5 Network Security Remedies for Telework

With the COVID-19 (coronavirus) global pandemic, many employers are recommending additional telework to help keep employees safe and productive. More and more, companies are embracing "remote teams" and allowing their employees the opportunity to work from home or telecommute. Yet home IT devices are still subject to many of the same threats as on-site business devices. Unsecured off-site routers, modems, and other network devices can cause big headaches for employers, and poorly configured home devices can affect the entire organization. They can still be attacked from any device on the internet, but they are also vulnerable to unauthorized access from neighbors and passersby.

The Center for Internet Security, Inc. (CIS) published the CIS Controls Telework and Small Office Network Security Guide to help combat security concerns affecting network equipment meant for personal or home office use. The following are high impact actions that can be taken by employees to immediately improve the security of their home networks.

1. **Practice smart password management and enable two-factor authentication (2FA) wherever possible.** This includes accessing the administrative router/modem, Internet Service Provider (ISP) web portal, or a mobile app used for home network management. Anyone with the ability to access these platforms may be able to access sensitive information traversing the home network and modify critical security settings within the network.
2. **Enable automatic updates for all routers and modems.** Software updates are extremely important as new security flaws are constantly discovered. Simply installing updates from the device manufacturer mitigates many of these problems. This is best accomplished by enabling "auto-update" with the device's administration page.
3. **Turn off WPS and UPnP.** Wireless Protected Setup (WPS) was initially designed as a user-friendly method for new devices to connect to a WiFi network. Unfortunately, it's been found to allow attackers to connect to WiFi networks without permission. Universal Plug and Play (UPnP) is a network protocol suite that allows devices on a network to easily communicate but has been found to contain numerous and severe security flaws. Getting these two settings correct can have a large positive impact on home network security.
4. **Turn on WPA2 or WPA3.** Old and ineffective types of cryptography plague older network devices. Ensuring strong forms of cryptography are in use within home networks can thwart others from viewing sensitive information without authorization. At a minimum, configure WPA2 for home use.
5. **Configure the router/modem firewall.** Firewalls help prevent malicious network traffic attempting to enter a network from reaching specific devices. Firewalls generally come built-in to most home routers but they must be properly enabled.

For a more detailed discussion on specific actions to defend your home network, download the **CIS Telework and Small Office Network Security Guide**

www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

The guide covers the entire lifecycle of home network equipment usage, including initial purchase, configuration, and safe disposal. The guide also provides an easy checklist that can be completed by employees to assess their networks and returned to the organization's IT department.

Contact Us
www.cisecurity.org