This was a poster and research I did for people I knew, on how to keep safe working from home during covid

The reason why I am writing this is due to Covid-19 forcing most people to work or study from home. For most of us this means we are using our own personal WIFI to connect to work systems or school documents instead of the secure network we are all used to having in the office. This means that we are now more open to attacks by common WIFI attacks than ever before.

Why this is important?

This is an important issue as during this period of work from home, there has been a higher amount of scams based on targeted emails than in previous periods. This shows that attackers are already thinking of ways to take advantage of the new landscape and are being proactive in changing their tactics to exploit this.

I have chosen not to focus too much on email scams as most people are already aware of these potential scams. I am going to write about less commonly known scams and threats, that are not known to people outside of the cyber security circle. I will be talking about war driving and free Wi-Fi scams.

War driving

This is an attack technique where the attacker will typically be in a car with a laptop and a small Wi-Fi antenna. They will drive around areas and while they drive around the laptop will be storing the information that it is receiving from the antenna. Then the laptop will be running a program that will be logging the data given to it into a map which will have the address and information needed for the attacker to go back and break into your Wi-Fi. The information that is being checked is which router version or brand it is and if there is a password on the Wi-Fi, attackers will try to crack the password by using default passwords that come with that specific router. This is information which anyone can find by doing a google search for the instruction manual of the router which will normally have the password within it.

Dangers

If attackers get onto your home Wi-Fi network this is a big issue as once they are on, they are able to see everything you are doing or connecting to. So if you are working on contracts or deals for your company , they will be able to see all of it and make use of it other by attacking the company you work for or selling the data if it is important on the dark web. The main thing that most people should be worried about is that when we are shopping from home, when we put in credit card information for payment, the hackers will be able to see this and then use our credit card for their own personal payments.

Ways to Mitigate

Change your router password to something secure (10 characters upper and lower, 1 special case)

Make sure the WIFI has a secure password too not e.g. Homewifi1

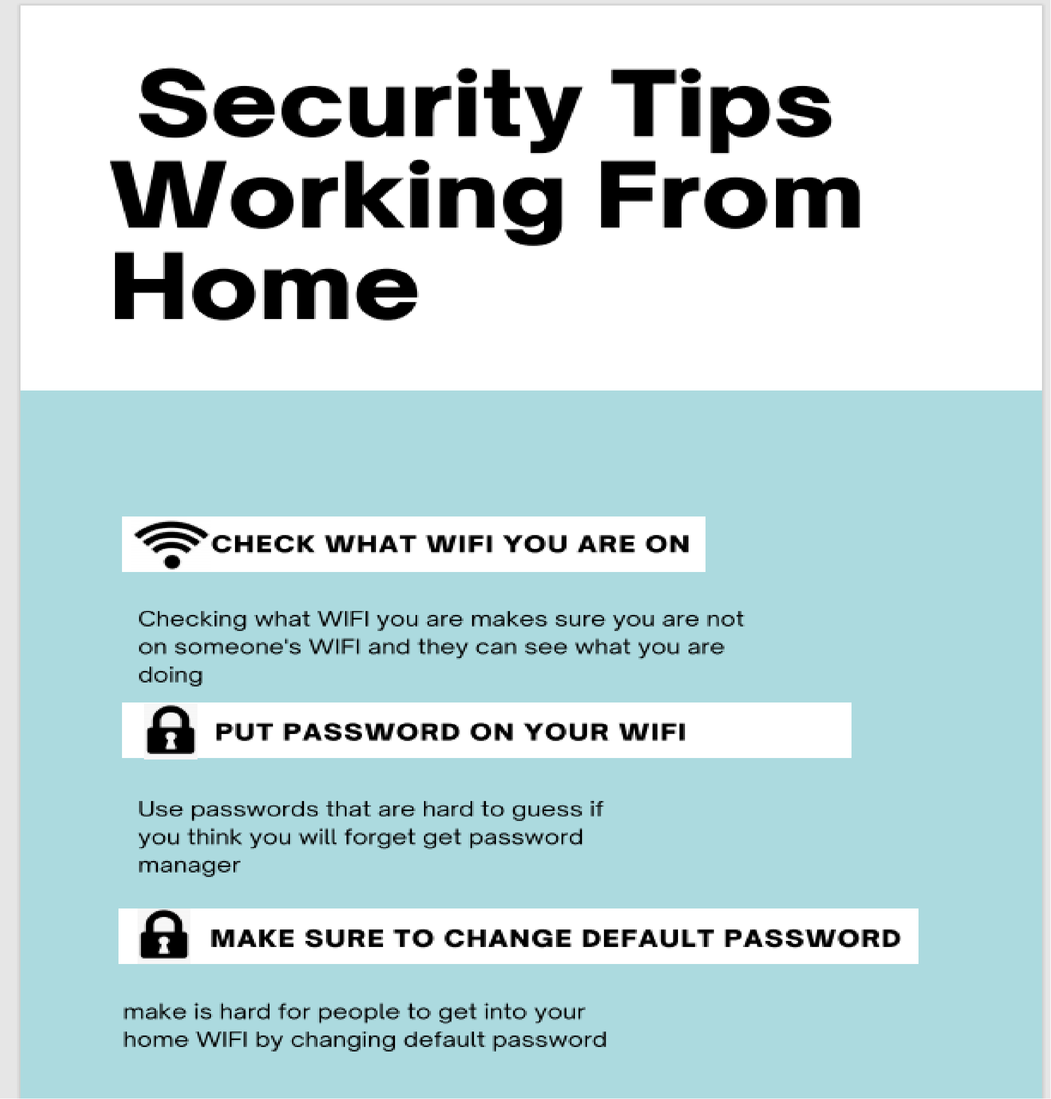
Reason to believe attack

The link below is from someone using the basics of this attack in the Netherlands. This is important as we have seen it happening over a year ago to big organisations, and now more people than ever are using home Wi-Fi as most people are working from home on laptops. This hack is not difficult to pull off and requires a tool that costs £99 that is widely available meaning I believe this will be the next wave of cyber-attacks we see. I think this attack will be used as a widespread attack tactics, not targeting a specific person, but attacking an area to see what initial information they are getting, and then deciding who to focus on.

https://fractionalciso.com/wifi-pineapple/

Poster

Below is a poster you can stick on the fridge or round the house so everyone can see it in the house and know how to defend against it.



Security Tips Working From Home

CHECK WHAT WIFI YOU ARE ON

Checking what WIFI you are makes sure you are not on someone's WIFI and they can see what you are doing

PUT PASSWORD ON YOUR WIFI

Use passwords that are hard to guess if you think you will forget get password manager

MAKE SURE TO CHANGE DEFAULT PASSWORD

make is hard for people to get into your home WIFI by changing default password