ARMY CRIMINAL INVESTIGATION DIVISION

5 September 2023

Cybercrime Prevention Flyer

Wireless Home Network Security

A wireless home network, commonly known as a home Wi-Fi network, is the internet gateway for internet of things (IoT) devices in most households. If the home Wi-Fi network is left unsecured, the network has the potential to become the cybercriminal gateway to all household internet connected devices: computers, smartphones, smartwatches, security cameras, appliances, and even baby monitors.

For many households, setting up a home Wi-Fi network is easy; contact an internet service provider (ISP), an ISP technician visits the home to set up a router or modem/router, the customer downloads an app to a smart device to establish the home Wi-Fi username and password, and then the customer connects all IoT devices to the home Wi-Fi network. But what the ISP technician failed to explain is that the username and password for the router or modem/router, along with other router options, is set to the factory default settings. A Wi-Fi router, the device emitting the household Wi-Fi signal, default username and password is often generic and easily obtainable. As the gateway to the household Wi-Fi network, an unsecured router, default username and password, is the only opening a cybercriminal needs.

Following these tips for network security can decrease the risk of becoming a victim. If additional assistance is needed to set up a router, a quick internet search for the make and model should provide a guide for configuration.

TIPS FOR HOME NETWORK SECURITY

- Use Wi-Fi Protected Access 3 (WPA3) encryption on the home router to increase wireless security. If WPA3 is unavailable, use WPA2. If the home router does not have either, consider upgrading the router.
- Change the router's default password. Router manufacturers often set the default password to "admin" or "password."
- Use a different password for the router's admin account and the Wi-Fi access.
- Log out of the admin account on the router when not actively using it.
- Change the default service set identifier (SSID), otherwise known as the Wi-Fi network name. It is recommended to use a unique name and not something that is linked to your identity or location.
- Disable remote access so that any changes being made to a router must be done in the physical location of the router.
- Set up a guest Wi-Fi network to limit the number of devices on the primary network.
- Enable automatic operating system and software updates. These updates often patch vulnerabilities.
- Turn on the home network router's built-in firewall as an extra layer of protection from outside access.
- Ensure the home network router firmware is up to date.
- Install antivirus software on devices and keep the software up to date.
- Turn the Wi-Fi network off when not in use, if possible. Some home security systems need the Wi-Fi on to stay connected.
- Routinely monitor the router for unknown devices or devices that are attempting to access the network.

ADDITIONAL RESOURCES

Home Network Security

How To Secure Your Home Wi-Fi Network

Protected Voices: Router Hardening

Authorized for widest release, without restrictions.

To receive Cyber Directorate Cybercrime Prevention Flyers, send an email to: **CYDIntel@army.mil**

CPF 0056-2023-CID461

Cyber Directorate Headquarters
Russell Knox Building
27130 Telegraph Road
Quantico, VA 22134