Hacking your Mind and Emotions

A Digression on Social Engineering

Branson Matheson

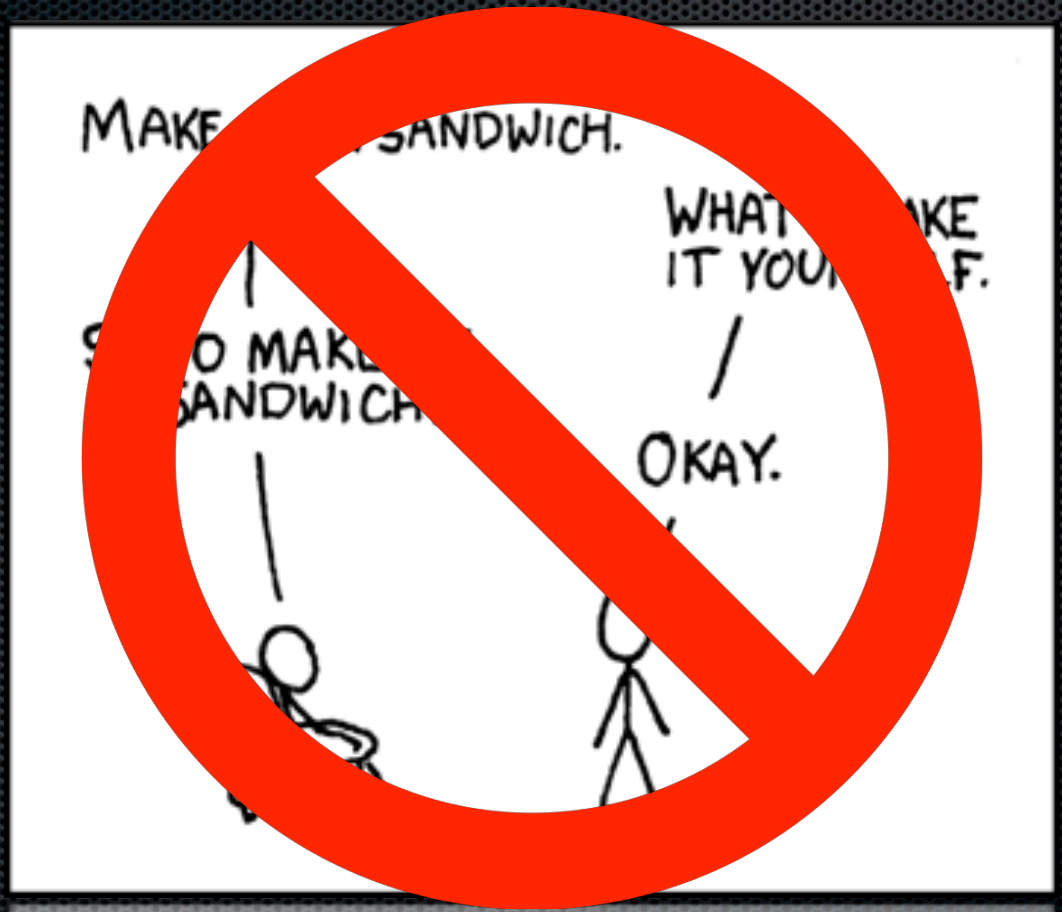
branson@sandsite.org

sandinak

- 26 Year Veteran of IT
  - Security and Systems Architect
  - Security Auditor and Penetration Tester
  - Teacher and frequent Speaker
  - Business Owner
  - Hacker of many hats
  - Geek

This presentation is not ..

A magical formula to make someone to give you Administrative Access



http://xkcd.com/149/

A step by step instruction manual for brain washing someone...

I am Elme[illegible]illionaire ..
I own a mansion and a yacht..

This presentation is..

Going to show you how people are routinely SE'd every day.

Going to raise your awareness of Social Engineering techniques

Going to give you some tools and ideas to use to defend against Social Engineering (SE) attacks.

Tour

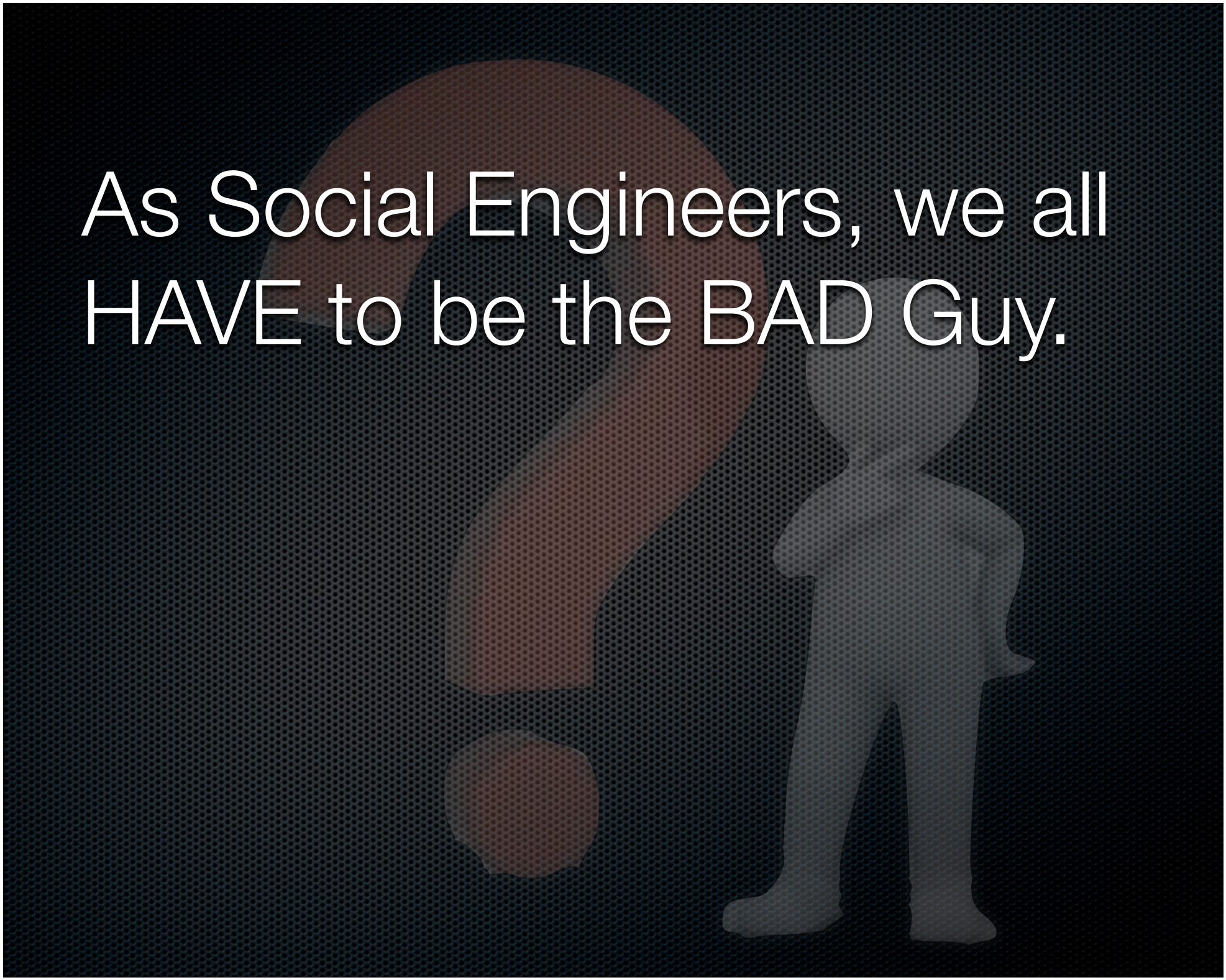
- Definitions
- SE Basics and Explanations
- A walk through
- Some examples
- Defense

Who are you?

Good guys?

Bad Guys?

As Social Engineers, we all HAVE to be the BAD Guy.



Deception

Con Artist

Con Artist

Someone who exploits human characteristics to obtain a goal using:

- greed, dishonesty, vanity
- honesty, compassion, credulity
- irresponsibility, desperation, naiveté

Mark

Mark

In con-artist terms.. this is the target.

Social Engineering

"... defined as the process of deceiving people into giving away access or information."[1]

Obtain a change in behavior that benefits some and/or disadvantages the target.

1: http://www.social-engineer.org/framework/Social_Engineering_Defined

Who social engineers?

Everyone Every Day

But not Everyone can do it maliciously.

Keys to Social Engineering

- think on your feet
- confidence
- understanding limits
- theatrics
- objective

Indications you may not be a good SE

- Cracking a smile when you're trying to discipline someone for something funny.
- Freezing up when confronted
- Appearance is too far outside the profiles of your targets
- Not comfortable play acting

Two major overall types

- Influencing on a large scale
  - societies
  - geological or political entities
- Influencing on a small scale
  - groups and individuals

Large Scale SE

- Government
- Law
- Religion
- War
- Advertising

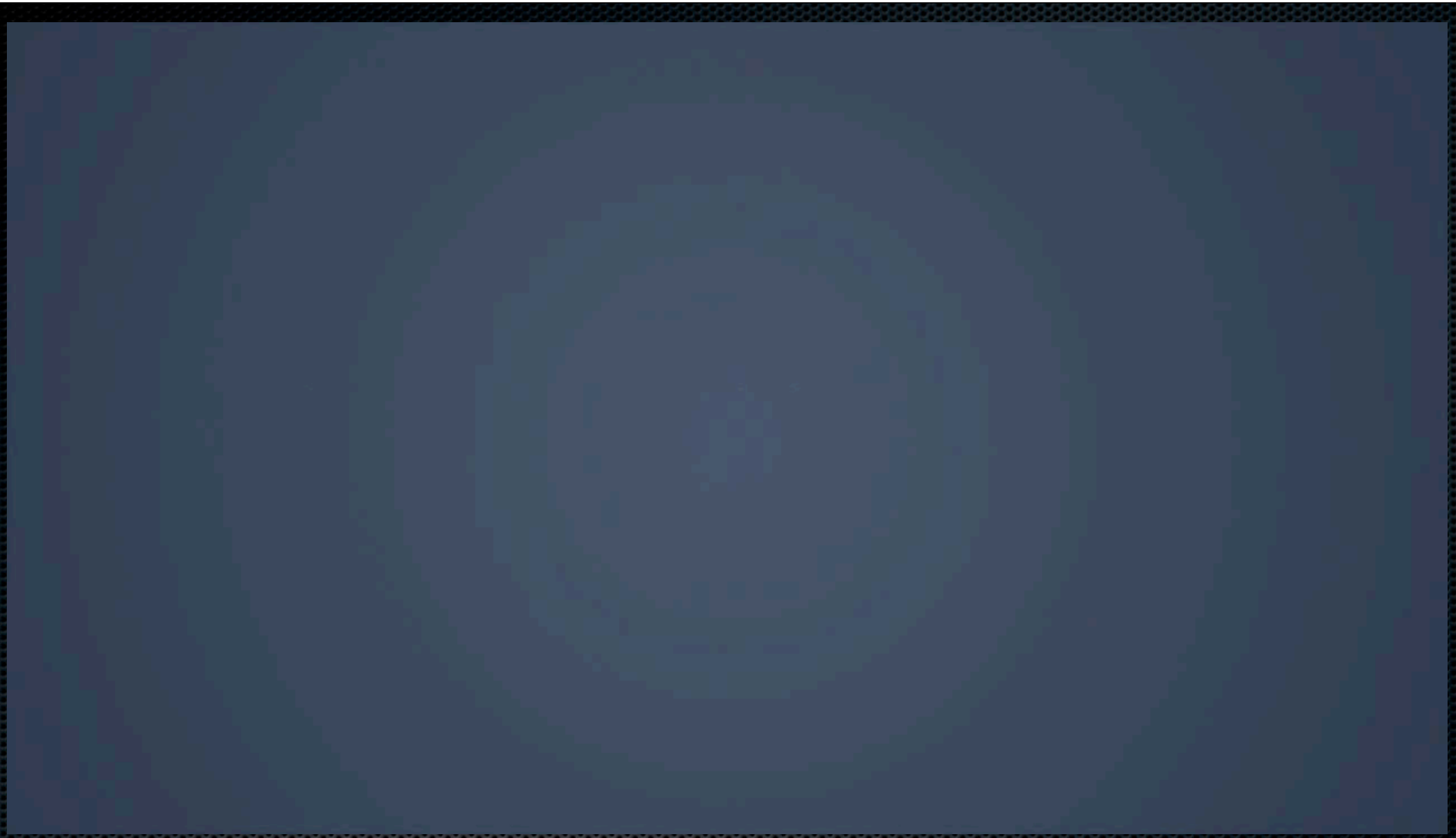
By earning the ideas and precepts of societal SE, we can gain useful insight concerning techniques used by hackers for social engineering.

The basics of SE

- Make the request seem normal, mundane, etc.
- Have a goal in mind
- Must be able to adapt
- Establish a false trust relationship
  - In some cases, this is automatic based on the situation.

Trust - Logical

- Make things appear as the mark expects
- Make a divergence for the mark seem normal
- Using “herd mentality” with groups



Improv Everywhere: Best Buy - YouTube

Implicit Trust

- Make things appear as the mark expects
- Make a divergence for the mark seem normal
- Situation or Location based

TEXT
"I Love IT"
to
XXX XXX XXXX
to win a prize!

SMS for Prizes

- Insert numbers here ;)

Trust - Emotional

- Change emotional state to garner trust
- Know the mark
- Build an environment to improve trust

Trust - Emotional

Lead-ins

- From the same place
- Do the same job
- I’m upset can you help me?
- I know you’re sensitive about XXXXXX

Human Based Methods

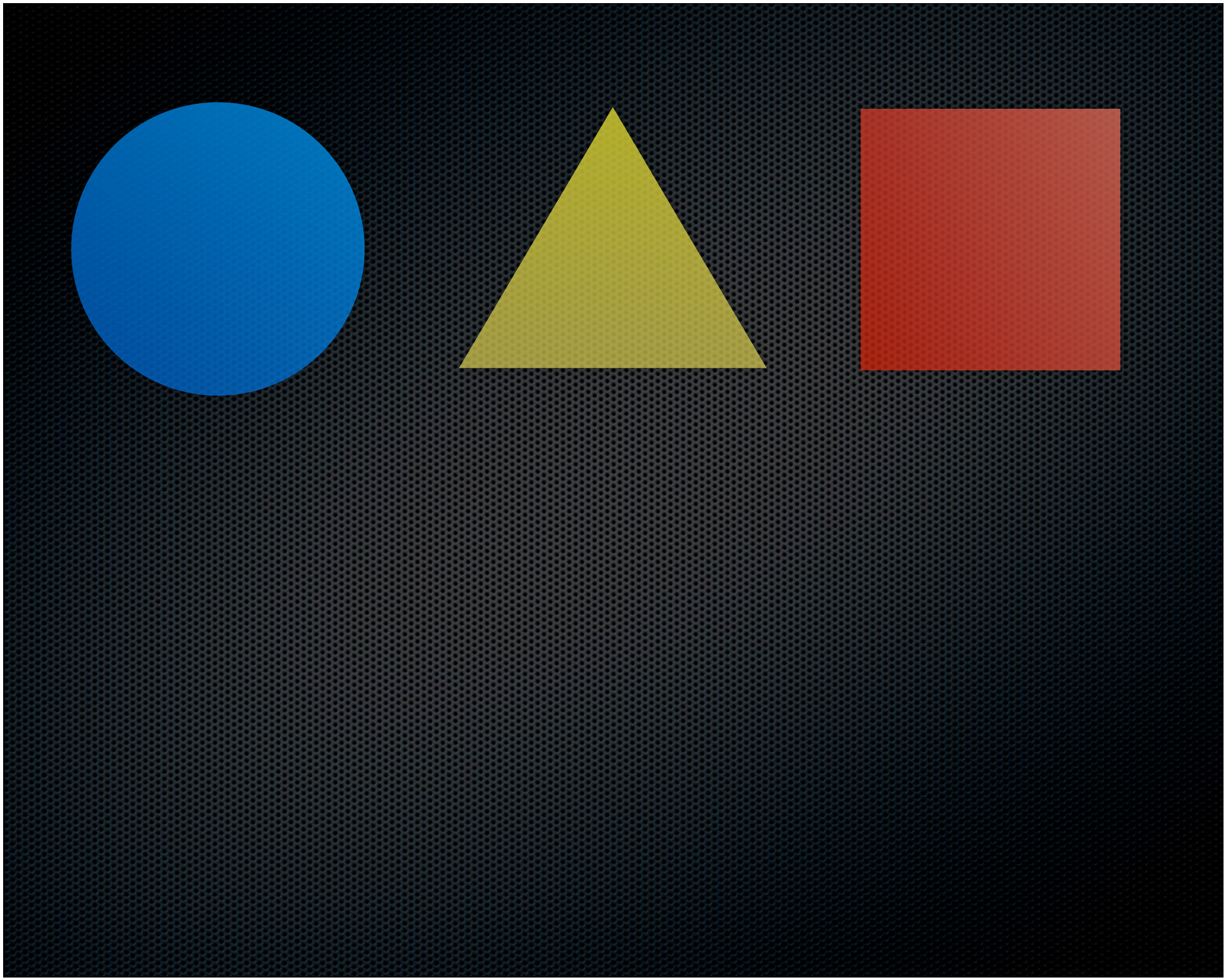
- Diffusion of responsibility
- Chance for ingratiation
- Trust relationship
- Moral duty
- Contrived Situation
- Perceived Requirement
- Personal Persuasion
- Guilt
- Identification
- Desire to be Helpful
- Cooperation
- Time-based pressure
- Psychological Profiling
- Misdirection
- Leading
- Perceived benefit
- Obfuscation of desire
- Fishing
- Distraction

Cool SAP CRM MARKETING Video - Ball Throwers

Day to Day Social Engineers

- They’re all around us, and they encourage us to behavior we normally wouldn’t do.
- Typically use:
  - the power of suggestion
  - herd mentality
  - time-based pressure

Another Example



Computer Based

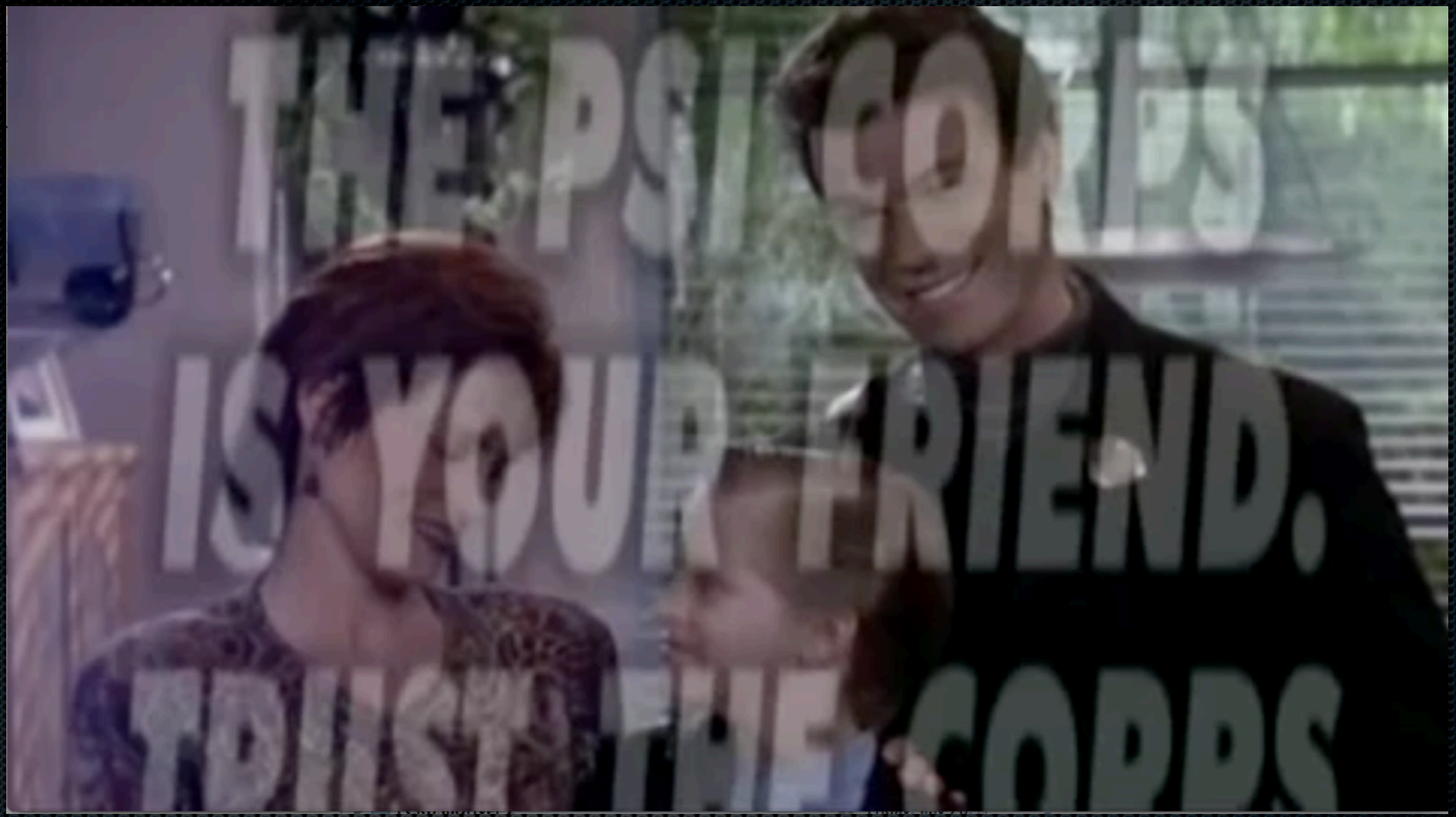
- Phishing
  - Smshing - using an SMS
  - Vishing - using IVR
  - Spear Phishing - individuals
  - Whaling - CEO's
- Baiting
  - CDROM
  - USB Key
- Social Media
  - using Facebook, twitter

Advertisers

Advertisers

- **Objective**: Get you to purchase a product
- **Methods**:
  - *Interruption*: Notice something you'd normally ignore (Raising the volume during commercials)
  - *Identification*: Using movement to garner attention to items you will recognize.
  - *Suggestion*: Triggering a response that you wouldn't ordinarily notice.

The Psi Corp - TV Spot #1 - YouTube


THE PSI CORPS
IS YOUR FRIEND.
TRUST THE CORPS

Businesses

Businesses

- **Objective**: Get you to purchase high dollar items from that store (or chain)
- **Methods**:
  - *Cooperation*: Using buying habits to send targeted ads
  - *Identification*: Monitoring and manipulating shopping patterns in stores

Car Salesmen

Car Salesmen

- **Objective**: Buy the car *today*!
- **Methods**:
  - *Misdirection* - Turning .. If [illegible]es guy is failing, transfer the mark to another
  - *Trust* - GoodCop/BadCop .."let me take this offer to my manager"
  - *Trust/Leading* - using "word tracks" to build rapport with the mark. Can also be used to turn the conversation in a particular direction.

Connection

Who are some of the BEST social engineers?

The wrong way to handle a police stop

Police

- **Objective**: Establish Guilt
- **Methods**:
  - *Fishing* - “You kids going to the concert?”
  - *Leading* - “Do you know why I pulled you over”
  - *Perceived Requirement* - they can search your car without a warrant.

Speed

Speed

- Computer based methods speed data return with enough targets, attackers may get a ‘hit’ easily just based on the numbers.. however...
- The amount of information the mark receives due to more active methods may be enough to recognize a change, and thereby an attack?

Methods

- Attackers have a plan!
  - Build their own scripts to counter your own defense
- Many attackers use Props as they lend credibility.
- Attackers will work hard to fit ‘normal’ as much as possible.

Information

- Attackers will play on trust of existing information sources
  - Caller ID on the phone
  - US Mail
  - “Brand Name” badging

Phone Interaction

- Use Anonymized phone numbers with “valid” Caller ID
- Ask for normal information to look like the pattern
- Exit with grace, suspicion after the fact is just as bad as during with caller id.
- If call starts to go south, will have an ‘out’ that seems plausible

Verbal Interaction

- Social Engineers will turn the conversation away from the point.
- Ask leading, open ended questions
- Leave dangling sentences

Physical Interaction

- Look the part
- Act the part
- Knowledgable
- Affable
- Empathetic

Walk thru SE attack

Walk thru SE attack

- Target Eval
- Target Recon
- Build/Plan your attack
- Perform the attack
- Wash, Rinse and Repeat

Timeline - Choose a Target

- same as network penetration
  - use tools they're used to
  - low-hanging fruit
  - best reward

Timeline - Target Evaluation

- Groups
- Individuals

Target Evaluation - Group

- Research is on the group itself, but can extend to segments which are more advantageous
- Because targeting is broad, and there are more possibilities, likely to get more responses
- Tbe collective information from the group can be more useful as well. (hints from multile sources)
- Makes a nice stepping stone for targeting individuals.

Target Evaluation - Individual

- Tend to require more research as the attack surface is more narrow
- Can be more difficult as while the number of vectors can be large, the actual surface is small.
- Can be more focused and go for more specific information
- Tend to be more advantageous in the end result.

Research - Passive

- Same tools used in penetration testing
  - Maltego
  - Google
  - PIG
  - Phone book
  - Public info (phamplets, location, building.. etc)

Reconnaissance - Active

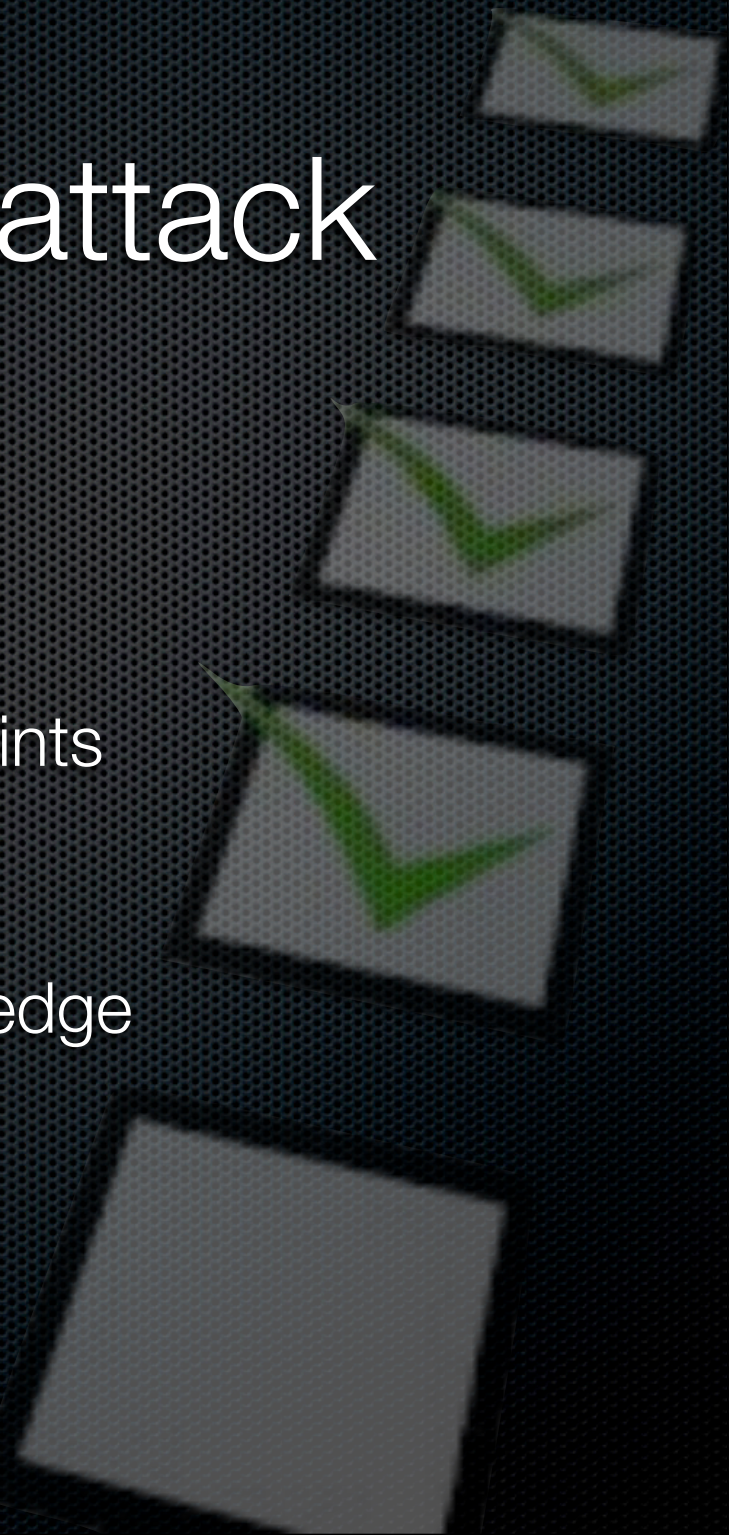
- dumpster diving
- visiting the location(s)
  - And locations close by....
- network tools

Reconnaissance - Social

- fbpwn - download targets profile even if hidden
- cree.py - twitter reconnaissance
- Google Plus -

Build profile(s) for attack

- identify goals
- review information for common points
- look for discrepancies
- search for key phrases and knowledge
- organize the information



Plan the attack

- entry points and conversation starters
- Identify tiers and individuals
- Low Hanging Fruit
- KISS!
- Evaluate impact on the mark

Perform the attack

- keep good logs
- record things (Local Laws may Protect You)

Generally, it is legal to record any conversation where all the parties to it consent (one party consent if all parties are in a state with corresponding law). The U.S. federal law only requires one-party consent to the recording of a telephone conversation, but explicitly does not protect the taping if it is done for a criminal or tortuous purpose. Many states have similar exceptions.[1]

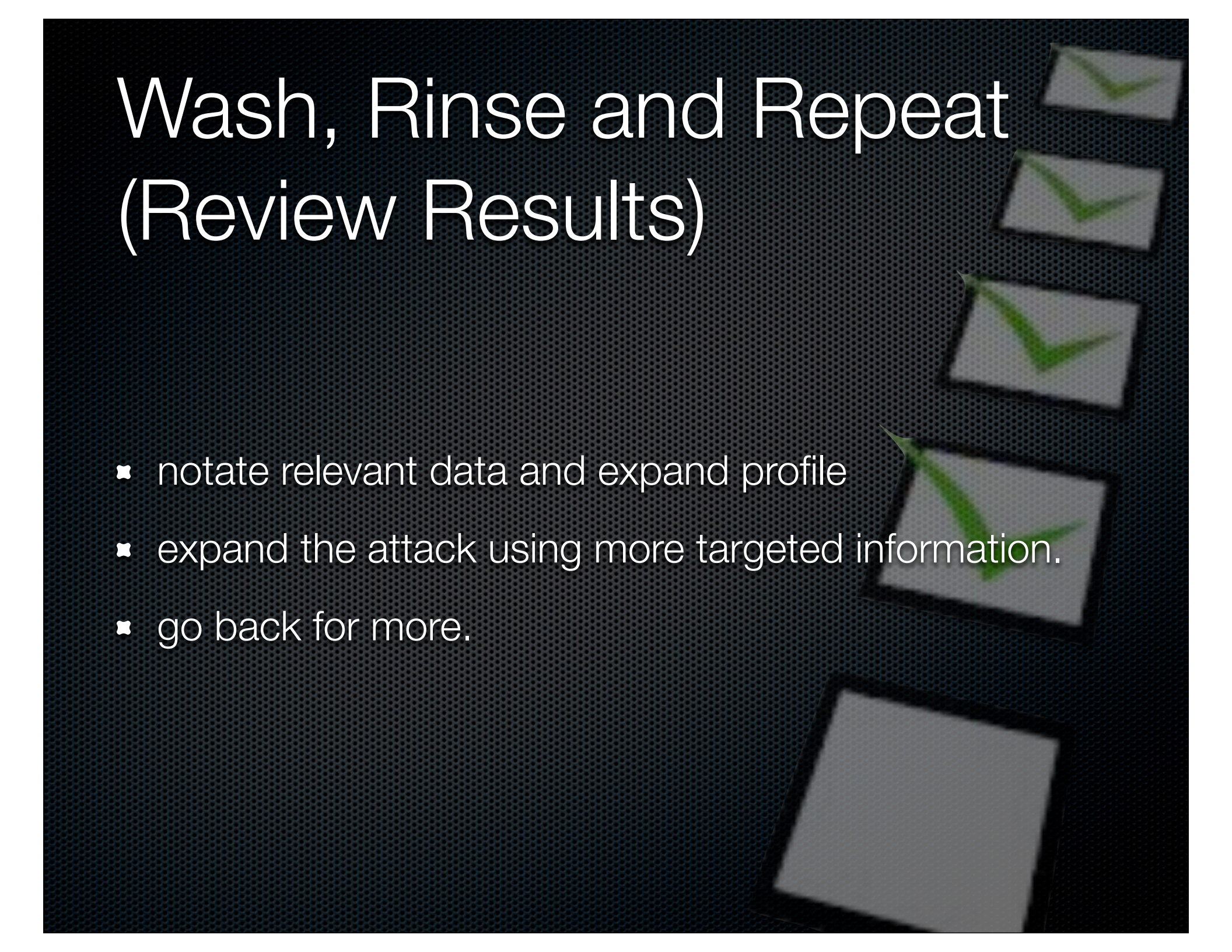
1:http://www.callcorder.com/phone-recording-law.htm

Utah Law

- Utah Code Ann. § 77-23a-4: An individual legally can record or disclose the contents of any wire, oral or electronic communication to which he is a party, or when at least one participant has consented to the recording, unless the person has a criminal or tortious purpose in making the recording.
- Under the statute, consent is not required for the taping of a non-electronic communication uttered by a person who does not have a reasonable expectation of privacy in that communication. See definition of "oral communication," Utah Code Ann. § 77-23a-3.
- Installing a hidden camera or audio recorder to tape a person in a "private place" without consent is a misdemeanor. Utah Code Ann. § 76-9-402. A "private place" is a place where one may reasonably expect to be safe from intrusion or surveillance. Utah Code Ann. § 76-9-401

1: http://www.callrecordingcenter.com/utah-call-recording-law.php

Wash, Rinse and Repeat (Review Results)



- notate relevant data and expand profile
- expand the attack using more targeted information.
- go back for more.

Examples of Successful Social Engineering Attacks

Extracting info with just a last name

Crash a Party

What can we do to prevent Social Engineering Attacks


Strange Behavior?
Conspiracy Nut!
Skeptic
That's an odd request...

Learn to recognize SE

- Think Differently
- Evaluate Information Requests
- Evaluate Information Requestors

Business Defense

Business Defense

- Don’t give out information unless you initiate the call *AND* you know the number is from a reputable source.
- Validate the caller
  - Get the number from a separate source
  - Ask for a call back number

Business Defense - People

- Valdiate the person's credentials
- Validate a person's right to the information or access
- Validate the requirement for the information
- If you have to give written information, ask for copies to retain so you know what's out there.
- Weigh the disclosure against the benefit.

Business - Advertising

- Don’t be a part of the problem. As a business, be reasonable in your approach to advertising.
- Don’t accept or create intrusive adverts where you can make the choice.
- Tout your businesses credentials on sensitive information security.

Business Defense : Awareness

- Know your information profile
- Security Awareness training is a MUST, and should be repeated.
- Have pre-planned scripts for validation of phone information.
- Have reaction plan when a determined attack is discovered.

Business Defense: Active Discussion

- At meetings, talk about what an attack might look like.
- Discuss recent attacks and how they might have applied to your group
- Discuss information leakage.

Personal

Phone Spam

- Turn the tables on them...
  - (I don’t advocate this ... much ;-)

How to handle a telemarketer

Personal - Phone Spam

- Use “phone firewalls” to vette inbound phone numbers
- Answer like a Business

  “Hello, Dominoes Pizza Yorktown, will this be delivery or carry out?”

Personal - Avoid Information Disclosure..

- Know the requirements and/or rights for disclosure
- Simply (politely) refuse to give information.
  - Sometimes this isn't an option
- Deflect the question (politicians are good at this)

Police: how to handle..

- Lets go back and see how this guy handles:
  - Avoiding direct questions
  - Protecting information
  - Controlling the conversation

The Right way to talk to the Police

Individual Defense: Info

- Know your requirements and rights and the rights of others with respect to information.
- Assume everyone's need to know is minimal
- Protect yours and others information zealously.

Individual Defense: Action

- Be aware of your surroundings
- Be critical of information token use
  - Look hard at ATM's and Gas pumps for skimmers
  - Protect RFID tagged things (passport, etc..)
- Be Aware of what you use and how you use it
  - Cell Phones...
  - Keyboards...

Review

- Definitions
- The basics
- A walk through
- Some examples
- Defense

Questions

Branson Matheson

twitter: @sandinak

web: sandsite.org

email: branson@sandsite.org