# The Art of Deception


## Kevin Mitnick

Chief Executive Officer
Defensive Thinking LLC
Los Angeles
www.defensivethinking.com

# What is Social Engineering?

"Using influence, deception, and/or psychological manipulation to persuade others to comply with a request."

What is the impact/threat of se?

# Why Attackers Use Social Engineering

- Easier than hacking a system
- No Intrusion Detection System (IDS) can detect SE
- Low cost/risk for the attacker
- Works on every O/S platform
- No logs (audit trail)
- Nearly 100% Effective
- General lack of awareness

# Security Laxity – Survey Results

- Nine in ten (90 per cent) of office workers at London's Waterloo Station gave away their computer password for a cheap pen, compared with 65 per cent last year.

# Typical Goals of the Attacker

- Source code
- Customer lists
- Financial data
- Marketing & new product plans
- Proprietary information on manufacturing processes
- Contract bids
- Merger & acquisition information
- Research documents
- Access to computing resources (DDOS)
- To see what they (hackers) can find

# Who Are the Prime Targets?

- Help Desk Personnel
- Customer Service Representatives
- Receptionists
- Administrative Assistants
- Security Guards
- System Operators and Technicians
- Sales and Marketing Staff
- Anyone who has electronic or physical access

# Common Attack Methods

- Reveal, transmit, or change password to a suggested word or phrase.
- Create an account (user or admin)
- Execute a program (Trojan horse attack)
- Reveal dial-in number or remote access procedures
- Add privileges or access rights to existing accounts
- Send or transfer confidential information

# Why Does Social Engineering Work So Well?

- Are not aware of the threat of SE
- Naturally want to help others
- Underestimate the value of information
- Want to stay out of trouble
- Have no personal investment in the information they are asked to provide
- Are often too busy to verify identity and authorization
- Do not realize the consequences of their actions.

# Factors in the Business Environment that Increase Risk

- Mounting pressure on employees to get work done quickly
- Increased reliance on off-site personnel
- Multiple office locations
- Job reviews based on level of performance and team participation – not security compliance.
- Virtual interaction with partners, vendors, and suppliers
- Focus on being part of the "team"
- High turn-over rate

# The Human Factor – Forces that Make People Vulnerable

People generally…

- Tend to implicitly trust others (propensity and prior history)
- Tend to help people they like
- Perceive that security is a waste of time or a work impediment
- Have illusions of invulnerability ("it won't happen to me" syndrome)

# Pretexting: The Con

- attacker gathers information in order to construct a pretext for contact
  - Establish identity & "need to know"
  - Develop plausible ruse to gain compliance
  - Build the target's confidence through prior knowledge or identity
  - Strategize the target's possible objections for non-compliance
  - Develop a counterargument to overcome any objections
  - Leaving an "out" to avoid raising suspicion

# Intelligence Gathering

- Collectively, small nuggets of seemingly useless information can be joined to form valuable information
- Key techniques:
  - Using the Internet
  - Open source information
  - Dumpster diving
  - Surveillance (cellular & two-way radio)

# Researching the Company

- Company web site
- Names of personnel
- Organization chart / structure
- Corporate newsletters
- Intra-company phone directory
- Lingo, terminology & server names
- Open positions, HR listings
- New Hires
- Information on telecommuters that use remote company resources
- Sales and marketing materials

# Digging up Personnel Information

- Phone numbers & Email addresses
- Title / position at company
- Job responsibilities / duties (access)
- Hobbies or special interests
- Schools attended
- Remote access privileges (telecommuters)
- Personal Web Page / Biography / Resume / Published papers
- Personal identifying information
- Work / Vacation schedules
- Past newsgroup postings

# Dumpster Diving: waste archeology

- Goldmine of information
  - Project names and plans, correspondence
  - Employee names, internal email addresses, phone directories, manuals, & calendars
  - Company letterhead, memos, notes
  - Discarded media (hard drives or removable media)
  - Yes, even user lists and passwords
- Incredibly, not illegal unless:
  - "No Trespassing" sign is posted
  - Trash is on private property

# How Attackers Bypass Verification Controls

- Call forwarding an existing employee's number
- Forging outbound Caller ID
- Compromising a trusted voice mail box
- telephone receptionist – fax exploit
- Using pre-paid Cellular phones
- Forging fax or e-mail headers

# Influence agents: Psychological triggers

- Liking
- Authority
- Reciprocation
- Consistency
- Scarcity
- Social validation

# Curiosity: killed the cat

- Plant a floppy or cdrom on the target's facilities
- Send an enticing email with a malicious attachment
- Influence the target to visit a web site that has malicious code

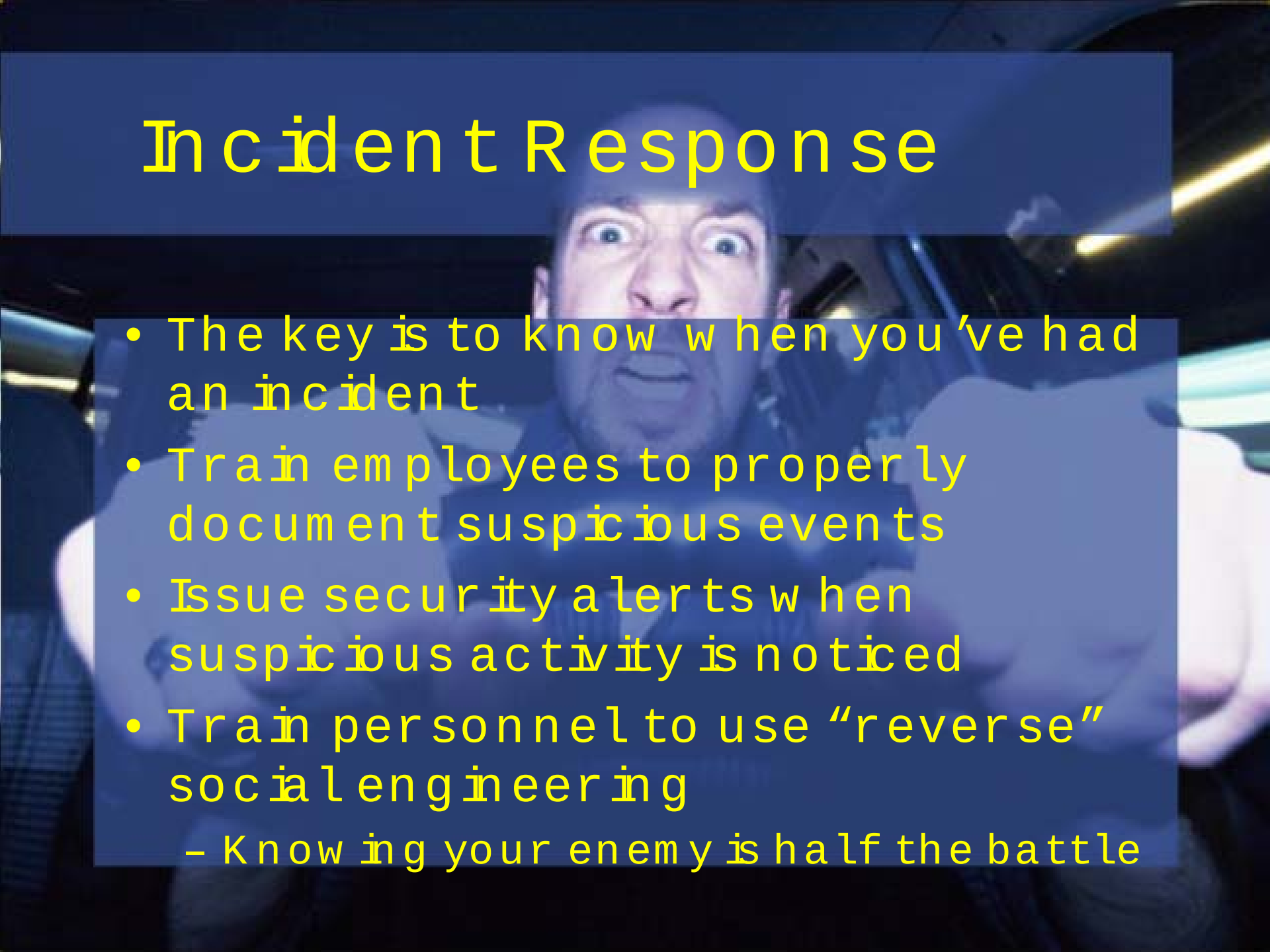
# How to recognize possible attacks

- Refusal to give contact information
- Out of the ordinary request
- Rushing with urgent request
- Mirroring interests and background characteristics
- Laying on too much flattery
- Intimidation using authoritative commands from management
- Offers help with an unknown problem
- Claims the request has been approved by management

# Building resistance to manipulation

- Demonstrate personal vulnerability
- Train employees to focus on the nature of the request
- Take a moment to evaluate a request
- Verify identity and authorization
- Modify enterprise politeness norms
- Change attitudes toward information – protecting vs. sharing
- Educate personnel *why* security protocols are critical to the business

# Incident Response



- The key is to know when you've had an incident
- Train employees to properly document suspicious events
- Issue security alerts when suspicious activity is noticed
- Train personnel to use "reverse" social engineering
  - Knowing your enemy is half the battle

# 8 steps to building the human firewall

- Security Policy
- Security Awareness training
- Inventory information assets
- Deploy data classification
- Social engineering pen-testing
- Incident Response planning
- Limit information leakage
- Using technology (Design & AV)

# Conclusion

- Social Engineering is the single, most effective and dangerous threat to information security
- Constant vigilance is required to mitigate this threat
- The most effective countermeasures are policies, awareness/resistance training, incident response and pen-testing

# Additional resources

- The Art of Deception – www.amazon.com/mitnick
- The Human Firewall Council
  - www.humanfirewall.org
- Dr. Kelton Rhoads
  - www.workingpsychology.com
- *Influence* by Robert B. Cialdini
- *Confidential* by John Nolan


HELLO! *SNICKER* THIS IS THE HELP DESK *CHUCKLE* I NEED YOUR PASSWORD!
What was your Name again?
copyright 2001
Native Intelligence