A Unique, Effective Approach to Interactive Training

The Wombat training methodology is based on research-proven Learning Science Principles that help to elevate the effectiveness of cybersecurity education. The interactive modules have earned kudos from customers and end-users alike, and they can help change behaviors and reduce risk at every level of your organization:

- Modules are brief and focused. Standard-length modules generally take 10 to 15 minutes to complete; mini-modules are designed to be completed in 5 to 7 minutes.
- Flexible, on-demand format minimizes disruption to daily work routines.
- Gamification techniques and interactivity keep end users engaged. Employees set the pace and receive feedback throughout.
- Mobile-responsive options allow users to take training anytime, anywhere, on any device. These modules also conform to the U.S. Section 508 standard and the Web Content Accessibility Guidelines (WCAG) 2.0 AA standard.
- All modules (except PHI) are available in 30 languages. Professionally translated and localized content delivers high-quality, engaging content for employees around the globe.

Data Protection and Destruction – Teaches employees how to apply best practices related to secure handling and storage of sensitive data throughout its life cycle.

General Data Protection Regulation: A Practical Overview – Instructs users about their role in GDPR compliance; how to make the right decisions about the data they create and handle; and the consequences of non-compliance. Applies to all foreign and domestic companies that house information about European residents. (mini-module)

Mobile Device Security – Explains important physical and technical safeguards, as well as ways to improve the security of mobile communications and connections.

Payment Card Industry Data Security Standard – Helps staff better manage credit card data; understand PCI DSS requirements; securely handle records and accounts; and act upon security breaches.

Physical Security – Introduces key components of physical security and helps employees understand how they can keep people, areas, and assets more secure.

Email Security or Anti-Phishing Phyllis™ – Teaches users to identify and avoid manipulative content, malicious and disguised links, dangerous attachments, inappropriate data requests, and other threats. (This game-based training is available in two formats.)

Mobile App Security – Shows users how to research applications and the implications of dangerous permissions.

Password Security – Teaches your employees how to create strong passwords, and explains best practices for keeping passwords safe.

Personally Identifiable Information – Instructs employees about ways to identify PII; best practices for handling, storing, and sharing PII; and the fundamental actions to take in the event of a PII breach.

Protected Health Information – Teaches employees how to safeguard PHI in accordance with HIPAA guidelines. They also learn about PHI identifiers and receive practical guidance for using, disclosing, transmitting, and storing PHI.

Read full descriptions and demo our modules on our website: wombatsecurity.com/educate.
Protection Against Ransomware – Provides brief but comprehensive training about how to recognize and prevent ransomware attacks. The best practices users learn are applicable in fighting other phishing and malware-based threats. (mini-module)

Safer Web Browsing – Shows employees how to avoid common pitfalls and dangers associated with web browsing and teaches them how to identify potentially dangerous URLs, prevent malware and virus downloads, and spot Internet scams.

Securing Your Email – Fundamental – Includes the following four mini-modules, which allow you to deliver brief but actionable training that targets specific risks to email users: Introduction to Phishing; Avoiding Dangerous Links; Avoiding Dangerous Attachments; and Data Entry Phishing

Securing Your Email – Advanced – Build upon the Securing Your Email – Fundamental series with these three highly-focused modules about sophisticated email threats: Email Protection Tools; Email Security on Mobile Devices; and Spear Phishing Threats

Security Essentials – Introduces users to security issues that are commonly encountered in day-to-day business and personal activities. It is an excellent option for new-hire education and as a yearly refresher course.

Security Essentials for Executives – Focuses on cybersecurity concerns that are unique to senior managers and executives. The module highlights best practices related to mobile devices, use of non-corporate networks, physical security, internal and external meetings, social media, and more.

Social Engineering – Goes beyond the phishing threat to explain dangers associated with smishing, vishing, social media, and impersonation attacks. Users also learn how to spot common social engineering techniques and traps.

Travel Security – Teaches users about cybersecurity safeguards that can protect their devices and data while traveling. (mini-module)

URL Training or Anti-Phishing Phil™ – Explains how URLs are constructed, common warning signs, and how to identify and avoid malicious links. (This game-based training is available in two formats.)

USB Device Safety – Focuses on the dangers associated with unknown USB drives and explains how users can protect their personal and corporate data and systems when using USB-based devices. (mini-module)

Safe Social Networking – Teaches users how to safely share and interact on social networking sites, and explains common traps and scams to avoid on these very public platforms.

Security Beyond the Office – Introduces best practices related to topics such as safe use of WiFi networks, the dangers of public computers, and practical physical security measures.

For more information, click here. | CONTACT US AT: RSAU@rsa.com

Read full descriptions and demo our modules on our website: wombatsecurity.com/educate.