Don't get Grinched by cybercrime during the holiday season

November 28 2015, byBree Fowler

Online fraud spikes during the holiday shopping season, as people searching for the perfect gifts take to cyberspace and head to traditional stores armed with their smartphones.

"The Pandora's box of cyberattacks is about to open," says Pete Tyrrell, chief operating officer for Digital Guardian, a Waltham, Massachusetts-based data protection firm. "The cybercriminals are getting more and more creative—and at the end of the day, it's your personal information at risk."

Here are some tips for protecting yourself and your information from online Grinches.

———

BEWARE OF GIFTS OF FREE WI-FI

It's awful tempting to sign on to a store's free Wi-Fi while you're out shopping, especially since store walls are notorious for blocking or weakening smartphone data connections. But fraudsters also may be lurking on the networks, ready to use that connection to steal credit card or other personal information.

"People may want to log on to their Best Buy or Amazon accounts to check prices, but open Wi-Fi is probably the least secure place to do that," says Michael Kaiser, executive director of the National Cyber

Security Alliance.

And never use open Wi-Fi connections to check bank account information. The last thing you want a hacker to have is a direct connection to your bank account.

If you're tech-savvy enough to use VPN software—short for "virtual private network," a technique for shutting would-be eavesdroppers out of your connection—on your phone, then free Wi-Fi is safe so long as you have the VPN on. For most people, though, it's simply best to stick to your cellular connection.

Shoppers also need to be on the lookout for less high-tech thieves when shopping online in crowded public places like coffee shops, says Nitin Bhandari, senior vice president for products at Opera Software Solutions. That means keepings your screens out of the views of others—even smartphones, which are bigger and easier to read from a distance than they used to be.

___

SWIM AWAY FROM POTENTIAL PHISH

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 shippers such as FedEx or UPS, saying that a payment for an order didn't go through, or that an order didn't ship.

Don't click on links in these emails. It could contain malware or take you to a fake website that looks very much like that of a legitimate company. Instead of getting help, you'll most likely have your personal information

stolen.

Panic over the possibility of not getting a gift in time can make people click before they think, Kaiser says. So, it's best to slow down. If you think an email is genuine, just go directly to the company in question's main website.

___

CHECK YOUR ACCOUNTS FOR "NAUGHTY" ACTIVITY

Both during and after the holidays, 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. Never use your debit card; if hackers get ahold of your number, they could clean out your bank account.

A dedicated email account can also help keep things organized.

It's also a good idea to use different user names and 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, says Tim Francis, the head of "cyber insurance" policies at Travelers.

____

IF IT LOOKS TOO GOOD TO BE TRUE ...

Websites and emails that advertise hot deals on popular or hard-to-find gifts, along with free or deeply discounted gift cards, are probably scams. "I still haven't been able to buy an iPad for $7," Tyrrell joked.

It's best to stick with e-commerce sites you know are real and go directly to those websites. Don't click on Web ads.

Shopping on the websites of companies you've previously done business with can also save you time and hassle, says Steve Platt, a vice president at credit monitoring company Experian.

Online retailers will be on the lookout for fraudsters too. That means they might be more likely to flag a transaction—and slow down your shopping—if they haven't dealt with you before.

"The more information they know about you and your purchases, the more likely you'll have a seamless experience," Platt says.