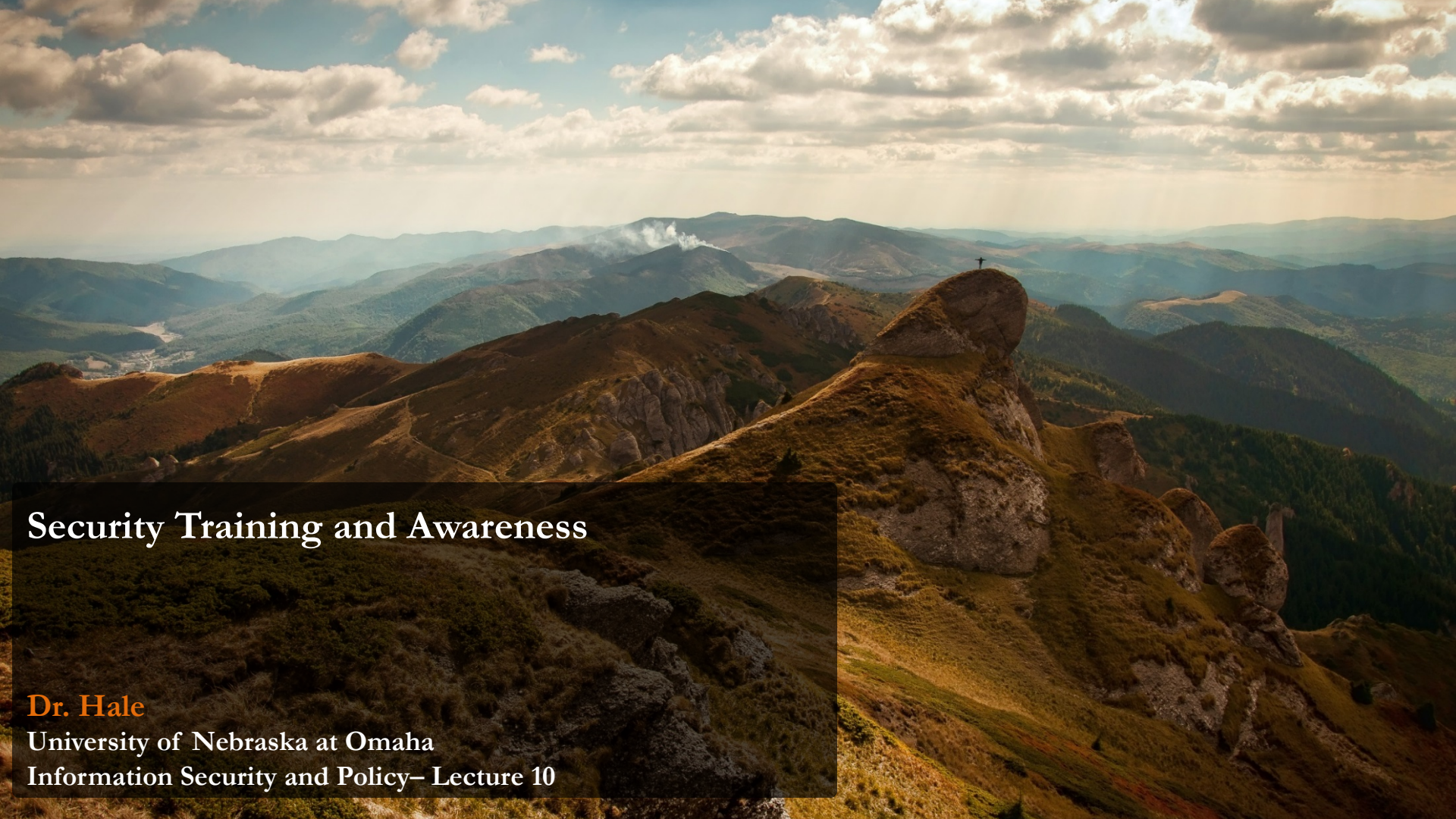


Security Training and Awareness

Dr. Hale
University of Nebraska at Omaha
Information Security and Policy– Lecture 10

Today's topics:

- Social Engineering
- Phishing

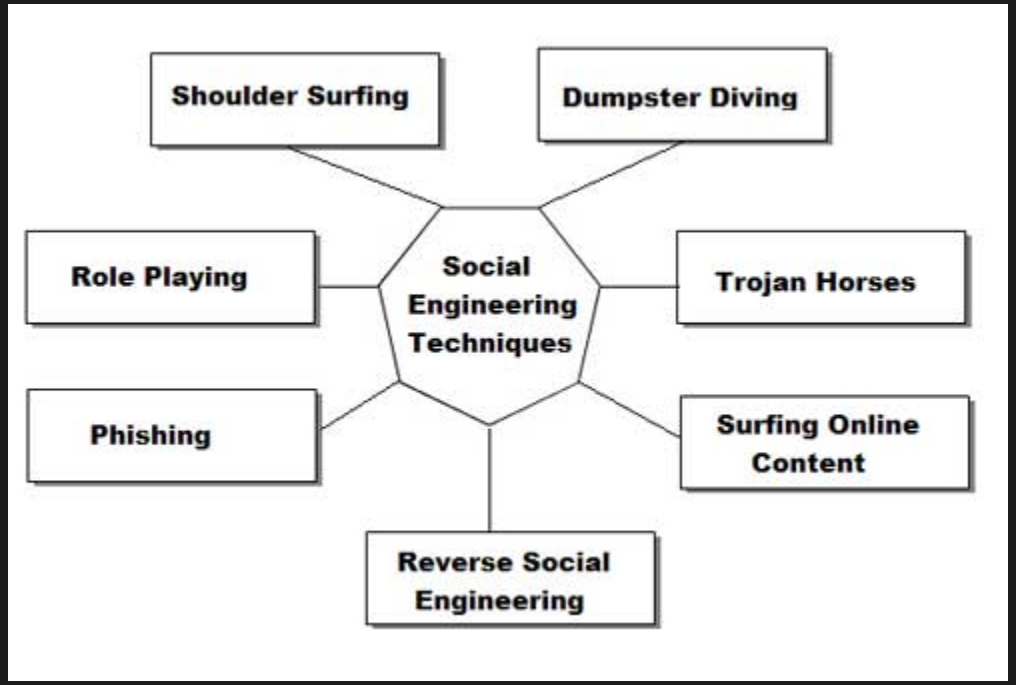
Security Training and Awareness

Security Policy is only as strong as the people who follow it.

Its (arguably) hardwired into the human psyche to want to help others and be social.

Social Engineering is a process that exploits brain chemistry and societal/cultural norms to build trust that is (often) then used for nefarious purposes.

Weapons of a Social Engineer



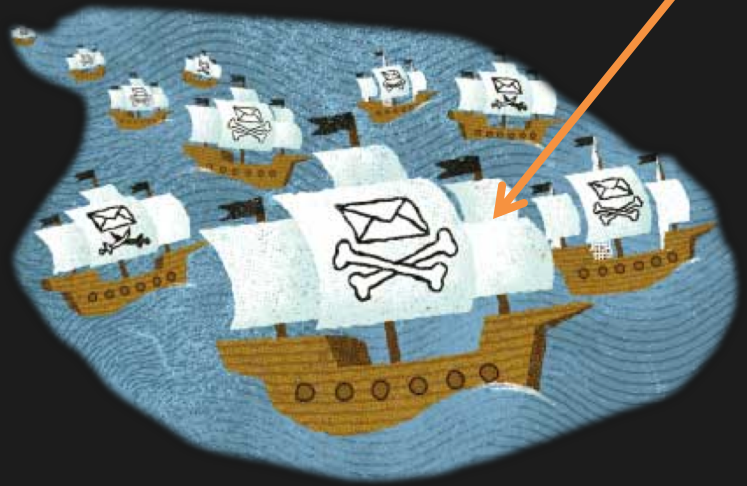
Social Engineering

Phishing is the most popular form of social engineering.

Lets start with some facts.

Actual Facts

ARRRRRRR



164 Million

Phishing Emails

(Every Day)

(60 Billion Yearly)

Actual Facts

147.5 Million

Crash and burn at spam filters

ARRun it's the googles

But that means…

Actual Facts

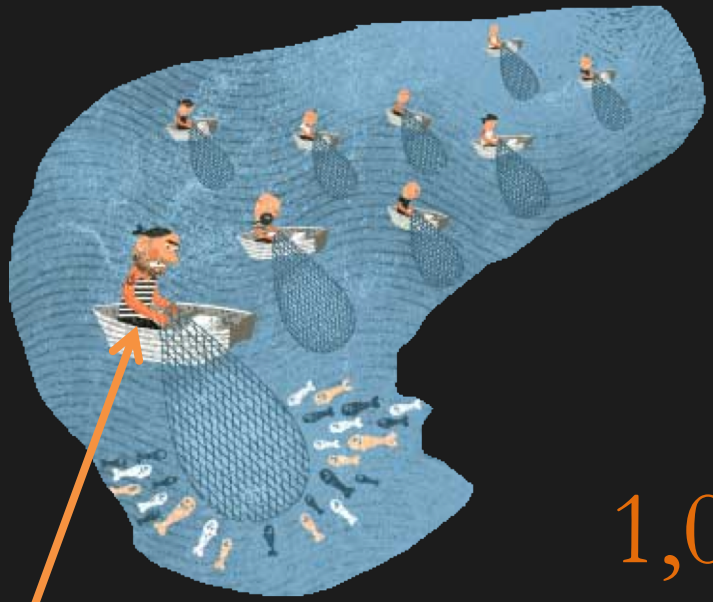
CHARRRRRRRGE

16.5 Million
(6 Billion Yearly)
Make it through Filters

and…

8.2 Million (3B)
are actually opened

Actual Facts



1,000,000 (356M)

(about 10%)

Links are clicked

I have you now

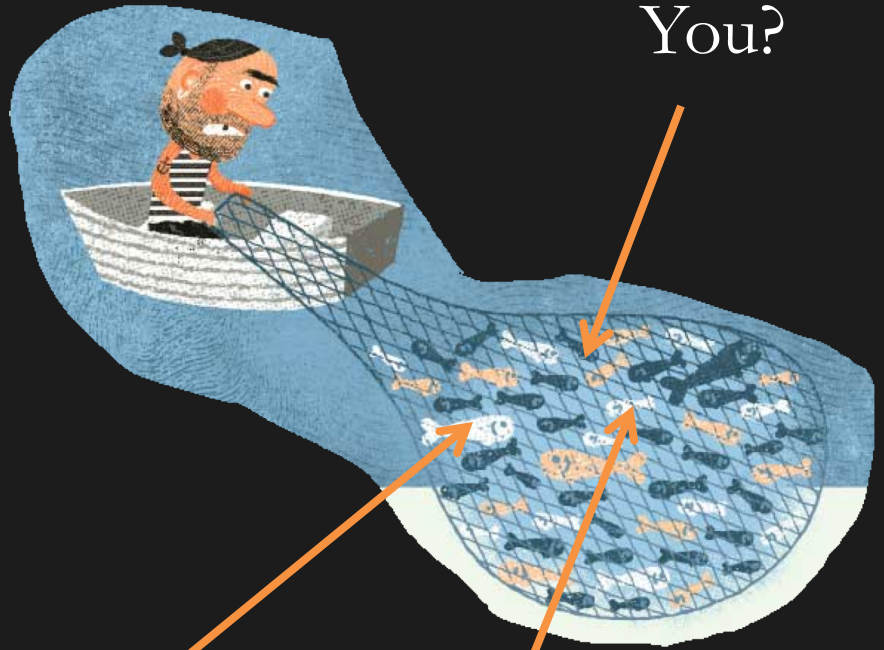
Increasing complexity, i.e. spear phishing or whale phishing…

Actual Facts

100,000 (28M)

(10%)

Fall for a scam and/or share their personal info.



Awesome Pirate graphics courtesy Canadian PSA (numbers updated to latest stats):
http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

We will come back to phishing prevention

For now – Lets look at social engineering in general and the tools of the trade

Social Engineering Lifecycle

Four main phases

- Footprinting
  - target and environment info
  - organizational chart, etc
- Establish trust
  - develop relationship with the target
- Manipulation
  - extract info from target
- Exiting
  - get away without drawing attention

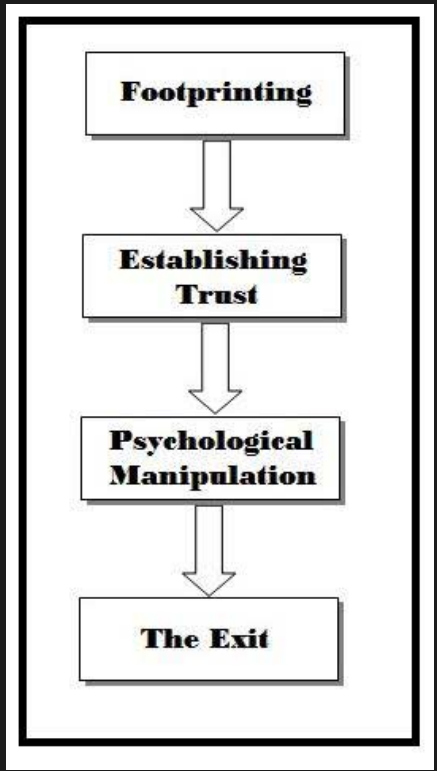


image: http://securityxploded.com/social-engineering-the-human-factor.php#Introduction

Best Pop-culture reference for Social Engineering:
House of Cards Gavin Orsey Sub-plot
(Kevin Spacey is apparently awful),
but this still great example of SE.

Social Engineering Lifecycle: Footprinting

Social Engineering Lifecycle: Establish Trust

Lisa Williams

Social Engineering Lifecycle: Manipulation

Social Engineering Lifecycle: Exit

Then again, its not hard to beat Hollywood realism

Social Engineering

Why it wasn't awful

https://twitter.com/GreggHoush

Social Engineering

Back to the point…

Human Behavior

Many reasons SE works

- Excitement of victory or gain (“you won 1 million dollars)
- Fear of Authority (earlier today)
- Desire to be helpful
- Fear of loss (also today)
- Laziness
- Ego
- Lack of Knowledge

image: http://securityxploded.com/social-engineering-the-human-factor.php#Introduction

implementing policy and avoiding social engineering requires two things:

- Awareness (what bad things can happen) and
- Training (how can I avoid said bad things)

Encouraging Awareness

- Raising awareness can improve compliance without training
  - e.g. "Click it or Ticket"
- In info. sec. there are many topics that fit well into awareness sessions:
  - implications of policy non-compliance (e.g. penalties)
  - web usage
  - shoulder surfing, tailgating
  - phishing attempts
  - pyramid schemes, etc
- Just knowing they exist makes users more wary and (hopefully) less prone to falling for attacks or violating policy

How to encourage awareness?

- Email advisories / adverts / posters
- Periodicals
- Conferences, seminars, courses
- Word of mouth
- New recruit orientations
- Active training (a big area of my research, we will come back to it)

Training

- More active than awareness
- Requires users to have some buy-in to be successful
  - users need to think it is relevant to them
  - shouldn't be too boring
  - should be just the right balance of in-depth and high level

How to train?

- Web-based videos / quizzes / role play scenarios
- Live role play
- Un-announced penetration testing and subsequent lessons-learned
- Onsite instructor training
- Interactive systems

Need to know what people need to know

- Its good to do a needs assessment to understand how well versed people are on [insert topic] (e.g. SE attacks or policy)
- Identify gaps in knowledge and target awareness and training efforts there
- Also good to measure how well the awareness/training program is working
  - How many people have attended awareness seminars? Gone through training?
  - Random polls
  - etc

Prioritize

Just like other info. sec. and risk mgmt. target biggest threats first

NIST(yes I know you probably hate this word) Support

- The 800-50 is a great resource for thinking about awareness and training
- Has sample awareness topics
- Has sample needs assessment questionnaires
- Has sample awareness and training metrics
- Good strategies for A & T

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

NIST(yes I know you probably hate this word) Support

needs assessment questionnaire

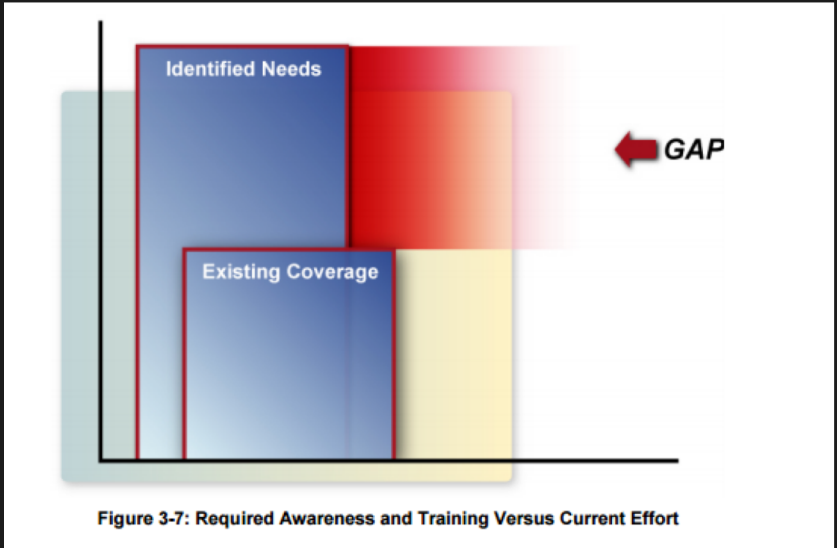


Figure 3-7: Required Awareness and Training Versus Current Effort

APPENDIX A—SAMPLE NEEDS ASSESSMENT INTERVIEW AND QUESTIONNAIRE

Current Assignment (Agency/Office): _____

Parent Organization (Department/Agency): _____

Rank or Grade: _____ **Date of Current Assignment** (mm/yy): _____

JobTitle: _____

This questionnaire is designed to find out about the knowledge, skills, and experience you use to administer your organization's automated information systems and networks. It asks about functions you perform, how you learned to do them, and the kinds of training you think would be of greatest benefit to you on the job. The information you provide will be used to design security training to meet the needs of (agency name) system administrators. The questionnaire should take you approximately 30 minutes to complete.

Part 1. Background:

1. Do you currently perform duties as a system administrator? ..... **Yes** **No**
   1a. If yes, do you do the job on a full-time basis? ..... **Yes** **No**
   1b. If less than full time, what percent of time do you spend doing system administration duties? ..... _____%
2. How long have you worked as a system administrator? _____ **Years** _____ **Months**
3. Do you have system administrators working for you? ..... **Yes** **No**
4. Do you work for a system administrator? ..... **Yes** **No**
5. Did you have formal training in system administration? ..... **Yes** **No**
   (If Yes, please specify below)

   _____ _____ _____
   (School or Vendor) Course Title/Name (Duration- Days) (Year)

   _____ _____ _____
   (School or Vendor) Course Title/Name (Duration- Days) (Year)

6. Did you have formal training in system security? (If Yes, please specify below)... **Yes** **No**

   _____ _____ _____
   (School or Vendor) Course Title/Name (Duration- Days) (Year)

   _____ _____ _____
   (School or Vendor) Course Title/Name (Duration- Days) (Year)

7. Please indicate the number of years of formal education you have completed. (e.g., HS =12 years, BA/BS= 16 years): _____
8. How many seminars or conferences relating to system administration or information systems security have you attended in the last year? _____
9. Do you regularly read computer/networking/software journals or magazines? (If yes, please specify below)..... **Yes** **No**

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Security Training

NIST(yes I know you probably hate this word) Support

….and hilarious (cringe worthy) example posters

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Security Training

Homework and Next Time

Social Engineering Toolkit lab

+

Read (i.e. glance) at the NIST 800-50

http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_