CYBER-HYGIENE
BEST PRACTICES

As **cyber-attacks** become more frequent and severe, it is increasingly important for organisations to practise good cyber-hygiene to minimise their loss exposures. Cyber-hygiene refers to habitual practices that ensure the safe handling of critical data and connected devices. **These practices can help keep technology, networks and data protected from digital threats, including malware, ransomware and other cyber-incidents.**

CONSEQUENCES OF POOR CYBER-HYGIENE INCLUDE:

- **Security breaches—**Cyber-criminals can take advantage of human error and poor security networks to access personal and business data.
- **Data loss—**Organisations can lose data when hard drives, online cloud storage and software-as-a-service applications aren't backed up or maintained.
- **Software vulnerabilities—**Software developers constantly update their programs with security patches to prevent known vulnerabilities. If this software is left unpatched, it could be more susceptible to cyber-attacks.
- **Antivirus weaknesses—**Outdated technology will be less effective at protecting organisations against the latest viruses and other digital threats.

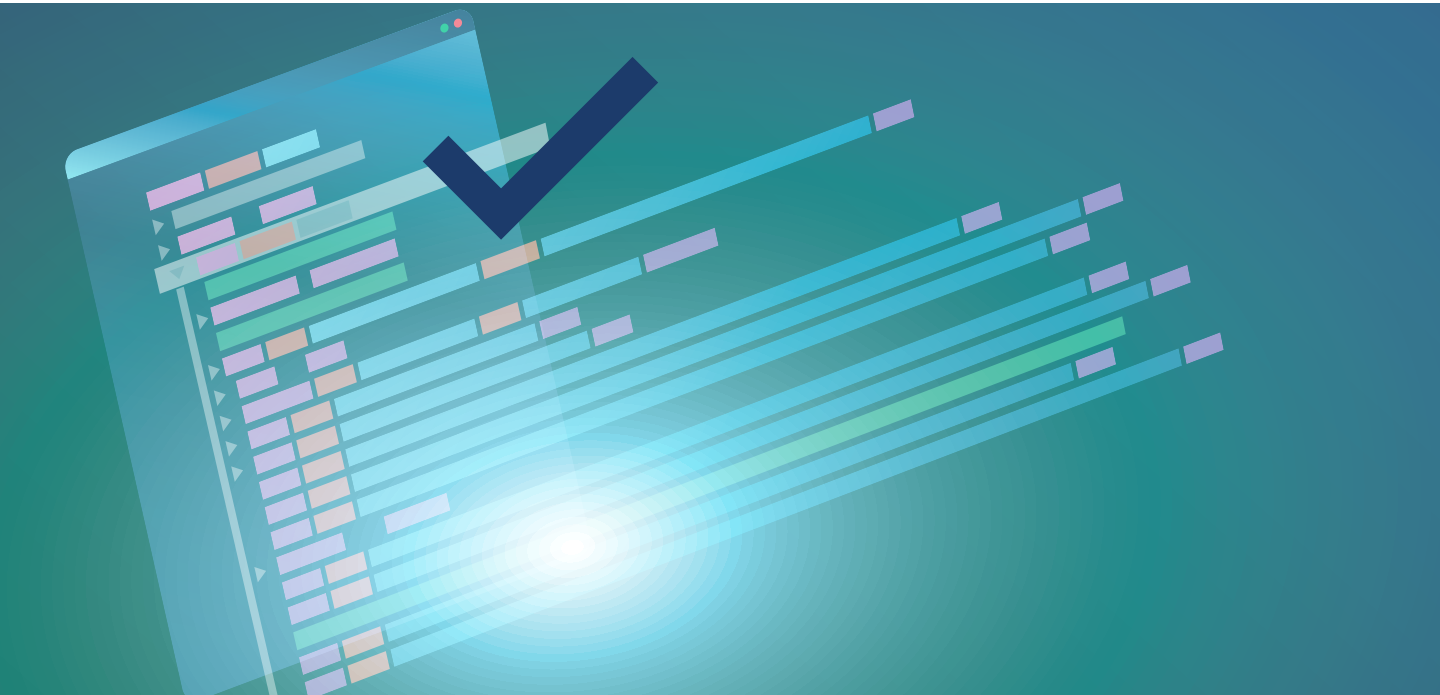
HERE ARE SOME KEY COMPONENTS OF CYBER-HYGIENE:

PASSWORDS

It is essential to use strong and complex passwords—those containing at least 12 characters and a mix of uppercase and lowercase letters, symbols and numbers—across workplace accounts. Users should change their passwords regularly and avoid sharing or repeatedly using them across different accounts.

MULTIFACTOR AUTHENTICATION

Important accounts, including email, social media and banking applications, should require multifactor authentication to limit the opportunity for cyber-criminals to steal confidential data.



DATA BACKUPS

Critical business files should be backed up in a separate and secure location, such as on an external hard drive or within the cloud.

FIREWALLS

A network firewall can help prevent unauthorised users from accessing company websites, email servers and other sources of information accessed via the internet.

SECURITY SOFTWARE

A high-quality antivirus program can perform automatic device scans to detect and remove malicious software, providing protection from various online threats.

EMPLOYEE EDUCATION

Employees are one of an organisation's most significant cyber-security vulnerabilities. Workforce education is vital to teach employees to identify phishing attacks, social engineering scams and other digital threats.

Daily routines, good behaviours and occasional checkups can make all the difference in ensuring an organisation's cyber-health is in optimal condition. Contact us today for more risk management guidance.