Welcome to the SeaComm Federal Credit Union podcast, your guide to financial information and what's going on at your credit union.

October 2018 was the 15th annual National Cyber Security awareness month, a collaborative effort between the U.S. Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) to ensure every American has the resources they need to stay safer and more secure online.

It's everyone's job to ensure online safety at work and at home.

The lines between our work and daily lives are becoming increasingly blurred, and it is more important than ever to be certain that smart cybersecurity practices carry over between the two. When you are on the job – whether it's at a corporate office, local restaurant, healthcare provider, academic institution or government agency —your organization's online security is a shared responsibility. A culture of cybersecurity in your organization includes all employees and smart cybersecurity practices should carry-over to your home online activities, as well.

Here are some tips from the National Cyber Security Alliance, the leading neutral nonprofit, public-private partnership devoted to educating and empowering our global digital society to use the internet safely and securely. These tips can make you safer and more secure at work and at home.

1. Keep a Clean Machine

Having the latest security software, web browser, apps and operating system is the best defense against viruses, malware and other online threats. Remember, mobile phones, point of sale systems if you own a business and tablets need updating too!

2. Always Back It Up

Put in place a system – either in the cloud or via separate hard drive storage – that makes electronic copies of the vital business information on a regular basis. At home, make regular backups of all your important documents, files and photos.

3. When in Doubt, Throw it Out

Whether at work or in personal lives, everyone should know not to open suspicious links in email, tweets, posts, online ads, messages or attachments – even if they know the source.

4. Lock Down Your Login

Enable the strongest authentication tools available for your online business accounts, such as biometrics or a unique one-time code through an app on your mobile device. This security feature is also available on personal accounts such as email, credit union and social media.

Cybersecurity in the workplace and at home is everyone's business. It's not just the job of the IT staff or business owner to ensure online safety at work. Creating a culture of cybersecurity includes everyone knowing how to protect themselves and the organization or business they work for.

For more information go to staysafeonline.org/ncsam.

That's it for this edition of the SeaComm Federal Credit Union podcast. Thanks for joining us!