State of Texas
CYBERSECURITY TIPS
Monthly Newsletter
From the Office of the Chief Information Security Officer, State of Texas November 2013 | Volume 7, Issue 11

Cyber Monday and the Online Shopping Season: What You Need to Know to Protect Yourself

Online holiday shopping continues to grow in popularity. According to American Express, for the first time, more people are expected to shop online on Cyber Monday than visit brick and mortar stores on Black Friday.[1] Shoppers are expected to spend nearly $62 billion online throughout the holiday season this year, up more than 15% from 2012. The use of mobile devices for online shopping (m-Commerce) is projected to reach almost $42 billion for the 2013 holiday season,[2] as more consumers are using these devices to compare prices, research products, locate stores, and make purchases to a larger degree than ever before.

Whether you'll be conducting transactions from your desktop, laptop, or mobile device, keep these tips in mind to help protect yourself from identity theft and other malicious activity on Cyber Monday and throughout the year:

- Secure your computer and mobile devices. Ensure that your computer and mobile devices are current with all operating system and application software updates. Anti-virus and anti-spyware software should be installed, running, and receiving automatic updates. Use a strong, unique password that is not used for any other accounts. Set a timeout that requires authentication after a period of inactivity.
- Use mobile applications with caution. As devices such as smartphones and tablets continue to gain popularity for online shopping, so too will the volume of attacks against them. Malware could be downloaded onto the device from seemingly legitimate shopping apps that can steal credit card and other sensitive information for transmission to cyber criminals. Update all apps when notified and disable Bluetooth and Near Field Communications when not in use to reduce the risk of your data—such as credit card numbers—being intercepted by a nearby device.
- Know your online merchants. Limit online shopping to merchants you know and trust. Only go to sites by directly typing the URL in the address bar. If you are unsure about a merchant, check with the Better Business Bureau or the Federal Trade Commission. Confirm the online seller's contact information if you have questions or problems.
- Consider using an online payment system or credit card. Where available, consider using online payment services which keep your credit card information stored on a secure server and then let you make purchases online without revealing your credit card details to retailers. If you do pay online directly to the retailer, use a credit card rather than a debit card. Credit cards are protected by the Fair Credit Billing Act and may reduce your liability if your information is used improperly.
- Look for *https* before you click *Purchase*. Before you submit your online transaction, make sure that the website address begins with *https*. The *s* stands for secure and indicates that communication with the website is encrypted. A padlock or key icon in the browser's status bar is another indicator. Make sure that your browser is up-to-date.

[1] **amexspendsave.mediaroom.com/index.php?s=34135&item=22#assets_123**

[2] **www.emarketer.com/Article/Mobile-Devices-Boost-US-Holiday-Ecommerce-Sales-Growth/1010189**

- Do not respond to pop-ups. When a window pops up promising you cash, bargains, or gift cards in exchange for your response to a survey or other questions, close it by pressing *Control F4* on Windows devices or *Command W* on Macs. Responding to these pop-up surveys may likely cause malware or spyware to be installed on your computer or device.
- Do not use public computers or public wireless access for your online shopping. Public computers and Wi-Fi hotspots are potentially unsecure. Criminals may be intercepting traffic on public wireless networks to steal credit card numbers and other sensitive information. Make sure that the settings on your computer or device prevent it from automatically connecting to Wi-Fi hotspots.
- Secure your home Wi-Fi. Control who has administrative access to your home Wi-Fi, and require all users on your network to authenticate using a strong password. Enable encryption settings and use WPA2 encryption.
- Be alert for potential charity donation scams. Cyber criminals try to take advantage of people's generosity during the holiday season and can use fake charity requests as a means to gain access to your information or computer/device. Think before clicking on emails requesting donations. Don't give your financial or personal information over email or text. Contribute by navigating to the charity's trusted address and never through a link in an email. Visit **www.irs.gov** to confirm whether an organization is eligible to receive tax-deductible charitable contributions.

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

- Attorney General's Office: **www.texasattorneygeneral.gov**
- Texas Consumer Protection Offices: **www.usa.gov/directory/stateconsumer/texas.shtml**
- Better Business Bureau: **www.bbb.org**
- Federal Trade Commission: **www.ftccomplaintassistant.gov**

ADDITIONAL RESOURCES

To learn more, visit:

- Shopping Safely Online: **www.us-cert.gov/cas/tips/ST07-001.html**
- Shopping Online: **www.onguardonline.gov/articles/0020-shopping-online**
- Six Rules for Safer Financial Transactions Online: **www.microsoft.com/security/online-privacy/online-shopping.aspx**
- Privacy When You Shop: **www.privacyrights.org/Privacy-When-You-Shop**
- Holiday Shopping Tips: **www.ic3.gov/media/2010/101118.aspx**
- IRS Exempt Organizations Check: **www.irs.gov/Charities-&-Non-Profits/Exempt-Organizations-Select-Check**

Brought to you by:	Distributed by:
MS-ISAC MULTI-STATE Information Sharing & Analysis Center™ A DIVISION OF CENTER FOR INTERNET SECURITY **www.msisac.org**	DIR Secure Texas **www.dir.texas.gov/securetexas**

FROM THE OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER, STATE OF TEXAS
300 W. 15TH ST., STE. 1300 | AUSTIN, TX 78701 | WWW.DIR.TEXAS.GOV/SECURITY