Social Engineering

Strathmore
UNIVERSITY

Learning Objectives

1. Social Engineering
2. Types of Social Engineering
3. Behaviors Vulnerable to attacks
4. Countermeasures for Social Engineering
5. Policies and procedures
6. Identity Theft
7. Countermeasures for Identity Theft

Phases of Social Engineering Attacks

Strathmore UNIVERSITY

Strathmore
UNIVERSITY

What is Social Engineering?

* Social Engineering is the human side of breaking into a corporate network

* it is the Tactic or trick of gaining sensitive information by exploiting the basic human nature such as Trust, Fear, Desire

* The attempt is to gain information such as Sensitive information, Authorization details, Access details

Strathmore UNIVERSITY

- An employee may unwittingly give away Key information in an email or by answering questions over the phone with someone they don’t know.

- They can talk with coworkers about a project at a local pub.

Strathmore UNIVERSITY

Social Engineering Techniques

- There's no single Security mechanism that can protect from Social Engineering Techniques used by attackers.

Strathmore UNIVERSITY

Types of Social Engineering

Human-Based Social Engineering

- Gathers information by interaction
- Attacks of this category exploits fear, trust and helping nature of people

Strathmore UNIVERSITY

- Posing as a legitimate end user
- Posing as an important user
- Posing as a Technical support
- Eavesdropping
- Shoulder surfing
- Dumpster diving

Strathmore UNIVERSITY

Tailgating

- An authorized person may be unaware of providing an unauthorized person access to a secure area.

- An unauthorized person, wearing a fake ID badge, enters a secure area by closely following an unauthorized through a door requiring key access

Piggybacking

Strathmore UNIVERSITY

- An authorized person provides access to an unauthorized person by keeping a secure door open

- “I forgot my key at home. Please hold the door ”

Strathmore UNIVERSITY

Reverse Social Engineering

- This is when the attacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way round

- Involves sabotage, marketing, providing support

Computer-based Social Engineering

Strathmore UNIVERSITY

- Carried out with the help of computers

It can be divided into:

- Mail/IM attachments
- Pop-up windows
- Websites/ sweepstakes
- Spam mail

Pop-Up windows

Strathmore UNIVERSITY

- Windows that suddenly pops-up, while surfing the internet and asks for users' Information to login or sign in

Strathmore UNIVERSITY

Hoaxes and Chain letters

- Hoax letters are emails that issue warnings To users on new virus, Trojans or worms that may harm the user's system.

- Chain letters are emails that offer free gifts such as money and software on condition that the user sends to a said number of persons

Strathmore UNIVERSITY

Instant Chat messenger

- Gathering of personal information by Chatting with a selected online user to Attempt to get information such as birth Dates and maiden names

- Acquired data is later used for cracking The user's accounts

Spam Email

Strathmore UNIVERSITY

- Email sent to many recipients without prior permission intended for commercial purposes

- Irrelevant, unwanted and unsolicited email to collect financial information, social security numbers and network information

Phishing Emails

Strathmore UNIVERSITY

- An illegitimate email falsely claiming to be from a legitimate site attempts to acquire user's personal or account information

- Lures online users with statements such As Verify your account, update your Infromation and you account will be closed or suspended

Insider Attack

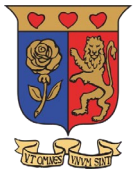
- If a competitor wants to cause damage to your organization, steal secret, or put you out of business, they just need to find a job opening, prepare a someone to pass, the interview, have that person hired and They have access.

Insider Attack Cont'

Strathmore UNIVERSITY

- 60% of attacks come from behind the Firewall and it is difficult to prevent

- It can only take one disgruntled employee wanting revenge to sell critical information.



Preventing Insider Attacks

- There is no single solution for an insider threat

Strathmore UNIVERSITY

Recommendations

- Separation of duties
- Rotation of Duties
- Least Privilege
- Controlled access
- Logging and auditing
- Legal Policies
- Archive critical data

Strathmore UNIVERSITY

Common Targets of social Engineering

- Receptionist and help desk personnel
- Technical support executives
- Vendors of target organization
- System administrators and users

Threats and Defenses

Strathmore UNIVERSITY

Major Attack Vectors used by hackers include:

- Online
- Telephone
- Personal approaches
- Reverse social engineering

Strathmore UNIVERSITY

Personal Approach Threats

- Intimidation
- Persuasion
- Ingratiation
- Assistance

Defenses Against SE Threats

Strathmore UNIVERSITY

3 steps are necessary to defend against SE threats

- Develop a security management framework
- Undertake risk management assessments
- Implement SE defenses within your security policy

Risk Assessment

Strathmore UNIVERSITY

- You need to assess the level of risk that an attack possesses towards your company for Deploying suitable measures

Risk Categories

Strathmore UNIVERSITY

- Confidential information
- Business Credibility
- Business Availability
- Resources
- Money

Factors That make Companies Vulnerable to Attacks

Strathmore UNIVERSITY

- Insufficient security training & awareness
- Several organization units
- Lack of appropriate security policies
- Easy access of information eg. Email IDs & extension numbers for employees

Why is SE Effective?

Strathmore UNIVERSITY

- Security policies are as strong as its weakest link and humans are then most susceptible factor
- Difficult to detect SE attempts
- No method to ensure complete security from SE attacks

Warning signs of an Attack

Strathmore UNIVERSITY

Attacker May:

- Show inability to give a valid callback number
- Make informal requests
- Show haste
- Unusual compliment or praise
- Show discomfort when questioned
- Threaten of dire consequences if information is not
- provided

Impact on the Organization

Strathmore UNIVERSITY

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuits and arbitrations
- Temporary or permanent closure

Countermeasures

Strathmore UNIVERSITY

- Training
- Password policy
- Operational guidelines
- Physical security policies
- Classification of information
- Access privileges
- Background check of employees and proper termination process
- Proper incidence response team

Identity theft

Strathmore UNIVERSITY

- Occurs when someone steals your name and other personal information for fraudulent purposes.

Identity Theft Countermeasures

Strathmore UNIVERSITY

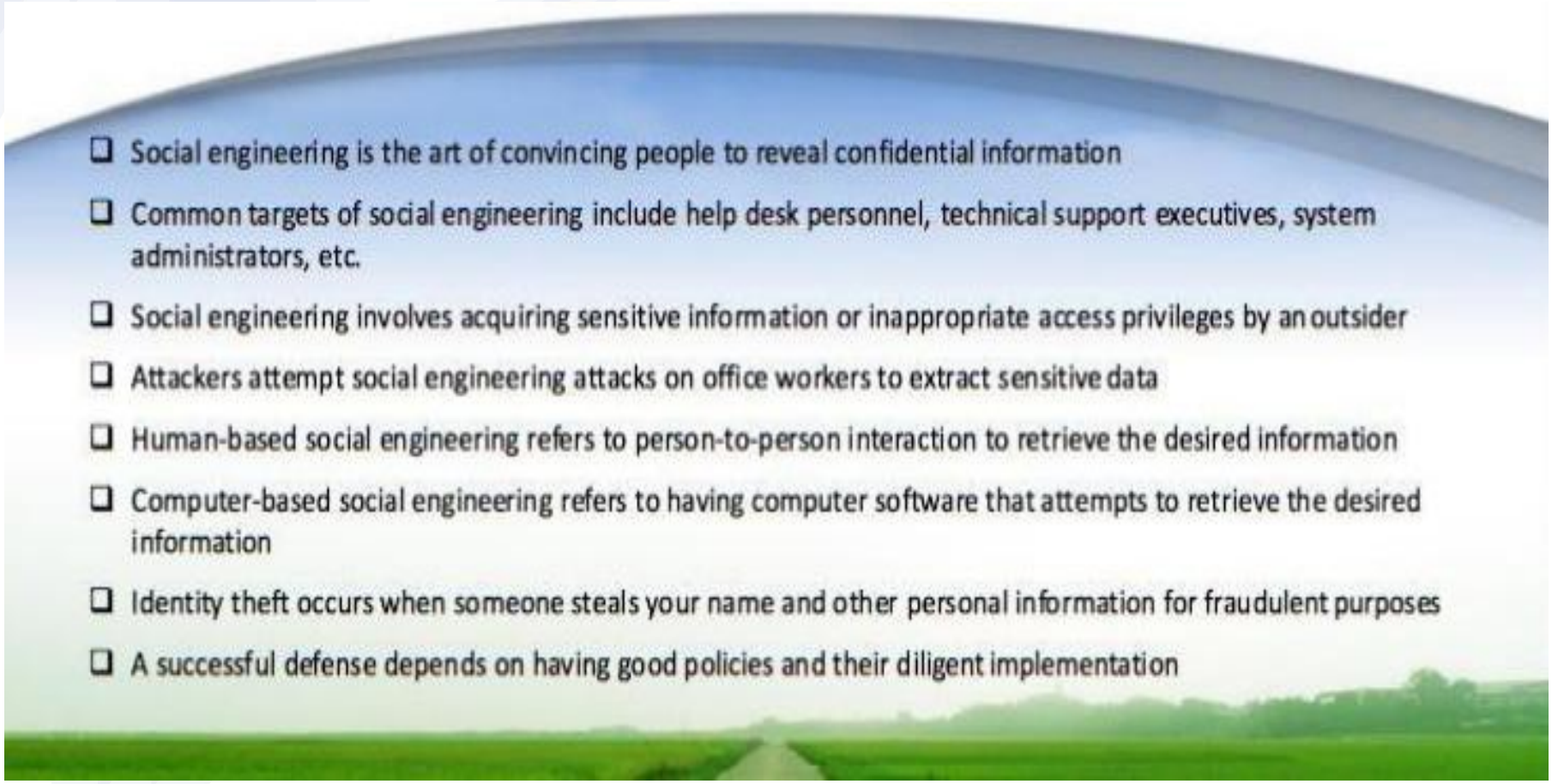
1. Secure or shred all documents containing private information
2. Ensure your name is not present in the marketers' hit lists
3. Review your credit card reports regularly and never let it go out of sight
4. Never give any personal information on the phone
5. To keep your mail secure, empty the mailbox quickly
6. Suspect and verify all the requests for personal data
7. Protect your personal information from being publicized
8. Do not display account/contact numbers unless mandatory
9. Monitor online banking activities regularly
10. Never list any personal identifiers on social media

Strathmore UNIVERSITY

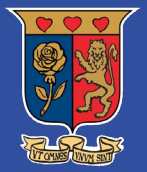
Exercise

- How to perform identity theft
- Impact of identity theft
- How to mitigate identity theft

Summary



- Social engineering is the art of convincing people to reveal confidential information
- Common targets of social engineering include help desk personnel, technical support executives, system administrators, etc.
- Social engineering involves acquiring sensitive information or inappropriate access privileges by an outsider
- Attackers attempt social engineering attacks on office workers to extract sensitive data
- Human-based social engineering refers to person-to-person interaction to retrieve the desired information
- Computer-based social engineering refers to having computer software that attempts to retrieve the desired information
- Identity theft occurs when someone steals your name and other personal information for fraudulent purposes
- A successful defense depends on having good policies and their diligent implementation



Strathmore
UNIVERSITY

Thank you!

Any Questions?

Strathmore UNIVERSITY

SOCIAL ENGINEERING LABS

Kindly follow this link to find the Labs for social engineering

https://daveeargle.com/security-assignments/labs/lab_social_engineering.html#part-1-msfvenom-with-fake-adobeupdateexe