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

Do you use a mobile device? Just about everybody does, I guess. Is it filled with personal information, such as contacts, email messages or other sensitive information? Do you use it to access your accounts here at SeaComm through mobile branch? Losing it, having it accessed without permission, or finding out it's infested with malware can be a big problem. Here are some tips to protect your devices and the information on them.

First of all, keep your device secure. Don't let it out of your sight when in public places, don't leave it unattended and make sure it's set to auto-lock after a certain amount of time without use.

Don't download apps that are not in the official app stores. Do some research on the apps you want, read the reviews, and only use the official stores to get those products. You'll have a lower chance of getting something nasty that steals your mobile branch login credentials, puts ransomware on the device, or just renders it useless.

Protect your device with a strong alphanumeric pass code. A typical four to six digit pin can easily be cracked in seconds; while a strong nine or more character alphanumeric pass code could take years, or even decades to crack. Combining lower-case letters, upper-case letters, numbers, and special characters increases the strength of the pass code exponentially. This ensures that all of the user's personal information and data contained on the phone or device are encrypted and almost impossible to access if the device is compromised. Your device should have a wipe function. If it's lost or stolen, all the data on it can be eradicated remotely and it should be set to erase all of the device's data automatically after a set number of password attempts. This will discourage hackers

Avoid using public Wi-Fi and Bluetooth, even if they are password protected. For transactions that may involve sensitive data, use the cellular data connection on the device, or wait until you can access a secure network like work or home. Also, disable the Bluetooth function if you don't need it.

Be sure to have the proper security software on your device. Just make sure you do your due diligence to ensure it's legitimate and the right choice for your device. And of course, stick to downloading it from the official app store.

Always load the latest patches and software updates as soon as they are available. It will help alleviate any security vulnerabilities.

Your mobile device can make your life easier, just be sure it's as secure as possible.

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