FS-ISAC

Your Institution Logo

Security Tips Newsletter

December 2023 | Issue No. 5

Security is Everyone's Responsibility

'Tis The Season For Scams

It 'tis the season… for fraud.

Did you know "about half of consumers who said they've been targeted by an online holiday shopping or phishing scheme ended up getting scammed, according to a new survey by Norton, a seller of cybersecurity software? Respondents who fell victim to scammers lost an average of $1,500," it said according to a report by Forbes.

Scam Prevention Tips

Remain vigilant during the 2023 holiday season by reviewing these common scams.

Gift Card Scams. Budgets can become tight when finding gifts for your loved ones, so any financial relief is welcomed. You may, however, come across emails or pop-up ads offering free gift cards. Be wary of these tempting opportunities. They are often a ploy to collect your personal information that can be later used to steal your identity.

Charity Scams. Charity scams can take place online and even over the phone. According to the Federal Trade Commission (FTC), scammers will rush people into donating, or trick them by thanking them for a donation they never paid for and then asking for payment. They will also use vague and sentimental claims while asking for a donation but won't detail how they'll donate your money. Always research any charity before you donate and never give money by gift card, cryptocurrency, or wire transfer.

Package Delivery Scams. The Federal Communications Commission (FCC) warns of delivery notification scam calls and texts. These text messages and calls look like they're from a legitimate mail or package courier, such as the US Postal Service, and include a fake tracking link. The link will lead you to a website to enter personal information, or it will install malware, software designed to gain unauthorized access, on your phone or computer. The malware will then start stealing your information.

Fake Gift Exchanges. You're invited via social media to join a gift exchange, which sounds harmless and fun. Why wouldn't it be? If you buy one $10 gift for a stranger, you will receive as many as 36 gifts back! It's a hoax with the same premise as a pyramid scheme where it relies on constantly recruiting new participants. In the US, pyramid schemes are illegal, so it's best to just respectfully decline any invitations to participate.

Emergency Scam. No one wants to hear a family member or friend is dealing with an emergency, like a serious accident or incarceration. We quickly want to help, which is an admirable trait, but scammers take advantage of it. They target people claiming to be a family member or friend where the circumstance requires money to be resolved. Before sending any money, verify their story with other family and friends, but call directly. You can also ask questions that would be hard for an impostor to answer correctly.

Bogus Websites. Online shopping is convenient especially when trying to avoid the holiday shopping rush. When you do shop online, make sure to only use legitimate websites. Scammers use URLs that look remarkably similar to those of legitimate sites. Always double-check the URL before making a purchase and be wary of sites where the brand name is included with long URLs.

Malware Email. Don't be quick to click! Clicking on the wrong link or downloading a scammer's attachment can result in malware spreading to your computer. This computer virus or "bug" can steal personal information or even hold your device hostage unless you pay a price. Links and attachments can come in the form of emails or pop-up advertisements.

Puppy Scams. Pets make great gifts, but there's a lot you should first consider. Should you decide it's the right decision, be careful about adopting a pet online. You could end up with a puppy mill pooch, or nothing at all. Fake pet sellers can lure you into thinking you're getting a four-legged friend, only to take your money and not deliver.

What to Do If You Are Scammed

- If you feel that someone is scamming you, don't respond to the email, and block it. If it's a phone call – hang up!
- If you provide your personal information (account, date of birth, online banking userID, password, etc.) contact your financial institution immediately.
- Use multi-factor authentication wherever possible.
- Update security software on your computer and mobile device.