Somerbys IT

Cyber Security Awareness Training

A Complete Guide for Businesses

Why Cyber Security Awareness Training Is Crucial

Cyber threats are evolving faster than ever and your people are often the first target. According to the UK National Cyber Security Centre (NCSC), phishing remains the leading cause of data breaches, with **91% of successful attacks starting from a malicious email**. That means cyber criminals are counting on someone in your team clicking the wrong link or replying to a deceptive message.

Why this matters:

- A single click or weak password can compromise entire systems.
- Advanced AI tools make phishing emails more convincing and harder to spot.
- Neglecting human awareness exposes your data, finances, and operations to risk.

Real-World Consequences

What happened to Kettering based business, Knights of Old.

The tragic collapse of Knights of Old (KNP Group) illustrates just how costly cyber breaches can be, even for companies with long, reputable histories.

In 2023, this 158-year-old UK logistics firm was brought down by a ransomware attack that began with one weak, easily guessed password. Hackers from the Akira ransomware group gained access, encrypted all systems, destroyed backups, and demanded nearly £5 million in ransom. Unable to recover, the business entered administration, and 700 employees lost their jobs.

Despite having cyber insurance and meeting international standards, Knights of Old couldn't bounce back. This case underscores the severity of the consequences when basic cyber hygiene fails.

Cyber crime cost UK businesses over **£30 billion** in 2023, with phishing and ransomware among the most common attack methods

Source: UK Government Cyber Security Breaches Survey, 2024

Consequences of a Successful Cyber Security Breach

Operational Shutdown

Systems lock down, delivery routes stop, finance systems fail, and your business halts. (As with Knights of Old, vehicles grounded, operations ceased instantly.)

Data Loss and Recovery Failure

Without secure, tested backups, there's often no way to restore data, even with insurance.

Financial Ruin

Ransoms, often in the millions, plus recovery costs can be impossible to manage, especially with no access to financial records.

Reputational Damage

Customers, clients, and financial partners lose confidence quickly.

Mass Job Losses

As seen with Knights of Old, breaches can decimate entire local workforces and communities.

Spotting a Phishing Email: Practical Examples

Even with AI-generated quality, many phishing attempts still exhibit warning signs:

Check the Sender

Look for subtle domain oddities: e.g., micros0ft-support.com vs microsoft.com.

Spot Urgency or Threats

"Account suspended within 24 hours" emails are meant to make you panic.

Unexpected Links or Attachments

Hover to verify destination. If you didn't request it, don't click.

Offers Too Good to Be True

Free money or unrealistic discounts are red flags.

Almost-Correct Branding

Slight logo or layout discrepancies can alert trained eyes

How AI Is Changing the Game

Cyber criminals are using AI to craft believable, personalised threats: perfect spelling, tone, and context. That's why human awareness training must evolve in parallel with these technologies.

How Somerbys IT Protects Your Business

At Somerbys IT, we build your "human firewall" through robust Employee Security Awareness Training:

Phishing Simulations Safe, realistic tests to build instinctive response.

Social Engineering Scenarios Spot manipulation like pretexting or baiting.

Password Best Practices & MFA Encourage strong unique passwords plus multi-factor authentication.

Backup & Recovery Protocols Ensure backups are reliable and accessible when needed.

Incident Reporting Procedures Employees know what action to take if they spot something suspicious.

We tailor training to each sector's real-world threats, keep content interactive, and provide ongoing support to keep skills sharp.

Why Our Clients Choose Somerbys IT

We don't deliver generic, tick-box training. We tailor our sessions to your business sector, threat landscape, and working environment. This ensures employees leave with practical skills they can use immediately, rather than abstract theory.

Our approach:

- Interactive, real-world examples
- Regular refresher sessions to keep knowledge sharp
- Fully managed phishing simulation campaigns
- Ongoing support from our East Midlands-based IT team

91%

of data breaches start with a phishing email, making phishing the #1 cause of cyber attacks

Source: UK National Cyber Security Centre (NCSC)

Ready to strengthen your team's cyber skills?

Get in touch with the experts at Somerbys IT, we'll give you honest, no-jargon advice.

0333 456 4431 | info@somerbysit.co.uk

Dock 3, Space City
30 Exploration Drive
Leicester, LE4 5JU

Somerbys IT