

Fact Sheet

Headquarters, United States Army Europe

Office of the Chief of Public Affairs (OCPA)

Tel: 06221-57-7270, FAX: 06221-57-8986

DSN: (314) 370-7270, e-mail: ocpa.pi@eur.army.mil



Network security begins at home: How to be safe using public networks

What are the dangers of using public networks?

Most 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 the 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. New hacking tools -- available for free online -- make this easy, even for users with limited technical know-how. 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 you care about. 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 such as a hotel 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. You can be confident a hotspot is secure only if it asks you to provide a WPA password. If you're not sure, treat the network as if it is unsecured.

What can be done to protect users on public networks?

When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted (HTTPS). 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 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.

Some Wi-Fi networks use encryption -- WEP and WPA are the most common. WPA2 is the strongest. WPA encryption protects your information against common hacking programs. WEP may not. If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network.

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.

More information and tips for home network security and other personal protective measures can be found on the [U.S. Army Europe vigilance web page](#).