UCDAVIS

INFORMATION SECURITY OFFICE

Top 10 tips for cybersafe holiday shopping

It is that time of year again, festivities, family gatherings and holiday shopping! Many consumers will shop online this year to avoid the crowds. Adopt these cybersecurity tips to make your online shopping experience less risky.

1 Do not use public Wi-Fi for shopping activity.

Public Wi-Fi networks can be very dangerous. While they may be convenient to use, they are usually not secure and can potentially grant hackers access to your personal information. Never log in to any site where the transaction involves sensitive personal data while logged into a public Wi-Fi network.

2 Make sure eCommerce shopping sites are legitimate and secure.

Shop at well-known retailers that you trust. Before entering your personal or financial information into an online commerce site, ensure that the site you are on is legitimate and can be trusted. Look for the "lock" symbol (🔒) in the URL bar and make sure "https" is at the beginning of the URL indicating that encryption is used to protect your data.

3 Know what the product should cost.

Deal with legitimate vendors. Remember the adage, "if it is too good to be true, then it probably is." 'Bait and switch' or 'teaser' scams run rampant during the holiday season.

4 Do not use debit cards for payment.

When you are shopping online remember that it is best to use credit cards or payment services such as PayPal. Credit cards offer more consumer protections and less liability if your information were to be compromised. Alternatively, because debit cards are linked directly to a bank account, you are at a much greater risk if a criminal were to obtain this information.

5 Keep systems up-to-date.

Be sure to keep all of your internet accessible devices up-to-date. Most software updates improve security by patching vulnerabilities and preventing new exploitation attempts. This includes updates to your device operating system (OS), installed applications, and to your anti-virus software.

6 Think before you click.

Scammers take advantage of the surge in holiday deals and communication to send out their own viruses and malware. Be careful with messages regarding shipping confirmations and changes. Phishing scams include cleverly crafted messages that look like official shipping notifications.

7 Use strong and unique passwords.

Creating strong and unique passwords is still the best security practice for protecting your personal and financial information. Make sure your passwords are sufficiently long and complex utilizing a combination of upper- and lower-case letters, numbers, and special characters. MOST IMPORTANTLY, do not reuse passwords across multiple sites; especially between work and personal resources.

8 Avoid saving your information while shopping.

Never save usernames, passwords or credit card information in your browser and periodically clear your offline content, cookies, and history. Avoid saving your payment information in your account profile when completing an online transaction. If the site has the option, check out as "guest" to avoid giving personal/payment information online.

9 Don't share more than is needed.

Be alert to the kinds of information being collected to complete your transaction. If the site is requesting more data than you feel comfortable sharing then cancel the transaction and purchase elsewhere. You should only need to fill out required fields at checkout.

10 Monitor your financial accounts.

Even with good cyber hygiene and best practices, you may still find yourself a victim of a cyber scam. Pay close attention to bank and credit card accounts and be sure to monitor your credit report to ensure that there is nothing out of the ordinary.

"Top 10 tips for cybersafe holiday shopping" was inspired by the Nov. 2021 newsletter (Vol.16, issue 11) published by MS-ISAC (Multi-State Information Sharing & Analysis Center).

Email cybersecurity@ucdavis.edu for more information or to report an incident.