TIPS TO PROTECT SMART HOME DEVICES



Change Default Usernames and Passwords: Smart devices and gadgets often ship from the factory with default usernames and passwords. For example, the username is often **admin**, while the password is either also **admin**, or **1234**. Always change the default login credentials for your smart devices.

Secure Your Home Network: Use a strong Wi-Fi password and enable the network security features available on your home router. Smart devices are likely to be connected to your home or corporate network, the same network used for banking and other sensitive transactions. You may need to consult your ISP or a security professional for this one.

Use a Separate Network for Smart Devices: Consider setting up a guest network for your smart devices to isolate them from your primary devices; this provides an extra layer of protection. Smart devices often have limited security capabilities; sometimes they simply cannot accept a password longer than four numeric characters.

Updates Matter: Regularly update the software on your smart devices. These updates can add new features; more importantly they fix security weaknesses (vulnerabilities). Failing to keep software updated makes it easy for cyber criminals to gain access to your network, devices, and data.

Monitor Device Behaviour: Be vigilant for unusual or unexpected behaviour from your smart devices. If you have smart lights, and you notice the lights going on and off unexpectedly, you might assume it is malfunctioning. It could also be early signs of a cyber breach. Remain vigilant for anomalies.

Disable Unnecessary Features: Turn off any features or services on your smart devices that you are not using. It is easy to forget to update or configure features that we do not use often. It is best practice to disable or uninstall features and software that you do not require.

Secure Physical Access: Physically secure smart devices to prevent tampering. Unauthorised physical access can easily lead to compromise of smart devices. Most smart devices have a physical reset button that will reset the device settings to the default factory settings, including the default password (often 1234). As far as possible, restrict physical access to your smart devices.

GRANT HUGHES
SPEAKER - AUTHOR - ADVISOR

CyberAwareness
Influencing change, one message at a time