Wi-Fi security, explained.

Almost every week, we hear that yet another company has been “hacked”. Some-body has broken into their data networks and stolen valuable private information like the personal identification, credit card and banking information of their custom-ers.

But it’s not just large organizations that get attacked. If you have Wi-Fi in your home, you also have a data network and you could be vulnerable, too.

Why would anyone bother targeting my small Wi-Fi network?

If you bank and shop online, a lot of your own confidential data travels over your network. You may also keep private information on the computers, phones or tab-lets that you use to connect to your Wi-Fi. If your Wi-Fi isn’t secure, all that informa-tion could be targeted.

Finally, other people may try to use your Wi-Fi simply to avoid paying for their own. You may think this isn’t an issue if your Internet plan has unlimited data, but having too many devices connected to your Wi-Fi network can slow it down dramatically.

What kind of security should I have on my network?

In your home, you have a gateway (also known as a router, modem or access point) that you use to connect to the Internet. Most devices offer a choice of three ways to secure your network:

1. MAC Filtering: Every device in the world that's capable of connecting to a Wi-Fi network has a unique Media Access Control (MAC) address (sometimes also called a Wi-Fi address), in exactly the same way as you have a unique street address. No two devices have the same MAC address, so theoretically, you could tell your network only to connect devices you know. However, man-ually entering MAC addresses is a cumbersome process, and whenever you send something from one of your devices, your transmission is unencrypted and includes that device's MAC address. Hackers who might be monitoring Wi-Fi networks in your neighborhood can easily copy the MAC address and get into your network. There are also other ways they can "spoof" MAC ad-dresses and break in to your network.
2. WEP: This stands for Wired Equivalent Privacy and, as the name suggests, was designed to give wireless networks protection that's equivalent to wired networks. This is the oldest security option and it requires every device to pro-vide a password before it will allow them to connect. Unfortunately, hackers have found too many ways to get past this option.
3. WPA2: Wi-Fi Protected Access 2 (WPA2) also requires every device to provide a password in order to connect. It uses strong encryption to protect your data and is currently the best way to secure your Wi-Fi network. This is the most recommended option, and you should choose a strong password that cannot be easily guessed by other people. (There was a version 1, simply known as WPA. WPA2 is an improvement.)

Please note: These options can only prevent unauthorized access to your Wi-Fi network. You still need anti-virus protection to protect the apps and information on your computers, tablets and mobile devices. Every time you go online, use social media, browse a website or open an email, you could be vulnerable to viruses, worms, trojans, malware and other attacks. Ask an expert at your favorite computer store to recommend a good anti-virus application.