BAI SECURITY

Securing Your Network, Securing Your Success

Security Awareness Training and Simulated Phishing Platform

Helps you manage the problem of **social engineering**

Security Awareness Training

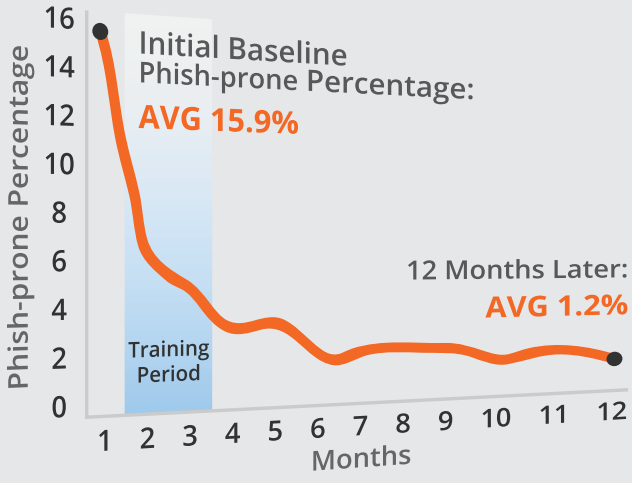
Old-school security awareness training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks.

Baseline Testing
We provide baseline testing to assess the Phish-prone™ percentage of your users through a free simulated phishing attack.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, community phishing templates and custom templates also available.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



The System Really Works

After years of helping our customers train their employees to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks, we decided to go back, and look at the actual numbers over a 12 month period.

We aggregated the numbers and the overall Phish-prone percentage **drops from an average of 15.9% to an amazing 1.2% in just 12 months.** The combination of web-based training and frequent simulated phishing attacks really works.

Security Awareness Training Features

Security Awareness Training

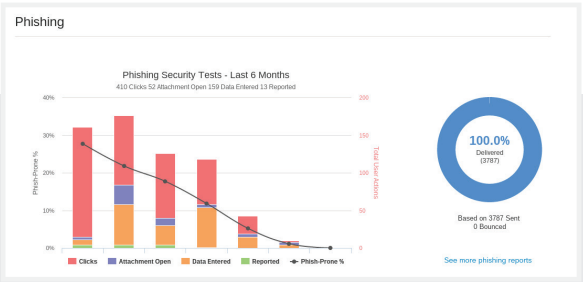
We offer three Training Levels: Core, Professional, and Advanced, giving you access to our content library of 300+ items based on your subscription level. BAI Security training modules specialize in making sure employees understand the mechanisms of spam, phishing, spear phishing, malware and social engineering.

- Interactive, web-based, on-demand, engaging training
- Create multiple training campaigns as ongoing or with a specified completion date
- Automated enrollment and follow-up emails to "nudge" users who are incomplete
- Auto-enroll new users added to a group or company
- Point-of-failure training auto-enrollment
- Dedicated Hosting Options, or run the course in your own LMS

Phishing

BAI Security's highly effective scheduled Phishing Security Tests keep your employees on their toes with security top of mind. Within the Admin Console you are able to schedule regular Phishing Security Tests from our large library of known-to-work templates, or choose a template from the community templates section where you can also share phishing templates with your peers.

- Year-round simulated phishing attacks
- Full library of successful phishing templates
- Set-it-and-forget-it scheduling of attacks
- Easily create your own templates
- Customizable landing pages
- Customizable "hover-links" when a user "mouse-overs"
- Phishing Reply Tracking allows you to track if a user replies to a simulated phishing email and can capture the information sent in the reply
- Tests for opening MS Office attachments and secondary action of enabling macros
- "Anti-prairie dog" campaigns that send random templates at random times preventing users warning each other
- Phish Alert Button add-in button gives your users a way to report simulated and non-simulated phishing attacks



Reporting and User Management

Our robust reporting capabilities allow you to easily access user training completions, Phish-prone percentage, compliance reports and more.

- Utilize at-a-glance Training Campaigns Dashboard to see campaign status, completion percentage and individual progress
- Specify user needs to "Read and Attest" Security Policy for compliance
- Advanced Phishing Reporting provides powerful features, for instance, a report of phishing failures by group or manager and many more reports
- Top 50 Clickers report
- Filter campaigns by recipient, delivered, opened, clicked, attachment, data entered, bounced, export in CSV
- Phishing Security Test results emailed to admin upon completion
- Our ***NEW* Active Directory Integration** allows you to easily upload user data and saves you time by eliminating the need to manually manage user changes

Advanced Features

Endpoint Compromise: Allows an internal "human pentest." Launch a simulated phishing attack - which if clicked on - comes up with a secondary ruse like a Java popup that the user is social engineered to click on. If the user clicks on the secondary action, their workstation can be scanned for several items specified by the admin.

USB Drive Test™: Allows you to test your user's reactions to unknown USBs. You can download a special, file from our admin console onto an USB drive which you can drop at a high traffic area. If an employee picks up the USB drive and uses it, the device will "call home" and report the fail.

GEO-location: See where your simulated phishing attack failures are on a map, with drilldown capability and CSV-export options.

Vulnerable Browser Plugin Detection: Automatically detect what vulnerable plugins any clickers on your phishing tests have installed in their browsers.

New Social Engineering Indicators: Turns every simulated phishing email into a tool IT can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email.

Get Your Free Phishing Security Test!

Find out what percentage of your employees are Phish-prone™

Contact us for information.

BAI SECURITY

900 National Parkway Suite 320, Schaumburg, IL 60173 • (847) 410-8180 • info@baisecurity.net • www.baisecurity.net

© 2017 BAI Security. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

BAI SECURITY

Securing Your Network, Securing Your Success

Security Awareness Training Subscription Levels

Our SaaS subscription is priced per seat, per year. We offer Core, Professional or Advanced levels to meet your organization's needs.

FEATURES	CORE	MOST POPULAR PROFESSIONAL	ADVANCED
Admin Management Console	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓
Automated Training Campaigns	✓	✓	✓
Monthly Email Exposure Check	✓	✓	✓
Phishing Security Tests		✓	✓
Phish Alert Button		✓	✓
Active Directory Integration		✓	✓
Phishing Reply Tracking		✓	✓
Endpoint Compromise: "Automated Human Pentesting"		✓	✓
USB Drive Test™		✓	✓
Vulnerable Browser Plugin Detection		✓	✓
Social Engineering Indicators		✓	✓
Training Access Level: Unlimited Library			✓

Core Level: All 27+ BAI Security training modules including monthly Email Exposure Check (EEC) Reports.

- Email Exposure Check monthly reports show you which email addresses from your domain are exposed on the Internet and are a target for phishing attacks

Professional Level: Includes all features of Core. Professional also includes our Advanced Phishing Features; Endporint Compromise, USB Drive Test, Vulnerable Browser Plugin Detection and landing page Social Engineering Indicators.

- Endpoint Compromise is a patent-pending functionality that allows an internal, fully automated "human pentest" (available for U.S. and Canada)
- USB Drive Test™ allows you to test your user's reactions to unknown USBs they find
- Vulnerable Browser Plugin Detection reports on browser / device used to open a phishing email and vulnerable browser plugins the user has installed
- Social Engineering Indicators patent-pending technology, turns every simulated phishing email into a tool IT can use to dynamically train employees by instantly showing them the hidden red flags they missed within that email

Advanced Level: Includes all features of Core and Professional. Advanced also includes Training Access Level: Unlimited, giving you full access to our content library of over 300 items including interactive modules, videos, games, posters and newsletters.

900 National Parkway Suite 320, Schaumburg, IL 60173 • (847) 410-8180 • info@baisecurity.net • www.baisecurity.net

© 2017 BAI Security. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Security Awareness Core & Professional Course Descriptions – Main Courses

Courses for All Employees

Core Security Awareness Training

Our new KnowBe4 Basic Security Awareness Training is 30 minutes long. It has the “Your Role” section from our 45 min. course. It also contains the shortened Red Flags section and a new "Common Threats" section that covers the fake Excel/CEO fraud threat as well as ransomware, and has a 10-question assessment at the end.

Ransomware

This course takes an employee through the basics of what ransomware is, how it came to be, and what the risks of ransomware are. It has a lot of the information of the immensely popular Ransomware Hostage Rescue Manual that KnowBe4 publishes for free. It's 25 minutes long and has a 10-question assessment at the end that needs to be passed with an 80% score.

Handling Sensitive Information Securely

This 15-minute module specializes in making sure your employees understand the importance of safely handling sensitive information, like Personally Identifiable Information (PII), Protected Health Information (PHI), Credit Card data (PCI DSS), Controlled Unlimited Information (CUI), including your organization’s proprietary information and are able to apply this knowledge in their day-to-day job for compliance with regulations.

Creating Strong Passwords

This 10-minute module covers the rules of how to create and use strong passwords in both an office environment and at the house. Employees learn the 10 important rules for safer passwords, minimum password length, how to remember long passwords, get trained in best practices like using pass phrases and how to use a different password for every website.

Mobile Device Security

This 15-minute module specializes in making sure your employees understand the importance of Mobile Device Security. They will learn the risks of their exposure to mobile security threats so they are able to apply this knowledge in their day-to-day job.

Safe Web Browsing

This 10-minute module takes employees through the basics of safe web browsing. They will learn how to avoid common dangers and the "do's and "don'ts" of safe web browsing. This module is set up to be fully interactive and could be presented as a quiz to take and "see how much you know".

Security Awareness Core & Professional Course Descriptions – Specialized Courses

SPECIALIZED AND INDUSTRY-SPECIFIC COURSES

CEO Fraud

In this 10-minute module, employees are quickly brought up to speed to inoculate them against what the FBI calls "Business Email Compromise" and what is commonly known as CEO Fraud. Concepts like social engineering, email spoofing, and the two ways that CEO Fraud is being perpetrated are covered. There is a short video with a live demo of an infected Excel file, and a short quiz to test understanding at the end. Downloadable PDF Resources: Social Engineering Red Flags, and Security Awareness: Best Practices.

Financial Institution Physical Security

This 20-minute module covers the protection of your employees, your customers and their funds, the premises, any security devices, computers, and networks, from physical circumstances and events that could cause serious losses or damage. This includes protection from robbery, kidnap/extortion, bomb threat, fire, natural disasters, burglary, and nuclear emergencies.

Basics of Credit Card Security

It is meant for all employees in any organization who handle credit cards in any form, whether taking orders on the phone, swipe cards on terminals or through devices connected to smart phones. It teaches employees to handle credit card information securely to prevent data breaches. Employees are taught the rules for paper copies of credit card data, and things to remember during data entry, including things NOT to do like sending credit card information through email and text and more. A quiz ends off this module.

GLBA Security Awareness Training

In this module, employees of financial institutions are stepped through the concepts of “Non-Public Personal Information”, or NPPI, best practices for protecting customers’ personal information, the employee's role in ensuring protection of NPPI, what is social engineering and how not to get tricked, how to protect against unauthorized access and misuse of protected information, and how to provide notice of an incident that may compromise customer information security.

Ransomware for Hospitals

Hospitals are currently targeted by cyber criminals, penetrating their networks and locking patient files with crypto-ransomware so that no data is accessible for any hospital worker. This short (7-minute) module gives anyone working in a hospital the basics of ransomware, email security and Red Flags they need to watch out for to help prevent very expensive attacks like this.

PCI Simplified

This 30-minute module uses real examples of credit card fraud, and how to protect your organization against this by being PCI compliant. This course is for anyone that’s responsible for handling credit cards in your organization and qualifies as Security Awareness Training. Especially owners, the CFO or Controller, managers and IT people in charge of credit card processing should take this course. After the training, you are able to download essential references regarding being or becoming PCI compliant.

Kevin Mitnick Security Awareness Training

This web-based interactive training using common traps, live demonstration videos, short tests and the new scenario-based Danger Zone exercise. Kevin Mitnick Security Awareness Training specializes in making sure employees understand the mechanisms of spam, phishing, spear phishing, malware, ransomware and social engineering, and are able to apply this knowledge in their day-to-day job.

Security Awareness Core & Professional Course Descriptions – Micro-Focused

MICRO-FOCUSED MODULES

Credit Card Security – Part 1

This 5-minute micro-module covers why it's so important to protect credit card information; what hackers are after, how employees are a key factor in keeping credit card information secure; and how malware can be used to capture this information.

Credit Card Security – Part 2

This 5-minute micro-module covers the rules for safely storing credit card information, the danger in texting credit card numbers, the rules for staying secure while working remotely, and the dangers of using Wi-Fi.

Danger Zone Exercise

This 5-minute micro-module is an interactive course all about phishing. There are four scenarios where the learner is asked to spot the potential threat. Each scenario provides valuable feedback based on the learner's responses. There are two versions of this course, one with sound and one without.

Email Spoofing

This 5-minute micro-module covers the very important topic of email spoofing. It defines social engineering and shows how hackers can infiltrate an organization and create spoofed emails that trick unsuspecting employees. It also covers a real-life example of just how dangerous email spoofing can be.

Handling Sensitive Information – Part 1

This 5-minute micro-module covers the basics of safely handling sensitive information and goes into Personally Identifiable Information (PII).

Handling Sensitive Information – Part 2

This 5-minute micro-module covers part 2 of safely handling sensitive information and goes into Protected Health Information (PHI).

Ransomware

This powerful 5-minute micro-module takes an employee through the basics of ransomware, the different methods used to infect a machine, and how hackers trick unsuspecting users into downloading infected files.

Social Engineering

This 5-minute micro-module defines social engineering and describes what criminals are after. It covers the three main areas of attack: digital attacks, in-person attacks, and phone attacks.

Social Media Best Practices

This 5-minute micro-module provides a brief overview of best practices that businesses and employees can implement to prevent attacks and protect sensitive information from social media hackers.

Strong Passwords

This 5-minute micro-module covers the rules of how to create and use strong passwords in both an office environment and at home. Employees learn the 10 important rules for safer passwords, minimum password length, and how to remember long passwords.

USB Attacks

This 5-minute micro-module covers the risks of picking up a USB stick and plugging it into a workstation.

Security Awareness Advanced Course Descriptions and Features

Cyber Security Awareness Interactive Learning Modules

Data Classification ILM Human Firewall ILM
Understanding and Protecting PII ILM Computer Security & Data Protection ILM OWASP Top Ten ILM
Call Center & Help Desk Awareness ILM Phishing Andrew's Inbox ILM
Ransomware ILM

Cyber Security Concepts Modules

Data Classification
Human Firewall
Identification & User Authentication
Malware
Mobile Security Basics Non-Technical Security Password Basics
Privacy
Secure Online Behavior
Security Triads
Social Engineering
The Top 10 Security Awareness Fundamentals
Call Center & Help Desk Awareness
Phishing Awareness
Understanding and Protecting PII
Top Ten Security Awareness Issues for New Hires
Computer Security & Data Protection
Executive Awareness and Leadership Module Workplace Violence and Safety
Active Shooter & Physical Incident Response

Cyber Security Awareness Compliance Modules

FERPA (Education)
FFIEC (Financial Compliance) GLBA (Finance)
HIPAA (Healthcare)
PCI-DSS (Retail Compliance)
Sarbanes-Oxley (Accounting)
Workforce Safety & Security Awareness

30+ Cyber Security Awareness Games

120+ Cyber Security Awareness Posters

Cyber Security Awareness Videos (2-5 mins)

A Day of Bad Passwords
APTs
Back Up
Being a Human Firewall
Beyond Phishing
Cyber Crime Starts with You
Data Breaches and You
Data Classification Overview
Data Loss and Insider
Dumpster Diving
Email Spoofing
Examples of Insider Jobs
Examples of Phishing
Firewalls

Cyber Security Awareness Videos (2-5 mins)

Free Wifi
Human Firewall and Data Classification
Introduction to the Cloud
Making Strong Passwords
Mobile Cyber Crime
Mobile Security Overview
Mouse Overs
Non-Technical Security Skills
Password Security
Phishing Contest Winner
Phishing From Facebook
Phishing From Netflix
Phishing From Your Bank
Phishing in Action
Physical Security Threats
PII and Compliance
Pretexting 1 (Fake Fraud Protection)
Pretexting 2 (Fake Help Desk)
Pretexting: Fake Executive to I.T.
Pretexting: From Fake Credit Card Company
Pretexting: Fake Employee to Help Desk
Pretexting From Fake I.T.
Privacy Vs. Security
Proper Hard Drive Disposal
Safe Surfing 1: HTTP vs HTTPS & Online Authentication
Security Myths Busted
Definition of Social Engineering
Social Media Data Mining
Spam
The CIA Triad
The Domains Triad
The Many Lives Triad
Types of Social Engineering
What Does a Social Engineer Look Like?
What is I.D. Theft
What is PII?
Why Security Awareness?
Low-Tech Hacks to Steal Your ID
The Many Lives of PII
Social Networking Do's and Don'ts
Social Media
Understanding Encryption
10 Ways to Avoid Phishing Scams
10 Ways to Keep PII Private
10 Ways to Stay Safe on Social Media
Incident Response 101
Your Security Awareness Journey
Non-Tech and Phys security tips and tricks
Dangers of USBs
Catching Malware
Hide Your Passwords
Introduction to Ransomware
Data Breach Overview
The Human Firewall's Top Concerns in all Three Domains