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

October is National Cyber Security Awareness Month so let's talk about smartphone security.

Your smartphone is probably the most widely used electronic device you own. With a wealth of features, social networking, and time-saving apps, smartphones have become an essential part of our daily routine.

Whether you are organizing your work schedule, ordering food, or keeping track of your fitness, a secure cell phone provides peace of mind that your personal data will not end up in the hands of crooks who could use it to do you financial harm.

We store and share a lot of sensitive and personal data on our phones – messages, pictures, videos, login credentials, passwords, and more. Whether you become a victim of a hack or simply lose your device, there is a lot at stake should your phone data get compromised.

So always make sure your screen is locked. There are several valid smartphone lock methods, and you can even use apps to lock your phone, so even if it's just a PIN, always lock your phone!

Also, keep your phone software updated. Smartphone security relies on constant updates to keep ahead of the hackers, so don't turn those automatic updates off. If you want to stay on top of things, make sure to actively keep track of operating systems upgrades in order to avoid a variety of potential smartphone security issues that stem from outdated software on your phone.

Be sure to create strong passwords. I've said this numerous times. Try using passwords that start with a capital letter, and include symbols and numbers. For even more security, you could try acronyms or even using a smartphone password manager.

And, of course, don't reuse passwords!

Don't save personal logins and payment details on your phone. Don't trade security for convenience by leaving major information stored on your phone, it could come back to haunt you if your phone is lost or stolen. And always be sure to always log out of secure sites when you're done.

Never click on links in text messages unless you are completely and absolutely sure it's legitimate. A bad link can contaminate your phone with malware or send you to a phishing site.

Download apps only from secure sources. Both Google and Apple have strict rules on what apps are allowed at their stores for a reason – many internet phone apps contain malware and exploits that are designed to steal personal data from your phone.

Install an antivirus solution on your mobile phone. There are many cell phone security apps for Android, iOS, and Windows mobile devices. You should use one for extra security.

Be careful when connecting to public Wi-Fi hotspots and unprotected sources of free internet. VPNs – virtual private networks – are an excellent solution. They work by connecting to an external server and masking your IP to hide your device's true location.

A surprising number of people don't realize the dangers of Bluetooth. While this handy device-pairing protocol can save you a lot of hassle in transferring files or connecting devices wirelessly, it can also be an easy way for hackers to get into your phone if you do not use it responsibly.

Make sure to keep your device from being discoverable and always turn off Bluetooth when you are not using it.

Always be thinking smartphone security, there is no guaranteed solution but the harder you make it for hackers, the less likely you will be victimized.

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