‘Tis The Season

FS-ISAC continues its year-end reminders to help members and their customers protect themselves against scams

Summary

Cybercriminals never take a day off, but during the holiday season, these thugs will initiate a variety of different social engineering ploys against consumers, small businesses, and financial institutions across the US. The holiday shopping season is underway and the National Intellectual Property Rights Coordination Center (IPR Center) is launching a new holiday shopping toolkit to help consumers protect themselves from substandard or even hazardous counterfeit toys, electronics, cosmetics, and other products.

The holiday shopping toolkit includes online shopping do’s and don’ts, ways to protect financial and banking information, educational videos and infographics, and general information on how to spot fake merchandise. Below are a few of the malicious websites, emails, text messages, and phone calls one can expect through the remainder of the year.

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.

Bogus Invoices. Fraudulent invoice emails may appear to be legitimate posing as a well-known tech company, supplier, or another firm you may or not use. The email contains a phony invoice for services, office supplies, and more. The email instructs you how to send payment or to click on a link or call a phone number if you did not authorize the purchase.

Charity Scams. Charity scams can take place online and even over the phone. According to the 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 U.S. 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 United States, pyramid schemes are illegal, so it's best to just respectfully decline any invitations to participate.

Temporary Holiday Jobs Scams. It's not uncommon for people to want to make some extra money with a seasonal job. You just have to be careful of employment scams, especially when retailers and delivery services often need extra help during the holidays. Be cautious of solicitations requiring you to share personal information online or pay for a job lead. Rather than apply online, go to a retailer location and apply in person.

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. Learn more about malware scams.

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.

2023 Spring Summit

Make 2023 the year you share your insight on cybersecurity with your financial services peers. Don’t miss the opportunity to submit a presentation for the FS-ISAC 2023 America Spring Summit! The deadline to submit is **6 January**. With this year’s theme, Forging a Resilient Future, the following topics will receive extra consideration: Building a Diverse Workforce, Securing the Supply Chain, Mastering the Ordinary with the Extraordinary (“Do the basic stuff well”), Cryptography (including Post-Quantum, Agility), Combatting Cyber Fraud; and Protecting Digital Assets, All submissions are reviewed by our Content Committee and FS-ISAC Content Team for technical merit, expertise, topic selection, approach, and interest to attendees. If you have submission-related queries, please contact summit@fsisac.com.