Common Scams (con't) ②

They generally claim that they need your account details to confirm a transaction or to investigate unusual activity. With access to your private data, they can now use your credit card to make purchases. Sometimes these are scams are carried out over the phone (IRS Scam.) A scammer calls and tells you that you owe money to the government and that you are facing jail time, and continue to harass you into paying it. They will encourage you to make payments through a wire transfer, prepaid debit card, or gift cards.

Security Software Scams - Security software scams send a pop-up message to your device stating that your privacy or security is compromised. They will often suggest you install some software to correct it. They might offer to do a cleanup for you. However, downloads from this pop-up install a virus onto your computer. After that you are directed to call the tech support phone number, where an agent takes over your computer. They pretend to find and clean up dozens of viruses and then sell you a security suite for hundreds of dollars. All of the software the agent installs on your computer was readily available online for free.

Continue reading on next page >

SENIOR CYBERSECURITY CHEAT SHEET

② Common Scams (con't.)

Lottery Scams - In this scam, you receive an email that tells you that you've won a significant but still believable amount of money. To obtain the funds, all you need to do is provide your bank account or credit card details. They need this so they can transfer the amount to you and then there is the small processing fee. Instead, the scammer accesses your accounts and withdraws funds. The email message will also tell you to respond quickly or risk missing out, and urge you to keep your winnings private or confidential, to 'maintain security.' Both major red flags!

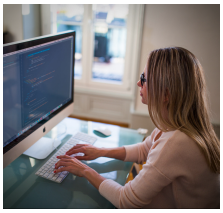
Romance/Catfishing Scams - A romance scam involves someone conning an individual by pretending to be their partner. The scammer will create a profile of a young person and reach out to other individuals. They will slowly talk to their victim, building trust, and a relationship. Eventually, they will ask for money for basic needs and other small things, slowly conning their victims out of their money.

Grandparent Scams - Grandparent scams are growing at an alarming rate. This scam specifically targets the elderly. Grandparents will receive a call or text message that is supposedly from their grandchild. In it, they desperately ask for help, saying they are in jail, at the hospital, or trapped somewhere dangerous. A scam like this is typically successful because it creates a sense of urgency. According to the FTC, individuals over the age of 70 have suffered the highest average losses to it.

Common Scams (con't) ②

Sextortion Scams - These involve an individual getting blackmailed into paying a ransom. A common theme is that grandpa visited an adult-themed website filled with malware. A keylogger and remote desktop program were installed on his computer while he's browsing the content. The keylogger will log his passwords, while the remote desktop program recorded everything he looked at, as well as him if he has a webcam. The scammer then uses the pictures, videos, and passwords they've collected to blackmail their victim into paying a ransom.

Be Cyberaware ③



These scams only scratch the surface, so the simplest way to keep yourself safe on the internet is to ignore any email you were not expecting and to only interact with people you know and trust, especially on social media. Remember, it's complicated for you to "accidentally" break the law online, so do not be fooled if someone says you've done something wrong, failed to pay a fine, or another similar story.

SENIOR CYBERSECURITY CHEAT SHEET

(CONTINUED)

④ Avoiding Scams

Because email is so critical in today's business world, organizations have established policies around how to handle this information flow.

Avoiding Email Scams - Verify the identity of the person sending you the email. If the email address and credentials check out but you're still suspicious, contact the person or company about the email before following through.

Tax Scams and Banking Scams - Never verify your identifying information to someone who contacts you, regardless of how they reached out to you. Neither your bank nor the IRS will never contact you like that. A quick call to them will confirm if these debts exist.

Security Software Scam - Never click a popup box that tells you your computer is infected. First, stay safe by downloading a robust antivirus security suite and keep it updated. Should you accidentally stumble upon a popup box by mistake, exit out and ignore it, then run a virus scan using your own installed software.

Lottery Scams - Remember that you can't win a lottery that you never entered. Ignore these emails and never send sensitive information or bank account details to a stranger.

Romancing/Catfishing Scams - If it seems too good to be true, it probably is. There are several warning signs to look out for:
If your partner refuses to talk on the phone, or won't take pictures.

Avoiding Scams (con't.) ④

- The relationship gets very serious, too fast.
- They start asking for money.
- Their social media profiles are bare, or newly created.
- Everything begins with an excuse.

It isn't always easy to spot romance scams. They often play out like real relationships. The number one defense is common sense.

Grandparent Scams Look for:
First: See what payment method the caller requests. Western Union, a gift card, or a wire transfer are red flags.
Then: Ask an identifying question that your grandchild would know.

Sextortion Scams - To prevent this scam, stay off porn sites. Install an update-to-date antivirus program that detects malware and can prevent it from infecting your computer.

Continue reading on next page >

SENIOR CYBERSECURITY CHEAT SHEET

⑤ Is That Website Legitimate?

Ensure that every website you interact with is legitimate and there are a few simple steps to follow. When you go to a website, make sure it has an HTTPS tag in the name at the top of your screen. It indicates that the site has SSL encryption which protects your data during transit and is vital if you are conducting any financial transactions. It is generally missing on untrustworthy sites. A safe website will also display a green padlock icon to the left of the website's URL. You can click on it to verify its security details. Finally, check the spelling of the web address. Fake websites often change a tiny detail to look like a different website. Sometimes it could be as simple as replacing 'o' with '0,' but you only see it if you're paying attention.

⑥ Protect your Identity

One way to protect your identity is to ensure that your system is safe from any external attacks like viruses. You also need to learn to spot the common scams and be skeptical of any message you receive online. Finally, keep a close watch on all your online accounts. Monitor your credit report and see if any new credit cards, loans, or other transactions made in your name. If you notice any suspicious activity, you can freeze your credit report and dispute the false transactions.

(CONTINUED)

Secure Online Shopping ⑦

Online shopping has made it convenient to get everything from clothes to basic grocery delivered right to your doorstep. However, it's essential that you only shop from sources that you trust and websites that are familiar to you.

- Always check the reputation and reviews of any online store before you use their services. A simple Google search provides you with many reports about users' experiences.
- Make sure you read their FAQs and Terms of Service to ensure they use sound policies.
- A legitimate website will always have SSL encryption. When you're checking out, make sure the required information is reasonable and necessary.
- No online store will need your Social Security number or your birthday to make a sale.
- It's also safest to use a credit card because you can file a claim if the website was fraudulent.
- If you shop online regularly, check your online statements to ensure that no false charges appear.
- When possible, only purchase using your home WiFi to avoid typing private information over a public network.

Continue reading on next page >

SENIOR CYBERSECURITY CHEAT SHEET

⑧ Banking Securely

Banks and financial institutions maintain high standards when it comes to protecting your financial data. However, there are several things you can do to ensure the security of your money.

- Use a private home network when banking. Who can see your data over public wifi? It's hard to know.
- If you can't avoid online banking while away from your network, sign up for a mobile data plan or set up a virtual private network (VPN).
- Use two-factor authentication. This additional layer of security sends a code to your mobile phone that you need to enter with your username and password before you can log in. If any outsider gains access to your login credentials, two-factor authentication will prevent them from gaining access to your accounts.
- Change your passwords regularly. Some data breaches involve old login credentials. If you change your password, a hacker won't be able to access your account with outdated information.
- Use a password manager like 1Password to store these details safely, while still changing them regularly.
- Avoid phishing emails that appear to come from your bank. As a rule, banks never call or email to confirm your details or passwords. If you receive a message, call the bank and confirm before you hand over sensitive information. If you have any questions regarding online bank security or or email to confirm your details or passwords. If you receive a message, call the bank and

(CONTINUED)

Banking Securely ⑧

confirm before you hand over sensitive information. If you have any questions regarding online bank security or want to know what extra steps you can take, contact the bank directly and ask their advice. They generally have customer service representatives trained to help you transact safely online.

Cyberawareness Social Media ⑨

The internet can be an excellent way to find friends, keep in touch with family, and be an active part of the community. Keep a few things in mind:

Everything you post is permanent. You have the option to delete a post. However, it stays on the server. There is a good chance someone saw it, or it was saved by someone already.

Be careful of what information you share. All information publicly shared can be used by others.

Make sure you know everyone you accept into your social network. Avoid accepting friend requests from people you've never met. They may have malicious intentions.

Use caution when you click links. Any third-party links, even those shared by your friends and family, could land you on a dangerous website. Sometimes just clicking a link, forwards that link as a message to everyone

Continue reading on next page >

SENIOR CYBERSECURITY CHEAT SHEET

⑨ Social Media (con't)

in your social network. It can not only be annoying but can also compromise the security of everyone in your circle.

Never let the website scan your email address book. Marketers or Criminals might use this list to spam everyone in your network.

Never give money to someone you've met through a social network. Imposter scams cost victims millions of dollars per year, and the victims are routinely "groomed" by the scammer. Known as the friendship or romance scam, it may go on for months before the subject of money comes up, but it will inevitably happen. Never send someone money, or agree to accept payment on someone's behalf, or other similar situations.

Stay Safe Online ⑩

The best way to protect yourself online is to know what to expect. Take the time to understand some widespread threats and learn how to avoid them.

Remember these tips:

- Don't visit unsafe websites.
- Ignore any emails from unknown senders.
- Protect your private information.
- Keep your email out of the hands of predatory marketing companies.
- Keep your antivirus up to date.
- Don't keep your passwords saved in a document on your computer, and change them regularly.
- Perform routine virus scans.

When you know what to look for, avoiding danger is easier. By using good internet browsing habits and robust security software, you can browse safely, check in on your loved ones, and enjoy all the benefits of being connected..

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH