NATIONAL CYBERSECURITY ALLIANCE

TIPS FOR SAFE ONLINE HOLIDAY SHOPPING

From the convenience of one-click ordering to the lure of next-day delivery, online shopping has grown tremendously in the past few years. But online shopping isn't just convenient for us and good for businesses, it's good business for cybercriminals. Scammers know we're rushing to find the perfect gifts before the holidays or sweep up the best Black Friday deals. They often use this busy time to trick us into paying for goods we won't receive or obtain personal information for financial gain. With a few simple tips, you can enjoy the convenience of shopping online and ordering gifts with peace of mind.

DO YOUR HOMEWORK
Fraudsters are good at setting up fake e-commerce sites, particularly during the holiday season. Prior to making a purchase, read reviews to hear what others say about the merchant and check sites like the Better Business Bureau. In addition, look for a physical location and any customer service information to confirm if the site is legitimate.

DON'T HESITATE TO UPDATE
Before making any online purchase, be sure that all internet-connected devices – including PCs, smartphones and tablets – are running the most current versions of software. These updates protect your devices form any new threats or vulnerabilities.

USE A SECURE WI-FI
Using public Wi-Fi to shop online for gifts is convenient, but it is not cyber safe. Don't make purchases via public Wi-Fi; instead, use a trusted Virtual Private Network (VPN) or your phone as a hotspot for a more secure shopping experience. Or, just save those purchases for later and wait until you're home and on your own secure network.

LOCK DOWN YOUR LOGIN
Create long and unique passphrases for all accounts and use multifactor authentication (MFA) when 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.

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.

STAYSAFEONLINE.ORG
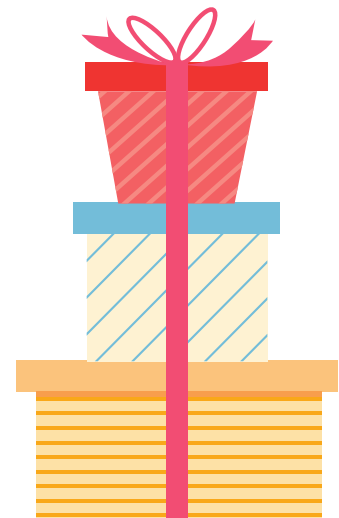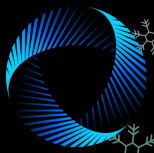
TIPS FOR SAFE ONLINE HOLIDAY SHOPPING

CONSIDER YOUR PAYMENT OPTIONS
Using a credit card is much safer 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 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, go in after the purchase and delete the stored payment details.

KEEP TABS ON YOUR BANK AND CREDIT CARD STATEMENTS
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 debit or credit card is used, you will receive an email or text message with the transaction details.

GIVE THE GIFT OF PEACE OF MIND

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 and security settings, set up a strong password, and deactivate any features they don't need. Don't let your loved ones learn the hard way. If you give them a device, also give them the gift of peace of mind.

ADDITIONAL RESOURCES

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