aztech

Cyber Security Awareness Training Service

Empower Your Team to Be the First Line of Defence Against Cyber Threats.

Cyber Security Services

The Challenge

With 90% of security breaches caused by human error, employees are often the weakest link in an organisation's cyber security defences. Phishing attacks remain the leading method for delivering malware and have become increasingly sophisticated and targeted.

Without proper training, employees may unknowingly expose sensitive business data which could lead to fines, lost revenue and non-compliance with industry regulations.

Key Business Outcomes:

Reduced Risk of Breaches:

Employees become active defenders, reducing the likelihood of successful phishing and malware attacks.

Enhanced Compliance:

Meet industry regulations and avoid fines by documenting employee cyber security training.

Improved Productivity:

Reduce downtime caused by cyber incidents and insider threats with better-prepared employees.

Strengthened Culture of Security:

Promote awareness across all levels of the organisation to create a proactive defence mindset.

Why Choose Us?

Expert-Led Approach: Benefit from our experienced trainers and cutting-edge learning tools.

Proven Effectiveness: Our clients see measurable reductions in successful phishing attempts and improved compliance scores.

Tailored Solutions: Training content is customised to address your organisation's unique risks and needs.

> "The Cyber Security Awareness Training we recieve on a monthly basis ensures that everyone is staying up to date with cyber security and not becoming complacent. The videos are really funny, really intelligent and keeps you motivated to keep up to date with the modules."
>
> **Claire McFarlane, Head of Compliance (Clearview Intelligence)**

aztechit.co.uk
0330 0949 420 | info@aztechit.co.uk

Service Overview

Our Cyber Security Awareness Training service provides comprehensive education tailored to your employees' needs. Our training empowers users to identify, report and prevent cyber threats, significantly reducing your organisation's exposure to risk.

Phishing Simulations: Test employee readiness with realistic scenarios to identify areas for improvement.

Workshops and Online Courses: Interactive sessions and video-based training make learning accessible and easy to understand.

Continuous Education: Ongoing access to resources, including newsletters, refresher courses, and updated materials, ensures knowledge remains current.

Personal Data Security: Training extends beyond the workplace, teaching users to protect their personal data to prevent cross-over risks to the organisation.

Example Use Cases

Minimise Breaches: Reducing human errors causing cyber security incidents.

Targeted Training: Identifying gaps with simulations and performance metrics.

Ensure Compliance: Meeting regulations and avoiding costly penalties.

How It Works:

Initial Assessment:
Identify current vulnerabilities and tailor training to address specific risks.

Interactive Training:
Use a mix of workshops, videos, and simulations to educate employees effectively.

Simulated Testing:
Conduct fake phishing campaigns to evaluate employee readiness and response.

Ongoing Support:
Provide continuous access to updated training materials and resources to maintain vigilance.

Detailed Reporting:
Deliver actionable insights to track progress and ensure training objectives are met.

What's Next?

Empower your employees to defend against cyber threats effectively. Book a consultation call to learn more about our Cyber Security Awareness Training service.