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

As shoppers scramble for last minute holiday deals, the crooks are ready to take advantage.

Some scams to watch out for:

Charitable giving is often done in December, which means that sham charities exploiting your goodwill via fake websites and pushy telemarketers. This is the most common holiday scam according to an AARP poll, so make sure you know who you are donating to and perhaps give locally.

As holiday packages crisscross the country, scammers send out phishing emails disguised as UPS, FedEx or U.S. Postal Service notifications of incoming or missed deliveries. Links lead to phony sign-in pages asking for personal information, or to sites infested with malware. Don't click on links in email or texts, instead contact the providers directly.

Despite the pandemic, 46 percent of U.S. adults plan to travel during the holidays this year, according to a survey. Spoof booking sites and email offer travel deals that look too good to be true and most likely are.

A custom letter from Santa makes a holiday treat for the little ones on your list, and many legitimate businesses offer them. But so do many scammers looking for personal information about you or, worse, your kids or grandkids, who may not learn until many years later that their identity was stolen and their credit compromised.

Here are some of the warning signs to look out for:

- Huge discounts on hot gift items, especially when touted on social media posts or unfamiliar websites.
- Spelling errors or shoddy grammar on a shopping website or in an email.
- A shopping or travel site does not list a phone number or street address for the business and offers only an email address or fill-in contact form.
- A site that does not have a privacy policy.
- An unsolicited email that asks you to click on a link or download an app to access a deal or arrange a delivery.

Remember to pay by credit card. That way you can dispute charges and limit the damage if it does turn out you were scammed.

Research unfamiliar retail, travel and charity sites online. Look online to see if the site has bad reviews or is connected with a scam.

Don't make a purchase donating to a charity or conduct other financial business online while using public Wi-Fi. It may not be secure.

Don’t make a purchase or donation if a website or caller seeks payment by wire transfer, gift card or prepaid card. All red flags and almost always a scam.

Things are hectic this time of year but it’s always worth it to take the extra time to think before you click or give out any information.

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