Monthly Security Tips

NEWSLETTER

November 2008 Volume 3, Issue 11

Internet Shopping – How to Enhance Your Security Online

From the Desk of Darrell Davis

The Holidays are Approaching – Help Protect Yourself and Shop Smart!

The holiday shopping season is upon us and the volume of online shopping is increasing. According to some estimates, holiday e-commerce spending totaled $29 Billion in 2007, an increase from $24 billion in 2006. While online shopping can be convenient and time-saving, you must shop smart and take precautions to mitigate the risks.

Below are some helpful tips to follow for a safe online shopping experience:

- ***Enhance the security of your computer***. Be sure to install a firewall and make sure your computer has the most current anti-virus and anti-spyware software before you begin your online shopping. Set your default settings on your computer to "auto update."

- ***Use strong passwords***. When creating passwords for online accounts, use at least eight characters, with numbers, special characters, and upper and lower case letters. Don't use the same passwords for online shopping websites that you use for logging onto your computer. Never share your login and/or password.

- ***Guard the security of your transaction***. When submitting your purchase information, look for the "lock" icon on the browser's status bar and be sure "https" or "shttp" appears in the website's address bar. The "s" stands for "secure."

- ***Don't email your financial information.*** Clear-text emails are not a secure method of transmitting financial information such as your credit card, checking account, or Social Security numbers.

- ***Keep a paper trail and check your credit card and bank statements regularly***. Print and save records of your online transactions, including the product description and price, the online receipt, and copies of every email you send or receive from the seller. Read your credit card and bank statements as you receive them and be on the lookout for unauthorized charges.

- ***Don't respond to pop-up messages***. If you get an email or pop-up message while you're browsing, don't reply or click on the link in the message, especially if it is asking for personal or financial information. Legitimate organizations don't ask for this information in these ways.

- ***Check the privacy policy.*** Know what information the merchant is collecting about you, how it will be used, and if it will be shared or sold to others. You can do this by checking the web site to make sure there is a privacy policy posted, and that you're comfortable with the way your personal information is treated under that policy. Look for seals from privacy enforcement organizations like TRUSTe or the Better Business Bureau (BBBOnLine). Be suspicious if you're asked to supply personal information not needed to make a purchase, such as your Social Security number, mother's maiden name or other personal information.

- ***Limit your online shopping to merchants you know and trust.*** If you have questions about a merchant, verify it with the Better Business Bureau or the Federal Trade Commission.

- ***Pay by credit card.*** Credit or charge card transactions are protected by the Fair Credit Billing Act. (Debit cards are covered under the Electronic Funds Transfer Act, but the potential protections provided will depend upon when you report the error, loss or unauthorized use.) Under the Fair Credit Billing Act, in the event of unauthorized use of your credit or charge card, you generally would be held liable only for the first $50 in charges. Some companies offer an online shopping guarantee that ensures you will not be held responsible for any unauthorized charges made online, and some cards may provide additional warranty, return, and/or purchase protection benefits.

- ***Use temporary account authorizations when available*.** Some credit card companies offer virtual or temporary credit card authorization numbers. This kind of service gives you use of a secure and unique account number for each online transaction. These numbers are often issued for a short period of time and cannot be used after that period. Contact your credit card company to see if they offer this service.

- ***Know who you are doing business with before placing your order***. Confirm the online seller's physical address and phone number in case you have questions or problems.

What to do if you are a victim of online fraud or encounter problems with the online shopping site:

If you have problems during a transaction, you can contact the seller, buyer or site operator directly. If those attempts are not successful, you may wish to file a complaint with the following entities:

- the Attorney General's office in your state
- your county or state consumer protection agency
- the Better Business Bureau at: www.bbb.org
- the Federal Trade Commission at: www.ftc.gov/

For more information about secure online shopping, please visit the following sites:

- **OnGuard Online**: www.onguardonline.gov/topics/online-shopping.aspx
- **US-CERT**: www.us-cert.gov/cas/tips/ST07-001.html
- **StaySafeOnline** www.staysafeonline.org/
- **Federal Trade Commission**: www.ftc.gov/opa/2008/11/smartshopping.shtm and www.ftc.gov/bcp/menus/consumer/tech/online.shtm
- **National Consumer League's Internet Fraud Watch**: www.fraud.org/tips/internet/
- **WatchGuard:** www.watchguard.com/infocenter/editorial/18714.asp
- **Online Cyber Safety:** www.bsacybersafety.com/video/

For more monthly cyber security newsletter tips visit:
www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC

www.msisac.org