Online Holiday Shopping

How to protect yourself

Consider the Source

When you come across a deal online, the first thing you should do is consider where it came from. If it 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.

Know the Signs

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. Deals with an extremely small window of opportunity and high sense of urgency are usually an invitation to trouble. When visiting online retailers, look for the 'https' prefix, the word 'secure', a padlock icon or combination of these in the title bar. The bar may also appear green in some web browsers if the site is verified secure. Scammers often use sites like Facebook and Twitter to disguise their efforts.

Protect Yourself

Don't use public wifi when shopping online. 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 that scammers have created to steal your information. Hovering over the link or ad may reveal the true address. If you're using a shared computer, use a private browser window. Doing so ensures someone else can't track your history and gain access to stored credit card or purchase information.

Keep Your Emotions in Check

A fantastic online deal is cause for excitement—and if an offer is good for a short time, fear of missing out can lead you to act without considering the consequences. If you let your emotions overtake you, however, you're playing into the hands of scammers. So, it's important to think with your head and not your heart. 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.

Barracuda®
Your journey, secured.