DR MOHIUDDIN AHMED *Lecturer of Cyber Security, Edith Cowan University*
LinkedIn: https://www.linkedin.com/in/mohi-ahmed-a0452420/
Website: https://www.ecu.edu.au/schools/science/staff/profiles/lecturers/dr-mohiud-din-ahmed

Industry-leading cyber-security expert. Passionate about strengthening university reputation, attracting students and increasing job readiness outcomes. Agile and driven professional with 5+ years of academic experience across higher education. Proven record of architecting and accelerating growth of academic and distance learning programs.

TIP 1. NO PERSONAL ACTIVITIES ON BUSINESS DEVICES

Social media platforms are used by cybercriminals to launch social engineering attacks. It is quite easy for cybercriminals to target victims based on the information available online, i.e., About Us/Team information from any business website. Hence, for the safety of the business, it is best not to allow any personal activities when using business devices.

TIP 2. CYBER-VET EVERY SINGLE EMPLOYEE

It is imperative to have a policy for cyber-vet employees. It takes just a single click on a malicious link to be compromised. As a part of recruitment, cyber-vetting should be taken very seriously. It is important more than ever because the employees cannot be monitored all the time as to who has access to sensitive business information.

TIP 3. DO NOT TRUST EVERYTHING YOU SEE ONLINE

In this age, it is a challenge to filter misinformation due to the plethora of online platforms. In addition, due to advances in deep fake technology, it is a challenge to differentiate fake from the original. Hence, before acting on information gathered from a single source, verify twice before taking any business decision.

TIP 4. DEFAULT SETTINGS ENTICE CYBERCRIMINALS

The internet-connected devices come with a default configuration. Cybercriminals capitalise on the default settings and are continuously scanning for such loopholes. Hence, all the business devices must be checked and configured to maintain security hygiene.

TIP 5. SEEK CYBER ADVICE - ASSUMPTION KILLS

If the business owners are not sound with technology, it is best to ask for advice. For example, just blindly trusting the Internet Service Providers and not changing the default Wi-Fi password might lead to catastrophic business disruption. Even if it is a small business, free cyber advice is available from several government agencies.

TIP 6. CONDUCT CYBER AUDITS REGARDLESS OF THE COMPANY SIZE

Auditing is important for any organisation; however, cyber auditing is equally important to ensure safety and privacy. An unregistered personal device used for business operations may open backdoors for cybercriminals. Even if there is little budget allocated for IT, from a data security and General Data Protection Regulation (GDPR) perspective, it is worthy of spending for cyber audits.

TIP 7. PATCH AND BACKUP

Delaying in patching might result in cyber-attacks and cyber-criminals are always scanning for vulnerabilities. Hence, it is important to keep track of updates and a bi-monthly schedule to monitor patching. Data backup is boring, yet important for business operations. Also, it is best to use reliable hard drives with encryptions to avoid data loss.

TIP 8. NEVER PAY RANSOM

Ransomware 2.0 is a new variant of ransomware to maximise the financial gains for cybercriminals. Even if a ransom is paid, cybercriminals have access to sensitive data and can blackmail again anytime they want. So, there is no point in paying a ransom and ever negotiating with cybercriminals. Always, have a business continuity plan in place.

TIP 9. DEVICES DO NOT LAST LONG - SET A LIFESPAN

Devices are not designed to last longer as the technology is advancing at a rapid pace. For business operations, it is better to lease the devices for a set period. There is always a trade-off between budget and security of business operations. If possible, always use the latest technology.

TIP 10. ZERO TRUST IS THE KEY

Regardless of the size of the business, it is always a good idea to incorporate a "Zero Trust" policy in IT operations. It is a wrong idea to have inherent trust within the business organisation. It is important to embrace the "Never Trust, Always Verify" concept and it will add another layer of security and privacy.