November 2019

Cybersecurity Newsletter

2d Marine Division G-6

Online Shopping, Keep yourself Secure

Overview

The holiday season is approaching and “Black Friday” is around the corner. Many of us will shop online in search of great deals and those unbeatable bargains, but also hoping to avoid the crowds. Unfortunately, cyber criminals will be active as well, creating fake shopping websites and using other tactics to scam people.

Fake Online Stores

Cyber criminals create fake online stores that mimic the look of real sites or that 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, and in some cases, your purchases might never be delivered. Take the following steps to protect yourself from fake online stores:

- When possible, purchase from the online stores you already know, trust, and have done business with previously. Bookmark online stores you have visited before and trust.
- Look out for prices that are significantly better than those you see at the established online stores. If the deal sounds too good to be true, it may be fake.
- Be suspicious if the website resembles the one you’ve used in the past, but the website domain name or the name of the store is slightly different. For example, you may be used to shopping at Amazon, whose website address is www.amazon.com, but end up shopping at a fake website that has a similar website address, where the letter o is replaced with the number 0.
- 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.”
- Use a unique password for each of your online accounts. Can’t remember all your passwords? Consider storing them all in a password manager. A quick web search on a reliable password manager can save you a lot of headache down the line.

Scammers on Legitimate Websites

Keep your guard up even when shopping at trusted websites. Large online stores often offer products sold by different individuals or companies that might have bad intentions. These web stores are much like swap meets, and you can’t always trust what you see or who you are doing business with. Check each seller’s reputation before placing the order. Be wary of sellers who are new to the online store or who sell items at unusually low prices.

Online Payments

Regularly review your credit report and card statements to identify suspicious charges. Enable the option to notify you by email, text, or app every time a charge is made to your credit card. If you find any suspicious activity, call your credit card company right away and report it. Avoid using debit cards whenever possible. Debit cards take money directly from your bank account; if fraud has been committed, you'll have a much harder time getting your money back. Another option is using well-known payment services such as PayPal for online purchases. Finally, consider using a gift card for online purchases.

Just because an online store has a well-designed, professional look does not mean its legitimate, 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 end up with a legitimate product and avoid getting scammed.

Current Cybersecurity Concerns

1. Phishing

   Phishing is an attempt to obtain sensitive information by disguising messages as coming from a trustworthy source, tricking victims into handing over access to email accounts, bank accounts, or credit/debit card information. Phishing is nothing new, but with the holiday shopping season approaching, cyber criminals are increasing the rate of attempts, and becoming more sophisticated in their methods, making them appear more convincing than that Nigerian prince we have all heard from.

2. Cross-site scripting (XSS)

   XSS attacks allow adversaries to use business websites to execute untrusted code in a victim's browser, making it easy for a cyber-criminal to interact with a user and steal their web session information used for authentication to hijack the site without any credentials. The first thing you can do, is ensure you are only conducting business on websites using and encrypted connection or the “https” url header. The second things, is to use trusted sites to conduct business.

3. Free Wi-Fi

   A few years ago, a major security flaw was found in all Wi-Fi enabled devices. Dubbed “KRACK”, if exploited, this vulnerability could allow hackers to bypass security features and view web traffic on a Wi-Fi devices network even if encrypted. They could then access all manner of sensitive information transmitted on that network such as, password and bank account information. Although most Wi-Fi device manufacturers have released patches for their devices, many public free Wi-Fi devices and network go unpatched or updated.

Contact your Cybersecurity Personnel

If you have additional questions, comments, or concerns, please contact the 2d Marine Division G-6 Cybersecurity Personnel at commercial 910-451-8360 or email 2mardiv_g-6_ia@usmc.mil.