Holidays Are High Time for Cybercrime

Consumers should watch out for the 12 scams of Christmas, McAfee warns

Munich, 16th of Dezember 2010. A season that should be merry can be downright scary when cybercriminals get their way over the holidays. This is why McAfee is warning consumers to beware of the 12 scams of Christmas. From taking advantage of our desire to give with fake charity scams, to trying to fool us into thinking that a friend is in need, cybercrooks are pulling every trick out of their sleeves to try to get a hold of our money and information this season. The truth is the holidays are a time when millions of consumers flock online, let down their guards and open up their wallets, making them more susceptible to cyber tricks. But users don't have to let the scammers ruin your holidays. Read about the 12 scams of Christmas and learn how to avoid them.

The Scams:

1. iPad Scams - Apple's latest gadget is the hot gift of the season and cyber scammers know it. They have been busy extending bogus offers for free iPads on social media sites and via spam. In one version of the scam, consumers are asked to purchase lower-priced products in order to get the free iPad, only to have the crook take off with their credit card number.

2. "Help! I've been robbed" scam - In this scam cybercriminals compromise users' accounts to send messages to their friends that appear to be coming from the victim. The message typically says that they've been robbed while traveling abroad and need a friend to wire them money in order to get home. This is a particularly insidious scam over the holidays when many people are traveling and it's easier for their friends to believe that they need help.

3. Fake gift cards - Knowing that gift cards are very popular over the holidays, cybercrooks are coming up with fake gift card offers with the goal of getting their hands on consumers information and money. In one phony offer, the crooks offered a "Free $1000 Best Buy" gift card to Facebook users who "liked" the phony Best Buy page, and then made victims disclose personal information to get the fake gift card.

4. Holiday job offers - With many people looking to make extra cash over the holidays, cyber scammers have been busy offering fake high-paying, work-at-home jobs in which they ask for personal information such as your email address, home address, and Social Security number, putting victims at risk for identity theft.

5. “Smishing” - Smishing, or phishing via text message, is becoming more common. Usually, the crooks send a text message that appears to come from your bank or an online retailer saying there’s a problem with your account and you should call a number to verify your information. They are actually trying to extract personal information, such as banking and personal details.

6. Holiday rental scam - With many people eager to get away during the holidays, we’re seeing an increase in holiday rental scams in which cybercrooks advertise attractive properties at rock-bottom prices on phony websites. Usually, they asked for deposits via wire transfer, making it difficult for victims to get their money back.

7. Recession scams continue - The economy may be slowly recovering but scammers know that many consumers are still looking for financial help. That’s why recession-related scams, such as pay-in-advance credit schemes and pre-qualified low interest loans are so dangerous. Victims are usually asked for a processing fee upfront that will go directly into the scammers’ pockets.

8. Grinch-like Greetings - Who doesn’t like to send a cheerful e-card over the holidays? Unfortunately, cybercrooks know this and distribute fake e-cards with links to computer viruses and other malware, or even pornography.

9. Low price traps - Scammers use auction sites and phony websites to offer too-good-to-be true prices on popular holiday gifts in the hopes of stealing information and money.

10. Charity scams - The holidays are traditional times for giving and cybercrooks like to take advantage of users generosity by sending spam emails or making phone calls, asking them to donate to a phony charity.

11. Dodgy holiday downloads - Holiday-themed jingles, screensavers, and animations are fun but not when they include malware. Scammers like to distribute dangerous downloads on sketchy websites or via spam, and label them as holiday cheer.

12. Hotel and airport Wi-fi - Many of us take to the road with our laptops during the holidays and use Wi-fi hotspots in hotels, airports and cafés to keep in touch. This makes it a tempting time for cybercrooks to try to hack into unprotected networks.

The Dangers: All of these scams target your money and personal information, and potentially leave you open to identity theft.
Bottom Line: As you go online this holiday season, be more cautious than usual. Avoid deals that look too good to be true and fiercely guard your personal information.

Tips to Avoid Becoming a Victim:

1. When shopping online, stick to reputable and well-established sites that carry trustmarks (icons or seals from third parties verifying that the site is safe), user reviews and customer support. Remember that reputable trustmark providers offer a live link from the trustmark icon, taking you to a verification website.

2. If you're worried you may be a victim of the scam, scan your computer for free using McAfee ® Security Scan Plus to scan for all kinds of threats such as viruses, Trojans and spyware.

3. You can preview a link's web address before you click on it to make sure it is going to an established site. If it is a shortened URL, which is common on social media sites, use a shortened URL preview tool such as http://mcaf.ee to preview the address.

4. Never download or click anything from an unknown source or respond to offers that arrive in a spam email, text or instant message.

5. Stay away from vendors that offer prices well below the norm. Don't believe anything that's too good to be true.

6. Use trusted and protected Wi-fi networks. Don't check bank accounts or shop online if you're not sure the network is safe.

7. Choose your favorite charity and donate directly, rather than respond to unsolicited charity pleas.

8. If you're looking for holiday employment, stick to well-established job sites.

9. Never respond to offers for easy credit or loans where you have to pay fees up-front.

Tips on What to Do If You Have Become a Victim:

1. If you have given your credit card or other personal information to the scammers, immediately call your credit card company to report the issue and place a hold on the card.

2. Contact the Cybercrime Response Unit at www.mcafee.com/cru, an online help center for advice and technical assistance, if you think you've been a victim of a cybercrime.

3. Make sure your computer is protected in the future by installing a complete security software suite that includes anti-virus, anti-spyware, and firewall protection, such as McAfee Total Protection™. Ensure that your software is always up to date (enable the "auto-update" feature) and perform regular scans.

Contact:

McAfee

Isabell Unseld
PR-Managerin Mittel-, Ost- und Westeuropa
Ohmstraße 1
85716 Unterschleißheim
089 3707-1535
isabell_unseld@mcafee.com

Harvard Public Relations

Felix Laubenthal
Guillermo Luz-y-Graf
Implerstraße 26
81371 München
089 532957-46
089 532957-30
mcafee@harvard.de
felix.laubenthal@harvard.de
guillermo.luz-y-graf@harvard.de