Commonwealth Office Of Technology Monthly Cyber Security Tips

NOVEMBER 2006 Volume 1, Issue 6

Safe Online Shopping

From the Desk of The Chief Information Security Officer

Shopping online offers lots of benefits that you won't find shopping in a store or by mail. The Internet is always open — seven days a week, 24 hours a day — and bargains can be numerous online. With a click of a mouse, you can buy an airline ticket, book a hotel, send flowers to a friend, or purchase your favorite fashions. The following tips can help you stay secure while doing your shopping online.

- **Know whom you're dealing with.** Anyone can set up shop online under almost any name. Confirm the online seller's physical address and phone number in case you have questions or problems. Contact the seller promptly if you have any problems with your order.

- **Beware of pop-up windows and sudden emails.** If you get an email or pop-up message while you're browsing that asks for financial information, don't reply or click on the link in the message. Legitimate companies don't ask for this information via email. In fact, clicking on the pop-up window or clicking on the link in the email might allow spyware on your system. Giving out confidential information via pop-ups or email can also lead to fraud or identity theft. Delete any suspicious emails, and close unwanted pop-ups by clicking on the "x" box in the top right corner - never click inside the pop-up window itself.

- **Know exactly what you're buying.** Read the seller's description of the product closely, especially the fine print. Words like "refurbished," "vintage," or "close-out" may indicate that the product is in less-than-mint condition, while name-brand items with "too good to be true" prices could be counterfeits.

- **Know what it will cost.** Check out websites that offer price comparisons and then, compare "apples to apples." Factor shipping and handling — along with your needs and budget — into the total cost of the order. Do not send cash under any circumstances.

- **Pay by credit or charge card.** If you pay by credit or charge card online, your transaction will be protected by the Fair Credit Billing Act. Under this law, you have the right to dispute charges under certain circumstances and temporarily withhold payment while the creditor is investigating them. In the event of unauthorized use of your credit or charge card, you generally would be held liable only for the first $50 in charges. Some companies offer an online shopping guarantee that ensures you will not be held responsible for any unauthorized charges made online, and some cards may provide additional warranty, return, and/or purchase protection benefits.

- **Check out the terms of the deal, like refund policies and delivery dates.** Can you return the item for a full refund if you're not satisfied? If you return it, find out who pays the shipping costs or restocking fees, and when you will receive your order. A Federal Trade Commission (FTC) rule requires sellers to ship items as promised or within 30 days after the order date if no specific date is promised.

- **Keep a paper trail.** Print and save records of your online transactions, including the product description and price, the online receipt, and copies of every email you send or receive from the seller. Read your credit card statements as you receive them and be on the lookout for unauthorized charges.

- **Don't email your financial information.** Email is not a secure method of transmitting financial information like your credit card, checking account, or Social Security number. If you initiate a transaction and want to provide your financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some fraudulent sites have forged security icons.

- **Check the privacy policy.** It should let you know what personal information the website operators are collecting, why, and how they're going to use the information. If you can't find a privacy policy — or if you can't understand it, consider taking your business to another site that's more consumer-friendly.

- **Keep your computer protected.** Protect your computer by using anti-virus and anti-spyware software, use a firewall, and use an email spam filter. It is important to keep these programs updated on a regular basis to keep your system safe from the latest threats. Keep your operating system and browser up-to-date with the latest security patches as well. That way if you do stumble onto a malicious or compromised website, your computer is less likely to become infected.

For more information on Safe Online Shopping, please visit:

http://onguardonline.gov/quiz/
http://www.onguardonline.gov/shopping.html
http://www.ftc.gov/bcp/conline/edcams/holiday/
http://www.staysafeonline.info/news/press_nov17_2005.html
http://www.safeshopping.org/tips.shtml

For more information and this and other topics please visit the Commonwealth Office of Technology's Website at http://technology.ky.gov/security/cyber_security.htm

http://technology.ky.gov

Brought to you by:

MS-ISAC
http://www.msisac.org

OnGuard Online | YOUR SAFETY NET™
http://onguardonline.gov