

The Role of People in Security



Chapter 4

The Role of People in Security

- Absolute protection of computer systems and networks is not possible.
- Technology alone will not solve the security problem.
 - No matter how advanced the technology is, it will ultimately be deployed in an environment where humans exist.
 - The human element is the biggest problem to security.
- Humans:
 - Deliberately or accidentally cause security problems
 - Circumvent security mechanisms.
 - Some people will not do what they are supposed to, and will create vulnerability in an organization's security posture.

Predictability

- Predictability is the key
- Information assurance process involves technology, processes, and people
 - Any of these can cause a breakdown in the security, however:
 - **Technology is predictable** - well-designed processes are, at least, consistent
 - **Human behavior is hard to predict and control**
 - Disastrous effects of employee-based actions:
 - Organizations should have mechanisms in place to ensure the secure behavior of the employees
- A significant portion of security problems that humans can cause result from poor security practices.

Information assurance (IA) is a strategic process that involves managing risks related to the use, processing, storage, and transmission of information or data

Human Attacks

- Social engineering
- Reverse social engineering
- Phishing
- Vishing
- Piggybacking and shoulder surfing
- Hoaxes
- Dumpster diving
- Installing unauthorized hardware and software
- Access by non-employees

ocial engineering is the act of manipulating people into performing actions or divulging confidential information. It exploits human psychology rather than technical hacking techniques to gain access to systems or information.

Social Engineering

- Technique in which the attacker uses deceptive practices to
 - Convince someone to divulge information they normally would not divulge.
 - Convince someone to do something they normally wouldn't do.
- Goal :
 - To obtain the pieces of information necessary to reach the next step.
 - Done repeatedly until the ultimate goal is reached.
- Seemingly innocuous information can be used
 - Directly, in an attack
 - Indirectly, to build a bigger picture to create an aura of authenticity during an attack

Step 1: Preparation:
An attacker wants to gain access to sensitive customer data stored in a company's database. The attacker researches the company's employees and identifies a junior employee, Sarah, who has access to the database but might be less suspicious of unusual requests.

Step 2: Impersonation:
The attacker creates a fake email address and crafts an email pretending to be Sarah's supervisor, David. The email is convincing and uses language typical of David's communication style. The attacker claims that there's an urgent need to review customer data for a critical project and instructs Sarah to provide access to the database immediately.

Step 3: Manipulation:
Feeling pressured to comply with her supervisor's instructions and wanting to be helpful, Sarah follows the email's instructions and grants access to the database. Unbeknownst to her, the attacker now has access to sensitive customer information.

Step 4: Threats or Bribery (Optional):
If the attacker encounters resistance or suspicion from Sarah, they might resort to threats or bribery. For example, they could threaten to report Sarah for insubordination or offer a monetary incentive in exchange for her cooperation.

Social Engineering

- May use means other than direct contact between the target and the attacker.
- Insiders may also attempt to gain unauthorized information.
 - The insider may be more successful.
 - They have a level of information regarding the organization.
 - They can better spin a story that may be believable to other employees.
- Why social engineering is successful
 - People desire to be helpful.
 - People desire to avoid confrontation.
 - Takes advantage of humans – the weakest link in the security chain

The most effective means to stop social engineering –
Proper training and education of users, administrators, and security personnel.

Phishing

- Type of social engineering
 - Attacker pretend to be a trusted entity
 - Typically sent to a large group of random users via e-mail or instant messenger
- Typically used to obtain
 - Usernames, passwords, credit card numbers, and details of the user's bank accounts
- Preys on users
 - PayPal, eBay, major banks, and brokerage firms

Phishing is a subset of social engineering that uses fraudulent emails or messages to trick victims into revealing sensitive data or credentials

Spear Phishing & Pharming

- Spear phishing
 - Relatively new term
 - Modification to normal phishing attacks
 - Special targeting using specific information
 - Designed to trick user into believing message is genuine
- Pharming
 - Redirects the user to a bogus website
 - Appears similar to the original
 - Convinces the user to give information



Recognizing Phishing

- Analyze any e-mails received asking for personal information carefully.
- Organizations should forewarn their users.
 - Never send e-mails asking for personal information.
 - Never request passwords.
- Watch for technical or grammatical errors.
- Strange URL address

Scenario: Bank Account Vishing Scam



Vishing

- Use of **voice technology** to obtain information
 - Variation of phishing
 - Takes advantage of the trust people place in the telephone network
 - Attackers **spoof calls from legitimate entities using VoIP**
 - Voice messaging can be compromised and used in these attempts.
 - Attackers hope to obtain credit card numbers or other information for identity theft.
- Successful because
 - Individuals trust in the telephone system.
 - With caller ID, people believe they can identify who is calling them.
 - Caller ID can be spoofed.

Step 1: Preparation:

An attacker obtains a list of phone numbers associated with customers of a particular bank through various means, such as purchasing lists from the dark web or conducting reconnaissance through social media.

Step 2: Impersonation:

The attacker calls a target, posing as a representative from the target's bank. They use spoofing techniques to manipulate the caller ID to display the bank's legitimate phone number, enhancing the credibility of the call.

Step 3: Deception:

The attacker informs the target that there has been suspicious activity detected on their bank account and that immediate action is required to secure the account. They claim that to verify the target's identity and protect their funds, they need to provide sensitive information, such as account numbers, PINs, or one-time passwords (OTPs).

Step 4: Manipulation:

Using persuasive language and creating a sense of urgency, the attacker pressures the target to comply with their requests. They may threaten account suspension or financial loss if the target fails to cooperate.

Step 5: Information Extraction:

Believing they are speaking with a legitimate bank representative, the target provides the requested information over the phone. The attacker now has access to the target's bank account details and can carry out fraudulent transactions or steal funds.

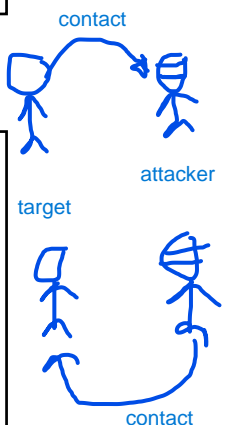
Shoulder Surfing

- Shoulder surfing
 - An attackers position themselves in such a way as to be able to observe the authorized user entering the sensitive information by
 - Looking over the shoulder of the user
 - Setting up a camera
 - Using binoculars
 - Targeted information
 - Personal identification number (PIN) at an ATM
 - Access control entry code at a secure gate or door
 - Calling card or credit card number
 - Defenses
 - Small shield to surround a keypad
 - Sophisticated systems- Scramble the location of the numbers
i.e. the top row at one time includes the numbers 1, 2, and 3 and the next time 4, 8, and 0.

Shoulder surfing is a form of social engineering attack where an individual, known as the shoulder surfer, observes or eavesdrops on another person's sensitive or confidential information, such as passwords, PINs, or personal identification numbers, without their knowledge or consent.

Reverse Social Engineering

- An alternate approach to social engineering
- The attacker hopes to convince the target to initiate the contact.
 - The attack may be successful because the target initiates the contact.
 - Attackers may not have to convince the target of their authenticity.
- Can result in increased trust
 - Trick is in convincing user to initiate contact
 - Easier to do during times of change or confusion
 - Company merges with another
 - One or more new hires that are not familiar with the company
 - New software roll out
- Not as well known as normal social engineering.
- Attacks can be extremely successful and harmful.



Initial Disruption: The attack begins with creating a problem (network outage) that affects the target's normal operations.
 Legitimate Appearance: The attacker poses as a trusted entity (IT support) offering a solution to the problem they created.
 Victim Initiation: The employees, seeking to resolve their connectivity issues, reach out to the attacker for help.
 Malicious Assistance: The attacker provides a solution that further compromises the target's security, such as installing malware.

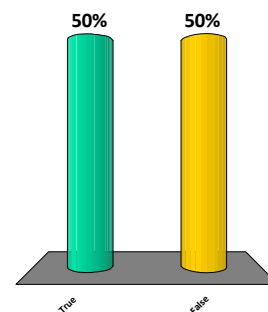
Reverse Social Engineering

- Methods of convincing the target to make the initial contact include:
 - Sending out a spoofed e-mail claiming to be from a reputable source that provides another e-mail address or phone number to call for “tech support.”
 - Posting a notice or creating a bogus Web site for a legitimate company that also claims to provide “tech support.”
- May be successful in conjunction with the deployment of a new software or hardware platform or when there is a significant change in the organization itself.

to try to make
someone believe in
something that is
not true,

Reverse social engineering involves contacting the target, eliciting some sensitive information, and convincing them that nothing out of the ordinary has occurred

1. True
2. False



Security Hoaxes

a humorous or malicious deception

- Can be very damaging if it causes user to take some action that weakens security
- Hoaxes designed to elicit user reaction
 - Delete a file
 - Change a setting
 - Spread the word
- Example:
 - A new, highly destructive piece of software that instructed users to check for the existence of a certain file and to delete it if the file was found.
 - Since the file mentioned was in reality an important file used by the operating system, deleting it caused problems the next time the system was booted.
- Defense
 - Training and awareness

Scenario: Fake Virus Warning

Description:

An employee receives an email with a subject line that reads, "Urgent: Virus Alert! Your Computer Is Infected!" The email claims to be from the company's IT department and warns employees that a dangerous virus is spreading rapidly across the organization's network.

Content:

The email contains detailed instructions for removing the supposed virus, including downloading and installing a suspicious software program attached to the email. It emphasizes the urgency of the situation and advises employees to act immediately to prevent further damage to their computers and the company's network.

Hoax Analysis:

Upon closer inspection, employees realize that the email lacks credibility and exhibits several characteristics of a security hoax:

The email is not from a legitimate IT department email address, and the sender's identity cannot be verified.

The language used in the email is sensational and alarmist, designed to provoke fear and urgency. The attached software program is unrecognized and may be malware disguised as a virus removal tool, suggesting that the threat is fabricated.

Response:

Employees report the suspicious email to the IT department, who confirms that it is indeed a security hoax. The IT department issues a company-wide communication to educate employees about recognizing and reporting security hoaxes,

Poor Security Practices

- A significant portion of human-created security problems
- Users create security problems via poor practices
 - Writing secrets down
 - Password selections
 - Piggybacking
 - Dumpster diving
 - Installing unauthorized hardware/software
- Causes
 - An individual user who is not following established security policies or processes,
 - A lack of security policies, procedures, or training within the user's organization.

write down passwords, PINs, or other sensitive information on physical notes or in easily accessible digital files.

Piggybacking occurs when an unauthorized individual follows closely behind an authorized person to gain access to a restricted area or system.



Passwords: Something You Know

- The simplest and most economical means of identifying an individual
 - Password management system will consistently:
 - Allow legitimate users to directly register for access
 - Allow forgotten passwords to be authenticated and reset by user
 - Allow IT support staff to authenticate callers for password management
 - Synchronize users across a range of platforms
 - Provide for immediate cancellation of passwords



Passwords: Something You Know

- Problem with passwords
 - Memory
 - Limitation of human memory to remember multiple passwords
 - Writing them down is a serious violation of information assurance or security protocol
 - Usage vulnerabilities
 - Short passwords – easily compromised by brute force, guessed or obtained through surreptitious means



Password Selection

- Computer intruders rely on poor passwords to gain unauthorized access to a system or network.
- Password Problems
 - Users choose passwords that are easy to remember and often choose the same sequence of characters as they have for their userIDs.
 - Users also frequently select names of family members, their pets, or their favorite sports team for their passwords.
- To complicate the attacker's job:
 - Mix uppercase and lowercase characters.
 - Include numbers and special characters in passwords.



Password Selection

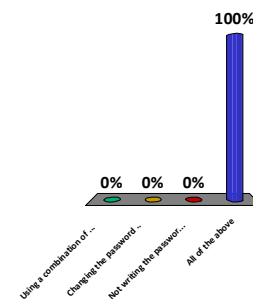
- Users tend to pick passwords that are easy for them to remember
 - Dates
 - Names
 - +1,2,3 on changes Mary1, Mary2, Mary3
- If it's easy for them to remember, it means that the more you know about the user, the better your chance of discovering their password.
- Password Dilemma
 - The more difficult we make it for attackers to guess our passwords, and the more frequently we force password changes, the more difficult the passwords are for authorized users to remember and the more likely they are to write them down.

Password Selection (*continued*)

- The rules for good password selection in general:
 - Use eight or more characters in your password
 - Include a combination of upper- and lowercase letters
 - Include at least one number and one special character
 - Do not use a common word, phrase, or name, and
 - Choose a password that you can remember so that you do not need to write it down.
 - Think of a phrase, song, poem or speech that you know by heart.
 - Use the first letter of each word in the phrase.
 - Jack be nimble, jack be quick, jack jumped over the candlestick
 - Becomes Jbnjbqjj0tcs!

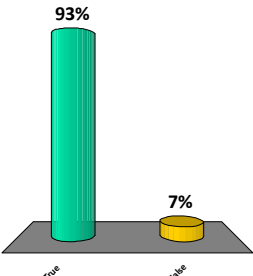
Which of the following are considered good practices for password security?

- A. Using a combination of upper- and lowercase characters, a number, and a special character in the password itself
- B. Changing the password on a regular basis
- C. Not writing the password down
- 😊 D. All of the above



The password dilemma refers to the fact that the more difficult we make it for attackers to guess our passwords, the more difficult the passwords are for authorized users to remember

1. True
2. False



Response	Percentage
True	93%
False	7%

Piggybacking

- Piggybacking
 - Related to Social Engineering Attack
 - The tactic of closely following a person who has just used an access card or PIN to gain physical access to a room or building.
 - Relies on the attacker taking advantage of an authorized user not following security procedures.
- Cause
 - People are often in a hurry and will frequently not follow good physical security practices and procedures.
 - Attackers know this and may attempt to exploit this
- Countered by
 - Training and awareness
 - Guards
 - Man trap

Dumpster Diving

- Attackers need some information before launching an attack.
- A common place to find this information is to go through the target's trash.
- This process, of going through a target's trash, is known as **dumpster diving**.
- If the attackers are fortunate and the target's security procedures are very poor, attackers may find userids and passwords.
- Manuals of hardware or software purchased may also provide a clue as to what vulnerabilities might be present on the target's computer systems and networks.
- Prevention
 - Sensitive information should be shredded. *tear or cut into shreds.*
 - Consider securing the trash receptacle.

Unauthorized Hardware and Software

- Organizations should have a policy to restrict normal users from installing software and hardware on their systems.
- Installing unauthorized communication software to allow them to connect to their machine from their home.
- Installing a wireless access point (**rogue access point**) so that they can access the organization's network from many different areas.
 - This creates a backdoor into the network and can circumvent all the other security mechanisms.
- There are numerous small programs that can be downloaded from the Internet.
 - Users cannot always be sure where the software originally came from and what may be hidden inside.

Employees may install unauthorized communication software, such as remote desktop applications or virtual private network (VPN) clients, to access their work machines from home for various reasons:

behaving in ways that are not expected or not normal, often in a way that causes damage

Employees may install rogue access points to create their own wireless networks within the organization's premises, allowing them to access the organization's network from multiple locations.



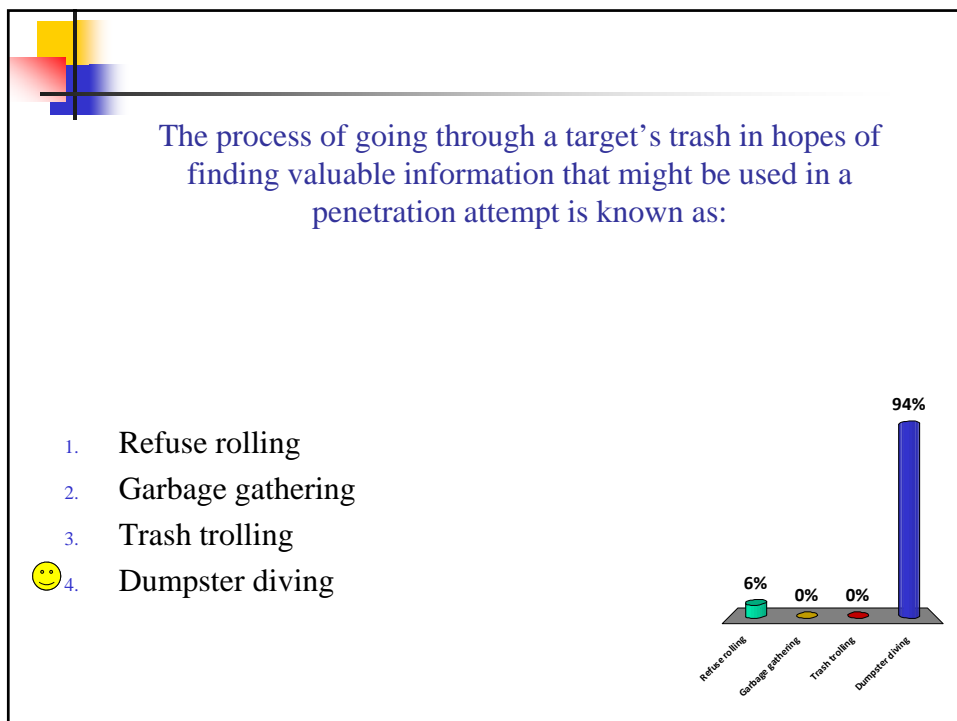
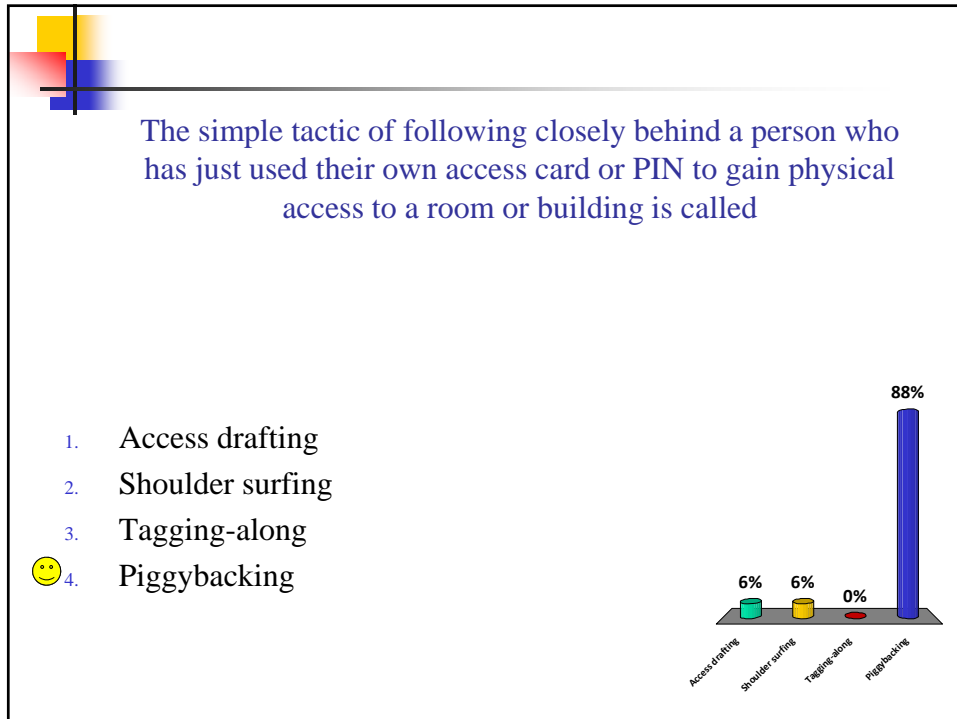
Installing Unauthorized Hardware and Software)


- Another example of unauthorized software is games.
- Many organizations **do not allow their users to load software or install new hardware without authorization.**
- Many organizations also screen, and occasionally intercept, e-mail messages with links or attachments that are sent to users.
 - This helps prevent users from unwittingly executing malware.
- Many organizations have their mail servers strip off executable attachments to e-mail so that users can't accidentally cause a security problem.



Physical Access by Non-Employees

- If an attacker can gain physical access, the attacker can penetrate the computer systems and networks.
- Physical access provides opportunity for individuals to look for critical information carelessly left out.
- With the proliferation of devices such as cell phones with built-in cameras, an individual could easily photograph information without it being obvious to employees.
- **One should examine who has legitimate access to a facility.**
- Prevention
 - Many organizations require employees to wear identification badges at work.
 - This method is easy to implement and may be a deterrent to unauthorized individuals.
 - It also requires that employees challenge individuals not wearing identification badges.






People as a Security Tool

- People-
 - The biggest problem and security risk, but also the best tool to defend against these attacks.

- Employees' responsibilities:
 - Recognize the type of information that should be protected.
 - Recognize how seemingly unimportant information may be combined with other information to divulge sensitive information (also known as data aggregation).



People as a Security Tool

- People can be an effective security mechanism.
 - Policies and procedures
 - Training and awareness
 - Many eyes
 - Challenge visitors
 - Report abnormal conditions

- Make everyone responsible and involved.



Security Awareness

- Organizations' role
 - Establish policies and procedures that define roles and responsibilities for all users and not just security personnel.
 - Conduct an active security awareness program for the organization's security goals and policies.
 - Depends on the organization's environment and the level of threat.
 - An active security awareness program will vary depending on
 - The organization's environment
 - The level of threat
 - Emphasize the type of information that the organization considers sensitive and that may be the target of a social engineering attack.



Individual User Responsibilities

1. Lock doors
2. No sensitive information in your car
3. Secure storage media containing sensitive information.
4. Shred sensitive documents before discarding.
5. Do not divulge sensitive information to individuals not authorized to know it.
6. Do not discuss sensitive information with family members.
7. Protect laptops that contain the organization's information.
8. Be aware of who is around you when discussing sensitive information.
9. Enforce corporate access control procedures.
10. Report suspected or actual violations of security policies.
11. Follow procedures established to enforce good password security practices.

Rules of Behavior

- Users must be aware of acceptable behavior and understand the consequences of noncompliance
 - Consequences should be spelled out and enforced through a set of rules of behavior
 - They should be in writing
 - They should delineate the responsibilities and expectations for each individual clearly
 - Everyone should understand the rules before they are allowed access
 - They have to be rigorous to ensure security, while giving enough flexibility to perform the jobs properly

An active security awareness program is an effective way of countering potential social engineering attacks

- 😊 1. True
2. False

