

MITNICK SECURITY CONSULTING, LLC

# 2-DAY SOCIAL ENGINEERING TRAINING COURSE OUTLINE

---

2004-2005

MITNICK SECURITY CONSULTING, LLC

7113 WEST GOWAN ROAD  
LAS VEGAS, NV 89129  
(702) 940-9881 TEL (702) 548-6505 FAX

[MITNICKSECURITY.COM](http://MITNICKSECURITY.COM)

# COURSE OUTLINE

<b>MODULE 1: UNDERSTANDING SOCIAL ENGINEERING</b>	<b>PAGE</b>
<b>Unit 1: <u>Social Engineering Overview</u></b>	<b>1-1</b>
1.1 Various Definitions of Social Engineering	1-2
1.2 What does Social Engineering really mean?	1-2
1.3 A Classic Case of Social Engineering – Rifkin Story (Case Study # 1)	1-4
1.4 Information Theft	1-6
1.5 The Categories of Social Engineers	1-7
1.5.1 Hackers	1-8
1.5.2 Industrial Spies / Industrial Espionage Agents	1-8
1.5.3 Foreign Governments / Economic Espionage Agents	1-8
1.5.4 Identity Thieves	1-9
Monster.com Online Job Listing – ID Theft Scam (Case Study # 2)	1-9
1.5.5 Disgruntled Employees	1-12
1.5.6 Competitive Intelligence Collectors	1-13
1.5.7 Information Brokers/ Private Investigators	1-13
1.5.8 Criminals/ Scam Artists	1-14
1.5.9 Bounty Hunters	1-17
1.5.10 Head Hunters	1-17
1.5.11 Terrorists	1-17
Brazen Airport Computer Theft / Terrorism (Case Study # 3)	1-18
1.6 Why Attackers Use Social Engineering?	1-21
1.7 Typical Goals of the Attacker	1-22
1.8 What Industries are Targets?	1-23
1.9 The Personality of the Attacker	1-23
1.10 Why Does Social Engineering Work so Well?	1-24
1.10.1 Security Laxity – Alarming Results	1-25
1.10.2 Cell Phone Firmware Code Theft (Case Study # 4)	1-26
1.11 Who Are the Prime Targets?	1-29
1.12 Vulnerabilities that Expose the Organization	1-29
1.13 Social Engineering Introduction: Discussion Questions	1-31

<b>Unit 2: <u>Social Engineering Attack Cycle and Methods</u></b>	<b>1-35</b>
2.1 Social Engineering Attack Cycle	1-37
2.2 Communication Methods	1-39
2.3 The Help Desk – First Line of Attack	1-42
2.4 Impersonating the Help Desk – Transcript of an Actual Attack (Case Study # 5)	1-44
2.5 Other Common Attacks	1-45
2.6 Other Social Engineering Methods	1-46
2.7 Combining Social Engineering with Technology – The Malware Attack	1-47
2.8 Spyware	1-48
2.9 Social Engineering/ Technical Attack: The Erroneous VeriSign – Issued Digital Certificates	1-49
2.10 Physical Intrusion: The In-Person Attack	1-50
2.11 The SE Pen-Test Case: Physical and Technical Intrusion (Case Study # 6)	1-51

<b>MODULE 2: PLANNING THE ATTACK</b>	<b>PAGE</b>
<b>Unit 3: <u>Intelligence Gathering</u></b>	<b>2-1</b>
3.1 How to gather information?	2-2
3.2 Demonstration: Obtaining Personal Information	2-5
3.3 Researching the Company	2-6
3.4 Digging up Personnel Information	2-7
3.5 Dumpster Diving	2-8
3.6 Dumpster Diving – SE Scenarios (Case Study # 7 and Case Study # 8)	2-9
3.7 Dumpster Diving – Demonstration Exercise	2-11
<b>Unit 4: <u>Elicitation</u></b>	<b>2-13</b>
4.1 Definitions	2-14
4.2 Goals of Elicitors	2-14
4.3 Characteristics of Successful Elicitors	2-14
4.4 Why Elicitation Works So Well	2-15
4.5 Common Targets of Elicitors	2-16
4.6 Structure of Elicitation Sessions	2-16
4.7 Elicitation Techniques	2-17
4.7.1 The Thought Bomb – Pique Interest	2-17
4.7.2 Quid Pro Quo	2-18
4.7.3 Sincere Compliment	2-19
4.7.4 The Soft Shoulder	2-20
4.7.5 Echoing	2-22
4.7.6 Silence	2-22
4.7.7 Quotation	2-23
4.7.8 Naïveté	2-24
4.7.9 Indirect Reference	2-25
4.7.10 Skepticism	2-25
4.7.11 Incorrect Statement	2-26
4.7.12 Critique	2-26
4.7.13 Setting Parameters	2-27
4.8 Elicitation Techniques – Exercise	2-27

<b>MODULE 3: PRETEXTING AND EXECUTION</b>	<b>PAGE</b>
<b>Unit 5: <u>Developing a Pretext</u></b>	<b>3-1</b>
5.1 Pretexting: The Con	3-2
5.2 Pretexting: Exercise	3-4
<b>Unit 6: <u>Key Psychological Principles</u></b>	<b>3-10</b>
6.1 Systematic vs. Heuristic Thinking	3-11
6.2 Two Modes of Thinking and Influence	3-12
6.3 The Langer Experiment – “Mindlessness” (Case Study # 9)	3-13
6.4 Heuristics – Shortcuts for Decision Making	3-14
6.5 Heuristics – Personal Discussion	3-15
6.6 How We Process Social Information	3-15
6.7 Bugs in the Human Hardware – Key Concepts	3-16
6.7.1 Attribution Theory (Social Categorization)	3-17
6.7.2 Cognitive Dissonance	3-18
6.7.3 Reactance	3-20
6.7.4 Context Confusion	3-21
6.7.5 Biases	3-22
6.7.6 Strong Affect	3-24
6.7.7 Overloading	3-25
6.8 Bugs in the Human Hardware – Exercise	3-26

<b>Unit 7: <u>Social Engineering Influence Matrix</u></b>	<b>3-31</b>
7.1 Social Engineering – Metacognition and the Matrix	3-32
7.2 Social Engineering Matrix	3-33
7.3 Dimension # 1 – Influence Tactics	3-34
7.3.1 Following the Crowd	3-35
7.3.2 Liking	3-36
7.3.3 Authority	3-38
7.3.4 Reciprocity	3-40
7.3.5 Commitment/ Consistency	3-42
The Code for the Day – A Social Engineering Exploit (Case Study # 10)	3-43
7.3.6 Scarcity	3-47
7.3.6.1 A Note on Prospect Theory	3-48
7.3.6.2 Prospect Theory – Research Study	3-48
7.3.7 Reward / Punishment	3-49
7.3.7.1 Self Esteem – Appeal to Ego vs. Intimidation	3-50
7.3.7.2 Moral Duty – Appeal to Virtue vs. Guilt	3-50
7.3.7.3 Material – Gain vs. Loss	3-51
7.3.7.4 Imagination – Curiosity vs. Fear	3-52
7.4 Influence Tactics – Resistance Strategies	3-53
7.5 Establishing an Incident Reporting Hotline	3-54
7.6 Establishing an Incident Reporting Organization	3-55
7.7 Influence at Work – Application Exercise	3-55
7.8 Dimension # 2 – Identity Creation	3-59
7.9 Identity Creation – Resistance Strategies	3-62
7.10 Verification and Authorization Procedures	3-63
7.11 Steps of the Verification Process	3-64
7.12 Dimension # 3 – Situation Processing	3-68
7.13 Application Exercise: Situation Processing	3-71
7.14 Situation Processing – Resistance Strategies	3-71
7.15 Dimension # 4 – Communication	3-72
7.16 A Note on Framing	3-75
7.17 Communication – Resistance Strategies	3-76
7.18 Dimension # 5 – Manipulation of Perceptual Cues	3-78
7.19 The Misleading Caller ID (Case Study # 11)	3-80
7.20 Manipulation of Perceptual Cues – Resistance Strategies	3-81
7.21 Case Study – Applying the Matrix	3-82

<b>MODULE 4: BUILDING THE HUMAN FIREWALL</b>	<b>PAGE</b>
<b>Unit 8: <u>Eight Steps to Developing the Human Firewall</u></b>	<b>4-1</b>
8.1 The Human Firewall – Introductory Concepts	4-2
8.2 Inventory Information Assets – Step 1	4-4
Vulnerability Assessment/ Security Plan Development	4-4
8.3 Establish a Data Classification System – Step 2	4-6
8.3.1 Classified Data Terminology	4-9
8.3.2 Document Management Guidelines	4-10
8.4 Security Policy Development – Step 3	4-10
8.4.1 Security Policy Development and Follow-Through	4-13
8.4.2 Security Policy Assessment – Discussion Questions	4-13
8.4.3 Select Security Policies and Procedures Specific to SE	4-15
8.5 Conduct Security Awareness Programs – Step 4	4-24
8.5.1 Security Awareness and Policy Adherence	4-28
8.5.2 Motivating for Participation	4-29
8.5.3 Introduce Testing Concepts	4-31
8.5.4 Reinforcing Training – Ongoing Security Reminders	4-32
8.6 Limiting Information Leakage – Step 5	4-33
8.7 Using Technology – Step 6	4-35
8.8 Pen-Testing using Social Engineering – Step 7	4-36
The SE Pen-Test Case Study	4-37
(Case Study # 12)	
8.9 Incident Response – Step 8	4-39
8.9.1 Incident Response Team	4-40
8.9.2 Incident Response Program Components	4-41
8.9.3 Competitive Intelligence	4-42

<b>Unit 9: <u>Application of the Human Firewall</u></b>	<b>4-43</b>
9.1 Case Study – Application Exercise (Case Study # 13)	4-44
9.2 Management Policies	4-49
Data Classification	4-49
Information Disclosure	4-51
Phone Administration	4-56
Miscellaneous	4-59
9.3 Information Technology Policies	4-67
General	4-67
Help Desk	4-68
Computer Administration	4-72
Computer Operations	4-84
9.4 Policies for All Employees	4-86
General	4-86
Computer Use	4-90
Email Use	4-96
Phone Use	4-98
Fax Use	4-99
Voice Mail Use	4-100
Passwords	4-102
9.5 Policies for Telecommuters	4-105
9.6 Policies for Human Resources	4-107
9.7 Policies for Physical Security	4-109
9.8 Policies for Receptionists	4-112
9.9 Policies for Incident Reporting Group	4-114
9.10 Action Planning Exercise – Instructions	4-115
Resources	4-118

MITNICK SECURITY CONSULTING, LLC

7113 WEST GOWAN ROAD  
LAS VEGAS, NV 89129  
(702) 940-9881 TEL (702) 548-6505 FAX

MITNICKSECURITY.COM