



CyberAngels

A program of Guardian Angels
keeping it safe

Secure Site Check

Before you enter personal information on any web site, verify that the site has security measures in place to protect the data you enter. How?

- Check that the web address of the page at which you are entering the information begins with [https](#). This indicates you are connected to a secure server which encrypts the information you exchange with that server.
- You should also look for a closed padlock symbol on the bar at the bottom of your browser screen. Double-clicking on the padlock brings up details about the site's security certificate. Check to be sure that the "Issued to" name matches the name of the site you intended to visit. By performing this check, you may be able to detect a "spoofed" (fake) site, since the names will differ.
- Some online stores will have right on their web site a seal or logo of the company that issued its security certificate. (Be aware, however, that some fraudulent sites have even forged security icons!)
- If your browser displays a message warning you that a site's security certificate is expired or invalid, take the warning seriously. You may not want to proceed with your purchase.

Additional Resources

Federal Trade Commission (FTC): [OnGuard Online](#)

Better Business Bureau: [Consumer Safe Shopping Site](#)

CERT: [Understanding Web Site Certificates](#)