HAPPY ONLINE *Holiday* SHOPPING

Cheers to a cybersecure holiday season! Cyber Monday 2017 is expected to be the biggest shopping day in U.S. history.[1] According to a Pew Research Center survey, Americans use a wide range of digital tools and platforms to shop, and roughly 80 percent of adults purchase products online.[2] Mobile has taken over holiday gift giving: last year, half of website visits and 30 percent of online sales were conducted via mobile devices.[3] Gift givers are going mobile to conveniently compare products, read reviews and make purchasing decisions while out and about. Technology also ranks high on shopping lists – from new laptops and gaming systems to tablets, the latest phones and Internet of Things (IoT) devices like video cameras, toys and appliances.

Whether you are giving the gift of connectivity or using it yourself, don't let hackers mess with the merriment. The National Cyber Security Alliance (NCSA) reminds everyone that all devices connected to the internet – including mobile and IoT – must be protected. And young people receiving technology for the first time need to understand how to use it safely and securely. In addition, older adults must make it their mission to continue to learn about and practice good cyber hygiene.

"All tech users – especially vulnerable audiences like teens and seniors – need to take responsibility and protect themselves against cyber threats, scams and identity theft – not only during prime shopping time, but every day," said Michael Kaiser, NCSA's executive director. "In past years, we have seen that scammers, hackers and cybercriminals are actively on the prowl during the holidays. Stay alert for phishing emails, deals that look to good to be true and warnings about packages that can't be delivered or orders that have problems. Continually learn about and always initiate basic safety and security practices, and you will connect with more peace of mind during the holidays and year-round."

1 http://www.techradar.com/news/cyber-monday-2017-deals
2 Pew Jan. 2016 http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/
3 Adobe Jan. 2017 http://www.cmo.com/adobe-digital-insights/articles/2016/11/8/2016-holiday-shopping-up-to-the-minute-data-from-adi.html#gsSXi=4ik

TEENS AND TECH

'Tis the season for many teenagers to receive their first smartphones, tablets or other devices. When giving the gift of technology, parents should also give the gift of safety. While most young people have grown up with technology and are comfortable navigating their online lives, the Keeping Up with Generation App: NCSA Parent/Teen Online Safety Survey revealed that teens and parents are aligned on their top three concerns (ranked as thing they are "very concerned" about), which are:

- Someone accessing a teen's account without permission (teens, 41%, vs. parents, 41%)
- Someone sharing a teen's personal information about them online (teens, 39%, vs. parents, 42%)
- Having a teen's photo or video shared that they wanted private (teens, 36%. vs. parents, 34%)

The good news is that teens turn to their parents for help, with almost half (47%) saying their parents are among their top three sources for learning how to stay safe online, compared with 40 percent who say their friends are top sources. With this is mind, giving a tech-inspired gift may offer the opportune time to begin the internet safety and security dialogue. And, interestingly, teens and parents share similar concerns and would like to learn more about the following – which may offer a good starting point for the tech talk:

- Preventing identity theft (parents, 45%, vs. teens, 44%)
- How to be safer when using free Wi-Fi networks (parents, 29%, vs. teens, 32%)
- Phishing (parents, 27%, vs. teens, 31%)

HELPING SENIORS STAY SAFE ONLINE

Similar to young people, seniors have their own cyber issues. An October 2016 study from Home Instead Senior Care revealed the following:

- Online shopping offers convenience and ease during the busy holidays, but be aware – nearly two out of every five American and Canadian seniors have been the attempted victims of online scams.
- When registering a new account on the latest tech gifts and gadgets you received, remember to change up your passwords. Sixty-eight percent of surveyed seniors use a single password or re-use passwords on multiple sites. Add variety to better protect your information.
- Holidays bring out the giving spirit in all. Don't let your heartfelt donation end up in the wrong place and jeopardize your personal information. Charity scams prey on emotions. Check that the charity to which you're donating is legitimate by looking up the number and calling it.

Whether you are a teen, parent or senior, be on the lookout for urgent online communications that might urge you to act quickly and click through links and open attachments or provide personal information. Be wary of emails about problems with your credit card or an account or the status of an online order. Exercise caution when seeing an ad or offer for which the discount is way below normal. 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.

GET READY TO CYBER SHOP SAFELY:

KEEP CLEAN MACHINES: Before searching for that perfect gift, be sure that all web-connected devices including PCs, smartphones and tablets are free from malware and infections by running only the most current versions of software and apps.
LOCK DOWN YOUR LOGIN: One of the most critical things you can do in preparation for the online shopping season is to fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.
CONDUCT RESEARCH: When using a new website for your holiday purchases, read reviews and see if other customers have had positive or negative experiences with the site.
WHEN IN DOUBT, THROW IT OUT: Links in emails, social media posts and text messages are often how cybercriminals try to steal your information or infect your devices.
PERSONAL INFORMATION IS LIKE MONEY. VALUE IT. 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 that you only need to fill out required fields at checkout.

NAVIGATING THE DIGITAL MARKETPLACE WHILE ON THE GO:

GET SAVVY ABOUT WI-FI HOTSPOTS: If you are out and about, limit the type of business you conduct over open public Wi-Fi connections, including logging in to key accounts such as email and banking. Adjust the security settings on your phone to limit who can access your device.
SECURE YOUR DEVICES: Use strong passwords or touch ID features to lock your devices. These security measures can help protect your information if your devices are lost or stolen and keep prying eyes out.
THINK BEFORE YOU APP: Information about you, such as the games you like to play, your contacts list, where you shop and your location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps.
NOW YOU SEE ME, NOW YOU DON'T: Some stores and other locations look for devices with Wi-Fi or Bluetooth turned on to track your movements while you are within range. Disable Wi-Fi and Bluetooth when they're not in use.

RESOURCES

U.S. DEPARTMENT OF HOMELAND SECURITY (DHS): DHS encourages shoppers to take special precautions when shopping and banking online. Check out the Mobile Banking and Payments tip card and other resources at dhs.gov/stopthinkconnect.
HOME INSTEAD SENIOR CARE: Whether it's the busy online holiday shopping season or day-to-day connectivity, test your internet skill set with Home Instead's "Can you spot an online scam?" quiz. This quiz was created in partnership with NCSA.

STOP | THINK | CONNECT™

STOPTHINKCONNECT.ORG

@STOPTHNKCONNECT STOPTHINKCONNECT