Holiday Crime Prevention Tip of the Day: Online Shopping (#2 in a Series)

It's Cyber Monday. Reduce the chances of becoming a victim of a crime! As always, everyone is busy and excited trying to get everything done. Don't be careless…criminals don't take the holidays off! Here are some prevention tips to think about while shopping online:

Online shopping

- **Be cautious of e-mails** claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from KNOWN senders. Always run a virus scan on attachments before opening.
- **Log on directly** to the official Web site for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- **Secure your computer**. Make sure your computer has the latest security updates installed. Check that your anti-virus and anti-spyware software are running properly and are receiving automatic updates from the vendor. If you have not already done so, install a firewall before you begin your online shopping.
- **Upgrade your browser**. Upgrade your Internet browser to the most recent version available. Review the browser's security settings. Apply the highest level of security available that still gives you the functionality you need.
- **Secure your transactions**. Look for the "lock" icon on the browser's status bar and be sure "https" appears in the website's address bar before making an online purchase. The "s" stands for "secure" and indicates that the communication with the webpage is encrypted. Also look for a broken key symbol indicating a non-secure connection. Some browsers can be set to warn the use if they are submitting information that is not encrypted.
- **Be wary of potential scams.** If the online offer sounds too good to be true, it probably is. Cyber criminals will look to take advantage of the volume of online shoppers to temp users to fall prey to online scams.
- **Use strong passwords**. Create strong passwords for online accounts. Use at least eight characters, with numbers, special characters, and upper and lower case letters. Don't use the same passwords for online shopping websites that you use for logging onto your bank, home or work computer. Never share your login information with anyone.
- **Do not e-mail sensitive data.** Never e-mail credit card or other financial/sensitive information. E-mail is like sending a postcard and other people have the potential to read it. Beware of emails requesting account or purchase information. Delete these emails. Legitimate businesses don't solicit information through email.
- **Ignore pop-up messages.** Set your browser to block pop-up messages. If you do receive one, click on the "X" at the top right corner of the title bar to close the pop-up message.

- **Do not use public computers** or public wireless to conduct transactions. Don't use public computers or public wireless connections for your online shopping. Public computers could potentially contain malicious software that steals your credit card information when you place your order. Criminals could be monitoring public wireless networks for credit card numbers and other confidential information.
- **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 or sold to others.
- **Make payments securely.** Pay by credit card rather than debit card. Credit/charge card transactions are protected by the Fair Credit Billing Act. Cardholders are typically only liable for the first $50 in unauthorized charges. If online criminals obtain your debit card information they have the potential to empty your bank account.
- **Use temporary account authorizations**. Some credit card companies offer virtual or temporary credit card numbers. This service gives you a temporary account number for online transactions. These numbers are issued for a short period of time and cannot be used after that period.
- **Select merchants carefully**. Limit your online shopping to merchants you trust. Confirm the online seller's physical address and phone number beforehand. If you have problems, concerns, or questions regarding a merchant, check with the Better Business Bureau or the Federal Trade Commission. Don't forget to review merchant's return policies to avoid product return issues.
- **Keep a record** of your online transactions, including the product description and price, the online receipt, and copies of every e-mail you send or receive from the seller. Review your credit card and bank statements for unauthorized charges.

For more information, check out our website for more Crime Prevention tips:
http://www.hooverpd.com/crime-prevention.php