State of Oklahoma

NEWSLETTER

November 2011 Volume 6, Issue 11

Tips for Secure Shopping Online During the Holiday Season

From the Desk of CPT Jeff Elliott, Oklahoma Office of Homeland Security

As the holiday season draws near, an increasing number of people will be doing their shopping in cyber space. Last year, online shopping expenditures in the U.S. reached a record $32.6 billion for the November-December period – marking a 12% jump from 2009. In fact, an estimated $1 billon was spent online in a single day--Cyber Monday 2010 (the Monday following Black Friday), according to comScore.* 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.

Below are some tips to facilitate a more secure online shopping experience:

1. ***Secure your computer.*** Keep your operating system and application software updated/patched. Be sure to check that your anti-virus/anti-spyware software is running and receiving automatic updates. If you haven't already done so, confirm that your firewall is enabled.

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

3. ***Secure your online transactions***. Secure Sockets Layer (SSL) is a technology to encrypt the credit card information that you send over the Internet. If you submit your financial information through an organization's website, be sure to look for indicators that the site is secure. Look for 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 communication with the webpage is encrypted.

4. ***Use strong passwords***. If you need to create an account using a password with the merchant, be sure to create a strong password. 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 any other account. Never share your login and/or password.

5. ***Avoid scams and fraud.*** Don't ever give your financial information or personal information over e-mail, text or by phone. Be aware of unsolicited communications purporting to represent charities. Always think before you click on e-mails you receive asking for donations and contact the organization directly to verify the request.

6. ***Do not use public computers or public wireless to conduct transactions.*** Do not 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 networks for credit card numbers and other confidential information.

7. ***Ignore pop-up messages***. Set your browser to block pop-up messages. If you get an e-mail or pop-up message that asks for your financial information while you're browsing, don't reply or follow the link. Legitimate companies won't ask for financial information in a pop-up message. Close out of the pop-up message by closing out of the browser.

8. ***Pay by credit card.*** Pay by credit card rather than debit card, as credit cards are protected by the **Fair Credit Billing Act** and may reduce your liability if your information was used improperly.

9. ***Keep a paper trail***. Print or save records of your online transactions, including the product description and price, the online receipt, and the e-mails you send and receive from the seller. Carefully review your credit card statements as soon as you receive them to confirm that all charges are legitimate. Contact your credit card company immediately if you have unauthorized charges on your account.

10. ***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 stored, how it will be used, and if it will be shared or sold to others.

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

Contact the seller or the site operator directly to resolve any issues. You may also contact the following:

- The Attorney General's office in your state www.naag.org
- Your county or state consumer protection agency www.usa.gov/topics/consumer.shtml
- The Better Business Bureau www.bbb.org
- The Federal Trade Commission 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
- **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
- **Privacy Rights Clearinghouse** https://www.privacyrights.org/Privacy-When-You-Shop
- **Internet Crime Complaint Center** http://www.ic3.gov/media/2010/101118.aspx

***Sources:**

ComScore:
http://www.comscore.com/Press_Events/Press_Releases/2011/1/U.S._Online_Holiday_Shopping_Season_Reaches_Record_32.6_Billion_for_November_December_Period

FTC:
http://www.ftc.gov/opa/2011/11/holidayshopping.shtm

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 MULTI-STATE Information Sharing & Analysis Center™

A DIVISION OF CENTER FOR INTERNET SECURITY