City of Dover

From the Desk of Andrew R. Siegel

The holidays are right around the corner and consumers are being bombarded with ads for discounted merchandise, free shipping and other special deals during the holiday season, and in particular for Black Friday and Cyber Monday. Last year, more than $1.7 billion was spent online on Cyber Monday, making it the highest volume day in history for online sales. [1] Online sales are expected to be significant again this year.

How can you maximize your transaction security? If the offer seems too good to be true, it probably is. Don't get blindsided by the lure of great discounts – the security of your information is what's most important. If you aren't prepared and cautious, you could become the next cyber crime victim, the cost of which could far exceed any savings you might have received from the retailer.

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

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 your anti-virus/anti-spyware software is running and receiving automatic updates. Confirm that your firewall is enabled.

2. **Use passwords.** It's one of the simplest and most important steps to take in securing your devices, computers and accounts. If you need to create an account with the merchant, be sure to use a strong 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.

3. **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.

4. **Pay by credit card, not debit 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. Check your statements regularly.

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.

6. **Look for "https" when making an online purchase.** The "s" in "https" stands for "secure" and indicates that communication with the webpage is encrypted.

7. **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.

8. **Do not click on links or open attachments in emails from financial institutions/vendors.** Be cautious about all emails you receive even those from legitiatmate organizaitons, including your favorite retailers. The emails could be spoofed and contain malware. Instead, contact the source directly.

9. **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.

10. **Use common sense to avoid scams.** Don't ever give your financial information or personal 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.

11. **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.

12. **Join Our Twitter Chat**. Join the Center for Internet Security (**@CISecurity**) and Sophos (**@Sophos_news**) on **Tuesday, November 25, 2014 at 2 p.m. EST/11 a.m. PST** for a Twitter Chat with more tips for staying safe online this holiday season. Use **#ChatCyberMon** to join us!

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

Provided By:

CENTER FOR INTERNET SECURITY®

STOP | THINK | CONNECT™

---

[1] https://www.comscore.com/Insights/Press-Releases/2013/12/Cyber-Monday-Jumps-18-Percent-to-1735-Billion-in-Desktop-Sales-to-Rank-as-Heaviest-US-Online-Spending-Day-in-History