Good Cyber Hygiene Habits

Keep your information safe

What is cyber hygiene?

Cyber hygiene is a useful metaphor for making informed decisions when using smart devices. It highlights the importance of proactively managing your cyber security to combat online threats. Cyber hygiene is about training yourself to think proactively about your cyber security, much like you do with your daily personal hygiene.

The concept of cyber hygiene includes three basic principles:

1. Using products and tools that meet your hygiene needs
2. Performing hygienic tasks correctly
3. Establishing a routine

Think about useful practices

Use the right tools for cyber hygiene

Imagine trying to brush your teeth without a toothbrush. Maintaining personal hygiene would be challenging, if not impossible, without the right tools. The same principle applies to cyber hygiene. Without proper products and tools, your personal information could be at risk.

Reputable antivirus and malware software, a network firewall, and strong password protection play crucial roles in safeguarding personal data. Together, these tools can enhance your confidence in the security of your home computer, laptop, smartphone, and other devices.

Be thorough and accurate with cyber hygiene

Regularly maintaining and securing your computer files is comparable to flossing your teeth for dental hygiene. Similarly to not flossing as frequently as the dentist orders, many users overlook the need to properly delete files on their computers. Did you know simply emptying the trash or recycling bin does not guarantee that sensitive data is gone?

To ensure sensitive data is truly deleted make sure to use data-wiping software. Get in the habit of regularly clearing out your data you no longer need and wiping it clean from your computer's hard drive.

Another critical aspect of security is password management. Be sure to create strong, unique passwords that are not reused or shared. Passwords should be unique and complex, containing at least twelve characters along with numbers, symbols, and capital and lowercase letters. Update passwords regularly to boost your cyber hygiene.

Make cyber hygiene part of your routine

Learning to consistently monitor your cyber security can increase your odds of avoiding online threats. Like any habit, cyber hygiene requires routine and repetition.

Begin your path to great cyber hygiene by setting reminders or marking your calendar to complete tasks, such as updating devices, running virus scans, checking for security patches, clearing your hard drive, and updating passwords.

Key steps for good cyber hygiene

Maintaining good cyber hygiene is a general practice that enhances your online safety and security. To optimize your cyber hygiene, here are nine essential steps to follow.

Step 1: Install reputable antivirus and malware software

Antivirus software is a critical component of your overall cyber hygiene in its protection against security breaches and other threats. Antivirus software performs essential functions, including:

- Identifying specific files to detect computer viruses, malicious software, or malware
- Scheduling and conducting automated scans
- Scanning individual files, entire computers, or external drives as needed
- Removing malicious codes and software
- Verifying the health status of your computer and other devices

Step 2: Use network firewalls

Incorporating a network firewall is another crucial practice for upholding good cyber hygiene. Firewalls serve as an initial defense in network security by blocking unauthorized users from accessing websites, mail services, and other web-accessible sources of information.

Step 3: Update software regularly

Regularly update your applications, web browsers, and operating systems to ensure you are using the most current versions that have resolved or patched potential vulnerabilities. To avoid alerting hackers, developers may not always notify users when a critical patch has been implemented. Enabling automatic updates will ensure you always have the latest protections in place.

Step 4: Set strong passwords

Setting strong passwords for all of your devices is essential. Changing your passwords regularly will help prevent hackers from figuring them out.

Firmware passwords are another layer of device security by helping to prevent others from using your computer. Firmware passwords protect your hardware by preventing your device from being restarted or reset without entering the password.

Step 5: Use multi-factor authentication

Two-factor or multi-factor authentication is a recommended approach that adds an additional layer of security. Two-factor authentication typically involves entering your password and username, along with a unique code that is sent to your mobile device. Multi-factor authentication enhances security further by incorporating biometrics, such as facial or fingerprint recognition. This makes it more challenging for hackers to access your device and steal personal information.

Step 6: Employ device encryption

Some companies automatically implement data encryption processes. You should also consider encrypting your own laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage that contain personal or private information.

Step 7: Back up regularly

Secure files by backing up important data offline, on an external hard drive, or in the cloud. This practice helps protect against various types of data loss, especially if hackers compromise your device.

Step 8: Keep your hard drive clean

When selling a laptop, tablet, or smartphone, it is important to ensure your personal or sensitive information is not transferred to the new owner. Simply deleting files or data may not suffice. As a part of good cyber hygiene, any devices being sold should be reformatted and the hard drive should be wiped clean.

Step 9: Secure your router

Protect your wireless network. This includes changing the default name and password that came with the router, disabling remote management, and logging out after set up. Additionally, make sure your router supports WPA2 or WPA3 encryption to maintain the highest level of protection for the information being sent over the network.

Remember, it is smart to practice good cyber hygiene habits. If you use the right tools, be thorough and accurate, and make cyber hygiene a part of your routine, you will be on your way to creating habits that will help keep you safe and secure online.