Online Shopping

Online shopping is convenient, easy, and quick. However, the Internet has unique risks, so it is important to take steps to protect yourself when shopping online.

Tune up your defenses.

Before you shop online, make sure you have a security suite (firewall, anti-virus and anti-spyware) installed and updated with the most current information. Also, keep your operating system and Web browser up-to-date. Apply the highest level of security available that still gives you the functionality you need.

Check sellers out.

Conduct independent research before you buy from a seller you have never done business with. Some attackers try to trick you by creating malicious Web sites that appear legitimate, so you should verify the site before supplying any information. Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill. Search for merchant reviews.

Make sure the site is legitimate.

Before you enter your personal and financial information to make an online transaction, look for signs that the site is secure. This includes a closed padlock on your Web browser’s address bar or a URL address that begins with shttp or https. This indicates that the purchase is encrypted or secured. Never use unsecured wireless networks to make an online purchase. Check out this GetNetWise tutorial for more info.

Take advantage of security features.

Passwords and other security features add layers of protection if used appropriately. In a rush to complete a transaction with a new vendor, it is tempting to create a simple password that you won’t forget. However, it is not hard to create complex, yet easily remembered passwords.

Protect your personal information.

When making a purchase online, be alert to the kinds of information being collected to complete the transaction. Make sure you think it is necessary for the vendor to request that information. Remember, you only need to fill out required fields on a vendors checkout form. Before providing personal or financial information, check the Web site's privacy policy. Make sure you understand how your information will be stored and used.

Use safe payment options.

Credit cards are generally the safest option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Also, unlike debit cards, credit cards may have a limit on the monetary amount you will be responsible for paying if your information is stolen and used by someone else. Never send cash through the mail or use a money-wiring service because you'll have no recourse if something goes wrong. Don't forget to review return policies. You want a no-hassle ability to return items.

Keep a paper trail.

Print and save records of your online transactions, including the product description, price, online receipt, terms of the sale, and copies of any email exchange with the seller. Read your credit card statements as soon as you get them to make sure there aren't any unauthorized charges. If there is a discrepancy, call your bank and report it immediately.

Turn your computer off when you're finished shopping.

Many people leave their computers running and connected to the Internet all day and night. This gives scammers 24/7 access to your computer to install malware and commit cyber crimes. To be safe, turn off your computer when you are not using it.

Be wary of emails requesting information.

Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Contact the merchant directly if you are alerted to a problem. Use contact information found on your account statement, not in the email.

Learn more about shopping online safety at:

- OnGuardOnline – Information from the Federal Trade Commission

Reprinted with permission from the Federal Trade Commission (2011)