

## Holiday Shopping Scams to Look Out For

December 12, 2012 - Tis the season to be jollyâ€¦ for crooks that is! That's because shoppers are out in droves, passing their credit cards to virtually anyone who has something to sell. Let's face it. It is easy to let your guard down at this time of the year. But doing so could be costly. In the worst cases, you could be defrauded, have no hope of recovering the money you've lost, and find out that your identity has been stolen. Here are a few scams to be on the lookout for.

### Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();
```

### Secret Shopper Scam

This scam is simple to pull off and those who are unemployed or having financial difficulty are especially vulnerable.

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. 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

What a bargain! You just found that new stereo 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 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.

### 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.

### 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.

### Mobile Phone Applications

This is a newer scam that is growing in popularity. As smart phones have become more common, crooks have taken notice. And most smart phones are more vulnerable to hacking than standard computers. If you have installed applications on your phone, if any of them came from unknown vendors, you may be in trouble. Malware applications of this type can log your key strokes and see everything you are doing on your phone. That includes making purchases or doing your online banking.

If you periodically sync your phone with your PC, then it could also infect your computer.

Either way, you may find your identity stolen and your bank account wiped out. And if you have a business bank account, you could wind up responsible for all of your losses. That's because even though consumer bank accounts have some legal protection from fraud of this type, businesses are required to take precautions to prevent this type of fraud. Installing malware on your phone or computer will likely mean that you didn't take those precautions and any money taken out of your accounts will be your loss and not the bank's.

### 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 - both snail mail and email - 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.

Just remember that it is up to you as the buyer to protect yourself.

byJim 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 me on Twitter:

Follow ACCESS