Security Tips Newsletter

December 2024 | Issue No. 16

Security is Everyone's Responsibility

Being Cyber Safe in 2025

Summary

Security is everyone's responsibility, but that doesn't mean you must have several cybersecurity degrees to protect your personal and financial assets. In this issue, we list some easy ways to reduce your risk and be cyber safe in 2025

Here's What you Can Do

Turn on Multifactor Authentication. Your accounts will be significantly less likely to get hacked if they're protected with Multifactor authentication (MFA). This layered approach to securing data and applications requires two or more credentials to verify your identity for login. MFA increases security because even if the hacker has one credential – such as your name – that unauthorized user won't be able to meet the second authentication requirement, so can't access the targeted physical space, computing device, network, or database

Update Your Software. Bad actors exploit flaws in computer systems. Network defenders are working hard to fix them quickly, but their work relies on all of us updating our software with their latest fixes. So, update the operating system on your mobile phones, tablets, and laptops. And update your applications – especially the web browsers – on all your devices too. Leverage automatic updates for all devices, applications, and operating systems as well. You may be too busy to install every update, but your PC or other electronic devices won't be if you activate automatic update settings.

Think Before You Click. Take a little time before you click that link or open that attachment. More than 90% of successful cyber-attacks start with a phishing email. Sadly, we are more likely to fall for phishing than we think – and false urgency and fake links are often the cause.

*False urgency***.**An email from your gas company says your service will be canceled unless you re-enter your card details right now. Or maybe your phone provider says you've been hacked and need to contact them ASAP. But should you? Slow down, and don't be alarmed about that urgent email. Carefully look at the subject line or preview the content of the

email. If the email provides the name of the business and asks for a response, locate its contact information elsewhere – such as its website – and use it to see if it's really that urgent.

*Fake links***.** Have you ever seen a link in a text or email that looks a little … *off*? Sure, it looks like something you've seen before and the sender is familiar – maybe your email service, your boss, your bank, or a friend. But when you click the link, you're asked to change or enter a password or verify personal information. Don't. It's likely a phishing scheme using a link or webpage that looks legitimate but was designed by bad actors to install malware on your machine or get your password, social security number, credit card number, or other sensitive information. Once they have that information, they can use it on legitimate sites. If it's a link you don't recognize, trust your instincts and think before you click.

Use Strong Passwords. Did you know the most common password is "password"? Followed by "123456"? Your child's name and birthday isn't much better. Using an easy password is like locking your door but hanging the key on the doorknob. Anyone can get in. Using strong passwords and, ideally, a password manager is much safer.

Here are some tips for creating a stronger password.

- Make it long – at least 16 characters
- Don't use the same password on multiple sites
- Use randomly generated passwords created by a computer or password manager. They're better than humans at being random

You can use a password manager to store all your passwords, too. That way you don't have to remember them all! If you go this route, make sure the password you use for the password manager is strong and memorable, and secure your account with MFA!

What to Do If You Are Scammed

- If you feel that someone is scamming you, don't respond to the email, and block it. If it's a phone call – hang up!
- If you provide your personal information (account, date of birth, online banking user ID, password, etc.) contact All One Credit Union immediately.

If You're a Victim

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

If you identify suspicious activity involving All One Credit Union, contact us immediately.