DR. AMMAR ALAZAB *Senior Cyber and Networking Security Lecturer in School of Information Technology & Engineering (SITE), Melbourne Institute of Technology*
LinkedIn/Website: https://www.mit.edu.au/about-us/academic/school-it-engineering/people-and-contacts/ammar-alazab

TIP 1. LIMIT ACCESS TO INFORMATION

This idea is referred to as the: 'principle of least privilege'. Employees should be able to access only the information they need, and only for the period required to perform their tasks. Granting permissions to a user beyond the scope of the necessary rights of an action can allow that user to obtain, or change, information in unwanted ways.

TIP 2. USE ANTI-VIRUS PROTECTION AND FIREWALL

Antivirus and Firewall should be used. Antivirus help to monitor a network or systems for malicious activity or policy violations. A firewall is a security measure that protects your device/s from unapproved access.

TIP 3. SEPARATION OF DUTIES

Work is divided up. Each team member performs only their portion of the task sequence. Separation of duties is used to make it difficult for an individual to violate information security and breach the confidentiality, integrity, or availability of information,

TIP 4. MULTI-LAYER SECURITY

Information security must be created in layers. Can be useful in resisting a variety of attacks. Layered security means protecting digital assets with several layers of security. If a hacker manages to breach one security measure, all sensitive data is still protected by the other layers of security that are in place. This makes it harder for a hacker to perform a successful cyber attack

TIP 5. DIVERSITY

Layers must be different. If attackers penetrate one layer. Same techniques will be unsuccessful in breaking through other layers. Breaching one security layer does not compromise the whole system

TIP 6. OBSCURITY

Security through obscurity is the principle of protecting things by hiding them. Obscuring inside details to outsiders. Difficult for attacker to devise attack if system details are unknown. Not revealing details such as type of computer, operating system version and brand of software used. Security through obscurity is reliance upon secrecy in software development to minimise the chance that weaknesses may be detected and targeted.

TIP 7. KEEP YOUR SOFTWARE UP TO DATE

Updates help patch security flaws. To prevent known vulnerabilities from being exploited, all software must be kept up to date. This means installing patches released by the software developers to close security holes found in their products. A software vulnerability is a security hole or weakness found in a software program or operating system. Hackers can take advantage of the weakness by writing code to target the

vulnerability.

TIP 8. AWARENESS ABOUT MALWARE

Effective security awareness training helps people understand proper cyber hygiene, the security risks associated with their actions and to identify cyber-attacks they may encounter via email and the web.

TIP 9. SET UP MULTI-FACTOR AUTHENTICATION

It will enhance your organisation's security by requiring your users to identify themselves by more than a username and password. It is an added layer that essentially double-checks that a user is, in reality, the user they're attempting to log in as - making it much harder to break.

TIP 10. USE A SECURE WI-FI CONNECTION

It's important to ensure the network is secured with Wi-Fi Protected Access security protocol. These security protocols encrypt your activity, making it harder for unauthorised parties to trace your online activity back to your device and gain access to personal data.