

BASIC DIGITAL SAFETY



Why digital safety matters?

- Cybercrime is on the rise with **phishing attacks** and **data breaches** increasing every year.
- Basic digital safety measures/cybersecurity practices and awareness can ensure **business continuity** and significantly reduce the risks and exposure of sensitive information that causes **financial** and **reputational damage**.



◆ 5 Digital Safety Tips ◆



1). Create strong **Passwords**

- Use at least 12 characters with a mix of letters, numbers and symbols.
- Avoid using the same password for multiple accounts
- Avoid personal information such as your birthdate (Jones & Patel, 2022).

2). Enable **Multi-Factor Authentication (MFA)**

- Adds an extra layer of security by requiring a secondary form of identification.
- Reduces the risk of unauthorised access even if your password is compromised (NIST, 2021).

For more tips and tools, visit:

- [National Cyber Security Centre \(NCSC\)](#)

3). Beware of **Phishing Scams**

- Check for suspicious links and emails claiming urgency.
- Verify the sender's email address before clicking links or downloading attachments (Anderson, 2020).



4). **Secure Your Devices**

- Keep software and antivirus updated to protect against vulnerabilities.
- Lock your device when not in use.
- Ensure **regular backups** to prevent data loss.

5). Avoid **Public Wi-Fi** for Sensitive Tasks

- Use a **VPN (Virtual Private Network)** to secure your connection when using public networks (Cunningham, 2019)

STAY CYBER SAFE - IT'S EVERYONE'S RESPONSIBILITY!