**FEROZE SODHI** - *CEO at Z Plus Cyber Security*
www.zplus.net.au
Email: info@zplus.net.au
Cyber Security Trainer and Consultant

## TIP 1. MUST CHANGE DEFAULT CREDENTIALS

Must change ALL the Default Credentials of your IoT devices. Especially of your Router Login Credentials. I'm not only talking about Wi-Fi username and password. But, the one you generally use to logon to the modem's home page at https://192.168.0.1 (this IP may vary from provider to provider, refer to your router booklet).

## TIP 2. TURN OFF YOUR IOT DEVICES INCLUDING ROUTER ONCE IN EVERY 24 HOURS

TURN OFF your IoT devices, including router, for at least 1 minute in every 24 hours (if possible). It will disconnect all temporary connections, if any. This is because some malwares reside in your device's RAM only.

## TIP 3. CHANGE YOUR PASSWORDS ONCE IN 3 MONTHS (EVEN MONTHLY, IF POSSIBLE)

Must change your all passwords once in every 3 months (even monthly, if possible). In this way, hackers will not be able to login to your accounts using stolen passwords.

## TIP 4. CONVERT YOUR PASSWORDS WITH MEANINGLESS PASSPHRASES

Change your passwords with a meaningless passphrase; plus combinations of upper, lower, numeric and special symbols. In this way attacker/hackers will not be able to guess it from your publicly available information.
e.g.: UncleRailwayHorse12!@

## TIP 5. REGULAR OFFLINE AND OFFSITE DATA BACKUP

Make sure you are taking regular data backups; and you also have backup copies offline and off site. This practice will help you to recover from incidents like a cyber attack or natural disaster.

## TIP 6. MULTIFACTOR AUTHENTICATION (MFA)

Must enable Multi Factor Authentication (MFA) on your all accounts (wherever possible). You can use OTP on your mobile device or Google Authenticator or Microsoft Authenticator etc. It will protect your account from hackers as you need a combination of more than one key to access your accounts.

## TIP 7. UPDATE SOFTWARE / OPERATING SYSTEMS

Make sure your all software and Operating Systems are up to date and all patches are installed.
BE AWARE OF FAKE UPDATES. VISIT VENDOR'S WEBSITE AND COMPARE YOUR SOFTWARE VERSIONS. HACKERS ARE SENDING PUSH NOTIFICATION IN YOUR SOFTWARE TO INSTALL MALWARE THROUGH FAKE SOFTWARE UPDATES.


## TIP 8. STAFF TRAINING

Humans are the weakest factor in your Cyber Security Chain. You, and your all staff members, must be fully trained and aware to deal with cyber incidents.

## TIP 9. DO NOT INSTALL FREE APPLICATIONS / SOFTWARE / PIRATED SOFTWARE

Do NOT install free applications/software unless they are from reliable and authentic sources. For example:- application from your bank or government are fine. But think twice before installing any third-party free applications, because you

don't know who the developers are and what sort of code they have embedded behind the scenes.
Pirated software are another cyber security threat. You will not get security updates/patches for pirated software. Therefore, vulnerabilities (if any) will remain there for hackers.

### TIP 10. REMOVE UNWANTED SOFTWARE AND USER ACCOUNTS

Remove all unwanted software and user accounts from your systems immediately.
Security patches are not available for obsolete software (most of the time).
Unwanted/ex-staff user accounts are risks to organisations. Someone may login and can cause damage using these types of accounts.