Stephen R Law
Director of Technology
John Stark Regional High School
Weare, NH 03281

Guide: Securing Your Home Network

With the COVID-19 crisis and the remote digital learning that is taking place, hackers are looking to exploit weaknesses in home networks as so many people are telecommuting. Since you are using a school-issued device with our security measures (Sophos, InterceptX, Windows firewall, GoGuardian, BitLocker encryption, Google apps over https), we feel our devices are in good shape. You, the human element, need to be mindful of phishing, software downloads, suspicious links. The last piece of this is your home network. Here are some steps you can take to improve the security of your home system.

Change your router password

Many home users just install a new router without changing the admin password. This list of default passwords is readily available online:
(https://proprivacy.com/guides/default-router-login-details)

Documentation on how to change the default router password is included with the quick start guides in most boxes or can be found on the support page on the manufacturer's website.

Change the default password to something STRONG. You can test the potential strength of a pasword here: https://howsecureismypassword.net/

Upgrade your router firmware

Your router is just like your computer. It needs updates periodically to add new features and enhancements but also to address security issues as they emerge. There are many guides online on how to do this, here is one:
https://www.lifewire.com/how-to-upgrade-your-wireless-routers-firmware-2487671

Here is a guide from Comcast/xfinity:
https://www.xfinity.com/support/articles/update-your-xfinity-equipment-online

Most manufacturers offer updates to router firmware for **supported** devices (if yours isn't supported, perhaps it is time to upgrade) through their websites along with support and instructions on how to do so. **I would NOT recommend getting firmware from any other site other than the manufacturer's site.**

Secure your home wireless

Securing your wireless network follows a similar path. Use good encryption (WPA2), use strong passwords for ALL networks broadcasting from your house (some routers have a 2.4Ghz and 5 Ghz networks running).

Here is one of many online guides on how to do this:
https://www.comparitech.com/blog/information-security/secure-home-wireless-network/

If your router supports a guest network (mine does), set up a network that your friends or visitors would use that is separate from your home's internal network. Some wifi devices like mine have a feature called "wireless isolation between SSIDs". This means devices on one wifi network (the guest network) can't access devices on the home's network.

Secure your home devices

Even if your router has been locked down, your firmware updated, and your wifi secured, you still have some considerations. Things like home security systems (e.g. Ring doorbells), smart speakers (e.g. Alexa) and wireless printers can all create back doors for hackers. Upgrading device firmware, changing default passwords, using strong passwords, and following security recommendations from the manufacturer all apply.

Here is a link from December on security issues with Ring doorbells that points out the security crisis in IoT devices.
https://www.wired.com/story/ring-hacks-exemplify-iot-security-crisis/

Here are some links to help (I will add to this as I find good ones).

Securing Smart Devices
https://www.dummies.com/consumer-electronics/smart-devices/10-ways-to-strengthen-alexa-privacy-and-security/