

Internet Protection Tips

When making an online purchase, or providing any type of confidential information, you want to be sure that you are sending information as securely as possible. The following are a few basic tips to help ensure your online safety and protection.

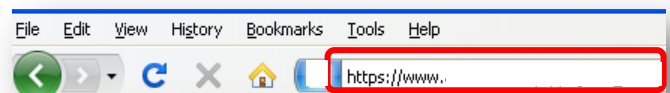
To help verify you are on a secure website, look for a small lock icon located in the bottom right corner of your browser window. The lock icon should always be in a locked position.

The lock signifies a secure site where data is encrypted. Encryption is a process where transmitted data is altered to make it unreadable, allowing the data to be sent safely over the Internet and readable only by the intended recipient. Banks and most online shopping sites, or sites requesting personal information are examples of websites that are commonly set up as secure sites.



Also, be sure that the website URL is:

https:// and not the typical **http://**



The “s” after http means that you have entered into a “secure session.” Once you log in or initiate a purchase requiring personal information, if you look in the address bar, you’ll notice that the front of the URL changes from **http** to **https**.

For added security, once your purchase or transaction is complete, you should immediately log out to end the session.

Additional Tips...

1. If a website where a username or password are required (blogs, forums, etc.), and it is not a secure site, be sure to use a username or password that is unique, and not something you would use anywhere else.
2. Email is not encrypted, so websites should not transmit confidential data via an email. Often when you sign in as a new user to a site, you’ll receive an email confirmation that may include your username, but generally does not include the password, in order to maintain your privacy.
3. Be wary of emails or popups that ask you for a username, or password, or any type of confidential information. Unless you have initiated the action, it is best to ignore any request for personal information.

The onus is on each individual to be as knowledgeable and careful as possible when providing confidential information online. Stay up-to-date regarding current scamming and phishing trends, and as always, it is best to err on the side of caution.