HOLIDAY CYBER-SCAMS INFORMATION

BY KIM WILLIAMS

Many people enjoy the holiday traditions of shopping, gift-giving and donating to charities during November and December. Unfortunately, these merry activities also create opportunities for scammers, who take advantage not only of the flurry of spending, but also of people's generosity and lack of free time during this busy season.

As in the past, consumers have to watch out for thieves lurking in malls and parking lots or burglars wanting to swipe new electronics. In addition, people now also need to be aware of the novel ways in which criminals might steal from them. New technologies that make shopping, donating to charities and staying in touch during the holidays simpler also make it easier for criminals to execute a variety of nefarious plans aimed at defrauding others. Unfortunately, in addition to separating people from their money, some of these schemes also wreak all types of havoc. For instance, some of these scams may install malware on your computer that can make files appear hidden, wipe out your hard drive, steal personal information or compromise your privacy.

Cyber-scams to watch for over the holidays include the following:

Social media traps. We trust our social networks, seeking their advice when we want to hire a plumber and sharing details about the restaurant we went to Friday night. Facebook® and other social media sites seem safe because our friends inhabit the same spaces. Crooks, however, seek to take advantage of the trust we place in social media sites. Ways they try to trick us include:

- **Phony profiles.** The person requesting your Facebook friendship looks nice, but he or she might be a criminal using a fake photo. If you "friend" a fake profile, then the scammer has access to your postings, personal information, and your list of friends too. Fake Facebook pages may also contain links to other pages that will infect your computer with malware, if clicked, or entice you to check out other scam sites.
- **Hacked profile pages of friends containing fraudulent offers.** If a friend's status states that he got a free iPad® by simply answering a few questions, you may be tempted to do the same. Be aware though that his page may have been hacked. The questions you answer may provide someone who wants to steal your identity or defraud you in some way with personal information. If anything sounds too good to be true, then it probably is. Don't be fooled.
- **Direct message scams.** You may tweet or post on Facebook that you are trying to find a particular holiday gift. Then you receive a message from someone you don't know offering to sell the product you want. This could be a scam. If you do not know the person making an offer, be careful before corresponding with him or her and giving away any money.

Fraudulent emails. Fraudsters may obtain your email address in any variety of ways. Once they have it, they may bombard you with spam designed to take your money or compromise your computer. Some of the spam emails may contain files that, when downloaded, disrupt or compromise your computer system. Be very careful when reviewing your inbox. Regularly delete emails in your spam folder and do

not open or click links within any emails from sources you do not recognize. Email scams to look out for during the holidays include:

- **Ransomware scam.** The Internet Crime Complaint Center (IC3) and the Department of Homeland Security have recently identified a new type of ransomware called “cryptolocker.” This malevolent file, when downloaded, encrypts the contents of the victim’s computer. The criminals demand a “ransom” within a certain period of time in order to have the files decrypted. At the time of publication, a way to decrypt the files without the use of the attackers’ private key has not been discovered.
- **Bank account scam.** The email advises your bank account has been compromised. It provides a number to call to reactivate your account, directs you to a website designed to gather personal information, or simply asks you to reply to the email and include personal data. The aim is to capture your account number, address, Social Security number or other information.
- **Charity scam.** The email claims it is collecting money for a specific charity and asks for a credit card number or sends you to a bogus website where personal information and your credit card number are gathered.
- **Malicious e-card.** The email looks like a greeting card, but when you open it, malware is downloaded onto your computer.
- **Bargain basement email.** This email offers some kindof promotion or bargain on a recognized brand. The recipient is directed to a website that—similar to the fake charity website—looks legitimate but is actually bogus and is set up to gather personal information and credit card numbers. Be especially alert for these emails on Black Friday and Cyber Monday as scammers may send emails on these days with a “one day only” limit attached to them to entice you to visit the site.
- **Hotel email scam.** This email appears to be from a hotel and claims that a transaction was charged to your credit card. It offers a refund if the recipient downloads and completes a refund form. Upon downloading this form, the user also unwittingly installs malware onto his or her computer. By filling out the form, the victim shares the personal information on it with fraudsters.

Mobile scams. Your smartphone or iPhone® is a minicomputer. It can be hacked and manipulated by criminals who want your personal information. Frauds to watch out for when using your mobile phone include:

- **Mobile malware.** Be cautious when downloading apps from unknown sources. Around the holidays, there are many apps that promise an inside scoop about sales, coupons, etc. If you download an app from Google® PlayTM, the odds are that it has been vetted for anything suspicious. If you obtain an app from an unknown third party site, however, you may also download malware onto your phone along with it. The malware may record your user names and passwords and, if possible, steal your social security number and credit card numbers. Ransomware scams can also be executed over Android Smartphones.

- **Phony text messages.** Watch out for text messages from any number you don't recognize. Most of the email scams mentioned above can also be proffered via text message.
- **Sham websites.** Securing a Web address (URL) that is similar to one belonging to a brand name product, company or charity and setting up a website that resembles a legitimate one are relatively simple tasks. Criminals sometimes establish phony websites as a place to execute a number of different scams.
- **Fake storefronts.** A phony website set up to look like a well-known or an unknown company may "sell" products or services that will never be delivered. The site collects your credit card number, PayPal funds or personal information without providing anything in return. Clicking links on these sites may also download malware onto your computer.
- **False Internet ads.** Internet ads may promise opportunities to work-from-home, obtain sought after holiday gifts or receive electronics simply by filling out surveys. Be wary of anything that sounds too good to be true.
- **Uncharitable websites.** These websites appear to belong to legitimate charities, but like the fake storefront websites, they really just want to gather your money and personal information.