U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

How to be safe using Public Networks

WHAT ARE THE DANGERS OF USING PUBLIC WI-FI CONNECTIONS?

Many public Wi-Fi hotspots don't encrypt the information you send over the internet, and are not secure.

If you use an unsecured network to log into an unencrypted website -- or a site that uses encryption only on its sign-in page -- other users on the network can see what you see and what you send. They could hijack your browsing session and log in as you. Your personal information, private documents, contacts, family photos, and even your login credentials, could be up for grabs. An imposter could use your account to impersonate you and scam people. In addition, a hacker could test your user name and password to try to gain access to other websites -- including sites that store your financial information.

IF THE NETWORK AT A LOCATION REQUIRES A PASSWORD TO BE USED, IS IT SAFER?

Wi-Fi hotspots in coffee shops, libraries, airports, hotels, universities, and other public places are convenient, but they're often not secure. When using a hotspot, it's best to send information only to websites that are fully encrypted. WEP and WPA encryption are the most common, and WPA2 is the strongest. WPA encryption protects your information against common hacking programs. WEP may not. You can be confident a hotspot is secure only if it asks you to provide a WPA password. To be sure a site is encrypted, look for a closed lock symbol in the address bar and an address that begins with "https".

WHAT ARE SOME WAYS TO PROTECT USERS ON PUBLIC NETWORKS?

- To be secure, your entire visit to each site should be encrypted, from the time you log in to the site until you log out. If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Don't use the same password on different sites. It could give someone who gains access to one of your accounts access to many of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up to date.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the Internet, even on unsecured networks. You can obtain a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees.
- Installing browser add-ons or plug-ins can help. There are add-ons available -- some for free -- that force a browser to use encryption on popular sites that usually aren't encrypted. They don't protect you on all sites - look for https in the URL to know a site is secure.
- Avoid using publicly accessible computers, such as those found in hotel business centers, libraries and cyber cafes. Cyber criminals can infect these machines with viruses of malicious software that allows them to capture your information.