MCAFEE WARNS CONSUMERS OF THE "TWELVE SCAMS OF CHRISTMAS"

Cyber-Scrooges Work Overtime During Holiday Season and on Black Friday/Cyber Monday, New Threats Hit Mobile, Email and the Web

SANTA CLARA, Calif., Nov. 9, 2011 – 'Tis the season for consumers to spend more time online - shopping for gifts, looking for great holiday deals on new digital gadgets, e-planning family get-togethers and of course, using online or mobile banking to make sure they can afford it all. But before logging on from a PC, Mac, or mobile device, consumers should look out for the "12 Scams of Christmas," the dozen most dangerous online scams this holiday season, revealed today by McAfee.

"Cybercriminals rub their hands with glee when they think of the holidays," said Gary Davis, director of consumer product marketing at McAfee. "Consumers are making travel plans, shopping for gifts and bargains, updating Facebook and connecting with friends. However, the vast majority have no security protection for their smartphones or tablets, despite using them heavily during the holiday season. Consumers need to stay one step ahead of this season's cyber-scrooges, and make sure they have protection for all of their Internet-enabled devices. Otherwise, they could risk giving the bad guys the biggest gift of all – their own personal and financial information."

McAfee's 12 Scams of Christmas

1. **Mobile Malware:** A recent National Retail Federation (NRF) survey, dated October 19, found that 52.6 percent of U.S. consumers who own a smartphone said they will be using their device for holiday-shopping related activities—whether it's to research products, redeem coupons, or purchase holiday gifts. Malware targeted at mobile devices is on the rise, and Android smartphones are most at risk. McAfee cites a 76 percent increase in malware targeted at Android devices in the second quarter of 2011 over the first, making it the most targeted smartphone platform.

   New malware has recently been found that targets QR codes, a digital barcode that consumers might scan with their smartphone to find good deals on Black Friday and Cyber Monday, or just to learn about products they want to buy.

2. **Malicious Mobile Applications** -These are mobile apps designed to steal information from smartphones, or send out expensive text messages without a user's consent. Dangerous apps are usually offered for free, and masquerade as fun applications, such as games. For example, last year, 4.6 million Android smartphone users downloaded a suspicious wallpaper app that collected and transmitted user data to a site in China.

3. **Phony Facebook Promotions and Contests** – Who doesn't want to win some free prizes or get a great deal around the holidays? Unfortunately, cyberscammers know that these are attractive lures and they have sprinkled Facebook with phony promotions and contests aimed at gathering personal information.

A recent scam advertised two free airline tickets, but required participants to fill out multiple surveys requesting personal information.

4. **Scareware, or Fake Antivirus software** – Scareware is the fake antivirus software that tricks someone into believing that their computer is at risk—or already infected—so they agree to download and pay for phony software. This is one of the most common and dangerous Internet threats today, with an estimated *one million victims* falling for this scam each day. In October 2010, McAfee reported that scareware represented 23% of all dangerous Internet links, and it has been resurgent in recent months.

5. **Holiday Screensavers**—Bringing holiday cheer to your home or work PC sounds like a fun idea to get into the holiday spirit, but be careful. A recent search for a Santa screensaver that promises to let you "fly with Santa in 3D" is malicious. Holiday-themed ringtones and e-cards have been known to be malicious too.

6. **Mac Malware** – Until recently, Mac users felt pretty insulated from online security threats, since most were targeted at PCs. But with the growing popularity of Apple products, for both business and personal use, cybercriminals have designed a new wave of malware directed squarely at Mac users. According to McAfee Labs™, as of late 2010, there were 5,000 pieces of malware targeting Macs, and this number is increasing by 10 percent month on month.

7. **Holiday Phishing Scams –** Phishing is the act of tricking consumers into revealing information or performing actions they wouldn't normally do online using phony email or social media posts. Cyberscammers know that most people are busy around the holidays so they tailor their emails and social messages with holiday themes in the hopes of tricking recipients into revealing personal information.

    - A common holiday phishing scam is a **phony notice from UPS**, saying you have a package and need to fill out an attached form to get it delivered. The form may ask for personal or financial details that will go straight into the hands of the cyberscammer.
    - **Banking phishing scams** continue to be popular and the holiday season means consumers will be spending more money—and checking bank balances more often. From July to September of this year, McAfee Labs identified approximately 2,700 phishing URLs per day.
    - **Smishing** –SMS phishing—remains a concern. Scammers send their fake messages via a text alert to a phone, notifying an unsuspecting consumer that his bank account has been compromised. The cybercriminals then direct the consumer to call a phone number to get it re-activated—and collects the user's personal information including Social Security number, address, and account details.

8. **Online Coupon Scams** – An estimated 63 percent of shoppers search for online coupons or deals when they purchase something on the Internet, and recent NRF data (October 19, 2011) shows that consumers are also using their smartphones (17.3 percent) and tablets (21.5 percent) to redeem those coupons. But watch out, because the scammers know that by offering an irresistible online coupon, they can get people to hand over some of their personal information.

- One popular scam is to lure consumers with the hope of winning a "free" iPad. Consumers click on a "phishing" site, which can result in email spam and possibly dealing with identify theft.
- Consumers are offered an online coupon code and once they agree, are asked to provide personal information, including credit-card details, passwords and other financial data.

9. **Mystery Shopper Scams** – Mystery shoppers are people who are hired to shop in a store and report back on the customer service. Sadly, scammers are now using this fun job to try to lure people into revealing personal and financial information. There have been reports of scammers sending text messages to victims, offering to pay them $50 an hour to be a mystery shopper, and instructing them to call a number if they are interested. Once the victim calls, they are asked for their personal information, including credit card and bank account numbers.

10. **Hotel "Wrong Transaction" Malware Emails** – Many people travel over the holidays, so it is no surprise that scammers have designed travel-related scams in the hopes of getting us to click on dangerous emails. In one recent example, a scammer sent out emails that appeared to be from a hotel, claiming that a "wrong transaction" had been discovered on the recipient's credit card. It then asked them to fill out an attached refund form. Once opened, the attachment downloads malware onto their machine.

11. **"It" Gift Scams** – Every year there are hot holiday gifts, such as toys and gadgets, that sell out early in the season. When a gift is hot, not only do sellers mark up the price, but scammers will also start advertising these gifts on rogue websites and social networks, even if they don't have them. So, consumers could wind up paying for an item and giving away credit card details only to receive nothing in return. Once the scammers have the personal financial details, there is little recourse.

12. **"I'm away from home" Scammers** – Posting information about a vacation on social networking sites could actually be dangerous. If someone is connected with people they don't know on Facebook or other social networking sites, they could see their post and decide that it may be a good time to rob them. Furthermore, a quick online search can easily turn up their home address.

"We don't want consumers to be haunted by the scams of holidays past, present and future," said Jim Walter, manager at McAfee Labs. "With the increase in malware and other attacks on smartphones, tablets and Macs, users need to stay vigilant and ensure they protect all of their devices, not just their home PC – they can't afford to leave the door open to cyber-grinches during the busy holiday season."

How to Protect Yourself

Internet users can protect themselves from cybercrime with the following quick tips from McAfee:

- Only download mobile apps from official app stores, such as iTunes and the Android Market, and read user reviews before downloading them.

- Be extra vigilant when reviewing and responding to emails.
- Watch out for too-good-to-be-true offers on social networks (like free airline tickets). Never agree to reveal your personal information just to participate in a promotion.
- Don't accept requests on social networks from people you don't know in real life. Wait to post pictures and comments about your vacation until you've already returned home.

Be sure you have active, comprehensive protection for all of your devices. McAfee® All Access is the only product that lets you protect a wide variety of Internet-enabled devices, including PCs, Macs, smartphones, tablets and netbooks, for one low price for individuals and families. To learn more, visit http://home.mcafee.com/store/all-access-security.

Special offer from McAfee
As millions of consumers begin to search and shop online during this holiday season, McAfee understands the importance of being aware of cybercriminals tactics and knowing how to stay protected from identity theft and online fraud.

From November 9 - 15, McAfee will be offering a complimentary PDF copy of a new book on http://www.facebook.com/mcafee called 99 Things You Wish You Knew Before(r)... Your Identity Was Stolen, authored by identity theft expert Robert Siciliano. The book is available in print, ePub, and PDF and can now be found on Amazon, Amazon Kindle, and the Sony eBook Store and http://www.99-series.com/store.html from $5.99-$14.97.

In the book, Robert proactively organizes, simplifies, and demystifies the entire issue of identity theft and computer fraud into bite size chunks to make consumers, families, employees and small businesses safe and secure. Consumers will learn the difference between Scareware, Ransomware and Spyware; about the types of cybercriminals, such as a Black Hat, Cracker, Script-kiddie and Hacktivist; and how to protect their identity online and in the physical world.

Additional Resources
- For the complete 12 Scams of Christmas article, go to https://blogs.mcafee.com/consumer/mcafee-twelve-scams-of-christmas
- Web surfers should visit the McAfee Security Advice Center and Facebook page at www.facebook.com/mcafee for information on the latest threats, and tips on surfing safely.
- VIDEO: A New World of Threats
- VIDEO: History of Malware

###

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 unrivaled 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