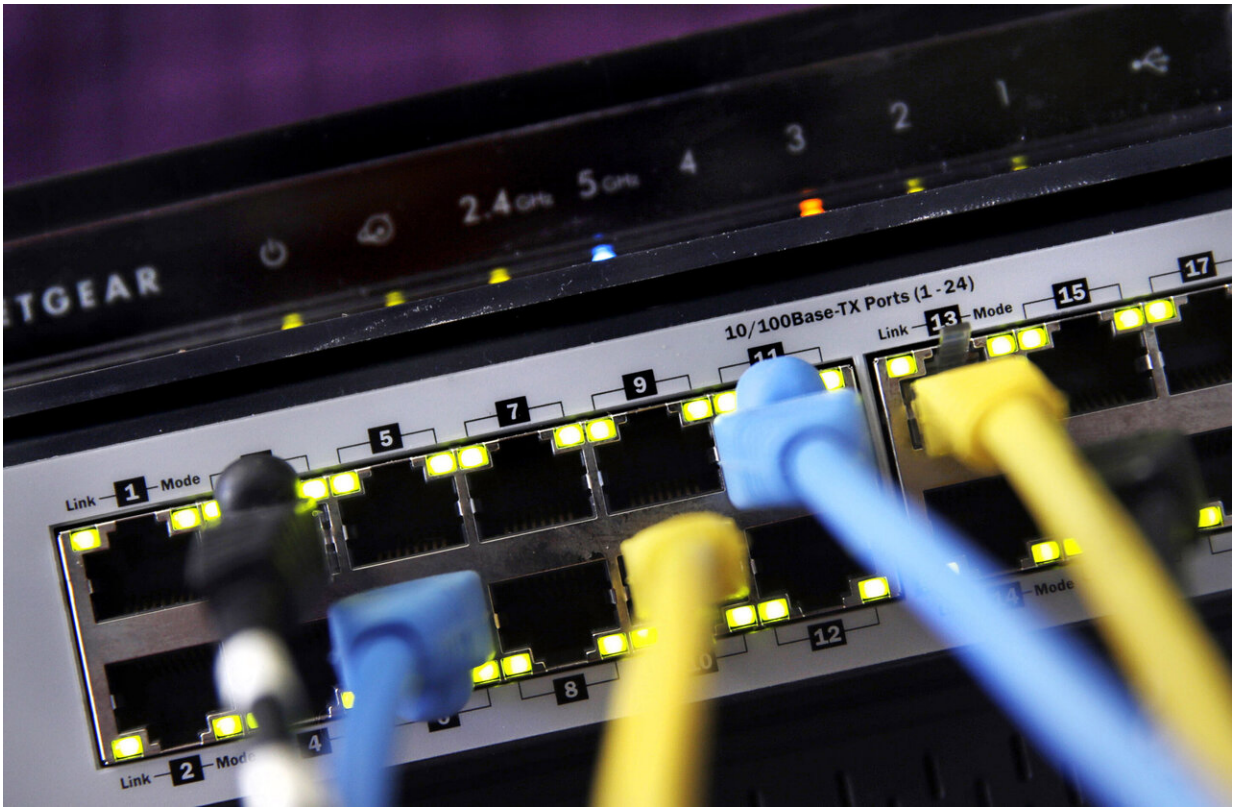
Bring in the experts: It's time to secure your home network

September 8 2020, by Frank Bajak



In this June 19, 2018, file photo a router and internet switch are displayed in East Derry, N.H. Not all that long ago, managing your home network's security didn't involve much more than installing an antivirus program on your PC. If only it were still so simple. Home networks are a major target for cybercriminals, who use innocuous smart gadgets as stepping stones to loot data from PCs and phones. Or they may co-opt the simpler devices into much larger "botnets" that can be used to wreak havoc across the internet. (AP Photo/Charles Krupa, File)

Not all that long ago, managing your home network's security didn't involve much more than installing an antivirus program on your PC. If only it were still so simple.

It's no long just about protecting the computer on which you may be working from home and the laptops the kids may be using as online school starts. Odds are good you've got a few other internet-connected devices around the house—phones, tablets, game consoles, maybe a "smart" TV or thermostat or refrigerator or light bulb or kid's toy or security camera or video-streaming gadget or voice-activated digital valet.

The average U.S. home now has 11 such devices, according to Deloitte, many of which are vulnerable to hacking. If you don't want cyber cat burglars traipsing across them, potentially spreading malware or ransomware as they go, you'll want to secure your entire home network.

WHAT ARE THE RISKS?

Home networks are a major target for cybercriminals, who use innocuous smart gadgets as stepping stones to loot data from PCs and phones. Or they may co-opt these simpler devices into much larger "botnets" that can be used to wreak havoc across the internet.

On average, one in three internet connections from home networks are made through devices other than computers or phones, so there's lots of opportunity for mischief if you don't lock your virtual windows to the networked world.

You can do it yourself, but that can be a lot of work, and the potential consequences of any mistakes could be significant. For most people, it makes better sense to pay for a network-protection service, whether offered by your internet provider or another business. Though it will cost

you.

HOW DOES THIS WORK?

Think of your home network as a bunch of cans tied to each other with strings. Those are all your in-house devices and the data they share with each other.

Now picture each of those cans tied to thousands of other strings outside your home. They are data connections your devices routinely make to other devices on the global internet. It's beyond our capacity to constantly monitor all those connections. We need help.

A good network-security service sets up firewalls to block unwanted data traffic, but it doesn't stop there. Since firewalls are imperfect, it will also monitor network traffic using artificial intelligence to detect unusual patterns. It keeps an eye on both your devices and malicious internet domains, alerting you to potential threats and blocking suspicious websites.

Typically, you'll be able to configure your security and respond to alerts from a laptop or phone. Providers let you block unauthorized users and websites from connecting to your home gadgets. Parents can also often use these services to set rules on the websites kids can visit and limits on screen time.

HOW MUCH DOES THIS COST? IS IT WORTH IT?

Internet providers now frequently offer security suites if you rent your modem or router from them. From Comcast, it costs $14 a month. Verizon charges fiber-optic FiOS subscribers $25/month but provides it for free with its premium gigabit plan.

If you recently bought your own router, security may come as a free trial and then a subscription. Or you can buy a separate service or standalone security appliance. Figure on paying about $100 a year.

"Most consumers don't have the necessary knowhow as to how to secure their home network," says Michael Philpott, a connected-home analyst with the Omedia tech research firm. "The only real option is to have a central solution that can monitor all connected devices."

Philpott says he's personally happy to pay a little extra for the peace of mind.

Start by checking out the service provided by your broadband provider or the maker of your router. Is the software easy to set up and to use? Check which security firm supplies the underlying security tools; Bitdefender, F-Secure, McAfee and Trend Micro are among industry leaders.

It's also possible to buy network-security kits directly from security companies, though you'll typically pay more for an extra monitoring device you'll add to your network. These often include anti-malware software for computers and phones.

Look for software that also lets you create two separate "virtual" home networks." Reserve one for work computers and networked data storage and use the other for smart TVs and speakers.

I'M NOT AFRAID OF TINKERING. WHAT CAN I DO MYSELF?

You're going to need to roll up your sleeves and get educated if you want to harden your home network's security on your own. Even then, if you do any kind of sensitive work at home it probably pays to shell out for extra protection.

See the links below for basic details to get you started.

More information: Basic network security: bit.ly/2Zg8pou

Protecting your router: bit.ly/334JuWc

U.S. guidelines: bit.ly/2R2Enjp

Security for working from home: bit.ly/3lWRBfY

Consumer Reports router test findings: bit.ly/2ZfWtDf