



## Beware the "Twelve Scams of Christmas"-----

### *McAfee, Inc. Warns Consumers About Most Popular Holiday Internet Scams*

By KI MAE HEUSSNER

Nov. 20, 2009—

On the first day of Christmas, my true love gave to me ... a virus in my PC?

Cybercriminals are a creative bunch, tricking even the most cautious users into disclosing sensitive information. But pay attention to the following 12 scams and, hopefully, they won't deceive you.

#### **1. Charity Phishing Scams Prey on Your Generosity**

Hackers are ready and waiting to take advantage of your generosity with e-mails and Web sites that appear to be from legitimate charitable organizations. They may look real, but the Web sites are actually designed to steal donations, credit card information and donor identities.

If you get a suspicious e-mail directing you to a company or charity's Web site, do not click on the link. Instead, go directly to the Web site by typing the address or using a search engine.

#### **2. Deliveries From Santa? No, Scammers**

Cybercriminals often send fake invoices and delivery notifications appearing to be from well-known delivery services. Opening a fake invoice online could prompt the installation of malware on your computer.

Before you click, take a good, hard look at the address the e-mail is coming from. If it's from Federal Express, it should be a short address from "Federal Express" or "FedEx,".

Pay attention to the language in the e-mail, bad grammar is often a red flag. Most importantly, be suspicious if the e-mail asks for credit card information, because a valid delivery notification would not ask for that.

#### **3. 'Let's Be Friends' -- Cybercriminals Target Social Networks**

Clicking on links in authentic-looking "friend request" e-mails from online social networks can automatically install malware on computers and skim personal information.

Instead of clicking on the link, log-in directly to your social network and make sure the request is actually there. If it is and you're still not sure you know the person, check out the person sending the request before you accept it.

#### **4. Thieves Like Holiday E-Cards**

They may be the environmentally-friendly option (and the more convenient one). But holiday e-cards are also a favorite among cyber thieves.

McAfee says it's discovered worms masquerading as Hallmark e-cards and corporate holiday promotions.

Instead of clicking on the link, open up a browser and enter the address yourself.

Or, if you don't know the person sending the e-card or it looks especially suspicious, you're better off deleting it.

## **5. 'Luxury' Items Can Cost More Than You Think**

If it looks too good to be true, maybe it just is. McAfee recently discovered a new scam that tricks shoppers into visiting malware-infected sites offering discounted luxury items from Cartier, Gucci and Tag Heuer.

Tech-savvy thieves even forge Better Business Bureau logos to convince shoppers of the sites' legitimacy.

If you want to buy a high-end item on end, type the company's address directly into your Web browser. And if you're looking for good holiday deals online, be sure to stick to respectable, well-known sites.

## **6. Be Wary of Public Wi-Fi Hotspots**

As you shop this holiday season, McAfee says to never shop online from a public computer or on an open Wi-Fi network.

There may be deals a plenty online but, if you're surfing the Internet on an open hotspot, hackers can spy on your activities and steal personal information as you enter it.

If you connect to a Wi-Fi network at the airport or at a hotel, be careful that you connect to the correct one. Look for signage on the wall directing you to the appropriate network and if you're not sure, ask someone.

## **7. 'Deck the Halls' Could Be Dangerous?**

As you prepare to carol with friends and family, you might search the Web for Christmas carol lyrics. But McAfee says that hackers create holiday-themed Web sites for people hunting for festive ringtones, carols and screensavers.

Downloading infected files could install spyware, adware or other malware on your computer.

Before you start surfing, make sure you have comprehensive and up-to-date computer security software on your computer. And, as you search, steer clear of links with misspellings and other errors.

## **8. Steer Clear of Job-Related E-Mail Scams**

The holidays are an expensive time and, if you're out of work, they can be extra stressful. But don't fall victim to scams targeting job-seekers with work-from-home opportunities and promises of high-paying jobs.

In these scams, McAfee says, once the job-seeker sends his information and pays the "set-up" fee, off the hackers go with their money.

### **9. Auction Sites Fraught With Fraud**

Auction sites can help you find good deals as you do your holiday shopping. But as you visit sites, make sure you actually land on eBay or Craigslist and not imposter sites.

And, as you place your bids, be careful about deals that look just a bit too sweet, as they probably are.

Scrutinize the seller information and pay attention to how they are asking you to pay. Safe browsing technology can warn you if the seller is directing you to a malware-ridden site.

### **10. Password Stealing Scams Rampant During Holidays**

Knowing that people are likely to make online purchase during the holidays, McAfee warns that password theft is rampant around this time.

Using low-cost tools that reveal your password and install malware that can record keystrokes, cyber thieves can access bank and credit card details.

To stay ahead of them, be vigilant about which sites you visit, think before you click and make sure your security software is updated.

[Click here for more tips on a secure password.](#)

### **11. Bank Online -- Carefully**

Be careful of official-looking e-mails from financial institutions, McAfee warns. Cyber thieves send e-mails asking consumers to confirm account information, including user names and passwords, and warn that accounts may become invalid if they don't comply.

Before you click on a link in an e-mail from your bank, make sure it was actually your bank that sent the message. Look carefully at the address and trust your gut. If it looks suspicious, open up a new browser and type in your bank's Web address on your own.

### **12. Scammers Can Hold Your Files for Ransom**

Once scammers have weaseled their way on to your computer, one of their options is to act like virtual kidnappers and hijack your files.

They encrypt the files to make them unreadable and inaccessible and then demand that you pay up if you want them back.

By following the above recommendations, you should enjoy a safe and happy holiday shopping season.