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 focus on a specific security topic. 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, which ensures that training can be accessed and completed by employees with disabilities.

Standard Modules

Email Security or Anti-Phishing Phyllis™ – Users learn to identify and avoid manipulative content, malicious and disguised links, dangerous attachments, inappropriate data requests, and other threats. Training is available in two formats: an interactive module and a character-driven training game.

URL Training or Anti-Phishing Phil™ – Employees learn how URLs are constructed, common warning signs, and how to identify and avoid malicious links. Training is available in two formats: an interactive module and a character-driven training game.

Social Engineering – This goes beyond the phishing threat and explains dangers associated with smishing, vishing, social media, and in-person attacks. Users learn how to avoid common social engineering traps and keep people, areas, and assets secure.

Mobile Device Security – Whether you issue corporate devices or you are part of a BYOD organization, your employees will benefit from learning important physical and technical safeguards, as well as ways to improve the security of their communications and connections.

Mobile App Security – A companion to Mobile Device Security, this module teaches users how to research applications and the implications of dangerous permissions.

Security Essentials – This module 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 refresher course.

Security Essentials for Executives – This training 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.

Password Security – We teach your employees how to create strong passwords, and explain best practices for keeping passwords safe.
Standard Modules (continued)

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

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

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

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

**Safe Social Networking** – Users learn how to safely share and interact on social networking sites. We explain common traps and scams to avoid on these very public platforms.

**Protecting Against Ransomware** – This mini-module provides brief but comprehensive training about ransomware. End users learn how to recognize and prevent ransomware attacks, and the best practices they learn are applicable in fighting other phishing and malware-based threats.

**Travel Security** – This mini-module is a must for end users who take corporate devices and data on the road. They will learn about cybersecurity safeguards that can protect them during domestic and international travel.

**USB Device Safety** – This mini-module quickly and effectively teaches your employees 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.

**PCI DSS** – This module helps staff better manage credit card data; understand PCI DSS requirements; securely handle records and accounts; and act upon security breaches.

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

**Compliance-Based Training (Standard Modules)**

Governance, risk management, and compliance (GRC) officers can use these modules to introduce the primary concepts of industry standards and explain employees’ roles in maintaining compliance:

**PII** – Employees learn how to identify PII; best practices for handling, storing, and sharing PII; and the fundamental actions to take in the event of a PII breach.

**PCI DSS** – This module helps staff better manage credit card data; understand PCI DSS requirements; securely handle records and accounts; and act upon security breaches.

**PHI** – We teach employees how to safeguard PHI in accordance with HIPAA guidelines. They learn about PHI identifiers and receive practical guidance for using, disclosing, transmitting, and storing PHI.