Enterprise Security
Monthly Cyber Security Tips
NEWSLETTER

November 2009 Volume 4, Issue 11

Online Holiday Shopping Tips

Online Holiday Shopping Tips

The holiday season is approaching quickly and many of us will be shopping online. comScore estimates that in one day alone last year --Cyber Monday on December 1--$846 million was spent in online shopping, marking a 15% jump from 2007. With the increased volume of online shopping, it's important that consumers understand the potential security risks and know how to protect themselves and their information.

The following tips are provided to help promote a safe, secure online shopping experience:

- ***Secure your computer***. Make sure your computer has the latest security updates installed. Check that your anti-virus/anti-spyware software is running and receiving automatic updates. If you haven't already done so, install a firewall before you begin your online shopping.

- ***Upgrade your browser.*** Upgrade your Internet browser to the most recent version available. Review the browser's security settings. Apply the highest level of security available that still gives you the functionality you need.

- ***Ignore pop-up messages***. Set your browser to block pop-up messages. If you do receive one, click on the "X" at the top right corner of the title bar to close the pop-up message.

- ***Secure your transactions***. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the webpage is encrypted. Some browsers can be set to warn the user if they are submitting information that is not encrypted.

- ***Use strong passwords***. Create strong 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 home or work computer. Never share your login and/or password.

- ***Do not e-mail sensitive data.*** Never e-mail credit card or other financial/sensitive information. E-mail is like sending a postcard and other people have the potential to read it.

- ***Do not use public computers or public wireless to conduct transactions.*** Don't use public computers or public wireless for your online shopping. Public computers may contain malicious software that steals your credit card information when you place your order. Criminals may be monitoring public wireless for credit card numbers and other confidential information.

- ***Review privacy policies.*** Review the privacy policy for the website/merchant you are visiting. Know what information the merchant is collecting about you, how it will be used, and if it will be

shared or sold to others.

- ***Make payments securely.*** Pay by credit card rather than debit card. Credit/charge card transactions are protected by the Fair Credit Billing Act. Cardholders are typically only liable for the first $50 in unauthorized charges. If online criminals obtain your debit card information they have the potential to empty your bank account.

- ***Use temporary account authorizations*.** Some credit card companies offer virtual or temporary credit card numbers. This service gives you a temporary account number for online transactions. These numbers are issued for a short period of time and cannot be used after that period.

- ***Select merchants carefully.*** Limit your online shopping to merchants you know and trust. Confirm the online seller's physical address and phone number in case you have questions or problems. If you have questions about a merchant check with the Better Business Bureau or the Federal Trade Commission.

- ***Keep a record***. Keep a record of your online transactions, including the product description and price, the online receipt, and copies of every e-mail you send or receive from the seller. Review your credit card and bank statements for unauthorized charges.

What to do if you encounter problems with an online shopping site:

If you have problems shopping online contact the seller or site operator directly. If those attempts are not successful, you may wish to contact 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 additional information about safe online shopping, please visit the following sites:

- **US-CERT:** www.us-cert.gov/cas/tips/ST07-001.html
- **National Cyber Security Alliance:** www.staysafeonline.org/content/online-shopping
- **OnGuard Online**: www.onguardonline.gov/topics/online-shopping.aspx
- **Online Cyber Safety:** www.bsacybersafety.com/video/
- **Microsoft:** www.microsoft.com/protect/fraud/finances/shopping_us.aspx

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