ENTERPRISE INFORMATION SECURITY PROGRAM
Keeping our organization's data safe.

Monthly Security Tips NEWSLETTER

Tacoma

November 2013 Volume 8, Issue 11

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

From the Desk of Paul Federighi, Chief Information Security Officer

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 (mcommerce) is projected to reach almost $10 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**. Be sure 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. Ensure you use a strong password and unique password, which 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 number—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 in case you have questions or problems.
- **Consider using an online payment system or credit card.** Where available, you may want to use 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, not 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 webpage address begins with "https." The "s" stands for secure, and indicates that communication with the webpage is encrypted. A padlock or key icon in the browser's status bar is another indicator. Also, make sure your browser is current and up-to-date.
- **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 for Macs.
- **Do not use public computers or public wireless access for your online shopping.** Public computers and Wi-Fi hotspots are potentially insecure. Criminals may be intercepting traffic on public wireless networks to steal credit card numbers and other sensitive information. Care should be taken that the settings on your computer or device prevent it from automatically connecting to Wi-Fi hotspots.
- **Secure your home Wi-Fi.** Make sure you control who has administrative access, and that any users

[1] http://amexspendsave.mediaroom.com/index.php?s=34135&item=22#assets_123
[2] http://www.emarketer.com/Article/Mobile-Devices-Boost-US-Holiday-Ecommerce-Sales-Growth/1010189

on your network authenticate with a strong password. Encryption settings should be enabled and strong - using WPA2 is recommended.

- **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 trusted address of the charity, never through a link in an email. To check if an organization is eligible to receive tax-deductible charitable contributions, visit the IRS website.

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**
  www.usa.gov/directory/stateconsumer/index.shtml
- **The Better Business Bureau**
  www.bbb.org
- **The Federal Trade Commission**
  www.ftccomplaintassistant.gov

For More Information:

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/articles/0020-shopping-online

- **Microsoft**
  www.microsoft.com/security/online-privacy/online-shopping.aspx

- **Privacy Rights Clearinghouse**
  www.privacyrights.org/Privacy-When-You-Shop

- **Internet Crime Complaint Center**
  www.ic3.gov/media/2010/101118.aspx

- **Internal Revenue Service**
  www.irs.gov/Charities-&-Non-Profits/Exempt-Organizations-Select-Check

Brought to you by:

CENTER FOR INTERNET SECURITY®

STOP | THINK | CONNECT™