EMERALD CREDIT UNION

Achieving Essential Cyber Hygiene for 2025

Technology continues to evolve rapidly, bringing the convenience of online services and the power of artificial intelligence (AI). It also opens new doors for malicious online actors. Hackers, data breaches, and malware have become common, unwanted visitors in our lives.

According to Zscaler's annual phishing report, phishing attacks, or fraudulent emails sent to gain your personal information and money, surged by nearly 60% in 2023. In recognition of Cybersecurity Month, we're sharing best practices for safeguarding your personal data and ensuring you step into 2025 with enhanced protection and peace of mind.

What's the Risk?

Our online activities often leave behind data trails that can be used to track our behavior and access our personal information. These activities include credit card transactions, online shopping, browsing history, messaging, phone records, GPS usage, and more. Numerous companies and individuals seek to collect and exploit this data for purposes like marketing, research, and customer segmentation. Others have malicious intentions, such as using your data for phishing, accessing financial information, or hacking into online accounts.

How to Protect Yourself

Cybersecurity may seem daunting, but dedicating just one hour each week to improving your cyber hygiene can make a substantial difference. Here are some essential practices that will enhance your online security immediately:

Avoid mobile/online banking on unsecure or public Wi-Fi networks. Public Wi-Fi networks are often not secure, making it easier for hackers to intercept your data. Don't make financial transactions on your mobile device when in restaurants, hotels, or other public places that offer free Wi-Fi, even if they provide a password. Wait until you are on a safe and private network, like your home.

Be cautious with unexpected emails. Do not click on links or attachments in emails you were not expecting. Phishing attacks often come in seemingly legitimate emails that trick you into revealing personal information or downloading malware.

Use a password manager. A password manager enables you to use a different password for every online login, which is an essential security practice. Password managers can autogenerate complex passwords for you and store them on encrypted servers, so you won't have to memorize them. Do your research to find the right one for you, but there are many free options available.

Use a Virtual Private Network (VPN). A VPN allows you to privatize your network and IP address, adding an extra layer of security to your online activities. You can set up a VPN for your home network, and some even offer mobile plans too.

Make sure your software is up to date. Ensure that all your software, including your operating system, browsers, and apps, is up to date. Updates often include patches for security vulnerabilities that hackers can exploit.

Enable Two-Factor Authentication (2FA). Enable 2FA on your online accounts whenever possible. This adds an extra layer of security by requiring a second form of verification in addition to your password, such as sending a code via text message or email to log into your accounts.

Alerts and notifications. We allow you to set up mobile alerts for your account activity. This can help you quickly identify and respond to any unauthorized transactions. Mobile alerts can be found within the Self Service tab of our Digital Branch.

By following these guidelines and using the resources provided, you can significantly reduce your risk of being hacked. Consistent and mindful practices are crucial to mounting a robust defense against cybertheft. **Remember that Emerald Credit Union will never contact you via email, text message, or phone call requesting personal identification or account information.**