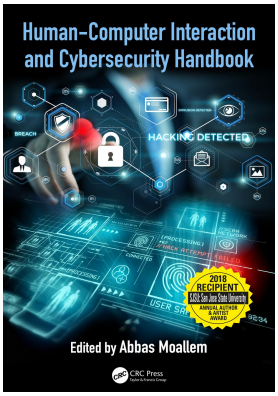


# Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

## Social engineering

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-7
Abbas Moallem
**Published online on: 24 Oct 2018**

*chapter seven*

# *Social engineering*

***Abbas Moallem***

*Contents*



## *7.1 Introduction*

Social engineering is "any act that influences a person to take an action that may or may not be in their best interest" (social-engineer.org 2017). "Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information" (wikipedia.org 2017). These deception techniques have been used throughout human history. They were used for financial gain, access to power, and spying on enemies and especially as war techniques for victory on

the battleground. From olden times, there is the tale of Greeks using a Trojan horse to enter the city of Troy (*Encyclopedia Britannica* 2017) and win the war. Also, we can refer back to Victor Lustig, the man who sold the Eiffel Tower in 1925 (wikipedia.org 2017). Certainly, all of history is full of examples of a human deceiving his/her fellow human. The most memorable films are where viewers find there to be a question of whether the character using deception is good or bad; there are certain moral claims that can serve to justify these otherwise illegal or illicit actions. One might remember the movie *The Sting*, directed by George Roy Hill (1973) telling the story of a young con man, in September 1936, seeking revenge for his murdered partner, who teams up with a master of the big con to win a fortune from a criminal banker or a more recent movie based on the true story of Frank Abagnale. He was one of the most famous impostors claiming to have assumed multiple identities. *Catch Me If You Can*, directed by Steven Spielberg (2002), tells the story of how Frank successfully conned millions of dollars' worth of checks as a Pan Am pilot, a doctor, and a legal prosecutor. Social engineering, and deception techniques now possible with the digital age, have started new lives. There is now the story of Kevin Mitnick (Mitnick and Simon 2002), who used his sophisticated skills to worm his way into many telephone and cell phone networks and vandalize government, corporate, and university computer systems. Arrested in 1995 (BBC 2002), after five years in prison for various computer and communications-related crimes, he wrote about his experience and illustrated the massive scale of social engineering and the effect on the computer security system as a whole.

Using social engineering techniques to access and break into any targeted computer system becomes almost a routine phenomenon with the expansion of the Internet, globalization, and computerization. The scale of usage goes way beyond a few famous cases and rather becomes an entire industry (legal—such as penetration testers—and illegal—such as phishing e-mails). The goal of social engineering techniques is to gain unauthorized access to systems or information to commit acts such as fraud, network intrusion, industrial espionage, or identity theft. Who are these social engineers? The groups or individuals who are or may be "social engineers" include but are not limited to the following:

- Hackers
- Penetration testers
- Spies
- Identify thieves
- Disgruntled employees
- Scammers

In addition to the preceding groups who are using social engineering with criminal intents, some reputable professionals might use social engineering techniques for a legitimate purpose by collecting information for their cases or customers. These professionals might include the following:

- Executive recruiters
- Salespersons
- Governments
- Doctor or psychologists
- Lawyers

## 7.2 Social engineering techniques

Social engineers use different techniques to acquire sensitive information from the legitimate users of a system. Since targeted individuals or organizations who are the victims of social engineering tend to not admit that they were attacked, it has been hard to find real social engineering scenarios, tools, or statistics about cases, outside of the few reported cases by social engineers who wrote and published books or article about their practice (Mitnick and Simon 2002). Another complexity is, of course, that social engineers do not report the tools or technology that they use or the statistics about their successes or failures. The information published is most often the scenarios used in penetration testing or security audits performed by security experts. Social engineers usually take advantage of the flaws in the security design of a technology product to then manipulate people. In a study conducted in New Zealand, Janczewski and Fu (2010) report that 40% of interviewed participants emphasized that in general, security strategies of the organization had poor security policies because they overlooked people errors. Social engineers often use the following techniques to collect needed information for their attacks:

- *Physical location:* Access to physical location such as workplace or home.
- *Phone:* One of the ways that social engineers attack is through phone calls. Social engineers may call using various scripts and pretexts to obtain information.
- *Trashing:* The collection of information through the targeted entity's trash (residential or place of work), which includes old computers, papers, reports, credit card bills, utility bills, medical insurance, bank statements, and similar items.
- *Mail theft*: This occurs when someone targets other people's mailbox and removes mail that has pertinent confidential information on it. As in trashing, a social engineer can obtain credit card bills and bank statements, anything that can be used to obtain detailed information about the targeted individual.
- *Social networking:* Social networking these days is easily accessible, and social engineers use social networking sites to collect information about any target (individual or organization). Technologies such as Google applications, online social networking websites (Facebook, Twitter, LinkedIn, etc.), discussion forums, and blog sites where people and organizations self-disclose all sufficiently feed the social engineer's information needs. According to one study, 93% of respondents in a global survey of 853 information technology (IT) professionals agreed that new technology products and social networking sites are used by social engineers as information-gathering tools (Chitrey et al. 2012). In the same survey, 72% of respondents believe that social engineers use the support of Google applications, 47% for social networking sites (79% for Facebook, 29% for Twitter, and 32% for LinkedIn), 60% for discussion forums, and 38% for blog sites. Huber et al. (2009) substantiated these public impressions in an experiment that confirmed that the information-gathering stage of social engineering can be automated to collect data from Facebook users without being blocked by the system or in another author-automated retrieval of the profile's attributes and list of top friends from MySpace by examining and extracting the relevant tokens in the parsed hypertext markup language code (Alim et al. 2009). Then, the information collected can be used for targeted sending of attached or phishing e-mails.

Sites such as Craigslist (http://craiglist.com) are also favorites for social engineers. The following are two typical cases of how Craigslist is used to hack people.

– Internet fraud case using Craigslist [case captured by A. Moallem (2016)]

> I needed to find a large home in San Diego for a large family gathering. All the places on Airbnb were either booked or too small. I searched all vacation rental sites with no luck, and I was running out of time. Then I remembered that we had once found a very nice vacation rental off Craigslist and had liked the place. Someone had rented out their timeshare. So I checked Craigslist and lo and behold there was a perfect large home at the right price available!
>
> I checked the address on Google Earth against the pictures of the home. All matched and looked great. I emailed, and he gave me a US phone number. I called, and he said since it's close to the rent date I'd have to deposit the check in the account of the co-owner to secure my reservation. Since it was a local Bank of America, I felt secure and did it. Then I sent the good news to the whole family!
>
> As I emailed about the time, when we would get there, and how to get the keys, etc., his answers were a little strange. Suddenly I was alarmed! I Googled the name of the co-owner and found a bunch of fraud cases showing up. I called my bank, but the check had already cleared. I called B of A, and they said they could not do anything. I called the police and they came to my home. I shared the names, emails, phone numbers, Bank of America account number, etc. But they said they could not do anything. The phone number was an Internet disguised one. The account was probably owned by a foreign account they could not prosecute. I could not believe that nothing could be done! At least we found out before all of us showed up at the place.

– Internet fraud case using Craigslist [captured by A. Moallem (2016)]

> I wanted to sell my motorcycle, so I put an ad on Craigslist. I had some inquiries, mostly text messages, and a few phone calls. Among those inquiries, came a text message asking about the condition of my motorcycle and the reason for selling it. After responding to his concerns, the "buyer" said he was satisfied with the condition and the price and willing to purchase it.
>
> Following my policy for doing any internet transactions, I asked him to call me on the phone; he texted back "I'm at work, and calling is restricted." I gave him the benefit of the doubt. Then he texted me: "Okay I'll take it. I'll have to pay you through PayPal because I am currently at the Hanscom Air Force Base in Bedford, Massachusetts. I have a mover that will come for pick up once the payment has cleared in your PayPal account." Then he texted "I added the agent fee of $475 and extra $50 for the MoneyGram charges to make it easier and faster for pick up" so that you have to pay out of your pocket now but would later be compensated. He asked me to send the money through MoneyGram.

> In the meantime, he bombarded me with text messages asking me if I had sent the money. That made me concerned about the whole thing. Therefore, I checked my PayPal account to see if the deposit was made, and I found out there was no fund deposited into my account. I became suspicious and told him that I had not received the money yet. He texted me to check my spam box, I did so, and I saw an email with PayPal logo look, but I was not convinced, therefore I called the PayPal to verify the email and to confirm the deposit, the agent told me there was no email sent from them and no funds were deposited into my account. So I became sure that it was a scam. I was so happy for not continuing the transaction and ended my communication with him by texting him: f*** you.

- *E-mail:* Phishing e-mails are another common way social engineers use targeted attacks on a larger scale to get access to information or the victims. The phishing e-mail continues to be a favorite technique and an easy way to collect credentials, access a user computer, and commit fraudulent e-commerce activities.
- *Shoulder surfing:* Using direct observation techniques, such as looking over someone's shoulder, to get information.
- *Texting:* With two-factor authentication, many people use their mobile phone and texting to set passwords or receive notification alerts from a bank account. Since it is easy to find the cell phone number of people, this has become a favored way to trick users.

No matter which techniques social engineers use to target their attacks, they rely on social psychology and different methods of persuasion to convince their victims. The bottom line is that they must choose the scenarios, pretext, and method of gaining trust and persuasion to be successful. The famous case of Shane MacDougall, who in front of a live audience called a Walmart store manager in a small military town in Canada and obtained a tremendous amount of information about the Walmart store through a convincing pretext and persuasion technique, is a good illustration (Cowley 2012).

In the following section, we will review theoretical foundations used in persuasion.

## *7.3 Theoretical foundations used in social engineering attacks*

The central question one might ask is why and how are social engineers successful? To answer this question, we need to better understand the principles of behavioral and cognitive psychology that social engineers use for their success. In this section, we will review a few fundamental frameworks explaining the principles of human behavior that social engineers successfully use to acquire users' credentials.

### *7.3.1 Schema theory*

The schema theory, first introduced by Frederic Bartlett (1932), works from the perspective that concepts have meaning if they relate to knowledge that an individual already possesses. A schema guides both information acceptance and information retrieval: it affects how humans process new information and how they retrieve old information from long-term memory. Piaget and Cook (1952) called schema the core building blocks

of intelligent "units" of knowledge, each relating to one aspect of the world, including objects, actions, and abstract (i.e., theoretical) concepts. Over our lives, as we learn and discover the world around us, our schemas expand and get complex. The more we know, the bigger and more complex our schemas become. However, the more we are aware, the easier it is to remember new information related to the schema. Thus, since the information exists in our heads, we can relate to it and organize and predict our actions. Activity schemas are called scripts. All of us have many scripts in our long-term memory for a variety of activities. The script will put us in a context, prepare our brain to respond, and prepare our consequent actions based on what we expect to happen. Let us look at the following script as an example:

Person 1: Johnny of computer support, how may I help you?
Person 2: Yes, I seem to have trouble with my laptop computer.
Person 1: What sort of trouble?
Person 2: Well, it wouldn't turn on.
Person 1: Are you in front of your computer right now?
Person 2: Yes.
Person 1: Kindly check if the computer is properly plugged in.
Person 2: Yes, it is.
Person 1: Now try to push the power button on your laptop computer.
Person 2: Ok, nothing happens.
Person 1: Can you please turn on the light in your room?
Person 2: Damn, I think we have no electricity.
Person 1: Sir, I guess that's why you can't turn on your computer.
Person 2: I guess so, thanks a lot.
Person 1: Thank you for calling and we are glad to be of service.

Most people using a computer are very familiar with this type of script and immediately understand that this is a call between a support agent and a customer or user and prepare themselves to answer. Now look at this script (Mitnick and Simon 2002):

Person 1: Good afternoon, this is Mary. How can I help you?
Person 2: Can you connect me to the transportation department?
Person 1: I am not sure if we have one. I'll look in my directory. Who is calling?
Person 2: It's Didi.
Person 1: Are you in the building? Or?
Person 2: No, I am outside the building.
Person 1: Didi who?
Person 2: Didi Sands. I had the extension for transportation, but I forgot what it was.
Person 1: One moment.
Person 2: What building are you in—Lakeview or Main Place?
Person 1: Main Place (pause). It's 805-555-6469 x123.
Person 2: I also want to talk to real estate.
Person 1: 805-555-6469 x456.
Person 2: How about accounts receivable at corporate in Austin, Texas?
Person 1: 805-555-6469 x789.

The social engineer created a script within a context that is very familiar and feasible to the victim, so it is then easy to convince the victim to provide the information needed. Our brains sort out a schema of a person who needs help with information rather than a social engineer to trick for getting information. Social engineers research and prepare a script that fits the norm for their victim's context, so that they will act accordingly. The central goal is ensuring that all the elements are compatible, logical, and natural.



### *7.3.2 Cialdini's six principles of influence*

In social engineering, like many other areas such as marketing, sales, politics, or negotiations, Cialdini's principles for influence are knowingly or unknowingly used to acquire information (Cialdini 1994). A thorough understanding of these principles can not only help prepare people to thwart social engineers but should also result in awareness and behavior modification in cybersecurity employee training.

#### *7.3.2.1 Reciprocity or obligation to repay*

The first principle of Cialdini (2009) is "reciprocity or obligation to repay." According to anthropologists, the rule of reciprocity is apparent in all human societies. Cialdini (2009, p. 23) believes that "one of the reasons reciprocation can be used so effectively as a device for gaining another's compliance is its power. The rule possesses awesome strength, often producing a 'yes' response to a request that, except for an existing feeling of indebtedness, would have surely been refused."

The reciprocity principle is widely used in many professional relationships within politics, marketing, and sales. It is also a common design behavior among all people, shown through actions such as gift giving and receiving or doing a favor and expecting to receive one in return. People feel obligated to reciprocate a gift even if the gift was unwanted. According to Cialdini (2009, p. 33), "a small initial favor can produce a sense of obligation to agree to a substantially larger return favor." For example, a small free token (dinner or drink) at an exhibition might facilitate a much bigger deal. "The rule allows one person to choose the nature of the indebting first favor and the nature of the debt-canceling return favor; we could easily be manipulated into an unfair exchange by those who might wish to exploit the rule."

The reciprocity rules are widely used by social engineers to gain trust and get a favor returned. Imagine that you are driving and got lost somewhere. After asking and receiving help from a passerby, you would be pleased to answer a question about your car or even offer up a bottle of water. Now imagine that you are sitting in a coffee shop struggling with your computer. Somebody seated next to you helps you solve your computer problems and in return asks you to let them use your computer to view an address. Probably, you would not refuse that request. Here is a scenario reported by Mitnick and Simon (2002, p. 248):

> An employee receives a call from a person who identifies himself as being from the IT department. The caller explains that some company computers have been infected with a new virus not recognized by the antivirus software that can destroy all files on a computer, and offers to talk the person through some steps to prevent problems.
>
> Following this, the caller asks the person to test a software utility that has just been recently upgraded to allow users to change passwords. The employee is reluctant to refuse because the caller has just provided help that will supposedly protect the user from a virus. He reciprocates by complying with the caller's request.

In this example, the social engineer gives some help and then puts the victim in a situation that obligates them to "repay."

#### 7.3.2.2 Consistency and commitment

Cialdini's (2009, p. 52) second principle states that "once we have made a choice or taken a stand, we will encounter personal and interpersonal pressures to behave consistently with that commitment." This applies to a variety of human behaviors in politics and the pattern of voting for a specific party, commitments to accept certain deals and policies, and so on. Social engineers use this type of behavior to push victims into revealing information or behaving in certain ways. For example, assume that you and a coworker are coming back from lunch at your office, and one of you scans the smart card to open the door. When you enter, a couple of other people walk in at the same time, or when you enter the office, out of courtesy, you keep the door open for the person after you. Social engineers might use these tailgating techniques to enter a protected zone. Tailgating is a simple scenario for a social engineer to enter a restricted area. If someone has learned the behavior of keeping the door open to let people come in behind them due to politeness, then he/she will consistently do it even when the security policy requires the door to be closed and for the next person to use his/her smart card to open it.

Here is an example of an attack according to Mitnick and Simon (2002, p. 248):

> The attacker contacts a relatively new employee and advises her of the agreement to abide by certain security policies and procedures as a condition of being allowed to use company information systems. After discussing a few security practices, the caller asks the user her password "to verify compliance" with policy on choosing a difficult-to-guess password. Once the user reveals her password, the caller makes the recommendation to construct future passwords in such a way that the attacker will be able to guess it. The victim complies because of her prior agreement to abide by company policies and her assumption that the caller is merely verifying her compliance.

This often happens because people might have experienced the same type of situation in the past with no bad results or consequences. After all, when your computer is not working, and you take it to a repair shop, they ask for your password and you give it voluntarily.

#### 7.3.2.3 Social proof

Cialdini's third principle is social proof, or the power over what others do. It states that "one means we use to determine what is correct is to find out what other people think is correct" (Cialdini 2009, p. 116). A variety of examples is provided in this very widely used principle, but we will use a simple one regarding the ways in which security policies are applied in an organization.

People follow personas that are accepted and considered to be correct. In the application of security policies and when people should follow the rules, social proof is fundamental. Imagine a situation where all coworkers instinctively lock their computer when leaving it behind. If someone does not follow the set behavior, everybody who follows that person will be observing and possibly copying an incorrect behavior. That is the reason why security policy execution is more effective when there is a security culture in an organization. In Western societies, everybody who leaves their home locks their door behind

them; this is considered to be a normal behavior. Now consider whether we do the same for computer or mobile devices and lock them when not using then. After all, we might have even more assets that we want to keep safe than home furniture.

#### *7.3.2.4 Liking*

Liking, or the obligations of friendship, is the fourth principle. According to Cialdini, we like to say "yes" to people whom we like and know on a personal level. The liking principle is primarily used by the salesperson who tries to create a sense of friendship with potential customers. That is why they start by asking some personal questions, such as how many children you have. Then they may acknowledge certain commonalities with potential buyers. During the day, we use this liking approach to get certain activities done more effectively, in customer support calls or whenever we have a request, or even when we want to get a better price with the mechanic's shop that is repairing our car.

Social engineering has become a champion in applying the liking approach. It is meticulously used in scripts and conversations down to the way the social engineers might be dressed or exhibit particular nonverbal behaviors. An effort is made to create a relationship with a victim through physical attractiveness, commonalities (showing shared interests or circumstances), compliments to the victim, cooperating (showing the victim that they have similar beliefs), and finally conditioning and association (showing the victim they hold the same beliefs).

#### *7.3.2.5 Authority*

The fifth principle is that of authority. We obey those in charge. "A multilayered and widely accepted system of authority confers an immense advantage upon society. It allows the development of sophisticated structures to produce resources, trade, defense, expansion, and social control that would otherwise be impossible" (Cialdini 2009, p. 180). Authority is the principle probably used most frequently among all social engineers in phishing attacks or voice calling. The effect of authority is one of the areas in social psychology that is largely observed and backed by research from the Milgram (2009) experiment (1974–2009) on the effect of authority on obedience, up to Zimbardo's Stanford Prison experiment (Wikipedia, 2017), where research concluded that people obey either out of fear or out of a desire to appear cooperative—even when acting against their better judgment and desires. Social engineers use these tactics in voice calling and extensively in phishing e-mails. In voice calling, the caller may pretend to be calling from the Internal Revenue Service (IRS), prosecutor's office, police station, or a law office. Here is a script of a voice call that the author has received on his home phone number:

> Voicemail from (877) 719-4201
>
> Hello, we have been trying to reach you. This call is officially a final notice from IRS internal revenue services. The reason of this call is to inform you that IRS is filing the lawsuit against you. So please call immediately on our department number 8777194201.
>
> I repeat 8777194201.
>
> Thank you.

The following is another example of a phishing e-mail message:

> After the last annual calculation of your financial activity, we have concluded that you are eligible to get the tax refund of $645.

> You may submit the tax refund application and give us 3-9 days to process it.
> A refund can be hindered by many different reasons.
> E.G. submitting invalid records or not meeting a deadline.
> To get information about your tax refund, please Open this link.
> Sincerely,
> Tax Refund Department
> Internal Revenue Service

Again in this e-mail, the IRS, that is, the Internal Revenue Service in the United States, is used to create fear and seek obedience. In fact, the IRS retains the legal authority to enforce liens and seize assets without obtaining a judgment in court.

#### *7.3.2.6 Scarcity*

The sixth principle is scarcity. It relies on the observation that we want what may not be available. The scarcity tactic operates on the value that people attach to things. Scarcity suggests that things are more valuable when they are less available. The scarcity tactic involves the "limited-number" or "deadline technique." The deadline technique works because it puts an official time limit on the product availability. The "limited-number" tactic works because it creates added value to a product by reducing the availability of the product. This tactic is widely used in marketing and particularly in e-commerce very effectively by underlying perhaps a discounted flight or hotel reservation with a limited number of seats or rooms at the discounted prices. Since people are very familiar with this pattern, it is primarily used by social engineers when sending a phishing e-mail about winning a prize, limited time offers of reduced subscription rates, and so on, using very famous e-commerce sites such as fake Amazon or Netflix offers. This is also an effective tactic for fake e-commerce sites. The fake sites may offer a huge discount on a specific product so people impressed by the discount place orders, not knowing that the site was not secure and their data are compromised by identity theft and fraud.

### *7.3.3 Stajano and Wilson principles*

To understand the general principles of human behavior that explain how scams worked, Stajano and Wilson (2009) studied a variety of scams and "short cons" that were investigated, documented, and recreated for the BBC TV program "The Real Hustle" and then extracted from them some general principles about the recurring behavioral patterns of victims that hustlers have learned to exploit. This study extrapolates several principles helping us understand where people are vulnerable to specific attacks. The followings are the suggested principles:

#### *7.3.3.1 Distraction principle*

While you are distracted by what retains your interest, social engineers can obtain what they want without you noticing. Here is an example:

> The young lady who falls prey to the recruitment scam is so engrossed in her task of accurately compiling her personal details into a form to maximize her chances of finding a job that she utterly fails even to suspect that the whole hiring agency might be fake.

In this case, the user is eager to get a job that is set to be really attractive; thus, she would provide all sorts of information to get a job without questioning the validity of the

agency and why she should be answering the questions that are not relevant to the job. Distraction is at the center of many fraud scenarios; it is also a fundamental ingredient of most magic performances. The authors underline the use of distraction as successful tools used to divert attention the same way as magicians manipulate attention and awareness to show their magic. (Macknik et al. 2008)

Stajano and Wilson believe that "it's not that the users are too lazy to follow the prescribed practice on how to operate the security mechanisms, but rather that their interest is principally focused on the task, much more important to them, of accessing the resource that the security mechanisms protect. The users just see what they're interested in (whether they can conveniently access the resource) and are blind to the fact that those annoying security mechanisms were put there." Thus, social engineers, like magicians, use these human vulnerabilities to achieve their goals. They divert the attention of the victim and manipulate them so that they provide answers to the attacker's questions.

#### *7.3.3.2 Social compliance principle*

Social compliance works like Cialdini's principle of consistency and commitment in that it is based on the way society trains people not to question authority. In phishing, this may present itself as a website that replicates the appearance of a bank's site and directs customers to it to steal their online banking credentials. The lesson for the security architect is that people are trained as a citizens to obey commands from authorities, who can be government agents (i.e. police officers), doctors or, in this case, a system administrator managing the network. This behavior can be a double-edged sword. Although people are pretty good at recognizing people they already know (by face, by voice, by shared memories, etc.), they are not very good at all at authenticating strangers, whether over a network, over the phone, or even in person. Incentives and liabilities must be coherently aligned with the overall system goals. If users of a product are expected to perform extra checks rather than subserviently submitting to orders, then social protocols must change to make this acceptable. Conversely, if the product's users are expected to obey authority from the company unquestioningly, those who exercise the authority must offer safeguards to relieve users of liability and compensate them if they fall prey to attacks that exploit the social compliance principle. The fight against phishing and all other forms of social engineering can never be won unless this principle is understood and taken on board.

#### *7.3.3.3 Herd principle*

"Even suspicious marks will let their guard down when everyone next to them appears to share the same risks" (Stajano and Wilson 2009, p. 13). This principle is based on the common recognition that people look at people around them to gain confidence in their actions. If you, as a customer, are seeing many people shop around you or purchase from a specific e-commerce site or if you are seeing that large numbers have reviewed a product or service, then these actions of others become a source of increased confidence motivating toward a purchase decision. However, all of this information may have been falsely created. A fraudulent site can easily simulate many reviews, shoppers, and almost all aspects of a legitimate site review or activity credential to gain consumer confidence. It is not hard for a hacker to create multiple aliases and set up a fake Facebook site with hundreds of friends or likes to gain the trust of his/her victims.

#### *7.3.3.4 Dishonesty principle*

Anything illegal you do will be used against you by the fraudster, making it harder for you to seek help. A prime example of this principle is the gadget scam. Imagine individuals

who bought a machine that can create prepaid credit cards. If it worked, it would clearly be illegal. Therefore, once they discover that it does not work, they cannot go to the police and complain about the seller, because the police might ask questions about what they intended to do with the device.

#### *7.3.3.5 Need and greed principle*

Your needs and desires make you vulnerable. When social engineers know what you want, they can easily manipulate you.

#### *7.3.3.6 Time principle*

When you are under time pressure to make an important choice, you use different decision-making strategies. Time, like "scarcity," pushes people to use less reasoning and rush to make unreasoned judgments.

### *7.3.4 Cialdini principles and phishing mails*

The phishing e-mail, despite the advent of some technological tools to capture them, is still a very useful tool for social engineers. The main reason is that phishing e-mails use deception techniques or, in the case of targeted attacks, very particular persuasion techniques. Social engineers, through a collection of data (manually or automatically) from social networking, can create a very specific context that seems very realistic to a recipient. Let us use a very simple example: Imagine you get an e-mail to your personal or professional e-mail address. The e-mail seems to be coming from your manager, informing you that in the management meeting the previous day, they talked about your efforts and performance. The manager says that they insisted on giving you a special bonus. They also provide a link to self-report some of your achievements arguing that the human resource (HR) department needs this information to process your bonus. When you click the link to enter your performance, the form requires you to log in with your username and password before reporting your achievements. You might not pay attention that this is not your usual HR application, but rather a Google form owned by social engineers outside your company who only wish to gain access to your authentication and password. Social engineers will effectively use some of the preceding persuading principles to acquire your trust and collaboration so that everything will work well for you. The decision-making in these cases is not governed by how smart the person may be, but by the contexts created through the psychological environment and how information is presented.

One study (Ferreira et al. 2015) investigated how the principles of Cialdini, Gragg, and Stajano (2003) relate to one another and tried to create more general principles of persuasion in social engineering. To do this, they organized a collection of phishing e-mails according to their goals: data theft, malware, and fraud. Then they tried to find patterns based on the principles of persuasion in social engineering. The results demonstrated that the most commonly used principles of social engineering are liking and similarity and deception followed by distraction. The next most common principles are authority for data theft; e-mail and malware; and commitment, reciprocation and consistency for malware and fraud e-mails.

## *7.4 Defense against social engineering attacks*

In the expansion and evolution of social engineering attacks against people and organizations, it is essential to be preventive and protected. Contrary to technological attacks

such as malware, viruses, or other types of hacking, protecting people and organizations against social engineering attacks is not that simple. The complexity comes from the fact that people have a hard time distinguishing lies from truths and perform very poorly at detecting deception. This poor performance happens despite the existence of ample cues that people can consider in determining deception. There is substantial psychological literature relating why people lie and how lies can be detected. Vrij (2000) has reviewed the relevant research on lying and detection in detail and shown that people are particularly poor at detecting lies (44% accuracy rate). DePaulo et al. (1985) and Bond and DePaulo (2006) report that the percentage of lie detection ranges from 45 to 60% when 50% accuracy is expected by chance alone. The psychological studies suggest that the poor performance in distinguishing lies from truth is related to factors such as cognitive biases (Burgon and Levine 2009). People tend to reason in a way that confirms their assumptions and ways of thinking even when the conclusion leads to systematic deviations from rationality or good judgment. In very recent history, we can observe how fake news (during the 2016 election in the United States) was used to influence and shape public opinion even when sufficient cues were available to differentiate facts from lies. (Allcott and Gentzkow 2017) There is the use of "heuristics" or "mental shortcuts," processes where one focuses on one aspect of a complex problem while ignoring other pertinent facts. Since honest behavior, in general, is most frequent, people tend to expect to hear the truth and are reluctant to think that the "truth" they are hearing is actually a "lie."

In differentiating attributes of a lie from the truth, research suggests that 62.2% of people think that individuals who lie tell longer stories than usual, pause in the middle of speaking, and use terms with less emotion or feeling (Bond 2006).

Since people have a hard time detecting lies or identifying if a social interaction comes from social engineers or reliable sources, we become motivated to find a technology or an automatized tool that can be used to filter fake, fraudulent interactions. Qin and Burgoon (2007) designed an experiment on deception detection where the performances of the human and an automated system were compared. The attributes in each deceptive case included the following:

- Vocal cues (talking time and speech disturbance such as vocalized pause and nonvocalized pause) and verbal cues
- Quantity [number of words, verbs, and complexity (syntactic complexity or average sentence length)]
- Diversity (lexical diversity, content word diversity, and redundancy)
- Specificity (temporal immediacy and temporal nonimmediacy)
- Affect (activation, pleasantness, and imagery)
- Uncertainty (modal verbs) and verbal (nonimmediacy: passive voice)

The results showed that the automated system using discriminant analysis to classify deception performed significantly better than humans in detecting deception. Humans in this study tended to judge all messages from the perspective of "senders as truthful," even when they knew about the possibility of error in human judgment. The result of this study confirms the previous study about the application of "cognitive heuristics" or "preconceived expectations for truthfulness" by people in detecting the deceptions (Chaiken 1980).

However, we still lack the general availability of reliable automated systems to augment human judgment in detecting deceptive calls, e-mails, or even face-to-face communication. The main issue continues to be the vulnerability of individuals who can be

manipulated in different ways. There is not and cannot be one type of protection that can be applied to all people because every human may be vulnerable in different areas. Thus, security needs to first identify the vulnerabilities for each group of people and then establish policy, training, and awareness measures. According to Gragg (2003), the defensive measure against social engineers should be "a multi-layered defense" that would include the following:

- Functional level: security policy
- Parameter level: security awareness training for all
- Fortress level: resistance training for key employees
- Gotcha level: social engineering land mines
- Offensive level: incident response

### 7.4.1 *Information security policy*

One of the foundations of protection against social engineering is having an information security policy (ISP). An ISP addresses data, programs, systems, facilities, tech infrastructure, users of technology, and third-party organizations. It provides employees with guidelines concerning how to ensure information security when they utilize information systems to perform their jobs. For such a policy to be effective, however, employees must comply with the ISP. Thus, the effectiveness of the ISP is not measured by how well the policy is defined and written, but rather by the degree of employee compliance with the policy. The employee's motivation to comply with their organization security policy is the key foundation for the success of the ISP. It is important that motivating factors and why it is important to comply with security policy are explained to employees, convincing them to comply with the ISP of the organization.

In addition, the organization must ensure that the ISP being implemented does not solely rely on technology-based solutions (Ernst and Young 2008). Both technical employees and human resource staff are authorized to use information systems. Several researchers have found that employees' abusive behavior and misuse of information systems, together with noncompliance with security policy, are information security risks. (Stanton et al. 2005) Some research applied the theory of planned behavior (TPB) (Ajzen 1991), to study the employees' behavior and intention in complying with the ISP. According to TPB, the attitude toward behavior, subjective norms, and perceived behavioral control together shape an individual's behavioral intentions and behaviors.

People have a positive attitude toward the actions when they perceive that they can control behaviors. This attitude also applies to the employee's intention to comply with the ISP of the organization. The results provide some evidence of the significant impact of motivational factors other than rewards and sanctions that reinforce an employee's compliance behavior. Bulgurcu et al. (2010) suggest that information security awareness (ISA) programs should be designed to focus employees' beliefs on cost and benefit, safety, and vulnerability and to create a security-aware culture within the organization to improve information security. Therefore, organizations should create security awareness training programs to ensure sufficient awareness and understanding on risk issues.

### 7.4.2 *Security awareness training*

In general, most people do not have comprehensive training on computer security. Their knowledge is limited to some sporadic sources of information. For example, a user might

buy a router to equip his/her home or office with a wireless network and follow some general steps to set its password and connect to the Internet. The user does not necessarily learn about home networking and security issues, how hackers attack, and so on. Similarly, companies invest a tremendous amount on technology solutions. However, the budget to train and educate employees on security issues is extremely limited, often only covering online trainings that employees are required to take.

Several studies have investigated the effectiveness of company awareness programs and information security training. The study conducted by Bulgurcu et al. (2010) suggests that ISA influences employee attitudes, directly and indirectly, to directly comply with the ISP. A meta-analysis conducted by Hauch et al. (2016) showed that training improved the overall ability to detect deception. Burgoon et al. (2008) conducted two studies with IT specialists in the US Armed Forces. They found that that their developed e-training system was successful for both teaching managers and employees to improve their participants' ability to detect deception. These training approaches focused on web-based trainings that taught people how to recognize the "cues" that deceivers unwittingly give out. They also showed that people who had been trained were able to "recognize the tactics that deceivers might use to hide the truth. Deception tactics are domain-specific, but deception cues are not context-specific. This means that cue-based training is applicable in a wide variety of organizations" (Burgoon et al. 2008).

### 7.4.3 *Resistance training for key employees*

Training, awareness, and knowledge by all individuals or employees are essential to prevent social engineering attacks. However, the training and awareness of some key employees is even more important since they might be more targeted than others. According to Gragg (2003), key employees include help desk personnel, customer service, business assistants, secretaries, receptionists, and system administrators/engineers. It is fundamental that people in these roles be trained and adequately prepared not to be persuaded in giving information away to social engineers. Gragg identified these techniques as follows:

- Inoculation: Employees would be exposed to the weakened arguments that will be used by the social engineer and anticipate the arguments of the social engineer (Sagarin 2002, p. 527).
- Forewarning: by warning employees how social engineers might use their vulnerabilities to persuade them to give them information that they want to acquire.
- Reality check: by making employees aware of their unrealistic optimism. Thus, they should not ignore legitimate risks.

### 7.4.4 *Persistence level*

One training and awareness program is not sufficient to protect people against social engineers who are creative and constantly designing new techniques. The key employees should particularly be regularly reminded and retrained about the new techniques and social engineering approaches.

### 7.4.5 *Gotcha level*

The Gotcha level defense is performed by alerting targeted employees about an attack that is in progress and how they should be prepared to address it and suggesting

techniques that they need to use. The techniques include but are not limited to the following:

- Be on the lookout for a security risk in the form of the physical presence of a social engineer—for example, an unapproved or expired badge or unescorted visitor.
- Monitor a centralized security log of events.
- Not calling back an individual who requests a password reset or requests information.
- Verifying the identity of anyone who is calling and trying to get information about the company.

### 7.4.6 *Offensive level*

This level involves creating a well-defined process that an employee can begin as soon as they suspect that something is wrong and go aggressively after the hacker and proactively inform potential victims, security professionals, and IT in the company.

## 7.5 *Conclusion*

Social engineering is an evolving practice with many sources of new perpetrators. Social engineers use well-known techniques and continually explore to find new ways to use human behavior to exploit the weakness in people unable to distinguish lies from truth to acquire information. Until technology offers automatic solutions to help users in detecting the lies and protecting people from being victims of social engineers, users will be required to gain awareness and knowledge to protect themselves from deception techniques. Cybersecurity experts should be constantly evaluating and detecting tactics of social engineering and providing efficient warning and training to protect personal and organizational assets.

## *References*

Ajzen, I. (1991): The theory of planned behavior, *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, 179–211.

Alim S., Abdul-Rahman R., Neagu D., and Ridley M. (2009): Data retrieval from online social network profiles for social engineering applications. *2009 International Conference for Internet Technology and Secured Transactions*, 1–5.

Allcott H., and Gentzkow M. (2017): *Social Media and Fake News in the 2016 Election*, January 2017. https://web.stanford.edu/~gentzkow/research/fakenews.pdf.

BBC (2002, October 14): *Mitnick, Kevin. How to Hack People*. http://news.bbc.co.uk/2/hi/technology/2320121.stm.

Bond, C. F. (2006): A world of lies: The global deception research team. *Journal of Cross-Culture Psychology*, vol. 37, no. 1, 60–74.

Bond, C. F., and DePaulo, B. M. (2006): Accuracy of deception judgments. *Personality and Social Psychology Review*, vol. 10, no. 3, 214–234.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010, September): Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, vol. 34, no. 3, 523–548.

Burgoon, J. K., and Levine, T. R. (2009): Advances in deception detection. In S. W. Smith and S. R. Wilson (Eds), *New Directions in Interpersonal Communication Research* (pp. 201–220).

Burgoon, J. K., George, J. F., Biros, D. P., Nunamaker Jr., J. F., Crews, J. M., Cao, J., Marett, K., Adkins, M., Fruse, J., and Lin, M. (2008): The role of e-training in protecting information assets against deception attacks. *MIS Quarterly Executive* 7(2) June 2008. https://www.researchgate.net/publication/220500702_The_Role_of_E-Training_in_Protecting_Information_Assets_Against_Deception_Attacks.

Chaiken, S. (1980): Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology*, vol. 39, no. 5, 752–766.

Chitrey, A., Singh, D., Bag, M., and Singh, V. (2012, June): A comprehensive study of social engineering based attacks in India to develop a conceptual model. *International Journal of Information & Network Security*, vol. 1, 45–53.

Cialdini, R. B. (1994): *Influence: The Psychology of Persuasion*. Collines Business. New York, NY: Harper Collins Publishers.

Cialdini, R. B. (2009): *Influence: Science and Practice* (5th ed.) (pp. 19, 52, 116, 180, 248). Boston, MA: Pearson Education.

Cowley, S. (2012, August 8): How a lying "social engineer" hacked Wal-Mart. *CNNMoney*. http://money.cnn.com/2012/08/07/technology/walmart-hack-defco.

DePaulo, B. M., Stone, J. I., and Lassiter, G. D. (1985): Deceiving and detecting deceit. In B. R. Schlenker (Ed.), *The Self and Social Life* (pp. 323–370). New York: McGraw-Hill.

*Encyclopedia Britanica* (2017): Trojan horse, Greek mythology (update 2015). https://www.britannica.com/topic/Trojan-horse.

Ernst & Young (2008): *Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey*. Ernst & Young, London. http://130.18.86.27/faculty/warkentin/SecurityPapers/Merrill/2008_E&YWhitePaper_GlobalInfoSecuritySurvey.pdf.

Ferreira A., Coventry L., and Lenzini G. (2015): Principles of persuasion in social engineering and their use in phishing. In *Human Aspects of Information Security, Privacy, and Trust*, vol. 9190 of the series Lecture Notes in Computer Science (pp 36–47).

Gragg, D. (2003): *A Multi-Level Defense Against Social Engineering*. SANS Institute InfoSec Reading Room, Singapore. https://www.sans.org/reading-room/whitepapers/engineering/multi-level-defense-social-engineering-920.

Hauch, V., Siegfried, L., Sporer, S. L., and Meissner, C. A. (2016): Does training improve the detection of deception? A meta-analysis. *Communication Research*, vol. 43, no. 3, 283–343.

Hill, G. R. (1973): *The Sting*, Written by David S. Ward, starring Stars: Paul Newman, Robert Redford, Robert Shaw. http://www.imdb.com/title/tt0070735/.

Huber, M., Kowalski, S., Nohlberg, M., and Tjoa, S. (2009): Towards automating social engineering using social networking sites. *IEEE International Conference on Computational Science and Engineering. CSE '09 Proceedings of the 2009 International Conference on Computational Science and Engineering*—Volume 03, 117–124.

https://www.social-engineer.org/.

https://www.wikipedia.org/.

Janczewski, J. L., and Fu, L. (2010): Social engineering-based attacks—Model and New Zealand perspective. *Proceedings of the International Multiconference on Computer Science and Information Technology*, 847–853.

Leahey, Th. H., and Harris, R. J. (2001): *Learning and Cognition* (p. 234). Upper Saddle River, NJ: Prentice Hall.

Macknik, S. L., King, M., Randi, J., Robbins, A., Teller, Thompson, J., and Martinez-Conde, S. (2008): Attention and awareness in stage magic: Turning tricks into research. *Nature Reviews Neuroscience*, vol. 9, 871–879, http://dx.doi.org/10.1038/nrn2473.

Milgram, S. (2009): *Obedience to Authority: An Experimental View* (9th ed.). New York: Harper and Row.*

Mitnick, K. D., and Simon W. L. (2002): *The Art of Deception: Controlling the Human Element of Security* (pp. 22, 246, 248). Hoboken, NJ: Wiley.

Piaget, J., and Cook, M. T. (1952): *The Origins of Intelligence in Children*. New York: International University Press.

Qin, T., and Burgoon, J. (2007): An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. In *Intelligence and Security Informatics*. Piscataway, NJ: Institute of Electrical and Electronics Engineers.

* An excellent presentation of Milgram's work is also found in Brown (*Social Forces in Obedience and Rebellion. Social Psychology: The Second Edition*. New York: Free Press, 1986).

Sagarin, B. J., Cialdini, R. B., Rice, W. E., and Serna, S. B. (2002): Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion. *Journal of Personality & Social Psychology*, vol. 83, no. 3, 526–541.

Spielberg, S. (2002): *Catch Me If You Can*, written by Jeff Nathanson and Frank Abagnale Jr, Starring Leonardo DiCaprio, Tom Hanks, Christopher Walken. http://www.imdb.com/title/tt0264464/.

Stajano, F., and Wilson, P. (2009, August): Understanding scam victims: Seven principles for systems security. University of Cambridge Computer, United Kingdom UCAM-CL-TR-754, ISSN 1476-2986 (Page 36). https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf.

Stanford prison experiment (2017): Stanford prison experiment, Wikipedia, Accessed March 2017, https://en.wikipedia.org/wiki/Stanford_prison_experiment

Stanton, J. M., Stam, K. R., Mastrangelo, P., and Jolton, J. (2005, March): Analysis of end user security behaviors. *Computers & Security*, vol. 24, no. 2, 124–133.

Victor Lustig (2017): Wikipedia, Accessed March 2017, https://en.wikipedia.org/wiki/Victor_Lustig

Vrij, A. (2000): *Detecting Lies and Deceit: The Psychology of Lying and the Implications for Professional Practice*. Chichester: Wiley.

What is Social Engineering (2017): social-engineer.org, Accessed March 2017, https://www.social-engineer.org/about/.