2020 Holiday Shopping Scams to Look Out For

October 12, 2020 - Tis the season to shop! In fact, it starts today. Walmart is kicking off the holidays with discounts, one day ahead of Amazon's Prime Day sales. And all of that means that the crooks will be out in droves for the rest of this year, trying to steal your credit card, banking and personal information. Letting your guard down could easily cast you into the realm of identity theft and fraud victims. Here are a few of the scams to be on the lookout for.

Secret Shopper Scam

This scam is simple to pull off and those who are unemployed or having financial difficulty are especially vulnerable. With the advent of COVID 19, that means millions of people who weren't vulnerable last year will be this time around.

Targeted victims of this scam receive a letter in the mail telling them that they have been selected to be a secret-shopper. A cashier's check accompanies the letter. They are told to deposit the check in their bank account and go shopping at the selected store. They can keep the merchandise that the purchase but any unused funds are to be sent back to the company that selected them by sending a personal check or money order.

What the victims discover is that the cashier's check they received is fake. Any money that they have sent the fraudsters is long gone, and they have no chance of getting it back. And if the victim sent a personal check, even if they manage to cancel the check in time to stop it from being cashed, the crooks now have the victim's full name, address, possibly their phone number and their checking account number & bank routing number. Anyone who finds themselves in this situation would be wise to close their old account and open a new one.

Phony Online Bargain Shopping Sites

This is an oldy, but a goody, that happens every year. That's because it works for the crooks behind it. And now that Prime Day is a thing, there is a very good chance that people will start running into fake websites that look just like Amazon, Walmart, Target and other well-known retailers to rip them off.

What a bargain! You just found that new cell phone that you have been looking for at 25% of the retail price. You pull out your credit card and buy it online. Now all you have to do is wait for it to show up! Actually, while you're waiting, you may also find that your credit card gets tapped-out. That's because the site you just purchased from wasn't actually from that well-known retailer you thought it was. Or it wasn't a legitimate site from a new bargain retailer. Either way, it was a fraud.

A few things to look out for here. If you've never heard of the retailer you are buying from, then do a little research first. They may be perfectly good, but maybe not. Also, if their domain name ends in something that looks oddâ€¦ like .co.in, .co.cn or .co.ru, you need to be very careful. These domains go outside of the United States. These particular examples are for India, China and Russia. Again, you may be going to a site that is perfectly good but unless you know for sure, you should probably find another retailer.

Don't just look at the domain name ending of the site you start out on. Hover over any links that you are about to click on for just a second or two. You should be able to see the address that you are about to be taken to. If it ends with anything but .com, .org or .net, think twice before you click. This holds true even if you typed the address of the site you were going to into the address bar yourself. People fat-finger their typing all the time and crooks know this. Because of this they often purchase domains that are one or two letters off from those of legitimate retailers. So, it's a good habit to look carefully at the links you are clicking on all the time.

And remember that it doesn't matter if you arrived at the site through a paid advertisement on a major search engine. Search sites don't necessarily check out all of their advertisers to see if they are legitimate. It's up to you to protect yourself.

Discounted Gift Cards

Some merchants will use discounted gift cards for marketing. For instance, you can go into Costco and purchase gift cards from a wide variety of merchants at a significant discount.

But you can also find discounted gift cards offered for sale on auction sites, public bulletin boards and in classified ads. Be very careful when considering these offers. In some cases, the cards are counterfeit. In others, they are legitimate cards that have been stolen or which all of the value of the card has already been used. If you get caught up in this scam, you have virtually no chance of getting your money back. And if you purchased the cards by furnishing a credit card number of your own, you could find yourself open to further victimization including identity theft.

On top of that, you'll be very embarrassed when you give a worthless card to your boss, friend or family member. There is really no way to keep the fact that you've been scammed a secret with this particular scam.

Online Shopping Coupons

This one involves the crooks offering coupons that can be redeemed online or in brick and mortar stores. Many of these scams use the names of well-known retailers. Only one catch. To get the coupon you need to provide virtually all of your personally identifiable information to the person or company that is offering you this great deal.

Again, falling for this puts you at risk for identity theft. And the coupon you receiveâ€¦ wellâ€¦ it's a fraud.
Other Scams

As every year, there are a wide variety of additional scams circulating; especially on the internet. These include phishing scams. With any of the scams listed here, there are several tell-tales signs that you should look for.
Misspellings

Mail messages from companies that you already do business with addressed to "Dear Sir" or which don't use your name. Also, in the case of snail-mail, messages that have an envelope addressed to "resident".

Websites with odd addresses or which have an addresses, or very long addresses. There are a lot of legitimate sites that do this, but this can also be a sign that the address is spoofed.

Any promotion that is so time sensitive that you don't have time to think too much about it. For instance, you get a telemarketing call offering a lavish vacation at a fantastic price but you have to make your decision to purchase right then and there. Even if you recognize the name of the company offering the deal - and there is a good chance that you will - walk away. You actually have no idea who the person at the other end of the phone line is or if they actually work for the company they claim to. And remember, you can't trust the phone number information that pops up on your caller ID for this either. Any criminal on the other end of the line doesn't even need to be particularly sophisticated to fake the caller identification information that you see.

And finally, any deal that sounds too good to be true. Yes, this is an old adage but it is as true today as ever. Do your homework before accepting any such deal.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS