(Approx. 953 words)

Vow to Maintain Your Home Network

By Kurt Jefferson, Editor, Central Kentucky Computer Society

January 2021 issue CKCS Newsletter

www.ckcs.org

lextown2 (at) gmail.com

Now that 2020 is finally, finally, finally over, it might be time to reflect on how well our home networks held up to the strain of constant use last year.

COVID–19 is keeping many of us at home and connected via Zoom, FaceTime, and Skype. That’s putting sometimes creaky Wi-Fi Internet networks under the microscope.

And many of us have discovered our sometimes-outdated routers, modems, PCs and Macs, iPads, keyboards, mice and trackballs, and other equipment aren’t faring too well under the strain. (November’s CKCS newsletter reported that iPad sales in America rose by 31% as of mid-summer as plenty of folks replaced old equipment with newer technology.)

In March, Forbes reported that Internet use in America climbed by as much as 70% as more of us were forced to work at home, students activated distance learning, and streaming (services such as Netflix and Amazon Prime) surged by at least 12% while demand for TV via cable plummeted.

Cable TV subscriber losses in 2020 could top the population of Chicago and Houston combined, headlines one article from BGR.com. And, as NoCable.org writes, “As many Millennials enter the workforce, they simply do not see the benefit of paying over $123 a month on cable service and are colloquially referred to as ‘Cord Nevers’.”

So if you or family members are using your Internet network more than ever, you have plenty of company. Just as your car needs maintenance, so does your Wi-Fi network. Yet, many of us don’t consider this until our home Internet stops working.

Consider the following:

* **If your Wi-Fi router** is more than four or five years old it might be time to replace it. A 2012 PCWorld article says heat could be the real culprit. Wi-Fi routers tend to get very hot. If your Internet connection is getting slower and slower or drops connections more often, heat might be damaging your router’s internal parts. Try pointing a small fan on your router and see if your Internet performance improves.
* **If your cable company** provides you Internet service, consider buying and installing your modem rather than paying the cable company to use theirs. That’s one way to cut your costs. The Wirecutter has tested several top models. Read their reviews to see which Wi-Fi router might fit your budget and home.
* **I checked The Wirecutter** before buying a new Wi-Fi router late last year. My six–year–old Apple Extreme Base Station was failing. (Apple no longer makes Wi-Fi routers.) Internet connections were periodically dropping, web pages loading more slowly, and the connection speed was dropping. (I use a Mac app called WiFi Explorer from the Mac App Store to get an overview of how well my home Internet network is functioning. WiFi Analyzer for Windows is another good tool.)
* **If your home is plagued** by Internet dead zones, consider installing what’s called a WiFi mesh networking kit. The Wirecutter spent more than 200 hours reviewing 24– mesh WiFi networking kits before it chose its top pick.
* **Update your WiFi router’s firmware.** “Firmware” is one of those words that cause some folk’s eyes to glaze over. You might as well be talking to an American audience about camels: Or what’s the difference between a Dromedary camel and a Bactrian camel? But as Tom’s Guide has repeated over and over, “Your router is the most important part of your home internet setup. It’s also probably the most vulnerable.” Why bother? Well, as Tom’s Guide writes, “…Updating your router’s firmware is a pain, but you’ve got to do it.” A firmware update can protect your entire home Internet network from hackers. Just do it. Enough said.
* **Internet Security 101:** Wow. Broadband Search outdid itself when it published this website offering some of the best advice on keeping your home Internet safe and secure. You’ll read tips such as pick better passwords and choose to use a virtual private network (especially when you’re using an iPad or laptop.)
* **Turn on your Mac’s firewall.** If your firewall is off, turn it on. Visit System Preferences, click on Security & Privacy. There’s a horizontal panel at the top of the window. Click on Firewall. Then, make sure there’s a green dot next to Firewall: On. Macs come from the factory with this turned off. Switch it on.
* **Turn on your Window’s firewall.** (Make sure it’s not disabled.) securicy.com tells you how to “enable your Windows” firewall. Make sure you leave it on.
* **Run antivirus and anti-spyware software.** Learn more from PCMag and its article, “Do You Really Need to Buy an Antivirus App or a VPN Anymore?” (Obviously, the answer is YES.)
* **Protect your smart speaker.** (You know, speakers that react to your verbal commands.) If you’ve got one of the many smart speakers (Amazon, Google, Apple, and Sonos all make smart speakers) in your home, be aware they can be hacked. As Norton notes, 39–million Americans owned smart speakers in 2019. Norton’s website offers ten tips to keep your smart speakers secure.
* **Use a Passcode, Touch ID, or Face ID** on your iPad & iPhone. It’s a pain to enter a series of numbers, touch the home button or allow the camera to snap your headshot every time you use your tablet or smartphone. But consider this: An iPhone and iPad are among the two top stolen electronic devices in America. Think about it. Turn on “Find my App” on all of your Apple devices: Macs, iPhones, iPads & iPod touch. A passcode can save you plenty of grief, especially if you use your iPad or iPhone for online banking.