Social Engineering

TOPICS

- Social Engineering Concepts
- Social Engineering Techniques
- Identity Theft
- Social Network Impersonation
- Social Engineering Countermeasures

WHAT IS SOCIAL ENGINEERING?

- The art of influencing / manipulating / convincing people to reveal confidential information
- Targets weakness of people to be helpful
- Exploits human oversight
- Relies on a lot of information being gathered from reconnaissance
  - employee names and contact info
  - Detailed job postings

ORGANIZATION VULNERABILITY FACTORS

- Insufficient security training
  - employees may not be aware that they are already targeted
- Lack of security policies
  - No rules on what can be shared or how things should be done
- Easy access to information
  - Sensitive data may be too accessible to employees

WHY IS IT EFFECTIVE?

- Humans are the most susceptible factor even if you have a strong security policy
  - Too trusting
  - Ignorance
  - Moral obligation
- Attempts are difficult to detect
- No method to ensure complete security
- No protection through hardware or software

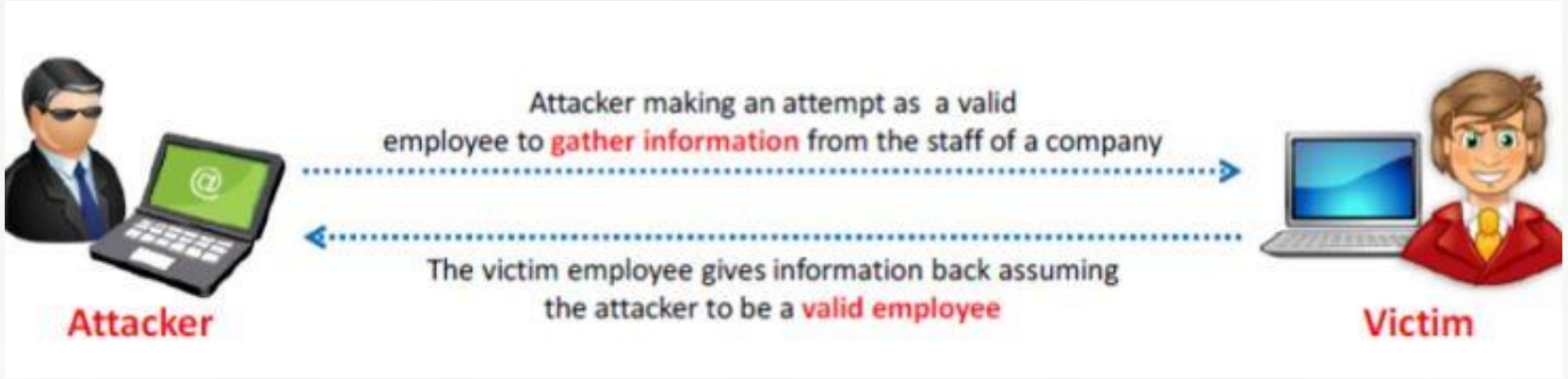
ATTACK PHASES

1. Research the target
   - Website footprinting
   - Dumpster diving
2. Select victim
   - Identify disgruntled employees ← easy target
   - Do in depth research
3. Build the relationship
4. Exploit the relationship

COMMON TARGETS

- Receptionists
- Tech Support Executives
- System Administrators
- Vendors of the Organization
- Users and Clients

COMMON TARGETS



Hackers try to extract sensitive data such as

- Security policies
- Sensitive documents
- Passwords
- Office network infrastructure

TYPES OF SOCIAL ENGINEERING

Human Based	• Gathers info through interaction • Exploits trust, fear or helpful nature • Ex: Impersonation
Computer Based	• Uses a computer and Internet systems to extract information • Ex. Phishing, Fake mail
Mobile Based	• Carried out through mobile apps • Ex. Publishing fake apps, SMS

HUMAN-BASED SOCIAL ENGINEERING

- Posing as legitimate user
  - Give identity and ask for sensitive info
  - “Hello, this is John from Department X. I forgot my password. Can I get it?”
  - Take advantage of reciprocation
- Posing as important person
  - Posing as a VIP, valuable customer, etc..
  - “Hi I’m John, CEO secretary. My boss just sent me to get those audit documents from you. Will you please provide them to me?
  - People usually don’t question authority
  - Hoping to get favors from higher ups

HUMAN-BASED SOCIAL ENGINEERING

- Posing as tech support
  - Call as technical staff, make up a nonexistent problem, then ask for ID and password
  - “Sir, this is John, tech support from company X. We just experienced a system crash and we need to check if your data is intact. Can you provide me your credit card number so that I can check your account?”
  - Exploits people who are not technically proficient

HUMAN-BASED SOCIAL ENGINEERING

- Eavesdropping
  - Unauthorized listening of conversation
- Shoulder surfing
  - Using observation techniques to get PINs, passwords, account numbers, etc.
- Dumpster diving
  - Looking for treasure in trash, e.g. financial information, contact information, bills

HUMAN-BASED SOCIAL ENGINEERING

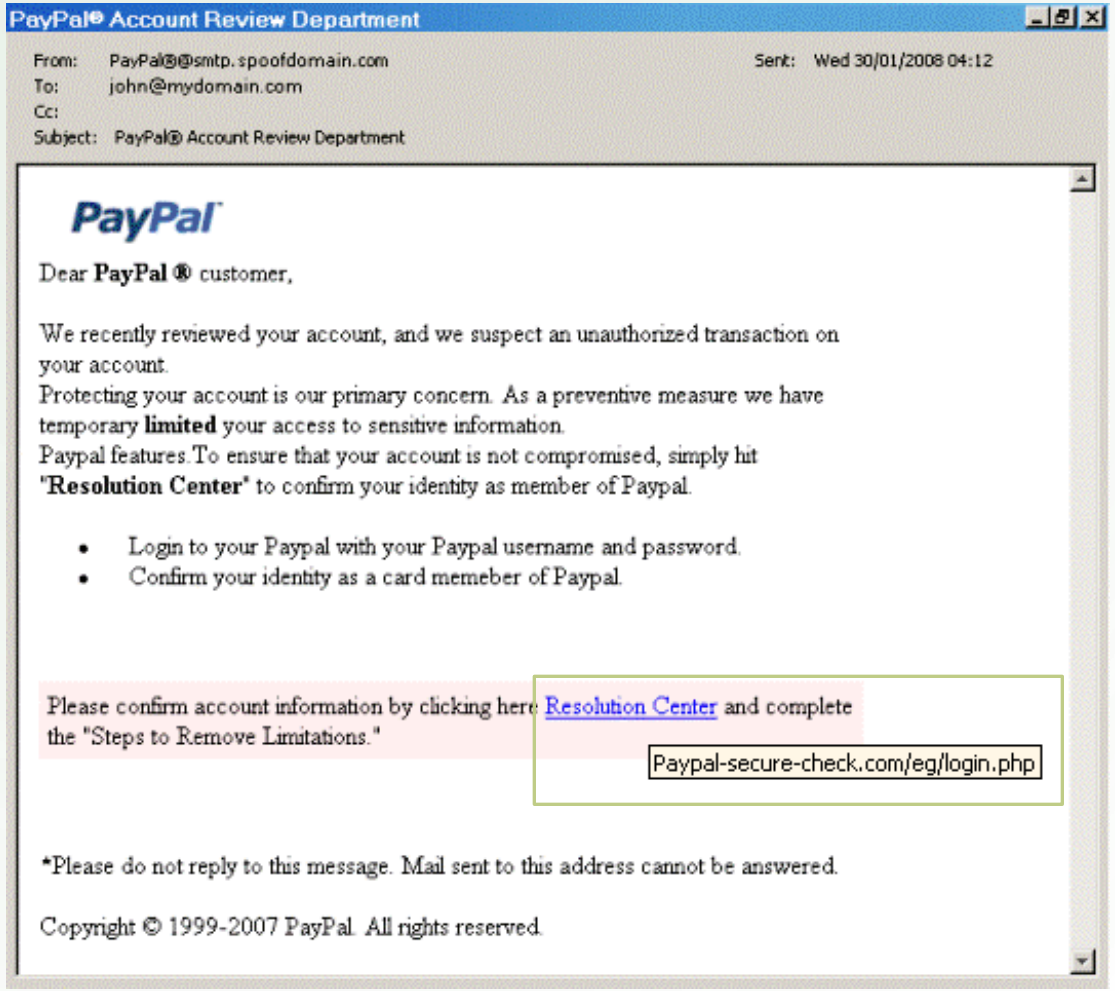
- Tailgating / Piggybacking
  - Unauthorized person closely following an authorized person through a secured entrance
- In person
  - Physically survey a secured area by posing as a janitor, customer etc.
- Reverse Social Engineering
  - Posing as a person oh high authority and give wrong info on person in order to sabotage

COMPUTER-BASED SOCIAL ENGINEERING

- Pop Ups
  - Trick people into clicking on a link that leads them to a page asking for personal info or downloads malware

COMPUTER-BASED SOCIAL ENGINEERING

- Phishing
  - Attacker usually gets account or banking information using official-looking emails
- Spear phishing
  - A form of phishing that targets specific people



MOBILE-BASED SOCIAL ENGINEERING

- Malicious Apps
  - Create apps that intentionally have malware .
  - Download a popular app and repackage so to create a version that contains malware
- Using official-looking SMS to ask for credentials

IMPERSONATION ON SOCIAL NETWORKS

- Organization Details:
  - gather confidential info and create accounts in other's names
- Professional Details
  - Use fake profiles to create a network of friends to extract information
- Contacts and Connections
  - Look for more people for further social engineering
- Personal Details
  - Mimic behavior

EX. FACEBOOK

1. Create a fake group for employees of company X
2. Invite the real employees
3. Have them post personal info
4. Use this info for further social engineering

IDENTITY THEFT

- Occurs when someone steals personally identifiable information for malicious purposes
- Used to impersonate somebody
- Methods for stealing an identity
  - Social engineering
  - Stealing personal devices and belongings
  - Phishing
  - Mail theft


SOCIAL ENGINEERING
SPECIALIST
Because there is no patch
for human stupidity

SOCIAL ENGINEERING DEFENSES

- Train employees to safeguard passwords
- Keep secure areas properly locked
- Proper enforcement of policies
- Escort guests
- Use paper shredders
- Tight badge security
- Employee background check and proper termination
- Protect personal info from being publicized