

# Social Engineering Techniques

Contributed by: Thomas Kurian Ambattu (thomasambat@gmail.com)

1	Social Engineering over phone
<b>Complexity Level</b>	Low
<b>Situation:</b>	The Social Engineer pickups the phone numbers from a group of employees and make calls. The Social Engineer tries to extract personal information of the employees.
<b>Expected Output</b>	Personal Information of the target group
<b>Simulation</b>	The SE (Social Engineer) pretends that he is calling from a magazine and wants to feature the target in the cover page of the next edition. The target out of excitement and enthusiasm give all the personal details.

2	Social Engineering over email
<b>Complexity Level</b>	Low
<b>Situation:</b>	The Social Engineer randomly collects email IDs from a group of targeted audience and sends mail that ask for their personal details
<b>Expected Output</b>	Personal Information of the targeted group
<b>Simulation</b>	The SE sends an email to the target telling that they are selected as a valuable professional and will receive an award from the organization. In order to complete the submission process the user must provide the personal information in the specified format.

3	Tailgating
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer tries to tail gate an employee for an unauthorized intrusion into the facility

<b>Expected Output</b>	Unauthorized access into the area
<b>Simulation</b>	The SE walks along with a group of employees to the main door, and conveniently enters into the facility following another person.

<b>4</b>	<b>Physical Security</b>
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer tries to skip the physical security check and tries to gain unauthorized access into the facility
<b>Expected Output</b>	Unauthorized access into the area
<b>Simulation</b>	The SE at the physical security check pretends that he has an appointment with the MD and is already late. He promises that he will do the physical security check after the meeting.

<b>5</b>	<b>Physical Security</b>
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer skips the physical security check of the electronic device and enters into the facility
<b>Expected Output</b>	Unauthorized access into the area with the electronic device
<b>Simulation</b>	The SE at the physical security check declares that he is not carrying any electronic devices. He shows his mobile phone as the one which has no camera, but hides another mobile phone with camera and a USB device in his other pocket and enters the facility

<b>6</b>	<b>Physical Security</b>
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer gives a fake sl.no and model of the laptop or electronic device during declaration at the physical security check enters into the facility

<b>Expected Output</b>	Unauthorized access into the area with the electronic device
<b>Simulation</b>	The SE declares that he has got a laptop and gives a sl.no which is fake, the physical security fails to verify the slno on the same.

<b>7</b>	<b>Physical Security</b>
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer introduces himself as the new senior manager and enters into the facility without an ID card.
<b>Expected Output</b>	Unauthorized access into the area without proper ID card
<b>Simulation</b>	The SE pretends that he is appointed as the Sr.Manager and doesn't have an ID card as this is his first day. If the physical security issues a Visitor ID Card, he pretends to be angry and ask the security "How dare you issue a visitor ID card, if you repeat the same, you lose your job" and walks into the facility.

<b>8</b>	<b>Physical Security</b>
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer enters the facility with a fake ID card.
<b>Expected Output</b>	Unauthorized access into the area without proper Authentication
<b>Simulation</b>	The SE shows a fake ID card and tailgates a person without reading the card at the control point. He pretends that the card is swiped, but before getting the door closed, he tailgates the previous person.

<b>9</b>	<b>Physical Security</b>
<b>Complexity Level</b>	Medium
<b>Situation:</b>	The Social Engineer enters the facility with a fake ID and proximity card
<b>Expected Output</b>	Unauthorized access into the area without proper

	Authentication
<b>Simulation</b>	The SE tries to enter the facility with a fake ID card and reads the proximity card. The card doesn't work at the point. He pretends to be angry and asks the security guard on why the card is not working and asks him to open the door. The security guard opens the door and the target is compromised.

<b>10</b>	<b>Baiting</b>
<b>Complexity Level</b>	High
<b>Situation:</b>	The Social Engineer leaves a CD in the cafeteria
<b>Expected Output</b>	Unauthorized access of electronic media
<b>Simulation</b>	The SE leaves a genuine looking CD-Rom labeled "Appraisal for the Year" at the cafeteria. An employee out of curiosity takes the CD and tries to open the CD-Rom on his computer.