Users: Your First Line of Defense

Ari Elias-Bachrach
Defensium llc

May 2014

About Me

• Application Security nerd, training instructor
• Former pen tester
• Former infosec engineer
• Wanted to increase my impact on security
• Make CBTs
• Trainer
• Develop e-learning classes
This Talk Will Cover Effective Training For Non-Security Personnel

Why We Do Training

How To Give Advice

Make Training Relevant

Use Social Psychology

Users: Your First Line Of Defense
Why We Do Training

Users: Your First Line Of Defense
Attacking Are Targeting End Users More

Technical Problems Have Technical Solutions.
Non-Technical Problems Have non-Technical Solutions.
Training Works

Source: Threatsim, 2013 State of the Phish
Training Works

Source: 2013 Verizon Data Breach Investigations Report
How To Give Advice
Give Positive Advice.
Instead of telling people what NOT to do, tell them what to do

No Running
In the House!

In The House
We Walk
The Security Industry Gives Advice Mostly in the Negative Form

Don't click the link
1,500,000 results

Report a phishing email
54,400 results
The Security Industry Gives Advice Mostly in the Negative Form

Cross Site Scripting
2,710,000 results

Output Encoding
110,000 results
Give Positive Advice

Common security advice:
- Don't click the link
- Don't use “product”
- Don't use easily guessable passwords
- Don't have any of these vulnerabilities
Give Positive Advice

Good security advice:
- When you get a phishing email....
- use “other product”
- To make a good password...
- Code in the following way....
Users: Your First Line Of Defense

Training Needs to be Relevant
Pick Your Topics Based on Real Needs

What causes our IT incidents here?
➢ Phishing attacks?
➢ SQL injection?
➢ Viruses coming in through sneakernet?
➢ Loss/theft of laptops and smartphones?
Training Needs to be Relevant

Don't Rely on Gimmicks – Focus on Concrete Things People See
Training Needs to be Relevant
Don't Rely on Gimmicks – Focus on Concrete Things People See
Training Needs to be Relevant
Don't Rely on Gimmicks – Focus on Concrete Things People See

- Get to work and hold door open for “coworker” at 8:00
- Discuss work over lunch in restaurant at 12:00
- Write some code for a new web application
- Get an email from the helpdesk with instructions to fill out a form at 2:00
- Go home. Leave desk unlocked at 5:00
Do Not Teach Them The Language of Security, We Need to Speak Their Language

Dictionary of Information Security

256 pages

Users: Your First Line Of Defense

lattice model: security model for information flow control in a system, based on the lattice that is formed by the security levels in a system and their partial ordering, possibly by subject or content. A simple example might be a grid with levels of security (management, internal, public) and different topic areas (customer data, research data, payroll). A manager in accounting would need to have management level access to payroll data, but would not necessarily need more than public access to research data.

Layer 2 Tunneling Protocol (L2TP): Internet client-server protocol that combines aspects of PPTP (Point-to-Point Tunneling Protocol) and L2F (Layer 2 Forwarding) and supports tunneling of PPP (Point-to-Point Protocol) over an IP network or over frame relay or other switched network. It is a type of virtual private network. PPP can in turn encapsulate any OSI layer 2 protocol. Thus, L2TP does not specify security services it depends on protocols layered above and below it to provide any needed security.

leapfrog attack: use of information, access, or resources obtained illicitly from one host to compromise another host. Also, the act of connecting through one or more hosts to confuse a trace.

least privilege: principle that requires that each subject be granted the most restrictive set of privileges needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.
Do Not Teach Them The Language of Security, We Need to Speak Their Language

Vulnerability
- SQL Injection
- Confidentiality
- AES Encrypted

Bug
- Prepared Statement
- Eavesdrop
- Protected
Use Social Psychology – There are Six Factors of Influence

1) Reciprocity
2) Commitment
3) Social Proof
4) Liking
5) Authority
6) Scarcity
Reciprocity – A Person Feels Like They're Repaying A Favor
Commitment – Once Committed to a Position, People Stick to it

Source: Yes: 50 Scientifically Proven Ways to Be Persuasive, Noah J Goldstein
Commitment – Once Committed to a Position, People Stick to it

Click-through doesn't do much
If you can get people to read and sign a physical document, especially in a group, they're publicly supporting the position.

Mobile Location Analytics
Code of Conduct

Preamble
Mobile Location Analytics (MLA) provides technological solutions for retailers by developing aggregate reports used to reduce waiting times at check-out, to optimize store layouts and to understand consumer shopping patterns. The reports are generated by recognizing the Wi-Fi or Bluetooth MAC addresses of cellphones as they interact with store Wi-Fi networks.

Given the potential benefits that Mobile Location Analytics may provide to businesses and consumers, it is important that these practices are subject to privacy controls and are used responsibly to improve the consumer shopping experience. This Code puts such data protection standards in place by requiring transparency and choice for Mobile Location Analytics.

Who is Covered
This Code is intended to provide an enforceable, self-regulatory framework for the services provided in the US to retailers by Mobile Location Analytics ("MLA") companies.

I. Principle One: Notice
MLA Companies shall provide consumers with privacy notices that are clear, short, and standardized to enable comprehension and comparison of privacy practices.

a. MLA Company Privacy Notice
MLA Companies shall take reasonable steps to require that companies using their technology display, in a conspicuous location, signage that informs consumers about the collection and use of MLA Data at that location. Such steps shall include preposing standard or model contract language, providing companies with model language for in-store signage, developing a standardized symbol or icon to be included with such signage, and using other reasonable efforts to promote the use of in-store signage.
Commitment – Once Committed to a Position, People Stick to it

Do you think that the security of our data is important? Why?
Commitment – Asking Questions Can Force a Person To Commit to a Position

Compare these 3 options

If you get a phishing email, please call the help desk.

The next time you get a phishing email, will you call the service desk?

The next time you get a phishing email, what will you do?
Liking – People are More Likely To Be Influenced By People They Like

People like people who:
• Look like them
• Are Attractive
• Make them feel good (compliments, etc.)

Not really possible for infosec to use this right? :-}
One Way to Make A Department More Likeable is To Humanize it.
One Way to Make A Department More Likeable is To Humanize it.

Who should this email be sent from?

1) The IT Security department
2) A person
People do what they perceive everyone else to be doing.
Social Proof – Do What Everyone Else is Doing

These Statements are actually detrimental!

“Last year our company had 237 incidents caused by people using weak passwords.”

“Last year our company had 37 incidents caused by people clicking on links in phishing emails”
Social Proof – Do What Everyone Else is Doing

These are much better

“In a company audit, we found that 95% of our employees are using strong passwords.”

“Last year we received 25,000 phishing emails, of which 99% were caught by the spam filter or ignored by the recipients.”
Nurses were told to:
• Via an order over the phone
• Administer an unauthorized drug
• Above the maximum dosage
• From a Doctor they'd never heard of

95% did as they were told

Source: Rusch, Jonathan. The "Social Engineering" of Internet Fraud
Authority – Some People's Positions Are Influential

Who is an authority where you work?

- Manager
- VP
- CEO
- IT Department
Scarcity – People Are More Likely To Want Something Perceived as Scarce

While supplies last!

Act now!

This offer ends soon!

Sale ends...
Conclusion

Why We Do Training

How To Give Advice

Make Training Relevant

Use Social Psychology
Further Reading

To Sell is Human
Dan Pink

Predictable Irrational
Dan Ariely

Influence
Robert Chialdini
CSRF: Not All Defenses Are Created Equal

Ari Elias-Bachrach

ari@defensium.com
@angelofsecurity

Defensium llc
http://www.defensium.com