Internet & Cybersecurity Protection

One need not use the internet or a computer to become part of the digital world and cyber age. Is it possible to wipe your tracks? Yes, but not an easy thing to accomplish. It takes time and money to eliminate your electronic trail. You have a presence in the cyber world. Learn how to protect it.

More than ever, families are spending increasing amounts of time on the internet. With every social media account you sign up for, every picture or vacation destination you post, medical records you update, or banking transactions you complete, you share information about yourself with the world. You are in a unique position to help yourself and your loved ones against dangerous risks, including cyber intruders. When on-line:

1. **Think before you click.**
2. **Limit the information you post on social media from personal addresses to where you like to grab a cup of morning coffee. Many people don't realize these random and innocent details are all criminals need to target you, your loved ones, and your financial and physical belongings. Keep social security numbers, account numbers, and passwords safe, as well as specific information about yourself, such as full name, address, birthday, and even vacation plans.**
3. **Make sure your devices are accounted for and locked when not in use. Avoid sharing location, personal identifying information (PII), or sensitive information on social media platforms. There is no 'Delete' button on the internet. Share with care because**

even if you delete a post or photo within seconds after sharing it, chances are, someone saw it and may have documented it with a screenshot.

4. **If you or a loved one experience harassment or bullying online, document the evidence and work with your social media provider and local authorities. Block the individual. Do not respond to the person unless instructed to do so by the police.**
5. **Always check the legitimacy of websites and 'friend' requests before accepting or sharing personal messages. Cybercriminals use phishing tactics, hoping to fool their victims by impersonating individuals or companies. If you have any doubt about the validity of the sender, even if the details seem accurate or if an email looks unusual, do not respond, and do not click on any links or attachments in the message or site. When available, use the 'junk' or 'block' option. You need to be aware some spammers have several phone numbers and websites spitting out calls and messages. Even if you block a number or site, you may continue receiving spam. In addition, you have verified your number or email as being legitimate.**
6. **Encourage loved ones to check with you, a parent, guardian, or relative before they click links, open attachments or respond to unfamiliar messages.**
7. **To stay anonymous (or as close to it as possible), you need to give up your Windows or Mac operating system. Switch to a Linus distro. The best way to go is Tails: The Amnesic Incognito Live System.**
8. **To lessen tracking of sites you visit and searches you make, drop Google, Bing, Yahoo, etcetera, and use DuckDuckGo.**
9. **For the closest thing to anonymous email, check Proton Mail. It is reputed to be the best there is.**

10. **There is no 100% guarantee but consider installing a TOR software browser system. The United States National Security Agency (you know, the "No Such Agency" agency) refers to TOR as, "... the king of high-secure, low latency internet anonymity." For further explanation and information, go to www.torproject.org.**

Be smart on the internet at home, at school, at work, on mobile devices, and on the go.

Identity theft is one of the fastest-growing personal crimes. It can occur on or off the internet. A hack of your bank account, a lost credit card, someone overhearing your social security number and birth date, a lost driver's license—these are ways identity thieves become you. You need to stop them in their tracks.

It is in your best interest to follow all safety alerts and notifications your bank or financial institution provides. Install any anti-virus and firewalls your use on your desktop, laptop, or tablet on your smartphone. They are miniature computers and are susceptible to breaches as any.

Social engineering is when criminals try to use 'social skills' to try to compromise your personal security. Some ways to tell if an attempt is being made are:

- **Messages with an urgent plea for help. The message is a good clue it could be a hoax. For example, you may receive a message from a relative or a friend telling you they're in a bad situation. They need help, usually in the form of money.**

- **Messages with a seemingly legitimate backdrop. A scammer will send a message that seems to come from a legitimate company, financial institution, or school; it may even seem to come from a personal account of someone you know.**
- **They may present a problem and ask you to verify or provide information. In this scenario, the scammer includes a link that looks right and has all the correct logos and content but then asks you to verify passwords or credit card numbers.**
- **Notify you're a winner of a sweepstake or contest. You are not a winner – emails or calls with promises of prizes or recognition for contests you don't remember entering, or for being the millionth visitor, turn into the scammer needing your banking or routing information to send the money.**

Make personal cybersecurity a priority:

- **Own it. Be extra cautious of any emails, texts, or phone calls that encourage you to act quickly or ask for a payment, including pre-paid cards.**
- **Secure it. Avoid being tricked into proving your identity. Do not give away personal information such as passwords, PIN numbers, or your social security number.**
- **Protect it. If it sounds too good to be true, it is. We've all heard and read this before. So, why do people continue to get taken by scams? Protect yourself and do not click links in messages to enter personal information, reset passwords, or enter payment information unless you started the process.**

Identity theft, also known as impersonation fraud, is a growing problem worldwide. A stolen identity is difficult to prevent in its entirety with the explosion of personal information distributed daily over the internet, phones, and other mediums. Even if you're able to enact every conceivable protection known, any information you provide to legitimate sources is subject to hack by thieves or sale by insiders. It's a constant battle and you need to remain careful and vigilant to reduce the chance of becoming a victim.

Identity theft can occur in ways other than over the internet or by computer. If you lose your Social Security card, driver's license, bank statement, or a host of other documents or information, or if they are stolen, a person can obtain enough information to steal your identity. Keep credit and debit cards separate from identification cards, in particular, any which include your address. Never write PIN numbers and carry them with your cards or in your wallet. Leave the Social Security card at home in a secure location and once again, provide no one with information either over the internet, by phone, or face-to-face unless you make the contact.

Set up Two-Factor Authentication with your bank(s), any credit companies, and places you do business and exchange personal and financial information with. This system normally works with a person logging into a website account by entering their User ID and password as normal. When you set it up, the system will ask if you want to receive a call or have a text message sent to the phone number on record. You will receive a one-time code. Enter the code in the dialog box that will show on the computer or your phone there is a set time limit.

Another alternative is you receive a text on your mobile phone with a link to click on. After doing this, you're logged into your account.

Here are general tips to help you in your quest to maintain your information and keep it as confidential as can be:

Some ways criminals snatch your information include:

- **Buying information from sources who work at banks, credit bureaus, and etcetera.**
- **Going through trash (good idea to have a shredder for susceptible documents like bills and credit card statements).**
- **Hacking into an unsecured site on the internet you've provided information to.**
- **Stealing mail, purses, and wallets to obtain information.**
- **Posing as a legitimate individual who needs information from you, like a caller from your bank.**

To help you not become a victim:

- **Any unauthorized financial transactions you notice need to be reported immediately to the financial institution and police.**
- **Credit reports should be checked at least once per year. Any questionable remarks need to be reported in writing and followed up on until corrected.**
- **If you did not make the call, do not provide your credit or debit card information over the phone.**

- **Question, and question some more, anyone who asks for information.**
- **Maintain a list of phone numbers to tell banks and companies about any theft or loss of credit or debit cards.**
- **Keep your PIN numbers confidential (don't even share them with your dog. Sorry Fido).**
- **Ask credit bureaus to place a statement on your report if your identity has been stolen.**
- **Any person you know who receives credit card or bank statements in another person's name needs to be reported to authorities.**
- **You get notices of unpaid driving tickets you never received.**
- **You see unknown accounts on your credit report.**
- **The IRS blocks you from filing federal taxes because it says you already filed for this year—when you didn't.**
- **You get confirmation of changes to your physical or email address you didn't request.**
- **You receive either bills, medical insurance explanation of benefits statements, or dental insurance explanation of benefits statements for healthcare services you didn't receive.**
- **You're told that you maxed out a particular medical or dental insurance benefit when you know that you didn't.**
- **Your cellphone unexpectedly loses service.**
- **Law enforcement shows you a warrant for your arrest for a crime you didn't commit.**

If your identity is stolen:

- **Act quickly. As soon as you become aware someone has assumed your identity, you need to make notifications.**
- **Call the security department of creditors and financial institutions. Close the accounts and develop different passwords for any new accounts.**
- **Call Equifax, Trans Union, and Experian. Insist they place a fraud alert in your file.**

Request no new credit be issued without direct approval from you. These are the numbers for their fraud departments:

Equifax — 800 525-6285

Trans Union — 800 680-7289

Experian — 888 397-3742

- **Call your local law enforcement and file a report.**
- **Call the Federal Trade Commission at 877 438-4338 and file a report with them.**

To help reduce the multitude of threats with wireless networks, you should:

- **Install a firewall on your wireless modem.**
- **Protect your Service Set Identifier. Avoid publicizing your SSID (this is the name of a network). Research whether you can change the default number.**

- **Restrict access. The only ones who should have use of your network are trusted family members and friends. Allow or restrict media access control by filtering media access control addresses.**
- **Maintain anti-virus software. Install and update anti-virus software. I use Norton®.**
- **Encrypt data. This prevents a person who might access your network from seeing data.**
- **Change default passwords. This should be self-explanatory, but network devices come with preset passwords. Change them.**

Kids are prime targets for identity thieves because they have no credit histories and no one is checking. I will save this specific subject matter for a future Blog – *Cyber Security & Children.*

Stop.Think.Connect is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone. The Campaign provides free resources available to everyone that are tailored to multiple demographics, including small businesses, students, educators, parents, and many others.


CERTIFICATE OF COMPLETION
This is to certify that
John Yonitch
has completed
Cybersecurity Awareness
Erika Ragonese
Director, CDSE
Verification Code
9uJs6CLHVL