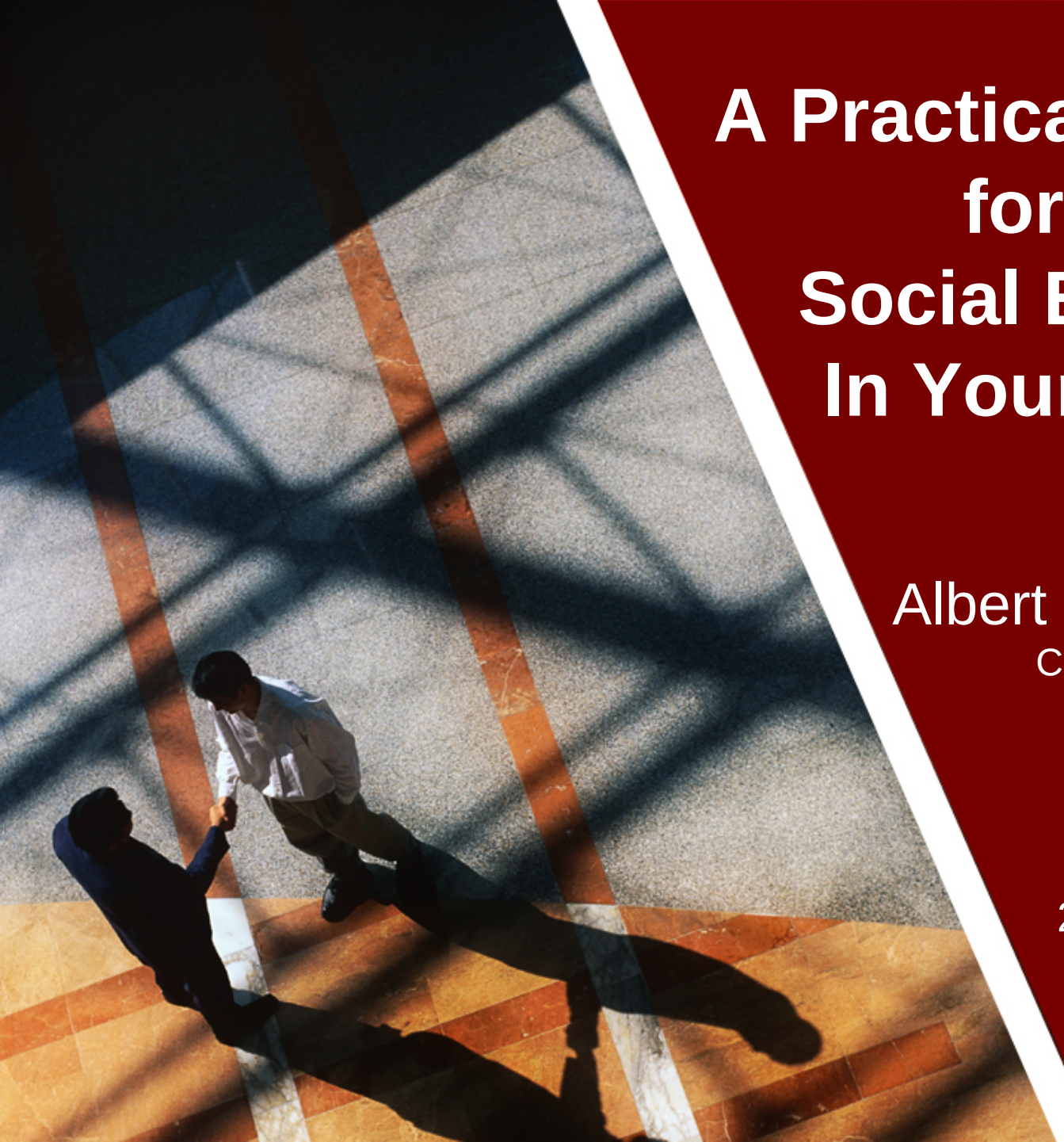


A Practical Approach for Combating Social Engineering In Your Enterprise

Albert Lewis, CISSP-ISSMP, CISM, IAM, IEM, PMP, ITIL

FISSEA
21st Annual Conference
March 12, 2007
Gaithersburg, MD

Introduction

❖ Secure IT Solutions, Inc.

- Information assurance consulting and solutions provider offering enterprise security engineering and architecture, risk management, education and training, and certification and accreditation.

❖ Albert Lewis, CISSP-ISSMP, CISM, IAM, IEM, PMP, ITIL

- Provides strategic guidance to several federal clients for creating information assurance programs that comply with legal and regulatory requirements while protecting critical infrastructure.
- Helped create the CSIRC/SOC for the Army National Guard headquarters in response to 9/11.
- Teaches graduate courses in information assurance at Johns Hopkins University.

Secure IT Solutions

“War is based on deception.”

Sun-tzu, (~400 BC), *The Art of War, Strategic Assessments*

"We are inclined to believe those whom we do not know because they have never deceived us."

Samuel Johnson (1709 – 1784)

Session Description

- The strongest perimeter defense can be compromised quite easily by the low-tech social engineer who preys on unsuspecting users
- Thwart attacks by learning the psychological techniques currently in use
- Prepare your users for attack via an effective awareness program

Session Description

- The strongest perimeter defense can be compromised quite easily by the low-tech social engineer who preys on unsuspecting users
- Thwart attacks by learning the psychological techniques currently in use
- Prepare your users for attack via an effective awareness program

Session Description

- The strongest perimeter defense can be compromised quite easily by the low-tech social engineer who preys on unsuspecting users
- Thwart attacks by learning the psychological techniques currently in use
- Prepare your users for attack via an effective awareness program

Presentation Goals

- **Goals for Today's Presentation:**
  - To raise your awareness about social engineering (SE) methods and attack vectors
  - To provide real-world insights and tips you can put to use today to protect your organization

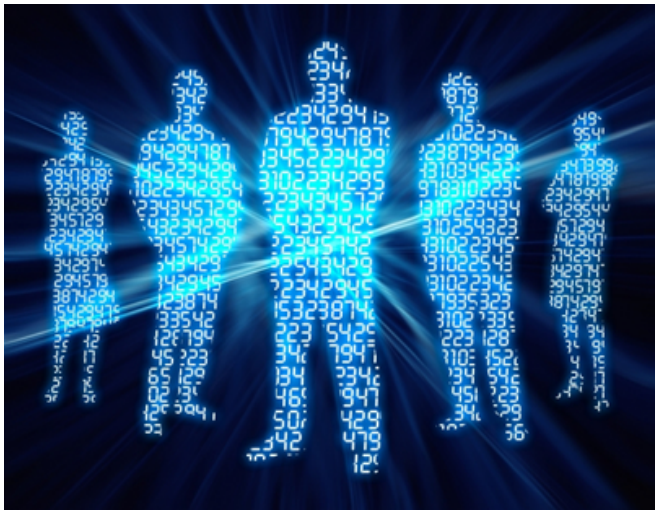
Human Firewall?

"I know a lot of highly-confidential company secrets, so my boss made me get a firewall installed."

What is Social Engineering?

❖ Social Engineering (SE)

- Manipulating people (rather than machines) into divulging confidential information or gaining access
- Takes advantage of predictable human responses to psychological "triggers"
- SE attacks can be both technical and non-technical in nature



Social Engineering Terms

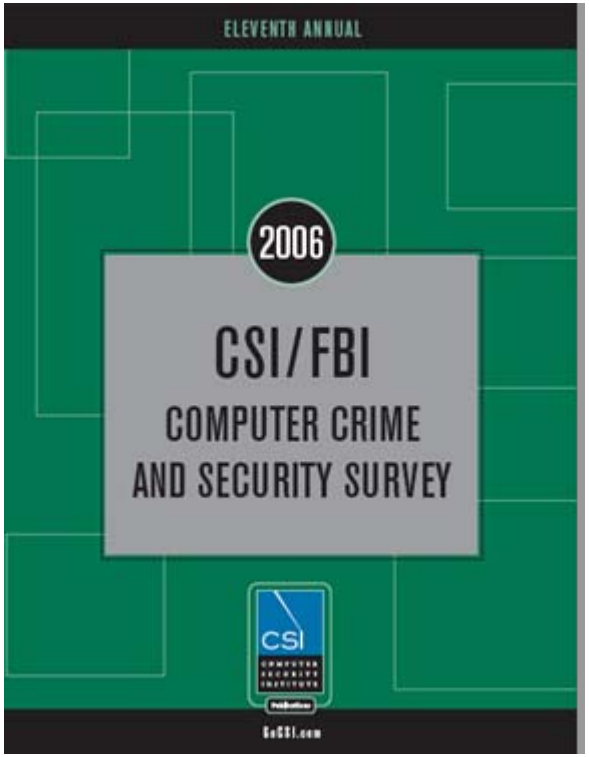
- **Active attack**
  - Interaction with target to elicit information
  - Phone, in-person, online
- **Passive attack**
  - Gather information to use in launching further social engineering attacks or attacks on systems
  - Open source intelligence (Internet, trash)
- **Pretexting**
  - Creating and using an invented scenario to persuade a target to release information or perform an action

2006 CSI/FBI Survey

- **CSI asked security practitioners:**

  "What do you think will be the most critical computer security issues your organization will face in the next two years?"

- **Social engineering beat out:**
  - Malware, zero-day attacks, data back ups



Security Questions

- **Questions good security professionals might ask themselves:**
  - Where is my information systems infrastructure most vulnerable?
  - What are the critical areas where I need to apply available resources to best manage risk?

Security Questions

- Questions good security professionals might ask themselves:
  - **What is the greatest security risk facing my organization?**

Social Engineering

- In 2004, **Gartner** advised that the greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses

"We believe social engineering is the single greatest security risk in the decade ahead."

Rich Mogull
Research VP, Gartner

Who Are Social Engineers?

- **Social Engineers are:**
  - Malicious hackers
  - Competitive intelligence
  - Cybercriminals
  - State-sponsored cyberwarfare agents
  - Terrorists
  - Scam artists
  - Disgruntled employees

Why Do They Do It?

- **The goals of the social engineer are the same as any malicious hacker**

- **Social engineers are after:**
  - Your information
  - Your trade secrets
  - Your money
  - Your IT resources

Why Social Engineering?

- **Because It's Easy…**
  - Easier to bypass human nature than multiple layers of technical defenses

- **Because It Works…**
  - Results are predictable because humans are "engineered" to respond automatically to certain psychological triggers

Systematic Decision Making

- **Good business relies on good decision making**
- **Employees should:**
  - Approach problems rationally
  - Ignore irrelevant information
  - Weigh relevant information appropriately
  - Remain open minded
  - Resist tendency toward bias and fallacies

People are Not Computers

"We don't evaluate security trade-offs mathematically…instead, we have shortcuts, rules of thumb, stereotypes, and biases – generally known as 'heuristics.'"

Bruce Schneier

"The Psychology of Security," February 28, 2007

People are Not Computers

"The problem is that [heuristics] can fail us...Our social and technological evolution has vastly outpaced our evolution as a species, and our brains are stuck with heuristics that are better suited to living in primitive and small family groups."

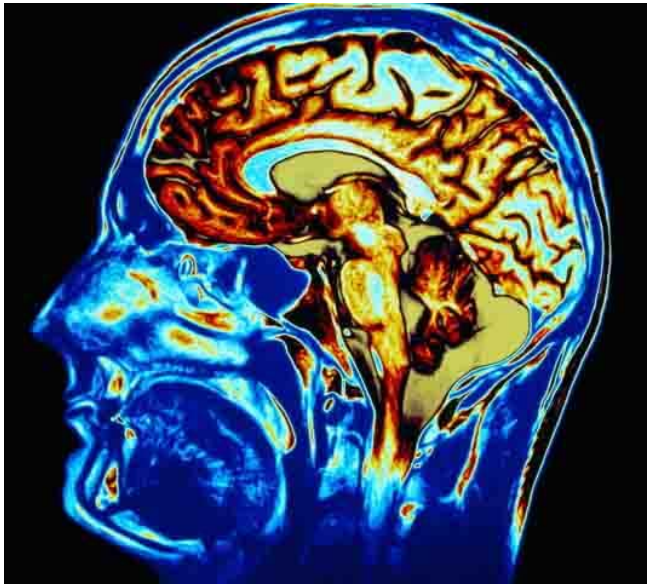
Bruce Schneier

"The Psychology of Security,"
February 28, 2007

Heuristics and Biases

- **Heuristic thinking**
  - Proceeding by trial and error, rather than by systematic analysis
  - Basing decisions solely on previous outcomes
  - Relying on “gut instinct”

- **Cognitive biases**
  - Bandwagon effect
  - “Just following orders”
  - Foot-in-the-door effect



Heuristic Thinking

- **In social situations, people tend to think less systematically, more heuristically**
- **Heuristic thinking serves a purpose**
  - Organizations desire efficiency
  - Elimination of all shortcuts, rules of thumb, and biases would seriously impact productivity
- **Problem**
  - Outcomes of heuristic thinking are predictable
  - Easily manipulated by social engineer

Rules of Thumb, Triggers

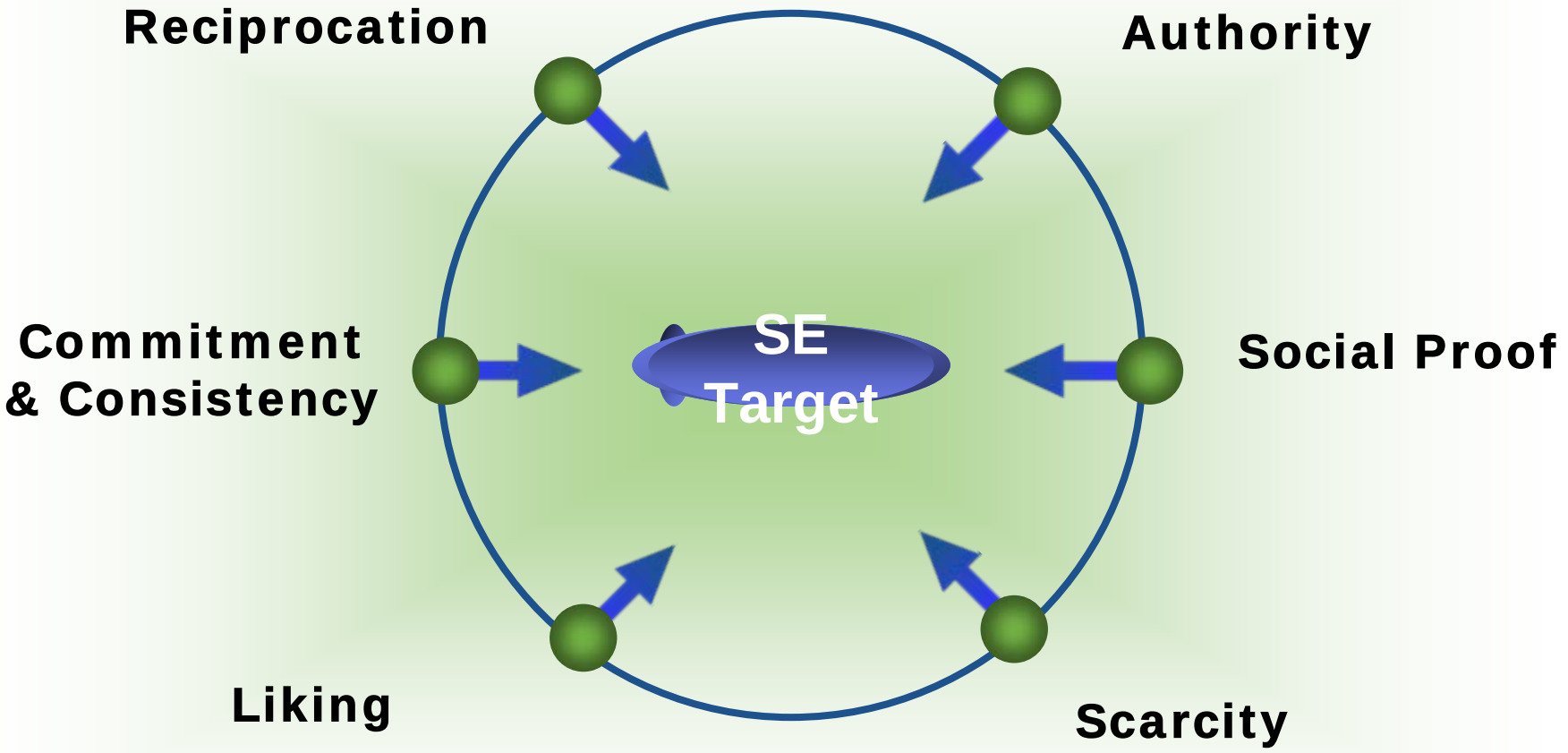
"We haven't the time, energy or capacity … to recognize all aspects in each person, event and situation we encounter."

"Instead we must use…our rules of thumb to classify things according to a few key features and then respond mindlessly when one or another of these trigger features is present."

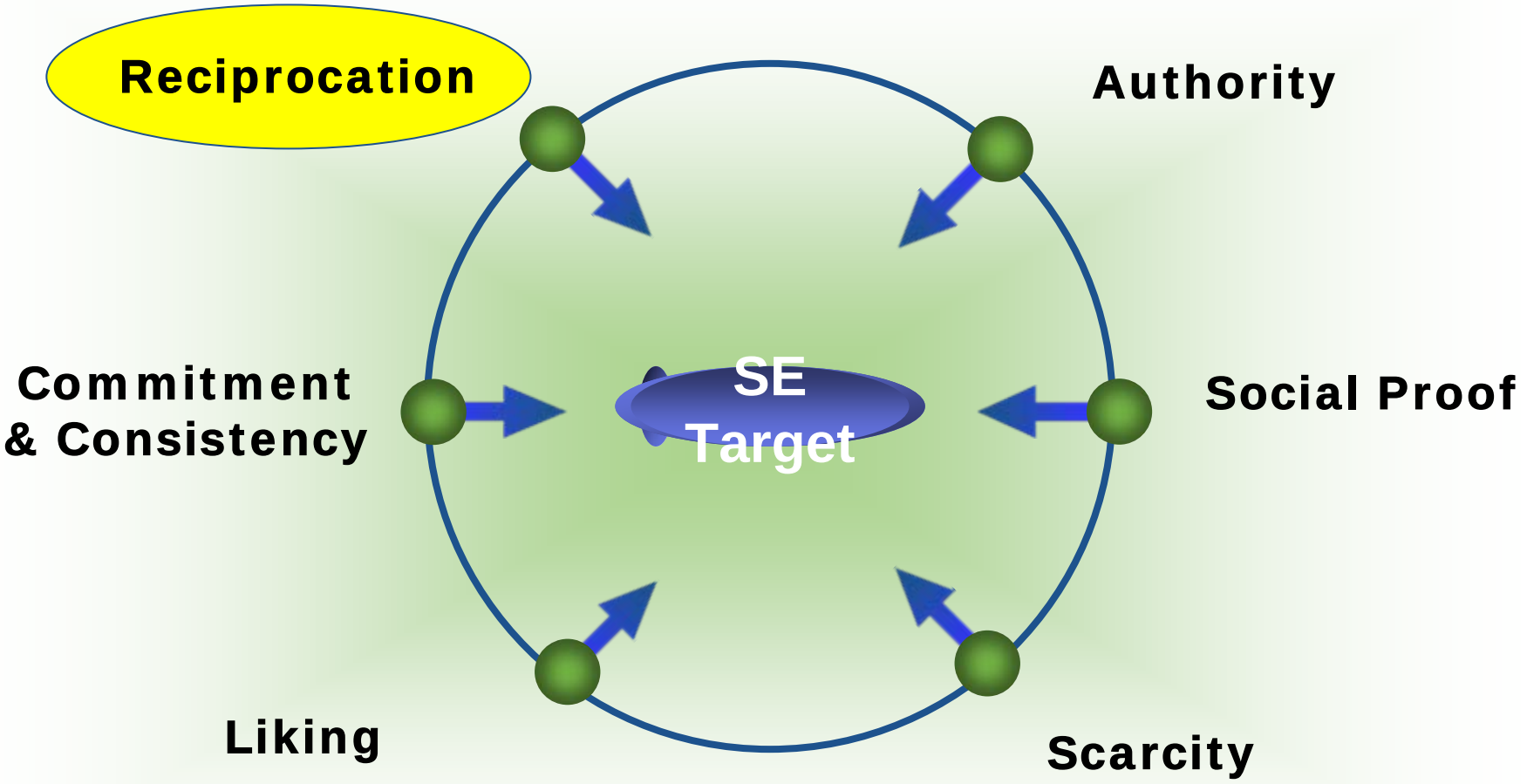
Robert B. Cialdini, Ph.D.

"Influence: The Psychology of Persuasion," 2007

Psychological Triggers



Psychological Triggers



Trigger ➔ Reciprocation

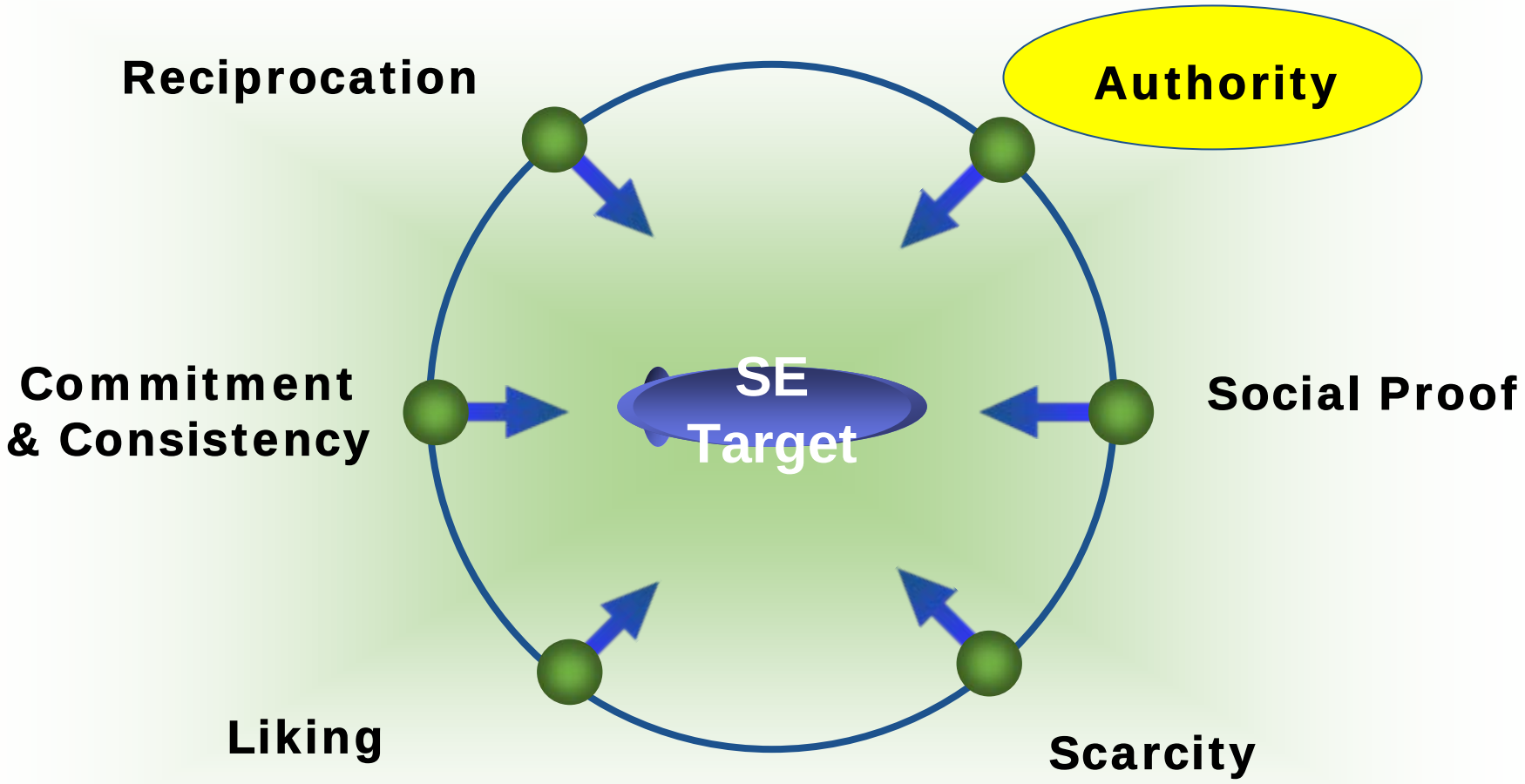
❖ Reciprocation

- Taking advantage of human desire to respond in kind to perceived favors
  - Cup of coffee for your password?

❖ Methods of Attack

- Offer false information to "help" user which forms an underlying obligation (reverse social engineering)
- Yield points in an argument

Psychological Triggers

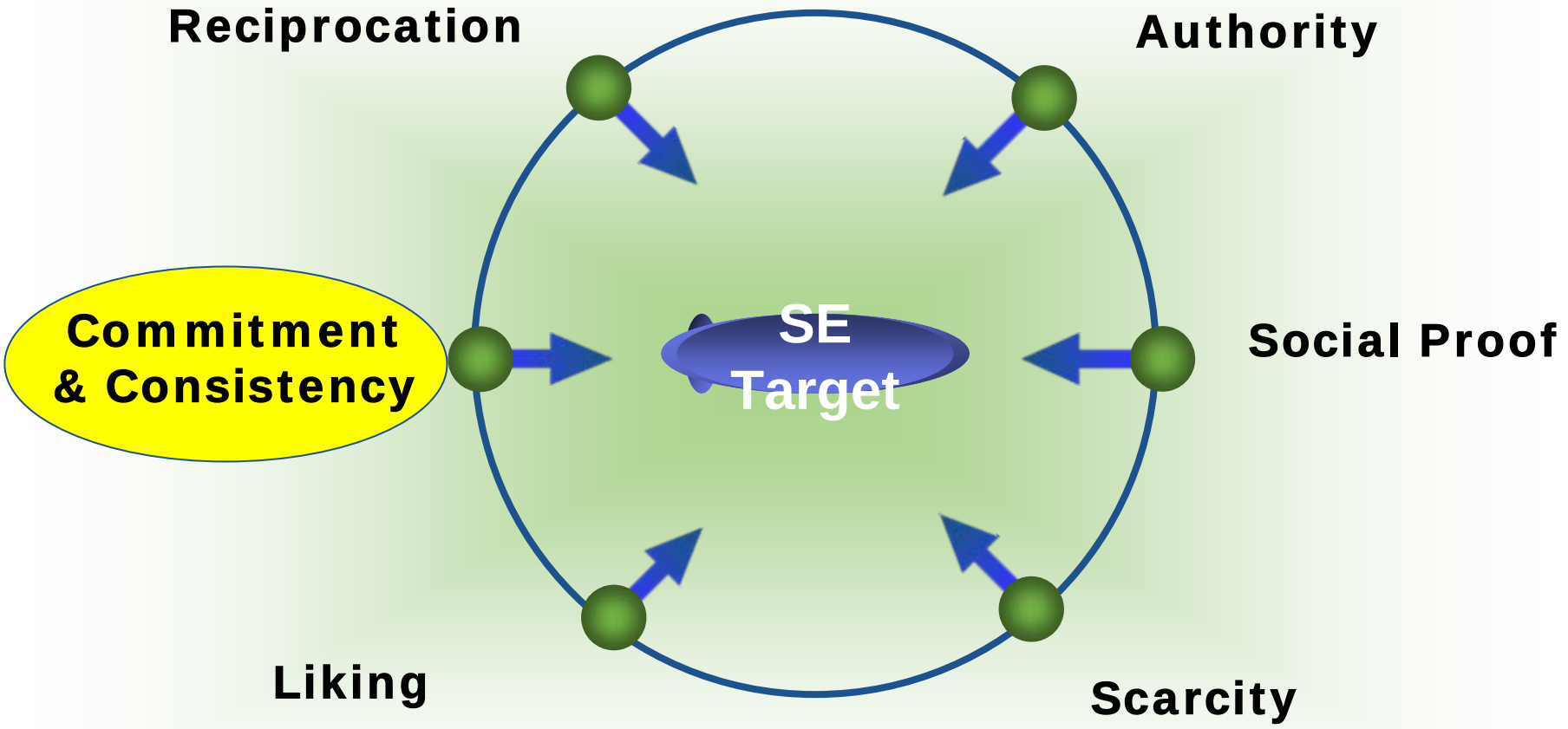


Trigger → Authority

- **Authority**
  - People generally tend to conform to the dictates of authority figures
    - Milgram psychology experiments
    - Fast food strip-search case

- **Methods of Attack**
  - Telephone
    - Call to obtain a forgotten password or other information
  - In Person
    - Clothing, falsified badges

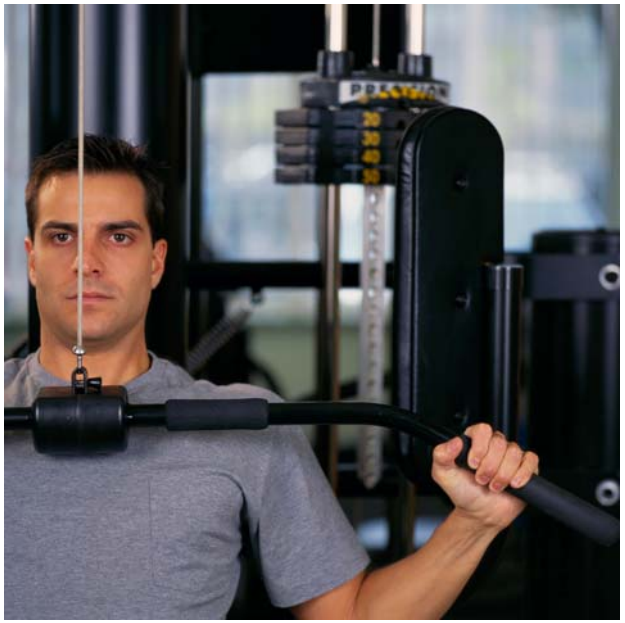
Psychological Triggers



Trigger ➔ Commitment & Consistency

❖ Commitment and Consistency

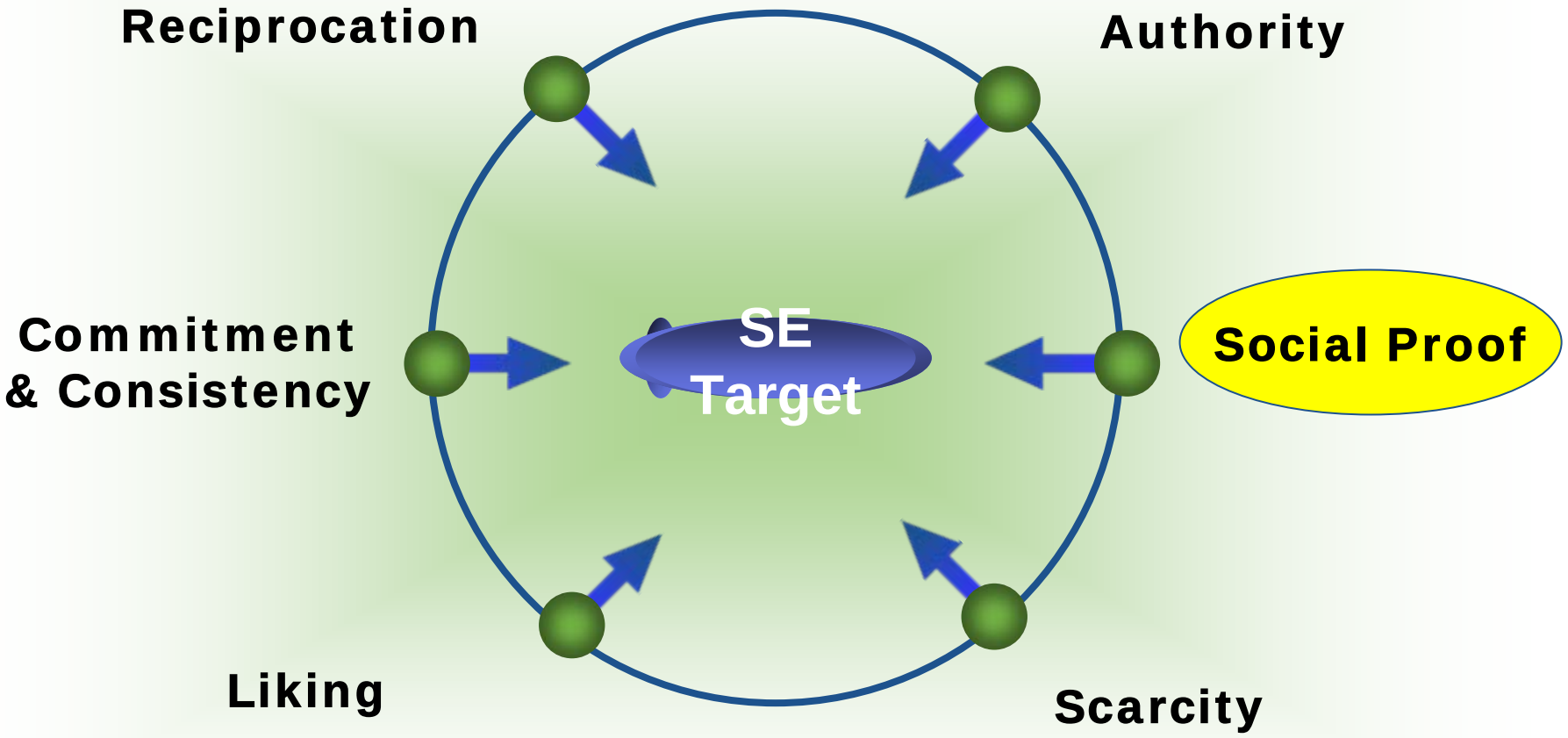
- Once we take a stand or commit, we need to be (and appear) consistent with what we have already said and done
  - Race track experiment
  - The gym membership



❖ Methods of Attack

- Give a new employee a false security policy, then request their password to verify against policy
- Information by attrition

Psychological Triggers



Trigger ➔ Social Proof

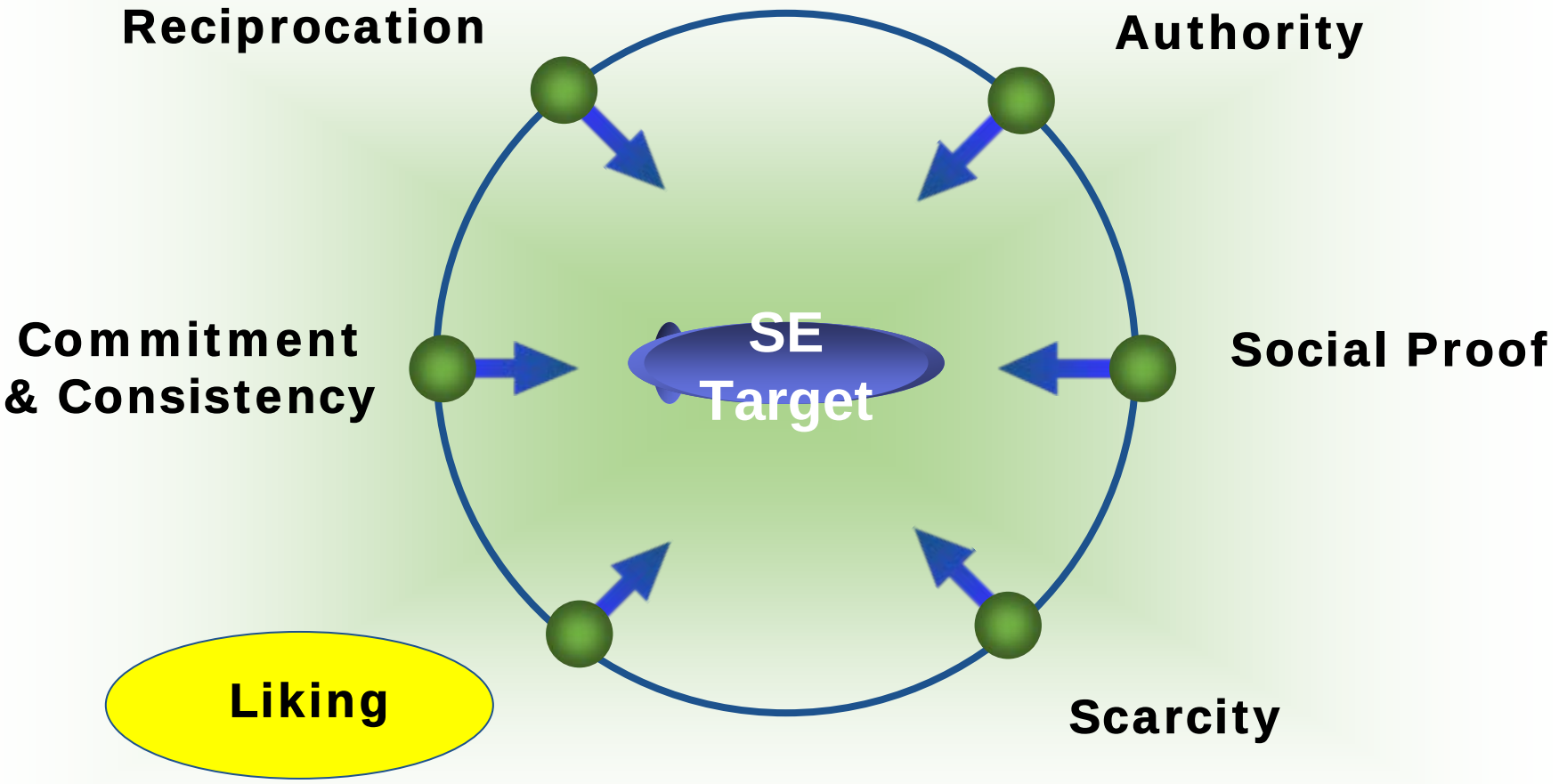
❖ Social Proof

- Pressure to follow the crowd
  - Celebrity endorsements
  - Canned laughter

❖ Methods of Attack

- Name dropping to influence actions
- “Linda and Bob in accounting gave me their passwords. Now I need yours.”

Psychological Triggers



Trigger ➔ Liking and Similarity

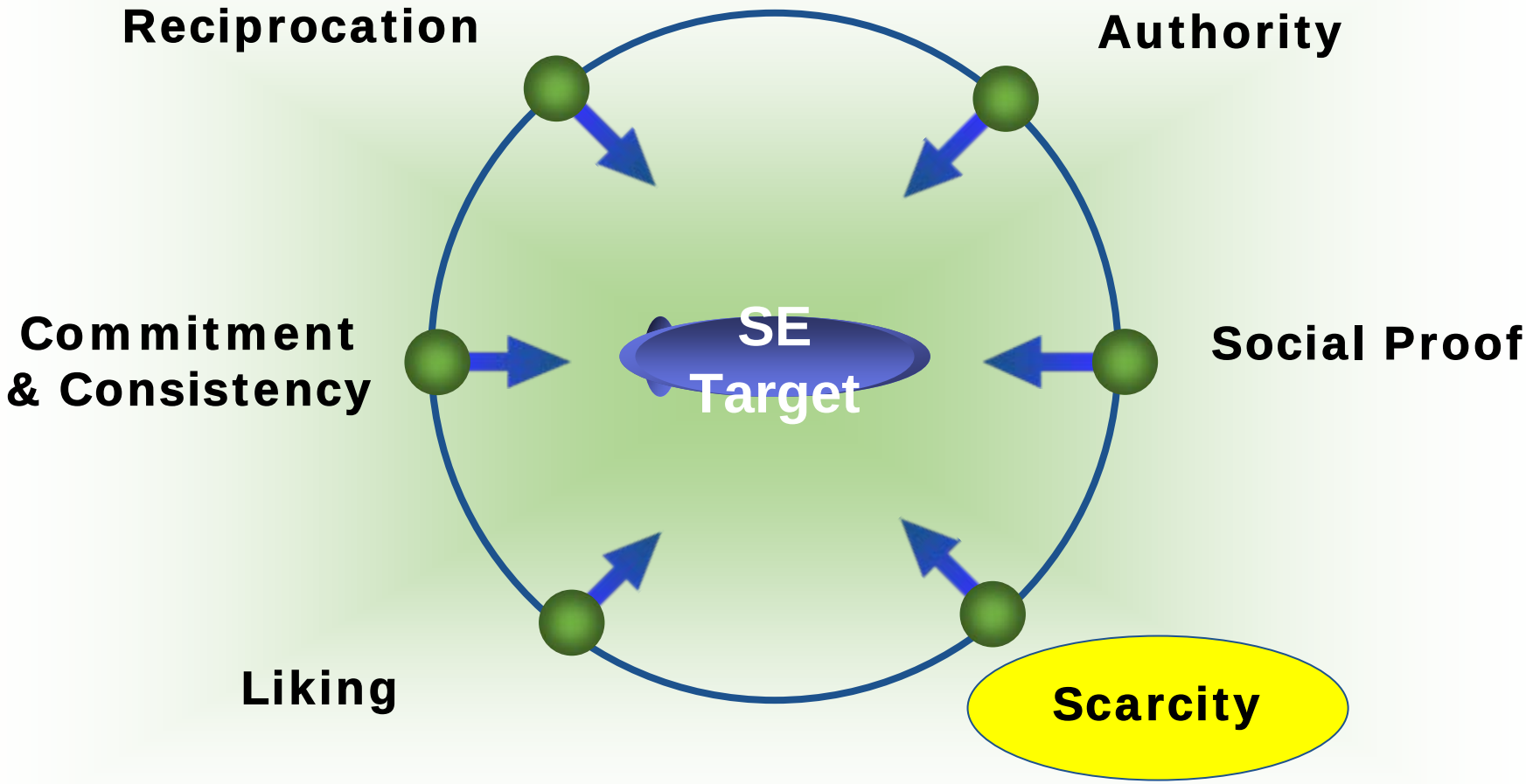
❖ Liking and Similarity

- Humans naturally tend to associate with those who like the same things, or are similar to them in some way

❖ Method of Attack

- Through conversation, attacker probes for a personal connection to establish rapport
- “You like football? So do I! How about those Redskins!”

Psychological Triggers



Trigger → Scarcity

Scarcity

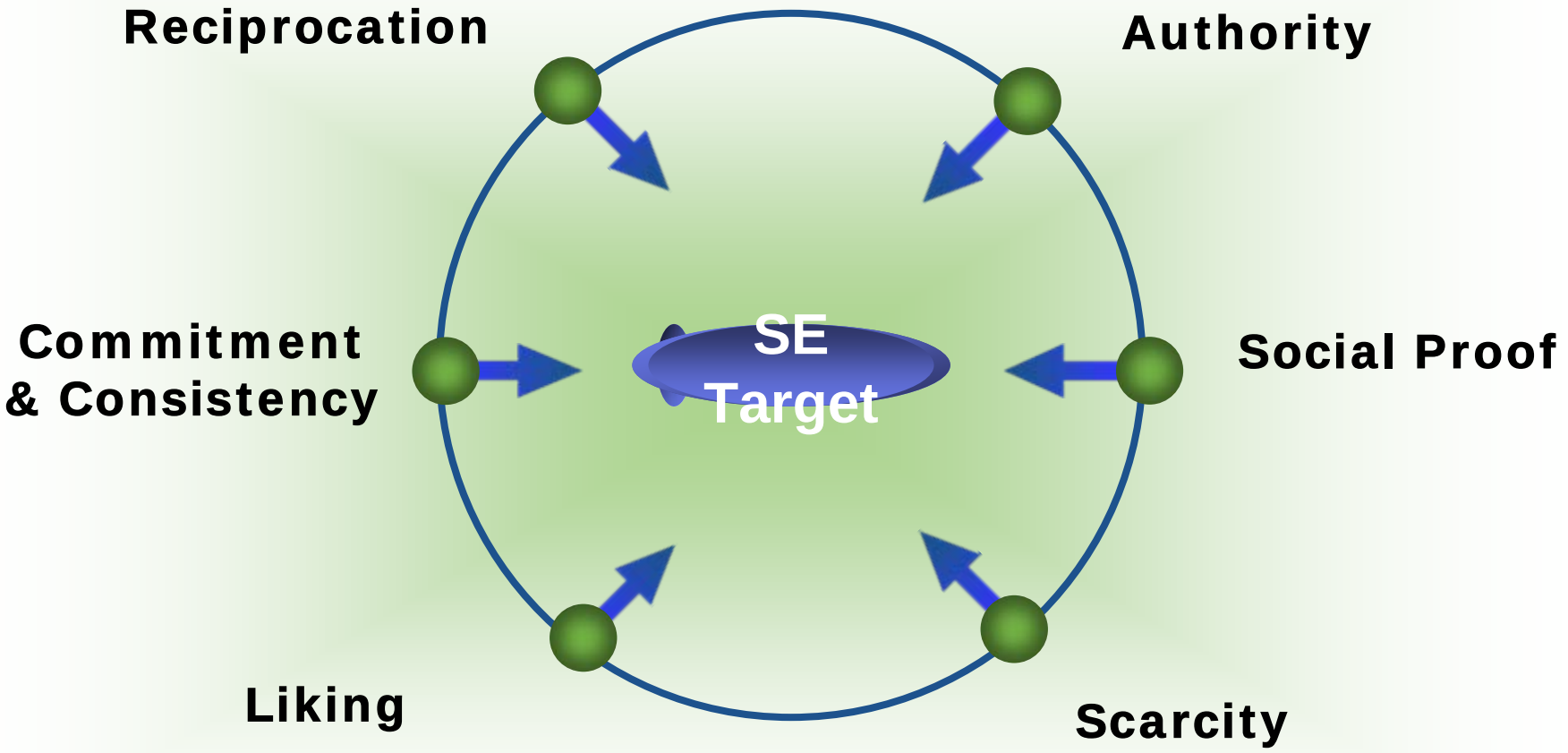
- People tend to comply when they believe that an object is in short supply, highly sought after, or is available only in scare quantities

Methods of Attack

- Phishing emails
- Pop-ups
- “Click here to download software to prevent further pop-ups!”

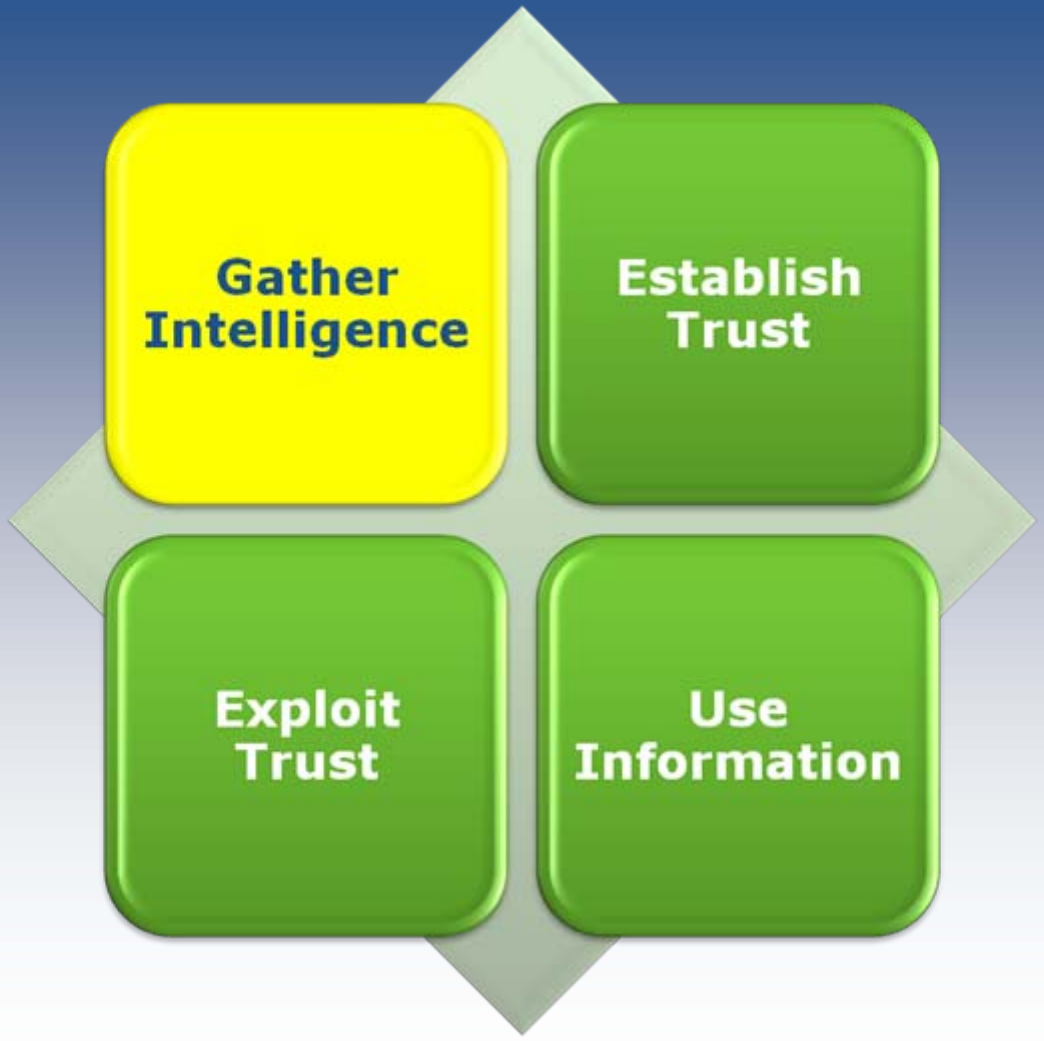
Act Now! Supplies Are Limited!
Operators Are Standing By!

Psychological Triggers

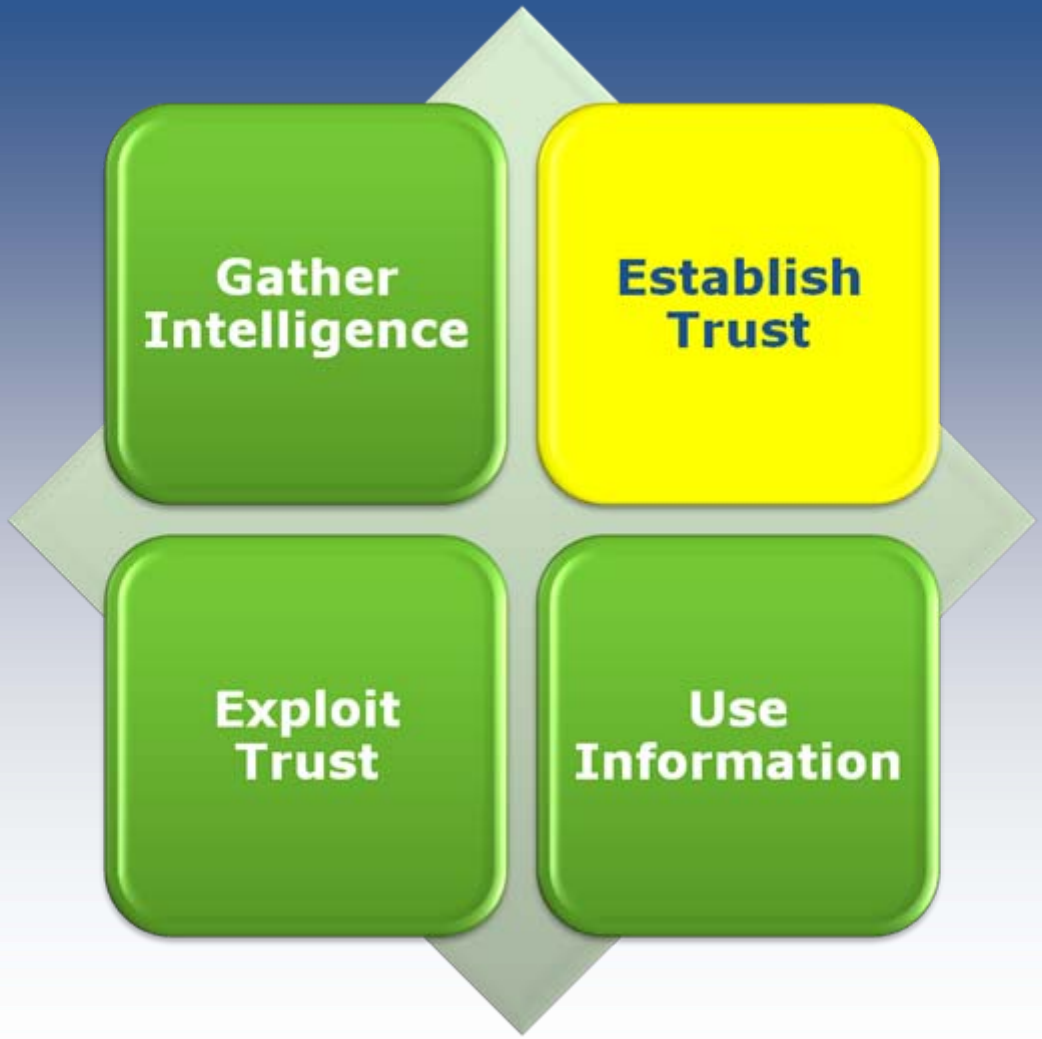


Social Engineering Attack Cycle

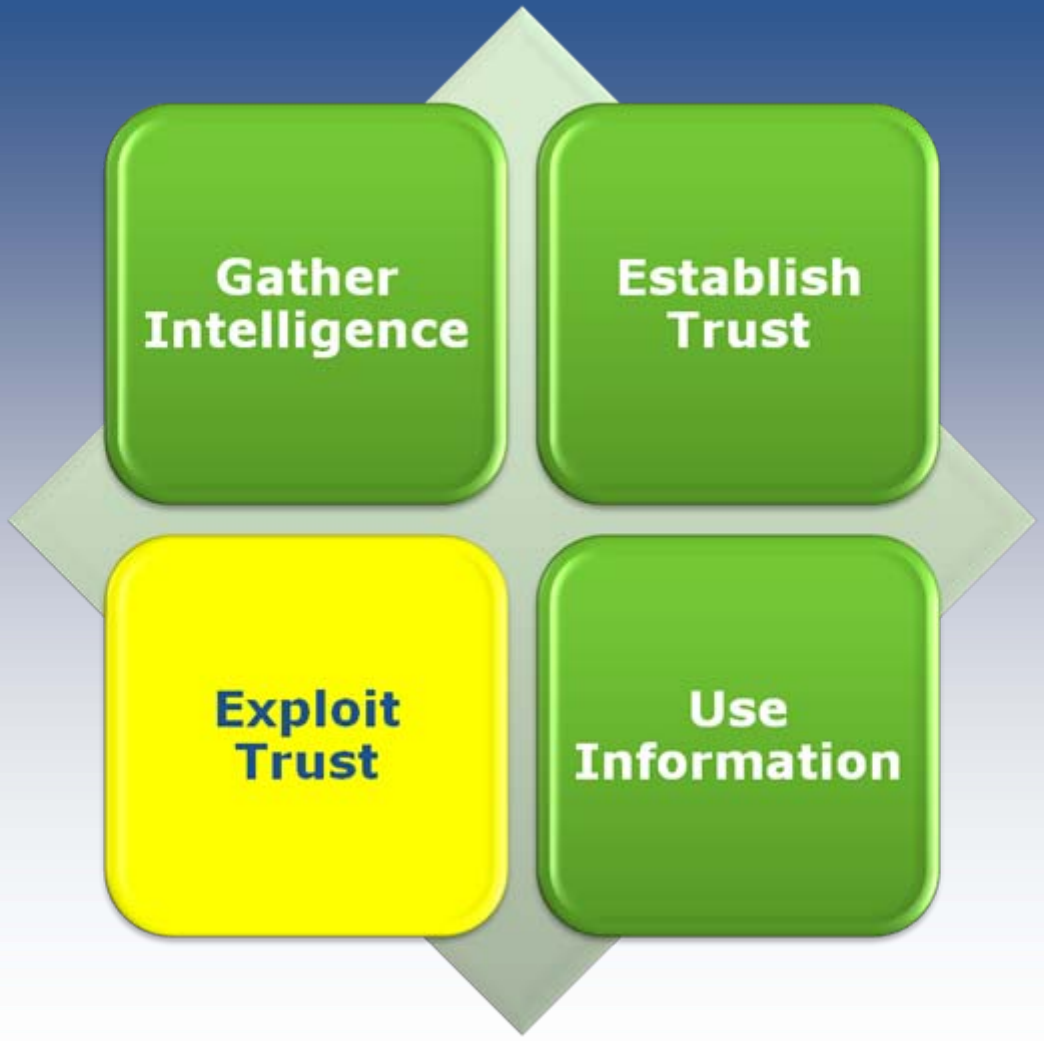
Social Engineering Attack Cycle



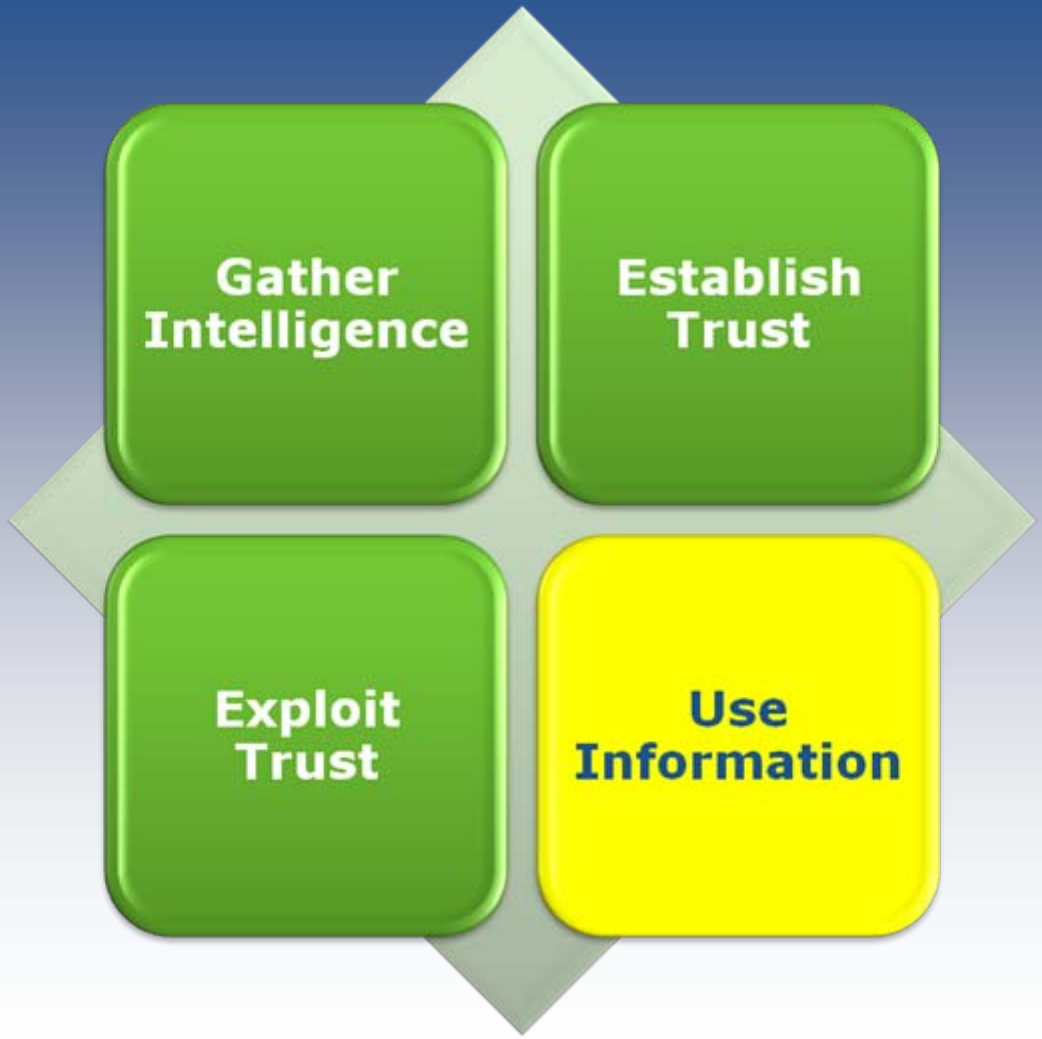
Social Engineering Attack Cycle



Social Engineering Attack Cycle



Social Engineering Attack Cycle



“How do you eat an elephant?”

“One bite at a time.”

African Proverb

Social Engineering Attack Vectors

Social Engineering Attack Vectors

Attack Vector ➔ Phone

❖ Why Do They Use It?

- Low risk, high reward
- Can be used from remote locations
- Easy to conceal SE's true identity
- Hard to arrest "a voice"
- Have a detailed knowledge of phone systems

Attack Vector ➔ Phone

- **Why is it Effective?**
  - Universal target, everyone has a phone
  - Easier to deceive people over phone than in person
- **How is it Used?**
  - Find “weakest link” to gather intelligence (usually non-technical personnel)
  - Gather various pieces of seemingly innocuous information
  - Establish a relationship to use in the future

Attack Vector ➔ Phone

❖ Who is the Target?

- **Front Line / Administrative Staff**
  - Receptionist, shipping/receiving, etc.
- **Help Desk**
  - Desire to help and resolve user problems
    may override the need for security
  - SE use “lingo” to give the appearance of insider
- **Anyone with Information**
  - Budget, R&D, Financial, Marketing, and Personnel Departments

Social Engineering Attack Vectors

Attack Vector ➔ Personal/Face-to-Face

- **Social engineer physically enters premises and interacts with personnel**
  - Manipulates, cons, or coerces to get information or further access

- **Yields invaluable information, but at a high risk**
  - Can lead to identification and possible arrest
  - Usually a last resort

Attack Vector ➔ Personal/Face-to-Face

- **Employed by highly skilled SE's**
  - Experts in use of psychological triggers as well as:
    - Spying
    - Piggybacking
    - Shoulder surfing
    - Eavesdropping
- **Vulnerable building areas:**
  - Reception
  - Mail room
  - Smoking area
  - Open office areas

Attack Vector ➔ Personal/Face-to-Face

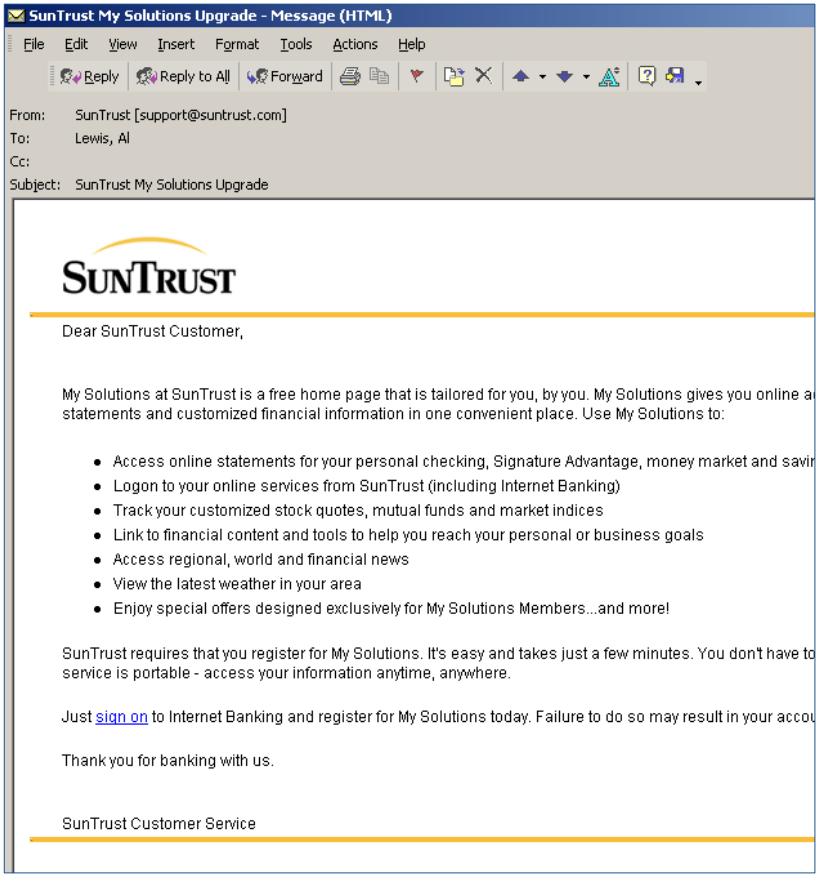
- **Surveillance**
  - Lead to key information for SE (name to be dropped in another attack, etc.)
  - Could just be eavesdropping
  - Might use listening or recording device

Social Engineering Attack Vectors

Attack Vector ➔ Online / Electronic

❖ Email

- Phishing emails appear as legitimate requests
- Low-risk, can emanate from non-US source; beyond legal bounds
- Can be distributed to:
  - Mass audience
    - Phishing
  - Specific target
    - Spear Phishing



Attack Vector ➔ Online / Electronic

- **Road Apples**
  - USB devices loaded with malware to capture information
  - Left in a location sure to be found (bathroom, elevator, sidewalk)
  - Can appear to be legitimate corporate device or a vendor giveaway
  - Once connected, a Trojan collects passwords, login's and and machine-specific information emailing the findings back to the attacker

Social Engineering Attack Vectors

Attack Vector ➔ Trash

- **Why do SE's Use it?**
  - Organizations throw away sensitive information without shredding
  - Low level of protection – no one is guarding the dumpster
  - Less riskier than in-person, but more than phone
  - No reasonable expectation of privacy

- **Trash dumpsters often contain valuable corporate and client information:**
  - Telephone lists
  - Organization charts
  - Account numbers
  - User IDs

Social Engineering Attack Vectors

Attack Vector → Reverse

- **Reverse Social Engineering**
  - Attacker creates situation where victim requests help from the attacker
    - Hacker deletes user files, offers to assist user in recovery
- **Pop-ups (Dialog boxes)**
  - Electronic messages offering help
    - Virus removal
- **Relies upon trust and sense of urgency**

Attack Vector ➔ Summary

- Everyone has information - Everyone can be an SE target
- Social engineer will chose lowest risk to get information from “weakest link”
- Social engineer will use human weaknesses to get pieces of the puzzle
- With aggregated information, a social engineer can accomplish their goal

The Deception…

- Most information security practitioners have an engineering background
- Strong bias toward resolving most security problems with technical controls

“You can have the best firewalls, encryption tools and such in place, but they will neither detect nor protect you from a social engineering attack.”

Kevin Mitnick

The Lies…

- Successfully conducting SE attacks requires great skill
- Like malicious hacking, to succeed at SE, you need sophisticated tools (listening devices, micro cameras, etc.)
- Only foolish people are susceptible to SE attacks
- Our security program is strong enough –
  We don't need a separate focus on social engineering

The Truth…

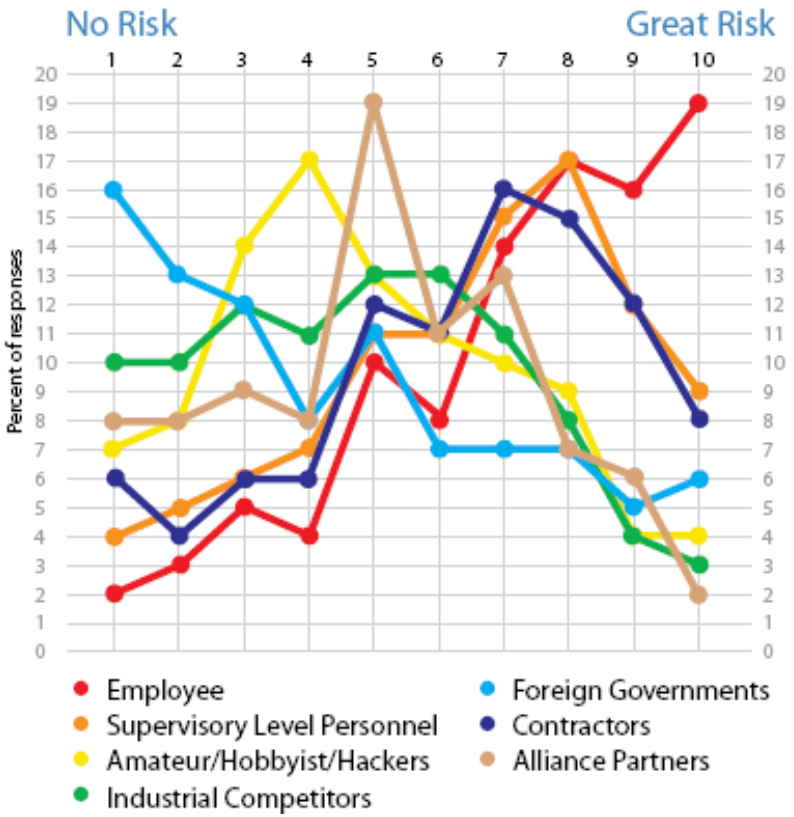
- Your biggest security threat and vulnerability is people
- Not just people…your people…maybe even you
- Your users are vulnerable to social engineers
- They may also be social engineers
  - Misuse of authority to access sensitive information
  - When no one is looking what are they seeing?
  - Senior managers who violate security policy

Insider Threat

- When asked to rank a list of categories in terms of the threat to the organization's information systems:

600 ISSA members ranked *employees* as the *greatest risk*

ISSA End Point Security Survey
ISSA Journal, September 2007, page 20



CIO/CSO Global Security Survey

"This year marks the first time employees beat out hackers as the most likely source of a security incident."

CSO Magazine, October 2007
Global Security Survey, page 32

CIO

Likely Sources of Incidents

Recognition of the insider threat is a sign that awareness is increasing, largely due to the controls that have been put in place over the past five years.

WHO ATTACKED US?

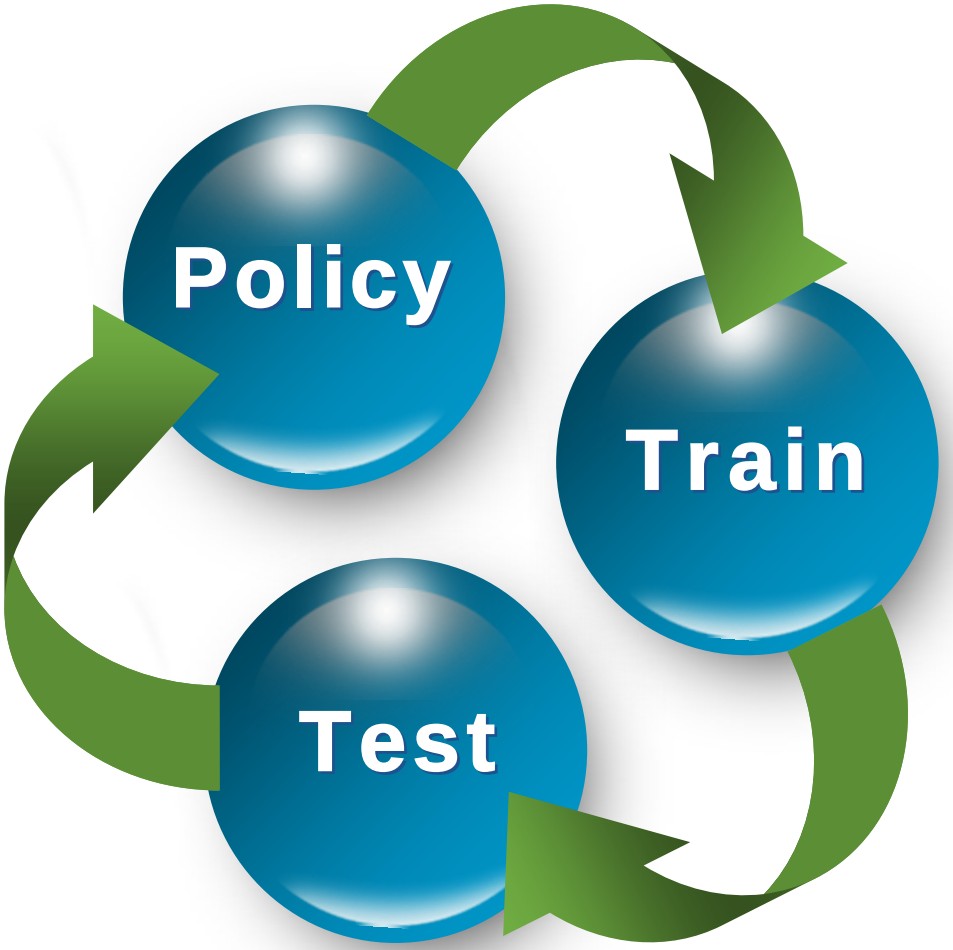
	2006	2007	2007 Security Executives Only
Employee/former employee	51%	69%	84%
Hacker	54%	41%	40%

Our Challenge

❖ Lead by Example

- Security managers and practitioners
  - Implement standards and guidelines for countering social engineering in your organization
- We're all in this together
  - "Catch them doing right"
- Employees will follow SE policies to a greater degree if they understand why it's critical

A Plan for Combating Social Engineering



A Plan for Combating Social Engineering

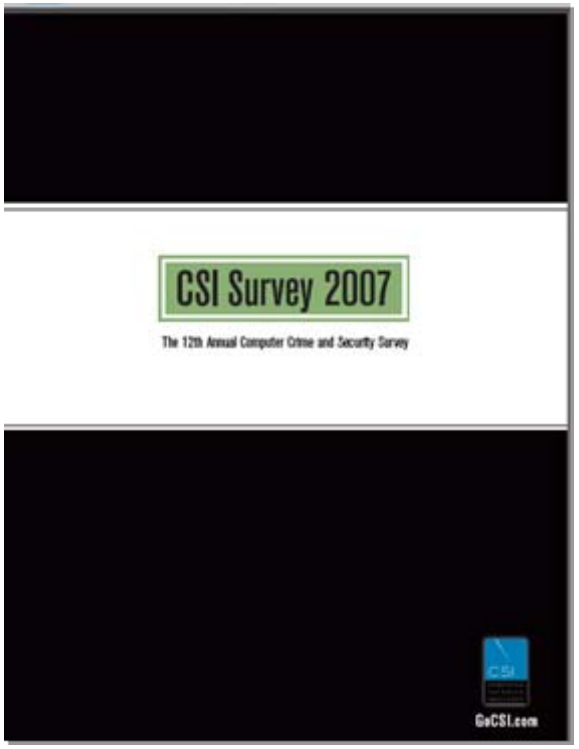
- **Policy**
  - Conduct a thorough policy review
    - Confronting strangers
    - Call-back policy
    - No piggyback policy
    - Helpdesk procedures
- **Identify areas of policy needing improvement**
  - Passwords are personal
  - Secure all entrances
    - Loading dock (smoking area)

A Plan for Combating Social Engineering

- **Training**
  - No one is immune to social engineering
  - Minimize probability of social engineering success by including SE training as part of annual security awareness training for entire staff
- **Scenario-Based, Role-Based**
  - Training that is tied directly to the employee's role and that involves scenarios will be most effective

Social Engineering Testing

- **CSI Survey 2007 respondents indicated:**
  - 13% test the effectiveness of the training by checking whether employees can detect internally-generated **social engineering** attacks
  - The vast majority of respondents do not practice regular social engineering testing



Social Engineering Testing

❖ Know Thy Enemy; Know Thyself

- The best way to measure the effectiveness of your security controls against social engineering is to test them

❖ SE Vulnerability Assessment

- Tailored assessment, using specific attack vectors and techniques agreed upon in advance

❖ Results

- Used to identify weaknesses
- Should be kept confidential

Sun Tzu
c. 544 – 446 BC

Thank You

Albert Lewis
Albert.Lewis@SecureITSolutions.US

Secure IT Solutions

2010 Corporate Ridge
Suite 700
McLean, VA 22102
Phone: 703-749-1496
Fax: 703-749-7719

References

- Robert Cialdini, Ph.D., “Influence: The Psychology of Persuasion,” HarperCollins, New York, NY, 2007.
- Kevin Mitnick and William Simon, “The Art of Deception,” Wiley Publishing, Indianapolis, IN, 2002.
- David Lieberman, Ph.D., “Get Anyone to Do Anything,” St. Martin’s Press, New York, NY, 2000.
- Charles Lively, “Psychological Based Social Engineering,” December 2003. SANS Institute. Accessed: September 19, 2007. http://www.giac.org/certified_professionals/practicals/gsec/3547.php
- Sarah Granger, “Social Engineering Fundamentals: Part I”. Security Focus. December 2001. Accessed: September 19, 2007. http://www.securityfocus.com/infocus/1527
- Sarah Granger, “Social Engineering Fundamentals: Part II”. Security Focus. January 2002. Accessed: September 19, 2007. http://www.securityfocus.com/infocus/1533
- Jonathan J. Rusch, “The Social Engineering of Internet Fraud,” 1999. Accessed: September 19, 2007. http://isoc.org/inet99/proceedings/3g/3g_2.htm
- NISCC, “Social engineering against information systems: What is it and how do you protect yourself?” June 2, 2006. Accessed: September 19, 2007. http://www.cpni.gov.uk/Docs/SocialEngineering08a06.pdf
- Robert Vamosi, “Don’t Be Duped By Hackers Without Computers.” CNET Reviews Security Watch. March 15, 2004. Accessed: September 19, 2007. http://reviews.cnet.com/4520-3513_7-5125804-1.html