ANOO DOWLUTRAO *Cyber Security Consultant, DXC Technology Australia*
www.linkedin.com/in/anoopama-dowlutrao

Anoo has over 10 years experience in the banking sector. Cyber security is one of the top concerns of the banking sector. There are numerous ways to break into an account and this is when the curiosity about cyber security started. While Penetration Testing is one of her main interests, Anoo is pursuing the CEH and CISSP. She is currently managing cyber projects and ensuring her clients are happy and in safe hands.

TIP 1. STAFF AWARENESS OF CYBER SECURITY

Security awareness training is a must nowadays. The company can conduct security awareness training every quarter to educate the employees about common scams and how to avoid being hacked. The training materials must always be up to date with the ongoing evolution of technology and hacking techniques.

TIP 2. CREATE SIMPLE CYBER SECURITY POLICIES

Cyber security policies need to be created and distributed to the employees. There should be a clear set of rules of cyber security policies for all the employees to follow. These rules will vary from business to business and may contain rules about policies of usage of social media, bringing your own devices (BYOD), and authentication among all.

TIP 3. CONTROL ACCESS TO DEVICES

Every access point poses an individual risk, so limit access to each employee, depending on their roles and responsibilities. There must be a clear policy about the different layers of system rights and privileges. Administrative privilege should be given only to staff who requires them to minimise the risk.

TIP 4. MAKE USE OF MULTIPLE LAYERS OF PROTECTION

Use strong password policies and make it a company policy for all employees to follow. The employees must make use of strong passwords; which must be changed regularly. Applications such as antivirus and VPN will ensure the networks and endpoint are safe from attacks.

TIP 5. ALL SOFTWARE MUST BE UP TO DATE

The software on devices must be up to date. Outdated devices are often the source of weak protection and easy prey for hackers. There are often patches updates or version updates and the employees must be aware not to ignore those updates. The company should have clear guidelines about software updates and make sure everyone follows them by sending regular communications.

TIP 6. HAVE A RISK ASSESSMENT REGULARLY

Conducting regular checkups is healthy for the business. After doing the risk assessment, try to fix the issues in order to minimise any risks. This will enable the employees and employer to be safe in case of an emergency.

TIP 7. COMMUNICATE CLEARLY TO EMPLOYEES

Sometimes the emails regarding important information are being missed due to wrong formatting and long emails. Important emails must be clearly labelled as "Urgent" or "Important" so that it drags the attention of the employees. Any incident must be communicated immediately with an urgent label. The document should also be labelled as public, internal, commercial, or restricted, so as not to bridge any confidentiality act.

TIP 8. HAVE AN INCIDENT RESPONSE PLAN

Along with the risk assessment, there must be a clear incident response plan. The incident response plan will enable the employees to follow guidelines and prevent further incidents or losses to the company. Have a risk register of all the risks the company might face and some proposed solutions from cyber security experts

TIP 9. SECURE ONLINE PAYMENTS

Nowadays everything is online, and businesses are often scammed with false invoices to make payments. Create some rules such as if the payment exceeds a certain amount, the accounts team will have to call and authenticate that payment or there must be a four-eye principle for authorising the payment.

TIP 10. CONDUCT CYBER SECURITY SIMULATIONS

Conducting cyber security simulations will enable employees to be on guard for any incidents. It should be based on the level of the employees' jobs, and they should be able to take away lessons from these simulations. If the employee failed the simulation, they could have an awareness session to gain the knowledge.