Cyber Hygiene: Top 5 Ways to Be Cyber Smart

Technology has become an increasingly integral part of our everyday lives—it gives us invaluable tools for productivity and helps us be more efficient and connected than ever. Unfortunately, the very aspects of technology that make it so appealing and helpful can also make the digital world a gold mine for threat actors. With that in mind, **our focus for Week 1 of Cybersecurity Awareness Month (Be Cyber Smart) is cyber hygiene**.

What is cyber hygiene?

Cyber hygiene can be thought of in much the same way as personal hygiene—it's about training yourself to think proactively about your cybersecurity, just as you do with personal wellness. Except, instead of shampoo and toothpaste, **cyber hygiene uses tools like strong passwords, multi-factor authentication, data backup, and software and firmware updates to secure your personal information and make sure you're ready to safely connect with the digital world**. Making sure you check the boxes next to these cybersecurity best practices is the best way you can #BeCyberSmart!

Create Strong Passwords

One of the best ways to protect information is to ensure that only authorized people have access to it, and passwords are the most common means of authentication. Passwords only work, though, if they are complex and confidential. **Boosting password security is foundational to good cyber hygiene and significantly improves your ability to avoid a data breach.** Best practices for creating and maintaining strong passwords include:

- Avoid passwords based on personal information or dictionary words
- Use the most complex password a platform will allow
- Use unique passwords for each platform
- Adopt a password manager to simplify password management and ensure secure storage

Use Multi-Factor Authentication

Multi-factor authentication (MFA) is a cybersecurity best practice that offers an additional layer of protection by requiring two of the following three types of credentials: **something you know** (like a password or PIN), **something you have** (like a token or ID card), and **something you are** (like a facial scan or fingerprint). Biometrics, like facial or fingerprint recognition, make it harder for hackers to gain access to your device and personal information.

Install Reputable Antivirus Software

Since our topic is cyber hygiene, we'd be remiss if we didn't discuss viruses and antivirus software. A computer virus is like a cold. It's designed to spread from one device to the next, spreading malicious codes and programs that can make your computer "sick" and give threat actors access to your devices. **Antivirus software is used to prevent, scan for, detect, and remove computer viruses and malware.** It's an essential part of your cyber hygiene practices

Stay on Top of Software and Firmware Updates

Keeping your apps, web browsers, and operating systems (OS) updated is a key component of cyber hygiene because **updates help ensure you're utilizing versions that have eliminated or patched possible vulnerabilities**. Software developers issue security patches any time they discover flaws that could let in viruses or hackers.

Back Up Your Data

Help secure your files by keeping copies of important documents. This way, if you are the victim of ransomware or other cyber threat, you will have access to and can restore your data from a backup. **Use the 3-2- 1 rule as a guide to backing up your data**: keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite.

Cyber Hygiene Resources:

- National Cybersecurity Alliance, *Own Your Role in Cybersecurity: Start with the Basics*: https://staysafeonline.org/wp-content/uploads/2020/04/Own-Your-Role-in-Cybersecurity_-Start-with-the-Basics-.pdf
- CISA Security Tip ST04-003, *Good Security Habits*: https://us-cert.cisa.gov/ncas/tips/ST04-003