TIPS FOR SAFE ONLINE SHOPPING

Reduce Risk and Improve Security of Your Financial Information During the Holidays

Carefully review your credit card statements as soon as you receive them to confirm that all charges are legitimate.

Shopping on the Internet has quickly become a major part of the world's economy. People have grown to rely on the Internet for everything from music to airline tickets. This holiday season and throughout the year, know what to look for when shopping online to reduce your risk and improve the security of your credit and debit card information. No initial cash flow needed.

PROTECT YOUR ONLINE TRANSACTIONS

If you submit your financial information through a merchant's Web site, be sure to look for indicators that the site is "secure." Look for "https" in the Web site's address bar before making an online purchase. The "s" stands for "secure" and indicates that communication with the Web page is encrypted. Encrypted sites also display an icon of a locked padlock, typically in the status bar at the bottom of your Web browser or right next to the URL in the address bar.

SHOP WITH TRUSTED MERCHANTS

Limit your online shopping to merchants you know and trust. Confirm the online seller's physical address and phone number in case you have questions or problems. Never give anyone your credit card information by e-mail.

USE STRONG PASSWORDS

If you must register using a password with the merchant, make sure you are using a strong password. Use at least eight characters, with numbers, special characters and uppercase and lowercase letters. Never use the same passwords for online shopping Web sites that you use for any other account, and never share your login and/or password with anyone for any reason.

DO NOT USE PUBLIC COMPUTERS OR PUBLIC WIRELESS TO CONDUCT TRANSACTIONS

Public computers may contain malicious software that steals your credit card information when you place your order. Criminals may be monitoring public wireless networks for credit card numbers and other confidential information.

IGNORE POP-UP MESSAGES

Set your browser to block pop-up messages. If you get an e-mail or pop-up message that asks for your financial information while you're browsing, don't reply or follow the link. Legitimate companies won't ask for financial information in a pop-up message. Close out of the pop-up message by closing out of the browser.

KEEP A PAPER TRAIL

Print or save records of your online transactions. Carefully review your credit card statements as soon as you receive them to confirm that all charges are legitimate. Contact your credit card company immediately if you have unauthorized charges on your account.

REVIEW PRIVACY POLICIES

Review the privacy policy for the merchant's Web site 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.

KEEP YOUR SYSTEM AND APPLICATION SOFTWARE UPDATED/PATCHED

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