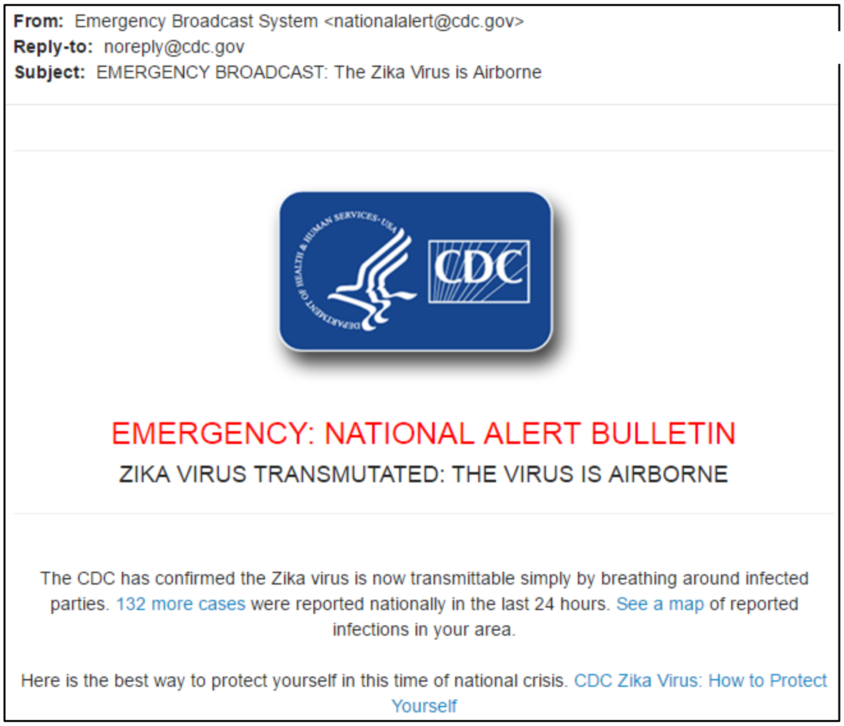
THE LeMoyne-Owen COLLEGE
Leadership. Opportunity. Change.

LeMoyne-Owen College Security Awareness Training Program

Twentieth century security awareness is not effective in the twenty-first century. Today, employees are frequently exposed to sophisticated phishing and ransomware attacks. LeMoyne-Owen College (LOC) utilizes a combination of frequent simulated phishing attacks and web-based security awareness training. LOC provided an initial baseline test to assess the Phish-prone™ percentage of admin, faculty, and staff email users through a simulated phishing attack. Users that clicked on links or open attachments were then provided on-demand, interactive, engaging training with common traps, live Kevin Mitnick demos and new scenario-based Danger Zone exercises. Ongoing monthly phishing campaigns, combined with integrated online Security Awareness Training, ensure employees are immunized against the mechanisms of spam, phishing, spear phishing, malware and social engineering. Enterprise-strength reporting, showing stats and graphs for both training and phishing are provided to LOC management.

Sample phishing email campaign for LOC admins/faculty/staff:



From: Emergency Broadcast System <nationalalert@cdc.gov>
Reply-to: noreply@cdc.gov
Subject: EMERGENCY BROADCAST: The Zika Virus is Airborne

EMERGENCY: NATIONAL ALERT BULLETIN

ZIKA VIRUS TRANSMUTATED: THE VIRUS IS AIRBORNE

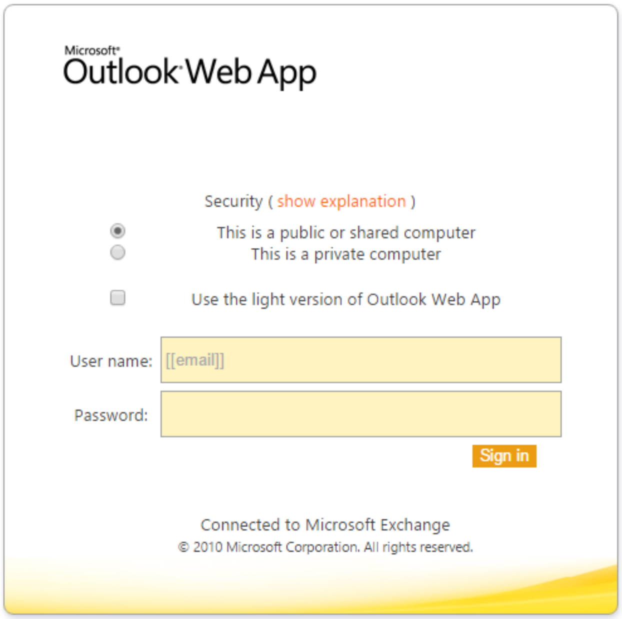
The CDC has confirmed the Zika virus is now transmittable simply by breathing around infected parties. 132 more cases were reported nationally in the last 24 hours. See a map of reported infections in your area.

Here is the best way to protect yourself in this time of national crisis. CDC Zika Virus: How to Protect Yourself

- On-demand, browser-based training featuring “The World’s Most Famous Hacker”
- Multiple awareness training modules available
- 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

The LOC Security Awareness Training Program has the ability to 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 things like user name, IP address and other data related to that user's workstation and Active Directory as specified by the admin.

Sample Landing Page to test Social Engineering Vulnerability:



Microsoft® Outlook Web App

Security (show explanation)

● This is a public or shared computer
○ This is a private computer

□ Use the light version of Outlook Web App

User name: [[email]]

Password:

Sign in

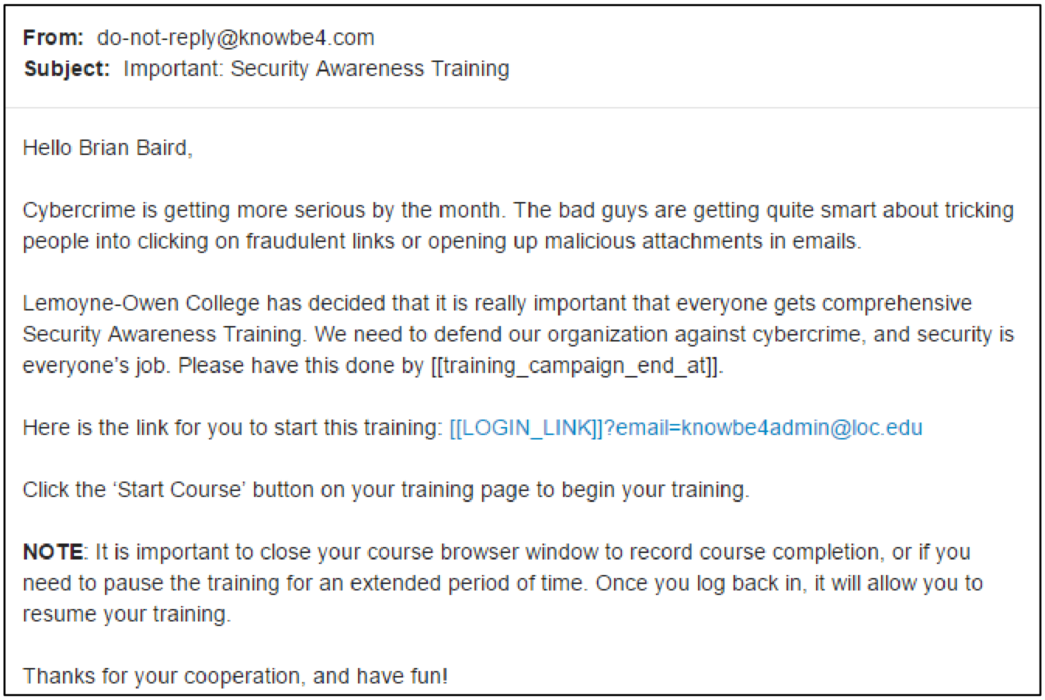
Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.

LOC utilizes highly effective, scheduled Phishing Security Tests to keep LOC employees on their toes with security top of mind. Within the Admin Console, we are able to schedule regular Phishing Security Tests from a large library of known-to-work templates:

- Monthly simulated phishing attacks
- Full library of successful phishing templates
- Set-it-and-forget-it scheduling of attacks
- 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

- Advanced Phishing Reporting provides powerful features, for instance, a report of phishing failures by group or manager and many more reports
- Utilize at-a-glance Training Campaigns Dashboard to see campaign status, completion percentage and individual progress
- Filter campaigns by recipient, delivered, opened, clicked, attachment, data entered, bounced, export in CSV
- Top 50 Clickers report
- Specify user needs to “Read and Attest” Security Policy for compliance
- Phishing Security Test results emailed to admin upon completion

Sample Enrollment Email for Security Awareness Training:



From: do-not-reply@knowbe4.com
Subject: Important: Security Awareness Training

Hello Brian Baird,

Cybercrime is getting more serious by the month. The bad guys are getting quite smart about tricking people into clicking on fraudulent links or opening up malicious attachments in emails.

Lemoyne-Owen College has decided that it is really important that everyone gets comprehensive Security Awareness Training. We need to defend our organization against cybercrime, and security is everyone’s job. Please have this done by [[training_campaign_end_at]].

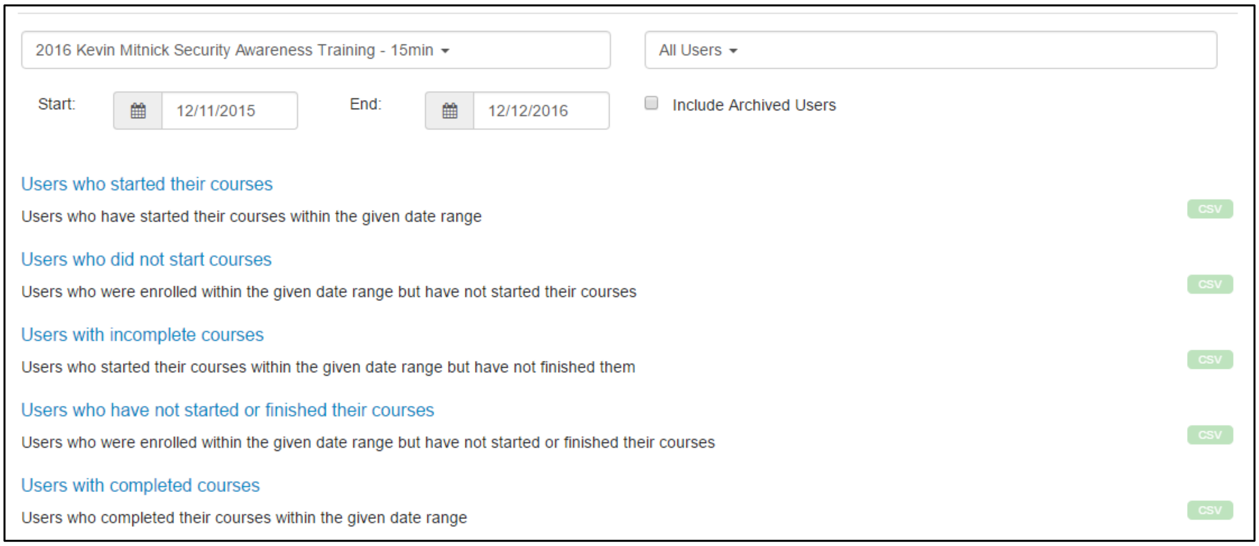
Here is the link for you to start this training: [[LOGIN_LINK]]?email=knowbe4admin@loc.edu

Click the ‘Start Course’ button on your training page to begin your training.

NOTE: It is important to close your course browser window to record course completion, or if you need to pause the training for an extended period of time. Once you log back in, it will allow you to resume your training.

Thanks for your cooperation, and have fun!

Security Awareness Training Reporting Dashboard – End User Reports



2016 Kevin Mitnick Security Awareness Training - 15min ▾ | All Users ▾

Start: 12/11/2015 End: 12/12/2016 □ Include Archived Users

Users who started their courses

Users who have started their courses within the given date range CSV

Users who did not start courses

Users who were enrolled within the given date range but have not started their courses CSV

Users with incomplete courses

Users who started their courses within the given date range but have not finished them CSV

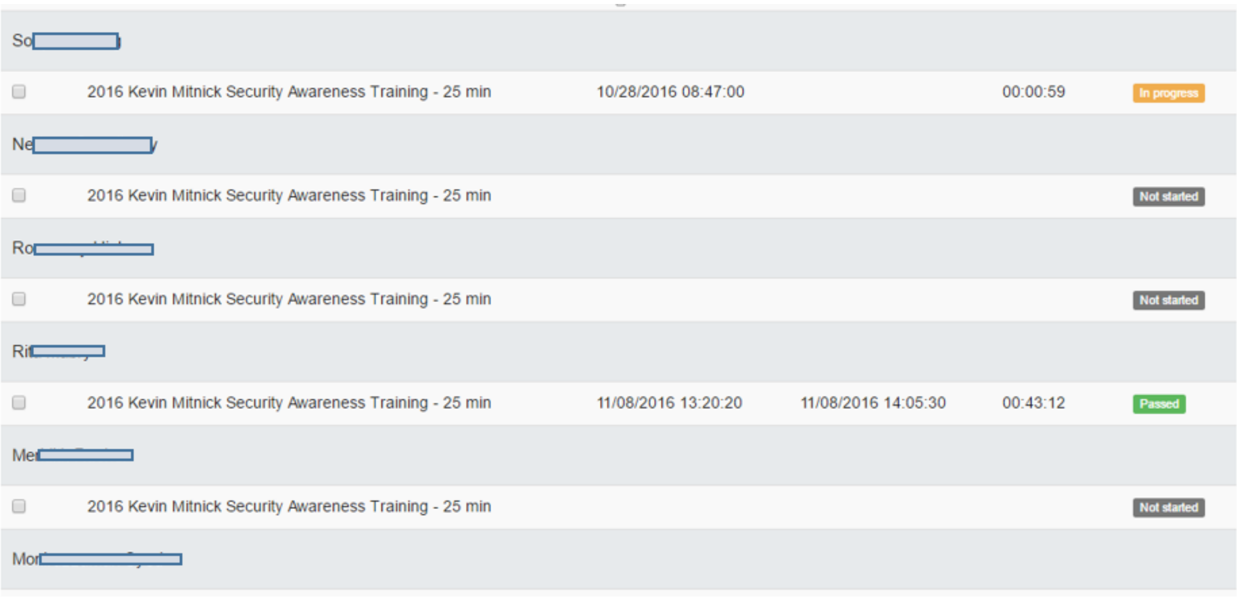
Users who have not started or finished their courses

Users who were enrolled within the given date range but have not started or finished their courses CSV

Users with completed courses

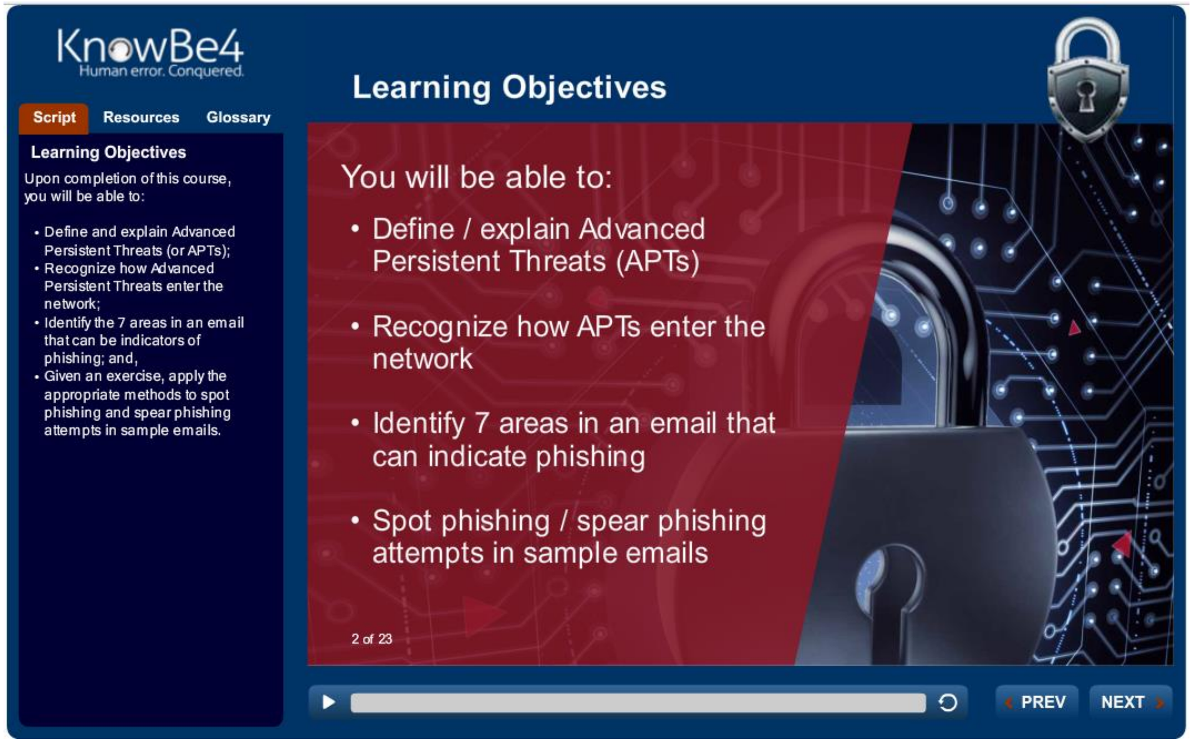
Users who completed their courses within the given date range CSV

Security Awareness Training Reporting Dashboard – Sample End User Status Report



[redacted]					
□	2016 Kevin Mitnick Security Awareness Training - 25 min	10/28/2016 08:47:00		00:00:59	In progress
[redacted]					
□	2016 Kevin Mitnick Security Awareness Training - 25 min				Not started
[redacted]					
□	2016 Kevin Mitnick Security Awareness Training - 25 min				Not started
[redacted]					
□	2016 Kevin Mitnick Security Awareness Training - 25 min	11/08/2016 13:20:20	11/08/2016 14:05:30	00:43:12	Passed
[redacted]					
□	2016 Kevin Mitnick Security Awareness Training - 25 min				Not started
[redacted]					

Sample Screens from Online Security Awareness Training Courses:



Learning Objectives

Upon completion of this course, you will be able to:

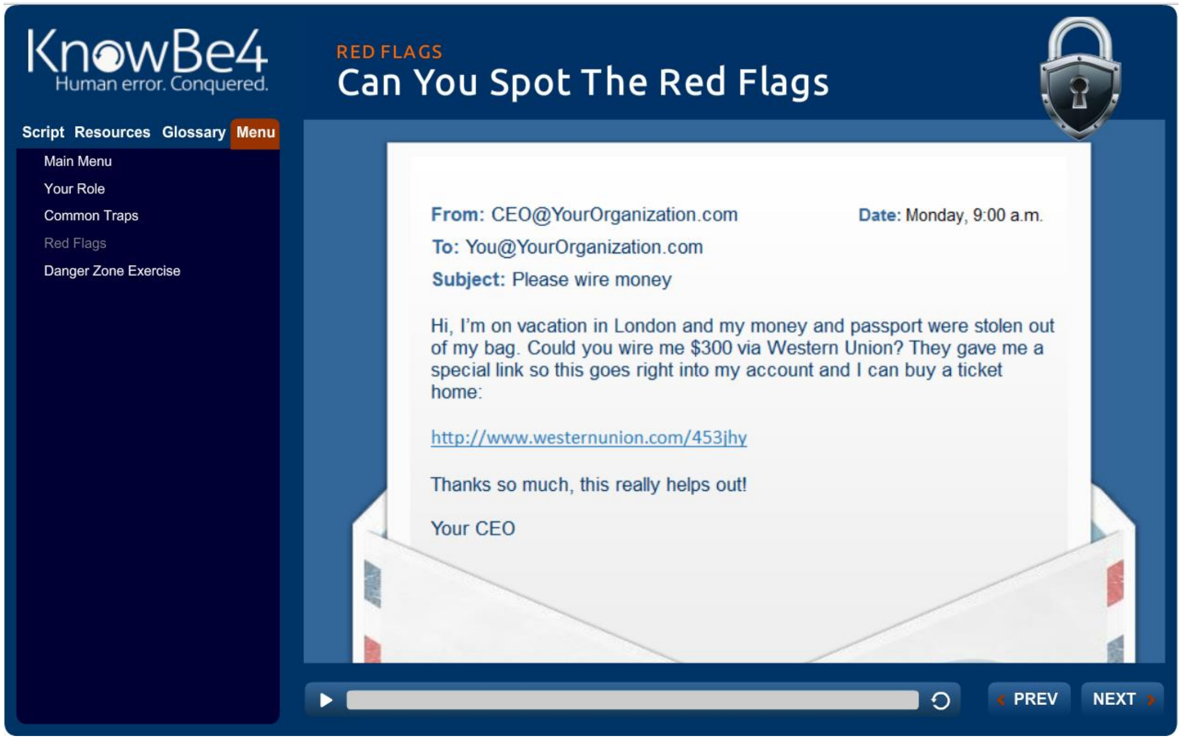
- Define and explain Advanced Persistent Threats (or APTs);
- Recognize how Advanced Persistent Threats enter the network;
- Identify the 7 areas in an email that can be indicators of phishing; and,
- Given an exercise, apply the appropriate methods to spot phishing and spear phishing attempts in sample emails.

Learning Objectives

You will be able to:

- Define / explain Advanced Persistent Threats (APTs)
- Recognize how APTs enter the network
- Identify 7 areas in an email that can indicate phishing
- Spot phishing / spear phishing attempts in sample emails

2 of 23



RED FLAGS

Can You Spot The Red Flags

From: CEO@YourOrganization.com **Date:** Monday, 9:00 a.m.

To: You@YourOrganization.com

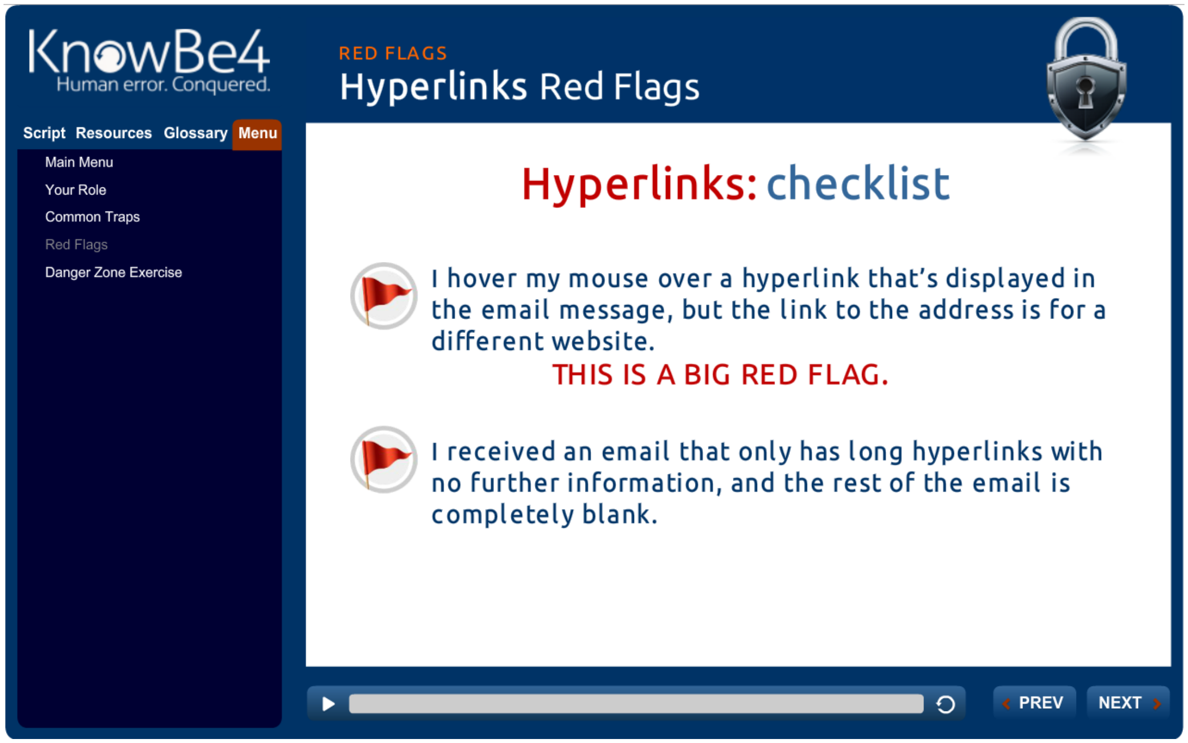
Subject: Please wire money

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Western Union? They gave me a special link so this goes right into my account and I can buy a ticket home:

http://www.westernunion.com/453jhy

Thanks so much, this really helps out!

Your CEO



RED FLAGS

Hyperlinks Red Flags

Hyperlinks: checklist

I hover my mouse over a hyperlink that's displayed in the email message, but the link to the address is for a different website.

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.