The 12 Scams of Christmas

Phishing scams are an ongoing problem, however there is a HUGE increase in the number of scams that start around Thanksgiving and go through Christmas. Cyber-criminals take advantage of distracted staff to launch targeted attacks. Over the next 12 days we'll highlight some of the most popular scams that you should be on the lookout for this holiday season.

1. **Fake Shipping Notifications:** We recommend that you do NOT click on ANY tracking links from FEDEX, UPS or the USPS. Instead, go directly to their website and type in the tracking number in question or log in to your account and check open orders directly.

2. **Email Deals: Don't click that deal!** If a sale sounds too good to be true, it probably is. Ask yourself, "Did I sign up for emails from this retailer? Did I ever supply my email address to this site?" If the answer is "No," then immediately delete the email. Remember: on your computer you can hover over the link and check for typos, repeated letters, or strange words in the link that could indicate an impostor website. If you're really interested in the sale, go to the retailer's website or inquire with customer service to see if the sale is real.

3. **Online Shopping:** It's best to type in the URLs of your favorite holiday shopping sites manually, and only click top-ranked search results when browsing. This precaution will prevent any "malicious" links with executable codes from installing something nasty on your computer or device.

4. **Santa Letter Scams:** Knowing that every child would love a reply letter from Santa, phishers manipulate parents' heart strings by offering great deals on "Santa letters." Before ordering your child or grandchild a Santa letter, check for reviews and a good Better Business Bureau (BBB) rating. Even then, don't provide too many details about your child/ grandchild, such as their birth date, school name, pet's name, etc.

5. **Bogus Charities:** Cyber criminals play on our charitable nature during the holidays. Most legitimate charity websites use .org, not .com. Also, beware of charities with copycat names or small variations in the spelling of the website. The best policy is to call the charity directly or visit their website directly instead of clicking on email links.

6. Long-lost Friends Scams: Online scammers can also send bogus links from fake organizations through your friends' contact lists to get to you. These emails look normal, as they're coming from a familiar name. Ask yourself, "Has this person ever sent me a message like this before? When was the last time I talked to this person?" The best policy is to pick up the phone and ask if they sent you the email. Your "friend" may not know that they've been compromised and that emails are being sent out with their account or in their name.

7. **Social Media Ads:** Criminals replicate a legitimate ad (Best Buy, Amazon, Macy's) and when you click on it, malware or ransomware can be installed on your phone or other devices. Our best advice is refrain from clicking on ads during the holiday season and don't click on anything while on your phone! It's more difficult to figure out what's legitimate and what's a scam when on your phone. If you see a great deal, go directly to the vendors website. That same deal should be on the site. If it's not, you can always call customer service and inquire.

8. **Pet Scams:** While a year-round issue, pet scams (puppy scams are the most used) hurt families seeking to add a family member to their household for the holidays. Pet scams are often difficult to avoid as cute pictures, and good deals pull at the heartstrings and wallet. To prevent this fraud, only purchase pets through reputable sources such as: Petsmart, the local shelter, breeders that can provide references or other local adoption agencies.

9. **eCards:** Receiving an eCard, especially at Christmas is not unusual. However, as always, there are bad guys out there looking to take advantage and they see eCards as an easy way to do that. Malicious eCards can contain spyware or malware, designed to infect your computer and steal your data. In some cases eCards have been the source of ransomware, a virus that locks down your files and demands payment to unlock them. Here are some clues that can help you spot a malicious e-card; look out for spelling mistakes and poor grammar and never install .exe files.

10. **Mobile Attacks:** Don't let your guard down just because you are on a mobile device.Be just as careful as you would on any desktop! Watch out for ads, giveaways and contests that seem too good to be true. Often these lead to phishing sites that apear to be legit. Don't trust any messages that attempt to get you to reveal any personal information! And, always think before you click!

11. **Money Transfers:** Got an email from your boss telling you to transfer money? STOP – don't do it! Well, don't do it until you verify with a phone call that you're supposed to send that money. This time of year cyber-criminals ramp up targeting those in finance and HR with phishing emails that look completely legitimate. Many banks and insurance companies are refusing to refund money stolen this way. The best thing you can do is slow down, take a few minutes and call whomever is asking you to send the money and verbally verify that you should.

12. **IRS & Other Government Scams:** Who likes getting a call or email from the IRS? Nope, not me either. During the holidays aggressive criminals pose as IRS agents with the intention of stealing money or personal information. This scam comes in two forms. There's the nasty email demanding payment or they will confiscate your property and put you in jail. Then there's the phone scam, or what's known as "voice phishing" where the phone call phone threatens arrest, or business license revocation if you don't pay a bogus tax bill. These calls most often take the form of a "robocall," a text-to-speech recorded voice mail with instructions to call back a specific telephone number and the phone number is spoofed to look like it's coming from Washington D.C. The IRS will never call you to demand payment, they always communicate via a letter first and then a certified letter.