THREATS TO IDENTITY

In Case of Identify Theft

- Notify your bank & credit card companies.
- Report ID Theft to www.FTC.gov.
- File a Police report.
- Change all passwords including on social media.
- Let friends and family know in case the criminal now has access to your emails and social media accounts.

What to Lock Down

- Any Personal Identifiable Information (PII).
- Your credit report.
- Your child's credit report.
- Your social media accounts (use the Smartcards to lock accounts down).

Actions for the Physical World

- Be aware of your surroundings.
- Invest in a safe for the home.
- Shred documents, bills, and any mail.
- Don’t give out your SSN.
- Be mindful of shoulder surfers (whether on your phone, computer, at an ATM, etc.)
- Look out for credit card skimmers at ATMs and gas pumps.
- Use a locked mailbox.
- Check financial statements frequently.
- Read medical statements.
- Use credit cards instead of debit cards.
- Sign the back of credit and debit cards.

Actions for the Cyber Domain

- Use Two Factor Authentication whenever it’s an option.
- Update your devices' virus protection and your passwords.
- Clear cookies and browser history frequently.
- Update, Update, Update!!! Make sure to allow your device to update to ensure you have the most up-to-date security features.
- Make sure you backup all your devices.
- Encrypt your emails.
- Never save credit or debit card information to devices, apps, or accounts for quick and easy checkout.
- Verify the source of your emails and check the links. Legitimate business emails will not ask for your PII, password, or account number.
- Don't accept friend requests from strangers.
- Start using a VPN if you aren’t already using one.

Note: Be sure to check out https://haveibeenpwned.com. Use your own email address to see if your personal data has been compromised in any data breach. Not all data breaches are included on this website, but it is a great start to managing your identity.

THREATS TO IDENTITY

- When buying a new car, don't leave the paperwork in the glove compartment or elsewhere in the car. Criminals who break into cars can use that information to steal your identity, not just your car.
- Consider posting travel (vacation) photos and information after you return from your trip so that criminals don't know you are away and your house is empty.
- If you are buying or selling something online and it seems too good to be true, chances are it is. A simple Google search might end up saving you a lot of time and hard-earned money.
- Consider turning off your wifi as soon as you get into your car to leave your house.
- Consider how many people have access to public wifi, then consider only using privately secured wifi.
- Consider an open-phone policy with your children so you can access their phone any time and without notice. Remember if you are “friends” with your kids online that’s only half the battle, it’s important to check on their accounts to see who and what they are talking about.
- It's always great to donate but consider verifying the authenticity of a charity and/or website first. Perhaps visiting an official website or calling the official number.
- Gamers: Consider who you are communicating and sharing information with and perhaps limit online gaming interactions to only people you have met face-to-face.
- Consider logging off your email and social media accounts when you are not using them, especially on your computer. Doing so will limit the access if an intruder gets access to your computer, either through physical access or by hacking in.

Useful Resources and Links

https://www.identityforce.com/blog
https://www.commonsensemedia.org/privacy-and-internet-safety
https://www.ftc.gov/
https://identity.utexas.edu/
https://www.getsafeonline.org/
https://staysafeonline.org/
https://www.idtheftcenter.org/
https://www.irs.gov/
https://www.usa.gov/identity-theft
https://www.consumer.gov
https://www.transunion.com