Cybersecurity Reminders

FOR PERSONAL DEVICES & AT HOME

PENFED CREDIT UNION

Have you ever heard the saying, "Safety Begins at Home"?

It's true, especially in the context of the internet. Once a hacker gets access to an unprotected home network, they're pretty much free to do what they want. Malware campaigns, data and identity theft, and botnets are just a few of the possible ways a hacker can exploit a vulnerable home network. This is why setting up a secure home network should be a number one priority for everyone.

These days, more and more of our home devices are connected to the internet. Each device we add increases our security needs. Follow these tips to keep your home network secure.

Secure your Wi-Fi network. Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username. If you have multiple devices, do not use the same password.

- **Enable two-factor authentication.** Always enable two-factor authentication on your email, social media and online banking. Stronger authentication helps verify that a user has authorized access to an online account.

- **Keep your PC or mobile device up to date.** Install updates for your apps and operating system as soon as they become available.

- **Know your apps.** Be sure to review an app before downloading and installing it. Check to make sure that the app vendor or developer is reputable.

- **Be aware that apps may request access to your location and personal information.** Only allow access if it makes sense to the functionality of the app.

- **Consider what you share.** Limit the amount of personal data you share online. Your full name, address, school or work locations, and other sensitive information should not be published widely.

- **Disable geo-tagging on posts and in pictures.** This feature lets people online know where you are—including criminals. Why advertise that nobody is home?

- **Limit your online social networks to the people you actually know in real life.** Criminals spend hours online under aliases trying to defraud people out of information. Remember, if you limit your social networking information to only friends, adding one of these bad actors gives them access to it.