Why Wombat?

Our Security Education Platform gives you access to assessments, interactive training modules, reinforcement materials, and comprehensive reporting features. You decide what to deploy, and when and where to deploy it. Measure results at every step and use analysis to tailor your future efforts.

The Wombat Success Story

At Wombat Security, a division of Proofpoint, we think education is about more than sharing facts and figures. We think it's about using knowledge to drive action. Our assessment tools and suite of interactive training modules have two equally important aims: to help your employees understand security threats *and* implement the best practices needed to reduce risk to your organization.

Customers who apply our Continuous Training Methodology have enjoyed many benefits, including up to a 90% reduction in successful external phishing attacks and malware infections; fewer helpdesk calls; increased reporting of suspicious emails; and an overall improved security posture. These results are achieved by implementing the **Assess, Educate, Reinforce, and Measure** components of our methodology, either in part or as a complete solution.

Our approach allows you to reduce the risks (and costs) related to employees' poor cybersecurity behaviors. With our cloud-based Security Education Platform — an enterprise-grade learning management system (LMS) purpose-built for security professionals — you can easily manage your IT security awareness and training program from a single interface:

- Teach employees how to recognize, avoid, and report suspected phishing attacks
- Identify the users who have the best or worst understanding of critical risk areas
- Automatically assign follow-up education based on assessment results
- Select from a comprehensive set of more than 30 brief, software-based interactive training modules
- Deliver attention-grabbing awareness campaigns and regularly remind users of best practices
- Monitor employee completion of assignments and deliver automatic reminders
- Measure improvement over time with robust business intelligence features and sharable reports
- Assess and train global employees with localized content available in more than 30 languages
- Receive free program and technical support services as part of the Wombat Advantage

Assess Using CyberStrength and Simulated Attacks

Our assessment tools give you important insights into your organization's level of susceptibility and allow you to narrow in on key areas of vulnerability. Used individually or in conjunction, our CyberStrength® Knowledge Assessments and our ThreatSim® simulated phishing, smishing (SMS/text message phishing), and USB attack tools help you establish a baseline understanding of vulnerability, which is critical for measuring results and analyzing effectiveness.

Educate Using Interactive Training Modules

Each of the 30+ modules in our ever-expanding library offers interactive training about important cybersecurity topics. Mini-modules provide 5 to 7 minutes of training; standard modules can generally be completed in 10 to 15 minutes. Our development and design processes are based on key Learning Science Principles, and we employ methods that have been proven to be more effective than annual training presentations and other non-interactive approaches. Our modules engage users through hands-on decision-making, improving knowledge retention and facilitating longer-term behavior change.

You can select from a wide range of topics — including critical areas like phishing, ransomware, social engineering, passwords, and mobile device security. All modules are available on demand and localized content is available in more than 30 languages. Users have the opportunity to learn in their native languages, and they can access training as their schedules allow, putting less strain on busy workdays.

Reinforce With PhishAlarm and Security Awareness Materials

Our PhishAlarm® email reporting button gives your users the ability to report suspicious emails to your security and incident response teams with a single mouse click. An email client add-in, PhishAlarm can reduce the window of risk associated with active phishing attacks within your organization. It also automatically provides positive behavior reinforcement by immediately thanking end users (via a pop-up or email message) for reporting suspected phishing emails. To streamline response and remediation, add PhishAlarm Analyzer to quickly scan and prioritize reported emails for your infosec security team.

Our Security Awareness Materials include videos, posters, images, and articles that allow you to create awareness campaigns and regularly remind employees about important cybersecurity principles. When these materials are viewed and shared on a regular basis, they elevate awareness, reinforce positive behaviors, and keep best practices top-of-mind for all employees.

Measure Results via Comprehensive Business Intelligence Tools

Our detailed, dynamic security dashboards give insights into each assessment and education component you choose to include in your security awareness and training program. You'll be able to track results and employee interactions with our ThreatSim Simulated Attacks, CyberStrength Knowledge Assessments, interactive training modules, and our PhishAlarm button. Reports can be scheduled and exported for easy sharing and integration with other security-related data.

Our business intelligence tools go beyond the basic metrics offered by other platforms to deliver actionable data points and valuable insights into program activities. You'll have access to important information about who completed which assignments, who fell for specific simulated attacks, which concepts employees understand well, topic areas of weakness, improvements over time, and email reporting actions. User data can be characterized and sorted using custom fields such as job function, geographic location, department, hire date, etc. If you are applying gamification techniques to your program, our reports will make it easier for you to track participation rates and top-performing departments and users.

Quotes From Our Customers

"We have been using Wombat for over two years now and one of the reasons we chose to go with them was not just because we felt the product offered more than their competitors technically, but also because the user education experience had the edge with tone, pace, and multinational options. The product itself is constantly evolving, and there's always something new to offer our colleagues by way of education."

Lesley Marjoribanks, Customer & Colleague Security Awareness Manager, Royal Bank of Scotland

"We selected Wombat because they offer a comprehensive cybersecurity preparedness platform. Wombat's Platform enables us to assess internal risk and target training to employees who need it most, thereby strengthening our security profile. We value the opportunity to collaborate with Wombat as the company continues to expand its suite of cybersecurity training modules."

Manager of IT Security and Risk Management, Del Monte Foods

"Since partnering with Wombat, we've seen a significant increase in user awareness and recognition of suspicious emails. Instead of clicking on these messages, our employees are reporting them. Our users have caught and alerted us to more than ten separate phishing attacks, and in the 10 months following the launch of our Wombat training program, we have seen a dramatic decline in infections due to inappropriate email activity."

Senior Manager of IT Operations, Monongahela Valley Hospital, Inc.

"As of mid-July, there were over 400,000 successful completions of [Wombat Security's] *Safer Web Browsing*, *Password Security*, *Email Security*, and *Mobile Device Security* training modules. Over 32,000 users have completed the *Mobile Device Security* training module in the last two weeks. This is amazing for non-mandatory training. We have now justified the cost of training with just those four modules! We are very happy with our investment."

Security Awareness and Training Director at a large technology company

Real-World Results

Our customers' results are perhaps the best way to illustrate our success in improving end-user awareness and creating lasting behavior change. Following is a summary of some of our customers' success stories. You can access full case studies on our website.

Royal Bank of Scotland

A historic international financial institution with more than 80,000 email users, the Royal Bank of Scotland used our ThreatSim Phishing Simulation and interactive training modules to raise awareness and create a more responsible cybersecurity culture. The program successfully engaged employees and stakeholders, and RBS reduced its end users' phishing susceptibility by more than 78%.

College in the Northeastern US

After pairing our simulated phishing assessments and interactive training modules, a large public college in the Northeastern US saw a significant reduction in malware and viruses, a 90% reduction in successful phishing attacks, significantly fewer support requests, an increase in the number of users reporting incidents and attacks, and a greater awareness of issues.

Global Engineering Services Company

Following engagement with our Managed Services team — who executed a program that included simulated phishing and USB attacks, CyberStrength assessments, and associated training modules — an international construction and engineering services company lowered its rate of malware infections by 42%, saving its IT staff hundreds of hours of remediation time.

Global Manufacturing Company

In less than six months, a large international manufacturer saw a 46% average reduction in infected PCs (spyware, malware, and viruses) across its 40+ global locations after using our anti-phishing training.

US Utility Company

A large utility company in the western US implemented a security awareness and training program to train users how to recognize and avoid phishing attacks. Using a combination of monthly simulated phishing emails (which increased in difficulty as the program progressed), education, and reinforcement materials, the organization reported a 67% reduction in susceptibility 18 months into the program.

ROI

Wombat Security customers have shown a strong return on investment due to the effectiveness of our security education solutions. The global manufacturing company that experienced a 46% reduction in infected PCs (spyware, malware, and viruses) also saw an **annualized ROI of more than 7x** based solely on their helpdesk technician time savings. This equated to almost eight times the purchase price of their Wombat Security solution. But you don't need extreme results to see the value in your investment. Another of our customers — one of the world's largest banks — showed a positive ROI in fewer than 12 months with just a 10% decrease in susceptibility to attack.

Our security awareness training tools have been proven to reduce the costs associated with employee downtime and equipment remediation related to cyberattacks. This speaks volumes about the effectiveness of our methodology. However, returns that are measurable in dollars are just one benefit of our approach. Our customers have enjoyed other positive results that come with a spike in awareness and an understanding of security best practices. These value-added outcomes include overall risk reductions such as fewer viruses, malware infections, and associated helpdesk tickets; lower helpdesk call volumes; increased cybersecurity knowledge across the organization; increased adherence to security policies and compliance requirements; and an improved security posture.