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

If the mere thought of your computer being hacked frightens you, you're not alone. And tech support scammers know how to exploit that fear to their own advantage. They work to scare you into believing your computer is compromised and then offer to "fix" the problem – for a fee. The Federal Trade Commission's Consumer Sentinel Network got nearly 143,000 reports about tech support scams in 2018. According to the FTC, These scams usually start with a phone call or a pop-up warning of a computer problem that gives a number to call. Scammers often claim to be Microsoft or Apple – they may even spoof caller ID to make it look like one of these companies really is calling. In another twist, they get people who actually do need computer help to call them by posting phony customer support numbers for well-known companies online.

They may open system folders or run scans that seem to show evidence of a problem. Then they ask for money for supposed repairs and things like bogus service contracts. In 2018, people reported losing $55 million to these scams. And while many people did not lose any money, those who did reported losing hundreds: the median individual reported loss was $400. Credit cards were the top method of payment people said they used, and that's good news – credit card companies can reverse fraudulent charges. But many others said the scammer convinced them to pay by giving the PIN numbers on the back of gift cards, often iTunes or Google Play cards. For most in this group, the money is simply gone. Tech support scams stand out for the disproportionate harm they may be causing older adults. People 60 and over were about five times more likely to report losing money to these scams than younger people. Money isn't the only thing people lose on this scam. By allowing scammers remote access to their computer, people hand over control. Scammers can then readily steal sensitive information or install spyware.

Now, here are some things you can do to avoid these scams:

- Do not click any links or call a number that pops up on your screen warning of a computer problem.
- Hang up on unexpected calls from anyone who claims to be tech support.
- Don't believe your caller ID – it can be easily spoofed.
- Never give control of your computer or share passwords with anyone who contacts you. Keep your security software up to date.
- If you need help, contact a computer technician that you trust. Don't just rely on an online search.

If you've been scammed, change any passwords you shared and scan your computer for malware. If you did give out your credit card number, let us know. Check your statement and contact us to reverse the charges for those bogus services. If you later get a call about a supposed refund, you can bet that's part two of the same scam – hang up.

And please share this information with the seniors in your life who spend time on their computers. You can report tech support scams to the FTC at ftc.gov/complaint. To learn more, visit ftc.gov/techsupportscams.

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