Networking

Your home network handles a large amount of your traffic for most, if not all of your devices. If someone gains access to your router, they can view all traffic going in and out, and if you aren't using a VPN--all of your web traffic is fully visible. On top of that, routers are *susceptible to malware infections, like the recent widespread one in the US, as well as password cracking, since routers are always live and people have unlimited time to figure out the password.* Luckily, there are lots of things we can do to secure our home routers. Let's do it!

Promotional Spot

First, make sure your router is using at the very least *WPA2 encryption, since the previous WEP encryption allows anyone with half a mind to get into your router. It's been cracked for years and it's criminal for it to still be an option.*

The next thing is to change the default password. Manufacturers have been getting better about this, but some models of routers use the same default password; meaning if someone gets the model of your router, they can search online what the password is and you're, in a nice way, screwed. *Go to this website and search for your router, hopefully it doesn't use the same password.* Even if it doesn't, *most default passwords aren't strong enough, so you should still change it, more on that soon.*

Before getting into the password, let's discuss how to make sure attackers can't figure out the model for our router. First, make sure the SSID, *the public name of the router, doesn't reveal anything about the router, or yourself. Revealing the router model is a security concern. And giving personal data is a privacy concern.* It's good to use random SSIDs like *"Furry Lemur", "Nutella Sticks", or my personal favorite: "That's what she SSID"*. Don't forget to double-check the visibility of your router and make sure it isn't visible from any easily accessible window or door.

As for the password, you should be using the password *rules outlined in lesson 3.4* to get yourself a secure password, which no one will be able to crack within their lifetime (using current technology).

Okay! Now, you have a router using at least WPA2 encryption, a non-revealing SSID, and a super secure password. These precautions have no effect on your convenience besides typing in a complex password once on each device. All of this should be implemented by everybody.

Some of you watching might be asking, should I hide my SSID altogether? *Hiding your SSID will hide your router on the list of visible devices, requiring you to manually input the SSID and password.* This seems like it's more secure, since it requires someone to know both your SSID and password to connect to the router. But, it doesn't make that much of a difference. *Certain operating systems leak your SSID, and tools used by hackers can see the SSID anyway.* So the only person this protects you against is your not so tech-savvy neighbor looking for free wifi. No matter what, hiding your SSID won't work against you, it just won't really protect you from genuine threats.

What are some other things you can do to improve the security of your router? Glad you asked :)

Like we've mentioned *earlier in lesson 3.2,* make sure everything is up to date--including your router. **** hold manual **** Refer to your manual for instructions and do this as often as possible to receive the latest security patches.

A big no-no is using the WPS button to connect to your router. *WPS is a button you push that lets you quickly connect to a wireless connection without typing a password.* All it takes is physical access for someone to connect to your network. On top of that, *attacks like Pixie Dust can crack WPS-enabled routers in hours.* In short, disable WPS.

You can take your security a step further by only allowing a connection to a specified device via a MAC address, we discussed these in the previous lesson. *This way, only devices you specify connect to the router, and any other device is blacklisted.* But, similar to hiding your SSID, this won't stop an experienced hacker, *since tools like aircrack-ng r*eveal the authorized MAC addresses, and the attacker can spoof the MAC address to mimic an accepted device. So, once again, this will only help keep out your neighbor.

Something I'd recommend you do do, is installing a VPN on your router, *which will route every device on the network through the VPN. Not only does this mean you don't need to worry about VPN software on every device, but it also allows you to connect devices like your Xbox and other electronics to the VPN. Not to mention that a router counts as one device, allowing you to connect a huge number of devices to the VPN service-- a little workaround for VPN device restrictions.*

The last thing you can do, although more technical and on the advanced side, is installing custom firmware on your router, specifically *openWRT or pfSense. openWRT is FOSS and based on the Linux kernel, giving you much better security than most proprietary firmwares that came with routers The other option is pfSense, another FOSS firmware based on FreeBSD.* It's known to be extremely

reliable and secure, although more advanced to set up than OpenWRT. They're both very good, so I would research the features to see what's best for you, *although keep in mind not every router is compatible, so make sure to check beforehand if your device is supported.*

Queue Outro Promos

That is all I have to say about routers. They aren't crazy complex, and it's one of the most important devices to lockdown, so make sure you're implementing this as soon as possible. The next lesson is going to *talk about radios, how they're used to track you,* and what you can do about them. Thank you for watching, and I will see you then!