# Securing your wireless network

- We talk all the time about computer scams and being secure online.
    - Installing a third-party free or retain antivirus.
        - Although Microsoft's Windows Defender (formerly Microsoft Security Essentials) may be sufficient, it is also a big target.
    - Keep good practices by:
        - Not clicking on pop-ups or phony security warnings not from your installed antivirus software.
        - Not opening attachments to emails or contained links unless you have verified it is from whom it claims.
            - Or just always going to the site directly and NEVER using the links.
- An area we might ignore or take for granted is the actual wireless signal we ourselves are producing and relying on.
- In order to have a wireless signal, we need a network.
- We use a router, or ISP provided modem and router combined.
- When we install the router (or have installed by the ISP), it is usually set up "**secured**",
    - Meaning in order to connect to our wireless network (our signal or SSID), we need to either provide a network key, sometimes referred to as a passphrase or password.
    - That prevents just anyone from connecting to our network.
        - And seeing all our devices (computers, printers, hand-held devices).
- However, what most do not consider is protecting the access to their **Router Configuration Utility**.
- Only some router software, during installation creates a unique password also for entering the Router Configuration Utility.
    - All routers require an ID and password.
    - The router does have an ID and password provided by the manufacturer.
    - That ID and password however is the same for the entire model series, or even the entire manufacturer line or routers.
    - Mal-intents know, or can easily find those default IDs and passwords.
- Once into the router configuration utility, you can find all the device IP addresses attached to that router,
    - And often even the network security key.
    - Once in the Router Configuration Utility, some unscrupulous person can even change the security key and set up an administration password (the password needed to enter the Configuration Utility.

## Securing your wireless network

- If you reset your router for any reason,
    - Often done because the network security key has been lost or forgotten.
    - You remove all security to both the router and the network.
        - In other words it is now in a state which anyone can connect to.
    - You must either run the initial installation program, or enter the Configuration Utility to restore security.
    - Be sure to use WPA or WPA2 (WPA Personal).
        - Don't use WPA Enterprise.
        - Enterprise requires a server (such as in businesses) to authenticate your credentials.
- Using your Router Configuration Utility is what we are discussing this evening.
- Understand, no one is entirely hack-proof.
    - It depends on the persistence of the hacker.
    - But some measures can reduce your likelihood.

**Knowing your Router and Configuration Utility**

- Every router has a default IP address which you can insert into a browser address bar, such as 192.168.1.1.
    - You can find your "default gateway" by googling the manufacturer, within the user manual, or by opening a Command Prompt (search **cmd**, then type into the black box which appears **ipconfig**.
- When you type in the IP address, and hit ENTER on the keyboard,
    - A box opens requesting the User ID and administration password.
    - This is not your computer's administrator password (if you have one).
- The information they are requesting is specifically provided by the manufacturer (unless you or your installer did in fact change the default).
    - Google for the default password of your specific mode router, or refer to the user manual, under manual setup, advanced setup, or some similar phrase.
    - The default ID is often either the word **admin**, or left blank.
    - The default password is often **password** or **default**.
- If the default password doesn't work, it is likely (assuming you have the correct default information) whoever set up you router did provide a unique password.
    - The User ID is often set and cannot be changed.
    - The password is always changeable.
    - Try using the same password as the password to connect.
    - As a last resort, you can reset the router, and start over.
        - Usually a small button requiring a pin or pen tip to hold in.
        - Remember, if you do that, either set up the security key and SSID identical to the original, or you will need to change the settings in all your devices.
- Once into the Configuration Utility, look for Advanced or Administration to change the router access password.

## Securing your wireless network

Other Router Security measures available

- MAC address filtering
    - Every computerized electronic device has a MAC address (media access control).
    - You can set it so the router will only allow specific MAC addresses to connect.
    - This will also prevent friends or family t connect new devices without re-entering the Configuration and adding their devices.
- Disable any remote router administration ability
- Using public wireless makes you a target for hackers.
    - Increases the risk of being infected with Trojans, keyloggers, remote administration tools (RAT)
- Use strong passwords
    - Avoid merely use known words, as these can be discovered more easily.
    - Use run together words.
        - Instead of rooster, use henrooster.
        - Or avoid real words altogether.