

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: Making sure your network is secured

You would never use a wireless hotspot or a shared computer at the public library to do your online banking, would you? You've read the warnings and seen the TV commercials about protecting yourself from people eavesdropping on your wireless communications in places like these. But an unsecured home wireless network is just as dangerous. Many people may not even know if their home wireless network is secured or how well it is secured.

The box at right shows how to check your network security.

Even if your network is secured it may still be vulnerable to hacking. At a minimum you should ensure that your system is using WPA or WPA2 (Wi-Fi Protected Access) instead of WEP (Wired Equivalent Privacy) as your encryption type, that you are using strong passwords, and that you are not broadcasting your default SSID (Service Set Identifier).

Not all wireless encryption methods are the same. WEP is an older type of wireless encryption and has been proven insecure. WEP can be cracked in a few minutes using free utilities downloadable from the Internet. Some older home wireless routers and wireless cards in computers do not support the stronger encryption methods WPA and WPA2. If this is true for your home network you may want to consider upgrading your equipment.

Never use the default administrator user name and password that came with your wireless router. Strong passwords are at least eight characters long and contain a mix of numbers, letters and special characters. If someone is able to access your router configuration settings they can disable the security you have set up. Avoid using words, names or your telephone number as passwords to connect to your wireless network from a laptop or mobile device.

Your SSID is the name that is broadcast from your wireless router, and identifies it from other wireless routers. Most wireless routers broadcast the manufacturer's name by default in the SSID. But leaving the manufacturer's name in the SSID gives potential hackers additional information on how to hack your home network. Never use your home address or personal identifying information in your SSID. Remember the information in your SSID can be broadcast and is viewable by anyone who wants to see it.

What are the dangers of having an unsecured or poorly secured home wireless network? Having an unsecured or poorly secured home wireless network can result in someone else logging into your network and using up your bandwidth. Not only is this annoying and frustrating but in Germany it could subject you to a fine if a third party uses your unsecured home wireless network to illegally download music copyrighted material. Worse yet, if someone gains access to your wireless network they could install malicious programs to copy all your keystrokes or steal your credit card or banking information. They could also use your home network to hide behind while they attack other networks.

The information here is designed to provide basic information on securing a home wireless network. There are other more advanced actions you can take, such as SSID cloaking, firewall packet filtering, and MAC address filtering, to name a few. Most wireless routers come with a reset switch on the back panel so if you mess up, simply reset your router and try again.

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](#).

Checking your home network security

Windows 7 users

- Click 'Start' and then 'Control Panel'
- Change the 'View by' settings to 'category' if necessary and click 'Network and Internet'
- Click 'Connect to a network.' A pop-up will open that lists available networks
- Move the cursor over the network to which you're connected and read the security type. If it reads 'unsecured,' you need to take action to secure it

Windows Vista users

- Click 'Start' and then 'Connect to'
- Click the drop-down menu and select 'All'
- Mouse over the network to see the 'Security type.' If it reads 'unsecured,' you need to take action to secure it. Some versions of Vista show the security status without having to mouse over