



Centre  
TECHNOLOGIES

LAYERED SECURITY

# EMPLOYEE SECURITY AWARENESS

Prevent malicious attacks at their source—before the click.



**EDUCATION**

Tailored and engaging security training based on current threat landscape



**PRIORITIZED**

Analyzing behaviors and risks to blueprint a tailored training program for improvement



**SIMULATED**

Real-world scenario phishing campaigns and simulated phishing security tests



**CONTINUOUS**

Rigorous process and reporting providing visibility to security posture and awareness improvements



**EMPLOYEES SUSCEPTIBLE TO PHISHING ATTACKS**  
due to careless clicking of malicious emails\*

**RAPID INCREASE OF SECURITY AWARENESS**  
decreasing vulnerability by 50% in the first 90-days\*

The graphic shows a central interface with a calendar icon labeled 'TAILORED ONLINE TRAINING', a video player with a play button, and a list of training modules. To the right is a 'SECURITY AWARENESS VISIBILITY AND REPORTING' section with a donut chart and a percentage sign. Below the interface is a 'SIMULATED EMAIL PHISHING CAMPAIGNS' section showing an open envelope with a skull icon and a red arrow pointing to an 'OPEN' button. A text box at the bottom right contains the text: 'Gain insights that blueprint a path to stronger security posture. ASK US ABOUT SECURITY VISIBILITY'.

\*KnowBe4, 2019 Top Three Industries at Risk By Size

# LAYERED AWARENESS THAT ENHANCES SECURITY POSTURE



## TAILORED ONLINE TRAINING

- Curates training curriculum videos aligned to prioritized security topics
- Segments training curriculum for specific departments, roles, access and influence
- Delivers enhanced training curriculum based on additional compliance requirements, including:
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Security Standard (PCI)
  - California Consumer Privacy Act (CCPA)
  - Personally Identifiable Information (PII)
  - General Data Protection Regulation (GDPR)

## EXAMPLE SECURITY TRAINING TOPICS

- Current Common Threats and Trends
- Two-Factor Authentication
- Password Security
- Social Engineering
- Phishing Fundamentals
- Reporting Unsolicited Phishing Emails
- Ransomware

## SIMULATED EMAIL PHISHING CAMPAIGNS

- Sends simulated phishing emails to targeted employees and departments
- Monitors open and click rates of email campaigns to measure phishing vulnerabilities
- Analyzes behavior patterns and themes
- Identifies beneficial security training and initiatives to correct phishing-prone behaviors
- Continuously evolves blueprint for future phishing campaigns that improve and enrich awareness and visibility
- Adjusts blueprint of recommended security training and future phishing campaigns to optimize behavioral improvements

## SECURITY AWARENESS VISIBILITY AND REPORTING

- Delivers visibility to security risk scores by location or group
- Aggregates security training completion percentage rates and scores by employee, location or group
- Reports phishing campaign fail rate over time
- Reveals areas to prioritize security training
- Provides individual employee security awareness report card based on training and phishing campaigns
- Centralized portal for viewing security posture statistics along side other Centre services