Cyber Safety Tips For Online Shopping

According to the National Retail Federation, more consumers are using their smartphone or tablet to research or make a purchase this holiday season. Follow these simple cybersecurity tips and practices before and while shopping online.

- **Keep a clean machine.** Before picking out that perfect gift, be sure that all internet-connected devices – including PCs, smartphones and tablets – are free from malware and infections by running only the most current versions of software, web browsers and other apps.
- **Use secure Wi-Fi.** Using free public Wi-Fi to shop online while at your favorite coffee shop is tremendously convenient, but it is not cyber safe. Don't make purchases while connected to public Wi-Fi; instead use a virtual private network (VPN) or your phone as a hotspot.
- **Lock down your login.** Create long and unique passphrases for all accounts and use multi-factor authentication wherever possible. Multi-factor authentication will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-timecode sent to your phone or mobile device.
- **Resist the urge.** Be wary of offers too good to be true – no matter how tempting they might be. Buy only from trusted and established online retailers and avoid websites of retailers you've never heard of.
- **Think before you click.** Pay attention to emails you receive. Don't open emails from unknown senders or click on links in suspicious messages.
- **Shop securely.** Not only should you make sure your internet connection is secure. Check to make sure you're shopping on a site that uses SSL protection. The easiest way to tell is to check your browser's address bar. Look for https is the URL. Sites without the s are not safe to submit payment information or other personal details.
- **Pay wisely.** Use a credit card or pre-paid debit card instead of a debit card linked to your bank account. Or use a reliable, established third-party payment service, such as Google Pay, Apple Pay or PayPal.
- **Monitor your accounts.** Check your online financial accounts regularly for suspicious spending. Also, take advantage of text and email alerting services that many banks and credit card companies now offer.