DATASHEET

TrustLayer Security Awareness Training

Defend against cybercriminals and stregthen 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 Security Awareness Training works

Our 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.

✓ Out of the box configuration allows for rapid, effective deployment without administrative burden

✓ Use default journeys, build your own, or create custom Content Packs with training and phishing simulations.

✓ Fully SCORM compliant for users wanting to house content within their learning management system (LMS)

✓ Single sign-on for users with automated user synchronisation with Active Directory and Google Workspace.

✓ Multi-lingual options – important for customers with multiple office locations

✓ Automated delivery of simulations and training journeys, onboard new hires seamlessly and support compliance efforts

✓ Automatic report and dashboard creation

Microsoft 365 Integration

TrustLayer Security Awareness Training has been developed with a Microsoft365 integration that will handle the management of your employees meaning that you can deliver one of the best cyber security training programmes available in the market.

Reporting & Analytics

The industry-leading reporting suite provides insightful metrics including he following:

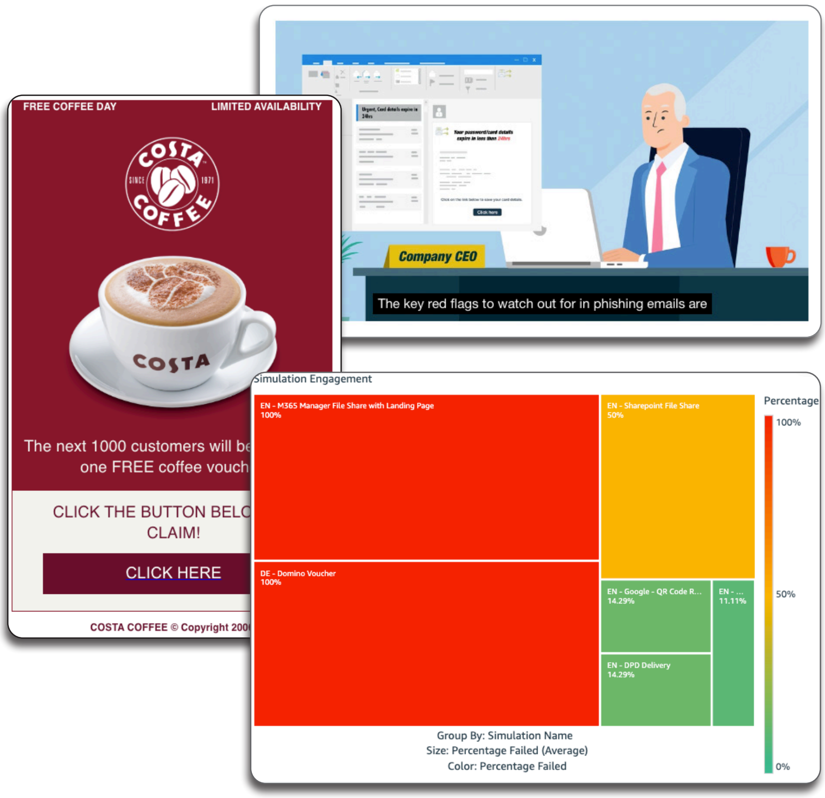
✓ Risk Score (Company, Department, Indiviual)
✓ Heat Maps - Overview of Simulations
✓ Engagement by Type
✓ Course Completion Rates

SECURITY AWARENESS TRAINING FACTS

- 74% of all cyber attacks start at the inbox.
- 92% of malware is delivered via Email.
- 43% of all cyber attacks are aimed at SMB’s
- Over 90% of cyber attacks involve staff error

USE CASES

- **Reduce Insider Threat:** implement simple organisation-wide training to reduce susceptibility to cyber threats.
- **Targeted Training:** Focus on specific departments or roles that may be more vulnerable to attack.
- **New Employee Onboarding:** Integrate cyber security awareness into the onboarding process to instill best practice from day one.
- **Regulatory Compliance:** Support your compliance efforts, or cyber insurance requirements by providing documented and audit-ready training programmes.



FREE COFFEE DAY LIMITED AVAILABILITY

The next 1000 customers will be one FREE coffee vouch

CLICK THE BUTTON BELO CLAIM!

CLICK HERE

COSTA COFFEE © Copyright 200

The key red flags to watch out for in phishing emails are

COSTA COFFEE
SINCE 1971
COSTA
Urgent, Card details expire in 24hrs
Your password/card details expire in less than 24hrs
Click here
Company CEO
Simulation Engagement
EN - M365 Manager File Share with Landing Page 100%
EN - Sharepoint File Share 50%
DE - Domino Voucher 100%
EN - Google - QR Code R... 14.29%
EN - ... 11.11%
EN - DPD Delivery 14.29%
Percentage
100%
50%
0%
Group By: Simulation Name
Size: Percentage Failed (Average)
Color: Percentage Failed

KEY FEATURES

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 programs 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 synchronization 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

Enhanced Cyber Resilience	Reduce the likelihood of security breaches by equipping employees with the knowledge to recognize 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	Organizations 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.

> "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*