TOP SAFETY TIPS *for* ONLINE HOLIDAY SHOPPING

Don't let the magic of the shopping season turn to mayhem. Anything connected to the Internet, including mobile devices like smartphones and tablets, need to be protected – especially during heavy use periods, such as the holidays. Scammers and cybercriminals can be active this season as well. Everyone should be on alert for emails that might urge us to act quickly and click through links and open attachments, which are often malicious. Be wary of emails about problems with your credit cards or an account or the status of an online order. The bad guys know we are price sensitive when shopping online. Exercise caution when an ad offers unusually steep discounts. Being a safe and secure shopper starts with STOP. THINK. CONNECT.— Take security precautions, think about the consequences of your actions online and enjoy the conveniences of technology with peace of mind while you shop online. Remember these tips during all online purchases and not just during the holidays!

Online Shopping Tips:

Conduct research: When using a new website for purchases, read reviews and see if other consumers have had a positive or negative experience with the site.

When in doubt, throw it out: Links in emails, posts and texts are often the ways cybercriminals try to steal your information or infect your devices.

Personal information is like money: value it and protect it: When making a purchase online, be alert to the kinds of information being collected to complete the transaction. Make sure you think it is necessary for the vendor to request that information. Remember, you only need to fill out required fields at checkout.

Use safe payment options: Credit cards are generally the safest option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered.

Don't be disappointed: Read return and other polices so you know what to expect if the purchase doesn't go as planned.

Protect your $$: When shopping, check to be sure the site is security enabled. Look for web addresses with https:// indicating extra measures to help secure your information.

Source: National CYBER SECURITY Alliance, 2015

Shopping On the Go:

Now you see me, now you don't: Some stores and other locations look for devices with WiFi or Bluetooth turned on to track your movements while you are within range. Disable WiFi and Bluetooth when not in use.

Get savvy about Wi-Fi hotspots: Limit the type of business you conduct over open public WiFi connections including logging onto key accounts, such as email and banking. Adjust the security settings on your device to limit who can access your phone.

Basic Safety and Security Tips:

Keep a clean machine: Keep all web-connected devices — including PCs, mobile phones, smartphones, and tablets — free from malware and infections by running only the most current versions of software and apps.

Get two steps ahead: Turn on two-step authentication — also known as two-step verification or multi-factor authentication — on accounts where available. It adds a layer of protection beyond the logon and password.

Make better passwords: If your passwords are weak, improve them by adding capital letters or numbers and symbols, and using different passwords for every account.

QUOTE *from* NCSA'S EXECUTIVE DIRECTOR

" It's no surprise that tech gifts are at the top of our holiday shopping lists. And with the season's marked increase of online and mobile shopping, everyone needs to take responsibility and protect themselves against cyber threats, scams and identity theft - not only during this high-volume timeframe but all year long," said Michael Kaiser, NCSA's executive director. "We have seen in past holiday seasons that scammers and cybercriminals are active as well. Be on alert for phishing emails and deals online that look too good to be true. Follow basic safety and security advice when online and when connecting on the go."