Warmest Digital Wishes! Tis the season for online gift buying. The National Retail Federation forecasts an increase in online holiday sales this year between 7 and 10 percent over last year – to as much as $117 billion.¹

In 2016, high-tech connected devices such as fitness trackers, video cameras and wearables – known as the Internet of Things (IoT) – are on wish lists and gift guides like never before. A new survey² from the National Cyber Security Alliance (NCSA) found that more than a third of holiday gift givers (36%) plan to purchase internet-connected gadgets and gear for family and friends. But wait: before you give the gift of connectivity, don’t let hackers get in your way. According to the survey, 54 percent of respondents reported a raised level of concern about the security of their internet-connected devices following the “distributed denial of service” or DDoS attack in October. This cyber attack used internet-connected devices, such as cameras, home appliances and baby monitors, to disrupt popular online platforms like Amazon, Twitter and Reddit.

Furthermore, the survey disclosed that 62 percent admit to being “somewhat confident” to “not confident at all” about these devices’ safety and security. And an astounding 66 percent are either “not sure” or do not think there is enough information available on how to secure their devices.

“People are genuinely excited about IoT devices and the many benefits they bring to our lives,” said Michael Kaiser, NCSA’s executive director. “We like to remind everyone that in order to function correctly these devices need to collect information about the user – turning them into the ‘Internet of Me.’ We strongly encourage all digital citizens to pay close attention to and learn as much as they can about how to secure their devices.”

Online shoppers have their security and privacy antennae up when shopping; the survey revealed 25 percent had abandoned a purchase, with nearly 10 percent of those doing so between two and four times in the last year. Here are the top three reasons respondents gave for abandoning a purchase because of security concerns:

• Too much information was being asked of me in relationship to the transaction (47%)
• I could not determine if my information was being handled securely (36%)
• I just did not feel confident about the transaction (32%)

Consumers are, however, getting smarter and taking action to protect themselves. The survey spotlighted the following security and privacy measures they are practicing:

• Changing the password on their device before using it (47%)
• Trying to understand what personal information the device collects, how it is being used and how it is stored (45%)
• Reading information from the manufacturer about how to keep the device secure over time (34%)
• Keeping IoT mobile apps (e.g., Nest, doorbell, video camera and security system.) up to date with the latest software updates (30%)
• Researching the past history of security/privacy concerns about a device (27%)

Being safer and more secure while shopping online is a high priority during the holiday season, a key time for online gift buying. This year’s Cyber Monday – which falls on November 28 – is predicted to be the biggest and busiest ever, generating $3.36 billion in sales with 9.4 percent growth compared to 2015.³ And, along with IoT, technology is expected to impact the gift-giving ritual in entirely new ways, with virtual reality, artificial intelligence and mobile and alternative payments taking over the online purchasing landscape.

¹ National Retail Federation Holiday Headquarters, October 4, 2016.
² NCSA Online Holiday Shopping Survey, November 10, 2016.
³ Adobe 2016 Digital Insight Shopping Predictions, October 27, 2016
“More consumers are shopping online than ever before, and everyone needs to be extra cautious and protect themselves even more against cyber threats, scams and identity theft. Good cybersecurity practices must be a critical focus not only during heavy-volume timeframes, but all year long,” said Kaiser. “Keep in mind that online shopping also means it’s scammer season. There are ‘can’t miss’ offers everywhere. It’s nearly impossible for thrifty cybershoppers to visit the digital marketplace without thinking about identity theft, credit card fraud or compromising financial data and other personal information that hackers actively seek.”

NCSA’s STOP. THINK. CONNECT.™ campaign recommends following this basic safety and security advice:

Get Ready to Cyber Shop Safely:

• 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.

• Keep clean machines: Before searching for that perfect gift, be sure that all web-connected devices – including PCs, mobile phones, smartphones, and tablets – are free from malware and infections by running only the most current versions of software and apps.

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

While Navigating the Digital Marketplace:

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

• 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 that you only need to fill out required fields at checkout.

Resources for staying safe and secure while shopping online during the holidays:


• Take a look at the Federal Trade Commission’s tips and video for safe, hassle-free online shopping – https://www.consumer.ftc.gov/articles/0020-shopping-online

• The Better Business Bureau’s “Holiday Helper” offers advice for smart holiday shopping – www.bbb.org/holidayhelper

• Before buying a new connected device this holiday season, take a look at ESET’s Internet of Stranger Things survey for tips and findings to keep you and your family’s digital lives safer – https://www.eset.com/us/resources/detail/survey-internet-of-stranger-things/

Methodology

As part of widespread efforts to promote online safety education and awareness, NCSA commissioned Zogby Analytics to conduct an online survey of 1,215 adults in the U.S. on Nov. 9 and 10, 2016. Based on a confidence interval of 95 percent, the margin of error for 1,215 is +/-2.8 percentage points.

Made possible in part by a grant from the Digital Trust Foundation.