Social Engineering Intrusion: A Case Study

Paper By M. Sillanpää and J. Hautamäki

Presentation by Sadra Setarehdan

Social Engineering

- Exploit humans
- Use various methods which in most cases is customized for a specific target
- Defence against social engineering attack is even harder than against normal attacks using information technology in different forms
- nothing unusual about social engineering.

A Case Study

- An in-depth study of one person, group, or event.
- Pros:
  - Allows researchers to collect a great deal of information
  - Give researchers the chance to collect information on rare or unusual cases
  - Permits researchers to develop hypotheses that can be explored in experimental research
- Cons:
  - Cannot necessarily be generalized to the larger population
  - Cannot demonstrate cause and effect
  - May not be scientifically rigorous
  - Can lead to bias

Structure

Background information

Organization is a big Finnish public company whose employers' number is almost two thousand and revenue almost one billion euros.

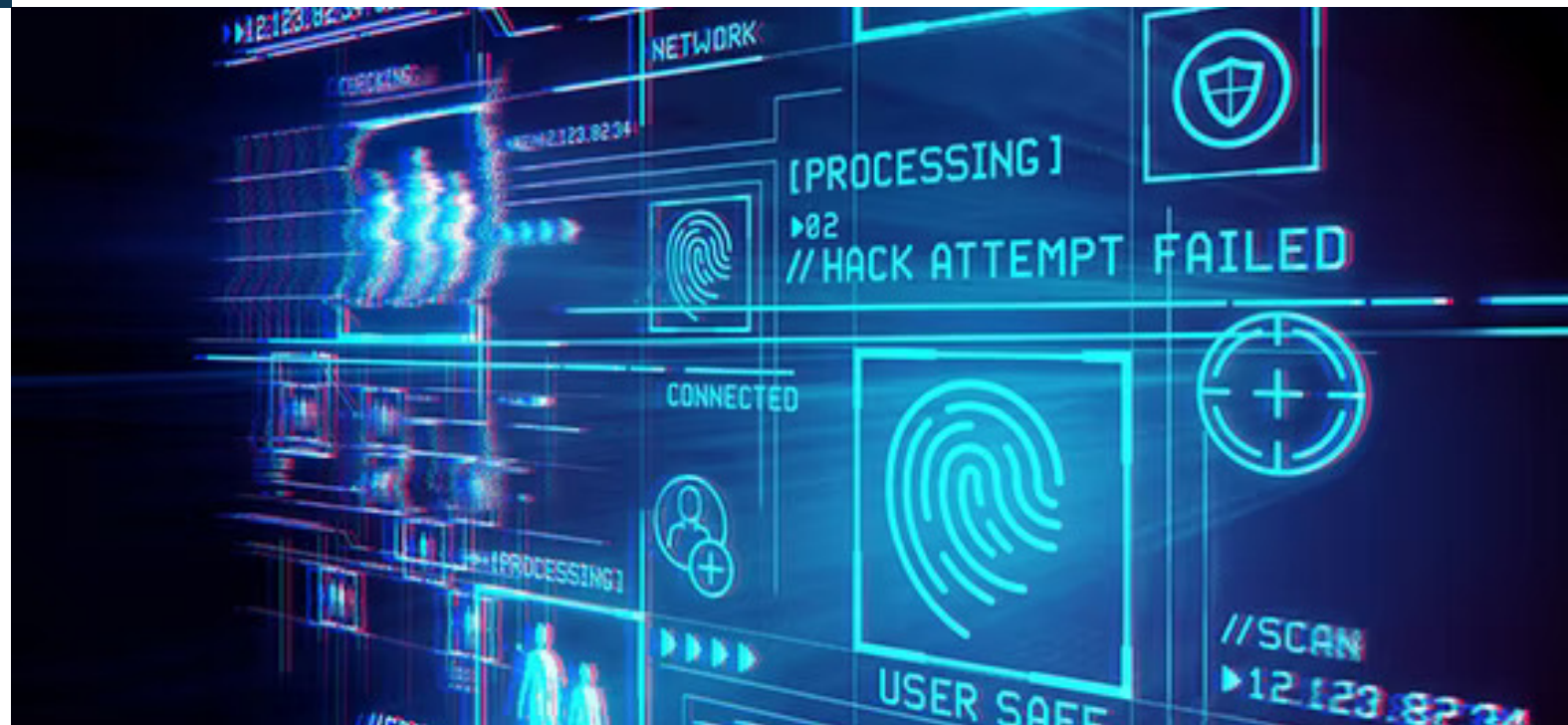
The aim of this study was to find out how the employees of the target organization react and act in situations of social engineering attacks.

3 stages of this study

1- Survey questions

2- Reconnaissance

3- Physical penetration



Survey questions

1

Survey Results

From total of 70 employees

Use of secure password

61 % use a strong password (q. 1)

37 % use the same password for multiple sites and services (q. 2)

10 % use the same passwords in work related systems, and some personal public services (q. 3)

fire alarm & Tailgating

96 % lock their workstations and then leave their workstation (q. 4)

83 % don't let an unknown person enter through a locked door after themselves (q. 8)

89 % check the key properly and make sure it is not fake (q. 11)

phone call

77 % start different ways to confirm the identity of the caller. (q. 6)

97 % do not answer the ID number question in case of phone call phishing (q. 9)

USB & Email

70 % do not connect an unknown USB memory stick to their computer (q. 7 and 10)

51% verify an email, and 3% trust a co-worker and open it. 26% ignore that email. 20% report phishing emails. (q. 13)

Reconnaissance

2

Information gathered

About people and structure of company

- Personnel names and jobs
- Main business plan
- Organization structure and images
- Charity area and some of their customers
- Email addresses and phone numbers
- Social media links
- Organization reports
- Personnel Id card

About computers and networks

- IP address space range
- Public DNS servers and their link
- Public mail servers
- Subdomains
- Email address structure
- Services/Port numbers on each server
- Hash values

Physical penetration

3

Case 1

First case included two different scenarios. The first scenario was carried out five times on a single day in about three hours' time slot. The other scenario was done four times; however, on different days and a different time of day.

Scenario	Time	Breaching point	Success rate (attempts/successful)	Information about breach
1.1	Morning when employees come to work. (7.30 am – 10 am)	Personnel main entrance	3/3 Success	No questions asked and not looking behind. Not trying to get any floors.
1.2	(7.30 am – 10 am)	Side door	2/2 Success	Getting inside via stairs and elevator to the floors with "helpful" employees.
2.1	Morning (8 am)	Car garage	1/1 Success	Through car park to the building and onto the floor in the elevator with employee.
2.2	Midday (10 am)	Personnel main entrance	1/1 (tailgating) Success 0/1 (moving without ID badge) Failure	Tailgating inside and onto other floors. Got caught by an unfamiliar employee on the floor.
2.3	Morning (7.30 am)	Personnel main entrance	1/1 Success	Tailgating to the building and then with another employee onto the floor in the elevator.
2.4	Morning (about 7.30 am)	Side door	1/1 Success	Un-familiar employee opened the door from inside and let me pass. Used elevator with other employees and got onto the next floor. No questions or any verification asked.

Case 2

In second case used a fake ID card. Personal information to ID card, like name, photo, logo and job title in organization, was founded from website in gather phase. Case executed six times and at a different time and on the different day to get more statistics.

Attempt	Time	Succeed (F) or or Failed (F)	Information and summary
1.	11.30 am	S	Receptionists were deceived by the fake card.
2.	7.30 am	S	An employee opened the door and helped to get to the first floor in the elevator. The ID card was not checked.
3.	9 am	S	The side door was used through which access was gained to the floor in the elevator with an employee. The employee took a closer look at the card but did not ask to see it better.
4.	8 am	S	Floor accessed via an elevator. The employee did not look at the ID card at all.
5.	8 am	S	The ID card was not looked when access inside was gained. The floor was accessed with another employee.
6.	9.30 am	F	Very good security behavior from one of the consultants. Very sharp eyes, good questions to verify the ID and information given to the security team.

Case 3

Third case was almost the same as first case 1 except in this case author did not even try to hide a possible ID card. This case was performed twice over three days.

Test scenario	Duration	Information about attempt
1.	1	Moved from end to end on the floors. Greetings from familiar employees but no questions or other interruptions. Tailgated sometimes to another floor.
2.	2	Same as above but duration was longer.
Related to the case 1 breaches and their information	4	No interruptions when walking. Only got caught once by unfamiliar employee.

Conclusion

On paper, everything looked good; however, in the real situation people behaved differently.

Discussion

1. Survey design and questions
2. Number of attempts for each case/scenario in pen testing
3. Cases/Scenarios were vague