McAfee for Business

McAfee's "12 Scams of the Holidays" List Educates Shoppers on How to Avoid Unwrapping an Online Threat and Keep Their Digital Lives Safe

Cybersecurity Threats Heighten During the Holiday Season as More Consumers are Expected to Unknowingly Share Their Personal Information Across Their Devices

SANTA CLARA, Calif. — Nov. 11, 2014 — **McAfee, part of Intel Security**, today announced its annual "**12 Scams of the Holidays"** list to educate the public on the most popular ways cybercriminals scam consumers during the holiday season as they surf their digital devices. Cyber scrooges leverage all types of digital devices, social media platforms and mobile apps to take advantage of consumers' distraction during this festive and busy time of year.

This fall, holiday shopping sales are expected to surge from last year to an estimated $616.9 billion[1]. E-commerce sales are also predicted to rise between 8-11% this year to more than $105 billion, with 56% of smartphone owners planning to use their device while shopping[2]. With four out of five U.S. households with Internet access conducting banking transactions online[3], being vigilant about safe online behavior this holiday season is more important than ever.

"As consumers shop, bank and share more while on the go, they open themselves up to threats from criminals who want to steal their personal information," said Gary Davis, Chief Consumer Security Evangelist at McAfee. "Understanding what to watch out for and how to properly secure their devices gives consumers additional information to protect their digital lives."

To help educate and protect consumers and businesses this holiday season, McAfee has identified this year's top **"12 Scams of the Holidays"**:

1. **You've Got Mail!** — As holiday sales continue to migrate online, the risk for shipping notification and phishing scams are increasing. Though malware is a year-round risk, since many people do their holiday shopping online, consumers are more apt to click on a shipping notification or phishing e-mail because they think it is legit.

2. **Deceptive Advertising** — Everyone is searching for steals and deals during the holidays. Keep your eyes peeled (and your wallet in check) when online shopping for this season's most coveted products. Dangerous links, phony contests on social media, and bogus gift cards are just some of the ways scammers try to steal your personal information and ruin your holiday cheer.

3. **Chilling Charities** — 'Tis the season for giving. During the holidays, many consumers give back by donating to their favorite charity. Sadly, no good deed goes unpunished. Be wary of fake charities that could reach you via email, or are shared virally through social media.

4. **Buyer Beware** — There are just some scams that you can't help but fall victim to, unfortunately. Point of sale malware that leads to exposing credit card information falls into this category. Make sure you check your credit card statements vigilantly and stay on top of breaking news to be aware and prepared.

5. **iScams** — New mobile apps for Android and iOS devices are added every day. Thanks to the ongoing advancement of technology, your mobile device can control the temperature in your house, keep you

connected to social media and add cool filters to your holiday photos. Even the most official-looking or festive apps could be malicious and access your personal information.

6. **Getting Carded** — Digital e-cards to spread the holiday cheer are fun, easy and most importantly, thoughtful. While you may want a loved one to send you "Season's Greetings," hackers are looking to wish you a "Merry Malware!" Well-known e-card sites are safe, but be wary of potential scams that cause you to download malware onto your device.

7. **Holiday Travel Scams** — With travel on the rise during peak holiday times, online scammers are ready to take advantage of the fact that consumers often become less vigilant about their safety. Fake online travel deal links are bountiful, but there are also risks that exist once you arrive at your destination including spyware that can access your information through logging onto infected PCs onsite.

8. **Bank Robocall Scam** — When holiday spending increases and consumers are aware of the abuse to their bank accounts and credit cards, hackers use this as an opportunity. In most cases, consumers receive a fake phone call from one of these institutions from an automated (or not) "security agent" stating that the user's account has been compromised and requesting personal information including the account password, to make changes.

9. **ATM Skimming** — During the holiday season, you need cash and are usually in a rush to get it. Criminals can access your information at ATMs by installing skimming devices to steal the data off your card's magnetic strip and either using a video camera or keypad overlay to capture your PIN. A simple solution: look carefully at your ATM for anything suspicious and cover the keypad when entering your PIN.

10. **Year in Review Traps** — Many news services capitalize on the holidays by developing "Year in Review" articles. Companies should warn their employees about the risks of clicking on these types of links from their work emails. Links from phony sources could infect and compromise the security of company devices.

11. **BYO...Device** — With an increase in travel, activity (and bubbly!) over the busy holiday season, people are more likely to forget their smart phones in public places. While inconvenient for them, it is also way for hackers to access sensitive personal information and business data if the appropriate security measures are not in place.

12. **Bad USB Blues** — During the holiday season, you may see an increase in gift baskets from vendors who want to continue doing business with your company in the upcoming year. One of the most popular items in these baskets includes branded USBs. Beware of allowing your employees to use these, as undetectable malware is sometimes pre-installed on them.

To stay protected and ensure a happy and safe holiday season, McAfee has shared these safety tips:

- ***Do Your Research***
  Whether online shopping, donating to charities, or tracking your gifts, do your research to make sure the company you are working with is legitimate.
  - Do an online search of the company you're buying items from to see if there's any news about recent risks
  - Go to the company's homepage to make sure it is a genuine business
  - Instead of clicking on a link in an email for a shopping deal, visit the site directly

- ***Analyze Apps***
  Before downloading a new app, review it to make sure you know exactly what you're putting on your smartphone.
  - Only download apps from an official app store and not a third party
  - If the app requests too many permissions, do not download it. It may be requesting access to information on your phone that you would prefer to keep private, and certainly more information than it needs
  - Use antivirus software and learn more about FakeInstallers here

- ***Bank Carefully***
  People are spending more money during the holidays than they do all year. Cyber criminals may try and use this fact to more easily scam consumers.
  - If your bank calls requesting information, hang up and call them back through the official main phone

number. It's important to talk to your banker through the official number so you know it is legitimate
    - When withdrawing money, be aware of your surroundings. Check to make sure that you are in a safe place to enter your information. If anything looks amiss, leave
    - Inspect the ATM for loose wires or machine parts that may have been tampered with. This could indicate hackers trying to fix the machine for their benefit

- ***Stay Informed***
  Holiday season or not, cyber scams and identity theft happen very frequently throughout the year. Now that shopping season has begun and the danger is heightened, it is important to constantly be aware of new cyber-attacks or threats in the marketplace.
    - Follow breaking news stories for new security breaches to stay alert and be on top of your game
    - Only shop for holiday gifts at retailers you know have not been compromised
    - Check your credit card statements often to make sure that you were not affected.

- ***Educate Your Employees***
  You'll want to make sure that your employees know how to protect themselves, and their devices with your sensitive company information – at all times, but especially during this hectic holiday travel and shopping season when devices are more likely to get misplaced and people let their guard down.
    - Ensure devices are secured with complex passcodes to allow access to smartphones, tablets or laptops
    - Share the most common scams that exist around the holidays with your employees so they know what to be on the lookout for and how to stay protected

If you do plan to search for deals online, use apps or open shopping related emails, make sure your entire household's devices have protection, such as the McAfee LiveSafe™ service, which protects all your PCs, Macs, tablets and smartphones. The McAfee LiveSafe service also includes the McAfee® Mobile Security app, which protects your smartphone or tablet from all types of malware. The app guards you from the latest mobile threats by offering enhanced privacy and backup features, location tracking, and McAfee® SiteAdvisor® technology to help you steer clear of dangers when searching on a mobile device.

You can also help others to stay safe online this holiday season by giving advice and sharing updates with family and friends. McAfee and Dell's Season of Sharing Sweepstakes* rewards you for doing just that, with prizes including a $1,000 gift card to Dell.com** along with McAfee LiveSafe service.

Additional Resources
For more information on McAfee's 12 Scams of the Holidays list and tips on how to stay safe while using digital devices, please visit the:

- Webpage: www.mcafee.com/12scams
- Press release: http://www.mcafee.com/us/about/news/2014/q4/20141111-01.aspx
- Gary Davis's thoughts on the latest scams: http://blogs.mcafee.com/consumer/12-scams-of-holidays-2014
- Robert Siciliano's blog post and infographic: http://blogs.mcafee.com/consumer/12-scams-2014
- To join the conversation during the holidays, use hashtag #12Scams at www.facebook.com/IntelSecurity and follow @McAfeeConsumer

###

** US residents only. No purchase necessary. Sweepstakes is from November 4 – December 12, 2014. For official rules, prize descriptions and odds disclosure, visit 12scams.com . Void where prohibited.*

***Terms and conditions apply. See www.dell.com/giftcard.*

[1] https://nrf.com/media/press-releases/optimism-shines-national-retail-federation-forecasts-holiday-sales-increase-41

[2] http://www.internetretailer.com/2014/10/16/record-44-us-holiday-shoppers-will-go-online

[3] http://www.americanbanker.com/bulletins/-1020520-1.html

About Intel Security
McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live

and work safely and securely in the digital world. www.intelsecurity.com.

Note: McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries. Other names and brands may be claimed as the property of others.

Media contacts:
Eva Ross, DKC News
eva_ross@dkcnews.com
212.981.5218

Mary Salvaggio, McAfee
mary_salvaggio@mcafee.com
646.527.5858