From the desk of
Shelley Winter
CIO

Stress Less This Holiday Season With These 10 Shopping Tips

It is that time of year again, festivities, family gatherings and holiday shopping! Many consumers will avoid brick and mortar stores and choose to shop online instead. As such, it is important to remain vigilant and be aware of the cyber risks while online shopping. While legitimate businesses are after your money, so are cybercriminals. When it comes to holiday shopping, you should be wary of online criminals. The following 10 cybersecurity tips will make your online shopping experience less risky, not to mention keep you in the spirit of the season and safer from those on the "naughty list".

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 not usually secure and can potentially grant hackers access to your personal information. Never log in to banking/financial sites or any site where the transaction involves sensitive personal data while logged into a public Wi-Fi network. If you do use public Wi-Fi networks, make sure that you are using a trusted network, that you do not allow it to connect automatically, and that you are completely logged out of it before logging into any site for transactions involving sensitive personal data. Please consider that it may be in your best interests to avoid public Wi-Fi networks altogether.
2. Make sure eCommerce shopping sites are legitimate and secure.	Shop at well-known retailers that you trust and where you have previously done business. Before entering your personal or financial information into an online commerce site, you must ensure that the site you are on is legitimate and can be trusted. Verify the site is the one you intended to visit by checking the URL. Also, look for the "lock" symbol in the URL bar and make sure "https" is in the beginning; indicating that encryption is used to protect your data.
3. Know what the product should cost.	Deal with legitimate vendors. The adage goes, "if it is too good to be true, then it probably is." 'Bait and switch' or 'teaser' scams run rampant during the holiday season! Use a service like ResellerRatings.com; allowing users to review online companies and to share their experiences purchasing from those companies as part of your diligence in protecting your interests.
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. In a dispute regarding a purchase made with a debit card, you'll be in a weaker position because the merchant will already have your money and it may take weeks to get it back. With a credit card you'll have time to dispute a charge before any money is actually paid out.

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. This is one of the most important and easiest things you can do to help prevent criminals from exploiting vulnerabilities enabling them to access your information.
6. Think before you click.	Scammers take advantage of the surge in holiday deals and communication to send out their own viruses and malware. Scams have significantly evolved in quality and can appear as legitimate discounts or reputable special offers. Be careful with messages regarding shipping confirmations and changes. Phishing scams include cleverly crafted messages that look like official shipping notifications. Always use official channels to stay updated. As always, NEVER open an email from someone you do not know, did not expect to receive, or from a site you have not visited.
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. Consider creating a cryptic passphrase that is longer than the typical password, but easy for you to remember and difficult to crack. 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 autosaves your payment information, go in after the purchase and delete the stored payment details. Better yet, 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.

For more information on holiday shopping safety, visit the following resources.

- https://us-cert.cisa.gov/ncas/current-activity/2020/11/24/online-holiday-shopping-scams
- https://staysafeonline.org/wp-content/uploads/2020/11/Online-Holiday-Shopping-1.pdf

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™