DR. FLORENCE MWAGWABI
Senior Lecturer in Information Technology
Academic Chair of Transnational Education (IT)
Murdoch University (Singapore)

TIP 1. THE HUMAN FACTOR

Humans make mistakes, understanding the human element is paramount. Threats originating from trusted insiders are easy to commit, yet difficult to detect - technology alone is not enough to solve cyber-security threats… we need to shift the focus to understanding the human factor.

TIP 2. IMPORTANCE OF TRAINING

While Security Training is the key to winning the cyber-security fight, the effectiveness of training wanes over time. Cyber-security training must be continuous.

TIP 3. MOBILE DEVICES

Use Mobile Device Management (MDM) to enforce your organisation's usage policies on employee mobile devices. While MDM may seem complex for SMEs, there are affordable options including cloud solutions that SMEs should consider.

TIP 4. WORKING REMOTELY

Common cyber-security risks from remote work include, neglecting policies such as password lock screen. If you are among the majority of organisations who currently plan to maintain remote work, take physical security seriously.

TIP 5. PASSWORD SECURITY

To this day, the top most commonly used password is 123456 - take password security seriously. Consider multi-factor authentication and utilising a password management tool.

TIP 6. REDUCE RISKS

We can never reduce cyber-security risks to zero. Determine your security risk appetite, then work on reducing security risks to your organisation's risk appetite.

TIP 7. KEEP UP TO DATE

Two key malware infection vectors are phishing attacks and exploitation of vulnerabilities. Both can be mitigated by keeping your software and anti-virus protection up to date.

TIP 8. CONSIDER THE CLOUD

Contingency planning is paramount. For SMEs with tight budgets do not ignore the power of cloud solutions.

TIP 9. RANSOM DEMANDS

Do not pay ransom. The majority of those who do pay a ransom do not get their entire data resources back.

TIP 10. SIMULATE ATTACKS

In addition to traditional cyber-security roles, consider creating an internal team of hackers to run simulated phishing attacks and simulated hacks … also referred to penetration testing.