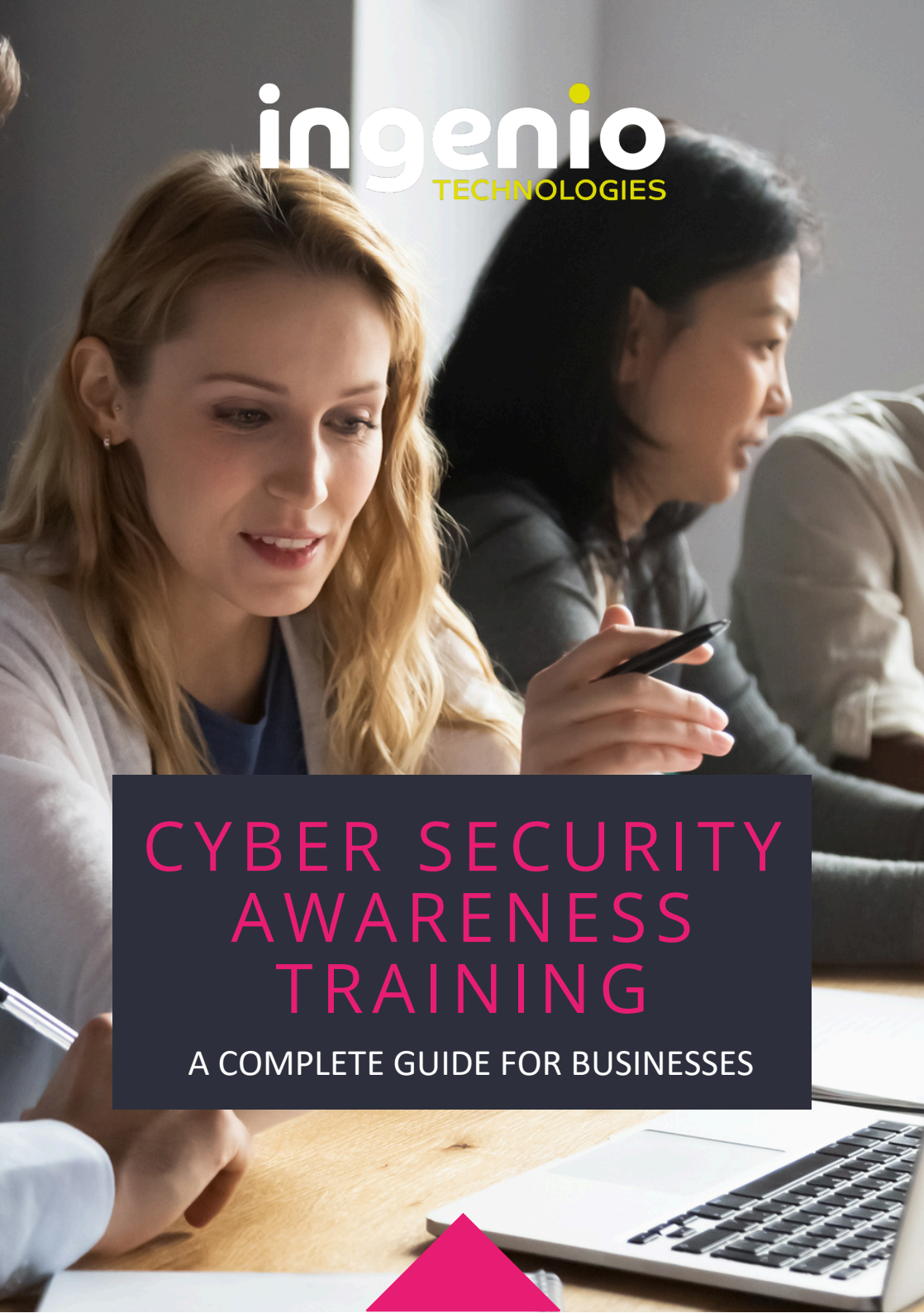
ingenio
TECHNOLOGIES
CYBER SECURITY AWARENESS TRAINING
A COMPLETE GUIDE FOR BUSINESSES

ingenio TECHNOLOGIES

Empower your team. Protect your business.

Why cyber awareness is your strongest defence

Technology can only go so far. The truth is that most cyber incidents begin with human error: an employee clicking on a malicious link, reusing a password, or sharing sensitive information without realising the risk.

According to the UK Government's Cyber Security Breaches Survey 2024, 84% of businesses that suffered a breach said it was caused by a preventable human mistake.

At Ingenio Technologies, we believe the key to stronger cyber resilience lies in knowledge, culture, and accountability. When your team understands the risks - and knows how to act - they become your greatest defence.

Key reasons to invest in awareness training:

- Prevent data loss and downtime caused by simple mistakes
- Reduce the likelihood of ransomware or phishing attacks succeeding
- Protect customer trust and brand reputation
- Strengthen compliance with GDPR, ISO 27001, and insurance requirements
- Empower your employees to act confidently and responsibly

THE EVOLVING THREAT LANDSCAPE

Cyber attacks are becoming more sophisticated, more targeted, and more relentless. Even small businesses are prime targets because attackers know they often lack the same defences as larger corporations.

Common threats facing UK businesses

- **Phishing and spear phishing:** deceptive emails designed to steal login credentials or trick staff into transferring money
- **Ransomware**: malicious software that encrypts files and demands payment to restore access
- **Data leaks and insider threats:** caused by misconfigured systems, poor password habits, or careless data handling
- **Business email compromise (BEC):** attackers impersonate senior leaders or suppliers to approve fake payments
- **Social engineering:** psychological manipulation of staff to bypass technical controls

Every click, download, or file share carries potential risk - which is why ongoing awareness is critical.

BUILDING A PEOPLE-FIRST CYBER CULTURE

An effective cyber security strategy isn't about fear; it's about empowering people to make smart, secure decisions every day.
At Ingenio Technologies, we help businesses build a security-first culture where awareness is second nature. That means embedding good habits into daily workflows, not just once-a-year training sessions.

Our approach includes:

- **Interactive workshops** – engaging, real-world scenarios that show staff exactly how threats appear in their inbox or browser
- **Bespoke training modules** – tailored to your organisation's systems, roles, and risk profile
- **Regular phishing simulations** – safe, controlled campaigns that measure awareness levels and identify where extra support is needed
- **Refresher sessions and updates** – bite-sized learning to reinforce vigilance and stay current with new attack trends
- **Clear policies and procedures** – guidance on password management, remote working, and data handling
- **Reporting culture** – encouraging employees to report suspicious activity without fear of blame

Only 27% of UK employees feel confident identifying phishing emails.

That means over 7 in 10 could be putting your business at risk with a single click.

Source: YouGov Cyber Security Perception Survey 2024

HOW TO RUN EFFECTIVE CYBER AWARENESS TRAINING

If you're managing your own internal training or working with a partner like Ingenio, these are the foundations of a successful programme:

1. Make it practical

Focus on real-world scenarios rather than theory. Employees need to recognise genuine phishing attempts, not just textbook examples.

2. Keep it continuous

Cyber awareness isn't a one-off project. Threats evolve constantly — training should too. Use quarterly refreshers or monthly "micro-learnings".

3. Lead from the top

Senior leadership should champion cyber awareness. When directors take part, it sends a clear message: security is everyone's responsibility.

4. Track and measure progress

Use data to demonstrate improvement. Key metrics include phishing simulation results, reporting rates, and reduction in security incidents.

5. Create a no-blame culture

Encourage employees to report suspicious activity, even if they've clicked on something by mistake. The faster you know, the faster you can contain.

MEASURING IMPACT: TURNING AWARENESS INTO RESILIENCE

At Ingenio Technologies, we help you turn training into measurable improvement.
Through detailed reporting, you can track how awareness translates into safer behaviour and compliance readiness.

Metrics we track include:

- Percentage of staff completing training
- Phishing click-through rate reduction
- Time taken to report suspicious emails
- Number of incidents prevented or contained
- Confidence levels across departments

These insights help you make data-led improvements and demonstrate accountability to insurers, auditors, and clients.

COMPLIANCE, ACCOUNTABILITY, AND REASSURANCE

Cyber awareness training supports compliance with several key regulations and standards:

- **GDPR:** ensures staff understand how to handle personal data responsibly
- **NIS2 Directive (for critical services):** introduces stricter requirements for cyber readiness and staff awareness
- **Cyber Essentials and ISO 27001:** both require ongoing training and user awareness as part of certification

When you can evidence that your team receives regular, up-to-date training, it strengthens your compliance position and builds confidence with regulators and stakeholders.

What sets Ingenio's training apart

Our cyber awareness solutions are built around three core principles:

1. Practical learning, not tick-box compliance
We deliver workshops and phishing simulations that reflect the reality of modern working environments — hybrid teams, remote access, and multi-device setups.

2. Ongoing engagement
We use short, high-impact sessions throughout the year to keep awareness fresh and relevant.

3. Measurable outcomes
Every programme includes reporting and recommendations for continual improvement, aligned with your security goals and industry standards.

CASE IN POINT: A REAL EXAMPLE FROM THE SOUTH EAST

A Sussex-based financial firm we work with was experiencing repeated phishing incidents. After introducing Ingenio's tailored training programme:

- ✓ Phishing click rates dropped from 21% to under 3% within six months
- ✓ Employee reporting of suspicious emails tripled
- ✓ The company achieved Cyber Essentials Plus certification ahead of schedule

That's the power of combining education with accountability.

Your next step: protect your business with confidence

Cyber awareness is the foundation of a secure, resilient business. It empowers your team, protects your reputation, and supports long-term growth.

Here at Ingenio Technologies, we make cyber awareness training simple, effective, and measurable - helping organisations across the South East stay one step ahead of evolving threats.

Ready to strengthen your human firewall?

Your people are your first line of defence. Let's make sure they're equipped to spot and stop cyber threats before they cause harm.

Speak with the Ingenio team today to find out how our tailored awareness training can protect your business.

CONTACT US TODAY.

01273 806211

hello@ingeniotech.co.uk

www.ingeniotech.co.uk