Preparation 1

Objective: Establish contacts, define procedures, and gather information to save time during an incident.

■ Raise user awareness and security policies

Never give any personal or corporate information to an unidentified person. This could include user IDs, passwords, account information, name, e-mail address, phone (mobile or landline) numbers, address, social security number, job titles, information on clients, organization or IT systems.

The goal of the social engineer is to steal human resources, corporate secrets or customer/user data.

Report any suspicious event to your manager, who will forward it to the CISO in order to have a centralized reporting.

■ Have a defined process to redirect any "weird" request to a "red" phone, if needed.
Red phone number must be clearly tagged as "Social Engineering". **The phone number has to be easy to identify in the global phone directory of your company but requests on reverse number should not be displayed.**
Red phone line should always be recorded for evidence collecting purposes.

■ Prepare to handle conversation with social engineers to identify which information could help tracking the attacker and his goals.

■ Check your legal department to see which actions are allowed and which reactions they can handle.

Identification 2

User part

Objective: Detect the incident, determine its scope, and involve the appropriate parties.

■ **Phone call** / someone you don't know calls you/your service, asking for detailed information.

▪ If the contact works out of the company and requests for information that could be valuable for a competitor, deny his requests and go to part 3.

▪ If the contact pretends to be an employee of your company but the phone number is hidden or not internal, propose that you call back to the declared number in the directory. If the supposedly attacker agrees, call back to check. If he rejects this option, go to part 3.

> The attacker might use several techniques to entice his victim to speak (fear, curiosity, empathy ...). Do not disclose information in any case.
> Listen carefully to his requests and at the end ask for a phone number to call back or an email address to reply.
> Take notes and stay calm, even if the attacker is shouting or threatening, remember he tries to use human weaknesses.

> If you can go further, the following information will be precious:
> - the name of the correspondent,
> - requested information / people
> - accent, language skills,
> - industry language and organizational knowledge,
> - background noises
> - time and duration of the call

■ **E-mail** / Someone you don't know requests detailed information.

▪ If the contact has an "out of the company" e-mail address and requests information that could be valuable for a competitor, go to part 3.

▪ If the contact uses an internal e-mail address but is asking for weird information, ask him some explanations and use the company directory to get his manager's name that you'll place as a copy.

■ Eventually notify top management to inform them that an incident has been encountered relating to a social engineering attack. They might understand the goals depending on the context.

Containment 3

User part

Objective: Mitigate the attack's effects on the targeted environment.

At this step, you should be pretty sure that you're dealing with a social engineering attack.

Actions for all employees:

■ **Phone call**

▪ If the attacker urges you to give a phone number, follow these steps:
  - Use the "red phone line" from your CERT/CSIRT, if existing.
  - Give him the number with an invented name.
  - Immediately call your CERT/CSIRT team explaining what happened and the chosen invented name.

▪ If the attacker stresses you too much and does not let you time to find the Red Phone number, ask him to call you back later, pretending a meeting.

▪ If the attacker wants to reach someone, follow these points :
  - Place on hold the attacker and call CERT/CSIRT team and explain what happened
  - Transfer the conversation of the attacker to CERT/CSIRT team (do not give him the number)

■ **E-mail**

▪ Forward to your security team all email including headers (send as attached documents) for investigation purposes. It might help to track the attacker.

Containment — 3

Actions for CERT or incident response team:

- **Phone call**

  - Resume the conversation with the attacker and use one of these techniques:
    - Impersonate the identity of the people whom the attacker is willing to speak
    - Slow down and make last the conversation and entice the attacker to make mistake.
    - Explain him that social engineering attack is forbidden by law, punished by sanctions and that lawyer team will handle the issue if it continues
  - If the trap phone number has been used, prepare to "burn it", create another one and display it in the directory.

- **E-mail**

  - Collect as much information as possible on the email address:
    - Analyze the email headers and try to locate the source
    - Search the e-mail address with Internet tools
    - Geolocalize the user behind the email address

- Aggregate all social engineering attacks to visualize the scheme.

Remediation — 4

Objective: Take actions to remove the threat and avoid future incidents.

Some possible remediation actions can be tried:

- Alert the law enforcement and/or file a complaint,
- Discuss the problem in circles of trust to know if the company is facing this issue alone,
- Threaten the attacker with legal actions if he can be identified

Recovery — 5

Objective: Restore the system to normal operations.

Notify the top management of the actions and the decisions taken on the social engineering case.

Aftermath — 6

Objective: Document the incident's details, discuss lessons learned, and adjust plans and defences.

Inform your hierarchy and subsidiaries about the incident, this could help to avoid similar attacks later.

Report

An incident report should be written and made available to all the actors of the incident.

The following themes should be described:

- Initial detection
- Actions and timelines
- What went right
- What went wrong
- Incident cost (direct and indirect losses)

Capitalize

Actions to improve the social engineering handling processes should be defined to capitalize on this experience, specially awareness.

IRM #10
Social Engineering Incident
How to handle a social engineering incident (phone or e-mail)

Abstract

This Incident Response Methodology is a cheat sheet dedicated to handlers investigating on a precise security issue.
Who should use IRM sheets?
- Administrators
- Security Operation Center
- CISOs and deputies
- CERTs (Computer Emergency Response Team)

Remember: If you face an incident, follow IRM, take notes and do not panic. Contact your CERT immediately if needed.

Incident handling steps

6 steps are defined to handle security Incidents

- **Preparation: get ready to handle the incident**
- **Identification: detect the incident**
- **Containment: limit the impact of the incident**
- **Remediation: remove the threat**
- **Recovery: recover to a normal stage**
- **Aftermath: draw up and improve the process**

IRM provides detailed information for each step.