Training Employees to Recognise & Avoid Advanced Threats

Joe Ferrara, President & CEO, Wombat Security Technologies

Rashmi Knowles, Chief Security Architect EMEA, RSA The Security Division of EMC

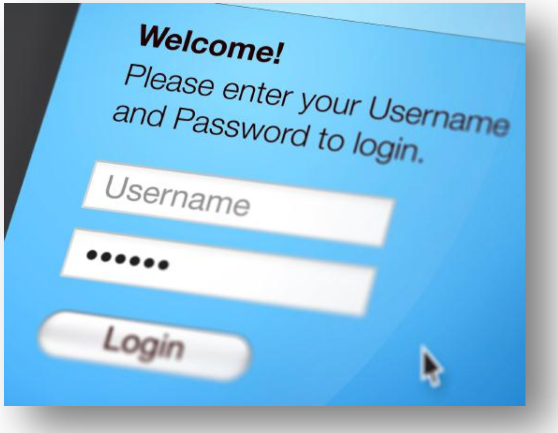
Session ID: STAR-302

Session Classification: General Interest

RSA CONFERENCE
EUROPE 2012

Agenda

- Social Engineering
- The human element of cyber security
- New approaches to training
- How is EMC training employees?
- Evaluation of results



Welcome!

Please enter your Username and Password to login.

Username

••••••

Social Engineering Scenarios

- In-person, email, smartphone, fixed phone, social networking, snail mail
- The entry point for broad attacks
- Phishing attacks are over 50% of security incidents (1)

(1)US CERT percentage of 2011 reported incidents

Increasingly Sophisticated Attacks

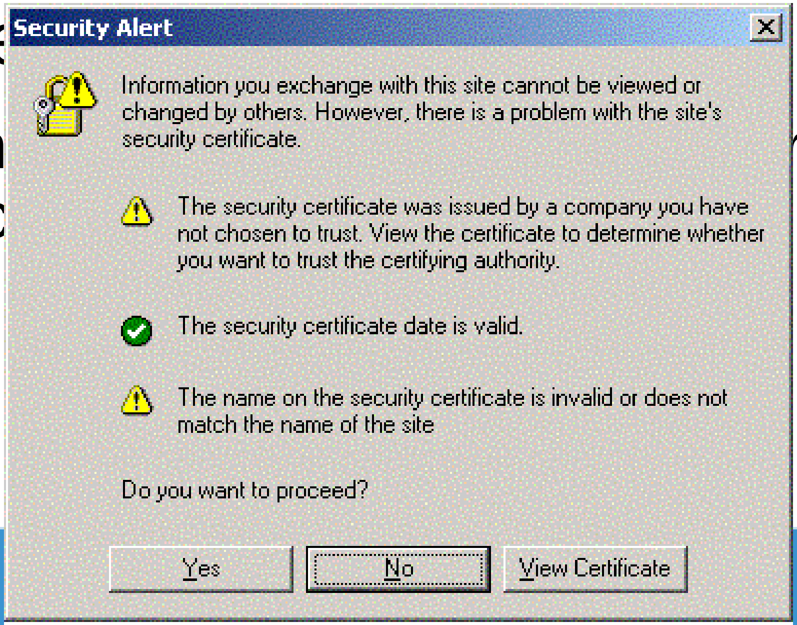
- Spear-phishing targets specific groups or specific individuals
- Leverages information about your organization or group
- Uses information specifically about you
- Social phishing 4 to 5 times more effective

Bob Smith is retiring next week, click here to say whether you can attend his retirement party

Email subpoena from the US District Court in San Diego with your name, company and phone number, and your lawyers name, company & phone number…

Technology Alone Won’t Work

- Tempting to just buy software or hardware that promises to solve these problems, however
  - Attackers are very resourceful, constantly looking to circumvent defenses
  - Security controls lag behind technology adoption
  - Technology alone can’t motivate people
- Recent bre issue
  - Spear ph king malware, other soc



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Humans are the Weakest Link

- 82% of large organizations had staff driven incidents(1)
- 47% had employees lose or leak confidential information(1)
- 86% of companies cite humans as their greatest vulnerability(2)

Overlooking the human element is most common mistake in computer security

1 PWC Information Security Breaches Survey (April 2012)
2 Deloitte Global Security Survey (Feb 2009)

Training has a Big Role to Play

- Lack of understanding
- Wide range of scenarios
- Required knowledge is vast & growing
- Practical strategies not easy to articulate
- Security is a secondary task
- Delivery methods must be compelling

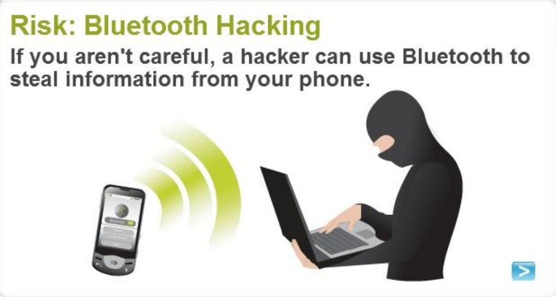
“Root cause is often a failure to invest in educating staff about security risks”

PWC Information Security Breaches Survey (April 2012)

Why has Traditional Training Failed?

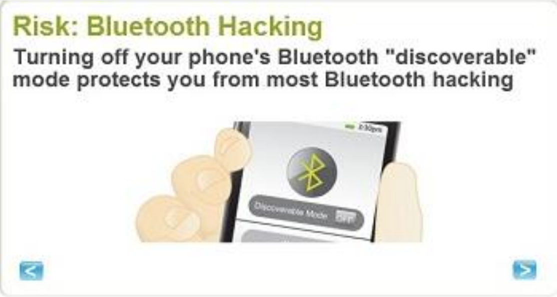
- It's boring!...out of context, and too long
- Limited user interaction or motivation
- Security team competency is not education
- Limited measurement, feedback and continuous improvement

A New Training Approach



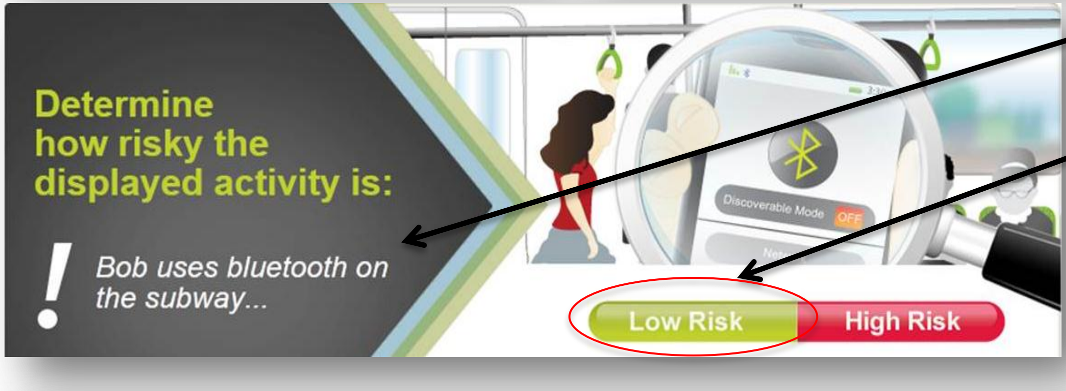
Risk: Bluetooth Hacking

If you aren't careful, a hacker can use Bluetooth to steal information from your phone.



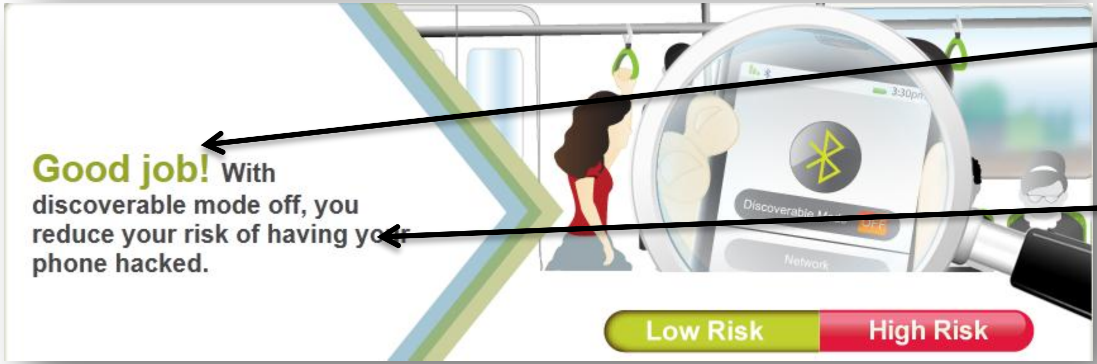
Risk: Bluetooth Hacking

Turning off your phone's Bluetooth "discoverable" mode protects you from most Bluetooth hacking



Determine how risky the displayed activity is:

! *Bob uses bluetooth on the subway...*



Good job! With discoverable mode off, you reduce your risk of having your phone hacked.

Bite-sized training & interventions

Present concepts and procedures together

Story-based environment

Learn by doing

Create teachable moments

Provide immediate feedback

Use conversational content

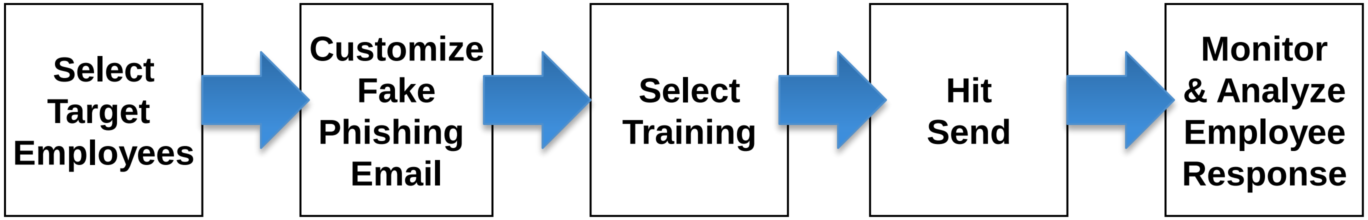
Collect valuable data

Essential Tools for Effective Training

- Training via simulated attacks
- Interactive software & gaming
- Learning by doing
- Training in context & story telling

Training via Simulated Attacks

- Training as part of daily routine
- Just-in-time training for those that fall for attack
- Creates a unique “teachable moment”
- Significantly increases training penetration
- Provides detailed reporting & metrics



Select Target Employees

Customize Fake Phishing Email

Select Training

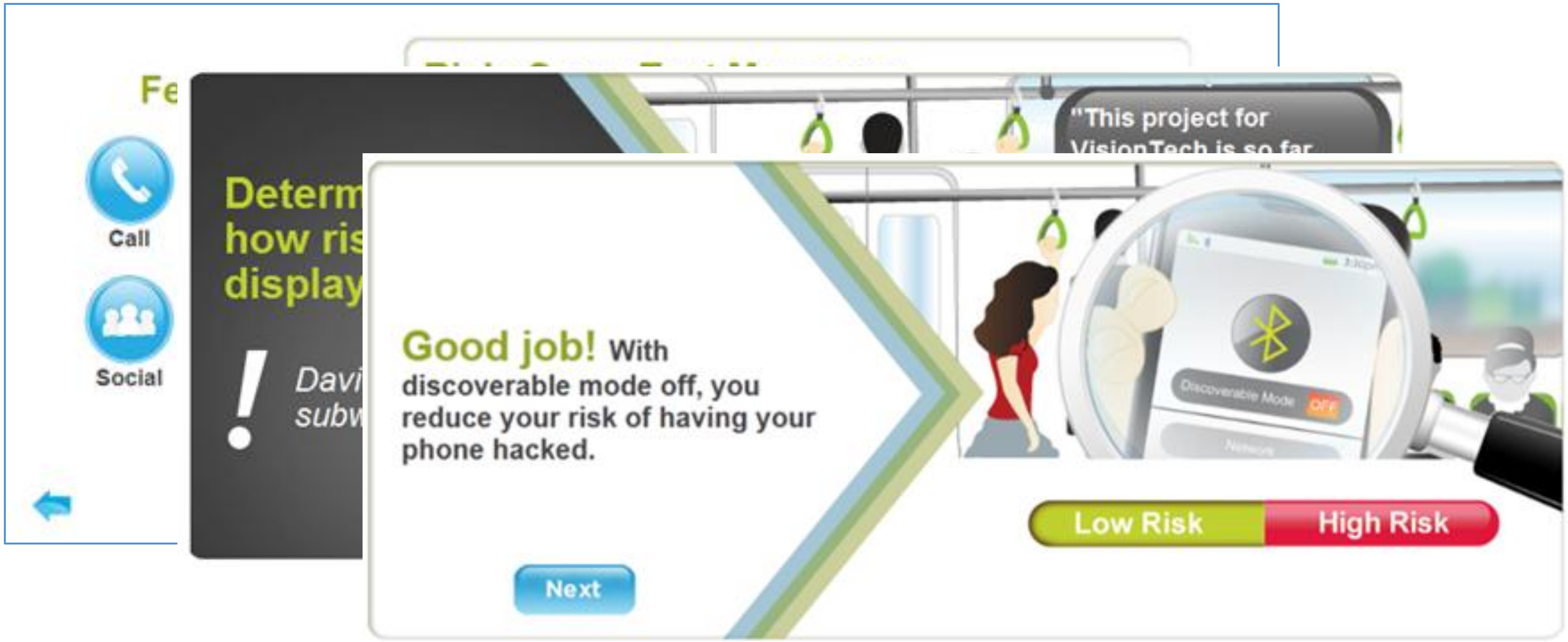
Hit Send

Monitor & Analyze Employee Response

Training via Micro-Games

- Training doesn't have to be boring or take long
- Micro game format, play for short time
- Two-thirds of Americans played a video game in past six months
- Not just young people or males
  - Average game player 35 years old
  - 25% of people over 50 play games
  - 40% of casual gamers are women

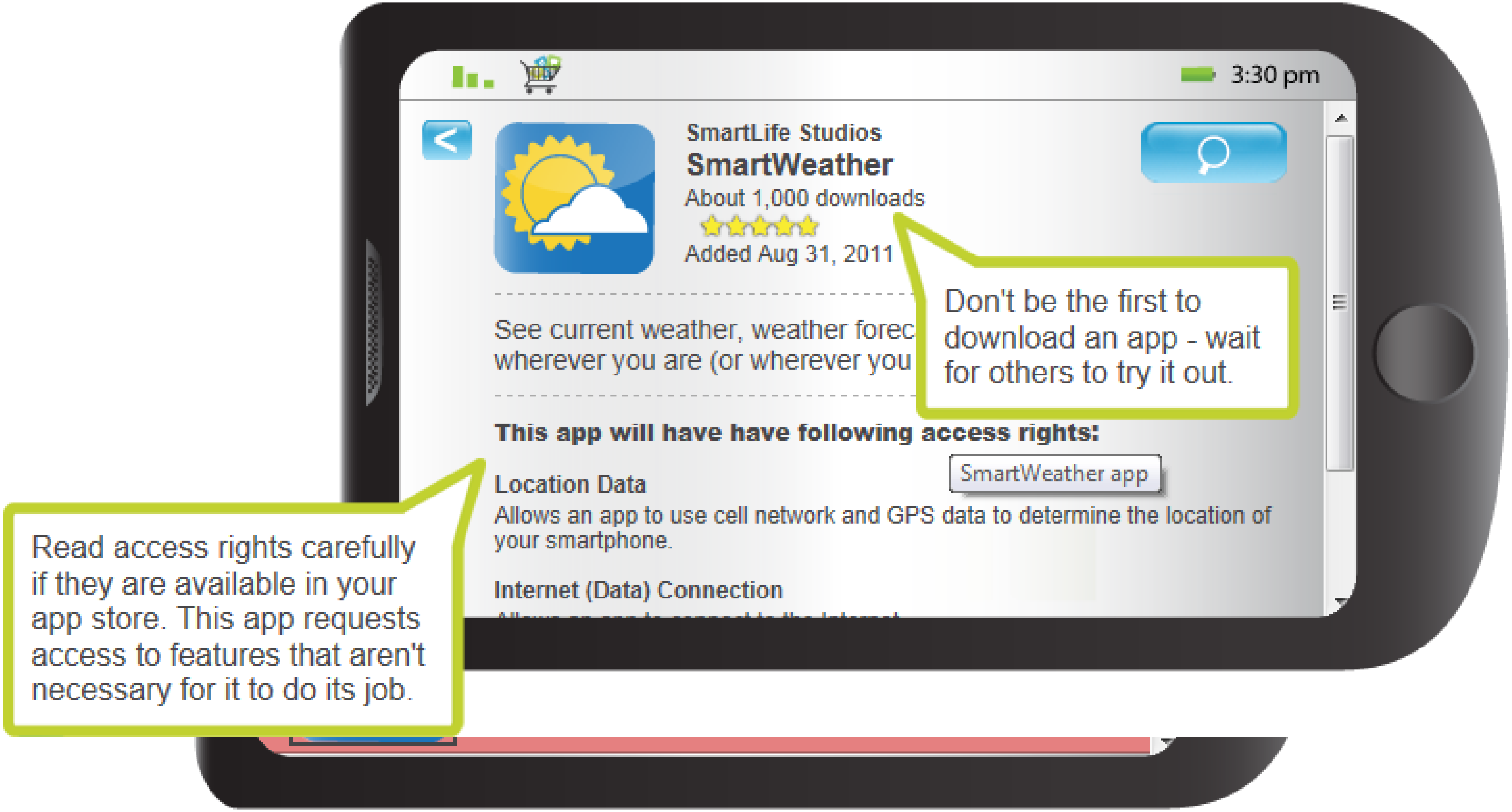
Learning by Doing is Critical



Good job! With discoverable mode off, you reduce your risk of having your phone hacked.

- Teach people to better appreciate the risks
- Create mock situations
- Force them to make decisions
- Provide them with feedback

From Simple to Realistic Scenarios



3:30 pm

SmartLife Studios

SmartWeather

About 1,000 downloads

Added Aug 31, 2011

See current weather, weather forec
wherever you are (or wherever you

This app will have have following access rights:

SmartWeather app

Location Data

Allows an app to use cell network and GPS data to determine the location of your smartphone.

Internet (Data) Connection

Allows an app to connect to the Internet

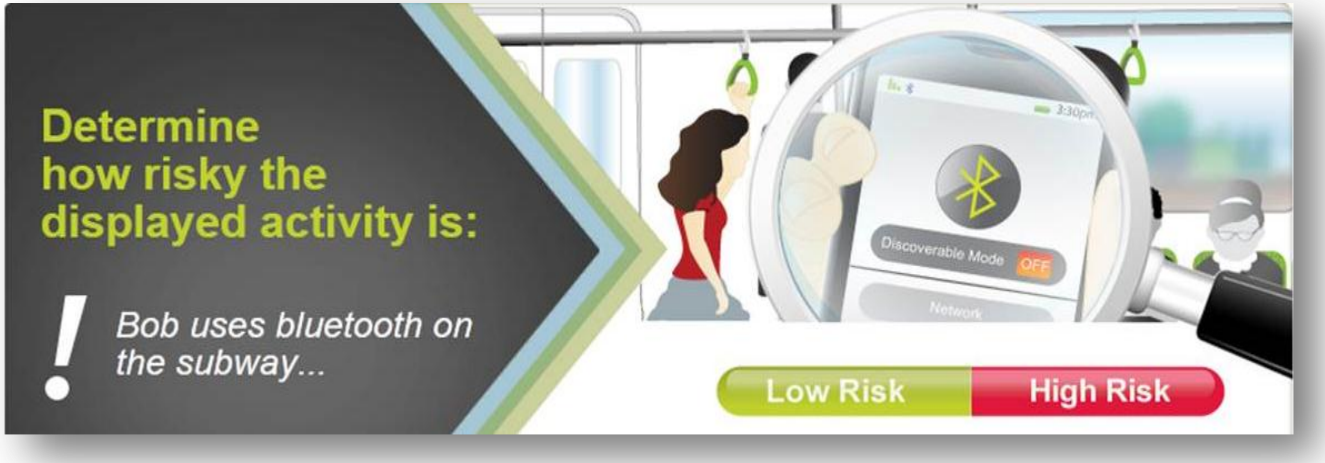
Don't be the first to download an app - wait for others to try it out.

Read access rights carefully if they are available in your app store. This app requests access to features that aren't necessary for it to do its job.

Click on the safer app.

Creating scenarios & Telling stories

- Stories enhance learning
- Characters engage users
- Scenarios provide context
- Enable unique teachable moments
- Provide longer-term retention



Determine how risky the displayed activity is:

! Bob uses bluetooth on the subway...

How EMC is Training Employees to Recognise and Mitigate Advanced Threats

Rashmi Knowles CISSP

RSA, The Security Division of EMC

Session ID: STAR-302

Session Classification: General Interest

RSA CONFERENCE EUROPE 2012

Understanding EMC's Culture and Human Psychology

….the key to effective security awareness

Engaging

Aligned with my interests and goals

Friendly competition

Sharing information

Inviting comment on ideas & issues

Technical & intellectual challenges

Competitive geeks rule!

We ignore the unimportant stuff until we have no choice.

Our aim is to get through required training as quickly as possible before we….

…return to battle the daily spam stream.

Off putting

Focused on GSO's self-interests

Stern memo's

Finger wagging

Blind compliance

Lengthy training courses

Obstacles e.g. extra clicks

Overview of FirstLine Program

Website

EMC Social Media

CBT & IL Training

Posters

Emails

Phishing Tests

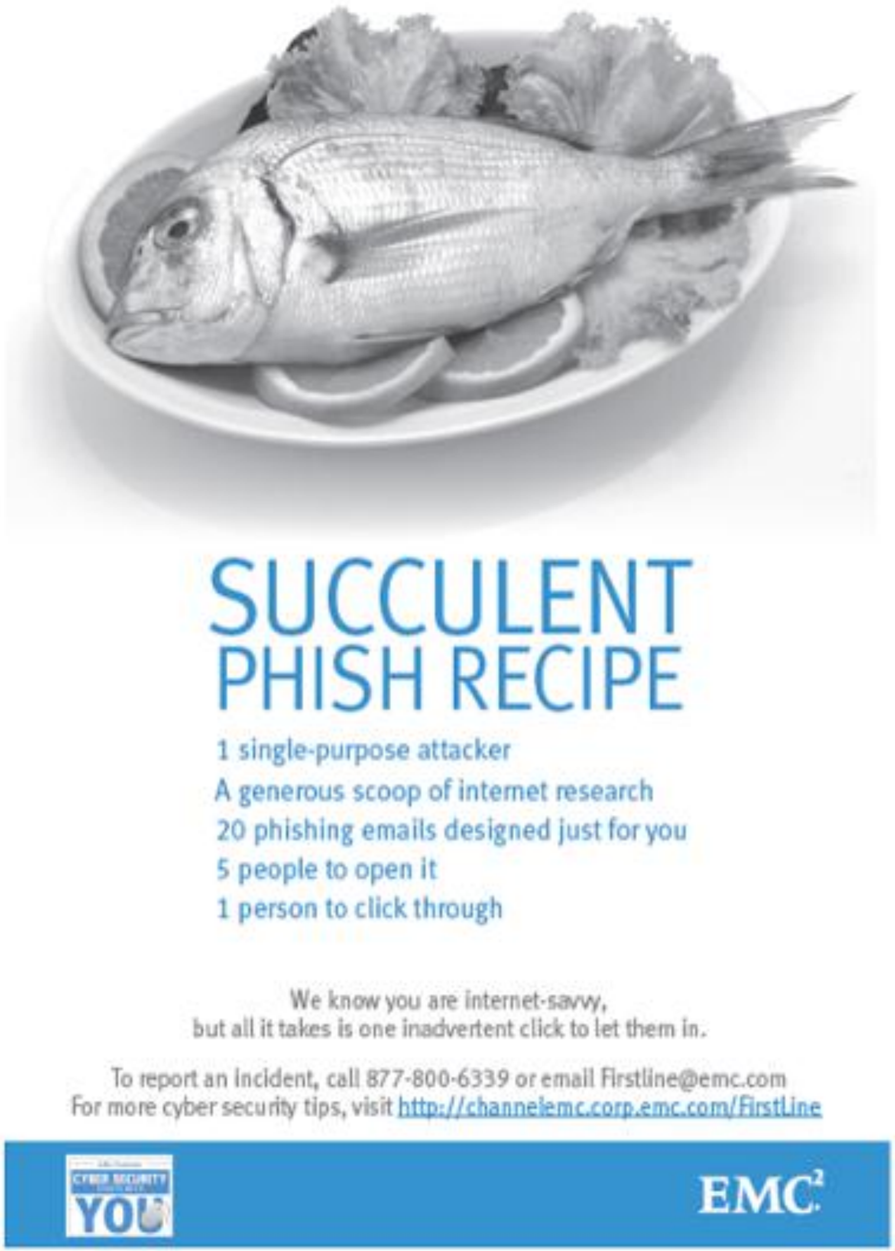
Multimedia

Threat Briefings

EMC ONE
Online Network of EMCers
EMC
EMC UNIVERSITY
STRENGTHEN YOUR PASSWORD
J@B1tW79!
EMC
EMC FirstLine
THINK
BEFORE YOU CLICK
PHISHING
eduTube

Key Accomplishments:

- Multimedia and game based training against APT’s and phishing; regular newsletters
- Presented Threat Briefings
- Trained all new hires
- Proactively phished 500+ employees (average failure rate 15%)
- Series of 4 security awareness posters distributed to offices in 21 countries



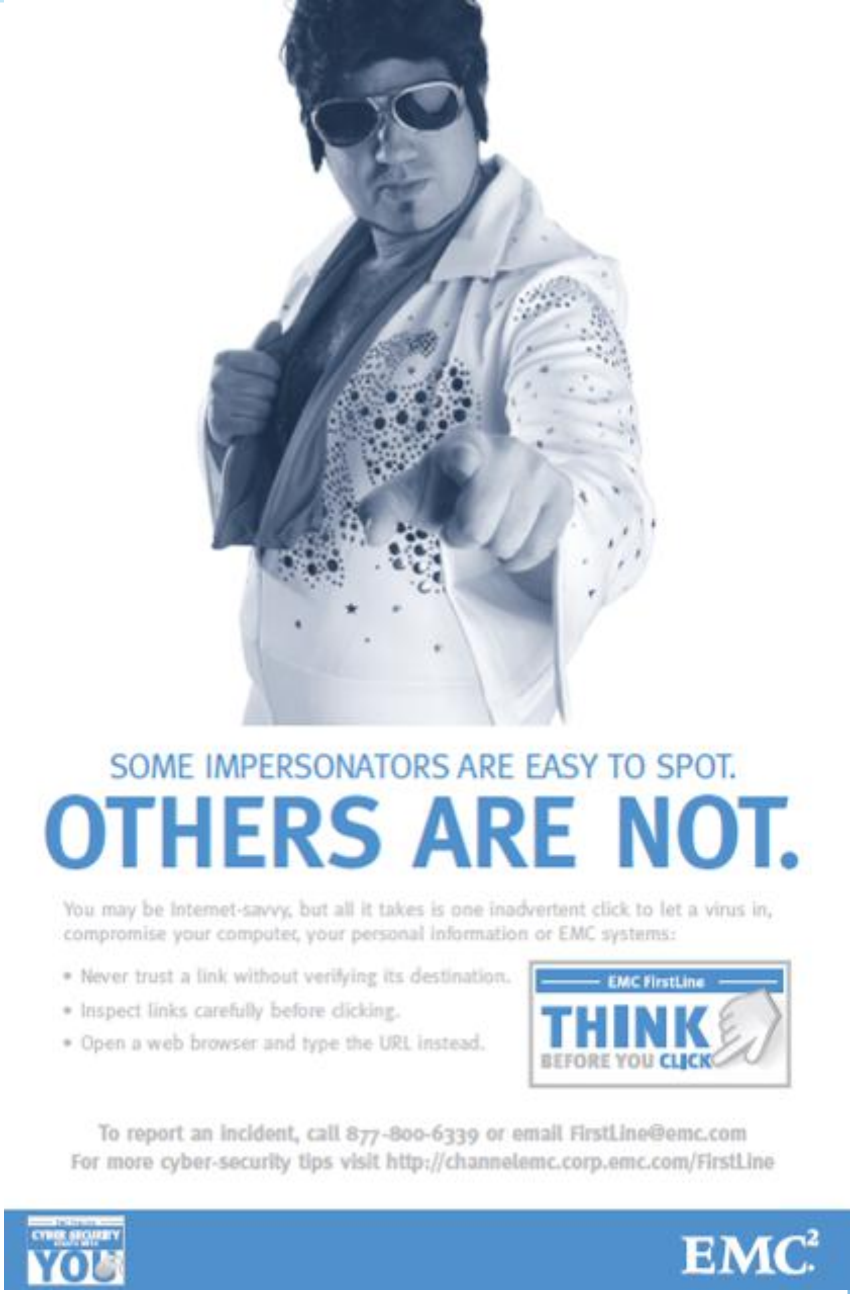
SUCCULENT PHISH RECIPE

1 single-purpose attacker
A generous scoop of internet research
20 phishing emails designed just for you
5 people to open it
1 person to click through

We know you are internet-savvy,
but all it takes is one inadvertent click to let them in.

To report an incident, call 877-800-6339 or email Firstline@emc.com
For more cyber security tips, visit http://channelemc.corp.emc.com/FirstLine

EMC²



SOME IMPERSONATORS ARE EASY TO SPOT.

OTHERS ARE NOT.

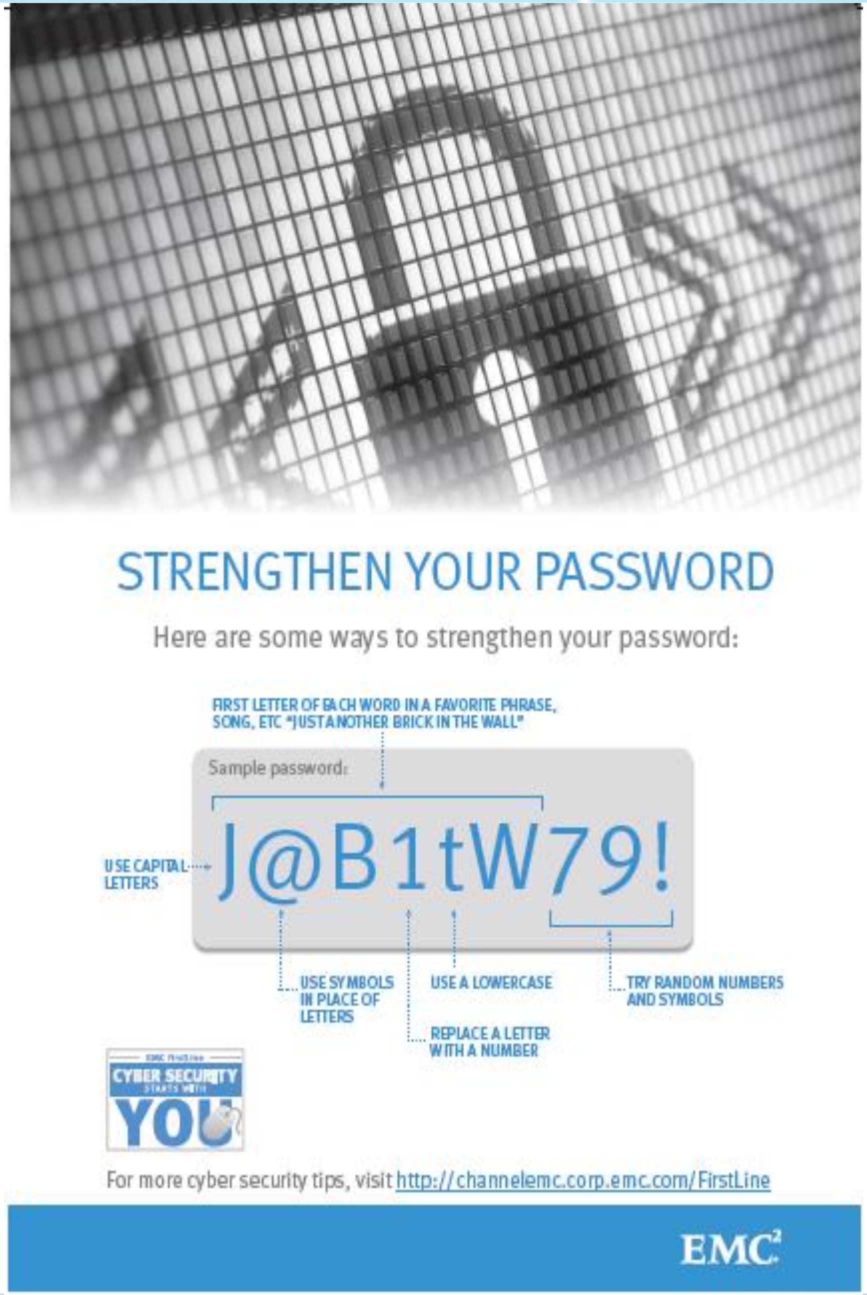
You may be Internet-savvy, but all it takes is one inadvertent click to let a virus in, compromise your computer, your personal information or EMC systems:

- Never trust a link without verifying its destination.
- Inspect links carefully before clicking.
- Open a web browser and type the URL instead.

EMC FirstLine
THINK
BEFORE YOU CLICK

To report an incident, call 877-800-6339 or email FirstLine@emc.com
For more cyber-security tips visit http://channelemc.corp.emc.com/FirstLine

EMC²



STRENGTHEN YOUR PASSWORD

Here are some ways to strengthen your password:

FIRST LETTER OF EACH WORD IN A FAVORITE PHRASE, SONG, ETC "JUST ANOTHER BRICK IN THE WALL"

Sample password:

J@B1tW79!

USE CAPITAL LETTERS

USE SYMBOLS IN PLACE OF LETTERS

USE A LOWERCASE

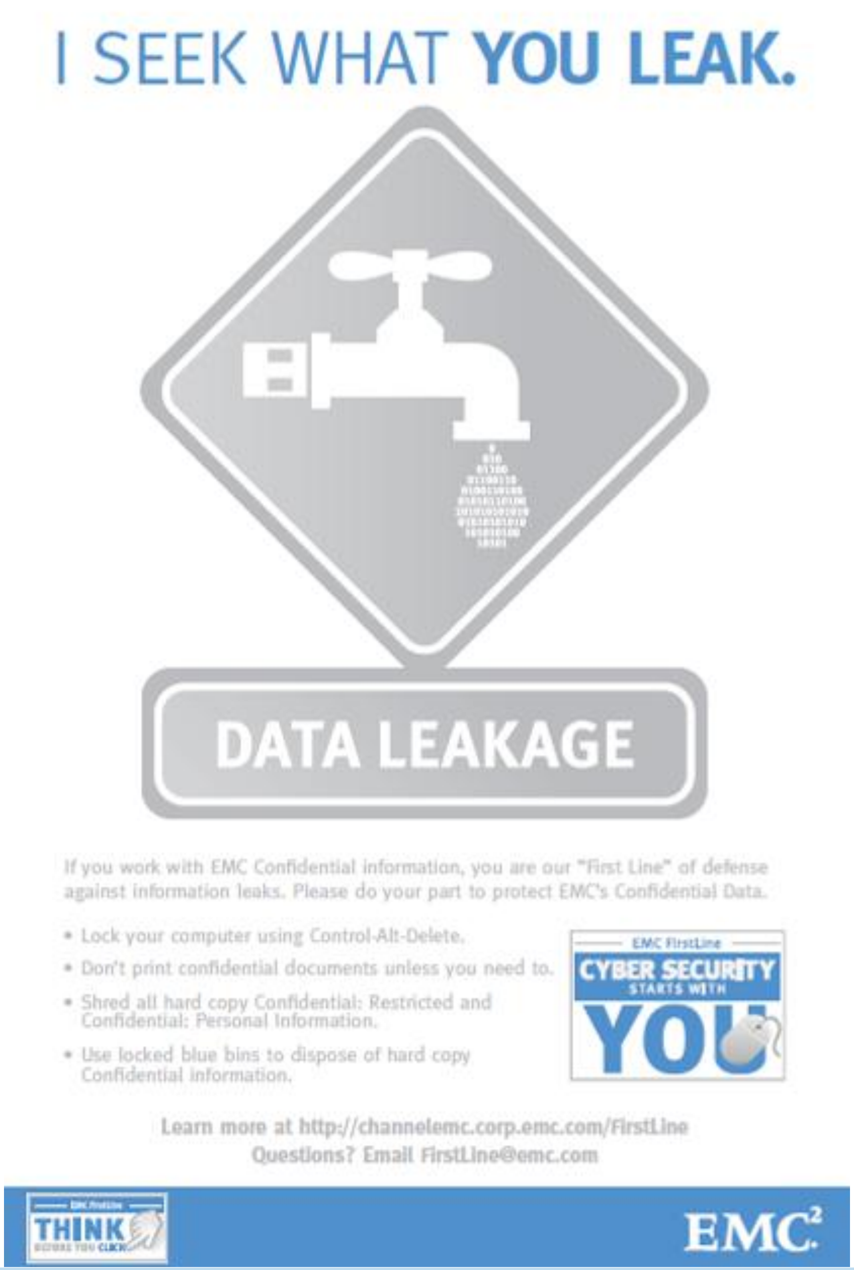
REPLACE A LETTER WITH A NUMBER

TRY RANDOM NUMBERS AND SYMBOLS

CYBER SECURITY STARTS WITH YOU

For more cyber security tips, visit http://channelemc.corp.emc.com/FirstLine

EMC²



I SEEK WHAT **YOU LEAK.**

DATA LEAKAGE

If you work with EMC Confidential information, you are our "First Line" of defense against information leaks. Please do your part to protect EMC's Confidential Data.

- Lock your computer using Control-Alt-Delete.
- Don't print confidential documents unless you need to.
- Shred all hard copy Confidential: Restricted and Confidential: Personal Information.
- Use locked blue bins to dispose of hard copy Confidential information.

EMC FirstLine CYBER SECURITY STARTS WITH YOU

Learn more at http://channelemc.corp.emc.com/FirstLine
Questions? Email FirstLine@emc.com

THINK

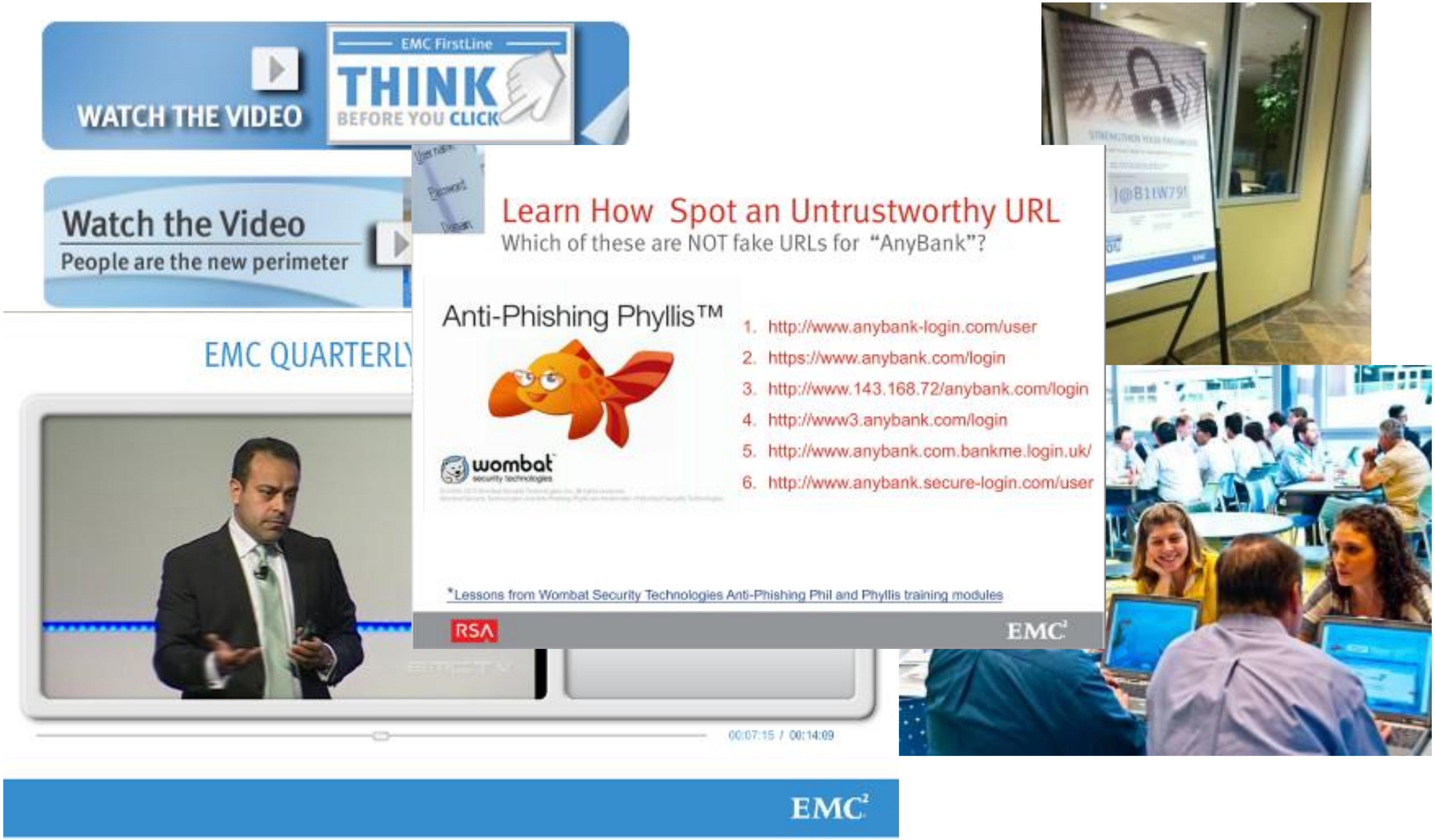
EMC²

Mandatory Information Security Training Requirements

Current training covers six topics in 60 minutes

Threats	Internet Use
Malicious websites, phishing, Malware, Social engineering, social networking	Appropriate use, downloading content, use of administrator accounts, corporate owned machines vs unmanaged devices
Securing Devices	**Email , Instant Messaging, Telephone**
Appropriate use, installation of software, accepting patch installation prompts, maintaining appropriate security software, using mobile devices	Opening unknown attachments, verifying links and claims in emails, verifying identity in person/on the telephone
Confidential Information	**Physical Security**
Handling confidential information including personal information, when to encrypt	Securing your workstation, mobile devices while traveling

EMC Employee Awareness - Train & Test



Learn How Spot an Untrustworthy URL

Which of these are NOT fake URLs for "AnyBank"?

Anti-Phishing Phyllis™

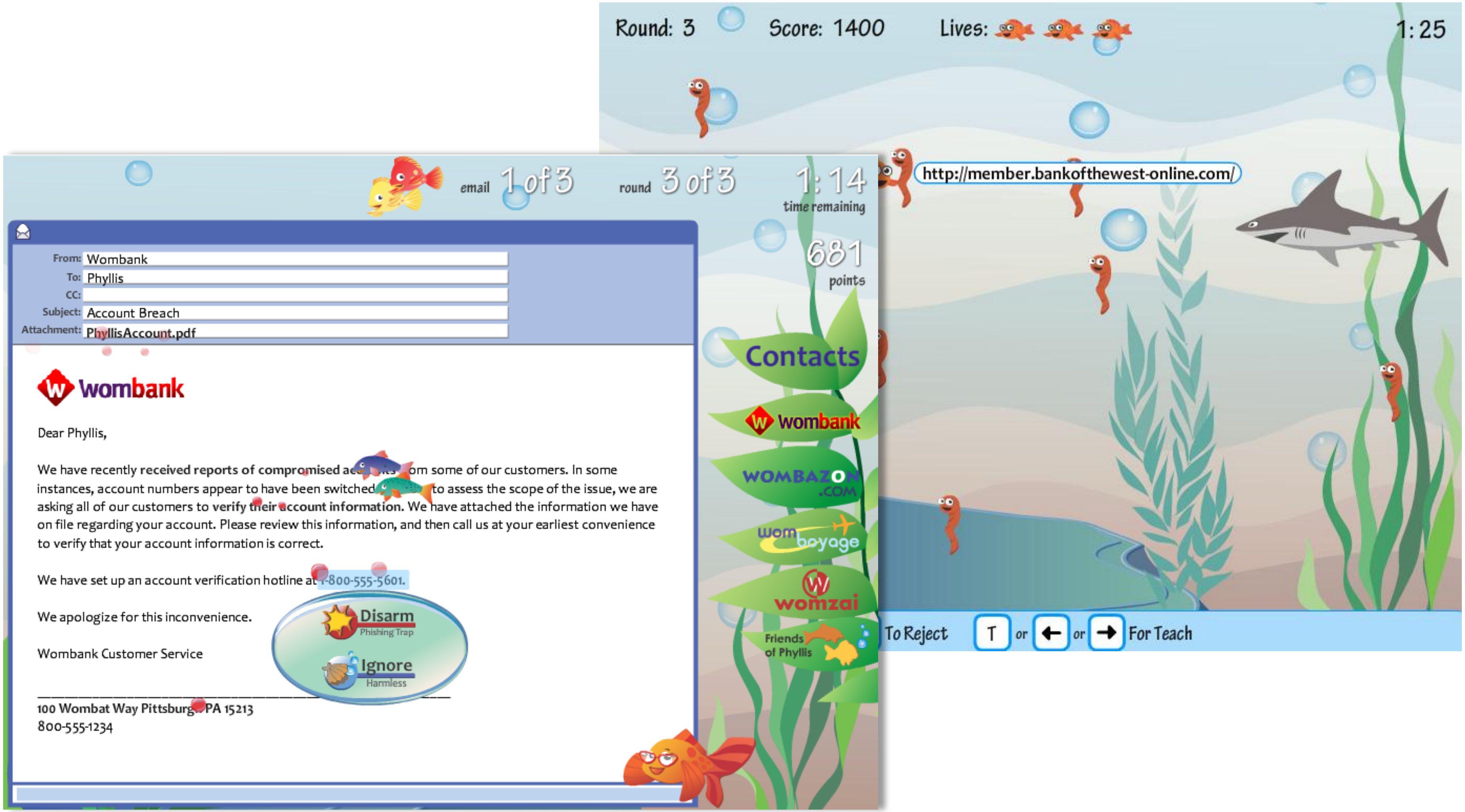
wombat security technologies

1. http://www.anybank-login.com/user
2. https://www.anybank.com/login
3. http://www.143.168.72/anybank.com/login
4. http://www3.anybank.com/login
5. http://www.anybank.com.bankme.login.uk/
6. http://www.anybank.secure-login.com/user

*Lessons from Wombat Security Technologies Anti-Phishing Phil and Phyllis training modules

RSA EMC²

Gaming Scenario



From: Wombank
To: Phyllis
CC:
Subject: Account Breach
Attachment: PhyllisAccount.pdf

wombank

Dear Phyllis,

We have recently received reports of compromised ac... om some of our customers. In some instances, account numbers appear to have been switched to assess the scope of the issue, we are asking all of our customers to verify their account information. We have attached the information we have on file regarding your account. Please review this information, and then call us at your earliest convenience to verify that your account information is correct.

We have set up an account verification hotline at 1-800-555-5601.

We apologize for this inconvenience.

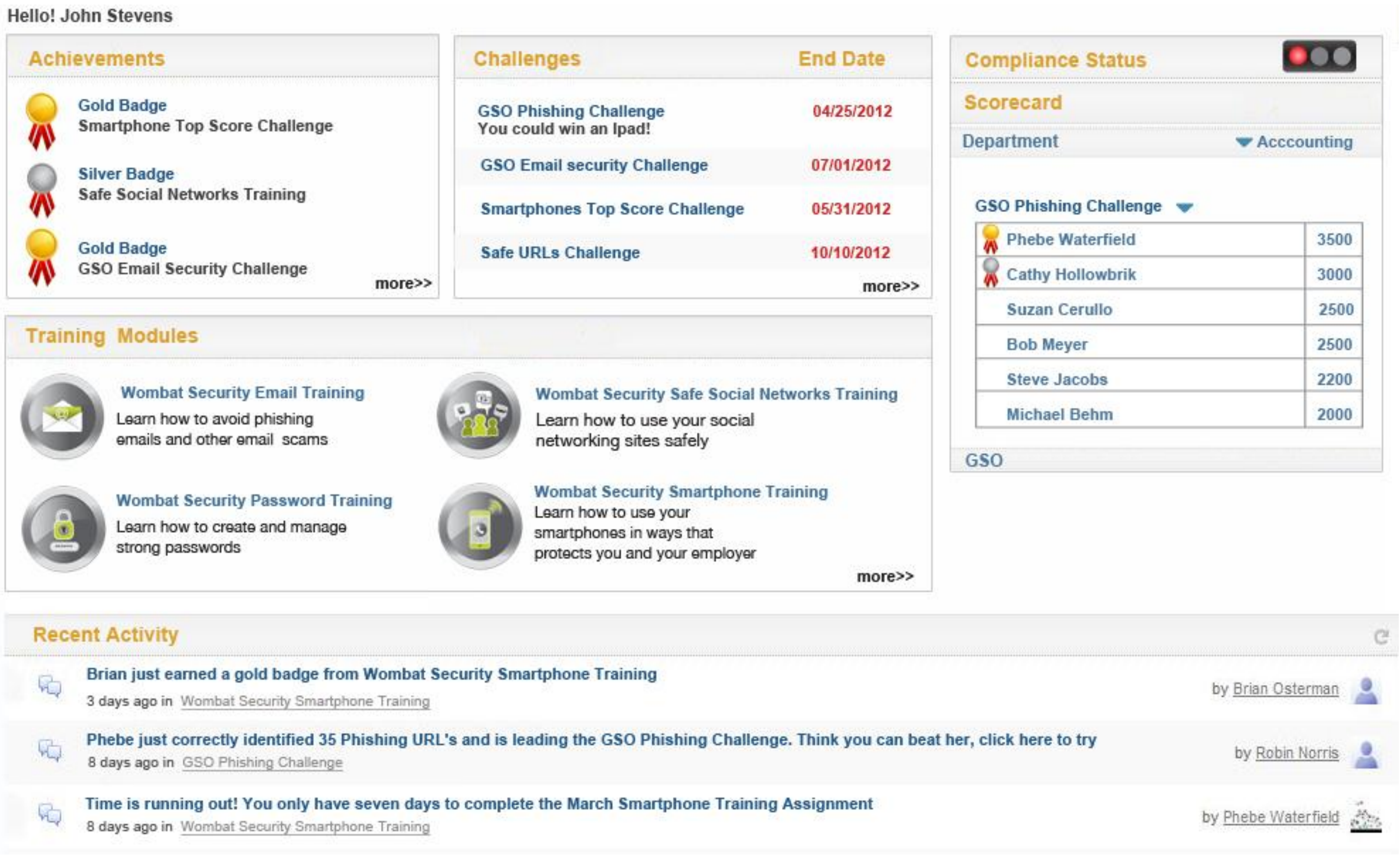
Wombank Customer Service

100 Wombat Way Pittsburgh, PA 15213
800-555-1234

EMC's Human Firewall Certification

- Mandatory training completed
  - Information security policy
  - Privacy awareness
- Tests
  - Passed a phishing test
  - Passed a clear desk test
- Attended a threat briefing session

Training Dashboard Mockup



Hello! John Stevens

Achievements

Gold Badge
Smartphone Top Score Challenge

Silver Badge
Safe Social Networks Training

Gold Badge
GSO Email Security Challenge

more>>

Challenges

Challenges	End Date
GSO Phishing Challenge You could win an Ipad!	04/25/2012
GSO Email security Challenge	07/01/2012
Smartphones Top Score Challenge	05/31/2012
Safe URLs Challenge	10/10/2012

more>>

Compliance Status

Scorecard

Department ▾ Acccounting

GSO Phishing Challenge ▾

Phebe Waterfield	3500
Cathy Hollowbrik	3000
Suzan Cerullo	2500
Bob Meyer	2500
Steve Jacobs	2200
Michael Behm	2000

GSO

Training Modules

Wombat Security Email Training
Learn how to avoid phishing emails and other email scams

Wombat Security Safe Social Networks Training
Learn how to use your social networking sites safely

Wombat Security Password Training
Learn how to create and manage strong passwords

Wombat Security Smartphone Training
Learn how to use your smartphones in ways that protects you and your employer

more>>

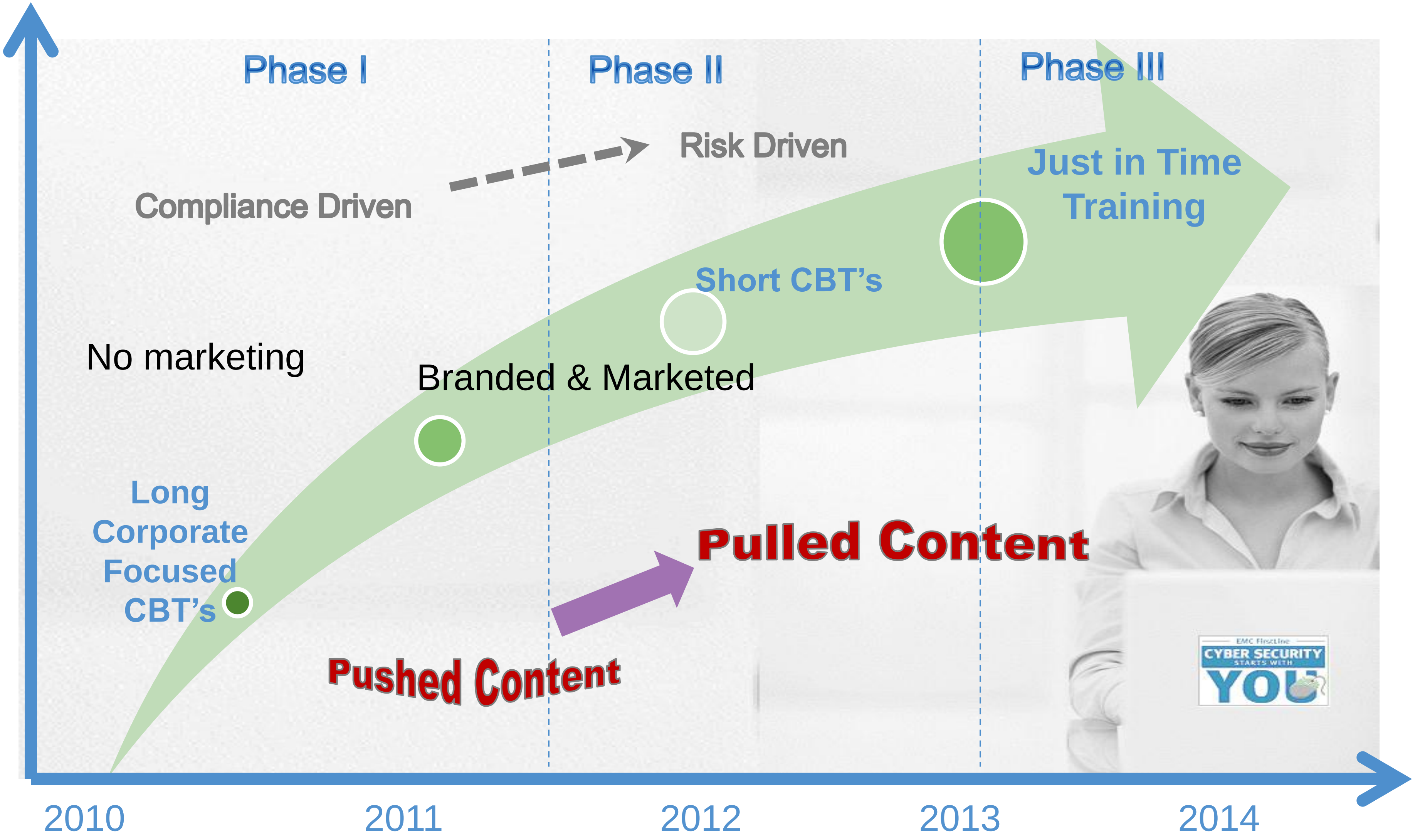
Recent Activity

Brian just earned a gold badge from Wombat Security Smartphone Training
3 days ago in Wombat Security Smartphone Training
by Brian Osterman

Phebe just correctly identified 35 Phishing URL's and is leading the GSO Phishing Challenge. Think you can beat her, click here to try
8 days ago in GSO Phishing Challenge
by Robin Norris

Time is running out! You only have seven days to complete the March Smartphone Training Assignment
8 days ago in Wombat Security Smartphone Training
by Phebe Waterfield

Security Training Roadmap



Phase I

Phase II

Phase III

Compliance Driven

Risk Driven

Just in Time Training

Short CBT’s

No marketing

Branded & Marketed

Long Corporate Focused CBT’s

Pulled Content

Pushed Content

2010

2011

2012

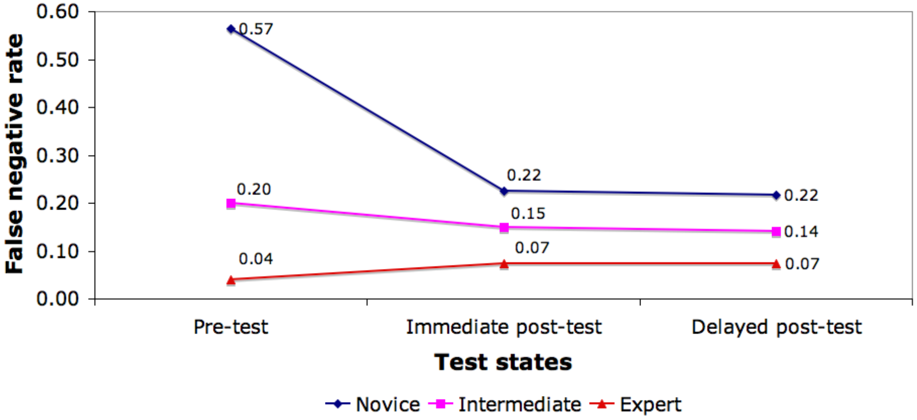
2013

2014

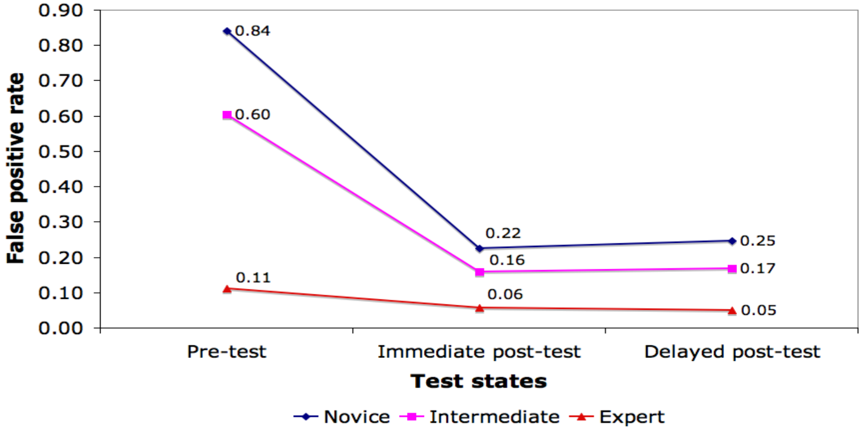
Evaluation of Game-based Training

- Peer-reviewed study validating results
- Tested security game with ~4500 users
  - Huge improvement in identifying phishing URLs
  - Also dramatically lowered false positives
- 50% decrease in susceptibility after training

Label a phishing site as legitimate



Label a legitimate site as phishing



Key Tools for Effective Training

- Tool #1 Training via simulated attacks
- Tool #2 Interactive software & gaming
- Tool #3 Learn by doing techniques
- Tool #4 Train in context
- Tool #5 Tell a story

Summary

- Humans don’t have to be your weakest link
- A security awareness program reduces your risk
- Yes, security awareness training can work
  - Phishing failure rate below 5% post training
- Training must be engaging, efficient & measurable
- Leverage learning science for the best results
- Knowledgeable users are your best defense

Thank You