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
Agenda

- Social Engineering
- The human element of cyber security
- New approaches to training
- How is EMC training employees?
- Evaluation of results
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 breaches highlight the issue
  - Spear phishing, social networking malware, other social engineering attacks
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
Create teachable moments
Present concepts and procedures together

Story-based environment
Learn by doing
Create teachable moments
Provide immediate feedback
Use conversational content
Collect valuable data

A New Training Approach
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

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

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
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

EMC²
RSACONFERENCE EUROPE 2012
Overview of FirstLine Program

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://channel EMC.corp.emc.com/Firstline

Some impersonators are easy to spot.
Others are not.

You may be internet-savvy, but it takes 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.

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

Here are some ways to strengthen your password:

- Use capital letters
- Use symbols in place of letters
- Use a lowercase letter with a number
- Try random numbers and symbols

Sample password: J@B1tW79!

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

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.

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

For slide 4, see hidden slide.
## Mandatory Information Security Training Requirements

Current training covers six topics in 60 minutes

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

Learn How to Spot an Untrustworthy URL
Which of these are NOT fake URLs for “AnyBank”?

2. https://www.anybank.com/login

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

Dear Phyllis,

We have recently received reports of compromised accounts from some of our customers. In some instances, account numbers appear to have been switched. In order 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 1-800-555-5671.

We apologize for this inconvenience.

Wombank Customer Service

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

[Image of phishing email and gaming interface]
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
Security Training Roadmap

Phase I
- Compliance Driven
- No marketing
- Long Corporate Focused CBT’s

Phase II
- Risk Driven
- Branded & Marketed
- Short CBT’s
- Pulled Content

Phase III
- Just in Time Training

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
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