NATIONAL CYBERSECURITY ALLIANCE

TIPS FOR SAFE ONLINE SHOPPING

As more consumers purchase goods and services online, cyber criminals take advantage of this opportunity to swoop in and steal your sensitive information. There are steps consumers can take to better secure accounts and transactions.

TAKE-ACTION TIPS

KEEP A CLEAN MACHINE

Before making any online purchase, be sure that all internet-connected devices – including PCs, smartphones and tablets – are 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 necessarily cyber safe. Don't make purchases via public Wi-Fi; instead, use a Virtual Private Network (VPN) or your phone as a hotspot for a more secure shopping experience.

LOCK DOWN YOUR LOGIN

Create long and unique passphrases for all accounts and use multifactor 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.

GIVE AND TEACH

Purchasing an internet-connected device for a loved one? Don't assume they know how to use it securely. Take a moment to teach recipients how to configure privacy settings, how to deactivate any unnecessary features, and how to use the devices responsibly and securely. Don't let your loved ones learn the hard way. If you give them the gift, own your role in helping them understand how to use it securely.

THINK BEFORE YOU CLICK

If you receive an enticing offer via email or text, do not be so quick to click on the link. Instead, go directly to the company's website to verify the offer is legitimate.

NATIONAL CYBERSECURITY ALLIANCE

TIPS FOR SAFE ONLINE SHOPPING

TAKE-ACTION TIPS

DO YOUR HOMEWORK

Fraudsters are good at setting up fake e-commerce sites. 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.

DON'T GIVE IT ALL AWAY

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.

ADDITIONAL RESOURCES

- **Cybersecurity & Infrastructure Security Agency:** Cybersecurity Tips
  https://www.us-cert.gov/ncas/tips
- **Cybersecurity & Infrastructure Security Agency:** Shopping Safely Online
  https://www.us-cert.gov/ncas/tips/ST07-001
- **Federal Trade Commission:** Cybersecurity Basics
  https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics
- **Adobe & NCSA:** Security Awareness Video: Phishing and Ransomware
  https://youtu.be/D_yAYhjNE-0