Week 5: Securing network devices

Our network devices, such as our modems and routers at home, are not something we typically give much thought to. Once your ISP (Internet Service Provider) or our IT staff connects them during the initial setup of your internet service, they typically just work. They provide a steady, reliable connection for all your devices – computers, phones, and more – to easily get on the internet to check your email, social media, browse the internet, watch videos and movies, and more.

The devices should be thought of like a computer though as they need the same attention in many aspects. From updates to ensuring the strongest security feature is enabled, to ensuring the WiFi network has a strong password.

Updating your devices

Your internet equipment needs updates to protect against vulnerabilities and ensure it is running the most stable version of the software.

AT&T Motorola Modem

Arris Spectrum Modem

If your ISP provided your modem or router or in some cases they integrate routers into their modems, yielding an "all-in-one" device, reach out to them to ask if the equipment is running the latest software.

For equipment provided by our CP IT department, please reach out to us at 1-800-373-7521 or helpdesk@ssndcp.org to let us know a time when we can assist with checking for updates.

Encryption on your WiFi Network

It is important to ensure that all of your data is properly encrypted when using devices on your Wi-Fi network. Wi-Fi Protected Access Version 2 (WPA2) or Wi-Fi Protected Access 3 (WPA3) are the latest security protocols your router may be running. Older protocols, WEP and WPA, both contain security vulnerabilities and should be avoided. **WPA2-PSK with AES** encryption (sometimes labeled as WPA2-Personal) is still widely used and is a secure option as it continually changes to meet security standards and maintain interoperability. PSK stands for pre-shared key and is generally the encryption passphrase.

Cisco Linksys WiFi Router

If you see a notification that tells you that you are connected to a Wi-Fi network that is not secure it's because it uses an older security standard. For example, this can occur if you connect to a Wi-Fi network that uses older security standards that have known flaws. This issue can be fixed by updating the encryption type on the router or by replacing the router. If you are seeing such a warning please reach out to us for assistance.

A strong WiFi Password

Like your user account passwords, the password to your WiFi (Wireless network) should be long and complex. It should be at least 15 characters long and include a combination of letters, numbers, and symbols.

Linksys WRT54G Wireless Router (an example of an older router that needs replacing)

Once you have it set, be sure to take tuck away for future reference, preferably storing it within a password manager, like LastPass. That way, in the event you need to reconnect your computer or get a new device that you would like to connect to, you have it handy. You may have guests that would like to connect devices too so you would need it then as well.

As we use our home networks now more than ever before, please take the time to ensure your equipment is safe from cybercriminals. Ensure the "door" to your network is secured and locked just like the front door to your home.

We are here to assist! If you have any questions or need assistance, please contact us at 1-800-373-7521 or via email at helpdesk@ssndcp.org. To check out more articles about securing your digital life, visit our security awareness section.