How to Avoid the Busy Holiday Scamming Season

You're not the only one joyfully anticipating the holiday season. Cyber criminals are all aflutter, too, as they look forward to the killing they'll make ripping off innocent shoppers like you. Here are some of the most common ways these thieves operate, because awareness can help you avoid becoming yet another victim.

Antisocial media

Beware those enticing ads that turn up on Facebook and other social media sites offering vouchers, gift cards and deep discounts, as well as the online surveys these ads often link to. These offers are often only empty promises designed to steal your personal information.

Additionally, if you receive concert, theater or sporting event tickets as a gift, never post pictures of them online. Cyber thieves spend lots of time monitoring social media, just waiting for the opportunity to create phony tickets they can resell from your barcode image. If your ticket is resold, you might just find yourself out of a seat on the night of your event. It's also unwise to post live from an event that gives criminals a heads-up that your home is empty and ripe for picking. Better to wait until the next day to post about the wonderful time you had.

Pandora's inbox

It may be a mystery to you how cyber thieves got your private email address, but it's chillingly clear they're up to no good. Your inbox may fill up with all kinds of legitimate-looking product offers and delivery notices this holiday season, but clicking on links of bogus ones or entering personal information on the linked sites can provide criminals with the opportunity to steal your identity.

Apps are far from immune

With mobile apps available for just about everything, it's a sad sign of the times that certain free mobile apps (often disguised as games) have been specifically designed to steal personal information from your phone. This is a particularly scary development since many people use their phones to secure their cars and homes. For this reason, only install apps from familiar companies and, at the very least, find a third-party review from a trusted site if you're interested in an app from an unfamiliar source.

USB Trojan horses

Lots of people use portable USB drives, which makes it all the more important to avoid those being distributed as giveaways this holiday season unless they're from a trusted source. These innocent-looking devices are often used as a method of introducing malware to computers.

Gifts that keep on giving ... to criminals

A spirit of generosity is traditional at holiday time, but if you're not careful, your donations may never make it to the needy. Fake charities that skillfully tug at your heartstrings abound at this time of year, just waiting for

you to willingly give your hard-earned cash to scammers. Before donating, be sure to check out charities thoroughly, to make sure that they're not only legitimate, but also that they allocate the bulk of funds toward their causes rather than “administrative costs.”

Tips to avoid holiday scams

These strategies will also help keep you a step ahead of scammers:

- Only shop online with reputable businesses you trust, using secure websites with an address that begins with https.
- Don't shop or bank over public Wi-Fi.
- Protect your credit card privacy by covering your account number with your hand when shopping in public.
- Don't respond to suspicious unsolicited calls or emails. Only open email attachments from senders you trust, and contact businesses only through their official websites, phone numbers or email addresses.
- Monitor your credit to catch fraud at its earliest stages.

Scammers may be smart, but you can still outsmart them. A little foreknowledge and caution go a long way toward ensuring you'll enjoy a safe and memorable holiday season.

© Copyright 2016 NerdWallet, Inc. All Rights Reserved