



wombat[®]
security technologies

5 Reasons Why Your Security Education Program isn't Working (and how to fix it)

February 2015

Presentation Agenda

- 5 Reasons Your Program isn't Working
- 10 Learning Science Principles
- Continuous Training Methodology
- Case Studies



A close-up, grayscale photograph of a hand holding a computer mouse. The hand is positioned on the right side of the frame, with fingers gripping the mouse. The background is a blurred computer keyboard, suggesting a workspace. The overall image has a professional, technical feel.

95% of security
incidents
investigated in
2013 were
attributed to
Human Error

IBM Security Services, 2014 *Cyber
Security Intelligence Index*

5 Reasons Security Awareness Doesn't Work

1. Happens once per year
2. Relies on video or slides
3. Tells the end user what to do but not why
4. Training sessions are longer than 15 minutes
5. Focuses on awareness of threats but not behavior change

Informational not Educational





wombat[®]
security technologies

Keys to Effective Security Training Program

Conceptual and Procedural Knowledge

Conceptual knowledge provides the big picture

Procedural knowledge focuses on specific actions to solve the problem

How to apply this principle:

- Training should always describe why something is a threat before telling the trainee what to do
- Give actionable information. Specific steps they should take to protect themselves.



Serve Small Bites

People learn better when they can focus on small pieces of information.



How to apply this principle:

- Limit the time a lesson takes to 10 minutes or less
- Keep the lesson concepts very simple
- Don't train on all cyber threats at once

Reinforce Lessons

Without frequent feedback and practice, even well-learned abilities go away. Security training should be ongoing, not a one-off.

How to apply this principle:

- Have the users practice concepts immediately after learning them
- Repeat the same lessons throughout the year
- Repetition increases retention



Train in Context

Present lessons in the context which the person is most likely to be attacked.

How to apply this principle:

- Create a situation that users can relate to
 - You're sitting at your desk and an email comes in...
 - You receive an SMS from a number you don't recognize...
- Simulate the user interface when possible



Give Immediate Feedback



“Calling it at the point of foul” creates teachable moments and increases impact.

How to apply this principle:

- After each practice exercise explain why an answer is correct or incorrect to reinforce the lesson.

Let Them Set the Pace



Different baseline knowledge requires a different learning pace

How to apply this principle:

- Web-based training enables trainees to go at their own pace
- Allow users to take the training over and over again

Tell a Story



People remember stories much better than facts and data

How to apply this principle:

- Keep one set of characters in a particular scenario throughout training

Involve Your Students

Being actively involved in learning helps students remember things better.

How to apply this principle:

- Immediately after each lesson give trainees opportunity to practice what they've learned multiple times.
- Use multiple realistic scenarios

Measure Results

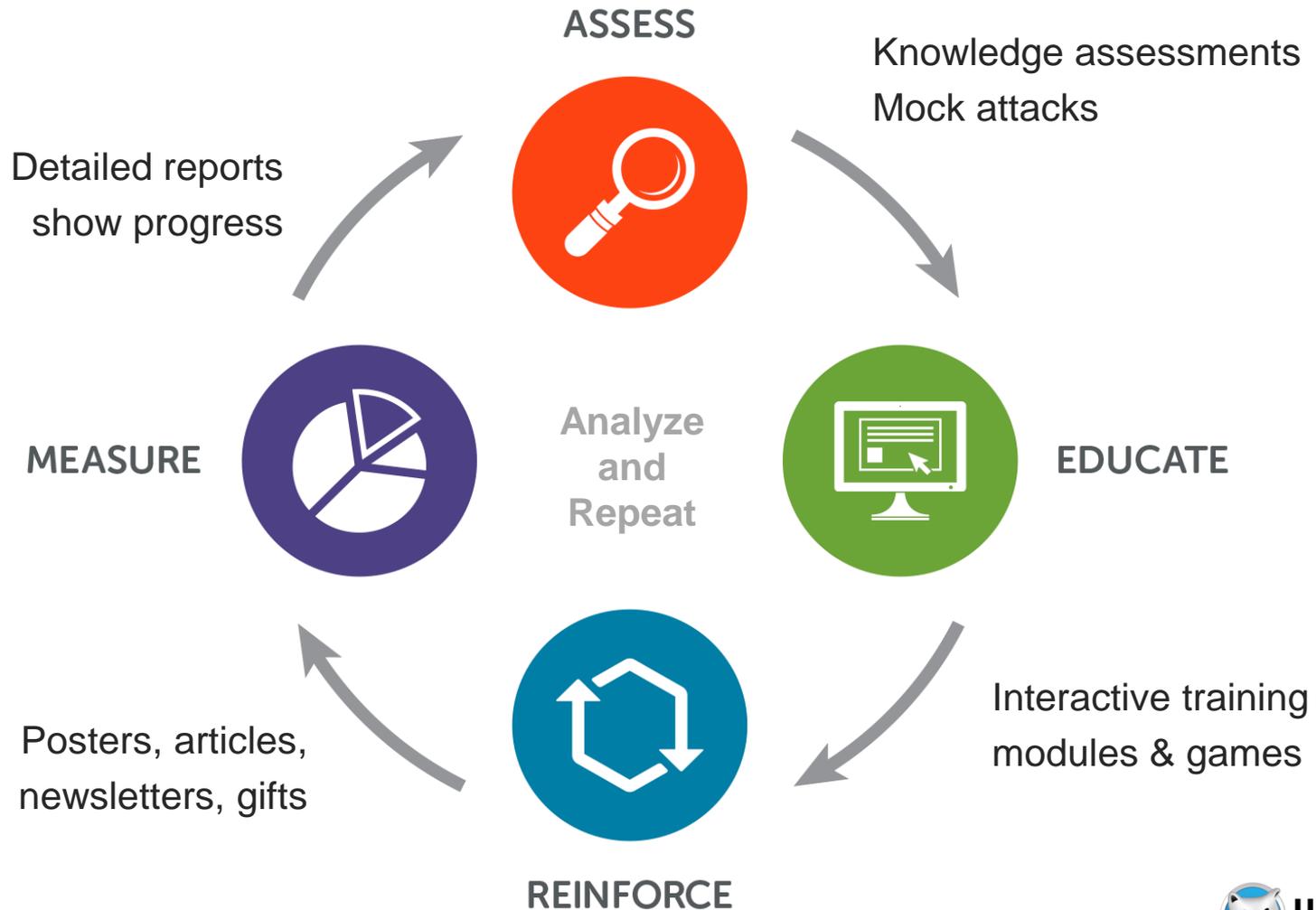


Collecting baseline data, and new data after each training campaign, provides positive reinforcement to trainees

How to apply this principle:

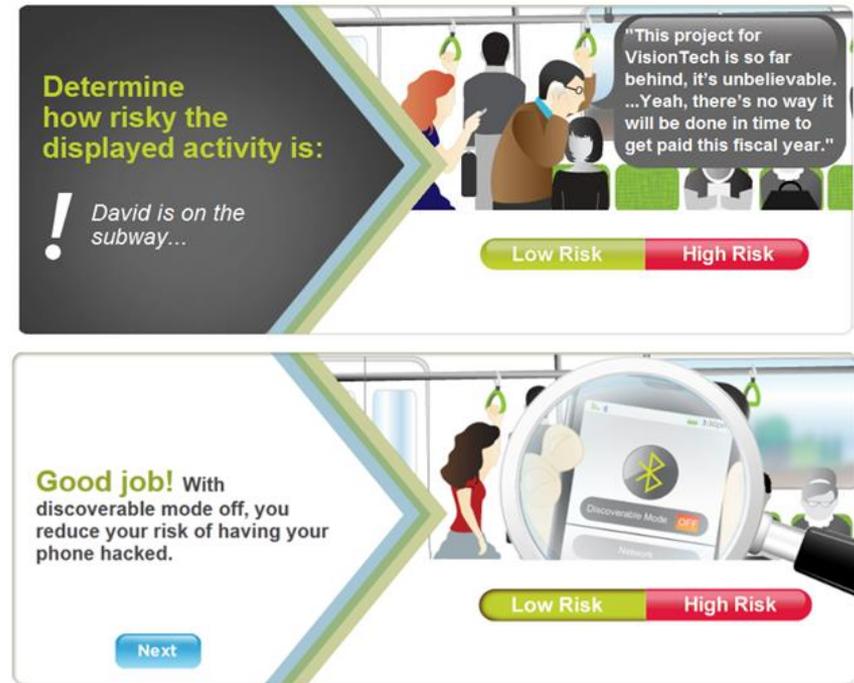
- Ensure that your training program supports more than just collection of completion data
- Perform annual, or more regular, assessments to measure knowledge, not to train

Continuous Training Methodology



Assessments & Mock Attacks

- Assess knowledge and vulnerability
- Gather baseline results
- Intelligence for planning
- Motivate users



From: Lisa Hagendorf <lhagendorf@wombatsecurity.com>
Date: Friday, October 24, 2014 at 1:14 PM
To: Brian Kennedy <bkennedy@wombatsecurity.com>
Subject: Video from the Tech 50 afterparty!

Hey Brian!

Thought you might enjoy this, I took some video at the afterparty Tuesday night and put together a highlight video. Let me know what you think before I tweet it! Check it out [here](#).

Thanks,
Lisa



Leveraging Teachable Moments

- Intervention training
- 30-60 seconds
- Immediate feedback
- Provides context

OH NO!!!
This could have been a malicious link.

Untitled Message - email
File Edit View Insert Format Tools Table Window Help
Hey John!
Thought you might enjoy this. I took some video at the afterparty Tuesday night and put together a highlight video. Let me know what you think before I tweet it! Check it out [here](#).
Thanks,
Lisa

Wombat Mail - email
File Edit View Insert Format Tools Table Window Help
Hey John!
Thought you might enjoy this, I took some video at the afterparty Tuesday night and put together a highlight video. Let me know what you think before I tweet it!
Thanks,
Lisa

This email tried to trick you into clicking on a link by pretending to offer information in your interest.

REMEMBER that anyone can send you an email and pretend to be someone you trust - Your boss, your bank, your friend, your family.

SAFETY TIP:
1- Always hover over a link when you receive an e-mail.
2- Look at the web address to make sure it is actually going where it claims to before you click on it.

<http://upload.videoshares.net/t/1414415413>

In-Depth Education

- Bite-sized education
- Learn by doing
- Stories & scenarios
- Provide immediate feedback
- Collect valuable data

Email Security
Round 2 - Less Obvious Threats

To: Phyllis
From: Bank of North America
Subject: Account Access

Attachments

Bank of North America

Phyllis,

We have seen repeated attempts to access your account from the IP address 128.2.239.54. We will need you to login and verify your account information prior to using your account again. Please login from the link below:

<https://www.bona.com/accountverify/>

Thank you for your prompt attention in resolving this.

Bank of North America Account Services

<http://www.bona.com.accountverify.cn/> Chicago, IL 60606

completed 33%

Next

MVerse Wireless
Purchase
Speak

Phyllis,

We have seen repeated attempts to access your account from the IP address 128.2.239.54. We will need you to login and verify your account information prior to using your account again. Please login from the link below:

<https://www.bona.com/accountverify/>

Thank you for your prompt attention in resolving this.

Bank of North America Account Services

<http://www.bona.com.accountverify.cn/> Chicago, IL 60606

completed 33%

Next

Good job! This link looks legitimate, but it points to a fraudulent site. Mouse over the link to see the actual URL.



Reinforce & Repeat

- Reinforce educational messages & imagery
- Review results
- Repeat and refine

Be Smart About Sharing on Social Networks



Hackers and scammers use social networks to try to harm you

Stay safe with these best practices

- Do not accept connections from people you don't know
- Be cautious of any odd emails or posts; they could be from a hacked account
- Never download software or files from links on social networks
- Assume all your posts are public; think before you share

©2008 Wombat Security Technologies, Inc. All rights reserved.



Browsing Smart = Browsing Safe

Don't rely on your browser to protect you



Your browser **can't stop you** from visiting a dangerous site or downloading malicious software.

Surf smart to stay safe!

Remember these best practices:

- Do not click links or downloads in pop-up windows
- Avoid the lure of free content — there's almost always a catch
- Be cautious of shortened URLs
- Turn off "Auto Complete" and "Remember Me" features

©2008 Wombat Security Technologies, Inc. All rights reserved.





wombat[®]
security technologies

Results that Prove out the Model

Case Study: Manufacturing Company

International manufacturer had phishing emails infecting machines despite strict email authentication program

Baseline Data

- More than 70 malware infections/day worldwide
- Average of 32 calls a month related to spyware, virus, and malware concerns

Manufacturing Company Goals

- Increase awareness of phishing attacks
- Reduce the number of malware infections
- Prove to the board that security awareness and training could achieve these results

“Any company that is not taking awareness seriously is hedging its bets. In my opinion, the single most important thing an organization can do is create a security awareness program.”



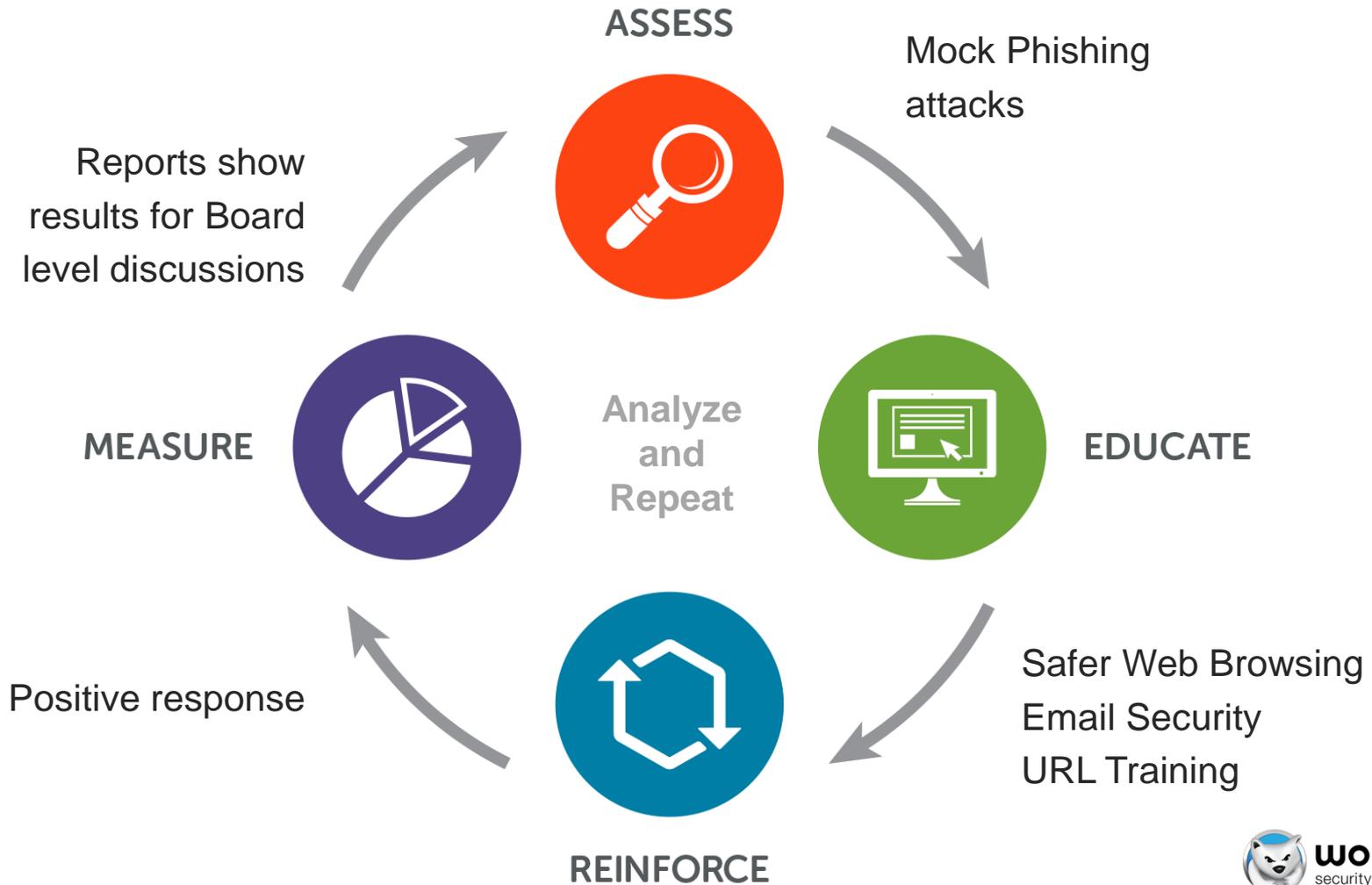
Manufacturing Company Education Program

- 5000 employees in countries around the world
- Voluntary training -- Safer Web Browsing, Email Security, and URL Training
- Mock phishing attacks using Random Scheduling

“I think the reason we’re getting such great support from our Board is because we’re able to show results on the things we’re doing, but the potential for cost reductions isn’t really the driver here. To me, it’s rooted in awareness. I feel this kind of work is essential to a secure work environment, and the Board concurs with that.”



Manufacturing Company Methodology



Manufacturing Company Results

- 46% reduction in malware infections from 72 per day to 39 per day (Europe 69% reduction)
- 40% reduction in help desk calls from 32 to 20 per month
- More than 700% return on investment based on cost to remediate infections
- Positive user feedback on the interactive nature of the training modules



Future Program Enhancement

- Move to mandatory training
- 4-6 additional training modules
- Targeted phishing to particular departments
- Broad knowledge assessments

“We’ve developed a healthy sense of paranoia throughout the organization. I think that’s the best result that can come out of the awareness training we’re doing.”



Conclusions

- Using the right approach end users can learn secure behaviors
- Continuous training methodology yields significant results to your bottom line
- There's more than one way to achieve positive results if you have the right ingredients
- Increase awareness of security issues with employees, executives and your Board
- Education can reduce overall organization risk





wombat[®]
security technologies

Wombat Security is a Leader in the NEW Gartner Magic Quadrant for Security Awareness Computer-Based Training (CBT) Vendors. Access the full Magic Quadrant report here:

<http://info.wombatsecurity.com/wombat-named-a-leader>