RISKS OF DEFAULT PASSWORD IN IoT DEVICES (CCTV) AND HOW TO MAKE THEM MORE SECURE.

IoT devices are devices that can connect to the internet or other networks and communicate with other devices or systems. They can collect, process, exchange and use data for various purposes, such as automation, monitoring, security, entertainment and health. IoT devices are becoming more common and popular in our daily lives, as they can make things easier, smarter and more efficient. Examples of IoT devices are sensors, smart home devices like smart speakers and smart wearables.

Some of the risks of default password in IoT devices are hackers can easily access and control your devices,steal your data, or launch attacks on other networks. For example, hackers can use voice assistants yo obtain sensitive information, spy on you through your camera, or unlock doors. Moreover, hackers can create large networks of compromised devices, called bot nets, that can be used to perform distributed denial-of-services (DDoS) attacks on websites or servers. For example, the Mirai malware infected hundreds of thousands of IoT devices by using common default user names and passwords and launched a massive DDoS attack that disrupted major internet services.

In addition to that, hackers can exploit vulnerabilities in your devices that may be fixed or updated by the manufacturers. For example, some IoT devices have hard coded passwords that cannot be changed or shared passwords across a family of devices, making them easy targets for attackers.

Default password in IoT devices can be made secure in different ways. Firstly, change the default password of your devices to strong and unique ones that are hard to guess. You can use a password manager to generate and store your passwords securely. In addition to that, update your devices regularly to fix any security vulnerabilities and bugs. You can enable automatic updates if possible or check the manufacturer's website for the latest firmware. Furthermore, use a secure network to connect your devices to the internet. You can use VPN to encrypt your traffic and prevent hackers from intercepting your data. You can also use a firewall to block unauthorized access and a separate network for your IoT devices to isolate them from your other devices.

Besides that, disable any unnecessary features or services on your devices that you don't use or need. For example,you cab turn off the microphone or camera when you are not using them or disable remote access if you don't need it. Moreover, review the privacy settings and permissions of your devices ands apps. You can limit the amount of data that they collect and share with third parties. You can also opt limit the amount of data that they collect and share with third parties. You can also opt out of any data collection or analytics programs that you do not agree with.