Five online shopping safety tips

By Jonas Thulin

11 Dec 2013

As more shoppers go online this festive season, here are five safety tips for secure online shopping to prevent one's computer from becoming infected and/or one's banking credentials being stolen.

© momius - Fotolia.com

1. ***Unsolicited emails:*** Spammers and scammers love the holidays, because they know a large number of people on the web during that time have their wallet open and are looking for bargains. While it may be tempting to click on an email link that says, "Great Deal on iPads... 50% off!" Be careful! By clicking on that link, you could be taken to a compromised website that downloads malware onto your computer. That malware can then be used to capture your computer key strokes, download additional malware, such as fake antivirus applications or simply turn your computer into a spam generator.

What to do: If the deal looks too good to be true, it probably is. However, if you are still tempted to click on that link, place your cursor over the link (without clicking on it) and check the URL where you would be directed had you clicked on it. If you do not recognise the URL, stay far away.

2. ***Nefarious search engine results:*** Search Engine Optimisation (SEO) attacks typically occur during major events and the holiday shopping season. SEO attacks occur when cybercriminals game a search engine's ranking algorithm in order to push their malicious websites to the top of key word search lists. They might use search terms such as "Holiday Sale," or "Year End Specials." When a user clicks on the malicious link, they could be taken to a website where their computer can be immediately compromised.

What to do: As with the tip above, before you click on a link, place your cursor over it to make sure it is not redirecting you to a different site than the one advertised. Look at the context of the search result link before clicking. Often SEO attacked sites contain content that might not make sense relevant to your search words. For example, there may be many keywords grouped together on a page and not in a properly formed sentence.

3. ***Unknown online retailers:*** If you discover an online store that is offering unbelievable specials on holiday merchandise, do some digging to make sure it is a legitimate store and not a false front that will disappear later that day along with your credit card information. In addition, even if they are legitimate, you will want to make sure their site has not been unknowingly compromised by SQL injection or other server attacks. Compromised websites will not always redirect you to a malicious site, but often will phish or surreptitiously try to install other forms of malware on your computer, such as Trojans, bots, key loggers and rootkits, which are designed to harm systems and steal personal information.

What to do: Make sure your antivirus client is up-to-date, as well as intrusion prevention to help guard against exploits that often are hosted on compromised sites. Exploits will transparently infect your system through a "drive-by" attack through software security holes. If you are hit by such an attack without proper mitigation, you will likely not even know you are infected.

4. ***Beware of friends bearing unsolicited links:*** Malicious links do not always come from spam emails. They could come from your closest friend whose machine has been unknowingly compromised. The infected machine may have a botnet that has been programmed to comb through email address books and send malicious links to everyone in them. The message might say, "Hey, check out the holiday sale going on here!" or "This place is having a 50% off holiday sale!" By clicking on the link, you could be taken to a malicious website that installs malware on your system or phishes for your credit card credentials.

What to do: Use some common sense. Does your friend normally update you on when sales and/or bargains abound? If not, then a simple reply (preferably using a different communication medium) asking, "Did you mean to send me this?" is all it will take. When they say "no," you can safely delete the email and inform your friend that they may want to run a system scan of their computer, because it could be compromised.

5. ***Beware of unsecured Wi-Fi hotspots:*** If you are a holiday shopper who likes to augment online shopping with actual store browsing and like toting your notebook along for the ride so you can do quick price comparisons, do not connect to an unknown unsecure hotspot. An unsecure hotspot allows hackers to capture all data that is flowing to and from the hotspot, enabling them to intercept logins and passwords, email messages, attached documents and other personal and confidential information.

What to do: If you feel the urge to jump online while you are in town, go to familiar locations that offer secure wired or Wi-Fi connections. Remember that phishing attacks can happen cross-platform, whether you are on your laptop or smart phone; so be sure to take all of the precautions outlined in the above steps.

ABOUT THE AUTHOR

Jonas Thulin is a security consultant at Fortinet.