New McAfee Survey Reveals Only 42 Percent of Consumers Take Proper Security Measures to Protect Their New Gadgets
Monday, November 21, 2016 05:01:00 AM (GMT)

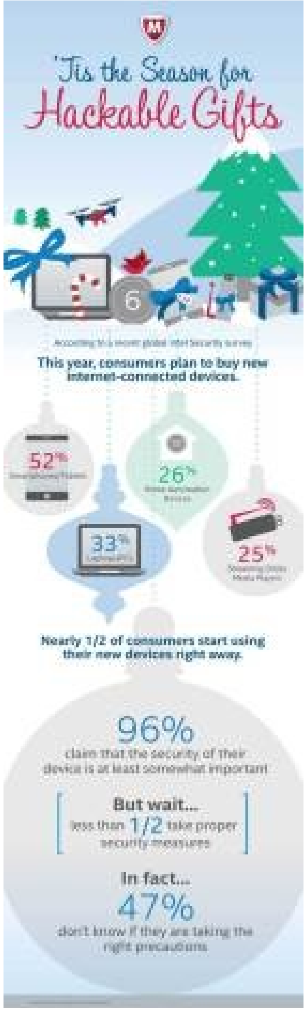
Streaming Sticks, Drones and Smart Home Products Top List of Devices that Can Compromise Consumers' Security if Left Unprotected

NEWS HIGHLIGHTS

- Survey reveals 84 percent of consumers will likely holiday shop online this year.
- Holiday season brings new gifts, and while 79 percent of consumers start using connected devices within the first day of receiving it, only 42 percent claim they take the proper security measures.
- Consumers know it's important to secure their devices, but nearly half (47 percent) are uncertain whether they are taking the proper security steps to do so.

Today Intel Security announced its second annual McAfee Most Hackable Holiday Gifts list to identify potential security risks associated with hot-ticket items this holiday season. The No. 1 most hackable gift category included laptops and PCs, followed by smartphones and tablets, media players and streaming sticks, smart home automation and devices, and finally, drones. To accompany the list, Intel Security conducted a survey to identify the risky behaviors consumers are engaging in during the holiday season and educate them on how to protect themselves.

This Smart News Release features multimedia. View the full release here:
http://www.businesswire.com/news/home/20161120005023/en/


'Tis the Season for
Hackable Gifts
According to a recent global Intel Security survey
This year, consumers plan to buy new internet-connected devices.
52%
26%
33%
Laptops/PCs
25%
Nearly 1/2 of consumers start using their new devices right away.
96%
claim that the security of their device is at least somewhat important
But wait...
less than 1/2 take proper security measures
In fact...
47%
don't know if they are taking the right precautions

Today's digital world is changing fast, and our reliance on the internet is ever increasing. The recent distributed denial of service (DDoS) attack was carried out by a botnet made up of unsecured webcams and other Internet of Things (IoT) devices, and crippled many popular websites connected to the Dyn domain. It's important that consumers understand they can help fight these attacks by ensuring their devices are updated and patched, which helps mitigate risks from the latest threats.

"Unsurprisingly, connected devices remain high on holiday wish lists this year. What is alarming is that consumers remain unaware of what behaviors pose a security risk when it comes to new devices," said Gary Davis, chief consumer security evangelist at Intel Security. "Consumers are often eager to use their new gadget as soon as they get it and forgo ensuring that their device is properly secured. Cybercriminals could use this lack of attention as an inroad to gather personal consumer data, exposing consumers to malware or identity theft or even use unsecured devices to launch DDoS attacks as in the recent Dyn attack."

While a majority of consumers are aware of the vulnerabilities in older connected devices like laptops (76 percent), mobile phones (70 percent) and tablets (69 percent), they lack awareness about the potential risks associated with emerging connected devices, such as drones (20 percent), children's toys (15 percent), virtual reality tech (15 percent) and pet gifts (11 percent). As technology continues to evolve, it is essential consumers understand the risks associated with even the most unassuming devices. While 81 percent of consumers believe it's very important to secure their online identities and connected devices, nearly half are uncertain if they are taking the proper security steps.

This Year's Most Hackable Holiday Gifts Include:

1. Laptops and PCs – Laptops and PCs make great gifts, however, malicious apps targeting PCs are unfortunately common, and are not just limited to

'Tis the Season for Hackable Gifts (Infographic from McAfee)

Windows-based devices.

2. Smartphones and Tablets – Survey results revealed that 52 percent of consumers plan to purchase either a smartphone or tablet this holiday season. Just like PCs and laptops, malware could result in personal and financial information being stolen.

3. Media Players and Streaming Sticks – Media players and streaming sticks have changed the way consumers enjoy movies and TV, but consumers can unknowingly invite a cybercriminal into their living room by failing to update their device.

4. Smart Home Automation Devices and Apps – Today's connected home devices and apps give users the power to control their homes from their smartphone. Unfortunately, hackers have demonstrated techniques that could be used to compromise Bluetooth-powered door locks and other home automation devices.

5. Drones – Drone sales are expected to grow to more than $20 billion by 2022. They can provide unique perspectives when it comes to shooting video and photos. However, not properly securing the device could allow hackers to disrupt the GPS signal or hijack your drone through its smartphone app.

Tips for Consumers to Protect Holiday Cheer

To stay protected for a happier and safer holiday season, Intel Security has the following tips:

- **Secure your device.** Your device is the key to controlling your home and your personal information. Make sure you have comprehensive security software installed, like McAfee LiveSafe™.
- **Only use secure Wi-Fi.** Using your devices, such as your smart home applications, on public Wi-Fi could leave you and your home open to risk.
- **Keep software up-to-date.** Apply patches as they are released from the manufacturer. Install manufacturer updates right away to ensure that your device is protected from the latest known threats.
- **Use a strong password or PIN.** If your device supports it, use multi-factor authentication (MFA), as it can include factors like a trusted device, your face, fingerprint, etc. to make your login more secure.
- **Check before you click.** Be suspicious of links from people you do not know and always use internet security software to stay protected. Hover over the link to find a full URL of the link's destination in the lower corner of your browser.

Find More Information:

- To learn more about the list and survey, check out:
  - **Blog post from Gary Davis:** https://blogs.mcafee.com/consumer/most-hackable-gifts-2016
    Twitter: Follow @IntelSecurity for live online safety updates and tips. Use hashtag #safeholiday to discuss the Most Hackable Gifts of 2016.

Survey Methodology

In September 2016, Intel Security commissioned OnePoll to conduct a survey of 9,800 consumers (aged 18-55+). Respondents were individuals who use an internet-enabled device on a daily basis in the following countries: Australia, Canada, France, Germany, Italy, Mexico, Netherlands, Spain, the U.K., and the U.S.

About Intel Security

Intel Security, with its McAfee product line, is dedicated to making the digital world safer and more secure for everyone. Intel Security is a division of Intel Corporation. Learn more at www.intelsecurity.com.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

Windows is a trademark or registered trademark of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark owned by its proprietor and used by Intel Corporation under license.

*Other names and brands may be claimed as the property of others.

No computer system can be absolutely secure

View source version on businesswire.com: http://www.businesswire.com/news/home/20161120005023/en/

--30-- JH/SF

Contact:

Intel Corporation
Craig Sirois, 214-405-2335
craig.sirois@intel.com
or
Zeno Group
Ashley Dolezal, 650-801-0931
ashley.dolezal@zenogroup.com

1.2

Industries: Technology, Data Management, Hardware, Internet, Networks, Software, Security, Mobile/Wireless
Languages: English
Primary Identifiers: INTC-US
Related Identifiers: 002WNN-E, INTC-US
Source: Intel Corporation
Subjects: Survey, Product/Service, Photo/Multimedia