BE SMART AND SAFE

Smart Home Protection

12 easy steps to secure your Smart Home

NTUC LEARNING HUB

CYBINT SOLUTIONS
Cyber Security Boot Camp
(2nd Cohort 2021)

"IoT without security = Internet Of Threats" – Stephane Nappo

1. Give your router a name.

Change the name the manufacturer gave it – it could identify the make or model (eg. TPlinkxxx) where there are known vulnerabilities. Give it a unique name not associated with you or where you live. Giving away your personal attribute is not wise.

2. Use a strong encryption method for Wi-Fi.

When you setup your network, use a strong encryption method, like WPA2 or higher. Change the default router username & password. This will improve your network security.

3. Setup a guest network.

Keep your primary Wi-Fi network private for yourself & home users. Visitors, friends and relatives can log into a separate network that is separated from your IoT devices.

4. Change default usernames and passwords

Most of the IoT devices come with default username & password (eg. admin, 0000, etc). This makes it easy for hackers to access your IoT devices to extract information about you. Any IoT devices using the default password are likely to be hacked.

5. Use strong passwords for Wi-Fi networks and devices.

Use unique & complex passwords made up of alphanumeric & symbols instead of simple & predictable password, such as "0000", "pass" etc. If such practice is not enforced, it increases your chance to be hacked especially when your IoT devices grew in your household.

6. Check the setting for your devices

Always check the privacy & security settings of your IoT devices. Some default settings could benefit the manufacturer more than you would expect.

"Passwords are like underwear: don't let people see it, change it very often, and you shouldn't share it with strangers." – Chris Pirillo

"One single vulnerability is all an attacker needs" – Window Snyder

7. Turn off features you do not need.

Some IoT devices include feature such as remote access & is often enabled by default. Remote access is the ability to access a computer or device from another device, at any time, and from anywhere. Be sure to turn it off if you do not need it.

8. Update your software as soon as it is available.

Mobile software update is important to patch a security flaw. Mobile security is vital since most of your IoT devices are connected to it. Similarly, be sure to download updates for your IoT devices as well.

9. Perform check on aging IoT devices on your network.

Your old security camera might need an upgrade to offer better security. Older devices have more vulnerabilities & it is prone to cyberattack.

10. Do the two-step authentication (2FA)

Two-factor authentication is the way to go to keep the bad guys out of your private accounts. Use it whenever possible.

11. Avoid public Wi-Fi networks.

Never use public Wi-Fi networks unless you are on a VPN (Virtual Public Network). As much as you like to manage your IoT devices through your mobile devices from your favorite cafe, this is definitely a bad idea.

12. Buy from trusted brand.

Cybersecurity is a top priority for consumers, but not always for brands. Do your research: look up the brand's website and search opinions on news-sites and forums. The time & dollars invested could give you a better return on privacy & most of all giving you a peace of mine.

"Technology trust is a good thing, but control is a better one." – Stephane Nappo