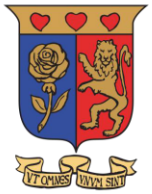
Social Engineering

Strathmore
UNIVERSITY

Instructor Info.

Name: Hinga Muchoki
Occupation: SOC Analyst
Email: hinga.muchoki@Strathmore.edu



Strathmore
UNIVERSITY

Strathmore UNIVERSITY

Objectives

- Understand social engineering techniques
- Describe social engineering concepts
- Perform social engineering from different techniques
- Describe insider threats
- Perform impersonation
- Describe identity threats
- Apply social engineering countermeasures
- Apply knowledge of insider threats and identity theft countermeasures

Strathmore UNIVERSITY

Social Engineering Concepts

- What is Social Engineering
- Targets of Social Engineering
- Impact of Social Engineering on an Organization
- Acts used by attackers
- Factors that make companies vulnerable to Social Engineering
- Why is social Engineering effective?
- Phases of Social Engineering Attacks

Strathmore
UNIVERSITY

What is Social Engineering?

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

The Tactic or trick of gaining sensitive information by exploiting the basic human nature such as Trust, Fear, Desire.

Information gained is such as Personal Identifiable Information, Authorization details etc.

Strathmore UNIVERSITY

Cntd'

- How do attacker gathers employee information about target i.e. (identify the various sources)

  Organization website (Emails, Names, Social Accounts, Numbers, Residence)
  Adverts on the site reveal the products.
  Blogs, Forums and other online spaces employees share personal information...

- After gathering information how do attackers executes social engineering (techniques):

  Impersonation
  Piggybacking
  Tailgating
  Reverse Social engineering…

NB

- People have conditioned themselves to not be overly suspicious, and they associate specific behaviors and appearances with known entities.

Question:
What makes you differentiate a Doctor from a Plumber or Farmer from a Network Engineer.

Social Engineering Targets

Strathmore UNIVERSITY

NB

The attacker makes sure they know the organization's perimeter and the people on its perimeter, such as security guards, receptionists, and help-desk workers, to exploit human oversight. (For instance the person you are attacking may ask who is the IT admin or who works at place A, B or C)

Receptionists and Help-Desk Personnel:

They readily share information if they feel they are doing so to help a customer

Technical Support Executives:

By pretending to be senior management, customers, vendors, or other figures, SE can obtain sensitive information

Example:

I may call Safaricom and pretend to be a customer who lost their m-pesa password or sim card just to understand the process of replacing one.

System Administrators:

They responsible for maintaining the systems. They may have critical information such as the type and version of OS and admin passwords. Can use different techniques to gain info they have.

Users and Clients:

Approach users and clients, by pretending to be a tech support person to extract sensitive information.

Task: Identify how an attacker can perform a sim swap and credit card scam

Senior Executives:

From various departments such as Finance, HR, and CxOs (CTO, CFO, CEO etc.) can be a good target.

Strathmore UNIVERSITY

Impact of Social Engineering Attack on an Organization

Economic Losses: Competitors may use social engineering techniques to steal sensitive information such as the development plans.

Damage to Goodwill: Social engineering attacks may damage that goodwill by leaking sensitive organizational data, this may affect how the company **relates** with its clients.

Loss of Privacy: If an organization is unable to maintain the privacy of its stakeholders or customers, then people can lose trust in the company and clients may discontinue their association with the company.

Dangers of Terrorism: Terrorists may use social engineering techniques to make blueprints of their targets to infiltrate their targets, we have a couple of incidents here in Kenya.

Lawsuits and Arbitration: Clients (investors) may take a company to court especially when their data is not held in the confidentiality they expect. This results in negative publicity for an organization and affects the business's performance.

Temporary or Permanent Closure: With combined lawsuits and arbitration may force the temporary or permanent closure of an organization and its business activities.

Strathmore UNIVERSITY

Acts Used by Attackers (Authority, Intimidation….)

Authority : Attackers take advantage of this by presenting themselves as a person of authority, such as a technician or an executive, in a target organization to steal important data.

Intimidation: Is to make timid or make fearful, think of a scenario where a friend or relative is held hostage and one is forced to associate with a cyber criminal.

Consensus or Social Proof: Consensus or social proof refers to the fact that people are usually willing to **like things or do things that other people like** or do.
Example:- You probably do not need to attend an event although your friend is attending, it may not be out of the ordinary to receive a link of the event from your friend.

Scarcity: SE creates a feeling of urgency in a decision-making process.
Example:- There are those products that attackers know you like and they may create websites with discounted value for the products.

Urgency: This implies encouraging people to take immediate action.
Example of the Safaricom agent hack where agent is tricked to send money to a foreign number.

Familiarity or Liking: This implies that people are more likely to be persuaded to do something when they are asked by someone whom they like.
Example:- People often allow someone to tailgate them if they like that person or are familiar with them.

Strathmore UNIVERSITY

Factors that Make Companies Vulnerable to Attacks

Insufficient Security Training: Employees can be ignorant about the social engineering tricks. Therefore, the minimum responsibility of any organization is to educate their employees about social engineering techniques.

Unregulated Access to Information: For any company, one of its main assets is its database. Providing unlimited access or allowing everyone access to such sensitive data might cause trouble. .

Several Organizational Units : Some organizations have their units at different geographic locations, a company like KPLC is situated in many locations and may have stations in different locations.
This sort of setup makes it easier for an attacker to access the organization's sensitive information.

Lack of Security Policies : It is a high-level document describing the security controls implemented in a company. These include but are not limited to password change policy, information sharing policy, access privileges etc.

Strathmore UNIVERSITY

Why is Social Engineering Effective?

Social engineering does not entirely deal with network security issues; instead, it deals with the psychological manipulation of a human being.

Human beings are most susceptible to variation despite having policies in place.

It is challenging to detect social engineering attempts. It is an Art and Science almost similar to a magic trick.

No method guarantees complete security from social engineering attacks.

No specific hardware or software is available to safeguard against social engineering attacks.

This approach is relatively cheap (or free) and easy to implement.

Strathmore UNIVERSITY

Phases of a Social Engineering Attack

Attackers take the following steps to execute a successful social engineering attack:

- Research the Target Company:

Before attacking the target organization's network, an attacker gathers enough information to infiltrate the system. Social engineering is one technique that helps in extracting information. The attacker researches basic information about the target organization, such as the nature of the business, its location, number of employees, and other facts. While researching, the attacker indulges in activities such as **dumpster diving**, **browsing the company's website**, and finding employee details.

- Select a Target:

After finishing their research, the attacker selects a target for **extracting** sensitive information about the organization. Usually, attackers try to reach out to **disgruntled employees** because they are easier to manipulate.

Strathmore UNIVERSITY

Social Engineering Techniques

- Human Based Social Engineering
- PC Based Social Engineering
- Mobile Base Social Engineering
- Videos
- Labs

Strathmore UNIVERSITY

Social Engineering Techniques

- **Human-based Social Engineering:**
  - Impersonation:
  - Eavesdropping:
  - Shoulder Surfing:
  - Dumpster Diving:
  - Reverse Social Engineering:
  - Piggybacking:
  - Tailgating:
  - Diversion Theft:
  - Honey Trap:
  - Baiting:
  - Quid Pro Quo:
  - Elicitation:

- **PC-based Social Engineering:**
  - Phishing and the different types.
  - Examples of Phishing Emails
  - Types of Phishing
  - Pharming
  - Catfishing Attack
  - Deepfake Attack
  - Phishing Tools

Strathmore UNIVERSITY

S.E. Techniques cntd'

- **Mobile-based Social Engineering:**
  - Repackaging Legitimate Apps
  - Fake Security Applications
  - SMiShing (SMS Phishing)

Strathmore
UNIVERSITY

HUMAN BASED SOCIAL ENGINEERING

Strathmore UNIVERSITY

Human-based Social Engineering:

Impersonation:
Social engineering technique where an attacker pretends to be a legitimate or authorized person
The attacker might impersonate a courier or delivery person, janitor, businessman, client, technician, or they may pretend to be a visitor.
< Popular with sim card scams in Kenya >

Eavesdropping :
Unauthorized person listening to a conversation or reading others' messages. Interception of any form of communication i.e. Audio, Video or Written an attacker can obtain business plans, phone numbers and addresses

Shoulder Surfing :
Looking over someone's shoulder as they key information into a device. Shoulder surfing to find out passwords, personal identification numbers, account numbers, and other information. Cameras may be installed in rooms to record victim actions.

Dumpster Diving :
Dumpster diving is the process of retrieving sensitive personal or organizational information by searching through trash bins. Attacker may pretend to be a cleaner. They can obtain: account numbers, bank statements, salary data, source code, sales forecasts, access codes, phone lists, credit card numbers etc.

Strathmore UNIVERSITY

Human-based Social Engineering ctnd':

****Reverse Social Engineering:**

Generally, reverse social engineering is difficult to carry out. This is primarily because its execution needs a lot of preparation and skills.

The perpetrator assumes the role of a knowledgeable **professional** so that the organization's employees ask them for information. They then manipulate the questions to draw out the required information.

Piggybacking:

For example, an attacker might **request an authorized person** to unlock a security door, saying that they have forgotten their ID badge.

Common courtesy, the authorized person will allow the attacker to pass through

Tailgating:

It is the act of following an authorized person through a secure entrance, as a polite user would open and hold the door for those following them. The attacker may wear a fake badge and closely follow an authorized person.

Diversion Theft: This technique is also known as "Round the Corner Game" or "Cornet Game." The main objective of this technique is to trick a person responsible for making a genuine delivery into delivering the consignment to the wrong location, thus interrupting the transaction.

-> Simply put, the delivery man is diverted to a different location by the SE.

-> This could also be used to send sensitive or confidential info to an unassociated person.

Strathmore UNIVERSITY

Human-based Social Engineering ctnd':

Honey Trap: The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

Baiting :

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. It relies on curiosity and greed of the end-user

-> Flash drive bait

-> Promise of monetary reward

Quid Pro Quo:

Quid pro quo is a Latin phrase that meaning "**something for something**."

In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials.

Elicitation:

Elicitation is the technique of extracting specific information from the victim by involving them in normal and disarming conversations.

Strathmore UNIVERSITY

SOCIAL ENGINEERING VIDEO

The videos covers human based Social Engineering.

1. https://www.youtube.com/watch?v=1kkOKvPrdZ4&list=RDLVrkz1ItKLAvk&start_radio=1

2. https://www.youtube.com/watch?v=YVqurfWzB-Q

Strathmore
UNIVERSITY

PC-BASED SOCIAL ENGINEERING

Strathmore UNIVERSITY

PC-based Social Engineering:

Which malicious programs are used by attackers?

viruses, trojans, and spyware, adware etc.

Assignment: Go research on these will ask randomly.

- Pop-Up Windows (as used in tricking users)
- Hoax Letters
- Chain Letters
- Instant Chat Messenger (as used by a Social Engineer)
- Spam Email
- Scareware

What is Phishing?

Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information.

When a user clicks on the malicious link, it redirects them to the fake webpage, where they are lured into sharing sensitive details such as their address and credit card information.

Strathmore UNIVERSITY

PC-based Social Engineering ctnd':

Types of Phishing

Spear Phishing, Whaling, Pharming, Spimming, Angler Phishing, Catfishing Attack, Deepfake Attack.

Spear Phishing:

Social engineering content directed at a specific employee or small group of employees in an organization to steal sensitive data

Whaling:

A whaling attack is a type of phishing that targets high profile executives like CEO, CFO, politicians, and celebrities who have complete access to confidential and highly valuable information.

Pharming:

A social engineering technique in which the attacker executes malicious programs on a victim's computer or server, when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website.

Pharming attack can be performed in two ways: **DNS Cache Poisoning** and **Host File Modification.**

Strathmore UNIVERSITY

Pharming Social Engineering ctnd':

DNS Cache Poisoning:

- The attacker performs DNS Cache Poisoning on the targeted DNS server.
- The attacker modifies the IP address of the target website "www.targetwebsite.com" to that of a fake website "www.hackerwebsite.com."
- When the victim enters the target website's URL in the browser's address bar, a request is sent to the DNS server to obtain the IP address of the target website.
- The DNS server returns a fake IP address that is already modified by the attacker. o Finally, the victim is redirected to the fake website.

Host File Modification:

- For windows: C:\Windows\System32\drivers\etc (location of file) <need to open from notepad as admin>
- An attacker sends a malicious code as an email attachment.
- When the user clicks on the attachment, the code executes and modifies local host files on the user's computer.
- When the victim enters the target website's URL in the browsers address bar, the compromised host file automatically redirects the user's traffic to the fraudulent website controlled by the hacker.
- **NB**:
  On most operating system the default configuration is that any mappings contained in the Hosts file overrides any information that would be retrieved from a DNS server.

Strathmore UNIVERSITY

PC-based Social Engineering ctnd':

Spimming:

SPIM (Spam over Instant Messaging) exploits Instant Messaging platforms and uses IM as a tool to spread spam. Attacker make use of bots (an application that executes automated tasks over the network) to harvest Instant Message IDs and forward spam messages to them. Spam, generally include advertisements and malware as an **attachment** or **embedded hyperlink**.

Angler Phishing:

Angler phishing is a cyber phishing fraud in which attackers target **disgruntled** users or **customers** over social media platforms. Attackers create a fake social media account impersonating the organization's helpdesk account and connecting to the disgruntled individuals via social media posts.

-> They may reply to individuals who raise complaints on social media or post fake service links. (The user will believe they have received feedback from a trusted source.)

Catfishing Attack:

Attacker performs identity theft, create a fake social media account and masquerade as the owner of the account. Later, they perform cyberbullying or other social engineering attempts for monetary gain against their victims.

-> Example: Tinder swindler

Strathmore UNIVERSITY

Catfishing Attack Social Engineering ctnd':

Signs of Catfishing:

- Avoids direct communication:
  A catfisher often avoids direct meetings, refuses to provide their contact number, avoids turning on their webcam, and makes emergency excuses of illness or travel.

- Maintains a single profile picture for a long duration:
  A catfisher maintains the same profile picture for years to falsify their age. Occasionally, attacker may download all the pictures of the victim at once and use them one by one for years to falsify their age.

- Maintains a good number of friends in their account:
  A catfisher maintains a good number of friends and balances the gender in their account.

- Requests for Money:
  A catfisher often requests money while pretending to be in danger. They attempt to leverage the emotional or business-oriented attachments of users.

Strathmore UNIVERSITY

PC-based Social Engineering ctnd':

Deepfake Attack:

A deepfake attack is a type of phishing attack in which attackers create false media of a person they target using advanced technologies such as ML and AI.
-> Some of the targets are individuals in senior positions

Performed by gathering **previously recorded audio** and video samples of the target person and then **cloning** those clips. Using these fake clippings, attackers may blackmail victims into paying a ransom.

What are signs of a Deepfake Attack?

Audio signs:

- Deviation from a natural speech pattern
- Robotic voice toning
- Poor audio quality

Video signs:

- Mismatch between speech and lip movement
- Uneven blinking or eye movements
- Frequent color changes in skin tone

Strathmore UNIVERSITY

Social Engineering Lab:

- Lab_1 -> DNS Cache Poisoning
  Done via modifying the hosts file of Windows Machine.

- Lab_2 -> Credential Harvester Lab Scenario

  Social Engineer Toolkit SET (setoolkit)

  Source: https://github.com/trustedsec/ptf

  Source: https://trustedsec.com/

Strathmore
UNIVERSITY

MOBILE-BASED SOCIAL ENGINEERING

Strathmore UNIVERSITY

Mobile-based Social Engineering:

Publishing Malicious Apps

The attacker first creates the malicious application — such as a gaming app with attractive features — and publishes it on major application stores using the popular names.
Once the application is installed, the device is infected by malware that sends the user's credentials, contact details and other info.

-> Who reads Terms and Conditions?? At the end of the day to use the app you need to accept.

Repackaging Legitimate Apps

Platform vendors create centralized marketplaces to allow mobile users to conveniently browse and install these games and apps. Usually, developers submit gaming applications to these marketplaces, making them available to thousands of mobile users.
A malicious developer downloads a legitimate game, repackages it with malware, and uploads it to the third-party application store. The malicious program installed on the user's mobile device collects the user's information and sends it to the attacker, or worse.

SMiShing (SMS Phishing)

Sending SMS is another technique used by attackers in performing mobile-based social engineering. SMS text messaging system is used to lure users into taking instant action such as downloading malware, visiting a malicious webpage, or calling a fraudulent phone number.

Strathmore UNIVERSITY

Social Engineering Techniques

- Insider Threats.
- Impersonation on Social Networks.
- Identity Theft.

Strathmore
UNIVERSITY

INSIDER THREATS

Strathmore UNIVERSITY

Insider Threats:

Insider threats to your network typically involve people who work as employees or contractors of your company. They know things about your organization that outsiders usually don't

-> Other Employees and their roles.
-> Applications being used.
-> Vendors they work with.

Some insider threats are purely accidental.
Maybe an employee will accidentally leave a USB thumb drive full of sensitive documents in a restaurant's washroom.

For this reason I have identified five types of insider threats.

1. Malicious Insider
2. Negligent Insider
3. Professional Insider
4. Compromised Insider
5. Accidental Insider

Strathmore UNIVERSITY

Types of Insider Threats:

Malicious Insider:

Malicious insider threats come from disgruntled or terminated employees who steal data or destroy company networks intentionally

Negligent Insider:

Insiders, who are uneducated on potential security threats or simply bypass general security procedures to meet workplace efficiency, are more vulnerable to social engineering attacks.

Professional Insider:

They are the most harmful insiders. They use their technical knowledge to identify weaknesses and vulnerabilities in the company's network and sell the organization's confidential information.

Compromised Insider:

An outsider compromises an insider and masquerades as a genuine insider. This is more difficult to detect since.

Accidental Insider:

The threat occur from the inadvertent exposure of confidential details to an external entity.

-> Unintentionally clicking on a malicious hyperlink.

-> Inadvertently disposing important papers

Strathmore UNIVERSITY

Indications of an Insider Threats?

Generally abnormal user activities that deviate from regular work activities.

Missing or Modified Network Logs :

To avoid detection, insiders may try to access the log files to delete, modify, and edit unauthorized access events, file transfer logs.

Behavioral and Temporal Changes:

Behavior such as frequent travel, anger management issues or constant quarrels with colleagues

Multiple Failed Login Attempts:

The insider can try to log in to unauthorized systems or applications by brute-force.

Unauthorized Access to Physical Assets:

Activities such as employees using authorized assets without authentication, trying to escalate their privileges beyond their job requirements

Why are Insider Attacks Effective?

Insider attacks can go undetected for years, and remediation is expensive.

Insider attacks are easy to launch.

Preventing insider attacks is difficult; an inside attacker can easily succeed

It is easy for employees to cover their actions by editing or deleting logs to hide their malicious activities.

It is very difficult to differentiate harmful actions from the employee's regular work. It is hard to identify whether employees are performing malicious activities or not.

Even after malicious activity is detected, the employee may refuse to accept responsibility and claim it was a mistake.

Strathmore
UNIVERSITY

IMPERSONATION ON SOCIAL NETWORKING SITES

Strathmore UNIVERSITY

Impersonation on Social Networking Sites

Today social networking sites are widely used by many people that allow them to build online profiles, share information and media such as pictures, blog entries, and music clips.

It is relatively easier for an attacker to impersonate someone. The victim is likely to trust the attacker and eventually reveal information

There are two ways an attacker can perform impersonation on social networking sites:

- By creating a fictitious profile of the victim on the social media site
- By stealing the victim's password or indirectly gaining access to the victim's social media account

From a site like LinkedIn, What info could be gathered?

Some social networking sites are a treasure trove for attackers because people share their personal and professional information on these sites, such as **name**, **address**, **mobile number**, **date of birth**, **project details**, **job designation**, **company name**, and **location**.

This info can be used for impersonation purpose.

Strathmore UNIVERSITY

Impersonation on Facebook

To impersonate users on Facebook, attackers use nicknames or aliases instead of their real names. They create fake accounts and try to add “Friends” to view others’ profiles and obtain critical and valuable information.

- Create a fake user group on Facebook identified as "Employees of" the target company
- Using a false identity, proceed to "friend," or invite actual employees to the fake group, “Employees of Company XYZ”
- Users join the group and provide their credentials such as date of birth, educational and employment backgrounds, or spouses’ names. (The attacker normally scans for this info)
- Using the details of any one of the employees, an attacker can compromise a secured facility to gain access to the building.

Strathmore UNIVERSITY

What are The Social Networking Threats to Corporate Networks?

Corporate users should be aware of the following social or technical security risks and threats:

Data Theft:
Social sites are huge databases accessed by many people worldwide, increasing the risk of information exploitation.

Involuntary Data Leakage:
Employees may unknowingly post sensitive data about their company on social networking sites, which might help an attacker to launch an attack on the target organization.

Spam and Phishing:
Employees using work e-mail IDs on social networking sites will probably receive spam and become targets of phishing attacks.

Malware Propagation:
Social networking sites are ideal platforms for attackers to spread viruses, bots, worms, trojans, spyware, and other malware.

Business Reputation:
Attackers can falsify information about an organization or an employee on social networking sites, resulting in loss of reputation.

Loss of Productivity:
Organizations must monitor employees' network activities to maintain security and ensure that such activities do not misuse the system and company resources.

Strathmore
UNIVERSITY

IDENTITY THEFT

Strathmore UNIVERSITY

Identity Theft

Identity theft is referred to as the illegal use of someone's identification. Identity theft occurs when someone **steals** others' personally identifiable information **for fraudulent purposes**.

Types of personally identifiable information stolen by identity thieves?

- Name
- Phone number
- Date of birth
- Bank account number
- Credit card information…

What do attackers do with the Info they have stolen?

- To open new credit card accounts in the name of the user without paying the bills ▪
- To open a new phone or wireless account in the user's name, or to run up charges on their existing account
- To open bank accounts with the intention of writing bogus checks using the victim's information
- To clone an ATM or debit card to make electronic withdrawals from the victim's accounts
- To obtain loans for which the victim is liable
- To impersonate an employee of a target organization to physically access its facility
- To sell the victim's personal information
- To order goods online using a drop-site

https://ntvkenya.co.ke/crime/eight-suspects-arrested-in-kes-500-million-fuliza-fraud-scheme/

Strathmore UNIVERSITY

How Do Attackers Obtain Personal Information for Identity Theft

Phishing, Skimming, Pretexting, Dumpster Diving…

Theft of wallets, computers, laptops, cell phones, backup media, and other sources of personal information

Physical theft is common. Attackers steal hardware from places such as hotels and recreational places (You know where you visit)

Internet Searches

Attackers can gather a considerable amount of sensitive information via legitimate Internet sites

Skimming

Skimming refers to stealing credit or debit card numbers by using special storage devices called skimmers

Keyloggers and Password Stealers (Malware)

An attacker may infect the user's computer with trojans, viruses, or other malware and then record and collect the user's keystrokes to steal passwords, usernames, and other sensitive information of personal, financial, or business import

Wardriving

Attackers search for unsecured Wi-Fi wireless networks in moving vehicles containing laptops, smartphones, or PDAs. Once they find unsecured networks, they access any sensitive information stored on the devices of the users on those networks.

Strathmore UNIVERSITY

What are Indicators of Identity Theft?

People do not realize that they are the victim of identity theft until they experience some unknown and unauthorized issues as a result of the theft.

There are certain signs people should watch out for:

- Unfamiliar charges to your credit card that you do not recognize.
- No longer receive credit card, bank, or utility statements
- Creditors call asking about an unknown account on your name.
- There are numerous traffic violations under your name that you did not commit.
- You receive charges for medical treatment or services you never received.
- There is more than one tax return filed under your name.
- Being denied access to your own account and unable to take out loans or use other services.
- Not receiving electricity, gas, water, or other services bills due to stolen mail.
- Sudden changes in your personal medical records showing a condition you do not suffer from

Strathmore
UNIVERSITY

Thank you!

Any Questions?