MCAFEE'S "12 SCAMS OF CHRISTMAS" KEEPS SHOPPERS AWARE OF ONLINE RISKS THIS SEASON

Cyber scrooges look to capitalise on the busiest shopping season of the year

Sydney Australia, 12 November 2013 – McAfee today released its annual "12 Scams of Christmas" list to educate the public on the most common scams that criminals use during the holiday season to take advantage of consumers as they shop on their digital devices. Cybercriminals leverage these scams to steal personal information, earn fast cash, and spread malware.
This Christmas, 70 per cent of Australians plan to do at least part of their shopping online. [1]

"The potential for identity theft increases as consumers share personal information across multiple devices that are often under protected," said Sean Duca, Enterprise Solutions Architect, McAfee APAC.

"Understanding criminals' mindsets and being aware of how they try to take advantage of consumers can help ensure that we use our devices the way they were intended – to enhance our lives, not jeopardise them," says Duca.

To help consumers stay alert for greedy Grinches as they surf the web for holiday travel deals and seek out gifts for their loved ones, McAfee has identified this year's top "12 Scams of Christmas":
1) Not-So-Merry Mobile Apps—Official-looking software for holiday shopping, including those that feature celebrity or company endorsements, could be malicious, designed to steal or send out your personal data. Criminals can redirect incoming calls and messages, offering them the chance to bypass two-step authentication systems where the second step involves sending a code to a mobile device.

2) Holiday Mobile SMS Scams—FakeInstaller tricks Android users into thinking it is a legitimate installer for an application and then quickly takes advantage of the unrestricted access to smartphones, sending SMS messages to premium rate numbers without the user's consent.

3) Hot Holiday Gift Scams—Advertisements that offer deals on must-have items, such as PS4 or Xbox One, might be too good to be true. Clever crooks will post dangerous links and phony contests on social media sites, and send phishing emails to entice viewers to reveal personal information or download malware onto their devices.

4) Seasonal Travel Scams—Phony travel deal links and notifications are common, as are hackers waiting to steal your identity upon arrival. When logging into an infected PC with an email username and password, scammers can install keylogging spyware, keycatching hardware, and more. A hotel's Wi-Fi may claim that you need to install software before using it and instead infect your computer with malware if you "agree."

5) Dangerous E-Seasons Greetings—Legitimate-looking e-cards wishing friends "Season's Greetings" can cause unsuspecting users to download "Merry Malware" such as a Trojan or other virus after clicking a link or opening an attachment.

6) Deceptive Online Games—Before your kids are glued to their newly downloaded games, be wary of the games' sources. Many sites offering full-version downloads of Grand Theft Auto, for example, are often laden with malware, and integrated social media pages can expose gamers, too.

7) Shipping Notifications Shams—Phony shipping notifications can appear to be from a mailing service alerting you to an update on your shipment,

when in reality, they are scams carrying malware and other harmful software designed to infect your computer or device.

8) Bogus Gift Cards—An easy go-to gift for the holidays, gift cards can be promoted via deceptive ads, especially on Facebook, Twitter, or other social sites, that claim to offer exclusive deals on gift cards or packages of cards and can lead consumers to purchase phony ones online.

9) Holiday SMiShing—During the holidays, SMiShing is commonly seen in gift card messages, where scammers pose as banks or credit card companies asking you to confirm information for “security purposes”. Some even include the first few digits of your credit card number in the SMS message to fool you into a false sense of safety.

10) Fake Charities—Donating to charities is common this time of year for many looking to help the less fortunate. However, cybercriminals capitalise on this generosity, especially during natural disaster events, and set up fake charity sites and pocket the donations.

11) Romance Scams—With so many niche dating sites now available to Internet users, it can be difficult to know exactly who the person is behind the screen. Many messages sent from an online friend can include phishing scams, where the person accesses your personal information such as usernames, passwords, and credit card details.

12) Phony E-Tailers—The convenience of online shopping does not go unnoticed by cyber scrooges. With so many people planning to shop online, scammers set up phony e-commerce sites to steal your money and personal data.

To keep consumers protected and ensure a happy holiday season, McAfee has shared the following safety tips:

· Review Apps

Review mobile apps carefully before downloading. Check the comments section and confirm the app’s legitimacy directly with the parties that the software claims are involved.

o Double-check that the “download” button is legitimate when attempting to install new apps on your phone.

o Use antivirus software and learn more about FakeInstaller here.

· Deals and Steals

If an offer seems too good to be true, it probably is. Purchase directly from the official retailer rather than from third parties online.

o Do your best to verify “low” prices on this season’s biggest sellers.

o Check gift cards that you receive for suspicious misspellings in the sender’s name or the name of the card company itself. Double-check IP

addresses on the sites you use for shopping and look at customer reviews to verify an e-tailer's legitimacy.

o Always check the domain name on shipping notification alerts and be cautious of any that you receive when you have not sent a package or requested them.

o Only download or buy games from reputable websites.

o Check in with retailers about the legitimacy of a deal you see advertised and talk to your children about how to spot and avoid online potential scams.

· Research Before Sharing

Banking and credit card companies should never ask you for personal information via text message. If you receive such a message, contact your bank directly via phone, secure website, or in-person. Some other specific examples include:

o Log on to trustworthy dating sites when looking for love online and be wary about sharing personal information of any kind to websites or individuals you encounter online.

o Do background research on the charity you'd like to donate to and think before sharing any type of personal information on a website that looks suspicious.

· Be Cautious When Traveling

Before traveling, make sure that all of your software is up-to-date and run a virus scan. If you're asked for a username and password after clicking a link, try using a fake input on the first login attempt. The extra few seconds it takes to load confirms that the page is actually looking for valid username/password combinations; scam sites will let you right in.

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 McAfee LiveSafe, which protects all your PCs, Macs, tablets and smartphones. It also includes McAfee Mobile Security, to protect your smartphone or tablet from all types of malware. This app also guards you from the latest mobile threats and risky apps, offers enhanced privacy and backup features, location tracking and the SiteAdvisor technology to help you steer clear of dangers when searching on a mobile device.

Additional Resources

For more information on McAfee's 12 Scams of Christmas list and tips on how to stay safe while using digital devices, please check out the:

· Webpage: www.mcafee.com/12scams

· Infographic and Robert Siciliano's thoughts on the latest scams

· Michelle Dennedy's article

· To join the conversation during the holidays, use hashtag #12Scams at www.facebook.com/mcafee and follow @McAfeeConsumer

###

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse and shop the Web more securely. Backed by its unrivalled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

[1] ING Direct survey, 2013