10 ways to avoid holiday hacking

By Cameron Huddleston, Kiplinger's Personal Finance magazine

The bad guys are out in force this time of year. Know the risks -- and how to protect yourself against online fraud and ID theft.

It's supposed to be the season of peace and goodwill, but scammers are everywhere. Identity thieves, computer hackers and fraudsters tend to increase their efforts over the holidays because more consumers are online purchasing gifts and looking for deals, says Dave Aitel, the CEO of Immunity, a software company that creates penetration-testing products (i.e., hacking tools). Scammers also take advantage of people's generosity during the season of giving.

Aitel says that people need to watch out for these 10 threats that could put them at risk of becoming victims of fraud or ID theft during the holidays:

1. Clickjacking. This popular Facebook scam involves online games that require you to click something that moves across your computer screen. You think you're clicking on a dancing Santa, but you could instead be clicking on a concealed link that might perform actions such as making your Facebook profile information public or giving scammers access to information stored on your computer. So don't click on those dancing Santas (or any other game that pops up on your computer or gets passed around on Facebook).

2. Drive-by downloads. This is a term that refers to downloading something that you didn't realize was a malicious program or a download that occurs without your knowledge. This might happen as you are browsing the Web during the holidays and visit unfamiliar sites with ads that promise deep discounts. If the site isn't legitimate, the ads probably aren't, either. Also avoid sites that require you to download a "codec" to view a video, because this is malicious software.

3. Infections from legitimate sites. Now is prime time for hackers to infect sites that get more traffic during the holidays with pop-up ads that have viruses. Aitel recommends installing an ad blocker on your browser, such as the free Adblock Plus, or using Chrome as your browser because it's harder for hackers to infiltrate.

4. Email phishing. Your inbox might fill up with donation requests or holiday deals over the coming weeks. If these emails come from people or groups you're not familiar with, delete them; they're likely attempts to steal your personal information or con you out of big bucks. Also watch out for emails claiming to come from your credit card issuer. You might assume that they're legitimate if you've been using your card frequently to make holiday purchases. But don't respond to any emails saying that there's a problem with your card. Instead, call your company directly using the number printed on the back of your card.

5. Text-message phishing (or smishing). Be wary of text messages with donation requests, notices of too-good-to-be-true deals or even gift card offers from major retailers. There's a good chance that they're fake. If you respond, you may be prompted to divulge personal information, such as your credit card number.

6. Phony apps. Be wary of the apps you download on your phone or Facebook page. Researchers recently found that Android phones are vulnerable to text message phishing if users download infected apps. Even legitimate apps might ask for too much information. So read the list of permissions an app requests to make sure it's not asking for information you don't want to provide.

7. Fake Google results. If you do a Google search for a popular toy your kid wants for Christmas, for example, there's a good chance that some of the results will be links to fake sites or images that have viruses or malware. That's because scammers build sites based on popular search terms. When doing your holiday shopping online, stick with sites you know.

8. Forced browsing. This advanced hacker technique is used to steal your passwords when you log into your accounts using a public Wi-Fi connection. (It gets its name from a computer being forced to browse without the user's knowledge.) So don't check your accounts online at the coffee shop or other public Wi-Fi spot. Even if you're just browsing the Web using a public Wi-Fi connection, you can put yourself at risk if you've set your browser to save the passwords to your accounts. Hackers can view your browsing history, go to sites you've visited and steal passwords without you knowing.

9. Wi-Fi sniffing. This technique allows hackers to see what you're doing on your computer if you're using a public Wi-Fi source. If you surf the Web on your smartphone, use your 3G (or 4G) network connection if you can because it is more secure than Wi-Fi. To protect your laptop from hackers, sign up for a personal virtual private network service, such as Private Internet Access, to secure your computer's Internet connection.

10. Digital profiling. Your digital profile is basically what you say about yourself on social media. And thieves can make use of this information. For example, you shouldn't announce on Facebook that you'll be out of town over the holidays. You put your home at risk of a break-in or of being used by criminals as a mailing address to ship illicit packages.

Find out more information about Countrywide Pre-Paid Legal Services, Inc