TN Department of Finance & Administration | Strategic Technology Solutions

Cyber Shopping Tips

Online shopping season is here

We want to thank our friends at the Center for Internet Security for providing these tips. You can find additional tips on their website at https://www.cisecurity.org/

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. It is important to **remain vigilant** and be aware of the cyber risks while online shopping. While legitimate businesses compete for your attention, so do cybercriminals. When it comes to holiday shopping, you should **be wary of online criminals**. The following cyber security 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."

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.

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.

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.

Keep systems up to date.

Be sure to keep all 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.

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.**

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.

To further Tennessee's cyber security posture, the TN Cybersecurity Advisory Council has committed to expanding a "whole-of-government" approach to include local governments and citizens. The first step towards this new approach is to improve cyber security communications and awareness. With this goal in mind, the Tennessee Cyber Hub at https://cybersafetn.gov was launched to increase security awareness and improve practices across public sector entities in Tennessee.

The information provided in this bulletin is intended to increase the security awareness of our employees and to help them behave in a more secure manner within their work environment. While most of these tips relate to maintaining a home computer, the increased awareness is intended to help improve our overall cyber security posture.

Do Your Part. #BeCyberSmart.

Best regards to all & happy holidays,

Curtis

TN Department of Finance & Administration | Strategic Technology Solutions

Curtis Clan | Chief Information Security Officer, CISSP