McAfee's Annual 12 Scams of the Holidays List

Keeping your digital life safe!

1. **You've Got Mail!** — As holiday sales continue to migrate online, the risk for shipping notification and phishing scams are increasing. Though malware is a year-round risk, since many people do their holiday shopping online, consumers are more apt to click on a shipping notification or phishing e-mail because they think it is legit.

2. **Deceptive Advertising** — Everyone is searching for steals and deals during the holidays. Keep your eyes peeled (and your wallet in check) when online shopping for this season's most coveted products. Dangerous links, phony contests on social media, and bogus gift cards are just some of the ways scammers try to steal your personal information and ruin your holiday cheer.

3. **Chilling Charities** — 'Tis the season for giving. During the holidays, many consumers give back by donating to their favorite charity. Sadly, no good deed goes unpunished. Be wary of fake charities that could reach you via email, or are shared virally through social media.

4. **Buyer Beware** — There are just some scams that you can't help but fall victim to, unfortunately. Point of sale malware that leads to exposing credit card information falls into this category. Make sure you check your credit card statements vigilantly and stay on top of breaking news to be aware and prepared.

5. **IScams** — New mobile apps for Android and iOS devices are added every day. Thanks to the ongoing advancement of technology, your mobile device can control the temperature in your house, keep you connected to social media and add cool filters to your holiday photos. Even the most official-looking or festive apps could be malicious and access your personal information.

6. **Getting Carded** — Digital e-cards to spread the holiday cheer are fun, easy and most importantly, thoughtful. While you may want a loved one to send you "Season's Greetings," hackers are looking to wish you a "Merry Malware!" Well-known e-card sites are safe, but be wary of potential scams that cause you to download malware onto your device.

7. **Holiday Travel Scams** — With travel on the rise during peak holiday times, online scammers are ready to take advantage of the fact that consumers often become less vigilant about their safety. Fake online travel deal links are bountiful, but there are also risks that exist once you arrive at your destination including spyware that can access your information through logging onto infected PCs onsite.

8. **Bank Robocall Scam** — When holiday spending increases and consumers are aware of the abuse to their bank accounts and credit cards, hackers use this as an opportunity. In most cases, consumers receive a fake phone call from one of these institutions from an automated (or not) "security agent" stating that the user's account has been compromised and requesting personal information including the account password, to make changes.

9. **ATM Skimming** — During the holiday season, you need cash and are usually in a rush to get it. Criminals can access your information at ATMs by installing skimming devices to steal the data off your card's magnetic strip and either using a video camera or keypad overlay to capture your PIN. A simple solution: look carefully at your ATM for anything suspicious and cover the keypad when entering your PIN.

10 **Year in Review Traps** — Many news services capitalize on the holidays by developing "Year in Review" articles. Companies should warn their employees about the risks of clicking on these types of links from their work emails. Links from phony sources could infect and compromise the security of company devices.

11. **BYO…Device** — With an increase in travel, activity (and bubbly!) over the busy holiday season, people are more likely to forget their smart phones in public places. While inconvenient for them, it is also way for hackers to access sensitive personal information and business data if the appropriate security measures are not in place.

12**. Bad USB Blues** — During the holiday season, you may see an increase in gift baskets from vendors who want to continue doing business with your company in the upcoming year. One of the most popular items in these baskets includes branded USBs. Beware of allowing your employees to use these, as undetectable malware is sometimes pre-installed on them.

Source:Webpage: www.mcafee.com/12scams Robert Siciliano