

# Twelve Online Holiday Scams to Avoid

By Suzanne Choney

[http://technolog.msnbc.msn.com/\\_news/2011/11/09/8720555-12-online-holiday-scams-to-avoid](http://technolog.msnbc.msn.com/_news/2011/11/09/8720555-12-online-holiday-scams-to-avoid)

Many of us are already shopping online, or will be soon, for the holidays. McAfee is pushing its software with its release of the "dozen most dangerous online scams" this season, but there's also some good info here. Consider it a gift of knowledge for you as you surf the Web for presents for your loved ones:

1. Mobile malware: More of us are using our phones for shopping, to research products or to redeem coupons. McAfee says Android phones are "most at risk," citing "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." McAfee also says 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 apps: "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, cyber scammers know that these are attractive lures and they have sprinkled Facebook with phony promotions and contests aimed at gathering personal information." One recent scam promised two free airline tickets — something that sounds appealing at this time of year especially — "but required participants to fill out multiple surveys requesting personal information."

4. Scareware, or fake antivirus software: We've seen lots of examples this year. "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." McAfee says it's one of "the most common and dangerous Internet threats today, with an estimated 1 million victims falling for this scam each day."

5. Holiday screensavers: Ah yes, we love our screensavers for special times of the years like Christmas. But some of the free ones are loaded with more than holiday cheer. "A recent search for a

Santa screensaver that promises to let you 'fly with Santa in 3D' is malicious," McAfee says. "Holiday-themed ringtones and e-cards have been known to be malicious too."

6. Mac malware: Those two words wouldn't have even been put together in the same sentence a few years ago. But, as McAfee correctly says, "with the growing popularity of Apple products, for both business and personal use, cyber criminals have designed a new wave of malware directed squarely at Mac users." McAfee Labs says as of a year ago, there were "5,000 pieces of malware targeting Macs, and this number is increasing by 10 percent month on month."

7. Holiday phishing scams: "Cyber scammers 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 cyber scammer."

Bank 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."

And, "smishing" — phishing by text message, usually involving banking — is also a growing problem. "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 and offers: Whether you're an extreme couponer or an occasional one, the season is rife with good online offers — and malicious ones. "Scammers know that by offering an irresistible online coupon, they can get people to hand over some of their personal information," McAfee says. "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." Another is that "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: "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: "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: Looking for the kind of gift that might sell out quickly this year? "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," says McAfee. "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: You know this by now, or should: "Posting information about a vacation on social networking sites could ... 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."

## Protecting yourself

Aside from buying McAfee's products, or those from another security vendor, here are some of McAfee's tips on staying safe in general, but especially in the weeks ahead:

- "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."