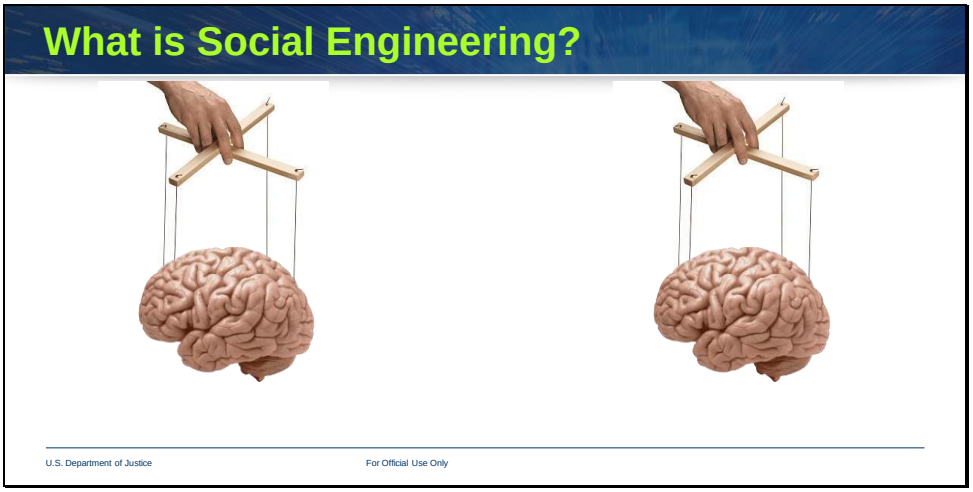
Cybersecurity Awareness Month

Social Engineering

Andy Thompson, SSCP, CISSP, GPEN

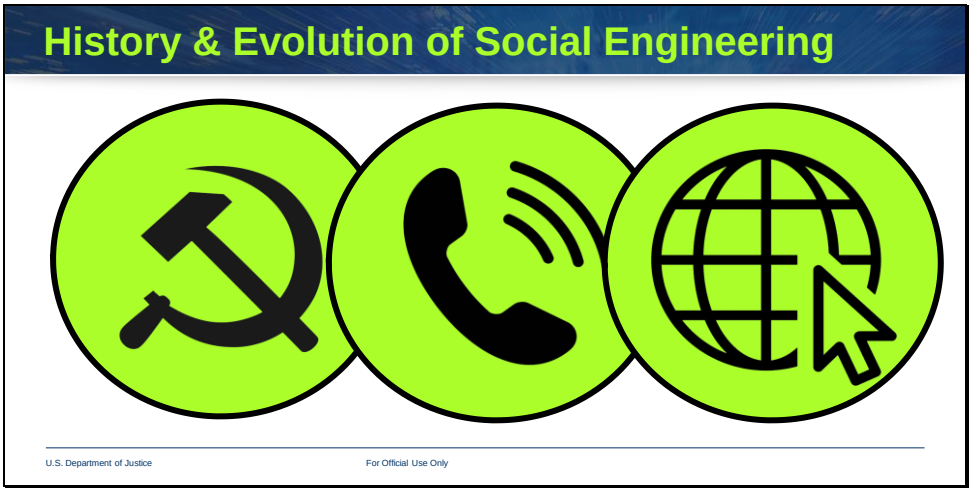
October 16, 2024

U.S. Department of Justice



Social Engineering

- The exploitation of human psychology and behavior for deceptive purposes.
- Manipulating individuals into divulging sensitive information or performing compromising actions.
- A tactic employed throughout history, but more prevalent in the digital age.
- Can occur both digitally and physically.



- Social engineering has been a part of human interaction for centuries.
- Manipulating people for personal or strategic gain is a timeless tactic.

Cold War Espionage

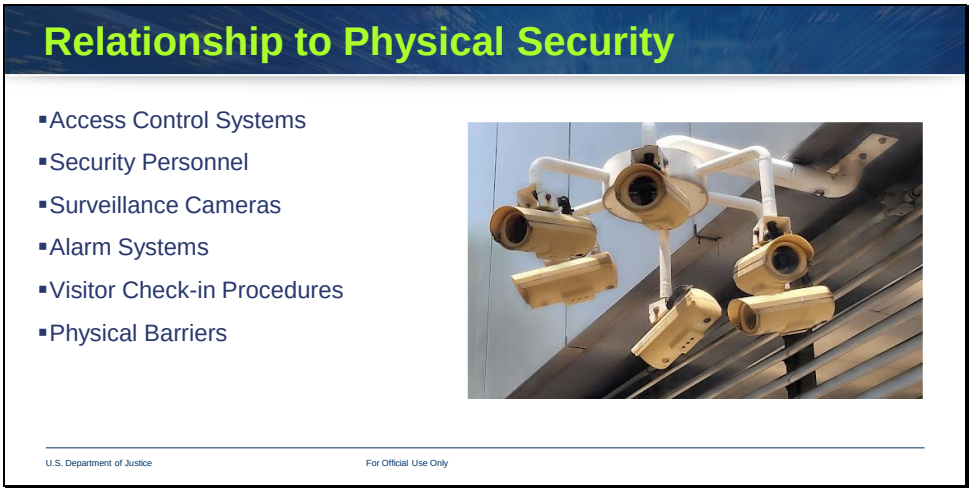
- Intelligence agencies used social engineering to recruit spies and gather intelligence.
- Spies and double agents employed trust, coercion, and persuasion to manipulate individuals.

Computer Hacking and Phreaking

- Early hackers and phreaks used social engineering to gain unauthorized access.
- Impersonation, trust exploitation, and manipulation of employees were common tactics.

Social Engineering and the Internet

- Phishing attacks emerged with the rise of the internet.
- Attackers sent deceptive emails to trick individuals into revealing sensitive information.
- This tactic has become more advanced and widespread over time.



Access Control Systems

- Manipulating individuals to bypass card readers, biometric locks, etc.

Security Personnel

- Deceiving guards or receptionists through trust exploitation or impersonation.

Surveillance Cameras

- Evading detection by appearing legitimate or exploiting blind spots.

Alarm Systems

- Convincing employees to disable alarms or delaying responses.

Visitor Check-In Procedures

- Impersonating visitors or contractors to gain unauthorized access.

Physical Barriers

- Manipulating individuals to open doors, gates, or bypass barriers.

Authentication and Access Controls

- Tricking individuals into revealing credentials or bypassing MFA.

Firewalls and Intrusion Detection Systems

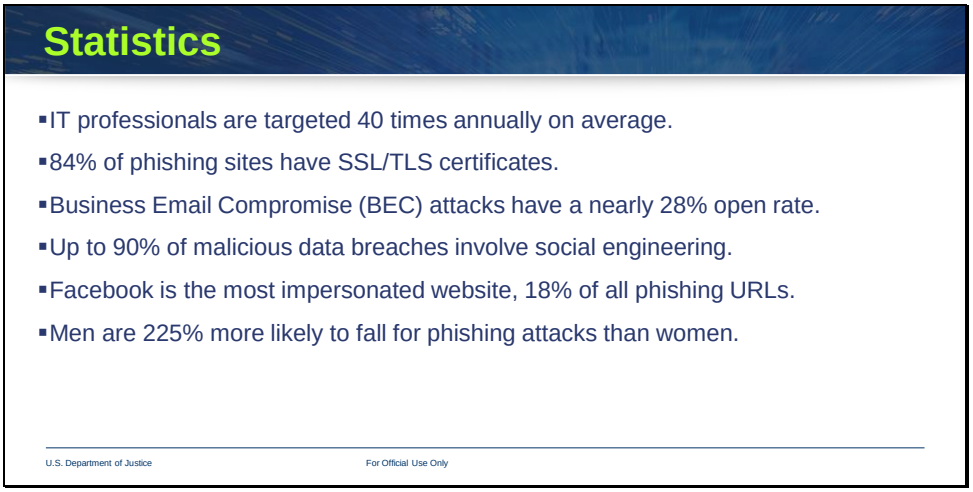
- Convincing users to introduce malware or compromise network security.

Data Encryption

- Stealing encryption keys or obtaining sensitive information before encryption.

Security Policies and Procedures

- Manipulating employees into violating policies or bypassing procedures.



IT Professionals as Targets

- IT professionals are targeted an average of 40 times annually.
- They have higher access privileges, making them attractive targets.

Phishing Sites and SSL Certificates

- 84% of phishing sites have SSL certificates, falsely implying security.

Business Email Compromise (BEC) Attacks

- BEC attacks have a high open rate of nearly 28%.
- Masquerading as trusted entities is highly effective.

Social Engineering and Data Breaches

- Up to 90% of malicious data breaches involve social engineering.
- Tricking employees is often easier than brute force attacks.

Most Impersonated Website

- Facebook is the most impersonated website, representing 18% of phishing URLs.

Gender Disparity

- Men are 225% more likely to fall for phishing attacks than women.

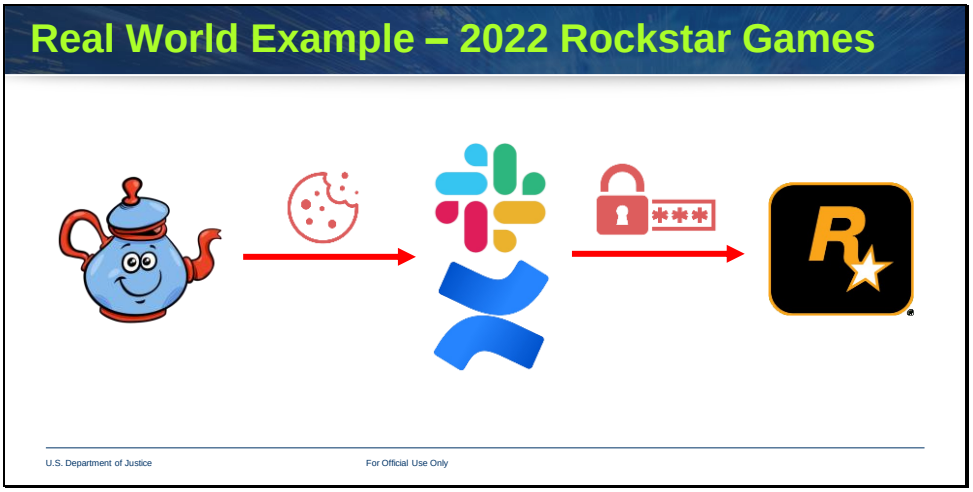
- In July 2020, Twitter experienced a major social engineering attack.
- Hackers targeted high-profile accounts (politicians, celebrities, companies).
- They gained access to Twitter's internal tools through social engineering.

Exploiting Trust and Access

- Hackers used their access to post fraudulent tweets from compromised accounts.
- These tweets promoted a Bitcoin scam, promising high returns.

Impact and Response

- The scam garnered approximately $121,000 for the attackers.
- Twitter had to temporarily block verified accounts and Bitcoin wallet links.



A Major Gaming Leak

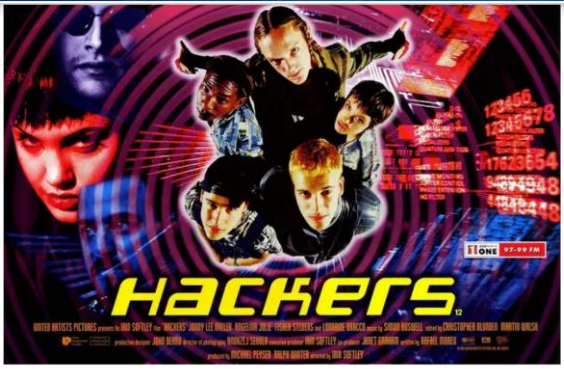
- Rockstar Games, the developer behind GTA, was targeted in September 2022.
- A hacker named Teapot exploited social engineering to gain access.

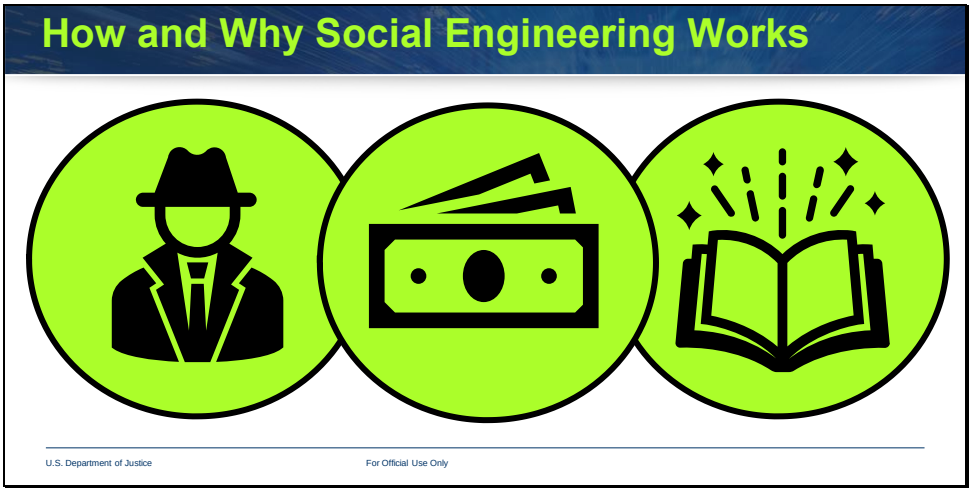
The Hack's Impact

- Teapot obtained GTA 5 and GTA 6 source code, along with other assets.
- Leaked videos were widely circulated online, despite takedown efforts.

How it Happened

- Teapot hijacked an employee's Slack application.
- Through impersonation, they obtained login credentials from another employee.


Hackers
ONE 97-99 FM



Government Espionage

- Obtaining classified information or disrupting rival nations.
- Compromising national security through manipulation.

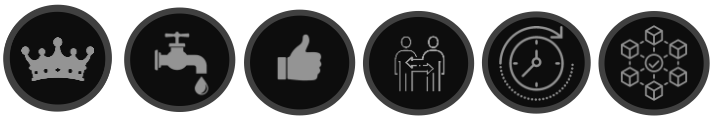
Corporate Data and PII

- Stealing trade secrets, intellectual property, or customer information.
- Gaining competitive advantage, selling data on the black market, or exploiting for financial gain.

Financial Gain

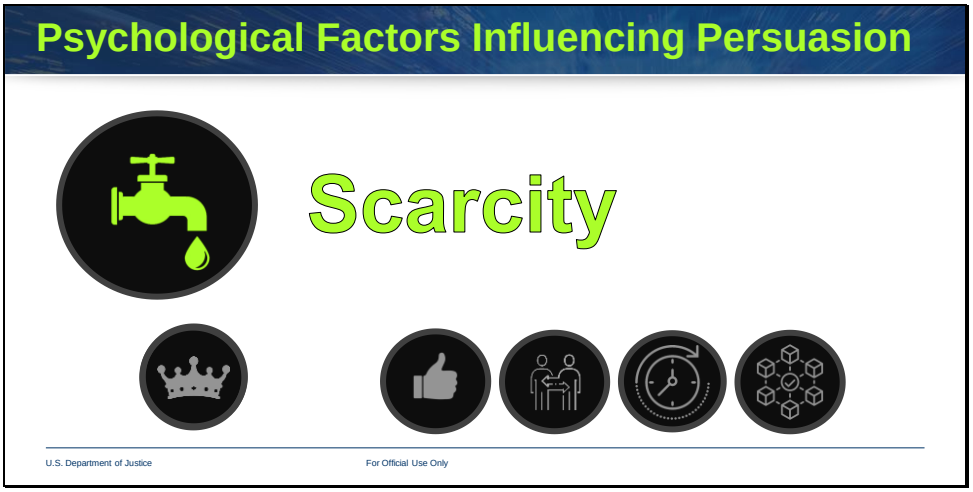
- Tricking individuals into revealing financial information.
- Carrying out fraudulent activities, unauthorized transactions, or identity theft.

Psychological Factors Influencing Persuasion



Authority

- People tend to follow authority figures without question.
- Social engineers may impersonate authority figures to gain trust and compliance.

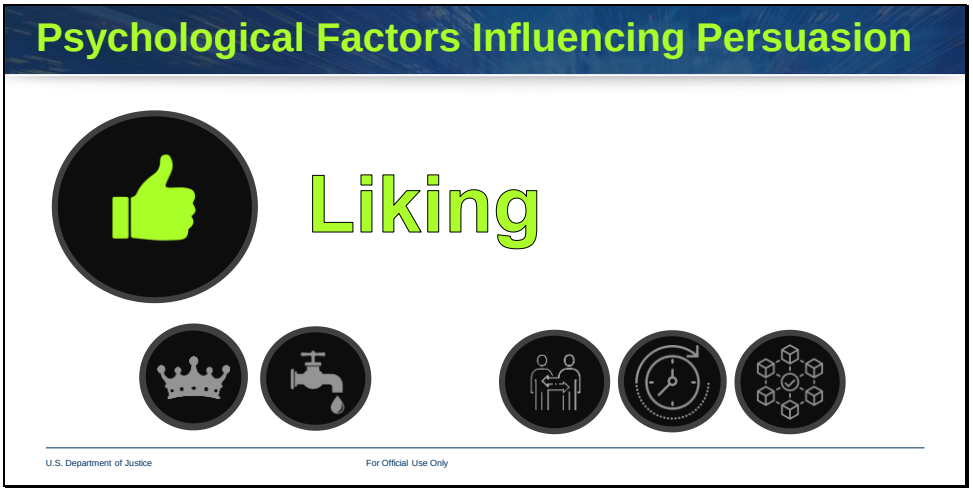


Scarcity

- Exploits the fear of missing out (FOMO).
- Creates a sense of urgency or limited availability.
- Can prompt impulsive decisions without careful consideration.

Example:

- A social engineer convinced a victim of a fake bank account scam, claiming urgent action was needed to prevent financial loss.

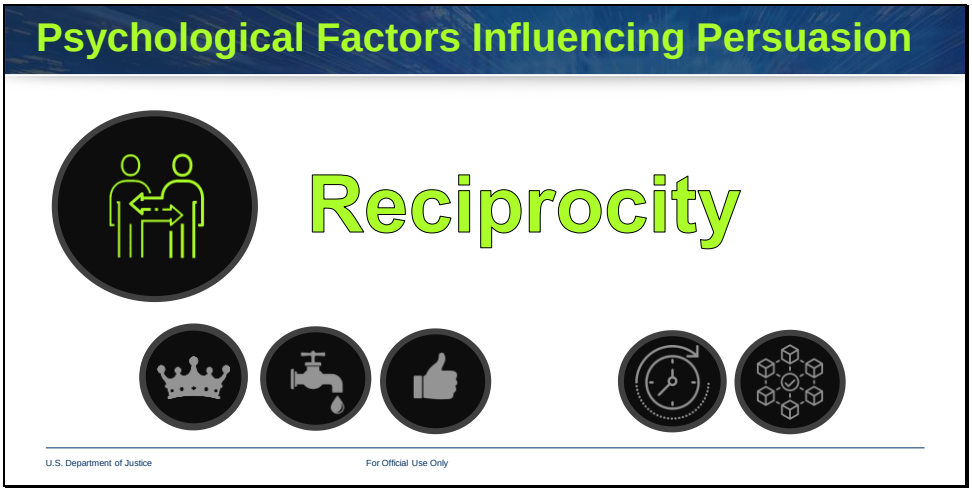


Liking

- Building rapport and likability increases compliance.
- Social engineers may use flattery, mimicry, or empathy to establish a positive connection.

Example:

- Showing genuine interest in a target's hobbies or interests can foster trust and cooperation.



Reciprocity

- People feel obligated to return favors or goodwill.
- Social engineers may initiate small acts of kindness to create indebtedness.

Examples:

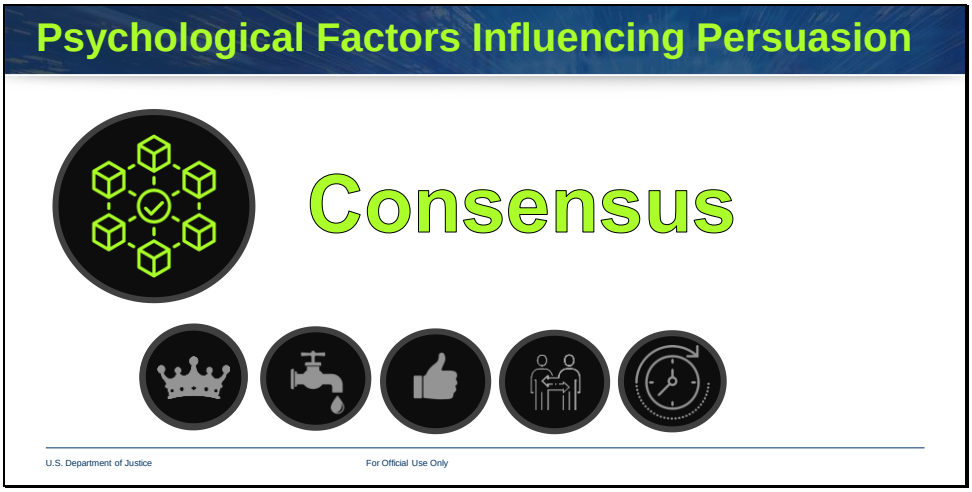
- Offering help with a task to create a sense of obligation.
- Buying a drink or covering expenses in a social setting.

Commitment and Consistency

- People tend to remain consistent with past actions and statements.
- Social engineers encourage initial commitments to influence future behavior.

Example:

- Obtaining a small initial agreement can lead to greater compliance with subsequent requests.



Consensus

- People look to others for guidance and validation.
- Suggesting widespread acceptance can influence decision-making.

Example:

- Claiming that many others have already taken a particular action to encourage conformity.

Tailgating

- Following closely behind authorized individuals to gain entry.
- Exploiting the tendency to hold doors open or using distractions.

Tip: Use an inconspicuous prop (e.g., large attaché case) to block IR beams in turnstyles.

Baiting

- Leaving physical devices (e.g., infected USB drives) to entice victims.
- Preying on greed or curiosity to encourage device interaction.

Example:

- Leaving a USB drive with a reward message to entice victims to plug it in.

Personal Appeals

- Leveraging emotions to manipulate individuals.
- Exploiting sympathy, urgency, or shared interests to gain trust.

Example:

- A pregnant woman using sympathy to gain access to restricted areas.

Impersonation

- Posing as someone else to gain trust and access.
- Using uniforms, fake IDs, or other props to appear legitimate.

Example:

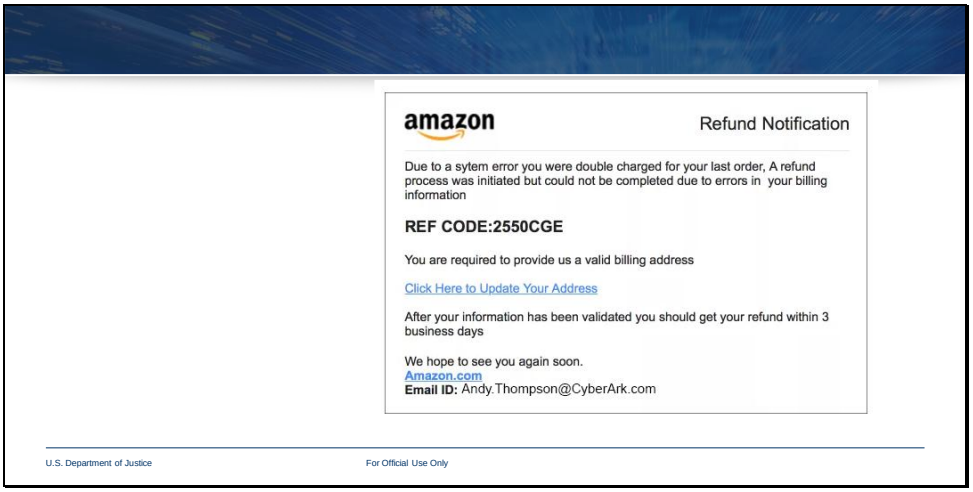
- A woman using a fake pregnancy prop to gain sympathy and access.

Pretexting

- Creating a fabricated scenario to obtain information or access.
- Posing as repair technicians, inspectors, or other personnel.

Example:

- Claiming to be a repair technician to gain access to a restricted area.



Phishing

- The most common social engineering tactic.
- Tricking individuals into opening attachments, clicking links, or logging in.

Example:

- A phishing email claiming to be from a bank, asking for account information.

Smishing

- Phishing via text message.
- Increasingly using images and QR codes to enhance credibility.

Example:

- A text message with a link to a fake website, claiming a special offer.

Vishing

- Phishing via phone calls.
- Can be highly effective with deepfake technology.

Example:

- A scammer impersonating a bank representative to obtain sensitive information.

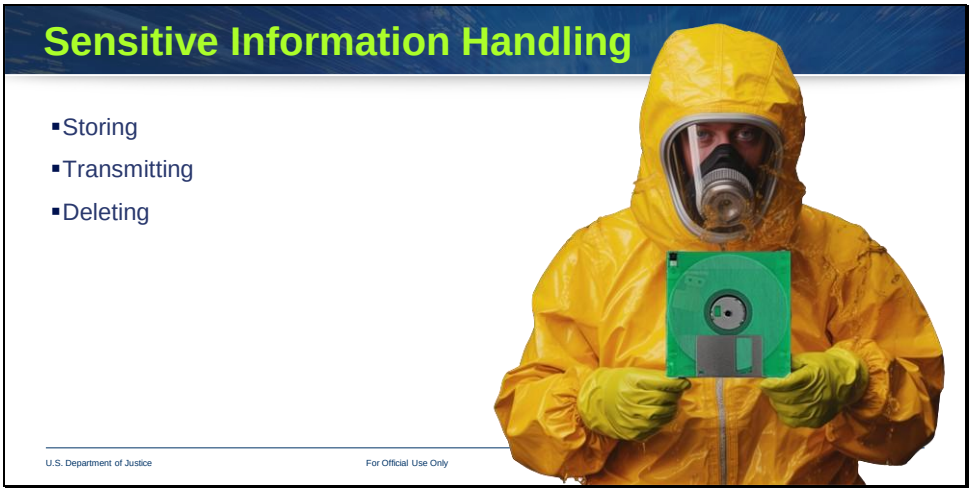
Deepfake Technology:

- AI-generated audio and video that can be indistinguishable from reality.
- Can be used to create highly convincing impersonations.

Example:

- A deepfake video of a CEO asking employees to transfer funds.

Countermeasures and Prevention



Defining Sensitive Information

- Data that, if compromised, can cause harm or loss.
- Includes personally identifiable information (PII), financial data, medical records, etc.

Encryption

- Encrypting files, databases, or storage volumes to protect data.
- Ensures that unauthorized individuals cannot decipher the data.

Secure Transmission

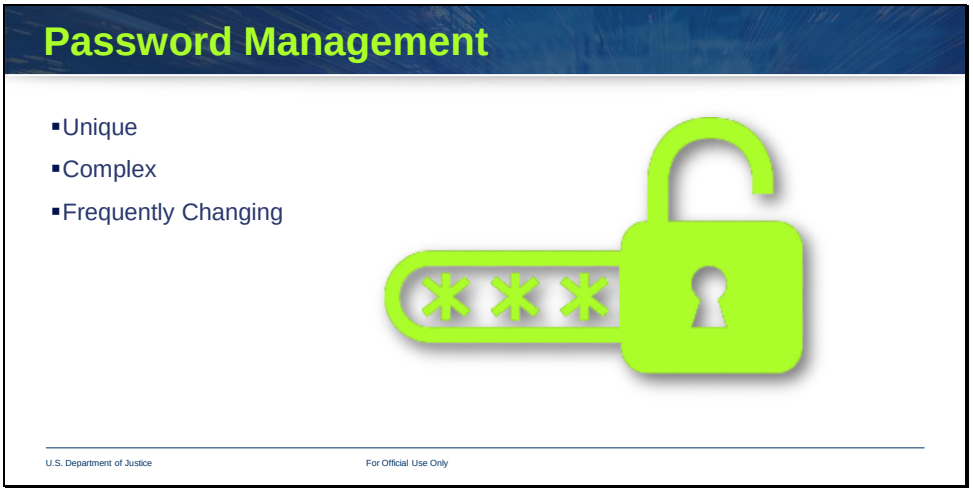
- Prioritize secure methods for transmitting sensitive information.
- Use protocols that protect data during transfer.

Disposal of Sensitive Information

- Establish clear guidelines for proper disposal.

Key Points

- Sensitive information requires robust protection.
- Encryption, secure transmission, and proper disposal are essential.
- Organizations must implement comprehensive measures to safeguard sensitive data.



Key Points

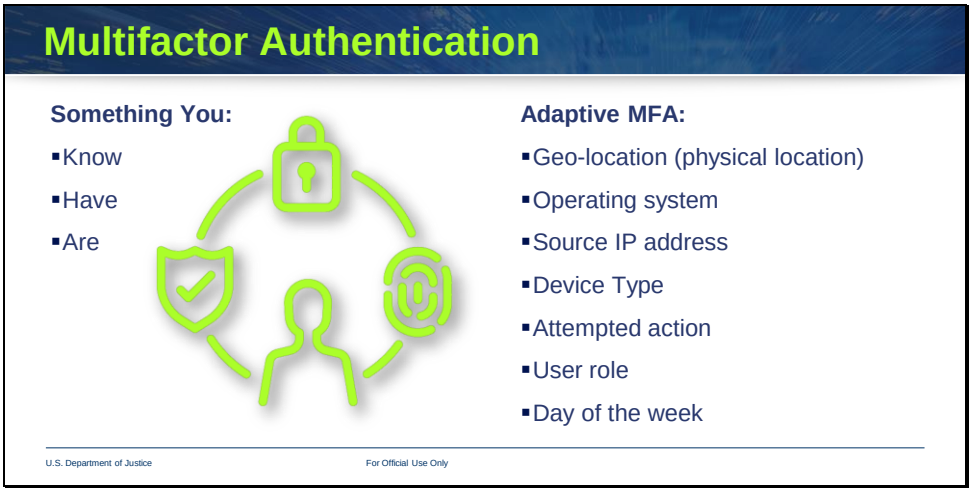
- Strong passwords are essential for security.
- Passwords should be unique, complex, and frequently changed (especially for highly privileged accounts).
- A robust password manager is crucial for managing multiple strong credentials.

Password Requirements

- **Unique:** Avoid reusing passwords across different accounts.
- **Complex:** Include a combination of uppercase and lowercase letters, numbers, and symbols.
- **Frequent Changes:** For highly privileged accounts, consider regular password updates.

Password Manager

- Use a strong password manager to securely store and manage credentials.
- Avoid weak password managers that may compromise security.
- Choose a password manager with robust features and security measures.



Enhancing Security

- MFA adds an extra layer of protection against social engineering attacks.
- Requires multiple forms of identification to validate identity.

Types of MFA

- **Something You Know:** Passwords, PINs
- **Something You Have:** Smartphones, secure USB keys
- **Something You Are:** Fingerprints, facial recognition

Avoiding Weak MFA

- **Avoid SMS-based MFA:** Vulnerable to SIM swapping.
- **Consider adaptive MFA:** Adjusts requirements based on context.

Adaptive MFA Factors

- Geo-location
- Operating system
- Source IP address
- Device type
- Attempted action
- User role
- Day of the week

Benefits of Adaptive MFA

- Provides more robust protection against unauthorized access.
- Reduces the risk of successful social engineering attacks.

Limiting Access

- Implement strict access control measures to prevent unauthorized access.
- Grant privileges based on the principle of least privilege.

Principle of Least Privilege (PoLP)

- Limit standing rights to the bare minimum.
- Ensure users have only the necessary access.

Zero Trust

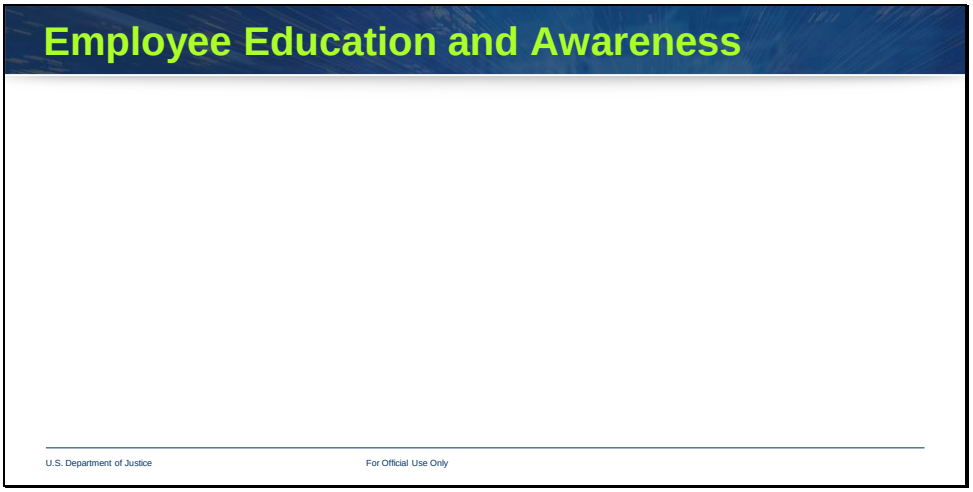
- Grant access only after authentication and verification.
- Avoid granting standing privileges.

Zero Standing Privilege (ZSP)

- Create roles on-demand as needed.
- Avoid pre-existing roles and privileges.

Benefits

- Reduces the risk of unauthorized access.
- Mitigates the impact of social engineering attacks.
- Enhances overall security posture.

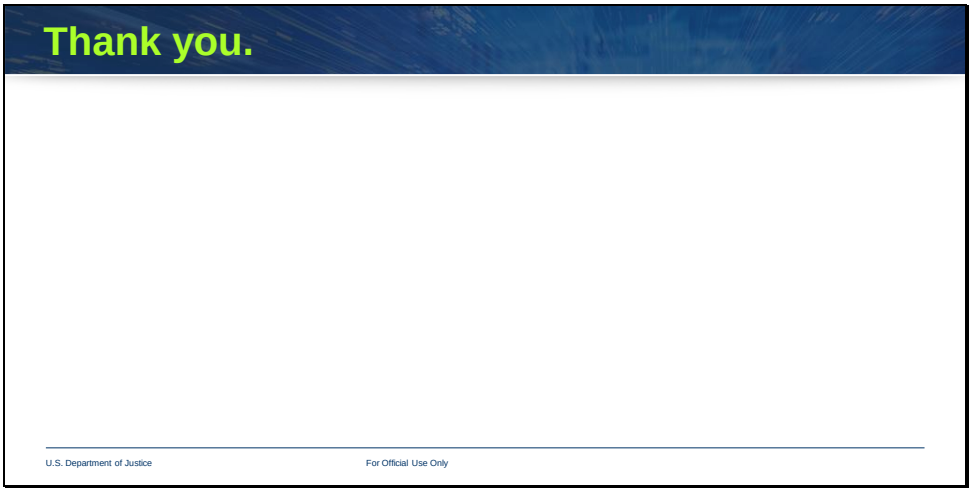


Employee Education and Awareness

- Empower employees to recognize and respond to social engineering tactics.
- Provide training on common techniques and red flags.

Key Points

- End users are not the weakest link, but a valuable asset.
- Investing in employee education strengthens security.
- Sharing knowledge and resources can help prevent social engineering attacks.



Please share this presentation with others to raise awareness and encourage colleagues and loved ones to learn about social engineering.