



Sidejacking

Sidejacking is a term used to describe the malicious act of hijacking an engaged Web session with a remote service by intercepting and using the credentials that identified the user/victim to that specific server. Typically, SideJacking is most common on sites that require authentication through a username and password, such as online Web mail accounts as well as social networking sites. SideJacking works only if the site catches a non-SSL cookie, so any Web site that uses SSL exclusively would be safe from SideJackers.

Sidejacking is the newest way that your information can be stolen. It works by accessing your system over a wireless network. This happens 99.9% of the time at free WiFi hotspots such as coffee shops, etc. You may think that your personal data is safe if you use a secure login, but that's not true these days. In fact, everything from the contents of your e-mail, who your friends and acquaintances are, and almost anything else you can think of could be easily exposed by hackers if browsed via WiFi networks. This is less likely on a home or business wireless network. But, it can happen there also.

The method by which this data could become exposed is nothing new. Many web services, such as Gmail, BlogSpot, Facebook, MySpace, LinkedIn, and Google AdSense use cookies to identify session information after the user has already logged in. Using a basic packet sniffer over a WiFi network and a proxy server to pass the information through, a determined hacker can easily sidejack the session information as his own by stealing session IDs straight out of the WiFi signal. This is not getting it off your computer where a firewall will protect you. This is grabbing it out of thin air. They can then use that session ID to represent themselves as the original user, which would allow them to do things like make blog posts, unfriend all of your Facebook friends and read or send e-mails.

Even though some sites, such as Gmail, offer secure, SSL-based login pages, things aren't quite so secure after you log in. Unlike many bank web sites that offer a secure browsing experience for the entire duration of the session, most sites dump the user right back out into unsecured territory after logging in, thus exposing their personal data to anyone who wants to get at it.

Of course, there are several easy solutions to protect your data. The obvious answer would be to stick to secured WiFi networks that you know and trust (such as your home and office network) that would not have any strangers on it running packet sniffers

(hopefully). But if you do need to use public access points, avoid accessing web pages that might transmit personal information. Another, very safe way to protect yourself, is to use a VPN (Virtual Private Network) while connecting to these public WiFi spots.

There is a free download that will do just this for you. You can get it by going to www.anchorfree.com and downloading their hotspot shield. This product will create this VPN for you.

For more information on this or on any other concern you have, please do not hesitate to contact me at jeff.lipshaw@aficc.com or at 248-425-0009.