MACKAY
Corporate Insurance Brokers

CYBER-RISKS & LIABILITIES

September/October 2025

Cyber-security Tips for a Distributed Workforce

Remote and hybrid working models have become a permanent fixture for many UK organisations. While this shift offers flexibility and productivity benefits, it also introduces new cyber-security challenges. Employees working from home or on the move may unintentionally expose their organisations to cyber-threats through several vulnerabilities, such as unsecured Wi-Fi, outdated software, weak access controls, inconsistent security practices, and limited physical security for devices used outside the office. Making matters worse, many cyber-criminals actively target remote workers, exploiting reduced IT oversight and increased reliance on cloud-based tools to infiltrate systems and access sensitive data. As such, it's vital that organisations take steps to protect their distributed workforce. Consider the following tips:

- **Use secure connections—**Employers should require staff to use virtual private networks (VPNs) to access company systems. VPNs encrypt internet traffic and protect sensitive data from interception on unsecured networks.
- **Enforce strong authentication**—Employers should implement multi-factor authentication (MFA) to add a layer of security beyond passwords and reduce the risk of unauthorised access due to stolen or weak credentials.
- **Provide company-managed devices**—Employers should equip employees with IT-managed devices to maintain consistent security standards and reduce malware risks.
- **Keep software updated**—Employers should ensure all work devices are regularly patched with the latest security fixes to prevent exploitation of known vulnerabilities.
- **Limit access to sensitive data**—Employers should apply the principle of least privilege (granting access to sensitive data only as needed based on job roles) to minimise damage from compromised accounts or insider threats.
- **Educate employees**—Employers should offer regular training to help staff identify phishing attempts, secure their devices, and report suspicious activity, as human error remains a leading cause of security breaches.

Keeping Passwords Safe: Choosing and Using a Password Manager

Password managers serve as secure vaults for employee login credentials, enabling staff to use strong, unique passwords without needing to remember them all. Organisations can choose between two main types: **first-party managers**, built into browsers or operating systems like Chrome, Safari and Firefox; and **third-party managers**, which are standalone applications from independent providers. First-party options benefit from deep integration with the security features of the operating system or browser they're built into, while reputable third-party tools can offer more advanced features. Both types typically use encryption and may support biometric authentication, making them a safer alternative to memorising or reusing passwords.

To maximise security, organisations should adopt several best practices when implementing password managers. These include requiring employees to use strong, unique master passwords and enable two-factor authentication (2FA) wherever possible. When selecting third-party tools, organisations should choose a provider with a strong safety record. Organisations should also provide training to help employees use password managers effectively and securely. Moreover, IT teams should watch for risks such as staff using unauthorised tools or saving passwords on unsecured devices.

For further cyber-security tips, contact us today.

Artificial Intelligence and the Increasing Threat of Phishing

Phishing attacks, in which cyber-criminals manipulate users into disclosing sensitive information or installing malware through fraudulent communications, have been a persistent cyber-security threat, often resulting in significant financial and reputational damage. Recently, cyber-criminals have begun leveraging artificial intelligence (AI) to power these attacks, making them more convincing and difficult to detect. As such, organisations must take proactive steps to protect themselves.

According to a report by cyber-security brand Norton, phishing scams rose by a staggering 466% in the first quarter of 2025, compared to the final quarter of 2024. The surge can be attributed in part to the rise in AI-powered scams.

How AI is Changing Phishing

Traditional phishing messages often contain obvious errors, making them easier to spot. In contrast, AI-powered phishing is highly personalised and polished. These attacks can mimic writing styles, reference specific details (like recent purchases or projects), and even generate realistic audio or video messages. AI also enables mass production of unique phishing emails, increasing the volume and reach of attacks. Moreover, AI-generated messages can bypass traditional security filters, making older detection methods less effective.

The Impact on Organisations

AI-driven phishing increases both the frequency and quality of attacks. Employees may receive multiple fraudulent messages daily, raising the chances of someone falling for a scam. Successful attacks can lead to financial loss, data breaches, and operational disruption. IT teams face added pressure to manage risks from remote work setups, shadow IT, and expanding attack surfaces.

How Organisations Can Respond

Despite the growing threat, organisations can take several steps to strengthen their defences. Consider the following measures:

- **Use advanced security tools**—Organisations should deploy anti-phishing software with AI-based detection to identify suspicious patterns and language. Encryption keys and login credentials should also be rotated regularly to reduce the risk of compromise.
- **Strengthen email and identity security—**Organisations should implement multi-factor authentication, enforce strong password policies, and use email filters to block malicious content. Staff should be encouraged to verify links and attachments before opening them and report anything that seems suspicious.
- **Train employees**—Organisations should provide ongoing cyber-security training and conduct phishing simulations to help staff recognise and respond to threats. Employees should feel empowered to question unusual requests, especially those involving financial transactions or credential sharing.
- **Establish clear policies and response plans**—Organisations should maintain up-to-date data protection policies and ensure all employees understand their responsibilities. Incident response plans should be tested regularly to ensure the organisation can act quickly and effectively in the event of a phishing attack or data breach.
- **Combine human and AI defences**—Organisations should use AI tools alongside human oversight to build adaptive, resilient security systems. This combination allows for faster detection of threats while ensuring complex or ambiguous cases are reviewed by experienced professionals.

Contact us today for additional cyber-risk management information and robust insurance solutions.