

Security Awareness Training

Turn your people into the strongest layer.

Defend against cybercriminals and strengthen your 'human firewall' through engaging, automated learning experiences. By combining real-world phishing simulations, bite-sized training modules and detailed analytics, you can cultivate a proactive cyber security culture.

HOW IT WORKS

Simulate. Train. Measure.

A SaaS web-based application delivers online security training for your employees, automatically serving simulations and training content to the right people at the right time.



REAL-WORLD PHISHING

Simulate

- Deploy templates or custom phishing scenarios, such as Microsoft 365, HMRC, Amazon and Dropbox, to assess and enhance employee vigilance.
- Automated delivery of simulations and training journeys onboards new hires seamlessly and supports compliance efforts.



BITE-SIZED JOURNEYS

Train

- Use default journeys, build your own, or create custom Content Packs with training and phishing simulations.
- Offer a variety of content styles including animated and live-action videos, quizzes and interactive modules, catering to diverse learning preferences.



RISK SCORED

Measure

- The industry-leading reporting suite provides Risk Score by company, department and individual, heat maps, engagement by type and course completion rates.
- Monitor training completion rates and phishing simulation outcomes, and identify high-risk individuals or departments.

Out-of-the-box configuration allows for rapid, effective deployment **without administrative burden.**

WHY IT MATTERS

The human layer is the one attackers target.

Security awareness training addresses the risk that technical controls alone cannot remove:

74% of all cyber attacks start at the inbox

92% of malware is delivered via email

43% of all cyber attacks are aimed at SMBs

Over 90% of cyber attacks involve staff error

USE CASES

Where it earns its place.

From organisation-wide baselines to targeted programmes for the roles most at risk.



Reduce insider threat

- ✓ Implement simple organisation-wide training to reduce susceptibility to cyber threats
- ✓ Focus targeted training on specific departments or roles that may be more vulnerable to attack



Onboard and sustain

- ✓ Integrate cyber security awareness into the onboarding process to instil best practice from day one
- ✓ Implement 12 or 24-month training programmes with monthly simulations and concise video modules, ensuring consistent engagement with minimal administrative effort



Evidence compliance

- ✓ Support your compliance efforts, or cyber insurance requirements, with documented and audit-ready training programmes
- ✓ Align with cybersecurity best practices and regulatory requirements by fostering a security-conscious workforce

98%

training completion rates

85%

decrease in simulation click rates

12 or 24

month automated journeys

Days

to deploy, not months

“Implementing, running, and maintaining the system requires very little administration – a huge advantage for small teams with limited resources.”

Principal Information Security Officer, Public Sector

THE PLATFORM

Built to run itself.

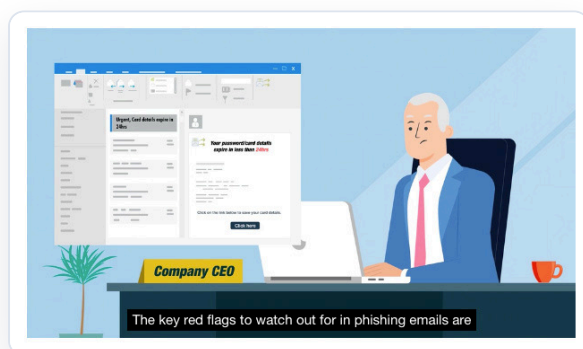
Automated delivery of simulations and training journeys, so programmes keep running without ongoing administration.

Out-of-the-box configuration	Allows for rapid, effective deployment without administrative burden.
Training journeys	Use default journeys, build your own, or create custom Content Packs with training and phishing simulations.
SCORM compliant	Fully SCORM compliant for customers wanting to house content within their own learning management system (LMS).
Single sign-on & sync	Single sign-on for users, with automated user synchronisation with Active Directory and Google Workspace.
Multi-lingual	Multi-lingual options, important for customers with multiple office locations.
Microsoft 365 integration	Developed with a Microsoft 365 integration that handles the management of your employees.
Automatic reporting	Automatic report and dashboard creation, with no manual set-up required.

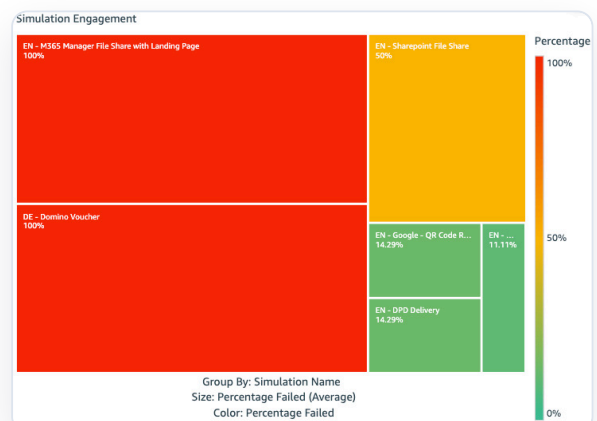
REPORTING & ANALYTICS

See who is at risk, by name.

Risk Score by company, department and individual, heat maps across simulations, engagement by type and course completion rates. Short, live-action and animated modules keep people engaged while the analytics show exactly who is at risk.



Short, live-action and animated training modules built for retention.



Simulation engagement heat map, sized and coloured by percentage failed.

KEY FEATURES

What you get out of the box.

Real-World Phishing Simulations	Deploy templates or custom phishing scenarios (e.g. Microsoft 365, HMRC, Amazon, Dropbox) to assess and enhance employee vigilance.
Automated Journeys	Implement 12 or 24-month training programmes with monthly simulations and concise video modules, ensuring consistent engagement with minimal administrative effort.
Multi-Format Content	Offer a variety of content styles, including animated and live-action videos, quizzes and interactive modules, catering to diverse learning preferences.
Customisable Content	Tailor training materials to align with organisational policies, branding and specific security requirements.
Seamless Integration	Integrate effortlessly with Microsoft 365 and Google Workspace for user synchronisation and single sign-on capabilities.
Comprehensive Analytics	Monitor training completion rates, phishing simulation outcomes, and identify high-risk individuals or departments through detailed reporting tools.

BENEFITS

What changes.

Enhanced Cyber Resilience	Reduce the likelihood of security breaches by equipping employees with the knowledge to recognise and respond to cyber threats effectively.
High Engagement	Achieve up to 98% training completion rates through engaging, concise content designed for easy consumption.
Reduce Susceptibility	Organisations have observed an 85% decrease in phishing simulation click rates, indicating improved employee awareness.
Efficient Implementation	Deploy the platform within days with minimal administrative overhead, allowing IT teams to focus on core responsibilities.
Compliance Support	Align with cybersecurity best practices and regulatory requirements by fostering a security-conscious workforce.

PART OF THE TRUSTLAYER PLATFORM

Security Awareness Training is part of the Users layer. Eight solutions, four layers, one platform.



Browse

Web

CASB

AI Exposure



Posture

CSPM

SSPM



Mail

Email

Archiving



Users

SAT