**Common network vulnerabilities**

**Insecure wireless networks**

An insecure wireless network is a network that can be connected to without any type of security features like a password or login. Unsecure networks lack cybersecurity measures that keep your information safe, they won’t have protections built into the network to prevent hackers. Public WI-FI networks are often unsecured, and connecting to them can be risky.

**Things not to do when using public wireless networks.**

* Connect to secured public networks whenever possible.
* Think about using a more secure web browser (e.g., Brave, Firefox) so you can enable features like always using HTTPS and secure DNS.
* Use a virtual private network (VPN) solution to ensure your privacy and anonymity are protected when you use public Wi-Fi. In addition, never access personal bank accounts, and sensitive personal data on unsecured public networks.
* Enable secure DNS in your web browser of choice so that all your searches are encrypted.

**Risks of using public Wi-Fi**

1. **Unencrypted networks** – Public Wi-Fi networks are often unencrypted, which means that data is transmitted in plain text and can be easily intercepted by hackers.
2. **Forced installation of malware** - Hackers can force the installation of malware on your device, which can cause damage to your device and steal your data.
3. **Malware distribution** - Public Wi-Fi networks can be used to distribute malware to your device, which can cause damage to your device and steal your data.
4. **Wi-Fi snooping and sniffing -** Hackers can use software to monitor your online activity and steal your data.

It is very important to note that even secured networks can be risky, and the level of security that you will find on Wi-Fi networks will vary greatly. Therefore, you should always use public Wi-Fi with caution and avoid accessing sensitive information when connected to public Wi-Fi networks.

Ways to determine if a public Wi-Fi network is secure:

* Look for encryption.
* Use a VPN
* Check the network name.
* Avoid sensitive activities.
* Use a personal hotspot.