Malware Infections Spike in November and December—Here's How Protect Your Personal Info

BY CHERYL S. GRANT

Cyber-savvy scammers are standing by to snag our personal information and infect our devices with malware. Here's how to protec against the privacy pirates this holiday shopping season.

ISTOCK/ANDRESR

Last Thanksgiving and Black Friday saw more online shoppersthan in-store shoppers for the first time ever, eclipsing the $5 billion mark in online sales. Sadly, unless those 108.5 million shoppers were vigilant, they may have put themselves at risk for acquiring malware. Not to be confused with spyware or adware, malware is malicious software that is designed to damage or access a computer without the owner being aware. Hackers may even look at you through your computer camera. They could peruse your personal photos and steal data such as your home address, bank codes, credit card numbers, and Social Security number; possibly even your entire identity. Or they could install a virus that systematically erases your entire hard drive. The scariest thing: You're at risk every time you click to complete a purchase. Here are 10 times to never ever use your credit card.

As we once again ramp up for holiday shopping — the National Retail Federation estimates that online sales this holiday season will increase between 3.2 percent and 3.8 percent over last year's spending — malware creators are also ramping up. Malware infections spiked 106% from Black Friday through Cyber Monday, 2016, according to data from Enigma Software, creator of PC security software and malware fixes. "The holiday shopping season is one of the busiest times of year for the cyber crooks who spread malware," ESG spokesperson Ryan Gerding has said. "They know lots of people will be online looking for deals and tracking their purchases, and that makes those people vulnerable."

Protect your devices by keeping an eye out for these warning signs:

Spam emails and links: Though an email message might seem to offer unbelievable deals from trusted stores that you regularly shop in, it's best to go to those stores' online destinations directly. Whatever you do, do not click on any links in these types of messages because they could trigger the download of malware when opened. The same goes for messages warning about possible problems with your accounts. Instead of clicking links in emails, always go directly to your bank's website, Paypal, eBay, or whatever account these emails might be flagging, to check for any issues.

Social media: Be wary of ads for amazing discounts, giveaways, alluring photographs, or sensational stories that are posted on sites such as Facebook and Twitter. If you receive a private message with such a link, just delete it. This is the age group most likely to be taken in by phone scams — and no, it's not Baby Boomers.

Fake apps: Cyber scammers are cloning apps to resemble authentic ones from reputable retail stores, such as Coach, Moncler, and Salvatore Farragamo. Use these tips to avoid accidentally buying from an unverified app.

Phony search results: Just because a result comes up on a legitimate Google search doesn't mean the website is legitimate. Be vigilant about clicking on unfamiliar sites—especially if you see misspellings or awkward language errors. And never agree to install software in order to continue shopping, because more than likely it has malware embedded in it.

Secure your computer: Install reliable anti-spyware and anti-malware software such as SpyHunter or Avast (go directly to those websites—never install from a link in an email). They're pretty easy to set up and could save you from major heartaches and headaches in the long term. Also, make sure to scan your computer with them often and install all updates as instructed.

Here are 20 secrets cyber scammers don't want you to knowabout how they steal your money and identity.