OUCH! November 2021

Shopping Online Securely

The holiday season is nearing. Soon millions of people will be looking to buy the perfect gifts, and many of us will shop online. Unfortunately, cyber criminals will be active as well, creating fake shopping websites and other online shopping scams to steal your information or money. Learn how you can find good deals without becoming a victim.

Fake Online Stores

Criminals create fake online stores that mimic the look of real sites or use the names of well-known stores or brands. When you search for the best online deals, you may find yourself at one of these fake sites. By purchasing from such websites, you can end up with counterfeit or stolen items, or your purchases might never be delivered. Take the following steps to protect yourself:

- When possible, purchase from online stores you already know, trust, and have done business with previously. Bookmark these online stores.
- Be suspicious of ads or promotions on search engines or social media that are significantly lower than those you see at the established online stores. If a deal sounds too good to be true, it may be a scam.
- Be careful with websites that have no way to contact them, broken contact forms, or use personal email addresses.
- Be suspicious if a website looks just like one you've used in the past, but the website domain name or the name of the store 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.amazonshoppers.com.
- Type the name of the online store or its web address into a search engine to see what others have said about it. Look for terms like "fraud," "scam," "never again," and "fake."
- Protect your online accounts by using a unique, strong password for each of your accounts. Can't remember all your passwords? Consider storing them all in a password manager.

Scammers on Legitimate Websites

Keep your guard up even when shopping at trusted websites. Online stores often offer products sold by third-parties - different individuals or companies - that might have fraudulent intentions. Such online destinations are like real-world markets, where some sellers are more trustworthy than others.

- 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.
- Review the online store's policy on purchases from such third parties.
- When in doubt, purchase items sold directly by the online store, not by the third-party sellers that participate in its online marketplace.
- Even with legitimate vendors, be sure that you understand the seller's warranty and return policies before you make your purchase.

Online Payments for Purchases

Regularly review your credit card statements to identify suspicious charges. If possible, enable the option to notify you by email, text, or app when a charge is made. 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. Avoid websites that only accept payment in cryptocurrency or require obscure payment methods.

Just because an online store has a professional look does not mean it's legitimate. If the website makes you uncomfortable, don't use it. Instead, head to a well-known site you can trust or have safely used in the past. You may not find that incredible deal, but you are much more likely to avoid getting scammed.

Guest Editor

Mark Orlando is a security leader who has defended networks at the Pentagon, the White House, and numerous private sector clients. Today he is the CEO and co-founder of cybersecurity firm Bionic, and is an instructor and course author at the SANS Institute. [Twitter: @markaorlando]

Resources

Making Passwords Simple: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Social Engineering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Messaging Scams: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Scamming You Through Social Media: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/