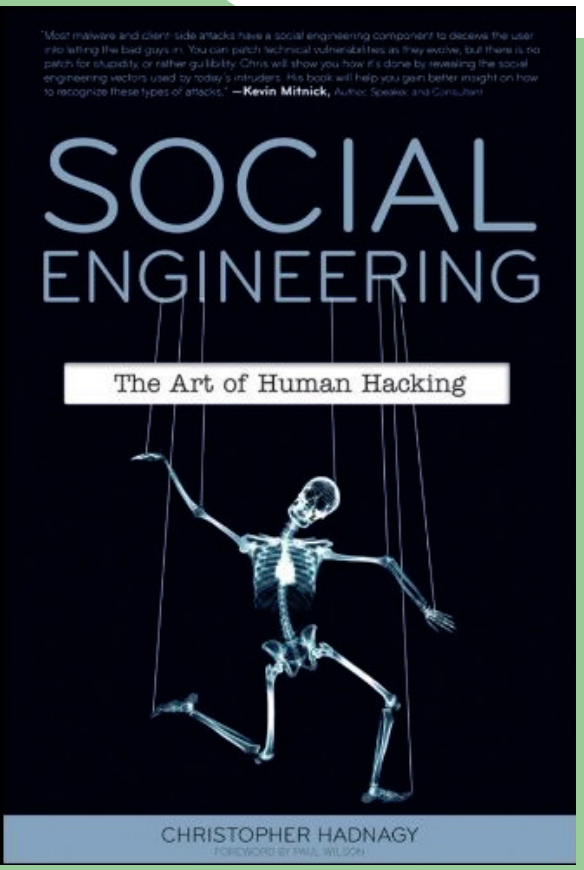
Social Engineering – The Art of Human Hacking



Dr. Fred Mtenzi

What is Social Engineering?

Better overview of Social Engineering

- Social engineering is the art of manipulating people into performing actions or divulging confidential information.
- In other words, making people do things or tell you secret information such as passwords and personal details.
- Social engineering is a component of many, if not most, types of exploits. Virus writers use social engineering tactics to persuade people to run malware-laden email attachments, phishers use social engineering to convince people to divulge sensitive information, and scareware vendors use social engineering to frighten people into running software that is useless at best and dangerous at worst.

Pretexting

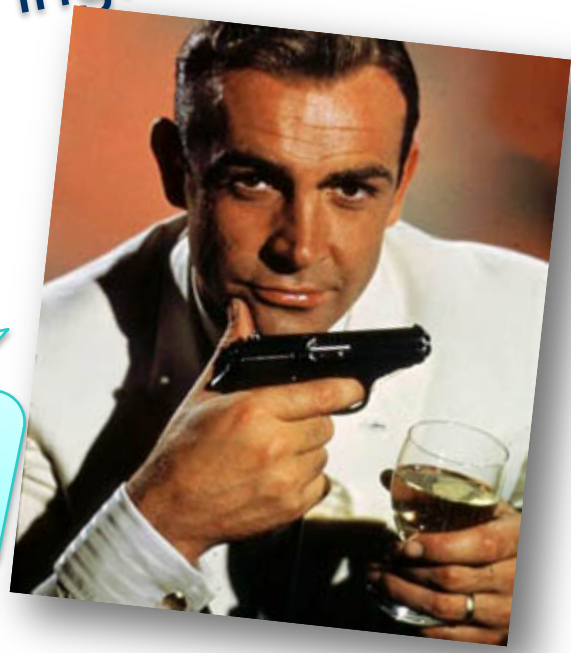
- Pretexting is the act of creating and using an invented scenario (the pretext) to engage a target victim in a manner that increases the chances the victim will divulge sensitive information or perform actions that would be unlikely in ordinary circumstances.

Social What ??

- Trick people in doing something you want (without hacking!)
- E.g.: Trick people into reveal their secrets
- The most secure systems in the world are still vulnerable!

Social Engineering!

Its easier than you think!



●And many more!

Many ways of doing it

- **Pretexting**
  Create a scenario and engage a victim, gain their trust and use it to gain information. E.g.: Impersonate a co-worker, ask about...!
- **Phishing**
  Gain private information by fraud. Typically via e-mail, requesting e.g.: credit card information from the victim.
- **Diversion theft**
  ”Con” a person to deliver their stuff elsewhere than intended. E.g.: Their secret information to you!
- **Baiting**
  “Real world Trojan Horse”. Leave some “infested” media for others to find; USB, CD, DVD, MicroSD, etc. When media is inserted into a PC, “auto-runs” can execute some malware.
- **Quid pro quo** (something for something)
  Call random phone numbers, pretend to be an IT-Supporter, ... Eventually you end up with someone that needs help... Trick them to give you access to their system, so that you might “help” them.

●Source:
●http://en.wikipedia.org/wiki/Social_engineering_%28security%29

Counter measures

- IT-Policies
- User education
- Physical security
- Two-phase (or more) security – defense in depth

The Weakest link

- People are the largest vulnerabilities in any network.
- Social engineering is based on decision making of human being.

Different types:

- Pretexting
- Diversion theft
- Quid pro quo
- Phishing
- Baiting
- IVR or phone phishing

Pretexting

- Created scenario to persuade target to release information
- Research
- Gathering information in advance about victim
- Build the trust
- Rely on personal past experience

Quid pro quo

- From Latin

"what for what"

- Indicates exchanges
- "Something for something"

in social engineering

- Can exchange a password for a pen

In survay, for instance

Phishing

- Method of fraudulently obtaining private information
- E-mail with verification
- Link to the fake web-page which look like real

Baiting

- Leaving some CD/DVD/USB with malicious program where it will be definitely found
- Have name like “salary from the last month”
- Curious employee will run it to see the context
- Access will be given by 3rd parties even without knowing

Summary

- We try to secure our system, to find all the vulnerabilities, to mitigate the risks but

  THE WEAKEST LINK in ANY system is PERSON
- Social engineering is based of human desision making
- There are several types pretexting, phishing, vishing, baithing and so on
- Collecting information about the victim will bring closer to the success

Conclusion

- We should educate people more that they should not easily trust others
- Password should be hard enough and hardly guessible
- No secret question like “mothers surname or pet name” should be ussed
- Check all the time the information which you get, if it is needed to call to the bank, use the phone number you have, not the one which is provided

Background & History (1)

- Trojan Horse
  - Trojan War
    - Greek mythology
    - C. 1200-1300 BCE
    - *Iliad* & *Odyssey* of Homer
    - Virgil's *Aeneid*
  - Greeks sailed to island of Tenedos
    - Pretended to abandon war
    - Left giant hollow horse with soldiers inside
    - Sinon, who convinced Trojans it was offering to Athena
    - Lacoon & Cassandra warned of danger
  - Greeks opened gates from inside, slaughtered Trojans, won war

Background & History (2)

- Definition: *obtaining information or resources using coercion or deceit*
- Manipulate trust or gullibility of people
- Often piece together information
  - Random order
  - Multiple victims / enablers
- Purposes vary but results often loss
  - Intellectual property
  - Money
  - Business advantage
  - Credibility….

Some Notorious Social Engineers

- Frank Abagnale, Jr.
  - See *Catch Me If You Can* movie
  - Impersonated pilot, attorney, teacher…
  - Passed phony checks
  - Became expert for FBI
- Kevin Mitnick
  - Many exploits
  - See earlier lecture on *History of Computer Crime*

Social Engineering Methods

- Impersonation
- Seduction
- Low-Tech Attacks
- Network and Voice Methods
- Reverse Social Engineering

Impersonation

- Criminals wear uniforms, badges, use right terms
- Adopt confident air of entitlement
- Pretending to be HelpDesk employees
  - Employees conditioned to cooperate
  - Technical knowledge reduces questions
  - Some HelpDesks violate standards by habitually asking for passwords (BAD)
- HelpDesk employees can be victims
  - Criminals pretend to be employees
  - Often assume identity of high-ranking executives
  - Sometimes bully HelpDesk staff into violating standard operating procedures

Seduction

- Long-term strategy
  - May study victim to learn background, habits, likes, dislikes, weaknesses
- Form bond with victim
  - Apparent friendship
  - Exploit good will to ask for favors
  - May use sexual relationship as lever to develop trust
- Foot-in-the-door technique especially useful
  - Ask for tiny deviation from standards
  - Gradually increase demands

Low-Tech Attacks

- Exploit physical weaknesses in defenses
- Often support social engineering
- Examples
  - Dumpster® Diving
  - Theft
  - Leveraging Social Settings
  - Exploiting Curiosity or Naïveté
  - Bribery
  - Data Mining & Data Grinding
  - Piggybacking / Tailgating
  - Phishing & Pharming
  - Spim, Spit, & Vishing
  - Trojan Code and Viruses

Dumpster® Diving

- Dumpster® is registered trademark of *Dempster Brothers* for mobile trash receptacles
- Discarded materials are not protected by law unless on private property
- Many organizations sloppily throw away confidential info
  - Papers
  - Magnetic media
- Criminals derive value from
  - Internal organization charts
  - Memoranda
  - Vacation schedules
- Use info for industrial espionage and impersonation

Theft

- Outright theft of confidential information
  - Paper
  - CD-ROMs
  - USB flash drives and disk drives
  - Backups
  - Entire laptop computers
  - Purses, wallets, briefcases
  - Trash bags
- Information used directly or for impersonation

Leveraging Social Settings

- Employees relaxing or traveling may let down guard
- Social engineers may deliberately eavesdrop
  - Company parties
  - Clubs, trains, coffee shops
- Classic errors
  - Talking about confidential matters
    - In public amongst themselves
    - To friendly strangers
    - Loudly on mobile phones
  - Letting strangers view computer screens
  - Leaving portable computers unlocked

Exploiting Curiosity or Naïveté

- Criminals (and researchers) have left media lying around
  - CD-ROMs
  - USB flash drives
  - iPod music players
  - Music CDs
- Victims routinely insert media into company computers
- Unknowingly load malicious software; e.g.,
  - Keyloggers – capture keystrokes and send them to criminals
  - Backdoors – allow criminals to seize control of compromised computer behind firewall

Bribery

- Exchange of value in return for violation of policy
- Dangerous for social engineer
  - Obviously wrong
  - Honest employees (or one with second thoughts) will report attempt to management
  - May lead to police involvement, arrest
- Success depends in part on employee attitude
  - Disgruntled, unhappy employees better
  - Contractors
  - Those about to quit or be fired anyway
  - Criminal may probe for attitudes using negative comments

Data Mining & Data Grinding

- Search engines
  - Reveal confidential information
  - Mine information about organizations
  - Use caches for pages that have been removed
  - Web history for older versions
  - Search-engine APIs provide special tools
  - See references to “Google hacking” using any search engine
- Data grinding
  - Extracting metadata from published docs
  - Unprotected DOC & HTML files may contain valuable info (e.g., author, e-mail address, ….)

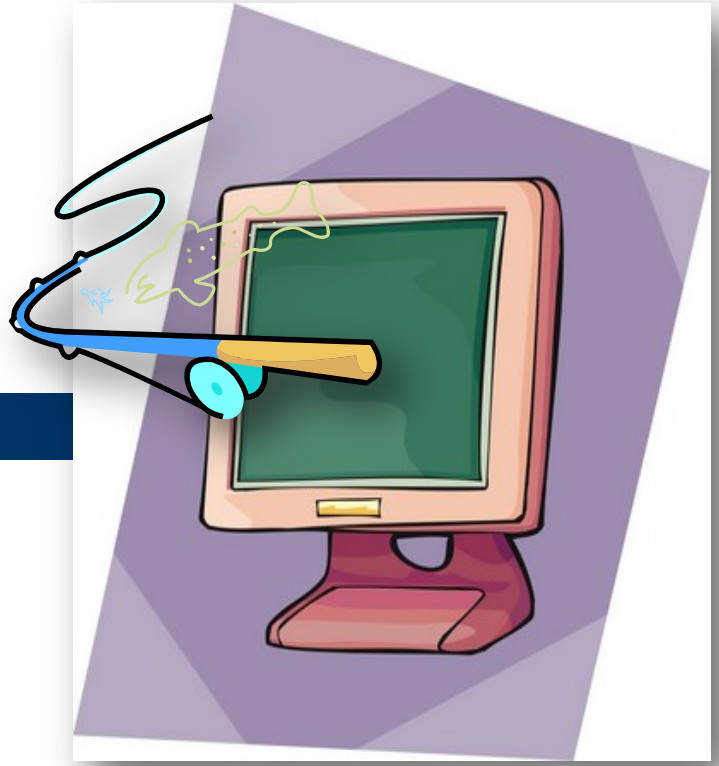
Network and Voice Methods

- Piggybacking / Tailgating
- Phishing & Pharming
- Spim, Spit, & Vishing
- Trojan Code and Viruses

Piggybacking / Tailgating

- Follow authorized employee into secured location
  - Using social expectations of victim
  - What is polite in normal society may be insecure an unwise for security
- Preparations
  - Dress like any other employee
  - Have excuse ready (“Forgot my card….”)
- Defenses
  - Explicitly forbid piggybacking & explain why
  - Teach employees using role-playing

Phishing & Pharming



- Phishing
  - Sending e-mail to trick user into providing personal information
  - Try to copy official correspondence
  - Paste logos
  - Often bad grammar, spelling mistakes
- Pharming
  - Fake Websites imitate real sites (banks, stores)
  - Collect login, financial information

Spim, Spit, & Vishing

- Spim
  - Instant messaging carrying spam
  - Try to trick victim by sending link to fake Website via IM
  - Bypass normal Web/e-mail content controls
- Spit
  - Spam over Internet telephony
  - Limited controls over such spam
- Vishing
  - Voice fishing: spam using phone & e-mail
  - Trick victim into answering questions about personal information

Trojan Code and Viruses

- Discussed above in slide "Exploiting Curiosity or Naïveté"
- Attackers insert malware on victim's computer
- Malware silently installed
- Collects or transmits confidential information
- Provides backdoor code to allow unauthorized access

Reverse Social Engineering

- Aka *knight-in-shining-armor attack*
- Social engineer creates a problem
  - E.g., a denial-of-service attack
  - Rename or move of critical file
- Arranges to seem to be only person who can solve problem
- Fixes the problem (easy if attacker caused it)
  - Gather information during solution
    - "I need to log on as you."
  - Victim may even forget that security policy has been violated
  - Gains trust for future exploitation

Psychology & Social Psychology of Social Engineering

- Psychology of Victim
- Social Psychology
- Social Engineer Profile

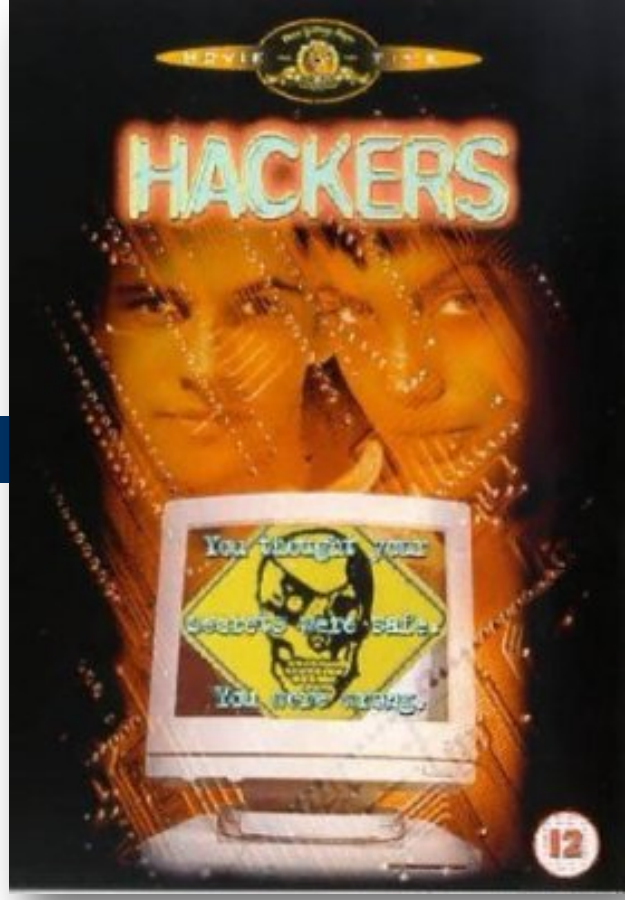
Psychology of Victim

- Cognitive biases aid criminals
- Choice-supportive bias
  - Go with the flow
  - Use what works most of time
- Confirmation bias
  - Remember what fits
  - See person in janitor outfit as janitor – regardless rules
- Exposure effect
  - What is familiar is comfortable
  - Gain trust by referring to familiar topics
- Anchoring
  - Focus on one trait at a time
  - Soothing, friendly demeanor covers intrusive questions

Social Psychology

- Schema is picture of reality
  - Defines normal ways of making judgements and decisions
- Many cognitive errors
  - Fundamental attribution error: assuming that behavior indicates stable, internal attributes
    - Therefore a pleasant, friendly social engineer cannot possibly be a criminal
  - Salience: people notice outliers
    - So social engineers try to blend in
  - Conformity, compliance & obedience
    - Social engineers exert (false) authority

Social Engineer Profile



- Not as in movies: may be
  - Outgoing
  - Confident
  - Well educated
  - Blend into environment (clothing, style, speech)
  - Good actor
  - Quick reactions to changing circumstances
- Dark side
  - Exploits relationships
  - Little or no empathy for victims (instrumental)
  - May be involved in criminal gangs

Dangers & Impact

- Consequences
- Success Rate
- Small Businesses vs Large Organizations

Consequences

- Loss of control over internal documents
  - Advantage to competitors – loss of market share
  - Stock manipulation – SEC investigations
  - Bankrupt company
  - Possible criminal proceedings against officers
- Loss of control over customer personally identifiable information (PII)
  - Legal ramifications including $$$ liability
  - Embarrassment
  - Human consequences of identity theft
- Difficulty tracking down how crime was committed
  - Destroy trust among employees

Success Rate

- Poor statistical base
  - Difficult to detect
  - Difficult to find documentation
- Anecdotal evidence from security experts
  - Social engineering works
  - Consensus that methods are often used…
  - … and highly successful
- Organizations must prepare to defend themselves against these methods (see below)

Small Businesses vs Large Organizations

Small Businesses

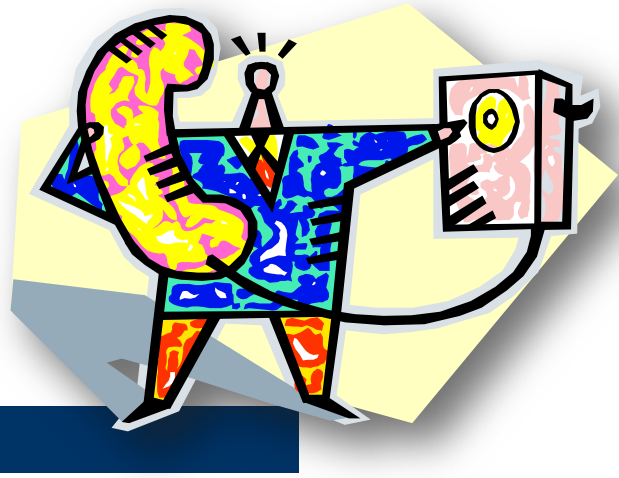
- Less prepared & more vulnerable
- People know each other
- More likely to suspect and challenge strangers
- Better communication – may report suspicions quickly to people they know
- Smaller workforce to train

- ***Large Businesses***
  - More fragmented: many strangers anyway
  - **Concern about embarrassment if stranger is executive from afar**
  - Bystander effect: let someone else deal with it
  - **Poorer communications: may never have met security officers**

Detection

- People
- Audit Controls
- Technology for Detection

People (1)



- Train employees to remember details of phone calls they receive when caller asks questions
  - Gender?
  - Caller ID?
  - Noise in background?
  - Accent?
  - What questions?
  - What answers?
- Beware questions about names of managers
- No employee should ask (let alone give) password

People (2)

- Ensure that employees know they will not be punished for enforcing security policies
  - No legitimate manager would threaten them for NOT violating security rules
  - Explicitly provide script for responding to threats ("Yes, I'll be glad to help you – please hold the line." – and then employee notifies Security Team)
- Provide employees with notification procedure
  - Whom should they call?
  - What information is most helpful (see previous slide)?

Audit Controls

- Real-time audits of log files *may* detect social engineering attack in progress
  - But no guarantees
  - Human manipulation may have no technical exploits until later in crime
  - Actual exploit may be very fast
- Post hoc audits may be useful in reconstructing crime
  - Trace how criminal used information winkled out of employees

Technology for Detection

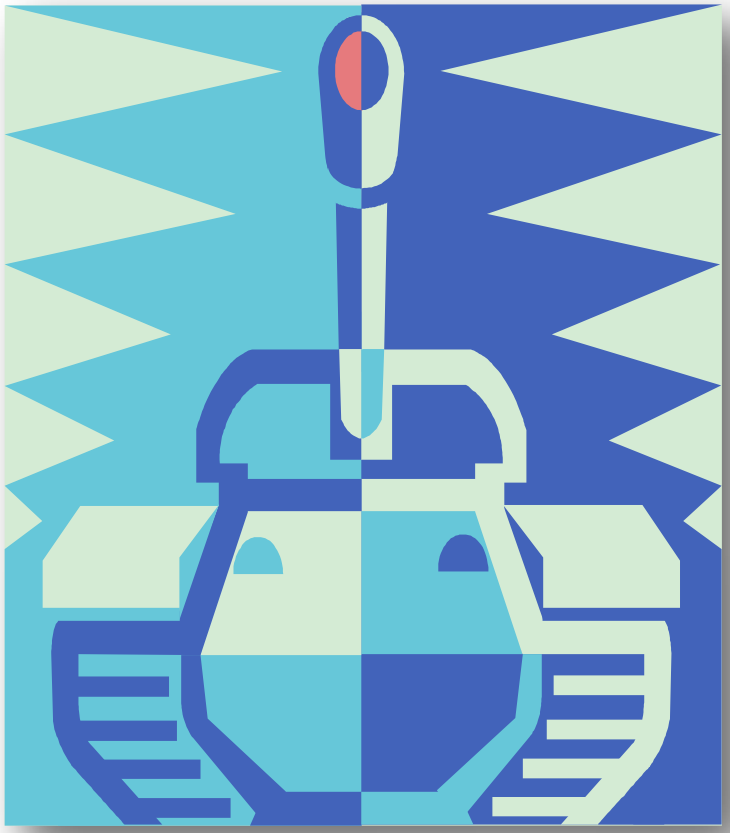
- Content-blocking technology
  - E-mail
  - Web pages
- Social Engineering Defense Architecture (SEDA)
  - Voice-recognition technology
  - Provides better logging of phone calls

Response

- Integrate social engineering attacks into *computer security incident response team* processes
- Collect forensic evidence
  - In real time if possible
  - ASAP
  - Interview human victims
    - Quickly
    - Humanely – do not give impression of looking for scapegoats

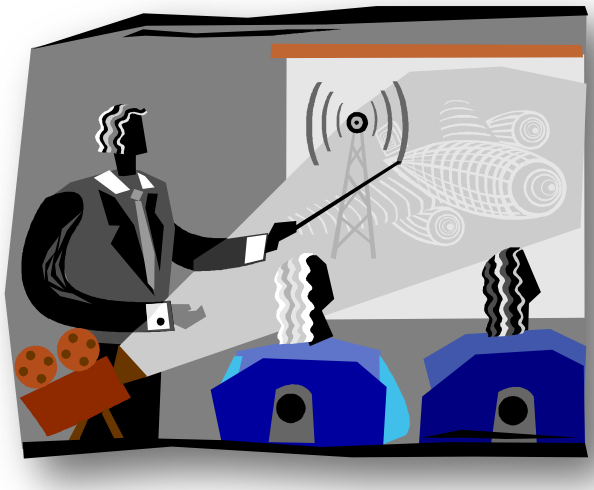
Defense & Mitigation

- Training & Awareness
- Technology for Prevention
- Physical Security & Encryption

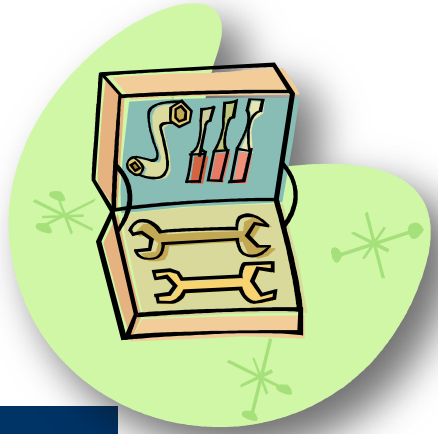


Training & Awareness

- Explain social engineering techniques to employees
  - Real case studies
  - Demonstrations
- Encourage and support challenges
  - Asking reasons for questions
  - Asking for employee identification
  - Checking for authorization for unusual requests
- Provide role-playing exercises to reduce reluctance
- Provide emergency response contact info



Technology for Prevention



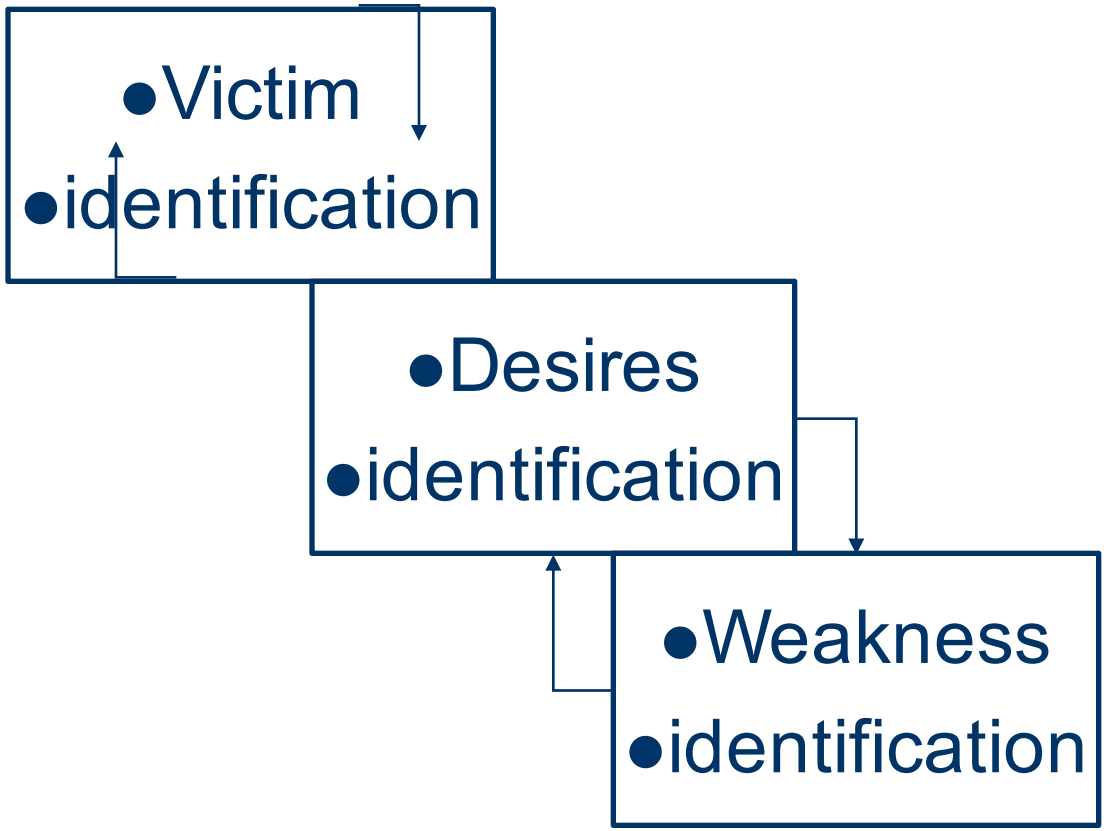
- Effective antimalware tools
  - Block viruses, Trojans
  - Block dangerous Web sites
  - Block dangerous phishing spam
  - Block popups, ActiveX controls
  - Restrict types of cookies
  - Use digital certificates to authenticate internal e-mail
- Control over software installation
- Cleanse documents of hidden metadata
- Check Web for unauthorized posting of confidential documents or information

Physical Security & Encryption

- Prevent theft of confidential information
  - Lock filing cabinets
  - Shred discarded documents
  - Protect Dumpsters® against divers
- Use data encryption
  - Laptop computers
  - Peripherals such as USB drives
  - Virtual private networks for remote access

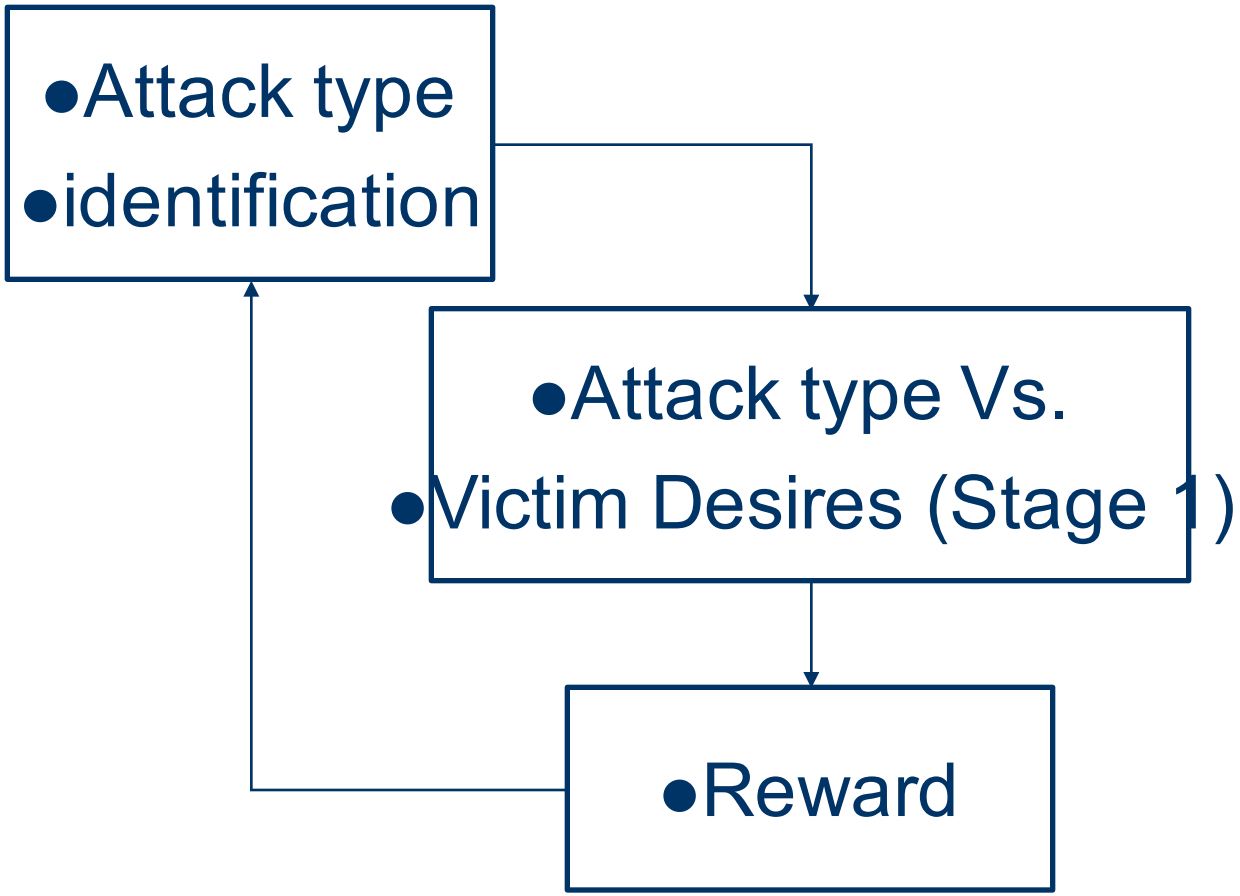
Pre-Contact Social Engineering model

- Stage 1

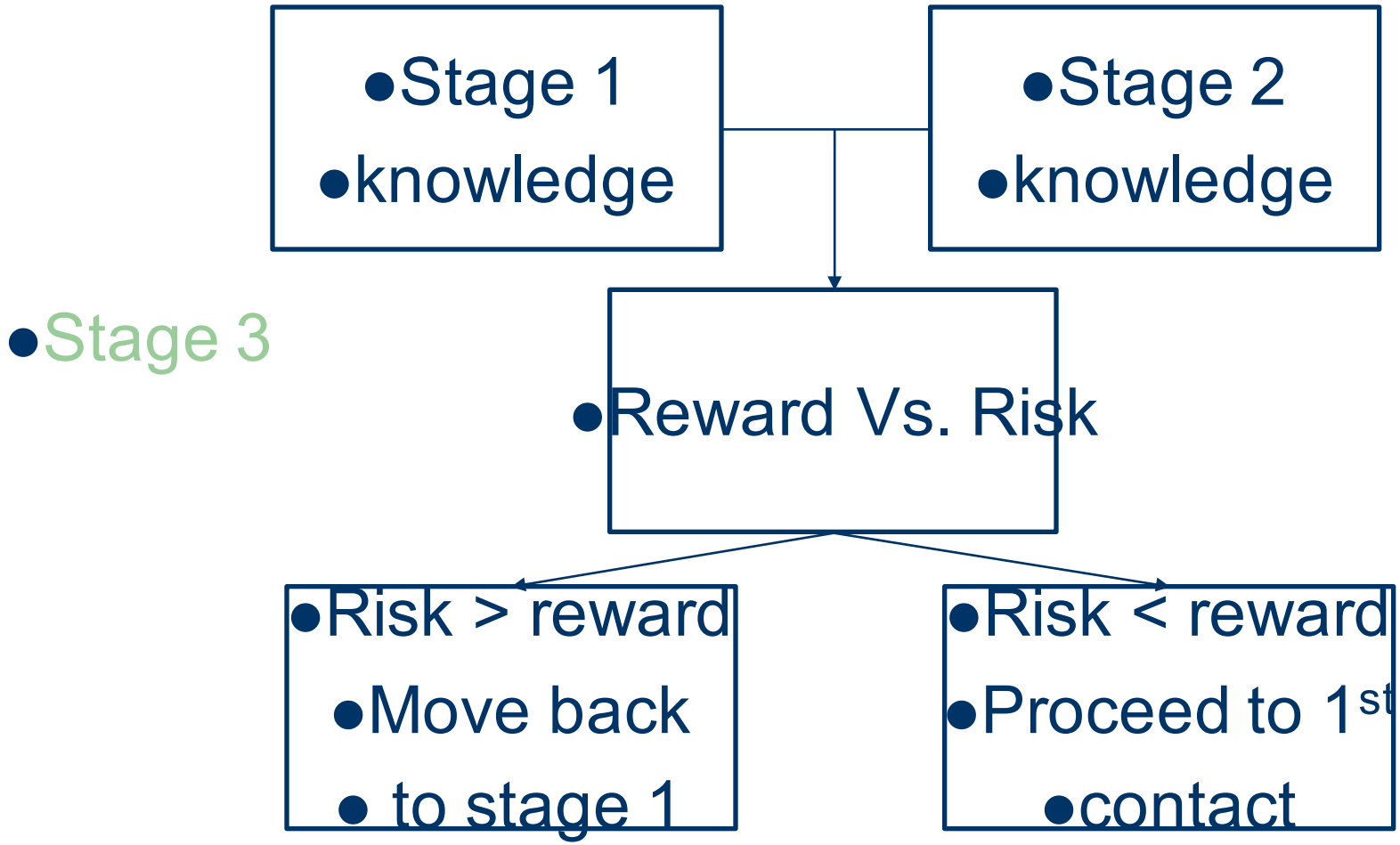


Pre-Contact Social Engineering model

- Stage 2



Pre-Contact Social Engineering model



Questions?