THE BALTIMORE SUN

Editorial: Avoid malware, phishing schemes when shopping online

DECEMBER 6, 2017, 7:20 PM

When it comes to Christmas and other holiday shopping, the internet has been a game-changer for many consumers. Shopping online allows you to easily compare prices, avoid crowds at stores and seek out hard-to-find items that make you look like a gift-giving genius.

But the increase in online shopping this time of year also leads to a proliferation of malware and spyware on people's computers and other electronic devices that can allow others to access sensitive data. Enigma Software, the makers of a popular anti-malware app, recently released data that malware infections spiked 123 percent during the Thanksgiving/Black Friday shopping weekend. That's up from 106 percent the year prior.

Baltimore was among the top 10 areas affected, seeing a 167.5 percent increase overall in malware infections during the four-day period from Black Friday to Cyber Monday.

The software company also warns that the biggest spike may be yet to come. In 2016, the biggest day for malware infections came in the middle of December, according to company spokesman Ryan Gerding.

Gerding said he believes the spike is a combination of malware makers taking advantage of people’s habits to trick them into clicking links that cause computer infections and more people shopping on the internet than ever before — the National Retail Federation estimated online sales for the holidays would be up 11 to 15 percent in 2017.

"Simply put, the bad guys know more people will be online looking for deals and checking on orders, and they have stepped up their attacks,” he said.

One way online crooks might be trying to take advantage of consumers is through sophisticated phishing emails that look like they come from legitimate online retailers or companies.

One such scheme, ironically, is to make it look like an account has already been compromised. Users will get what appears to be an email receipt for a purchase they didn’t make. If the user clicks a link to cancel the transaction, they’ll instead be taken to a site that installs malware on your computer.

If you receive an email that looks legit but doesn’t reflect a recent purchase, avoid clicking on links and instead login directly to your account with the retailer from the web browser.

Some other tips to keep in mind when shopping online or otherwise browsing the web is to be skeptical of websites that ask you to install any software before you can continue shopping — even if the software it’s asking you to install is something legitimate like your browser’s Flash player. Often, malicious software will be disguised to trick you into clicking on it.

Also, be wary of links found in social media messages on Twitter and Facebook, even if they are coming from your friends or someone you know. It’s possible, even likely, their account may have been compromised. If you get such a link, verify with that person before clicking it. (And if they have been hacked, they’ll be glad you let them know!)

It doesn’t hurt to have an anti-virus and anti-malware program on your computer. McAfee and Norton are among the most well-known and popular, but there are plenty of others out there, including Enigma’s SpyHunter. Malwarebytes and Cybereason are a few examples of free apps available.

Enjoy your holiday shopping online, just be mindful of what you click and don’t get caught in a web of malicious software.

Troop 1310 teaches container gardening

SHOW CAPTION

1 / 55

‹

Troop 1310 teaches container gardening

Glazing bowls for Empty Bowls

Tech Center to allow students from Pennsylvania into some programs

›

BE THE FIRST TO COMMENT