Barracuda **PhishLine**

User Anti-Phishing Training And Simulation Platform

Social engineering attacks can evade your best efforts to secure your gateway—and while securing the gateway is still necessary, it is no longer sufficient. Barracuda PhishLine is an essential tool to transform your employees from an attack vector into a robust layer of defense against phishing attacks.

The Barracuda Advantage

- Patented Highly Variable Attack simulations including: Phishing (Email), Smishing (SMS), Vishing (Voice), and Found Physical Media (USB/SD Card)
- Comprehensive SCORM-compliant user-training courseware
- Industry-leading analytics and reporting
- Program and address book automation with the PhishLine Workflow Subscription

Product Spotlight

- Hundreds of email lure templates, landing pages, and domains
- Workflow engine that automatically directs training and testing
- Users can instantly report suspicious emails to your help desk or incident response team with the Phish Reporting Button

Patented Multi-Vector and Multi-Variable Attack Simulations

Train your team on every facet of social engineering threats with PhishLine's complex multi-vector attacks that combine PhishLine campaigns with additional vectors such as Smishing (SMS/Text), Vishing (Voicemail) and Found Physical Media. Additionally, PhishLine's multi-variable campaigns allows administrators to use multiple simulation templates in a single campaign. This prevents users receiving the same mock phishing template and allow for hypothesis-based testing (A/B tests).

Customizable Simulation and Training Content

The PhishLine Content Center Marketplace™ contains hundreds of compelling simulation templates, landing pages, risk assessment surveys, and engaging multi-lingual training content in easy-to-use online catalogs. All content is fully customizable, and new simulation and training content is added daily to reflect the most recent threats and training resources available.

Phish Reporting Button

The Phish Reporting Button provides a powerful yet simple solution that allows users to report suspicious emails to your help desk or incident response team. You control the whole process without needing to develop and maintain your own "report a phish" button.

Key Features

Simulation

- 4 vectors:
  - Email "Phishing"
  - SMS "Smishing"
  - Voice "Vishing"
  - Found Physical Media
- Beyond the Click interactions such as:
  - Attachments
  - Credential Form
  - Feedback Form
  - File Upload
  - File Download
  - Geolocation Query
  - Unsubscribe Forms
  - Advanced Plugin Detection
  - Exit-Screen Pop-Ups

Education

- Courseware
- Posters and Newsletters
- Web Banners and Digital Learning Media
- Quizzes and Risk Assessment Surveys

Reporting and Analytics

- Collects over 16,000 data points
- Detailed Trend Analytics
- Local IP Detection
- Inbox Message Analytics (Out-of-Office messages and direct replies)
- Application, OS, and Vulnerability Profiling
- Customizable Reports and Dashboards

Incident Response

- Phish Reporting Button
- Incident Response Metrics and Dashboards
- Incident Response Workflows
- SEIM Integration

Administrative Features

- Multi-Factor Authentication
- Built-In Privacy Controls
- DLP Tagging
- Customizable X-Headers
- 62 Address Book Attributes
- Approval Workflows