proofpoint.

PROOFPOINT SECURITY AWARENESS TRAINING

KEY BENEFITS

- Change users' behaviour to reduce risks from phishing and other cyberattacks
- Prioritise and improve incident response
- Provide consistent training across the globe with multilanguage support
- Track results and progress with real-time reporting
- Reduce successful phishing attacks and malware infections by up to 90%

Proofpoint Security Awareness Training (formerly Wombat Security) helps you deliver the right training to the right people at the right time, turning your end users into a strong last line of defence to identify cyberattacks and protect your organisation.

With more than 90% of cyberattacks starting with an email, wary end users are critical to protecting your people and your data. While technologies that detect and block malicious emails are part of the solution, you can also reduce the likelihood of successful attacks such as phishing or ransomware through effective, broad-based security awareness training.

PROTECT YOUR ORGANISATION WITH THREATSIM PHISHING SIMULATIONS

ThreatSim® Phishing Simulations help you understand your organisation's susceptibility to a variety of phishing and spear-phishing attacks. With thousands of different phishing templates across 13 categories, you can evaluate users on multiple threat types, including:

- Malicious attachments
- Embedded links
- Requests for personal data

We add new templates every month. Our Dynamic Threat Simulation phishing templates are drawn from Proofpoint threat intelligence; others reflect customer requests and seasonal topics.

Users who fall for a simulated attack receive practical "just-in-time" teaching. They learn the purpose of the exercise, the dangers of real-world attacks and how to avoid future traps. You can also help your most vulnerable users by automatically assigning interactive training to anyone who falls for a phishing simulation.

ASSESS VULNERABILITIES WITH CYBERSTRENGTH

CyberStrength® is a powerful web-based knowledge assessment tool that identifies your employees' potential vulnerabilities — without having to run a simulated phishing attack. After establishing a baseline measurement of your employees' understanding, periodic reassessments allow you to track progress and target areas of concern.

We offer a library of more than 200 questions, across a range of critical cybersecurity topics. You can also create custom questions to gauge knowledge of your organisation's policies and procedures. With CyberStrength, you can identify where you are susceptible — from an organisational level down to the individual.

EDUCATE EMPLOYEES WITH ENGAGING, ACTIONABLE TRAINING CONTENT

Our growing, continuously updated content library offers interactive training modules, videos, posters and images in 35+ languages, with consistent, actionable messaging suitable for global organisations. Based on proven Learning Science Principles, our customisable education content covers a broad range of security risks, from phishing attacks to insider threats.

Our interactive training modules are available on demand and are mobile-responsive, so your users can take our training anytime, anywhere, on any connected device, maximising efficiency and convenience. The modules take an average of just 5 to 15 minutes to complete—minimising disruption to daily work routines—and conform to the US Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.

We also make it easy to alert your users to the most relevant phishing attacks and lures through our Attack Spotlight series—brief, timely content that teaches how to spot a current threat and avoid becoming a victim.

REDUCE RISKS WITH PHISHALARM, PHISHALARM ANALYZER, AND CLEAR

PhishAlarm® is an email client add-in that allows your people to report suspicious messages with a single mouse click. Users who report an email get instant positive reinforcement in the form of a "thank you" pop-up message or email. Using PhishAlarm Analyzer, reported messages are automatically analysed and enriched using multiple Proofpoint Threat Intelligence and reputation systems. And they are dispositioned as malicious, suspicious, bulk or spam.

With our CLEAR (Closed-Loop Email Analysis and Response) solution, reported messages are sent to TRAP (Threat Response Auto-Pull). In TRAP, the different classifications of messages can be automatically quarantined or alerted to incident response teams for investigation. With this solution, active attacks can be stopped in minutes with the help of trained end users.

ANALYSE RESULTS WITH FULL-FEATURED REPORTING

Our reporting capabilities provide the granular and high-level visibility you need into your employees' interactions with assessments, simulated attacks and training assignments. We offer responsive, easy-to-read reporting with a modern UI, providing more than just completion data so that you can evaluate progress, gauge ROI, and benchmark, track and trend user knowledge. You can use our dashboards to easily filter data, compare assessments, quickly add and remove measures and more.

You can also download and export data to share business intelligence with other stakeholders, perform more detailed analysis and evaluate metrics alongside other security events. Our Automated Reporting feature streamlines the export process, allowing you to schedule automatic delivery of reports at regular intervals to yourself and designated stakeholders within your organisation.

ABOUT OUR CONTINUOUS TRAINING METHODOLOGY

Industry research has shown that once-a-year classroom training is not effective in the battle against cyberattacks. Our unique Continuous Training Methodology is a cyclical approach that teaches users about best practices and how to employ them when facing security threats.

A continuous cycle of assessment, education, reinforcement and measurement maximises learning and lengthens retention. Our methodology sits in strong contrast to a "one and done" approach, giving you the flexibility to evolve your programme over time, identify areas of susceptibility and deliver targeted training when and where it's most needed.