ILS

RISK FOCUS >>

Digital Hygiene Essentials

Simple Habits, Strong Protection

Picture this...

- Leaked personal beneficiary data exposing them to physical retaliation
- Website and social media hacked ahead of a significant advocacy event
- Ransomware locking critical files and freezing emergency fund transfers mid relief roll-out.

These aren't hypotheticals - the **rise in cyber incidents** has the potential to turn digital slip-ups into full-blown crises.

NGOs are particularly vulnerable, given that they can hold large amounts of sensitive personal data.

What is the reality?

- According to the Hiscox 2025 Cyber Readiness Report, nearly 3 out of 5 **(59%)** small and medium enterprises experienced **at least one cyber-attack in the past 12 months**.
- A CyberPeace Institute survey from 2023 showed **56%** of NGOs report not having a budget allocated for their cybersecurity needs
- From cybercriminals’ scams, state surveillance, hacktivists' disruptive attacks, and insider betrayals, NGOs face **escalating cyber threats** daily.

ILS

Cyber security is about people, not just technology

- **One click can undo the best systems** while everyday consistent digital hygiene habits can go a long way in protecting your work and organisation.
- **Basic digital hygiene** is the first frontline defence against these risks, preventing 99% of attacks like phishing, ransomware, malware, business email compromise or identity theft.
- Its's crucial to encourage **open dialogue** and **early reporting** if mistakes are made.

ILS

Digital Hygiene Essentials

- Ensure regular device and **software updates** are completed; including firewalls, anti-virus and anti-malware.
- Enable **strong and unique passwords**, both on devices and accounts through a secure password manager and an authenticator-app for multi-factor identification (2FA).

Digital Hygiene Essentials

- **Secure connections:** avoid connecting to public Wi-Fi and/or USB charging points. Prioritize the use of your mobile data hotspot and systematically use a VPN if on an untrusted network.

- **Secure browsing**: use privacy-focused browsers *(e.g. Firefox, Brave)*.

- Ensure your devices (phones and laptops) are **encrypted**, use encrypted messaging apps *(e.e.g Signal, Session)*.

Digital Hygiene Essentials

- Always consider **data sensitivity** when sharing information.
- Ensure **regular back-ups** of all your important data, following the 3-2-1 rule (three copies of your data, on two different types of storage, with one copy stored off-site)

From an organisational perspective, we encourage you to conduct:

- **Organisation vulnerability scan** - assess your equipment, software, communication systems, cloud services, information sensitivity and management practice, policies and staff training needs.

- **Digital context risk assessment** – assess legal frameworks and requirements, threat actors, telecommunication stakeholders and identify the most prevalent threats.

At ILS, we support organisations and individuals to develop and reinforce their digital best practices.

👉Let’s talk. If you or your organisation are looking for advice and support, we’d love to hear from you.