# Why security awareness training? Ransomware, that's why.

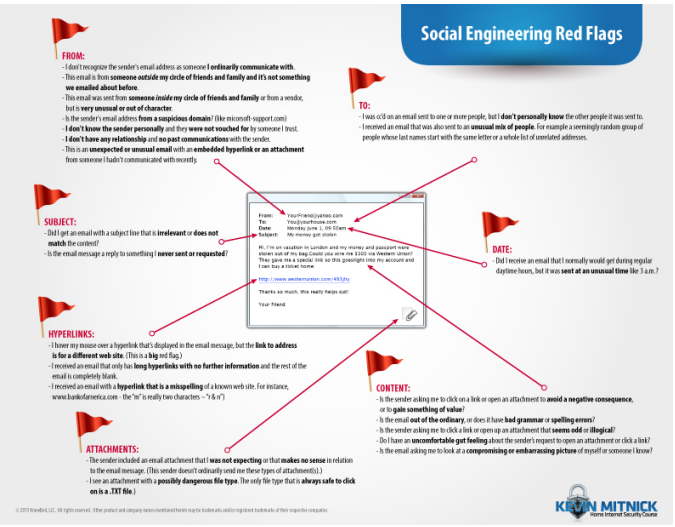
## KEVIN MITNICK Security Awareness Training

Traditional Security Awareness Training doesn't hack it anymore. Today, your employees are frequently exposed to sophisticated phishing and ransomware attacks. More than ever, your users are the weak link in your network security. They need to be trained by an expert like Kevin Mitnick, and after the training stay on their toes, keeping security top of mind.

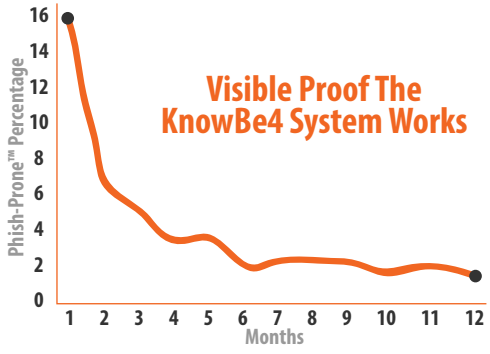
This is a high quality web-based interactive training using case-studies, live demonstration videos and short tests combined with frequent year-round simulated phishing attacks. Each case study ends with its own short multiple choice test and there is a phishing quiz at the end of the training.

Kevin Mitnick Security Awareness Training 2015 specializes in making sure employees understand the mechanisms of spam, phishing, spear-phishing, malware and social engineering, and are able to apply this knowledge in their day-to-day job.

## Social Engineering Red Flags™ with 22 things to watch out for



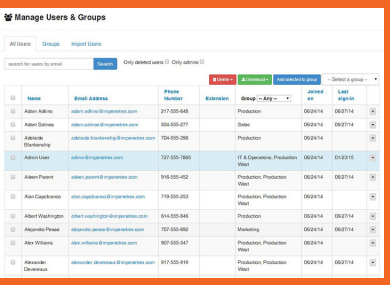

## Simulated Phishing Attacks



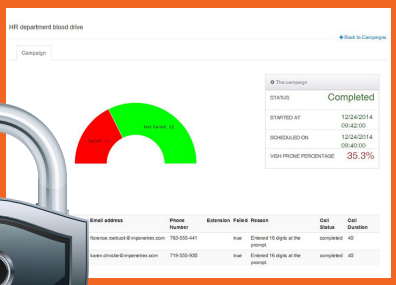

After a year of helping our customers train their employees to better manage the urgent IT security problems of social engineering, spear phishing and ransomware attacks, we decided to go back, and look at the actual numbers over those 12 months. We aggregated the numbers and the overall Phish-prone™ percentage drops from an average of 15.9% to an amazing 1.2% in just 12 months. The combination of web-based training and very regular simulated phishing attacks really works.

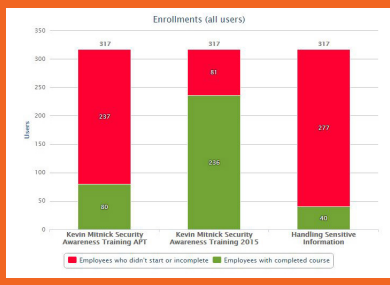
*"Social Engineering is information security's weakest link."*

– Kevin Mitnick, 'The World's Most Wanted Hacker', IT Security Consultant








# Kevin Mitnick Security Awareness Training 2015 Features

**Training:**

- On-demand, browser-based training by "The World's Most Wanted Hacker"
- Translated in 9 languages with video captions
- Multiple awareness training modules
- Allows you to create a "Human Firewall"
- Dedicated Hosting Options, or run the course in your own LMS
- Hints & Tips Security Awareness emails for compliance
- Point-of-failure training also possible
- Full time content development staff
- Visible training results: Phish-prone percentage™ for whole organization graphed over time

**Reporting:**

- Training reports (who started, who completed, who started but never finished) for all users or a specific group
- Enrollment %, Course Started %, Incomplete%, Completed Course, Acknowledged Security Policy
- Filter campaigns on recipient, delivered, opened, clicked, attachment, data entered, bounced, in CSV
- Specify user needs to "Read and Attest" Security Policy for compliance
- Individual User reports with their "open and click" history
- Reports on Browser / Device used to open phishing email
- Top 50 Clickers report

**Phishing:**

- Initial free Phish-prone™ percentage test for 100 users
- Year-round simulated phishing attacks
- Unlimited yearly use of all templates
- Set-it-and-forget-it scheduling of attacks
- Full library of successful phishing templates
- Easily create your own templates
- Customizable phishing attacks
- Customizable landing pages
- Phishing Security Test email reports sent to admin at the end of a phishing campaign
- "Anti-prairie dog" campaigns that send random templates at random times
- "Click Only" and traditional Data Entry of sensitive information, allowing for
- Customized scenarios based on public and/or personal information
- Tests for opening MS Office Attachments: Word, Excel, PPT, and PDF (also zipped)
- Variable phishing campaign length
- Summary Information about all phishing campaigns
- Free Phishing Attack Surface Analysis of emails belonging to your domain
- Phish-Prone Percentage Comparison for different user groups
- Program trend reporting
- Vishing Security Tests using IVR attacks over phone (Platinum Level)
- Customizable "hover-links" when a user mouse-overs
- Multi-domain accounts for admins or MSPs who manage multiple organizations (no extra charge)

**Additional Features:**

- Full time dedicated U.S.-based support staff
- Full and Partially Managed options
- Upload users as flat text, or as CSV with Groups functionality
- Bulk delete users using a CSV file
- Training and phishing history are archived even when users are deleted
- Support for single sign-on using Security Assertion Markup Language (SAML)
- Crypto-ransom guarantee

KnowBe4
Human error. Conquered.

Find out out affordable this is for your organization now

**Get A Quote**

KnowBe4, LLC | 601 Cleveland Street, Suite 240, Clearwater, FL 33755 | Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: sales@KnowBe4.com