Monthly Cybersecurity Tips Newsletter
October 2022 VOLUME 17, ISSUE 10 • 2022

Protect Your Identity This Cybersecurity Awareness Month

From the desk of Karen Sorady, VP for MS-ISAC Member Engagement

When you log on to a website, make an online payment, send an email, use a social network, post online, or even send a text, you're adding to your online identity. In today's world, it is unavoidable. The good news is there are ways you can protect yourself.

When logging on to a website, look at the address bar on the browser. If you see a padlock icon on the left-hand side of the address, the site is using encryption and verification. Clicking on the padlock shows the site's security certificate. Using only these types of sites ensures you are safely sharing your data. If you do not see the padlock icon, steer clear. Your data is vulnerable. When shopping online, visit only legitimate websites and use safe online payment options and digital wallets for a more secure checkout.

Be wary of suspicious emails or texts and never give out information unless you are certain where it is going and how it will be used. Do not open suspicious attachments. If you suspect a piece of communication is malicious, call the sender or company directly instead of replying to the email or clicking on a potentially malicious link or attachment.

Never throw away or give an unwanted device to someone else without factory resetting it and wiping all data from the device.

Bad actors can use your personal data in a variety of ways that can cause great harm. Identify theft is when a person or entity uses your information including your name, contact information, financial accounts, Social Security Number, and other personal information without permission. They can use this information to change your billing address, steal government benefits, open a bank account, apply for loans or lines of credit, use your money to make purchases online, or even commit crimes.

Doxxing is when an unauthorized person or entity collects and publishes personal information including private photos, messages, or other personal data for the purpose of harassing the victim. This is a different kind of identity theft that can jeopardize your safety and right to privacy. Keep your social profiles private and only connect with people you know. Check your privacy settings periodically and disable location tracking for applications installed on your device.

When using Wi-Fi in a public space, follow these safe use guidelines:

- Turn off auto-connect features on your phone or laptop to control which networks you connect to,
- Use a VPN to encrypt your data whenever possible,
- Don’t access personal or financial information,
- Don’t shop online,
- Don’t stay permanently signed into accounts,
- Pay attention to warnings, and
- Don’t leave your device unattended in a public place.

You can further protect your online identity by practicing good cyber hygiene.

It is important to choose strong passwords for your online accounts and home network. Create a strong password by combining upper- and lower-case letters, numbers, and symbols. Using a phrase known only to you can help you to remember a lengthy password. Do not use the same password or form of password on multiple accounts. Also, update them every few months. Keeping your devices up to date with the latest operating systems and security patches will help support

password strength. If you fill out security questions as a step in resetting a password, make sure they are challenging questions for which only you know the answer.

Use multi-factor authentication. MFA requires multiple factors to verify a user's identity, combining things you "know," like a password or pin, with things you "have," like a special code sent to your smartphone, or things you "are," like a fingerprint or facial recognition technology.

Creating strong passwords alone may not be enough. Password manager applications can ensure that your passwords are strong, unique, and updated regularly.

Reduce your digital footprint by deactivating/deleting old shopping, social media, and email accounts as well as unsubscribing from mailing lists that are no longer of interest.

Though bad actors are serious about their business and constantly finding new ways to get personal data, you can reduce your odds that you will become one of their victims by maintaining your security awareness and cyber hygiene.