‘Tis the Season to Be Skeptical - Shopping Online Securely

A Holiday Deal Too Good to Be True

Maya was thrilled when she found a pair of name-brand wireless headphones advertised at 70% off. The website looked professional, the holiday promotion felt urgent, and she even received a confirmation email minutes after placing her order. But days turned into weeks, and nothing arrived. Her emails and phone calls went unanswered, and soon after, her credit card was used for unauthorized charges. What started as a bargain became a costly lesson. Maya had been tricked by a fake online store designed to scam holiday shoppers.

Unfortunately, Maya’s story is not unique. As online shopping continues to grow, especially during the holiday season, cybercriminals are seizing the opportunity to lure victims with fake websites, counterfeit promotions, and shopping scams. The good news? You can shop online safely by recognizing common red flags and following a few simple tips.

Fake Online Stores

Cybercriminals create fake websites that mimic legitimate retailers or use the names of well-known brands. When you search for the best online deals, you may find yourself at one of these fake sites. Criminals often promote them on social media with wildly discounted items. By purchasing from such websites, you can end up with your credit card information stolen, counterfeit or stolen goods, or no delivery at all. Protect yourself by taking the following steps:

- **Shop with trusted retailers**. Buy from online stores you already know and have done business with previously. Bookmark them in your browser. You may not find that incredible deal, but you are far less likely to get scammed.
- **Be suspicious of deep discounts**. If an ad or promotion is significantly lower than those you see at established online stores, it’s probably a scam.
- **Check for contact details**. Avoid websites with no contact information, broken contact forms, or personal email addresses. A lack of physical addresses, phone numbers, customer service contacts, and clear return policies are also often clues of suspicious web sites.

- **Examine the web address**. Be suspicious if a website looks just like one you've used in the past, but the domain name or store name is different. For example, you may be used to shopping at Amazon, whose website address is www.amazon.com, but end up at a fake website that looks similar, but has the website address www.aamazon.deals.
- **Search for reviews**. Type the store's name or URL into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake."
- **Be wary of payment methods**. Sites that only accept wire transfers, gift cards, or cryptocurrency are often used by scammers.
- **Secure your accounts**. Protect your online accounts by using a unique, strong password. If remembering them is difficult, consider storing them in a password manager. Enable additional security features such as multi-factor authentication (MFA) and passkeys wherever they're available.

Scammers On Legitimate Shopping Websites

Some online stores offer products sold by individuals or small businesses, and scammers can hide among them. Check each seller's reputation before placing the order by reading their reviews. Be wary of sellers who are new to the online store, lack reviews, or who sell items at unusually low prices.

Online Payments for Purchases

Another way to protect yourself is to regularly review your credit card statements to identify suspicious charges. If possible, enable your credit card account to notify you by email, text, or by app whenever a charge is made to your credit card. If you find any suspicious activity, report it to your credit card company immediately. Use credit cards instead of debit cards for online payments. Debit cards take money directly from your bank account; if fraud is committed, you'll have a much harder time getting your money back. Electronic payment services or e-wallets such as PayPal are also a safer option for online purchases, since they do not require you to disclose a credit card number to the vendor.

Guest Editor

Tricia McMahon, President of the Women in Cybersecurity (WiCyS) San Diego Affiliate and Treasurer of WiCyS Education and Training, is committed to WiCyS' core mission of recruiting, retaining, and promoting women in cybersecurity. She holds an MS in Cybersecurity and is passionate about lifelong learning and professional development. linkedin.com/in/triciaamcmahon

Resources

How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
The Power of Password Managers: https://www.sans.org/newsletters/ouch/power-password-managers/
The Power of Passphrases: https://www.sans.org/newsletters/ouch/power-passphrase/

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch