MACKAY
Corporate Insurance Brokers

April 2026

COMMERCIAL
Insurance Profile

ClickFix Cyber-attacks Explained

Social engineering remains a leading cause of cyber-incidents, using deception to trick individuals into sharing sensitive information or taking harmful actions. One emerging method, the ClickFix cyber-attack (also known as ClearFake), relies on fraudulent error messages or verification prompts to convince users that something is wrong with their device and manipulate them into manually executing malicious commands—making these attacks harder to detect and more likely to bypass traditional security controls.

How ClickFix Attacks Work

ClickFix attacks typically begin when cyber-criminals compromise a website or platform and install malicious plug-ins. These plug-ins generate fake notifications that mimic legitimate browser or software alerts, such as:

- "Something went wrong while displaying this webpage."
- "There was an error during your latest update."
- "Please verify you are a human to proceed."

Users are then prompted to "fix" the issue by copying and pasting commands into tools such as PowerShell or a browser address bar. Once executed, these commands install malware, allowing attackers to access systems, steal data or deploy ransomware.

Because they rely on user interaction rather than automatic downloads, these attacks are difficult to detect and prevent. They now target multiple platforms—including Windows, macOS, iOS and Android—and, with the rise of cyber-crime-as-a-service, are becoming more widespread and sophisticated.

Potential Business Impacts

ClickFix attacks can lead to significant consequences, including:

- **Financial loss**—Theft of funds, intellectual property or sensitive data, as well as potential ransomware payments.
- **Operational disruption**—Malware can spread across networks, damaging systems and interrupting business activities.
- **Regulatory exposure**—Data breaches may trigger penalties under the UK's General Data Protection Regulation and the Data Protection Act 2018, along with reputational damage and loss of customer trust.

Risk Mitigation Strategies

Organisations can reduce their exposure to ClickFix attacks by implementing the following measures:

- **Employee training**—Deliver regular cyber-awareness training and discourage interaction with suspicious prompts or commands.
- **Usage policies**—Enforce safe browsing practices and restrict unauthorised scripts or commands.
- **System updates**—Keep software and systems up to date to address vulnerabilities.
- **Security tools**—Use endpoint detection and response, firewalls and threat monitoring solutions.
- **Network controls**—Segment networks and enforce strict access controls.
- **Vendor review**—Vet third-party providers to reduce exposure risks.
- **Response planning**—Maintain and test a cyber-incident response plan.

Contact Us Today

Contact the insurance professionals at MacKay Corporate Insurance Brokers for more information about developing loss control programmes tailored to your unique needs and purchasing appropriate coverage.

3 Learning and Development Trends to Monitor in 2026

Workplace learning is evolving amid slower hiring, shifting employee expectations and rapid advances in artificial intelligence (AI). UK employers are increasingly focused on building skills internally while ensuring development approaches remain flexible, practical and aligned with employee needs.

This article highlights three key learning and development (L&D) trends shaping the workforce in 2026.

1. Upskilling Takes Priority

With hiring slowing across many sectors, UK organisations are placing greater emphasis on developing existing employees. Internal mobility is becoming a key strategy for addressing skills gaps, particularly as employers struggle to source qualified candidates.

Research shows that 70% of employers cite finding candidates with the right technical skills as a major challenge, while 76% report difficulty filling roles due to talent shortages. As a result, upskilling is no longer optional—it is central to workforce planning.

Many organisations are introducing targeted, flexible training programmes that allow employees to build skills in areas such as digital operations, analytics, customer experience and AI-related tasks. Rather than relying on lengthy retraining, employers are using shorter, focused learning formats that support lateral or expanded career moves.

This approach can improve agility, strengthen retention and help employees maintain a sense of career progression without changing employers.

2. Career Growth Goes Beyond Traditional Management

Career advancement is also being redefined. Many employees—particularly younger professionals—are moving away from traditional management roles in favour of paths that prioritise flexibility, expertise and work-life balance.

This shift, often described as “conscious unbossing,” reflects a move away from rigid hierarchies towards more collaborative and empowered ways of working. UK research indicates that 52% of professionals prefer to progress as individual contributors, while 68% of Gen Z workers are not motivated by traditional management roles.

In response, organisations are encouraging managers to act as coaches rather than authority figures. Career pathways are becoming more fluid, allowing employees to move across roles, build specialised expertise and contribute in ways that align with their strengths.

This evolving model supports engagement and helps organisations retain talent by offering meaningful development opportunities without requiring a move into management.

3. AI Literacy Becomes Essential

As AI becomes embedded in everyday work, AI literacy is emerging as a core skill across all roles. Employees increasingly need to understand how AI tools function, use them responsibly and recognise when human judgement is required.

Rather than focusing on technical development, organisations are prioritising practical, accessible training that helps employees confidently use AI tools in their daily work. Common approaches include foundational training, hands-on learning opportunities, peer knowledge sharing and external courses.

Building AI literacy not only improves efficiency but also helps reduce uncertainty and resistance to new technologies. Organisations that invest in these capabilities are better positioned to maximise the value of AI while supporting employee confidence and adaptability.

Summary

The L&D trends shaping 2026 highlight a shift towards skills-based development, flexible career pathways and widespread AI adoption. Organisations that invest in these areas may be better equipped to build resilient, adaptable and engaged workforces.

For more risk management guidance, contact us today.