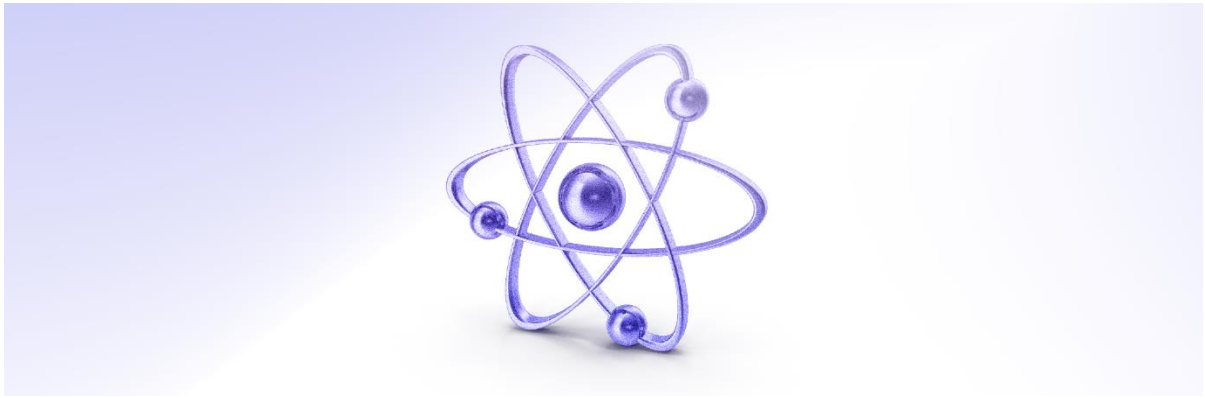
FS-ISAC | Security Tips Newsletter

1 November 2024 | Issue No. 15

Security is *Everyone's* Responsibility



‘Tis The Season For Scams, Again

Summary

December is the month when consumers need to step up their vigilance around fraud and cyber-attacks (though you should remain wary throughout the year). In addition to the usual suspects, be on guard against new scams that can/will ruin your holiday plans.

New Scams to Watch Out For

New threats include the following scams. Remember, *think before you click!*

Social Media Scams. Resist the temptation of clicking on ads on social media pages because they can direct you to a fraudulent website and give the gift that keeps on making you miserable by infecting your device with malware. Instead, visit the trusted retailer's website.

Look-A-Like Websites. Speaking of social media scams, threat actors create counterfeit websites that look like the real thing but are designed to capture credentials and account information or are laced with malware, software designed to give scammers unauthorized access to your device. Instead, visit the trusted retailer's website. Always double-check the URL before making a purchase and be wary of sites where the brand name is included with long URLs. Scammers use URLs that look remarkably similar to those of legitimate sites.

Fake Travel Booking Sites. Nothing will ruin your holiday travel like booking a trip on an imaginary travel booking site. When searching for travel destinations and booking travel, pop-up ads with unbelievable deals will trap your personally identifiable information leaving you stuck at home.

Compromise Account Alerts. Sure, the notice that you're overdrawn or under attack may look real but is not. Fraudulent alerts are designed to make you panic, click the link, and surrender your account information. The best bet is to contact your financial institution directly using trusted information.

The Usual Suspects

Remain vigilant during the 2024 holiday season by being aware of these common scams.

Gift Card Scams. Budgets can become tight during the holidays, so any financial relief is welcome. You may, however, come across emails or pop-up ads offering 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 made 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 cash 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 requesting personal information, or it will install malware 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 because 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 admirable, but scammers take advantage of it. They target people by pretending to be a family member or friend whose 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.

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

Puppy Scams. Pets make great gifts, but there's a lot you should first consider. One is the dangers of buying or 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 user ID, password, etc.) contact your financial institution immediately.
- Use multi-factor authentication wherever possible

If You're a Victim?

Immediately change any passwords you might have revealed. Consider reporting the attack to IC3.gov and the police, and file a report with the Federal Trade Commission.

Getting Help

If you identify suspicious activity involving your institution, contact them immediately.

12120 Sunset Hills Rd, Reston
VA 20190