Cybersecurity Awareness Training
Powered by KnowBe4 | Provided by Mother Technologies

mother technologies | KnowBe4

Cybercriminals aren't breaking in — they're invited in.

88% of data breaches are caused by human error.	**68% of breaches involve phishing and social engineering.**	**Only 3% of cybersecurity budgets go toward securing the human element.**

Cybercriminals know that your staff are the easiest way into your business. Whether it's a well-crafted phishing email, a fake invoice, or a spoofed CEO message, employees are the number one target.

Even the most advanced firewall or antivirus can't stop someone from clicking a malicious link. That's why keeping your employees cyber aware isn't optional anymore, it's essential. That is where KnowBe4 comes in.

KnowBe4: Train Your Human Firewall

Traditional cybersecurity focuses on the network. KnowBe4 focuses on your people, giving them the knowledge and instincts to identify cyber threats before they become company wide disasters.

KnowBe4 offers the world's most comprehensive platform for security awareness training and simulated phishing. As your MSP, we manage the setup, monitor your progress, and help reduce your risk.

Features of KnowBe4

Realistic Phishing Simulations

- Hands-free, AI-driven phishing emails that mimic real threats.
- Thousands of ready-to-use examples.

Engaging Training Modules

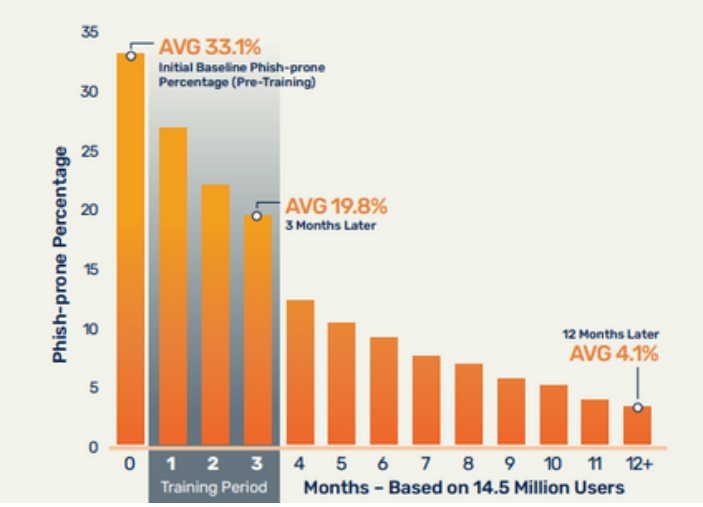
- Bite-sized videos, games, quizzes & interactive content.
- Customised for your industry and staff roles.

Advanced Reporting

- Visual dashboards and detailed metrics.
- Executive-level reports for compliance and ROI.
- Track human risk scores over time.

Simple Setup & Smart Automation

- Seamless integration with your staff directory.
- Automated campaigns, reminders and user onboarding.



Backed by Real-World Results

- Initial phishing risk: 34.3%
- After 3 months of training: 18.9%
- After 1 year: Just 4.6% of users still fall for phishing.

These results show the clear impact of ongoing security awareness training in significantly reducing phishing risk over time.

(KnowBe4 Industry Benchmark Report, 2024)

Traditional Training vs. KnowBe4

Traditional Awareness ✗	KnowBe4 Security Awareness ✓
Annual Slide Deck Sessions	Continuous, Interactive Training
No Real Testing	Simulated phishing & Social Engineering Tests
Hard to Measure	Actionable Metrics and Risk Scoring
Generic Content	Tailored to your industry and threat landscape
Limited Engagement	Gamified and Video-Based Learning

What Happens If You Don’t Train Your Staff?

When your employees aren't trained to spot cyber threats, you’re leaving the door wide open to attackers. Here’s what’s at stake:

Financial Loss

Phishing and ransomware attacks can cost thousands, or even millions through downtime, recovery, legal costs, and lost business.

Reputational Damage

A data breach can destroy customer trust. Once confidence is lost, it's hard to win back.

Human Error = Weakest Link

Even the best firewalls can’t stop someone from clicking a fake invoice, wiring funds to a scammer, or sharing login credentials with a fake CEO.

Compliance Penalties

Many industries now require proof of employee security training. Falling short can lead to fines or failed audits.

Smarter Attacks

Today’s phishing emails look real and criminals use AI to personalise them. Untrained staff are vulnerable to scams that even tech-savvy users might fall for.

Ready to reduce your cyber risk?

We’ll handle the technical side so your team can get trained, tested, and transformed into your human firewall.