November 2015
Volume 10, Issue 11

Safe Online Holiday Shopping

From the Desk of David A. Brown, State Chief Information Security Officer

It's that time of year again – food, fun, parties, and lots of online shopping. Online shopping can be a time saver, allowing you to quickly find the perfect gift, but it can also end with identity theft, malware on your computer, and other cyber unpleasantness. Rather than letting it ruin your holiday season, you can take a few simple security precautions, and be careful where you shop, to help reduce the chances of you being a cyber victim.

When purchasing online this holiday season—and all year long—keep these tips in mind to help minimize your risk:

1. **Be cautious what devices you use to shop online.** Mobile devices, such as smartphones and tablets, make shopping convenient at anytime and place, but they frequently lack the security precautions of a regular computer. If you use a mobile device to shop, make extra sure you are taking all the precautions listed below.

2. **Do not use public computers or public wireless for your online shopping.** Public computers and wireless networks may contain malicious software that steals your information when you place your order, which can lead to identity theft.

3. **Secure your computer and mobile devices.** Be sure to keep the operating system, software, and/or apps updated/patched on all of your computers and mobile devices. Use up-to-date antivirus protection and make sure it is receiving updates.

4. **Use strong passwords.** The use of strong, unique passwords is one of the simplest and most important steps to take in securing your devices, computers, and online accounts. If you need to create an account with the merchant, be sure to use a strong, unique password. Always use more than ten characters, with numbers, special characters, and upper and lower case letters. Use a unique password for every unique site. The August Newsletter contains more information about the dangers of password reuse and is available at: http://msisac.cisecurity.org/newsletters/2015-08.cfm

5. **Know 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, where available, and phone number in case you have questions or problems. Do not create an online account with a merchant you don't trust.

6. **Pay online with one credit card.** A safer way to shop on the Internet is to pay with a credit card rather than debit card. Debit cards do not have the same consumer

protections as credit cards. Credit cards are protected by the Fair Credit Billing Act and may limit your liability if your information was used improperly. By using one credit card, with a lower balance, for all your online shopping you also limit the potential for financial fraud to affect all of your accounts. Always check your statements regularly and carefully, though.

7. **Look for "https" when making an online purchase.** The "s" in "https" stands for "secure" and indicates that communication with the webpage is encrypted. This helps to ensure your information is transmitted safely to the merchant and no one can spy on it.

8. **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.

9. **Be careful opening emails, attachments, and clicking on links.** Be cautious about all emails you receive, even those purportedly from your favorite retailers. The emails could be spoofed and contain malware.

10. **Do not auto-save your personal information.** When purchasing online, you may be given the option to save your personal information online for future use. Consider if the convenience is really worth the risk. The convenience of not having to reenter the information is insignificant compared to the significant amount of time you'll spend trying to repair the loss of your stolen personal information.

11. **Use common sense to avoid scams.** Don't give out your personal or financial information via email or text. Information on many current scams can be found on the website of the Internet Crime Complaint Center: http://www.ic3.gov/default.aspx and the Federal Trade Commission: http://www.consumer.ftc.gov/scam-alerts.

12. **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's Attorney General's Office or Consumer Protection Agency
- The Better Business Bureau - www.bbb.org
- The Federal Trade Commission - http://www.ftccomplaintassistant.gov

Provided By:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

STOP | THINK CONNECT™

The information provided in the Monthly Security Tips Newsletter 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. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.