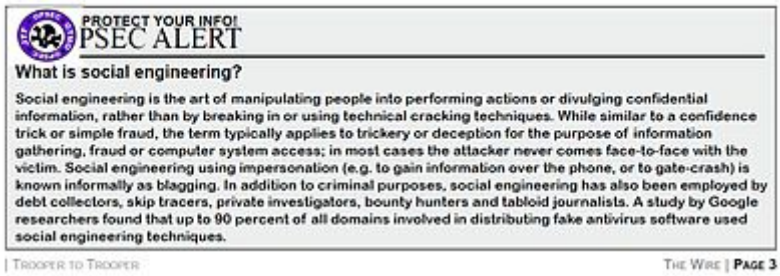
WIKIPEDIA

# Social engineering (security)

**Social engineering**, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.


PROTECT YOUR INFO!
PSEC ALERT

What is social engineering?

Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud or computer system access; in most cases the attacker never comes face-to-face with the victim. Social engineering using impersonation (e.g. to gain information over the phone, or to gate-crash) is known informally as blagging. In addition to criminal purposes, social engineering has also been employed by debt collectors, skip tracers, private investigators, bounty hunters and tabloid journalists. A study by Google researchers found that up to 90 percent of all domains involved in distributing fake antivirus software used social engineering techniques.

| TROOPER TO TROOPER THE WIRE | PAGE 3

OPSEC alert

The term "social engineering" as an act of psychological manipulation of a human, is also associated with the social sciences, but its usage has caught-on among computer and information security professionals.[1]

## Contents

**External links**

# Information security culture

Employee behavior can have a big impact on information security in organizations. Cultural concepts can help different segments of the organization work effectively or work against effectiveness towards information security within an organization. "Exploring the Relationship between Organizational Culture and Information Security Culture" provides the following definition of information security culture: "ISC is the totality of patterns of behavior in an organization that contribute to the protection of information of all kinds."[2]

Andersson and Reimers (2014) found that employees often do not see themselves as part of the organization Information Security "effort" and often take actions that ignore organizational information security best interests.[3] Research shows Information security culture needs to be improved continuously. In "Information Security Culture from Analysis to Change", authors commented, "It's a never ending process, a cycle of evaluation and change or maintenance." To manage the information security culture, five steps should be taken: Pre-evaluation, strategic planning, operative planning, implementation, and post-evaluation.[4]

- Pre-Evaluation: to identify the awareness of information security within employees and to analysis current security policy.
- Strategic Planning: to come up a better awareness-program, we need to set clear targets. Clustering people is helpful to achieve it.
- Operative Planning: we can set a good security culture based on internal communication, management-buy-in, and security awareness and training program.[4]
- Implementation: four stages should be used to implement the information security culture. They are commitment of the management, communication with organizational members, courses for all organizational members, and commitment of the employees.[4]

# Techniques and terms

All social engineering techniques are based on specific attributes of human decision-making known as cognitive biases.[5] These biases, sometimes called "bugs in the human hardware", are exploited in various combinations to create attack techniques, some of which are listed below. The attacks used in social engineering can be used to steal employees' confidential information. The most common type of social engineering happens over the phone. Other examples of social engineering attacks are criminals posing as exterminators, fire marshals and technicians to go unnoticed as they steal company secrets.

One example of social engineering is an individual who walks into a building and posts an official-looking announcement to the company bulletin that says the number for the help desk has changed. So, when employees call for help the individual asks them for their passwords and IDs thereby gaining the ability to access the company's private information. Another example of social engineering would be that the hacker contacts the target on a social networking site and starts a conversation with the target. Gradually the hacker gains the trust of the target and then uses that trust to get access to sensitive information like password or bank account details.

## Pretexting

**Pretexting** (adj. **pretextual**), also known in the UK as *blagging* or *bohoing*, is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances.[6] An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (*e.g.*, date of birth, Social Security number, last bill amount) to establish legitimacy in the mind of the target.[7]

This technique can be used to fool a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives.[8] The information can then be used to establish even greater legitimacy under tougher questioning with a manager, *e.g.*, to make account changes, get specific balances, etc.

Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators—or any other individual who could have perceived authority or right-to-know in the mind of the targeted victim. The pretexter must simply prepare answers to questions that might be asked by the victim. In some cases, all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet to create a pretextual scenario.

## Diversion theft

Diversion theft, also known as the "Corner Game"[9] or "Round the Corner Game", originated in the East End of London.

Diversion theft is a "con" exercised by professional thieves, normally against a transport or courier company. The objective is to persuade the people responsible for a legitimate delivery that the consignment is requested elsewhere—hence, "round the corner".

## Phishing

Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN or a credit card number. For example, in 2003, there was a phishing scam in which users received e-mails supposedly from eBay claiming that the user's account was about to be suspended unless a link provided was clicked to update a credit card (information that the genuine eBay already had). Because it is relatively simple to make a Web site resemble a legitimate organization's site by mimicking the HTML code and logos the scam counted on people being tricked into thinking they were being contacted by eBay and subsequently, were going to eBay's site to update their account information. By spamming large groups of people, the "phisher" counted on the e-mail being read by a percentage of people who already had listed credit card numbers with eBay legitimately, who might respond.

### IVR or phone phishing

Phone phishing (or "vishing") uses a rogue interactive voice response (IVR) system to recreate a legitimate-sounding copy of a bank or other institution's IVR system. The victim is prompted (typically via a phishing e-mail) to call in to the "bank" via a (ideally toll free) number provided in order to "verify" information. A typical "vishing" system will reject log-ins continually, ensuring the victim enters PINs or passwords multiple times, often disclosing several different passwords. More advanced systems transfer the victim to the attacker/defrauder, who poses as a customer service agent or security expert for further questioning of the victim.

## Spear phishing

Although similar to "phishing", spear phishing is a technique that fraudulently obtains private information by sending highly customized emails to few end users. It is the main difference between phishing attacks because phishing campaigns focus on sending out high volumes of generalized emails with the expectation that only a few people will respond. On the other hand, spear phishing emails require the attacker to perform additional research on their targets in order to "trick" end users into performing requested activities. The success rate of spear-phishing attacks is

considerably higher than phishing attacks with people opening roughly 3% of phishing emails when compared to roughly 70% of potential attempts. However, when users actually open the emails phishing emails have a relatively modest 5% success rate to have the link or attachment clicked when compared to a spear-phishing attack's 50% success rate.[10]

## Water holing

Water holing is a targeted social engineering strategy that capitalizes on the trust users have in websites they regularly visit. The victim feels safe to do things they would not do in a different situation. A wary person might, for example, purposefully avoid clicking a link in an unsolicited email, but the same person would not hesitate to follow a link on a website he or she often visits. So, the attacker prepares a trap for the unwary prey at a favored watering hole. This strategy has been successfully used to gain access to some (supposedly) very secure systems.[11]

The attacker may set out by identifying a group or individuals to target. The preparation involves gathering information about websites the targets often visit from the secure system. The information gathering confirms that the targets visit the websites and that the system allows such visits. The attacker then tests these websites for vulnerabilities to inject code that may infect a visitor's system with malware. The injected code trap and malware may be tailored to the specific target group and the specific systems they use. In time, one or more members of the target group will get infected and the attacker can gain access to the secure system.

## Baiting

Baiting is like the real-world Trojan horse that uses physical media and relies on the curiosity or greed of the victim.[12] In this attack, attackers leave malware-infected floppy disks, CD-ROMs, or USB flash drives in locations people will find them (bathrooms, elevators, sidewalks, parking lots, etc.), give them legitimate and curiosity-piquing labels, and waits for victims. For example, an attacker may create a disk featuring a corporate logo, available from the target's website, and label it "Executive Salary Summary Q2 2012". The attacker then leaves the disk on the floor of an elevator or somewhere in the lobby of the target company. An unknowing employee may find it and insert the disk into a computer to satisfy his or her curiosity, or a good Samaritan may find it and return it to the company. In any case, just inserting the disk into a computer installs malware, giving attackers access to the victim's PC and, perhaps, the target company's internal computer network.

Unless computer controls block infections, insertion compromises PCs "auto-running" media. Hostile devices can also be used.[13] For instance, a "lucky winner" is sent a free digital audio player compromising any computer it is plugged to. A "road apple" (the colloquial term for horse manure, suggesting the device's undesirable nature) is any removable media with malicious software left in opportunistic or conspicuous places. It may be a CD, DVD, or USB flash drive, among other media. Curious people take it and plug it into a computer, infecting the host and any attached networks. Hackers may give them enticing labels, such as "Employee Salaries" or "Confidential".[14]

One study done in 2016 had researchers drop 297 USB drives around the campus of the University of Illinois. The drives contained files on them that linked to webpages owned by the researchers. The researchers were able to see how many of the drives had files on them opened, but not how many were inserted into a computer without having a file opened. Of the 297 drives that were dropped, 290 (98%) of them were picked up and 135 (45%) of them "called home".[15]

## Quid pro quo

Quid pro quo means *something for something*:

- An attacker calls random numbers at a company, claiming to be calling back from technical support. Eventually this person will hit someone with a legitimate problem, grateful that someone is calling back to help them. The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker

access or launch malware.

- In a 2003 information security survey, 90% of office workers gave researchers what they claimed was their password in answer to a survey question in exchange for a cheap pen.[16] Similar surveys in later years obtained similar results using chocolates and other cheap lures, although they made no attempt to validate the passwords.[17]

## Tailgating

An attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access. Following common courtesy, the legitimate person will usually hold the door open for the attacker or the attackers themselves may ask the employee to hold it open for them. The legitimate person may fail to ask for identification for any of several reasons, or may accept an assertion that the attacker has forgotten or lost the appropriate identity token. The attacker may also fake the action of presenting an identity token.

## Other types

Common confidence tricksters or fraudsters also could be considered "social engineers" in the wider sense, in that they deliberately deceive and manipulate people, exploiting human weaknesses to obtain personal benefit. They may, for example, use social engineering techniques as part of an IT fraud.

A very recent type of social engineering technique includes spoofing or hacking IDs of people having popular e-mail IDs such as Yahoo!, Gmail, Hotmail, etc. Among the many motivations for deception are:

- Phishing credit-card account numbers and their passwords.
- Cracking private e-mails and chat histories, and manipulating them by using common editing techniques before using them to extort money and creating distrust among individuals.
- Cracking websites of companies or organizations and destroying their reputation.
- Computer virus hoaxes
- Convincing users to run malicious code within the web browser via self-XSS attack to allow access to their web account

## Countermeasures

Organizations reduce their security risks by:

**Standard Framework** Establishing frameworks of trust on an employee/personnel level (i.e., specify and train personnel when/where/why/how sensitive information should be handled)

**Scrutinizing Information** Identifying which information is sensitive and evaluating its exposure to social engineering and breakdowns in security systems (building, computer system, etc.)

**Security Protocols** Establishing security protocols, policies, and procedures for handling sensitive information.

**Training to Employees** Training employees in security protocols relevant to their position. (e.g., in situations such as tailgating, if a person's identity cannot be verified, then employees must be trained to politely refuse.)

**Event Test** Performing unannounced, periodic tests of the security framework.

**Inoculation** Preventing social engineering and other fraudulent tricks or traps by instilling a resistance to persuasion attempts through exposure to similar or related attempts.[18]

**Review** Reviewing the above steps regularly: no solutions to information integrity are perfect.[19]

**Waste Management** Using a waste management service that has dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff. Locating the dumpster either in view of employees so that trying to access it carries a risk of being seen or caught, or behind a locked gate or fence where the person must trespass before they can attempt to access the dumpster.[20]

# Notable social engineers

## Kevin Mitnick

Kevin Mitnick is an American computer security consultant, author and hacker, best known for his high-profile 1995 arrest and later five year conviction for various computer and communications-related crimes.[21] He now runs the security firm Mitnick Security Consulting, LLC which helps test companies' security strengths, weaknesses, and potential loopholes. He is also the Chief Hacking Officer of the security awareness training company KnowBe4, as well as an active advisory board member at Zimperium,[22] a firm that develops a mobile intrusion prevention system.[23]

## Susan Headley

Susan Headley was an American hacker active during the late 1970s and early 1980s widely respected for her expertise in social engineering, pretexting, and psychological subversion.[24] An ex-prostitute, she was known for her specialty in breaking into military computer systems, which often involved going to bed with military personnel and going through their clothes for usernames and passwords while they slept.[25] She became heavily involved in phreaking with Kevin Mitnick and Lewis de Payne in Los Angeles, but later framed them for erasing the system files at US Leasing after a falling out, leading to Mitnick's first conviction. She retired to professional poker.[26]

## Christopher Hadnagy

Christopher Hadnagy is a security professional and is recognized for writing the first extensive framework defining the physical and psychological principles of social engineering.[27] He is most widely known for his books, podcast and for being the creator of the DEF CON Social Engineer Capture the Flag and the Social Engineer CTF for Kids.[28]

## Mike Ridpath

Mike Ridpath Security consultant, published author, and speaker. Emphasizes techniques and tactics for social engineering cold calling. Became notable after his talks where he would play recorded calls and explain his thought process on what he was doing to get passwords through the phone and his live demonstrations.[29][30][31][32][33] As a child Ridpath was connected with Badir Brothers and was widely known within the phreaking and hacking community for his articles with popular underground ezines, such as, Phrack, B4B0 and 9x on modifying Oki 900s, blueboxing, satellite hacking and RCMAC.[34][28]

## Badir Brothers

Brothers Ramy, Muzher, and Shadde Badir—all of whom were blind from birth—managed to set up an extensive phone and computer fraud scheme in Israel in the 1990s using social engineering, voice impersonation, and Braille-display computers.[35][28]

## David Pacios

Creator of the concept of applied social engineering to distinguish between digital fraud and social hacking studying. Author of the book *Ingeniería Social Aplicada: Primera linea de defensa*.[36] Known for sharing his knowledge in public talks about human hacking and deep web shopping.

# Law

In common law, pretexting is an invasion of privacy tort of appropriation.[37]

## Pretexting of telephone records

In December 2006, United States Congress approved a Senate sponsored bill making the pretexting of telephone records a federal felony with fines of up to $250,000 and ten years in prison for individuals (or fines of up to $500,000 for companies). It was signed by President George W. Bush on 12 January 2007.[38]

## Federal legislation

The 1999 "GLBA" is a U.S. Federal law that specifically addresses pretexting of banking records as an illegal act punishable under federal statutes. When a business entity such as a private investigator, SIU insurance investigator, or an adjuster conducts any type of deception, it falls under the authority of the Federal Trade Commission (FTC). This federal agency has the obligation and authority to ensure that consumers are not subjected to any unfair or deceptive business practices. US Federal Trade Commission Act, Section 5 of the FTCA states, in part: "Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect."

The statute states that when someone obtains any personal, non-public information from a financial institution or the consumer, their action is subject to the statute. It relates to the consumer's relationship with the financial institution. For example, a pretexter using false pretenses either to get a consumer's address from the consumer's bank, or to get a consumer to disclose the name of his or her bank, would be covered. The determining principle is that pretexting only occurs when information is obtained through false pretenses.

While the sale of cell telephone records has gained significant media attention, and telecommunications records are the focus of the two bills currently before the United States Senate, many other types of private records are being bought and sold in the public market. Alongside many advertisements for cell phone records, wireline records and the records associated with calling cards are advertised. As individuals shift to VoIP telephones, it is safe to assume that those records will be offered for sale as well. Currently, it is legal to sell telephone records, but illegal to obtain them.[39]

## 1st Source Information Specialists

U.S. Rep. Fred Upton (R-Kalamazoo, Michigan), chairman of the Energy and Commerce Subcommittee on Telecommunications and the Internet, expressed concern over the easy access to personal mobile phone records on the Internet during a House Energy & Commerce Committee hearing on "**Phone Records For Sale:** *Why Aren't Phone Records Safe From Pretexting?*" Illinois became the first state to sue an online records broker when Attorney General Lisa Madigan sued 1st Source Information Specialists, Inc. A spokeswoman for Madigan's office said. The Florida-based company operates several Web sites that sell mobile telephone records, according to a copy of the suit. The attorneys general of Florida and Missouri quickly followed Madigan's lead, filing suits respectively, against 1st Source Information Specialists and, in Missouri's case, one other records broker – First Data Solutions, Inc.

Several wireless providers, including T-Mobile, Verizon, and Cingular filed earlier lawsuits against records brokers, with Cingular winning an injunction against First Data Solutions and 1st Source Information Specialists. U.S. Senator Charles Schumer (D-New York) introduced legislation in February 2006 aimed at curbing the practice. The Consumer Telephone Records Protection Act of 2006 would create felony criminal penalties for stealing and selling the records of mobile phone, landline, and Voice over Internet Protocol (VoIP) subscribers.

### HP

Patricia Dunn, former chairwoman of Hewlett Packard, reported that the HP board hired a private investigation company to delve into who was responsible for leaks within the board. Dunn acknowledged that the company used the practice of pretexting to solicit the telephone records of board members and journalists. Chairman Dunn later apologized for this act and offered to step down from the board if it was desired by board members.[40] Unlike Federal law, California law specifically forbids such pretexting. The four felony charges brought on Dunn were dismissed.[41]

## In popular culture

- In the TV show *White Collar*, Matt Bomer played a highly intelligent and multitalented con artist working as an FBI criminal informant.
- In the movie *Identity Thief*, Melissa McCarthy played a fraudster who used pretexting to get the name, credit card number and Social Security number of an executive (Jason Bateman) enabling her to steal his identity and commit credit card fraud.
- In the film *Hackers*, the protagonist used pretexting when he asked a security guard for the telephone number to a TV station's modem while posing as an important company executive.
- In Jeffrey Deaver's book *The Blue Nowhere*, social engineering to obtain confidential information is one of the methods used by the killer, Phate, to get close to his victims.
- In the movie *Live Free or Die Hard*, Justin Long is seen pretexting that his father is dying from a heart attack to have an On-Star Assist representative start what will become a stolen car.
- In the movie *Sneakers*, one of the characters poses as a low level security guard's superior in order to convince him that a security breach is just a false alarm.
- In the movie *The Thomas Crown Affair*, one of the characters poses over the telephone as a museum guard's superior in order to move the guard away from his post.
- In the James Bond movie *Diamonds Are Forever*, Bond is seen gaining entry to the Whyte laboratory with a then-state-of-the-art card-access lock system by "tailgating". He merely waits for an employee to come to open the door, then posing himself as a rookie at the lab, fakes inserting a non-existent card while the door is unlocked for him by the employee.
- In the television show *Rockford Files*, The character Jim Rockford used pretexting often in his private investigation work.
- In the TV show *The Mentalist*, protagonist Patrick Jane often uses pretexting to trick criminals into confessing to the crimes they committed.
- In the TV show *Burn Notice*, many characters are seen using social engineering; in Michael Westen's psych profile it is stated that he is very skilled in social engineering.
- In the TV show *Psych*, protagonist Shawn Spencer often uses pretexting to gain access to locations he would otherwise not be allowed into without police credentials.
- In the videogame *Watch Dogs*, protagonist Aiden Pearce states that he studied social engineering when growing up into a life of crime and uses social engineering tactics to manipulate other characters throughout the game to get the information he wants.
- In the TV show *Mr. Robot*, Darlene scatters USB flash drives (containing malware) outside a prison entrance, baiting a curious guard into compromising the prison's internal network when he plugs one of the drives into his computer workstation.
- In the movie *Who Am I*, the main characters are seen using various social engineering techniques.
- In French novels from Maxime Frantini [*Journal d'un hacker*, *L'ombre et la lumière*, *La cavale*, *La détermination du fennec*], hacker hero Ylian Estevez mainly uses social engineering for its attacks.[42]
- The movie *Mars Needs Women* contains examples of social engineering carried out by the aliens who are shown engaging in and utilizing these techniques to attain their goal: the capture of five Earth women for reproductive purposes to re-infuse their planet's female to male ratio.

## See also

- Certified Social Engineering Prevention Specialist (CSEPS)
- Code Shikara (Computer worm)
- Confidence trick
- Countermeasure (computer)
- Cyber-HUMINT
- Cyberheist
- Internet Security Awareness Training
- IT risk
- Media pranks, which often use similar tactics (though usually not for criminal purposes)
- Penetration test
- Phishing
- Physical information security
- Piggybacking (security)
- SMS phishing
- Threat (computer)
- Voice phishing
- Vulnerability (computing)

# References


1. Anderson, Ross J. (2008). *Security engineering: a guide to building dependable distributed systems* (https://books.google.com/books?id=ILaY4jBWXfcC) (2nd ed.). Indianapolis, IN: Wiley. p. 1040. ISBN 978-0-470-06852-6. Chapter 2, page 17
2. Lim, Joo S., et al. "Exploring the Relationship between Organizational Culture and Information Security Culture." Australian Information Security Management Conference.
3. Anderson, D., Reimers, K. and Barretto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge.publication date Mar 11, 2014 publication description INTED2014 (International Technology, Education, and Development Conference)
4. Schlienger, Thomas; Teufel, Stephanie (2003). "Information security culture-from analysis to change". *South African Computer Journal*. **31**: 46–52.
5. Jaco, K: "CSEPS Course Workbook" (2004), unit 3, Jaco Security Publishing.
6. The story of HP pretexting scandal with discussion is available at Davani, Faraz (14 August 2011). "HP Pretexting Scandal by Faraz Davani" (https://www.scribd.com/doc/62262162/HP-Pretexting-Scandal). Scribd. Retrieved 15 August 2011.
7. "Pretexting: Your Personal Information Revealed (http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre10.shtm)", Federal Trade Commission
8. Fagone, Jason. "The Serial Swatter" (https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html?_r=0). *New York Times*. Retrieved 25 November 2015.
9. "Train For Life" (https://web.archive.org/web/20100105024813/http://www.trainforlife.co.uk/onlinecourses.php). Web.archive.org. 5 January 2010. Archived from the original (http://www.trainforlife.co.uk/onlinecourses.php) on 5 January 2010. Retrieved 9 August 2012.
10. "The Real Dangers of Spear-Phishing Attacks" (https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html). FireEye. 2016. Retrieved 9 October 2016.
11. "Chinese Espionage Campaign Compromises Forbes.com to Target US Defense, Financial Services Companies in Watering Hole Style Attack" (https://www.invincea.com/2015/02/chinese-espionage-campaign-compromises-forbes/). invincea.com. 10 February 2015. Retrieved 23 February 2017.
12. "Social Engineering, the USB Way" (https://web.archive.org/web/20060713134051/http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1). Light Reading Inc. 7 June 2006. Archived from the original (http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1) on 13 July 2006. Retrieved 23 April 2014.
13. "Archived copy" (https://web.archive.org/web/20071011191205/http://md.hudora.de/presentations/firewire/PacSec2004.pdf) (PDF). Archived from the original (http://md.hudora.de/presentations/firewire/PacSec2004.pdf) (PDF) on 11 October 2007. Retrieved 2 March 2012.

14. Conklin, Wm. Arthur; White, Greg; Cothren, Chuck; Davis, Roger; Williams, Dwayne (2015). *Principles of Computer Security, Fourth Edition (Official Comptia Guide)*. New York: McGraw-Hill Education. pp. 193–194. ISBN 978-0071835978.
15. Raywood, Dan (4 Aug 2016). "#BHUSA Dropped USB Experiment Detailed" (https://www.infosecurity-magazine.com/blogs/bhusa-dropped-usb-experiement/). *info security*. Retrieved 28 July 2017.
16. Leyden, John (18 April 2003). "Office workers give away passwords" (https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/). Theregister.co.uk. Retrieved 11 April 2012.
17. "Passwords revealed by sweet deal" (http://news.bbc.co.uk/2/hi/technology/3639679.stm). BBC News. 20 April 2004. Retrieved 11 April 2012.
18. Treglia, J., & Delia, M. (2017). Cyber Security Inoculation. Presented at NYS Cyber Security Conference, Empire State Plaza Convention Center, Albany, NY, June 3-4.
19. Mitnick, K., & Simon, W. (2005). "The Art Of Intrusion". Indianapolis, IN: Wiley Publishing.
20. Allsopp, William. Unauthorised access: Physical penetration testing for it security teams. Hoboken, NJ: Wiley, 2009. 240-241.
21. "Kevin Mitnick sentenced to nearly four years in prison; computer hacker ordered to pay restitution to victim companies whose systems were compromised" (https://web.archive.org/web/20130613162729/http://www.justice.gov/opa/pr/Pre_96/February95/89.txt.html) (Press release). United States Attorney's Office, Central District of California. August 9, 1999. Archived from the original (http://www.justice.gov/opa/pr/Pre_96/February95/89.txt.html) on June 13, 2013.
22. Darlene Storm (19 July 2012). "Interview: World's most famous hacker, Kevin Mitnick, on mobile security & Zimperium" (https://web.archive.org/web/20131226121347/http://blogs.computerworld.com/security/20712/interview-worlds-most-famous-hacker-kevin-mitnick-mobile-security-zimperium). *Computerworld*. Archived from the original (http://blogs.computerworld.com/security/20712/interview-worlds-most-famous-hacker-kevin-mitnick-mobile-security-zimperium) on 26 December 2013.
23. Alex Williams. "Zimperium Raises $8M For Mobile Security That Turns The Tables On Attackers" (https://techcrunch.com/2013/12/20/zimperium-raises-8m-for-mobile-security-that-turns-the-tables-on-attackers). *TechCrunch*. AOL.
24. "DEF CON III Archives - Susan Thunder Keynote" (https://www.defcon.org/html/defcon-3/defcon-3.html). *DEF CON*. Retrieved 12 August 2017.
25. "Archived copy" (https://archive.is/20010417040854/http://home.c2i.net/nirgendwo/cdne/ch14web.htm). Archived from the original (http://home.c2i.net/nirgendwo/cdne/ch14web.htm) on 17 April 2001. Retrieved 6 January 2007.
26. Hafner, Katie (August 1995). "Kevin Mitnick, unplugged" (http://www.tomandmaria.com/ST297/Readings/mitnick%20esquire.htm). *Esquire*. **124** (2): 80(9).
27. "Social Engineering Framework" (http://www.social-engineer.org/framework/general-discussion/). Social-engineer.org. 1 October 2010.
28. *Social Hacking* (http://studall.org/all3-27238.html) (Thesis). Maxim Maximov, Ruslan Iskhakov. Retrieved 11 Feb 2003.
29. *Social Engineering: Manipulating the human* (https://books.google.com/books?id=8Wa9AwAAQBAJ&pg). Scorpio Net Security Services. Retrieved 11 April 2012.
30. "Mobile Devices and the Military: useful Tool or Significant Threat" (https://www.academia.edu/2548183/Mobile_Devices_and_the_Military_Useful_Tool_or_Significant_Threat). academia.edu. Retrieved 11 May 2013.
31. "Social Engineering: Manipulating the human" (https://www.youtube.com/watch?v=uAb0si2u8eI). YouTube. Retrieved 11 April 2012.
32. "BsidesPDX Track 1 10/07/11 02:52PM, BsidesPDX Track 1 10/07/11 02:52PM BsidesPDX on USTREAM. Conference" (http://www.ustream.tv/recorded/17736407). Ustream.tv. 7 October 2011. Retrieved 11 April 2012.
33. "Automated Social Engineering" (http://www.brighttalk.com/webcast/170/34997). BrightTALK. 29 September 2011. Retrieved 11 April 2012.
34. "Social Engineering a General Approach" (http://revistaie.ase.ro/content/70/01%20-%20Greavu,%20Serban.pdf) (PDF). Informatica Economica journal. Retrieved 11 Jan 2015.
35. "Wired 12.02: Three Blind Phreaks" (https://www.wired.com/wired/archive/12.02/phreaks_pr.html). Wired.com. 14 June 1999. Retrieved 11 April 2012.
36. Pacios, David. *Ingeniería Social Aplicada: Promera línea de defensa*. ISBN 1520300263.

37. Restatement 2d of Torts § 652C.
38. "Congress outlaws pretexting" (https://www.congress.gov/bill/109th-congress/house-bill/4709/). *109th Congress (2005-2006) H.R.4709 - Telephone Records and Privacy Protection Act of 2006*.
39. Mitnick, K (2002): "The Art of Deception", p. 103 Wiley Publishing Ltd: Indianapolis, Indiana; United States of America. ISBN 0-471-23712-4
40. HP chairman: Use of pretexting 'embarrassing' (http://news.cnet.com/HP-chairman-Use-of-pretexting-embarrassing/2100-1014_3-6113715.html?tag=nefd.lede) Stephen Shankland, 2006-09-08 1:08 PM PDT *CNET News.com*
41. "Calif. court drops charges against Dunn" (http://news.cnet.com/Calif.-court-drops-charges-against-Dunn/2100-1014_3-6167187.html). News.cnet.com. 14 March 2007. Retrieved 11 April 2012.
42. "Amazon.fr: Maxime Frantini: Livres, Biographie, écrits, livres audio, Kindle" (https://www.amazon.fr/Maxime-Frantini/e/B0081D5VPW/ref=sr_ntt_srch_lnk_4?qid=1474207818&sr=8-4). Retrieved 30 November 2016.

# Further reading

- Boyington, Gregory. (1990). 'Baa Baa Black Sheep' Published by Gregory Boyington ISBN 0-553-26350-1
- Harley, David. 1998 *Re-Floating the Titanic: Dealing with Social Engineering Attacks (http://smallbluegreenblog.files.wordpress.com/2010/04/eicar98.pdf)* EICAR Conference.
- Laribee, Lena. June 2006 *Development of methodical social engineering taxonomy project (http://faculty.nps.edu/ncrowe/oldstudents/laribeethesis.htm)* Master's Thesis, Naval Postgraduate School.
- Leyden, John. 18 April 2003. *Office workers give away passwords for a cheap pen (https://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/)*. The Register. Retrieved 2004-09-09.
- Long, Johnny. (2008). *No Tech Hacking – A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing* Published by Syngress Publishing Inc. ISBN 978-1-59749-215-7
- Mann, Ian. (2008). *Hacking the Human: Social Engineering Techniques and Security Countermeasures* Published by Gower Publishing Ltd. ISBN 0-566-08773-1 or ISBN 978-0-566-08773-8
- Mitnick, Kevin, Kasperavičius, Alexis. (2004). *CSEPS Course Workbook*. Mitnick Security Publishing.
- Mitnick, Kevin, Simon, William L., Wozniak, Steve,. (2002). *The Art of Deception: Controlling the Human Element of Security* Published by Wiley. ISBN 0-471-23712-4 or ISBN 0-7645-4280-X
- Hadnagy, Christopher, (2011) *Social Engineering: The Art of Human Hacking* Published by Wiley. ISBN 0-470-63953-9

# External links

- Social Engineering Fundamentals (http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics) – *Securityfocus.com*. Retrieved on 3 August 2009.
- "Social Engineering, the USB Way" (https://web.archive.org/web/20060713134051/http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1). Light Reading Inc. 7 June 2006. Archived from the original (http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1) on 13 July 2006. Retrieved 23 April 2014.
- Should Social Engineering be a part of Penetration Testing? (http://www.darknet.org.uk/2006/03/should-social-engineering-a-part-of-penetration-testing/) – *Darknet.org.uk*. Retrieved on 3 August 2009.
- "Protecting Consumers' Phone Records" (http://www.epic.org/privacy/iei/sencomtest2806.html), Electronic Privacy Information Center *US Committee on Commerce, Science, and Transportation* . Retrieved on 8 February 2006.
- Plotkin, Hal. Memo to the Press: Pretexting is Already Illegal (http://www.plotkin.com/blog-archives/2006/09/memo_to_the_pre.html). Retrieved on 9 September 2006.
- Striptease for passwords (http://www.msnbc.msn.com/id/21566341/) – *MSNBC.MSN.com*. Retrieved on 1 November 2007.

---