Monthly Security Tips NEWSLETTER

November 2012 Volume 7, Issue 11

Tips for Secure Shopping Online During the Holiday Season

Online shopping throughout the entire holiday season has become increasingly popular in recent years, and the trend is expected to continue this season. According to MarketLive, an e-commerce software and solutions provider, online shoppers in the U.S. are projected to spend more than $54 billion this holiday season, nearly a 17 percent increase over the $47 billion spent last year. The increase in online shopping coincides with an increase in mobile device use, and more shoppers will be using special holiday smartphone apps to find the best deals.

Before you click or tap to buy that "must have" item on your holiday list, check out these tips below to make sure you're doing everything you can to avoid becoming a victim of cyber crime:

1. ***Secure your mobile device and computer***. Be sure to keep the operating system and application software updated/patched on all of your computers and mobile devices. Be sure to check that any anti-virus/anti-spyware software installed is running and receiving automatic updates. Confirm that your firewall is enabled.

2. ***Know and trust your online shopping 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. ***Look for*** "***http***s" ***when making an online purchase***. The "s" in "https" stands for "secure" and indicates that communication with the webpage is encrypted. If you submit your credit card information through an organization's website, be sure to look for indicators that the site is secure. Look for a padlock or key icon in the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. You should also make sure that your browser software is current and up-to-date.

4. ***Password protect your mobile device and computer***. It's the simplest and one of the most important steps to take to secure your mobile device and computer. If you need to create an account with the merchant, be sure to use a strong password. Use at least eight characters, with numbers, special characters, and upper and lower case letters. Adhere to the tenant "a unique password for every unique site."

5. ***Do not respond to pop-ups.*** When a window pops up promising you cash or gift cards for answering a question or taking a survey, close it by pressing Control + F4 for Windows and Command + W for Macs.

6. ***Avoid scams and fraud.*** Don't ever give your financial information or personal information over e-mail or text. Be aware of unsolicited communications purporting to represent stores or charities. Always think before you click on e-mails you receive asking for donations and contact the organization directly to verify the request. Information on many current scams can be found on the website of the Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center: http://www.ic3.gov/default.aspx .

7. ***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. Additionally, criminals may be intercepting traffic on public wireless networks to steal credit card numbers and other confidential information.

8. ***Pay by credit card, not debit card.*** The safest way to shop on the Internet is to pay with a 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. ***Print your online transactions.*** 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 with 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:

- **Your State Attorney General's Office -** www.naag.org/current-attorneys-general.php
- **Your State Consumer Agency -** http://www.usa.gov/directory/stateconsumer/index.shtml
- **The Better Business Bureau -** www.bbb.org
- **The Federal Trade Commission -** http://www.ftccomplaintassistant.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** - http://www.onguardonline.gov/articles/0020-shopping-online
- **Microsoft** - http://www.microsoft.com/security/online-privacy/online-shopping.aspx
- **Privacy Rights Clearinghouse** - https://www.privacyrights.org/Privacy-When-You-Shop
- **Internet Crime Complaint Center** - http://www.ic3.gov/media/2010/101118.aspx
- **Smartphone Security** - Android vs. iOS

Sources:

- **Federal Trade Commission: Tips for Consumers**
  http://www.ftc.gov/opa/2011/11/holidayshopping.shtm

- **Daily Deal Media: Online Shopping Expected to Rise Nearly 17% this Holiday Season**
  http://www.dailydealmedia.com/789online-shopping-expected-to-rise-nearly-17-this-holiday-season/

- **PayPal Blog: Protect Yourself from Cyber Crime this Holiday Shopping Season**
https://www.thepaypalblog.com/2012/10/protect-yourself-from-cyber-crime-this-holiday-shopping-season/

Brought to you by:

MS-ISAC
MULTI-STATE
Information Sharing
& Analysis Center™
A DIVISION OF CENTER FOR INTERNET SECURITY