10 STEPS

TO TAKE RIGHT NOW TO SECURE YOUR BUSINESS WIFI NETWORK

01 MOVE YOUR ROUTER TO A PHYSICALLY SECURE LOCATION

Getting around many of the more sophisticated security precautions can be as simple as someone hitting the reset button on your router. It's vital to double-check that your router is in a secure location with restricted access: a locked cabinet or in an office that is always locked. You can even explore video surveillance options to have the router monitored 24/7.

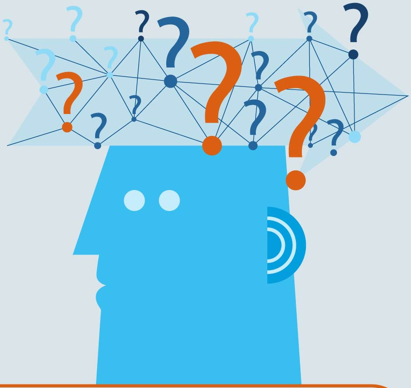
02 CHANGE THE DEFAULT ROUTER LOGIN INFORMATION

This is another tip that might seem elementary, but the truth is that the majority of hacks happen because targets don't cover the basics. The first web security precaution to take is setting a quality password and continuing to change it frequently. Most routers come with a default username and password such as "admin", and lists of default usernames and passwords for various routers can easily be found on the Internet.

The best passwords or passphrases are at least 15 characters long, with a mix of letters, numbers, and special characters. This goes double for the admin username and password that you need to log into the router in order to set the password.

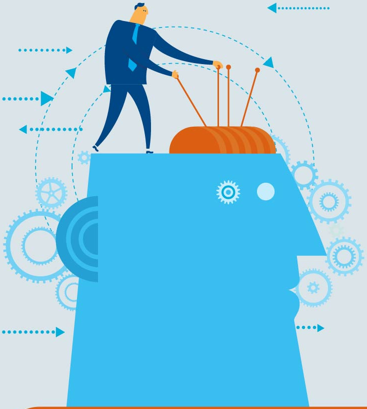
Share this passphrase or keycode with employees only as necessary. Most importantly, change the passphrase on a regular basis (quarterly is recommended) as well as each time an employee leaves the company. You can use something like How Safe Is My Password to test the security of your passwords.

03 CHANGE THE NETWORK NAME



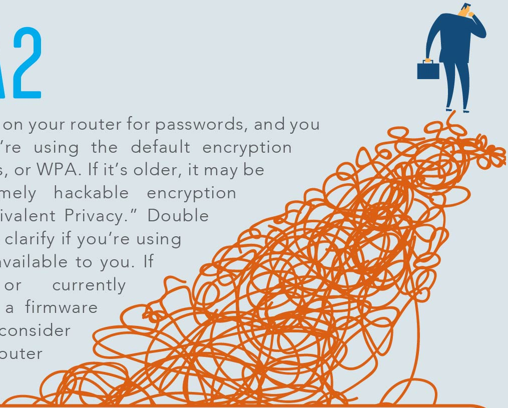
Getting around many of the more sophisticated security precautions can be as simple as someone hitting the reset button on your router. It's vital to double-check that your router is in a secure location with restricted access: a locked cabinet or in an office that is always locked. You can even explore video surveillance options to have the router monitored 24/7.

UPDATE YOUR FIRMWARE AND SOFTWARE 04

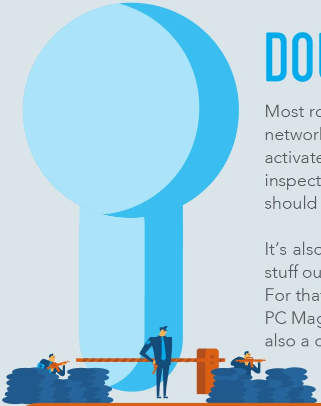


It's not exactly at the top of your to-do list, but it's still critical to your security: Periodically check to see if there have been any firmware updates for your router. These fixes are introduced to solve specific, documented vulnerabilities, so not patching them up is asking for trouble. This goes double for any network security software that you're running. Firmware updates usually self-install after downloading, making them a simple step in securing your router.

05 USE WPA2



There are usually a few options on your router for passwords, and you want to make sure that you're using the default encryption protocol WiFi Protected Access, or WPA. If it's older, it may be set to an outdated, extremely hackable encryption protocol WEP, or "Wired Equivalent Privacy." Double check your network settings to clarify if you're using the best encryption protocol available to you. If your router is older or currently WPA-incompatible, check for a firmware fix (as mentioned above), or consider upgrading to a newer router altogether.

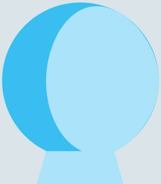


DOUBLE UP ON FIREWALLS 06

Most routers have a firewall built in that can protect your internal network against outside attacks, but it might not be automatically activated. It's generally called something like SPI (stateful packet inspection) or NAT (network address translation). Either way, it should be turned on and enabled in your router settings.

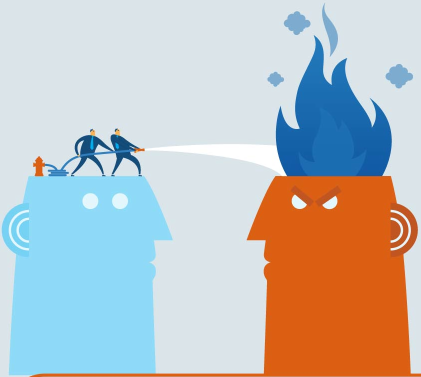
It's also important to make sure your own software doesn't send stuff out over the network or the internet without your permission. For that, you'll want to install firewall software on your PC as well. PC Magazine's top pick is Check Point ZoneAlarm Pro, but there's also a default firewall that comes with Windows.

07 SET UP PRIVATE ACCESS AND PUBLIC ACCESS



Having both employees and the public alike on the same network is a recipe for trouble. To separate the traffic, consider using a Service Set Identifier (SSID) to make two separate points of access to your network: a business-grade secure access point for your team, and a public one for customers. This isolates your business's computers from guests, providing an extra layer of protection.

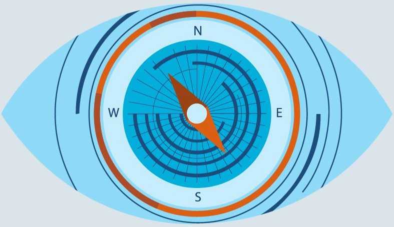
ELIMINATE ROGUE APS 08



A rogue AP is any unofficial access point to your network. These are often created by someone on your network who has bad connectivity in their office. The problem is that they might not be configured as securely as the rest of your network, giving attackers a window of vulnerability. Take the time to occasionally do access point scanning if your network is large enough.

09 TURN OFF WPS

Wi-Fi Protected Setup, or WPS, is the designed to make pairing a device with an encrypted network as easy as pushing a button. The problem is that it makes it simple for anyone with even a moment of physical access to your router to gain a foothold to your network. Again, it's important to keep your router in physically secure location. In addition, consider turning off this function unless you need it for something specific.



LIMIT OR DISABLE DHCP 10

The Dynamic Host Configuration Protocol (DHCP) server in your router is what IP addresses are assigned to each device on the network. You can limit your DHCP range to theoretically limit the number of things on your network, but that might be impractical with all of the different devices we use today that need a WiFi connection.

You could also simply disable DHCP entirely. This would mean that you'd need to go into each device and manually give them an IP address. This gives you a lot of control, but is fairly labor-intensive, depending on how many devices you need up and running on your network.

COX Business®
www.coxbusiness.com