proofpoint.

SAAS-BASED
SECURITY AWARENESS
AND TRAINING
FOR END USERS

INTRODUCTION

Wombat Security, a division of Proofpoint, provides SaaS-based educational solutions that help you:

- Create effective security awareness and training programmes
- Change end-use behaviour
- Reduce risk

Education is about more than just sharing facts and figures. It's about using knowledge to drive action.

Our Security Education Platform is built to deliver comprehensive security education that can be effectively and easily managed by you and your administrators.

This integrated platform gives you access to the to the key components of our Continuous Training Methodology–Assess, Educate, Reinforce and Measure–to help change behaviour and reduce risk within your organisation.

90% REDUCTION

The reduction our customers have experienced in successful external phishing attacks and malware infections using our four-step methodology to security education.

CONTINUOUS TRAINING METHODOLOGY

Our methodology is a continuous cycle that maximises learning and lengthens retention. It sits in strong contrast to a "one and done" approach, giving you the ability to identify areas of susceptibility, deliver targeted training when and where it is most needed, and evolve your programme over time. The steps in our unique **Continuous Training Methodology**, which are discussed in more detail in the subsequent sections, enable ongoing improvement and drive measurable behaviour change.

ASSESSMENT SOLUTIONS

Assess your susceptibility to attack using customisable knowledge assessments and simulated phishing, texting and USB attacks.

Our assessments pinpoint areas of vulnerability, motivate users to take training, and establish baselines to measure against later in your programme.

You can use multiple types of assessments to get a comprehensive view of your organisation's potential vulnerabilities—and manage them all from our Security Education Platform.

KNOWLEDGE ASSESSMENTS

Our CyberStrength® Knowledge Assessments are a great way to evaluate employee security posture in many different areas and help you tailor your education initiatives to the people and topic areas that need the most attention.

CyberStrength provides a library of more than 185 questions that cover a range of subjects, including:

- Safe interactions with emails, URLs and websites
- Proper use of mobile devices and mobile apps
- Understanding and avoiding social engineering scams
- Other behaviours that can harm your people, areas, data and systems.

You can also choose to use one of our Predefined CyberStrength assessments, which are made up of 10-15 questions on a specific topic and allow you to auto-enrol users into training if they fall below your pass/fail threshold.
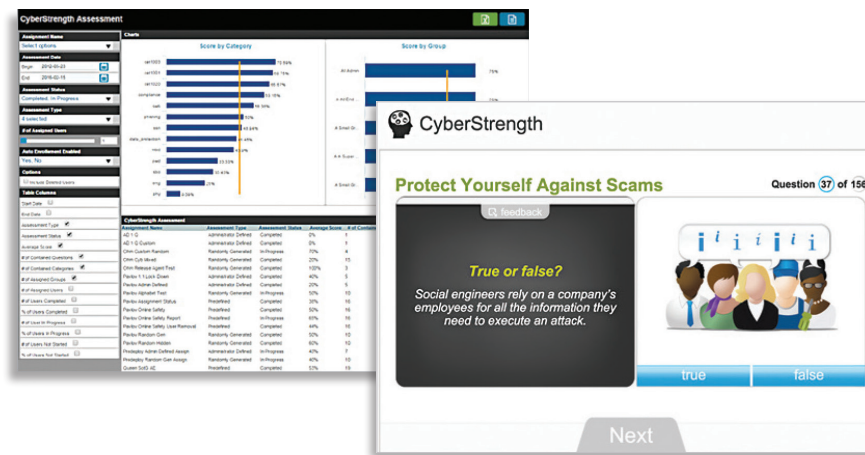
THREATSIM SIMULATED ATTACKS

Our ThreatSim® Simulated Attacks allow you to safely assess how your employees would engage with threat vectors in their day-to-day environment. Those who fall for attacks are automatically presented with a Teachable Moment, just-in-time guidance that lets users know what they did wrong and offers tips to help them avoid future threats. These brief messages highlight the dangers of attacks and motivate employees to participate in follow-up training.

- ### THREATSIM PHISHING SIMULATIONS
  Provides a variety of customisable email templates that address three key testing factors: attachments, embedded links and requests for personal data. No one else in the industry can offer multiple templates in one campaign and random scheduling of emails to spread out delivery, along with auto-enrolment of end users to targeted training if an employee falls for an attack.

- ### THREATSIM SMISHING SIMULATIONS*
  Send mock SMS/text attacks to assess your organisation's susceptibility to actual malicious messages and help to mitigate careless use of mobile devices.

- ### THREATSIM USB SIMULATIONS*
  Randomly place "infected" removable memory devices around your organisation to introduce your employees to the concept of malicious USB drives and gauge vulnerabilities.

*U.S. only

EDUCATION SOLUTIONS

Wombat grew out of the largest national research project on combating phishing attacks, which was performed at Carnegie Mellon University in 2008. Our educational approach uses key Learning Science Principles that engage users to change behaviour and have been proven to be more effective than once-a-year training presentations and videos.

Our current library of modules educate and engage users through hands-on decision-making, improving knowledge retention and facilitating longer-term behaviour change.

INTERACTIVE TRAINING MODULES

Our library of short, interactive training modules are jargon-free, written to a high-school level and have been translated and localised in more than 30 languages. We offer Standard Modules that are 10-15 minutes long, as well as Mini-Modules that are 5-7 minutes long. Mobile-Responsive modules allow users to take training anytime, anywhere and on any device. These modules also conform to the US Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard, which ensures that training can be accessed and completed by employees with disabilities.

Note: Courses are mobile responsive unless otherwise specified.

SECURING YOUR EMAIL
Advanced Series
- Email Protection Tools
- Email Security on Mobile Devices
- Spear Phishing Threats

INSIDER THREAT SERIES
- Insider Threat Overview
- Malicious Insider Threat
- Unintentional Insider Threat

SECURING YOUR EMAIL
Fundamental Series
- Introduction to Phishing
- Data Entry Phishing
- Avoiding Dangerous Links
- Avoiding Dangerous Attachments

COMPLIANCE-BASED TRAINING
- PII*
- PCI DSS*
- PHI*
- GDPR Overview
- GDPR in Action

PASSWORD PROTECTION SERIES
- Multi-Factor Authentication
- Password Management
- Beyond Passwords
- Password Policy

STANDARD MODULES
- Email Security*
- Protecting Against Ransomware
- URL Training*
- Travel Security
- USB Device Safety
- Security Essentials for Executives
- Data Protection and Destruction
- Security Essentials
- Mobile Device Security
- Social Engineering
- Mobile App Security*
- Security Beyond the Office*
- Physical Security
- Safe Web Browsing
- Safe Social Networking

*Currently available for desktop devices only

REINFORCEMENT SOLUTIONS

Wombat Security customers are creating a culture of security awareness within their organisations by using positive reinforcement techniques—and you can too. Our PhishAlarm® email reporting add-in and our portfolio of Security Awareness Materials help you make the most of your awareness and training efforts by continuing to emphasise best practices, encourage good behaviours and reduce your vulnerability to attack.

PHISHALARM

Our PhishAlarm email reporting button gives your users the ability to report suspected phishing emails to your security and incident response teams with a single mouse click.

An email client add-in, PhishAlarm extends phishing prevention to the desktop. This simple but effective tool can reduce the window of risk associated with active phishing attacks within your organisation. It also automatically provides positive behaviour reinforcement by immediately thanking end users (through a pop-up message or email) for reporting suspicious emails and encouraging them to continue those actions in the future. As an optional add-on to ThreatSim, PhishAlarm allows users to draw on their knowledge and use learned behaviours to stop social engineers and hackers in their tracks. Our PhishAlarm Analyser tool allows you to prioritise reported emails for faster remediation.
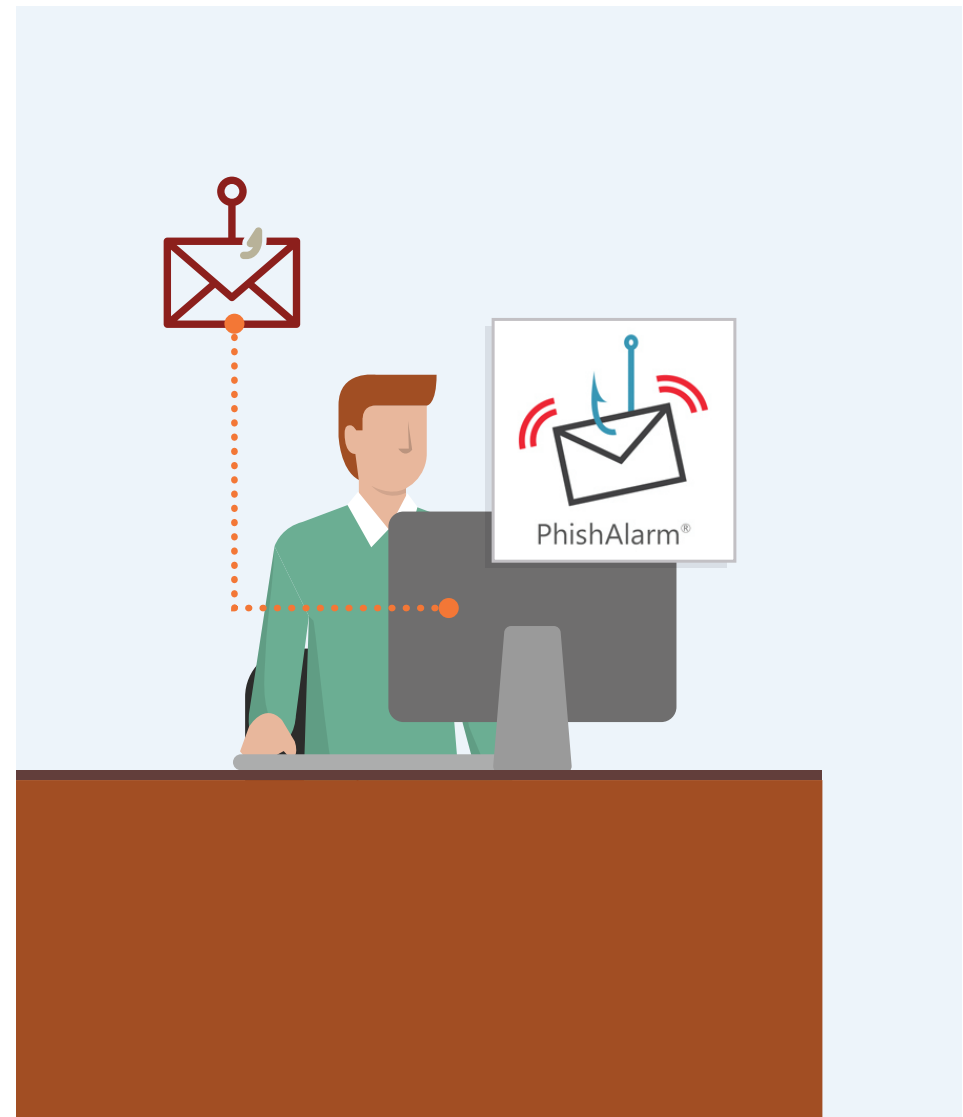
SECURITY AWARENESS MATERIALS

We make a clear distinction between awareness and education activities, and we encourage our customers to include both within their security awareness and training programmes.

Awareness Video Campaigns
A great way to introduce your employee base to security awareness and training initiatives—and create ongoing conversations—is via awareness campaigns. We provide videos, posters and images to help create a viral moment within your organisation, and quickly bring awareness to a new level. Available in different themes, our professionally produced videos offer a creative, attention-grabbing way to introduce end users to the idea of security training as you are planning your programme launch. Companion posters can be placed around your organisation to further enhance awareness initiatives and keep the conversation going. Use images to create signs, giveaways, screensavers and other visual elements to round off your campaign.

Education Materials
Our Educational Materials include a series of posters, images and articles that are designed to reinforce your education initiatives. These posters and images mimic the look and feel of our training modules, which helps to create visual continuity from one medium to another. There is also a continuity of content, as the posters reference the best practices users are taught during training, and the articles go into the same topics in more detail (while still keeping an end-user audience in mind).

Visit our website to view examples.

| INTRODUCTION | METHODOLOGY | ASSESSMENT SOLUTIONS | EDUCATION SOLUTIONS | REINFORCEMENT SOLUTIONS | MEASUREMENT SOLUTIONS | THE WOMBAT ADVANTAGE | SECURITY EDUCATION PLATFORM | PACKAGES |

MEASUREMENT SOLUTIONS

Educating your employees and improving awareness is critical to reducing your risk. But it's even better when you can actively monitor the progress and results of your efforts and use that analysis to plan your future assessment and training efforts.

The ability to measure your programme every step of the way lets you easily show results and the value of your security awareness and training programme.

IN-DEPTH REPORTING

Our Security Education Platform's detailed reporting capabilities allow you to track each employee's interaction with our simulated attacks, knowledge assessments and interactive training modules.

Our new, fuller-featured dynamic reporting functionality gives administrators more flexibility and additional insights into users' interactions with our interactive training modules. You can easily filter data, compare assignments, quickly add and remove measurement factors and more. Administrators can also download the data in CSV and Excel formats for data integration. Recently added Leaderboard reports aid in gamification of security awareness programmes to help drive engagement.
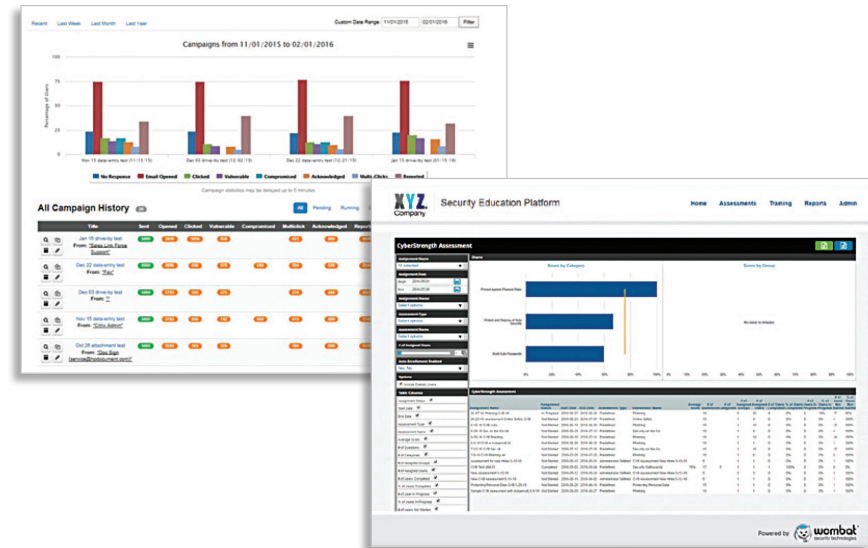
PHISHALARM ANALISER

Email Prioritisation for Faster Remediation

A companion to our PhishAlarm email reporting button, PhishAlarm Analiser provides security teams with a real-time ranking of suspicious emails in order of threat potential, allowing them to effectively allocate their time and attention to the most imminent and dangerous attacks to your network.

- ### CUTTING-EDGE TECHNOLOGY
  Identifies phishing attacks in real time (such as zero-hour attacks) and is constantly evolving and adapting to new email threat patterns.

- ### INTELLIGENT PRIORITISATION
  Prioritises emails as: Likely a Phish, Suspicious and Unlikely a Phish. PhishAlarm Analiser registers a low number of false positives.

- ### MACHINE LEARNING FUNCTIONALITY
  Thousands of real attacks from the wild are scanned each week and used to learn about and guard against increasingly sophisticated techniques, including spear phishing attacks.

- ### DELIVERY OF ACTIONABLE INFORMATION
  Within each prioritised message is a report that includes links to leading security intelligence sources so security analysts can quickly and easily dig deeper into the threat(s) associated with the reported email.

PhishAlarm Analiser is a software-based solution that can be installed as a virtual machine image on a local computer or deployed through the cloud.

THE WOMBAT ADVANTAGE

CUSTOMER SUCCESS MANAGER

Work with your dedicated customer success manager— provided at no additional cost—to establish and achieve your programme goals.

AWARD-WINNING SUPPORT

Plan and execute effectively with pre-launch and post-launch support (included with your licence). Superior service is always part of the package at Wombat.

UNLIMITED PLATFORM USE

Maximise your efforts with unlimited use of platform components for the number of specified end users in your licence at no additional charge.

MULTI-LANGUAGE SUPPORT

Ensure consistent training across the globe with the ability to deliver assessments and training in more than 30 languages.

ACTIVE USER COMMUNITY

Join the Wombat User Community and enjoy a variety of benefits, including discounted Wombat Wisdom registration and direct access to our product management team.

REAL-TIME REPORTING

Track the results and progress of assessments and training with extensive and exportable user analytics and metrics.

SECURITY EDUCATION PLATFORM

Our Security Education Platform delivers the solutions in the Wombat Continuous Training Methodology in a single, integrated platform. No other solutions on the market allow you the ease and efficiency of being able to assess and provide in-depth, interactive training all in one place. This easy-to-use, integrated platform gives you the ability to easily spot problem areas, implement solutions and see results.

KEY FEATURES

- ### CUSTOMISABLE CONTENT
  You can add logos, create content and templates for assessments, and customise messages in our Teachable Moments. In addition, our Training Jackets let you to add personalised and custom content to the start and close of each training module, including policy acknowledgments and completion certificates.

- ### SUPPORT FOR MULTIPLE LANGUAGES
  All of our assessments and interactive training modules are available in more than 30 languages—and growing. Check wombatsecurity.com/multinational for our most up-to-date list of languages.

- ### AUTO-ENROLMENT
  This exclusive feature allows you to automatically assign follow-up training to anyone who falls for a ThreatSim mock attack, or predefined CyberStrength assignment. This approach can dramatically improve the efficiency of your programme and engage those who need the most attention.

- ### MULTIPLE PHISHING TEMPLATES AND STAGGERED MESSAGE DELIVERY
  To help reduce the likelihood of your employees identifying and discussing mock attacks they receive, we offer the ability to send multiple different phishing email templates in one campaign. We also give you the ability to spread those messages over a desired date range, even specifying the hours of the day you would like them to be delivered to your employees' in-boxes. This also helps to lessen the impact on your email servers.

PACKAGES

Run your security awareness and training programme with one of our pre-configured packages.

ANTI-PHISHING

Focuses on teaching end users to defend against phishing attacks. Select from the most comprehensive and effective library of anti-phishing training available today.

FOUNDATIONS

Covers essential cybersecurity topics and can be used to prove security awareness and training has been delivered to your end users.

ENTERPRISE

Provides all of the products and features necessary to fully implement our Continuous Training Methodology, which produces the most effective behaviour change results.

INCLUDES	ANTI-PHISHING	FOUNDATIONS	ENTERPRISE
CyberStrength KnowledgeAssessments	Not Included	✔	✔
ThreatSim Simulated Phishing Attacks	✔	✔	✔
PhishAlarm Email Reporting Button	✔	✔	✔
PhishAlarm Analiser Threat Prioritisation	£ Add-On	£ Add-On	✔
End User Sync with Active Directory (AD)	✔	✔	✔
Interactive Training Modules	Select 3 of 6	Select 12	Includes more than 30
LMS (SCORM) Installation	£ Add-On	£ Add-On	✔
Education Materials	£ Add-On	✔	✔
Awareness Video Campaigns	£ Add-On	✔	✔

MANAGED SERVICES

No time to implement a programme?

Ask about our Managed Services offering. You specify the components and time line, and we develop a plan that covers everything from implementation to execution to measurement.

For an in-depth look at our Security Education Platform or to schedule an online demo, please visit **www.wombatsecurity.com** or call +44 (0) 118 402 9163 | US +1 (412) 621 1484.

proofpoint.   www.proofpoint.com