Shopping Safely Online

Online shopping has become a popular way to purchase items without the hassles of traffic and crowds. However, the Internet has unique risks, so it is important to take steps to protect yourself when shopping online.

Why do online shoppers have to take special precautions? The Internet offers a convenience that is not available from any other shopping outlet. From the comfort of your home, you can search for items from countless vendors, compare prices with a few simple mouse clicks, and make purchases without waiting in line. However, the Internet is also convenient for attackers, giving them multiple ways to access the personal and financial information of unsuspecting shoppers. Attackers who are able to obtain this information may use it for their own financial gain, either by making purchases themselves or by selling the information to someone else.

How do attackers target online shoppers?
There are three common ways that attackers can take advantage of online shoppers:

- Targeting vulnerable computers – If you do not take steps to protect your computer from viruses or other malicious code, an attacker may be able to gain access to your computer and all of the information on it. It is also important for vendors to protect their computers to prevent attackers from accessing customer databases.
- Creating fraudulent sites and email messages – Unlike traditional shopping, where you know that a store is actually the store it claims to be, attackers can create malicious web sites that mimic legitimate ones or create email messages that appear to have been sent from a legitimate source. Charities may also be misrepresented in this way, especially after natural disasters or during holiday seasons. Attackers create these malicious sites and email messages to try to convince you to supply personal and financial information.
- Intercepting insecure transactions – If a vendor does not use encryption, an attacker may be able to intercept your information as it is being transmitted.

How can you protect yourself?

- Use and maintain anti-virus software, a firewall, and anti-spyware software – Protect yourself against viruses and Trojan horses that may steal or modify the data on your own computer and leave you vulnerable by using anti-virus software and a firewall. Make sure to keep your virus definitions up to date. Spyware or adware hidden in software programs may also give attackers access to your data, so use a legitimate anti-spyware program to scan your computer and remove any of these files.
-
- Keep software, particularly your web browser, up to date – Install software patches so that attackers cannot take advantage of known problems or vulnerabilities. Many

operating systems offer automatic updates. If this option is available, you should enable it.

-
- Evaluate your software's settings – The default settings of most software enable all available functionality. However, attackers may be able to take advantage of this functionality to access your computer. It is especially important to check the settings for software that connects to the Internet. Apply the highest level of security available that still gives you the functionality you need.
-
- Do business with reputable vendors – Before providing any personal or financial information, make sure that you are interacting with a reputable, established vendor. Some attackers may try to trick you by creating malicious web sites that appear to be legitimate, so you should verify the legitimacy 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.
-
- Take advantage of security features – Passwords and other security features add layers of protection if used appropriately.
-
- 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.
-
- Check privacy policies – 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.
-
- Make sure your information is being encrypted – Many sites use SSL, or secure sockets layer, to encrypt information. Indications that your information will be encrypted include a URL that begins with "https:" instead of "http:" and a padlock icon. If the padlock is closed, the information is encrypted. The location of the icon varies by browser; for example, it may be to the right of the address bar or at the bottom of the window. Some attackers try to trick users by adding a fake padlock icon, so make sure that the icon is in the appropriate location for your browser.
-
- Use a credit card – There are laws to limit your liability for fraudulent credit card charges, and you may not have the same level of protection for your debit card. Additionally, because a debit card draws money directly from your bank account, unauthorized charges could leave you with insufficient funds to pay other bills. You can further minimize damage by using a single credit card with a low credit line for all of your online purchases.
-
- Check your statements – Keep a record of your purchases and copies of confirmation pages, and compare them to your bank statements. If there is a discrepancy, report it immediately.

Note: This article was produced by Mindi McDowell and Monica Maher, and copyrighted by the US-CERT. This article was used with permission as stated in Terms of Use, Copyright Permission. The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation.