8 SCAMS to watch out for this HOLIDAY SEASON

By the end of 2015, individuals and companies had been victimized by fraud to the tune of $1.5 billion... and that number is expected to have increased in 2016. Just as you protect your home with an alarm system, you should set up defenses for your credit and identity. During the holiday season, fraudulent activity spikes, but here's how to protect yourself from the eight most common scams.

1—BIG DATA BREEDS DATA BREACHES

Big data during the holidays is great for marketers; it's a bonanza of consumer information to use to lure shoppers to Black Friday deals and the like. However, while companies wrangle in the chaos of holiday orders, scammers search for weaknesses in a company's cyber-security. According to a top executive at one of the leading credit bureaus, "Data breaches are inevitable and most consumers are vulnerable to identity theft... especially during the holidays." In fact, 25% more consumers were affected by identity theft during the holidays in 2015 than in 2014!

The best way to reduce your risk of data breaches is use cash for all your purchases. According to a survey by TransUnion, however, only 20-percent of shoppers plan to pay with cash. If you're part of the 80-percent using plastic, use a credit card instead of a debit card. You have more purchase protection using a credit card than a debit card if a data breach occurs or fraud happens.

Other protections from data breaches include:

- Using a low-limit credit card for online purchases so you can detect fraudulent activity.
- Utilizing services like PayPal to lower the risk of your card information being lost at the retailer.

2—PACKAGE THEFT

E-commerce is great for holiday shoppers... but it's also great for thieves. Last year, Insurancequotes reported that 23 million people had packages stolen at their front door!

To prevent this from happening to you, have your packages delivered to your office or delivered to a pick-up area such as a UPS store or Amazon Locker. You can also set up tracking notifications so that you know when to expect delivery.

And while you're waiting for your packages, be on the lookout for this scam: a note on the front door saying you have a package waiting for pickup. The note asks for a call, often to a pricey number that leaves you on hold for a long period while they collect premium phone rates, or it leads to a person asking for details on your personal information.

3—ONLINE SHOPPING SCAMS

Phony online stores lure shoppers in through searches and online ads, enticing you with low-priced, high-quality items. These "bargains" cost you not only money, but also hours of time trying to fight the fraudulent transaction.

To avoid the pitfalls of the fake online merchant, only purchase from retail names you know and trust. You could also Google the site and look for reviews. Yelp is a legitimate site for reviews, as is the Better Business Bureau. Before you make a purchase online, double-check that "https" appears in the URL, which signifies that the site has passed stringent security compliance standards.

4—POISONOUS HOLIDAY E-CARDS

E-cards are popular during the holidays because they're a free, fun, and easy way to catch up with friends and family members. But beware because it's just as easy for scammers to use fake e-cards to steal your personal information. A lot of fake e-cards you may get are from your hacked address book or the hacked address book of someone you know. At first glance, the card may look legitimate, but once you open it, you've been phished.

The only way to avoid this from happening is paying attention to detail. The number one tell of a fake e-card is any kind of misspelling. The URL will have a subtle misspelled word or your friend's name is misspelled.

5—FAKE APPS

ConsumerAffairs is reporting a huge spike in fake apps. Scammers are using fake retail and product apps found in Apple's App Store to steal unsuspecting consumers' financial information. Many of these thieves rip off company or brand logos to make the fake app look real. So before you get that convenient retail or product app, make sure it's legit.

Just as with fake e-cards, fake apps will seem normal until you start looking at the details. Before you download that convenient retail or product app, make sure you check for the following:

- A nonsensical description
- No reviews
- No history of previous versions

6—GIFT CARD SCAMMERS

Scam artists skim or copy the codes on the back of gift cards before they're bought. After the card has been activated, the scammers drain the card's funds.

To prevent yourself from becoming a victim of compromised gift cards, buy gift cards displayed behind store counters, make sure preloaded cards are still loaded, and make sure the protective scratch-off strip is flawless.

7—MALICIOUS CHARITIES

During the holiday season we all feel an extra sense of giving. Grifters and thieves play on this sensibility by creating false charities and hitting you up on Twitter, Instagram, and in your e-mail inbox.

There are online resources to help you verify the legitimacy of charities. The website Charity Navigator is a non-profit organization that rates over 8,000 U.S-based charities operating throughout the world. Another way to get free reviews and evaluations on national charities is through the Better Business Bureau's Wise Giving Alliance.

8—CORRUPTED WI-FI

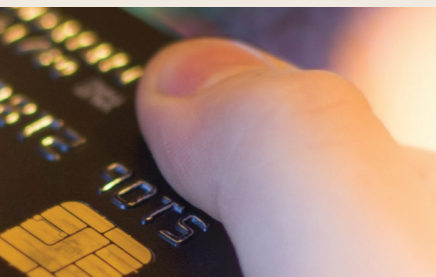
You'll probably hit the mall this holiday for some in-person price checking, and you'll probably have your smart-phone, laptop, or tablet with you. Please be careful because skimmers and scammers love to manipulate Wi-Fi signals in places like malls and coffee shops to gather your financial information. These people create Wi-Fi signals that mimic the signal you use, then hack your info when you connect to it.

To protect yourself from Wi-Fi manipulators, just don't make online purchases with your credit or debit card when you're in a public space.

WHO SHOULD YOU TURN TO?

If you catch the trouble soon enough, credit or identity fraud can be an inconvenience. If you don't, however, one instance can have long-term impacts. If, for example, someone bought an appliance using your name while you were trying to refinance your mortgage, then you might not get approved for the loan!

If you're curious to know if you've been affected, or if you know your credit is in disrepair and need help fixing it, please let us know so we can refer you to our recommended professionals.



Name
Company
Phone
Email