Click Thinking Spotlight

Online Holiday Shopping

Because countless numbers of online shoppers are victimized by scammers during the holiday season, it's important to know how to protect yourself. The following tips can help.

- If an online offer arrived in your email spam folder, be wary. Many cybercrimes start with phishing emails that mimic big-name retailers, and they usually end up here.
- Ads or offers that come to you through social media platforms should also be treated with skepticism. Scammers often use sites like Facebook and Twitter to disguise their efforts.
- Although cybercriminals are constantly refining their phishing emails, fake ads and fraudulent websites, there are signs you can look for to spot them.
- If the sender's email address doesn't reflect the company name, it's likely a fake. Spelling and grammar mistakes are another red flag.
- While holiday offers generally don't last long, deals with an extremely small window of opportunity and extreme sense of urgency are usually an invitation to trouble.
- When visiting online retailers, make sure they display the https prefix, secure padlock icon in the title bar or a combination of these. Sites with secure designations may also appear green in some browsers.
- Don't use public wifi for online holiday shopping. These networks are easy to hack, making personal information, like credit card or bank account numbers, accessible to scammers.
- Go directly to the sites you want to shop by keying in the web address. Hyperlinks in emails or clickable ads on social media can lead to fake sites scammers have created to steal your information. Hovering over links or ads may reveal the real address.
- If you're using a shared computer, use a private browser window for online shopping. This ensures someone else can't track your history and gain access to stored credit card and other personal information about your buying habits.
- A fantastic online deal is cause for excitement. If you let your emotions overtake you, however, you're playing into the hands of scammers. Slow down and make sure you know the deal is legitimate. If you have any doubts at all about the seller or the offer, don't take chances.
- If you're on a work device, delay any research or purchases until you can do it from your personal computer. This way, a successful phishing attack won't harm the entire network.

For the Online Holiday Shopping training module, see your manager or information security contact.