



Tips for Secure Shopping Online During the Holiday Season

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

THE FOLLOWING TIPS WILL HELP TO FACILITATE A MORE SECURE ONLINE SHOPPING EXPERIENCE:

- **Secure your computer.** Keep your operating system and application software updated/patched. Ensure 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.
- **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.
- **Secure your online transactions.** Secure Sockets Layer (SSL) is a technology used to encrypt the credit card information that you send over the Internet. If you submit your financial information through an organization's website, look for indicators that the site is secure. Look for the browser's status bar and make sure that *https* appears in the website's address bar before making an online purchase. The *s* stands for *secure* and indicates that communication with the web page is encrypted.
- **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 including 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.
- **Avoid scams and fraud.** Don't ever give your financial information or personal information over e-mail, text, or by phone. Beware 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.
- **Do not use public computers or public wireless networks to conduct transactions.** Public computers may contain malicious software that can steal your credit card information when you place your order. Criminals may be monitoring public wireless networks for credit card numbers and other confidential information.
- **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.
- **Pay by credit card.** Pay by credit card rather than debit card, as credit cards are protected by the Fair Credit Billing Act² and may reduce your liability if your information was used improperly.

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

²www.ftc.gov/opa/2011/11/holidayshopping.shtm

- **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 to 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 see unauthorized charges on your account.
- **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 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

ADDITIONAL RESOURCES

For additional information, please visit:

- 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: www.privacyrights.org/Privacy-When-You-Shop
- Internet Crime Complaint Center: www.ic3.gov/media/2010/101118.aspx

<p>Brought to you by:</p>  <p>www.msisac.org</p>	<p>Distributed by:</p>  <p>www.dir.texas.gov/securetexas</p>
---	---