

5. Check the company out. Only do business with companies that provide a physical address and a phone number. If you're suspicious, trust your gut feelings.  
\***Always**\* ask for references and check them carefully. A reputable company will be pleased to provide you with lots of references.
6. Only do business with companies that offer a strong guarantee and/or warranty. Ask the company what will happen if you want to return the product or service. Most reputable companies offer strong guarantees and stand behind their products, especially online.
7. Keep good records. Always print out a copy of any online products or services you purchase. Make sure you print out the Web page (including the Web address URL), any emails with the email address, and any other relevant information, including the date and time that you saw the offer and made the purchase. Save this information in case you need it later.
8. Be careful, but don't be paranoid. After all, most businesses on the Web are legitimate. Shopping online can provide tremendous advantages including the safety of not venturing out to shop! So don't throw the baby out with the bath water. Use good judgment, be careful, follow these tips, and you probably won't have any problems.



**Ophelia W. Livingston - Owner**  
**OWL Risk Management Consulting**  
 150 N Steele St, Suite 102 ♦ Sanford, NC  
 Phone: 919-208-8736 ♦ 1-866-579-7475  
 Email: [owriskmanagement@gmail.com](mailto:owriskmanagement@gmail.com)  
 Website: [www.owlrisk.com](http://www.owlrisk.com)



## Raising Awareness:

### Avoiding Fraud and Scams During The Holiday Season by Ophelia W. Livingston – MBA, MSIS, CISSP, CGRCM

#### Word of mouth is fraud's worst enemy!

The holidays are traditionally a time of giving, yet they're also a time when crooks try to take advantage of consumers. During the holiday season, scams targeting your pocketbook tend to pop up more frequently, so please be aware! Listed below are several fraud and scams that are circling around and making stops in your inbox and/or mailbox.



#### Holiday Electronic Greeting Cards

Seems harmless, right? How could a nice card of caterpillars hugging hurt anyone? Well, they've become so popular that scam artists have started using them as bait for installing malware on your computer. This is especially true around holiday times – Christmas, Valentine's Day, Mothers' Day, etc. when millions of people send or receive e-greeting cards and e-gift cards. Here's how it works:

You receive an email letting you know that "a friend" has sent you a holiday greeting card. When you click the link to open the card, you are either directed to a site with malware on it, or you'll be asked to

install a video plug-in or some other kind of software so you can view the card.

## SMISHING

"Smishing" is the newest twist on "phishing" - when you get an email from a supposedly trustworthy source like your bank or PayPal, claiming there's a problem with your account. The scammers hope you'll click the link in the scam email and enter in all your account information that they in turn use to steal your money.

Instead of an email, the "smishers" send you an SMS text message to your phone. The text says there's something wrong with your account and they provide a phone number they hope you'll call and then be duped into providing all your information. How can you prevent getting "smished"? Do your research. Before even thinking about calling the number, **Google it**. If it's a legitimate number, it should match the information on the financial institution's official website. If it's a scam, you'll probably uncover websites full of other people who also got "smished" and want to talk about it.



### Nigerian Email Scam

This scam has been used for over ten years and is sent out to victims via letter, e-mail, and fax. It consists of a message stating the sender has a large sum of money, usually around 35 million, and needs help transferring it out of Nigeria, or some other place. As a reward for your help, the sender promises to pay you a few million dollars.

## Eight (8) tips for shopping safely online during the holiday season

1. Use common sense. This seems obvious, but people don't always do it. Further, if you have a gut feeling that something isn't legitimate, you're probably right.
2. If possible, pay by credit card rather than by check or money order. Here's why: If you use your credit card to make a purchase and you encounter a problem -- and the company won't fix it -- you can notify (in writing) the bank that issues your credit card that you are disputing the charge, and you don't have to pay the charge while your dispute is being investigated. And, if the company doesn't deliver the item or they are a scam, you're in a much better position to get your money back.
3. Don't buy anything from companies that use bulk email solicitations. We recently heard from a colleague that she had purchased a lot of stuff on the Net, and had not even received about 60% of it! We were baffled. We, too, order a lot on the Net, and have *\*never\** not received an item. Investigating further, we discovered that all of the items which she had not received were promoted using bulk email. Every item she ordered from a Web site was, in fact, delivered. Since we have a strict policy never to buy from any company that spams, we had never encountered this problem.

Checking further, we discovered that other people who bought from companies that spam had similar experiences. So, this is another reason not to buy from companies which use bulk email -- there is a high probability you won't even receive the products you ordered!

1. If you're a shopper, beware of being short-changed, either intentionally or unintentionally. Both are easy to do in the frantic atmosphere at the cash register at this time of year.
2. And if you're the cashier, beware the flimflam, in which the scammer gives you a high-value bill then tries to change it for a smaller one and generally messes around until you lose track of what's going on. Again, there's often an accomplice.

How to avoid them: Have a fairly clear idea of the total cost before you go to the register and, if you can't make the right money, know what size of bill you'll use and how much change to expect. Don't move away from the register until you've checked your change and your receipt.

If you're a cashier, simply don't allow yourself to be pressured at the register. If you feel yourself getting confused, call a halt and, if necessary, call a supervisor.

### Charity-related holiday scams

The main scam: Holidays are just the best time for scammers to tug on our heartstrings. And the most likely place you'll encounter them is when they rattle a collection box in front of you either as you do your shopping or at your front door.

They may use all kinds of props to fool you, wearing seasonal costumes, dressed in familiar uniforms, wearing badges or carrying some other kind of bogus authorization. Often too,  
use kids to convince you they're genuine.

How to avoid it: If you don't have time to check out how genuine the collector is, simply don't give. If you want to help them, find the charity name and donate directly. Look for Salvation Army and other collectors actually inside stores they are a safer bet.

Once you respond stating your willingness to help, the sender explains that there are transfer fees for the transaction, and that you'll need to pay them. Surprise!! You get deeper and deeper into the scam as the money supposedly gets closer and closer to your bank account, but can't seem to quite get there without an increasing amount of money from you. These emails are constantly being modified. A new one message supposedly comes from a rich Iraqi businessman trying to get 120 million dollars out of the country. Here's a sample:

"We are christian and my father happens to be one of the few rich christian in iraq. One thing we ask from you, on behalf of my mother and sisters, is to please indicate your interest in helping us secure a safe place for the bulk of our fathers funds in the bank over here before the tyrant iraqi government clamp on it.

To learn more about Nigerian Email scams go to:

<http://www.nigerianemailscam.com/>



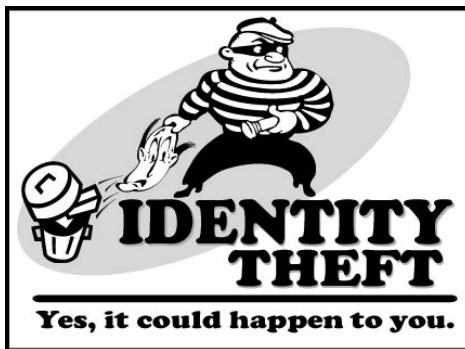
### Auction Fraud (eBay and Yahoo Auctions)

Auction fraud was the second most reported consumer fraud complaint to the FTC, totaling 51,000 auction complaints in 2002. The fraud is simple - put up a fake ad on eBay, let someone "win" the bid and send in their money, but never send out the merchandise. To learn more visit [www.scam.com](http://www.scam.com)

### **"You've Won a Prize!" Lottery Scam**

We all want to be winners, but if someone calls you on the telephone and offers you the chance to receive a "major" credit card, a prize, or other valuable item, but asks you for personal data -- such as your Social Security number, credit card number or expiration date, or mother's maiden name -- ask them to send you a written application form.

If they won't do it, tell them you're not interested and hang up. If they will, review the application carefully when you receive it and make sure it's going to a company or financial institution that's well-known and reputable. The Better Business Bureau can give you information about businesses that have been the subject of complaints.



### **Phony Identity Theft Protection or Credit Repair Scams**

The Federal Trade Commission has warned that some companies that claim to be identity theft prevention services are scam artists trying to get your driver's license

number, mother's maiden name, Social Security number and credit and bank account numbers. Don't ever give out any personal information over the phone or online unless you are familiar with the business that is asking for it. If you are unsure about a firm, check it out with the Better Business Bureau. Credit repair scams offer to erase accurate negative information from your credit file so you can qualify for a credit card, auto loan, home mortgage, or a job.

The scam: The scam artists who promote these services can't deliver. Only time, a deliberate effort, and a personal debt repayment plan will improve your credit. The companies that advertise credit repair services appeal to consumers with poor credit histories. Not only can't they provide you with a clean credit record, but they also may be encouraging you to violate federal law. If you follow their advice by lying on a loan or credit application, misrepresenting your Social Security number, or getting an Employer Identification Number from the Internal Revenue Service under false pretenses, you will be committing fraud.

### **"Make Millions Stuffing Envelopes!" Scam**

These business opportunities make it sound easy to start a business that will bring lots of income without much work or cash outlay. The solicitations trumpet unbelievable earnings claims of \$140 a day, \$1,000 a day, or more, and claim that the business doesn't involve selling, meetings, or personal contact with others, or that someone else will do all the work.

Many business opportunity solicitations claim to offer a way to make money in an Internet-related business. Short on details but long on promises, these messages usually offer a telephone number to call for more information. In many cases, you'll be told to leave your name and telephone number so that a salesperson can call you back with the sales pitch. The scam: Many of these are illegal pyramid schemes masquerading as legitimate opportunities to earn money.

### **Holiday scams at the cash register**

The mains scams: There are two (2) here, depending on which side of the counter you're standing.