NATIONAL CYBERSECURITY ALLIANCE

Happy Digital Wishes: Cheers to Safe Holiday Shopping

‘Tis the season of gift giving. Before you start making lists and checking them twice, give yourself the gift of cyber safety. According to the National Retail Federation, 73 percent of consumers plan to use their smartphone or tablet to research or make a purchase this holiday season. Don’t let cyber grinches turn merriment into mayhem. Following some simple cybersecurity tips and practices before and while you shop online will help ensure peace of mind during the holidays and year-round.

TAKE-ACTION TIPS FOR A CYBER-SAFE SEASON

Keep a clean machine. Before picking out that perfect present, 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 and apps.

Use a secure Wi-Fi. Using 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 via 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 (MFA) wherever possible. MFA will fortify your online accounts by enabling the strongest authentication tools available, such as biometrics or a unique one-time code sent to your phone or mobile device.

STAYING PROTECTED DURING THE MOST WONDERFUL TIME OF THE YEAR

Think before you click. During this hectic and heavily-trafficked time, there is a marked increase in the number of ads encouraging users to click on links. If you receive an enticing offer, do not click on the link. Instead, go directly to the company's website to verify the offer is legitimate.

Do your homework. Fraudsters are fond of setting up fake e-commerce sites this time of year. Prior to making a purchase, read reviews to hear what others say about the merchant. In addition, look for a physical location and any customer service information. It's also a good idea to call the merchant to confirm that they are legitimate.

Consider your payment options. Using a credit card is much better than using a debit card; there are more consumer protections for credit cards if something goes awry. Or, you can use a third party payment service instead of your credit card. There are many services you can use to pay for purchases – like Google Pay – without giving the merchant your credit card information directly.

Watch what you give away. During this season of giving, be alert to the kinds of information being collected to complete your transaction. If the merchant is requesting more data than you feel comfortable sharing, cancel the transaction. You only need to fill out required fields at checkout and you should not save your payment information in your profile. If the account autosaves it, after the purchase go in and delete the stored payment details.

Keep tabs on your bank and credit card statements. Be sure to continuously check your accounts for any unauthorized activity. Good recordkeeping goes hand-in-hand with managing your cybersecurity. Another tip for monitoring activity is to set up alerts so that if your credit card is used, you will receive an email or text message with the transaction details.