Don't get cyber-Scrooged! Tips for safe online shopping

December 21 2016, by Bree Fowler

In this Monday, Dec. 12, 2016, photo, a person searches the internet for sales, in Miami. With the holidays fast approaching, more people are using their smartphones and other devices to get a handle on their last-minute shopping. Hackers are on the hunt too, looking to steal personal information from easy targets. But experts say a few precautions can go a long way in protecting yourself from cyber Scrooges. (AP Photo/Wilfredo Lee)

'Tis the season to be jolly—but it's also the season for identity theft,

phishing and credit card fraud.

With Christmas just days away, people are using their smartphones and other devices to get a handle on their last-minute shopping. Hackers are on the hunt as well, looking to steal personal information from easy targets.

"People just need to have their radar up, so that when they're trying to get their perfect gift to grandma's house in time for Christmas day, they're not clicking on things they shouldn't," says Michael Kaiser, executive director of the National Cyber Security Alliance.

We've written earlier on how to avoid holiday scams in general, both of the technology kind and otherwise: apne.ws/2hRZ55V . Here are some other tips for staying safe this holiday season.

___

YOU'D BETTER WATCH OUT

Make sure your phone's operating system and all the apps you use to shop are up to date. That way you'll have the fixes for any recently discovered security problems.

You should also enable multi-factor authentication in the settings on your important accounts. This is a security measure that requires you to enter a temporary code in addition to your password when signing in; services often text this code to your phone. It complicates life for hackers should they somehow manage to get your password.

Improvements in credit card fraud detection have pushed hackers to focus on stealing legitimate login credentials, so adding an extra layer of protection to these accounts is a must, says John Dickson with the

cybersecurity firm Denim Group.

And while some cybersecurity experts question the value of changing your password frequently, Dickson says it's not a bad idea this time of year.

"If you had a New Year's resolution to change your passwords, move that up by about four weeks, because this is fraudster season," Dickson says.

___

SANTA (AND HACKERS) ARE WATCHING

Nobody likes to dip into their mobile-data plan, but you might want to set aside a few gigabytes for your holiday shopping.

Signing on to free Wi-Fi at a store or coffee shop can be risky. Hackers could be lurking on the networks, ready to use that connection to steal credit-card numbers or other personal information. If you're using free Wi-Fi, at least wait till you get home to check your bank account balances, Kaiser says.

___

FEAST OF THE PHISHES

Phishing spikes during the holiday season. Emails that offer great deals on holiday gifts or donation pitches from charities could actually be attempts to steal your credit card or login information. Another popular trick: Fake emails supposedly sent by online retailers or shipping companies.

Don't click on links in these emails, as they may lead you to a fake

website that looks legitimate. Instead, type in the company's website directly.

___

CHECKING IT TWICE (OR MORE)

Shoppers need to keep a close eye on their accounts. The easiest way to do this is to use the same credit card for all of your holiday shopping. Avoid debit cards—running up a credit card balance is one thing and can be challenged; draining your life's savings is another.

Use different passwords for your various shopping accounts. That way if one is compromised, it's less likely that the others will fall to hackers as well.

____

NAUGHTY OR NICE?

Websites that advertise hot deals on popular or hard-to-find gifts are probably scams. So are those touting free or deeply discounted gift cards. Stick with e-commerce sites you know are real. Don't click on web ads.

And if something advertised on a website or social media looks too good to be true, it probably is, says Brian Reed, chief marketing officer for ZeroFox, a cybersecurity firm that focuses on social media.

Instead of getting a great deal on a North Face jacket or a free iPhone, shoppers are getting their money and personal information stolen.

Also avoid apps that promise to generate gift card codes for various

retailers, Reed says. The apps can harm your device. And, if you manage to use a code, you're committing fraud.

___

GIVING THE GIFT OF IOT

Internet-connected gadgets—whether they be a "smart" thermostat, baby monitor or a talking toy—will be under many trees this year.

But the lack of security built into many of these devices is becoming an issue. Experts worry that they could be used to breach a home or business network and let hackers access another device that holds private information.

There's no way to tell from its box how secure any given gadget is, but an online search could fill you in on previously reported problems.

Default passwords should be changed right away, if possible. Do some research to understand exactly what personal information the device is collecting and where it's being stored or sent.

Down the road, make sure your smart devices get their security updates. That includes your wireless router. If it's an older model, you're probably going to need to get them from the manufacturer's website. Newer models often send updates through apps.

And if your router is really old and not getting updates, you might want to add that to your gift list.

"If that's your gateway and it's not secure, then you're allowing people to get into all of the devices connected to it," Kaiser says.