Contact Information:
Cyber Criminal Intelligence Program

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

Email
usarmy.cciuintel@mail.mil

CCIU Web Page
http://www.cid.army.mil/701st.html#sec6

CID LOOKOUT
ON POINT FOR THE ARMY

"Do What Has To Be Done"

CPF 0007-17-CID361-9H 27 July 2017

Are Wireless Networks Inherently Unsecure and Placing You at Risk?

It depends. If poorly configured, then yes, it can expose you to substantial risks. Every poorly connected device you connect to your internet router is a potential entry point into your network. Once into your network, a hacker can move about, spy on your activities, steal data or use your internet connection to do illegal things.

Vulnerabilities

The vulnerabilities are numerous. These are just a few.

- Default usernames and passwords – each new device has a default username and password. Often the combination is simple, such as admin and password. Default passwords are often the same for an entire product line. If a hacker can identify the type of device and you haven't changed the default username password combination, the default combination works rather handily.
- The Internet of Things (IoT) – Before too long, your smart refrigerator, coffee pot, doorbell, thermostat, iron, door locks and more will connect to the internet. You'll be able to tweet directly from your microwave. Your refrigerator will text you when your half & half expires. But any smart device connected to your internet, if not properly configured, is a threat to your safety and security.
- Firmware – the computer code built into each device, must be updated regularly. As vulnerabilities in firmware are identified, hackers quickly learn to exploit them. If you don't regularly update the firmware on your devices – all of them – you're at risk.
- Encryption – if you don't use encryption, your router username and password are broadcast in-the-clear. That means a nefarious, nearby user can electronically eavesdrop on the connection and learn both.

Wireless Network Security Tips

There are many things you can do to improve the safety of your home internet experience. But, with so many different makes and models of home routers, it's impossible to provide instructions for all. Before you undertake any configuration changes, use the internet to find how-to instructions. The internet will be your friend for this.

Here are useful things you can do to secure your home networks:

- Use router encryption – WPA or WPA2. Do not use WEP. It is easily broken.
- Change the default service set identifier (SSID).
- Do not broadcast your SSID.
- Enable Media Access Control (MAC) address filtering.
- Change your router's username and password and be creative with both.
- Enable firewalls on each computer and router.

- Update the firmware on all devices that connect to the internet. Including the less obvious. Like your smart refrigerator, coffee pot, baby monitor, and thermostat. Even better, ask yourself if your refrigerator really needs to communicate with your coffee pot…or anything at all, really.

Wireless Security Incidents

The following cautionary tales demonstrate the risks of poorly configured Wi-Fi devices.

- Detectives in Florida traced a man's tweeted bomb threats to a private residence. There, detectives found an unsuspecting man with a poorly configured wireless router. After breaking into that router, a criminal used it to send threats.
- Similarly, an Indiana Police Swat team raided a home and handcuffed all of the residents only to find someone unrelated had accessed the home's unprotected Wi-Fi and sent threats of murder and mayhem.
- Police officers in New Jersey woke a couple in the middle of the night looking for the individual responsible for downloading and sharing tens of thousands of illegal images and videos. A neighbor used the couple's Wi-Fi to download and distribute child pornography. Their Wi-Fi was not password protected.

Additional Resources

MICROSOFT – How to Create A Strong Password.
How To Geek – The difference between WEP, WPA, and WPA2 Wi-Fi Passwords.
Teddy Bears Leak Private Data – Two million voice recordings released.
Ransomware Affecting Smart TVs – It might be time for a new television.
Change Default Passwords Now! – If you own these devices.
Home Computer Security – Ten home computer security tips

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.