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

Today we're talking about ransomware. Did you know that there were nearly 1000 ransomware attacks on government agencies, educational institutions and health care providers with losses of nearly $7.5 billion in 2019, and that's not counting all the individual computers victimized.

So, what is ransomware? Well, it's a type of malicious software that infects a computer and restricts the users' access to it until a ransom is paid to unlock it. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the user's systems have been locked or that the user's files have been encrypted. Users are then told that unless a ransom is paid, access is denied. The ransom demanded from individuals varies greatly but frequently is $200–$400 dollars and must be paid in virtual currency, such as Bitcoin.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge and if the user is part of a network, the entire network can be victimized.

Here are some tips to prevent ransomware attacks.

- The first one is back-up. That's right, use a recovery system.
- Make sure you back-up your data. Also, use robust anti-virus software to protect your system from ransomware.
- Keep all the software on your computer up-to-date.
- Trust no one. Literally. Any account can be compromised so don't click on links, unless you're sure. As I said before, many times that's how the ransomware gets on your computer.
- Be sure to enable the "Show file extensions" option in the Windows settings on your computer. This will make it much easier to spot potentially malicious files.
- If you do discover a rogue or unknown process on your machine, disconnect it immediately from the internet or other network connections, such as home Wi-Fi. This will help to prevent the infection from spreading.

But again, don't click on email attachments and don't go to websites that you're not sure of.

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