

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



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.

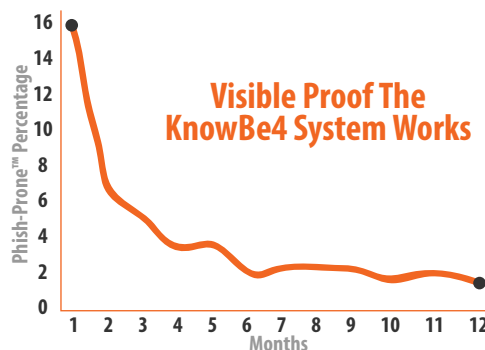
Kevin Mitnick Security Awareness Training 2015 specializes in making sure employees understand the mechanisms of spam, phishing, spear-phishing, malware and social engineering, and are able to apply this knowledge in their day-to-day job.

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

**Social Engineering Red Flags**

- FROM:**
  - I don't recognize the sender's email address as someone I **ordinarily** communicate with.
  - This email is from someone **outside my circle of friends and family** and it's not something we emailed about before.
  - This email was sent from someone **inside my circle of friends and family** or from a vendor, but it is very personal or out of character.
  - Is the sender's email address from a suspicious domain? (like misspelled support.com)
  - I don't know the sender personally and they were not vouched for by someone I trust.
  - I don't have any relationship and we've had communications with the sender.
  - This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I hadn't communicated with recently.
- TO:**
  - I was CC'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
  - I received an email that was also sent to an unusual mix of people, for example a seemingly random group of people whose last names start with the same letter or a whole list of unrelated addresses.
- SUBJECT:**
  - Did I get an email with a subject line that is irrelevant or does not match the context?
  - Is the email message a reply to something I never sent or requested?
- DATE:**
  - Did I receive an email that I normally would get during regular daytime hours, but it was sent at an unusual time like 3 a.m.?
- HYPERLINKS:**
  - I hover my mouse over a hyperlink that displayed in the email message, but the link to address is for a different web site. (This is a big red flag.)
  - I received an email that only has long hyperlinks with no further information and the rest of the email is completely blank.
  - I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofamerica.com - the "m" is really two characters - "i&n")
- ATTACHMENTS:**
  - The sender included an email attachment that was not expected or that makes no sense in relation to the email message. (This sender doesn't usually send me these types of attachments.)
  - I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .TXT file.
- CONTENT:**
  - The sender asking me to click on a link or open an attachment to avoid a negative consequence, or to gain something of value?
  - Is the email out of the ordinary, or does it have bad grammar or spelling errors?
  - Is the sender asking me to click a link or open up an attachment that seems odd or illegal?
  - Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
  - Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

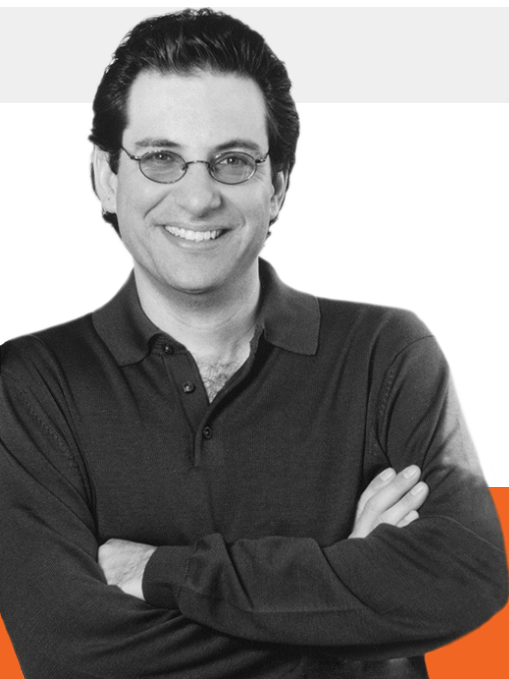
## Simulated Phishing Attacks



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



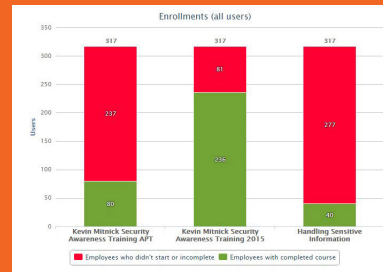
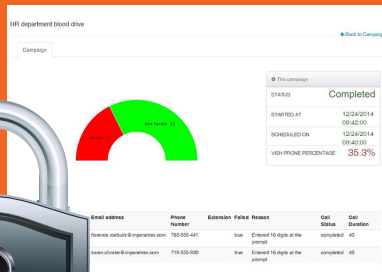
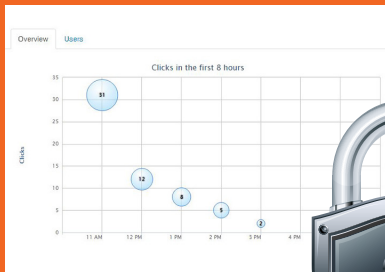
**Manage Users & Groups**

All Users | Groups | Import Users

Only selected users | Only active |

search for users by email

Name	Email Address	Phone Number	Extension	Group - Any - C	Last Login
Adam Adams	adam.adams@organization.com	719-555-5455		Production	08/24/14
Adam Barnes	adam.barnes@organization.com	564-555-9777		Sales	08/24/14
Adam Blumstein	adam.blumstein@organization.com	754-555-3066		Production	08/24/14
Adam Lopez	adam.lopez@organization.com	707-555-7865		IT & Operations, Production	08/24/14
Adam Parent	adam.parent@organization.com	916-555-452		Production	08/24/14
Alan Caplan	alan.caplan@organization.com	719-555-293		Production	08/24/14
Alan Washington	alan.washington@organization.com	614-555-946		Production	08/24/14
Alexander Pines	alexander.pines@organization.com	707-555-682		Marketing	08/24/14
Alex Wilkins	alex.wilkins@organization.com	807-555-347		Production	08/24/14
Alexander DeLeon	alexander.deleon@organization.com	917-555-919		Production	08/24/14



# 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

## 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

## 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
- Phishing 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)

- 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  
© 2015 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Features are subject to change without notice. All products mentioned are trademarks or registered trademarks of their respective companies. Copyright © 2015 KnowBe4