



Protect yourself from Cyber Grinches

Kelli Tarala

originally printed December, 2009

This time of year, everyone is looking for good sales for Holiday shopping. Many of us will be looking for irresistible deals at online retailers like Amazon.com or Buy.com. With this increased activity during the holiday shopping season, cyber crimes are expected to be high through the holiday shopping season. Since the October to December timeframe will be a key money-making season for today's financially motivated cyber criminals, we need to protect ourselves during any online shopping experiences.

In this article, we are going to examine how shoppers fall victim to cybercrimes, what precautions shoppers should take, and what action to take if something goes wrong.

How can I fall victim?

Unfortunately, there are many ways to fall victim to cybercriminals. They are financially driven and well organized. While we are not going to put them out of business, by taking some basic steps, we can make it difficult for them to trick or con us.

The first step is using email in a smart, suspicious way. If you do not know the person who sent you an email, do not open it and read it! While it is tempting to open it and see what it, that is exactly what the cybercriminal wants you to do. Another tempting area for most people is opening Holiday emails with games or cute pictures. Those holiday related

items generally hide bad software designed to compromise the security of your computer. These malicious emails can contain viruses and software that creates backdoor access to your computer system.

Another potential email threat involves emails that look like sales flyers. Legitimate companies send out emails regarding sales and coupons to potential customers. These emails often contain links to coupons on a website. Cyber criminals can also send out fake emails that look identical to legitimate companies' communications. When criminals send SPAM posing as legitimate companies, this is known as phishing. The word phishing is a variant of fishing and alludes to bait used to "catch" passwords and financial information. This risk is that a customer enters their credit card at this bogus website, and then cybercriminals use that credit card for more criminal activity.

If you have elected to receive sales emails or newsletters from companies selling on the Internet, never click on a link in an email. If you want more information, go directly to the company's website. Open your web browser and type in the address for the company, i.e. www.amazon.com.

Ok, you are willing to shop online. What precautions should you take?



Securing our Digital Future

Kelli Tarala

originally printed July 9, 2009

If you have decided to shop online this holiday season, here are some quick tips to protect your identity and credit card information.

- Shop with reputable brands
- Never enter personal information in a pop up window. Pop up windows may be generated by malicious software designed to capture your personal and financial information.
- Do not use your debit card. Use a credit card instead. There are more protections for credit card transactions than debit cards.
- Use multiple complex passwords for online shopping sites
- Look for the “s in https” at the top of the screen
- Check the privacy policy. Will this company sell your email to other companies? Will the company protect your personal information?

What to do when something goes wrong, or just doesn't feel right

As you are shopping online this season and taking precautions to protect your information, you still may become a victim of cybercrime. If you notice that your credit card was billed more than the amount you were expecting, or the merchandise does not arrive when promised, here are some steps to take to resolve these issues:

- Call the merchant. All legitimate companies will have a Contact Us Page on their website. It should contain a physical address, a telephone number, and email address.
- If you cannot work on the issue with the merchant, contact the credit card company and report the fraud.
- Contest the charges with the credit card company
- Contact the Better Business Bureau for further assistance. Their website is address <http://welcome.bbb.org/>

Vigilance

During this Holiday season, it is especially important to monitor your credit report. Many victims of cybercrimes do not realize they are victims until they have lost money. It is important to monitor your credit report and/or credit status on a regular basis to quickly spot anything unusual. Credit reporting agencies such as Equifax, Experian and TransUnion are good resources to utilize.

Have a happy Holiday season and be safe online!

Article reprinted courtesy

