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

Have you heard the term vishing? Vishing is the fraudulent practice of making phone calls or leaving voicemails purporting to be from reputable companies in order to induce individuals to reveal personal information, like financial account information and credit card numbers.

Well, recently we were alerted that a member received a phone call from an individual claiming that they were part of the SeaComm fraud department. The intended victim was asked to confirm or deny a charge and then verify their card number and account information. The phone call appeared on caller ID as coming from SeaComm and our phone number, however, this was NOT legitimate. Vishing and its fraud companions phishing, which involves email and smishing, which occurs with texts are favorite tools of scammers.

To defeat these fraud attempts, always remember… never give out any information unless you initiate the contact and are certain you have reached out to a legitimate phone number or website. Don't use links in emails to go to websites because the link could be fraudulent and send you somewhere you don't want to be. And remember, scammers often use social engineering techniques. By investigating your social media use, they can build a comprehensive picture of who you are and what online services you use. Using this information, they can develop phishing emails that are much more convincing. They also threaten bad outcomes if you don't do what they want immediately. Never take any action on the spur of the moment due to fear. If you receive a call, text or email like this, it's almost always fraud.

If you are a SeaComm cardholder, keep in mind that we do partner with SecurLOCK, also known as Falcon, to provide fraud protection services to our members. In the instance that suspected fraud is detected, SecurLOCK may reach out via automated phone call or text message to verify the charge, however, the call will not come from our phone number and they will not require you to give out detailed account information.

And if this isn't enough to worry about, student borrowers in New York State should be mindful of potential debt relief scams as the federal government moves to provide up to $20,000 in debt forgiveness. Borrowers should seek out trusted information at websites with .gov addresses, such as studentaid.gov. Borrowers should also not trust people or programs who call, email or text and make promises of early or special access or guaranteed eligibility. And borrowers should never give out their personal information like student aid IDs or social security numbers to anyone who contacts them.

Always be skeptical, if it seems too good to be true, it probably is. Remember that we will never call you, send a text message, or email you to retrieve your personal information, after all, we already have it. If you're ever in doubt on the legitimacy of a call, text or email, call us at (800) 764-0566.

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