

Wireless Network Security Hole

Please be aware that there is a new Firefox plug-in that makes it quick and easy to examine and use unencrypted data sent over any open wireless network. This makes it a simple matter for hackers to access Twitter, Facebook, Amazon, Flickr, some email sites, and other non-encrypted websites as if he or she were the account holder. This plug-in allows full access to any site that users may log into that does not have “https://” at the beginning of its web address. The “s” in “[https://](#)” means that the site has been secured and encrypted with a Secure Socket Layer certificate (SSL).

If you are on our public wireless network (or any public wireless network) and you type a username and password into a website that uses “[http://](#)” instead of “[https://](#),” the transaction you conduct on that site and account are vulnerable to theft and fraud.

This is not a new security risk; what is new is how easily anyone can now access your information with this browser plug-in. No open wireless network is completely safe, but entering user names and passwords only on https sites will provide a much higher level of security.