November 2018
Volume 13, Issue 11

Staying Secure While Shopping Online

Making #CyberMonday #CyberSecure

From the desk of Thomas F. Duffy, MS-ISAC Chair

It is that time of year where so many people prepare to purchase gifts for friends, family, and loved ones. Though it can be convenient to avoid the lines and rush for that latest Black Friday deal by shopping online, this also carries some risk. Cybercriminals are always working to steal your personal and payment information and the holiday shopping season is the perfect opportunity for this to happen. By following a few key practices, you can greatly lower your chances of becoming a victim of identity theft or fraud.

Choose Trusted Online Retailers and Apps

Always shop only with trusted online retailers. That means using a retailer you already know or one that is verified through another trusted entity. If you find a new possible shop to do business with, but are unsure about its reputation, try to find reviews from trusted sources such as the Better Business Bureau. It is important to stick to trusted review sources because there are several ways to fake online reviews, and there are places where cybercriminals can pay other criminals to post positive reviews. Even though an untrusted site might have the best prices, it is worth it to use a trusted online shop that is known to safeguard your information and purchases.

The same advice applies when downloading apps to help with your online shopping. Whether you are downloading a store app to get a coupon, a deal aggregator app to comparison shop, or a reward app that ensures you get points or cashback, it is important to stick to trusted apps from known developers. Unfortunately, fake apps appear in the app stores, purporting to be from a trusted source while other apps exist to capture your data without providing the services they claim to support. You can avoid many malicious apps by downloading your apps from Google Play, Apple App Store, Microsoft Store, or another trusted platform, selectively choosing which apps to download, and making sure you carefully read the permissions and app reviews.

Secure your Device, Connectivity, and Accounts

Keep your devices up-to-date, especially those you shop and bank with – Simply updating the device that you use for conducting your online shopping is a key cybersecurity practice. By keeping the device up-to-date with current patches and software, you ensure you have the manufacturer's latest security fixes in place.

Never use a public computer when shopping or banking – Using a public computer, like those found at libraries, can expose you to greater risk. It is best to use a trusted home device and network for anything involving financial transactions.

Never shop or conduct banking on unencrypted or public Wi-Fi – It is best to always conduct financial transactions or log on to sensitive accounts via a trusted Wi-Fi networks. Ideally, this should be from your home network, which should require a password and use WPA2 encryption.

Look for the lock icon on your browser - When a site has a lock icon on the browser window, or in the URL bar, it indicates that your communications with the site are encrypted. If you do not see a lock, look for "*https*" at the beginning of the URL, as this is the same thing as the lock.

Check out as a guest – By checking out as a guest, you prevent the online retailer from storing your personal account and financial information. This minimizes the amount of information that could be lost if the retailer is compromised. If you have or need an account with a retail website:

- ***Use a strong password –*** Be sure to use a strong, unique password. Always use more than ten characters, with numbers, special characters, and upper and lower case letters.
- ***Don't save your payment information with retailers –*** If you have an established account with a retailer, do not store your payment information with them. In the case of an account compromise, stored payment information may allow a criminal to make purchases using your financial information.

Be Wary of Fraudulent Emails and Advertisements

Look out for suspicious or unexpected emails – A common tactic of cybercriminals year round is to send fraudulent emails seeking to get you to click a link or open an attachment. When it comes to this time of year, they may make an email look like it contains tracking information for a shipment or a promotion for a store. The link or attachment might download malware or try to get you to enter your user credentials in a convincing, yet fraudulent login screen, so they can steal your password. Always avoid clicking direct links in emails, and if you receive an email with a tracking number in it, head to the shipping carrier's website in your browser and copy and paste the tracking number itself into the site.

Avoid clicking advertisements or pop-up windows of any kind – Advertisements embedded in websites and pop-ups have been known to be compromised by cybercriminals to distribute malware. It is best to avoid clicking them altogether. To close pop-ups, press Control + F4 on a Windows computer and Command + W on a Mac.