**MOHIT ARORA CO-FOUNDER,** *First Call IT*
LinkedIn - www.linkedin.com/in/mohitarora21
Website - www.firstcallit.com.au
(Cybersecurity Hero, ISO 27001 Information Security Lead Auditor, Enthusiast Entrepreneur)

Mohit with his third master's degree in Information Systems specialising in cyber security, holds 15 years of working experience in various domains and industries. After analysing various businesses; he concluded that today every organisation aims to thrive each day and technology proves to be a crucial component for their enhancement. At First Call IT, they believe in bringing this development whilst keeping Cyber Security at the core of any system integration.

## TIP 1. ANYONE, ANYWHERE

Do not think your company's size and location will attract or repel cyber-criminals. They cast a wide net of attacks and go after the most vulnerable. The first thing to adapt is a mindset that 'We can be next' and then be prepared to combat those attacks through staying alert to threats, implementing cyber security measures, and becoming invisible to those criminals.

## TIP 2. LICENSES AND CREDENTIALS

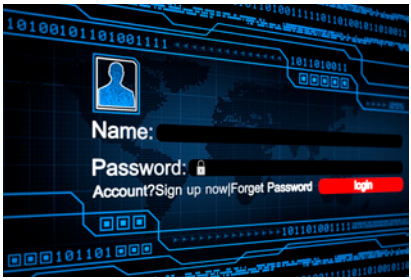
To save cost, companies with few staff members tend to share their licenses, where they also pass on the credentials to each other. The major demerit of this practice is:- once the hacker gets access to a single device, they can easily extend their arm and foot into another staff system. However, a platform such as Microsoft provides functionality of account 'alias' where two people with different username and password can reap benefit from a single account.

## TIP 3. PERSONAL VS BUSINESS ACCOUNTS

Many sole traders use their personal accounts for business related tasks, which opens the gate wide open for vulnerability. As we are usually less diligent towards our personal accounts and opt-in for various free subscriptions using private account logins. So, it is essential that we keep both personal and business accounts separate to reduce the size of the vulnerability window.

## TIP 4. ZERO TRUST

This framework is an effective management tool that can assist any organisation's management to reconcile the complicated threat landscape. The various guidelines direct to limiting the access of a company's data to only those who need it to do their job. Alongside, it also emphasises that no user should have enough privileges to misuse the system.




## TIP 5. MFA AND LENGTHY PASSWORDS

There are various free of cost Multi Factor Authentication (MFA) applications available in the market. Google Authenticator, Last pass, Microsoft Authenticator to name a few. It is essential that the company encourage their staff to use them. Alternatively, the password selection for all the accounts should be lengthy as the more the character count in a password, the harder it is to break.

## TIP 6. GAMIFICATION AND PHISHING SIMULATION

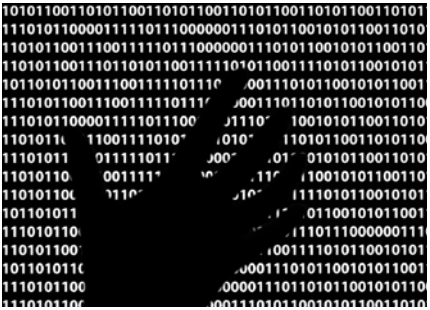
Each one teaches one, inter-department competitions, simulated phishing attacks and other related techniques should be incorporated into the organisation on regular basis. Also, it is important that winners are rewarded, something like secure employee of the month should be introduced to keep the security enthusiast high.

## TIP 7. AUTOMATION

The usage of automation functionality in security tools is very essential to retrieve regular benefits. Many platforms come with a threat detection and automated remediation feature. However, their meagre implementation process and overseas support restrict the buyer to avail such benefits. So, it's highly advisable to choose a product/company that can explain the features to you in a jargon-free manner and provide onshore support.

## TIP 8. AVAIL GRANTS

The Australian government is taking steps towards cyber security then why are we still sitting at the back seat? In the 2022 budget, government announced that SMEs can claim 120% of their expenditure on cyber security systems. It's time for businesses to avail themselves of this (and related schemes) to strengthen their security infrastructure.



## TIP 9. DATA BACKUP AND PROTECTION

What is the most important digital asset in your account books? It's definitely data. We give least importance to such a crucial component. Companies carry their data in single drive without any back-ups or migrating it on cloud. Its time SMEs step-up their game toward data security and perform regular backups.

## TIP 10. HYBRID PREPAREDNESS

There's no denying the fact that every business is following the trend of hybrid working - either forced due to COVID restrictions, or it is catalysed due to the pro it brings in economic resource utilisation. Businesses must start preparing themselves for this new normal of WFH (Work from Home) culture but in a secure manner. And it is crucial that SMEs choose professional partners who can assist them in their cyber security journey.