Online shopping: How not to get scammed

Brett Sholtis , bsholtis@ydr.com 4:50 p.m. EST December 6, 2016

(Photo: Paul Kuehnel, York Daily Record)

Online shopping has come a long way. This year, about 44 percent of holiday shopping happened online during Thanksgiving weekend, according to the National Retail Federation. That amounted to 67.8 million people launching their personal information into the cyber-sphere.

Giving up your digits is safer than it used to be, but it's still possible to get scammed, said Jeremy Smith, a program director for YTI Career Institute's computer system specialist program. The computer expert provided some tips on how to stay secure while making those holiday purchases.

Look for the padlock

If you use a modern Internet browser such as Google Chrome or Firefox, you should see a little green padlock icon on the address bar of most major shopping websites you visit, Smith said. That padlock means that you're surfing the web on a secure connection. Information you may type while shopping on that website — such as your address, name and credit card number — is encrypted, meaning that hackers can't see it.

"It's basically impossible for hackers to crack that," said Smith.

The padlock is found on shopping websites such as Amazon.com, Jet.com and others. If you don't see the padlock, check to make sure you didn't misspell the web address. Sometimes, one transposed letter is all it takes to lead you to a malicious website such as the infamous "Gmial.com" site — do not go there — which promptly loads a virus onto your computer if you're unfortunate enough to have fat-fingered your way there.

Read: Amazon just opened a grocery store without a checkout line (/story/tech/news/2016/12/05/amazon-go-supermarket-no-checkout-no-cashiers-artificial-intelligence-sensors/94991612/)

Be wary of emails

It's common to receive emails from online retailers, and most of the time those emails are legitimate, Smith said.

However, it's easy for hackers to send you an email that looks like it's from a retailer but is actually an attempt to steal your personal information. Though the email may look identical to a real email from somewhere such as Amazon or Barnes & Noble, it will contain attachments which, if you click on them, could upload viruses to your computer.

Hackers may also try to get you to click on a link that will lead you to a fake shopping website — and these days, those websites can look indistinguishable from the real thing.

As a smart shopper, your job is simple, Smith said. "Anytime you get an email from your bank or any website you frequent, don't click on any links, don't click on any attachments."

Instead, go to your Internet browser and re-enter the correct website address. If you truly need to update your security information, you'll be prompted to do so when you log on to the secure website.

Mobile shoppers still at risk

This year during Cyber Monday, 23 percent of online shoppers turned to their iPhones, Kindles and other mobile devices to make purchases, according to the National Retail Federation. Those consumers aren't immune from hackers, Smith said.

"You're more likely to catch a virus on your PC or laptop, but the hackers are starting to shift their attention to the mobile landscape," Smith said.

A recent Android virus named "Gooligan" infected more than 1 million smart phones — just in time for Cyber Monday. (/story/tech/news/2016/11/30/android-malware-infects-1-million-phones-globally/94676546/) That virus uses the Google Play app store to make "micro-transactions," small purchases that often go unnoticed in your checking account but add up to big money for con artists.

If you notice that your mobile device isn't running right — if it's slow, or if there are apps on the device that you didn't download — the only sure bet for cleaning it up is to do a factory reset, Smith said. Sync up the device to save photos, videos or other data you want to keep, and wipe the slate clean. After you reset your device, the virus should be gone.

Legal, but annoying

Not all risks come from hackers. Retailers themselves may add unwanted charges to an online shoppers' bill, Smith said. Technically, the shopper "agreed" to those services, but they were so hidden in the fine print of the sales agreement that the shopper may not have noticed them.

"Sometimes, during a checkout process or while you're making a purchase, by default you're signed up for the insurance policy or the free trial of a magazine," Smith said. "So you have to be very careful and un-check a check box that would actually bill you."

In addition, shoppers need to regularly check their bank statements. Small, mysterious transactions or unwanted services could mean that something went wrong while shopping online.

Other red flags

- "Pop ups" that ask for information are almost always malicious, Smith said.
- Generic emails that claim to be from a retailer but that don't have any personalized information are likely to be an effort to trick you into giving up information.
- A phone call claiming to be from a retailer, asking for a username or password, is likely an attempt at identity theft.

Read or Share this story: http://on-ydr.co/2gOoNqN