Social Engineering

Chapter · October 2021

DOI: 10.1007/978-3-319-78440-3_38

2 authors:

Jan-Willem H. Bullée

22 PUBLICATIONS **294** CITATIONS

SEE PROFILE

Marianne Junger

University of Twente

252 PUBLICATIONS **4,527** CITATIONS

SEE PROFILE

Social Engineering

Jan-Willem Bullée and Marianne Junger

Contents

J.-W. Bullée (✉)
Linköping University, Linköping, Sweden
e-mail: jan-willem.bullee@liu.se

M. Junger
University of Twente, Enschede, The Netherlands
e-mail: m.junger@utwente.nl

T. Holt, A. M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, https://doi.org/10.1007/978-3-319-90307-1_38-1

Abstract

Social engineering is the usage of social manipulation and psychological tricks to make the targets assist offenders in their attack. Among computer scientists, social engineering is associated with calling a target and asking for their password. However, this threat can manifest itself in many forms. In this chapter, four modalities of social engineering (i.e., voice call, email, face-to-face, and text message) are discussed. We explain the psychological concepts that are involved in social engineering. Including (i) why do people get victimized and (ii) how do offenders abuse the flaws in human reasoning. A series of field studies illustrates the sucess of social engineering. Furthermore, which group is most vulnerable to social engineering and to what extent do interventions counter the attack? Finally, we discuss some difficulties in investigating social engineering and conclude with some suggestions for future research.

Keywords

Awareness · Cognitive bias · Deception · Fraud · Intervention · Manipulation · Phishing · Scam

Acronyms

2FA	Two-factor authentication
CMC	Computer-mediated communication
CPR	Cardiopulmonary resuscitation
F2F	Face-to-face
PBX	Private branch exchanges
VCFA	Verification code forwarding attack

What Is Social Engineering?

> You have been traveling and just checked into your hotel room. As you walk into your room and set your bag down, your room phone rings. A nice girl introduces herself as Rebecca from the hotel front desk. She explains there has been an issue during check-in and she needs to re-confirm your credit card information. Assuming she is calling from the hotel front desk, you provide your credit card information. She then informs you everything has been resolved and to enjoy your stay.

The person who rang the traveler was not Rebecca from the front desk. Instead, it was an offender ringing every hotel room in an attempt to victimize someone. What happened that made the traveler give away his credit card details to a stranger? The scenario (The SANS Institute 2012) illustrates what is known as a social engineering attack. Abraham and Chengalur-Smith (2010) proposed the following definition: "*The use of social disguises, cultural ploys, and psychological tricks to get computer users (i.e., targets) to assist hackers (i.e., offenders) in their illegal intrusion or use of computer systems and networks.*" Social engineering can be conceived as a nontechnical type of attack based on human interaction complementing technical

attacks. One of the dangers of social engineering attacks is their harmless and legitimate appearance so that targets (i.e., a person and not the goal of the attack) are unaware of being victimized (The Federal Bureau of Investigation 2015; Hadnagy and Wilson 2010). The use of physical violence, extortion, bribery, blackmailing, and the like are not considered social engineering.

Cybersecurity incidents are more often caused by human failure (Chan et al. 2005) than by technology failure (Schneier 2000b). Consequentially, humans are the weakest link in information security (Happ et al. 2016). To put it bluntly: "*only amateurs attack machines, professionals attack humans"* (Schneier 2000a). Deception and manipulation are used by offenders to make targets assist in their victimization (Bosworth et al. 2014). The social engineering attack vector is considered the biggest threat to information systems (Rouse 2006).

In this chapter, we explain what social engineering is, including how this attack works, how successful it is, and what can be done to reduce victimization. The use of deception and fraud has been around for a long time. The next section provides a brief overview of some of the notable cases.

History of Social Engineering

Social engineering has been used already for quite some time as an attack vector. Below is a short overview of six notorious social engineering cases from ancient (and not-so-ancient) history.

Trojan War Perhaps one of the oldest accounts of social engineering is from Odysseus of the ancient Greek army. After a long decade of war with the Trojans, the Greek army retreated from the arena and left the Trojans a colossal wooden horse statue. The Trojans welcomed their gift into their city and celebrated the victory. During the night, Greek soldiers appeared from within the horse, and they conquered the city (Graves 1992). Myth or not, this example illustrates how the human element is tricked into achieving a goal that was impossible by technical means only.

Frank Abagnale The story of former conman Frank Abagnale has been told many times in books, musicals, and the film *Catch Me If You Can* (Internet Movie Database 2002). After his parents' divorce, teenager Frank ran away from home and was alone in the world. What started as a creative way to survive turned in a game. While he was only 16 years old, Frank managed to pose as a pilot for Pan Am Airlines. Later he pretended to be a resident pediatrician, an attorney, and allegedly a teaching assistant. Frank mastered the skill of forging checks, and by defrauding banks between age 16 and 21, he made $2.5 million. Eventually, however, he was caught and put in jail. Since his release, he has worked closely with the FBI for almost 40 years (Solon 2017).

Stanley Mark Rifkin Stanley Mark Rifkin worked as a computer consultant for the Security Pacific Bank in Los Angeles, in 1978. He was working on the development of a backup system for the wire room, which gave him access to the procedures on how the bank transfers money. A secret daily rotating code was needed to make a transfer. Stanley learned that the clerks wrote the code down on

a sticky note to save them from the trouble of memorizing it. By learning this code, Stanley managed to transfer $10.2 million to an offshore account in Switzerland. He had pulled off the biggest bank heist in the history, without using any violence or computer (Mitnick and Simon 2002).

ABN-AMRO In Antwerp (Belgium), the diamond capital of the world, €21.5 million worth in diamonds were stolen. Without the use of any violence, the offender managed to pull off this heist. His weapon? The offender, a regular customer, got to know the employees. By using charm and buying chocolates for personnel, he managed to copy the keys of the vault (Castle 2007).

Kevin Mitnick Kevin Mitnick is known as the world's most famous hacker and as the person who popularized the term "social engineering." In one of his early accounts, he social engineered a bus driver, which combined with a little dumpster diving, resulted in free bus rides (Gots 2011). In later years, Kevin applied his social engineering skills through the telephone. By carefully preparing the attacks, he was able to get access to parts of many Private Branch Exchanges (PBX) phone systems, which, among others, allowed him to make free long-distance calls. In 1993, Kevin was investigated by the FBI and convicted of several computer-related crimes (Mitnick and Simon 2002; Gots 2011).

RSA Security LLC breach In March 2011, a group of offenders used social engineering techniques to hack into RSA Security, the company (named after the initials of cofounders Ron Rivest, Adi Shamir, and Leonard Adleman) known for the RSA two-factor authentication tokens. By using social engineering via email (i.e., email phishing), the offender persuaded an employee to open an attached malware-containing spreadsheet file. The malware installed a backdoor that allowed the offender access to the machine. From there the offender was able to browse the network (Richmond 2011). The estimated cost of the breach was $66.3 million. In the period after the breach, RSA's gross margins narrowed from 67.6% to 54.1% (King 2011). Another aspect of the breach is the reputation damage RSA Security encountered. In the security business, one is only as good as one's reputation. The real impact of this attack is unknown; however, it gave the competition an opening for closing in (Savage 2012).

These six scenarios show that social engineering has been around for some time and can occur in different ways. The next section discusses in what forms social engineering can occur.

Different Types of Social Engineering, Their Success, and Countermeasures

There are endless ways in which attackers can trick other humans for their benefit. The Dutch Fraud Help Desk discerns 99 types of fraud; 12 being broad concepts (e.g., money laundering), 28 types are related to cyber (Information available at www.fraudehelpdesk.nl.). The FBI discerns 33 crime types (Internet Complaint Center (IC3) 2018a) and describes 18 online crime schemes (Internet Complaint Center (IC3) 2018b) (Namely: (1) Auction Fraud; (2) Auction Fraud – Romania; (3)

Counterfeit Cashier's Check; (4) Credit Card Fraud; (5) Debt Elimination; (6) Parcel Courier Email Scheme; (7) Employment/Business Opportunities; (8) Escrow Services Fraud; (9) Identity Theft; (10) Internet Extortion; (11) Investment Fraud; (12) Lotteries; (13) Nigerian Letter or "419"; (14) Phishing/Spoofing; (15) Ponzi/Pyramid; (16) Reshipping; (17) Spam; (18) Third Party Receiver of Funds). One way to categorize social engineering is by the type of communication with the victim. In this section, we explore four modalities offenders can use in social engineering, how successful they are, and the success of their countermeasures.

Voice Call

Social engineering via the telephone is also known as a phone scam, technical support scam, or cold call. For instance, since 2008, "the Microsoft scam" is carried out globally by offenders claiming to be employees of the Microsoft technical department (Arthur 2010). At first, native English speaking countries were targeted and later the rest of the world. The scam's script is as follows: the target receives a phone call at home, the offender introduces himself as an employee of the Microsoft technical department and informs the target that the integrity of this PC and data are at risk. To verify the claim of the offender, the target is persuaded to open a remote desktop connection to review some of the log files as evidence (Arthur 2010). Fortunately, the offender has a solution that will solve the problem. A small software tool that can be bought to prevent losing any data and payment is possible via credit card or PayPal. When later checking the balance of the bank account, the target realizes that his/her savings are gone. While the target thinks that he is doing the right thing by securing their computer system, he gets victimized instead.

It is hard to determine the success of this type of attack. In an attempt to get an indication of the prevalence, the Dutch Fraud Help Desk (an organization that collects reports on fraud) was contacted. In the period between 2015 and 2018, there were 4507 incidents reported, whereas 499 were victimized (11.1%). The total reported damage was €850,701, an average of over €1700 per victim. These numbers should be considered as a rough estimate, since this method of data collection is prone to biases (e.g., misremembering the account or feel too ashamed to report; refer to section "Surveys (Interviews and Reports)" for more details).

In an experimental setting, a technical support scam was performed on 92 employees (Bullée et al. 2016). Two weeks before the mock attack, one-third of the targets ($N = 28$) received an intervention. Another third of the targets ($N = 29$) received 1 week before the field test an intervention. The intervention consisted of two parts: (i) a flyer explaining what a phone scam was, why it was dangerous, and how to protect yourself; and (ii) a cardholder containing the text "Beware of scams. Verify all requests. Report all incidents." The result was that 40% ($N = 14$) of the employees in the control group followed all instructions of the offender to install the software, compared to 17,2% ($N = 5$) of those in the 1 week group ($\chi^2 = 3.935$, $df = 1$, $p = 0.047$). However, of those in the 2 week group, 42.9% ($N = 12$) complied with the offender ($\chi^2 = 0.052$, $df = 1$, $p = 0.819$); refer to Fig. 1 (Bullée et

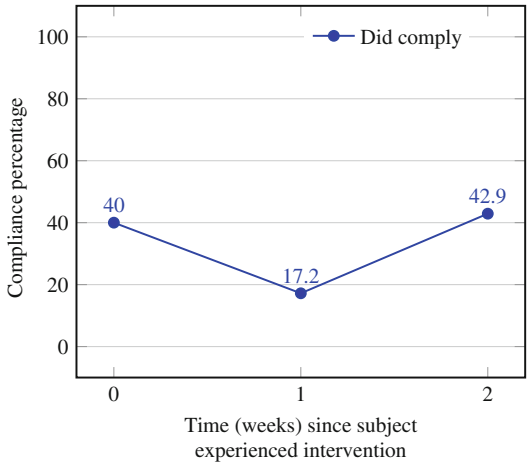

Fig. 1 Change in compliance with the offender over time

al. 2016). This means that there was a significant reduction in victimization for those who received the intervention 1 week before the mock attack; however, this effect was not present for the 2-week group.

Email

Social engineering via email is often referred to as "phishing." In email phishing, the target receives a malicious email that tries to convince him or her to visit a fraudulent website. These websites often have only one goal: tricking people in sharing sensitive information (e.g., passwords or social security numbers) (Ramzan 2010). Phishing is defined as "a *scalable act of deception whereby impersonation is used to obtain information from a target"* (Lastdrager 2014, p. 8). The first part of the definition ("scalable act") relates to the bulk distribution of messages. The second part ("deception whereby impersonation is used") is required to make it fraudulent.

Penetration testers argued that 80% of employees fall for phishing when the email says that there is a free iPad for the person who clicks on the link (from a discussion with the second author). On the other hand, a quick analysis of $K = 16$ studies, containing $N = 25{,}890$ research subjects, show the average success of phishing campaigns is in the range of 2–93% (average of 30.9% and weighted average of 17.2%). Each of the aforementioned studies used a different mock email and there were different types of users involved (e.g., students or employees). Furthermore, there could be a cultural aspect that influences the outcomes since the studies are performed in Europe and Northern America within different institutes. The conclusion is that the success of email phishing is unstable and heavily depends on both the message and the context. Although there are many differences among the studies, this gives a first indication of the general success of email phishing.

Regarding countermeasures of email phishing, the effect of training or playing a game has been investigated in both a laboratory setting (refer to Kumaraguru et al.

2007a, b; Alnajim and Munro 2009; Sheng et al. 2010; Parsons et al. 2015; Kunz et al. 2016; Lastdrager et al. 2017; Pars 2017) and in a field setting (refer to Kumaraguru et al. 2008, 2009; Caputo et al. 2014; Jensen et al. 2017; Jansson and von Solms 2013; Bullée and Junger 2019). One well-known awareness campaign is PhishGuru, a comic explaining what phishing is, how to recognize it, and aims to reduce victimization (Kumaraguru et al. 2007a). PhishGuru was tested both in a laboratory and a field setting. The results showed that it was able to reduce victimization and that this reduction was stable over time (Kumaraguru et al. 2007a, b, 2008, 2009). Another awareness training is NoPhish, which is an interactive web application, where the player is in eight levels educated on how to recognize a phishing email (Kunz et al. 2016). After playing the game, the subjects were better in recognizing phishing emails than before the game ($p = 0.004$). Finally, PHREE is a game-based training that aims to increase the skill of detecting phishing emails (Pars 2017). Before playing the game, 52% of the phishing emails were recognized, compared to 92% in the direct post-test after playing the game ($p < 0.01$) and 87% 1 week after ($p < 0.01$) (Pars 2017).

Face-to-Face

We have seen social engineering via a telephone call; the offender calls the targets and, e.g., tries to convince them to download malicious software. We have also seen social engineering via email (i.e., phishing), where the offender sends its target an email and persuades to visit a malicious website. The offender can also decide to visit the target physically and perform the social engineering face-to-face (F2F). Instead of calling the target on the phone or sending an email, they visit the target in person.

In a university in The Netherlands, a group of students was instructed to learn a script and perform an F2F social engineering attack (Bullée et al. 2015). In this attack, the offender had to go and talk to the target in person. The attack aimed to make the target hand over the office key to the offender (i.e., a stranger). Part of the subjects ($N = 46$) received, using random assignment, an intervention that consisted of three elements: (i) a flyer explaining what social engineering is, why it is dangerous, and how to protect yourself; (ii) a black key chain with the university logo on one side and the text "Don't give me to a stranger" on the other side (refer to Fig. 2a, b); (iii) a poster telling not to share your PIN, keys, or passwords.

The result was that 62.5% ($N = 45$) of the subjects in the control group surrendered their office key, compared to 37.0% ($N = 17$) of those in the intervention group ($\chi^2 = 7.34$, $df = 1$, $p = 0.007$) (Bullée et al. 2015). In many cases, the office key was attached to other keys and the whole bunch was handed over, including bike keys, house keys, car keys, master keys, loyalty cards, and USB storage devices.

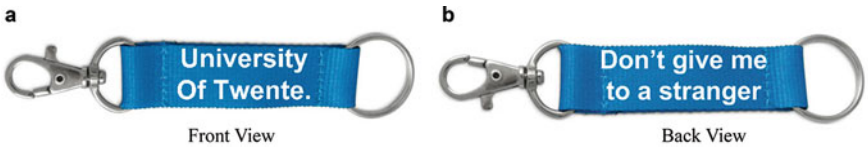

Fig. 2 Key chain. (Adopted from Bullée et al. 2015)

Text Message

Finally, we discuss social engineering via text message, also known as smishing or SMS phishing. Via SMS messages (or messaging mobile applications, e.g., WhatsApp), the offender tries to mimic legitimate communications, often aiming to gather personal information or money. This section describes three social engineering attacks via text message, one reasonably simple attack and two more sophisticated attacks.

First: In one account, the target receives a message via WhatsApp from one of its contacts that encourage to click and receive a £100 worth of vouchers for the supermarket. Clicking the link allows the offender to install malicious software on the phone (McGoogan 2016).

Second: An attack scenario, using WhatsApp, aims to steal money by impersonating a family member. The following MO is used: The offender informs the target of having a new phone number. This includes a matching profile picture of the person who is impersonated. The picture is harvested from social media, as well as family relations and how people interact with each other (Fraudehelpdesk.nl 2018a). Often there is first some chit chat, followed by a call for help. There are bills that need to be paid as soon as possible, and there are problems with the online banking system. To help the family member in need, you pay the bills (Radar 2019). While you think you are helping out, you get victimized instead.

The Dutch Fraud Help Desk received, over the first 6 months of 2018, 160 incident reports regarding fraud attempts via WhatsApp (Majid 2018). This is four times more than over the same period in 2017 (Fraudehelpdesk.nl 2018b), suggesting a big increase in this type of attacks. The reported accounts involved identity fraud where an offender pretended to be a family member (typically a son or daughter) and asked the target (typically a parent) to wire money for an emergency. On average, the damage was €2000 per case (Fraudehelpdesk.nl 2018b).

Although there is, to the best of our knowledge, no success rate known of this scam, the numbers indicate that it is snowballing. Further research is required to obtain a deeper understanding of this attack.

Third: This scenario describes how an offender uses SMS to bypass an additional security layer (i.e., two-factor authentication (2FA)). In 2FA, next to a username and password, a second factor (e.g., SMS verification code) is required to log in. The service provider sends the verification code to the phone number you registered, which provides an additional layer of security. However, the offender can "bypass" this second factor by sending a cleverly constructed SMS to the target; this attack is

also known as verification code forwarding attack (VCFA) (Siadati et al. 2017; Jakobsson 2018). This attack requires three parties: (i) O = offender, (ii) S = service provider and (iii) T = target, and five steps:

1. $O \rightarrow S$: The offender triggers service provider to deliver the verification code;
2. $S \rightarrow T$: Service provider sends verification code to the target;
3. $O \rightarrow T$: The offender tricks the target to forward the verification code;
4. $T \rightarrow O$: The target forwards the verification code to the offender;
5. $O \rightarrow S$: The offender logs in by providing verification code.

In the case of logging in to Gmail, this is how message exchange in steps 2 and 3 could look like (adopted from Siadati et al. 2017):

2. $S \rightarrow T$: *"Your Google verification code is 175197."*
3. $O \rightarrow T$: *"Did you request a password reset for your Gmail account? Delete this message if you did. Otherwise, send Cancel + the verification code we send you."*

The success of this attack is tested to be 50%.

The provider is an unwitting accomplice of this type of social engineering. To prevent this attack, an additional message can be added to the message users generally receive when being sent a verification code. By including an additional warning in the verification message (i.e., *"Please ignore this message if you did not request a code. Your Google verification code is 175197."*), those who forwarded their code was reduced to 8% (Siadati et al. 2017).

What to Do Against Social Engineering?

The previous section discussed four modalities of social engineering, their success, and countermeasures. There are other, more general, countermeasures that could be used. Several methods have been developed to support experts (e.g., law enforcement professionals) to distinguish liars from truth tellers. These methods are based on findings in the literature; however, effect sizes are usually small. The use of (i) increasing cognitive load and (ii) micro-expressions will be discussed.

Increasing the cognitive load relates to making an interview mentally harder. The rationale is that lying requires more cognitive resources than telling the truth. When the cognitive load is further increased, e.g., by making an additional request, the liars have more difficulty to cope with these requests than truth tellers. One of the ways to increase this cognitive load is by asking to tell the story in reverse order (Evans et al. 2013; Vrij et al. 2015). However, this technique also has been criticized for not being very helpful in practice. Furthermore, it was argued that the increased cognitive load could hamper the working memory and make truth tellers also have a difficult time telling their story (Verschuere et al. 2018).

Micro-expressions are reflections of emotions that we want to hide (Ekman 2001; Wu et al. 2017). By using a combination of (i) motion features (i.e., video recording),

(ii) audio features (i.e., voice recording), and (iii) transcript features (i.e., written text), researchers managed to come up with a predictor for deception. In the context of courtroom trial video clips, they demonstrated that the predictor performed 11% better than humans who were asked to make a classification (truth or lie) on the same data (Wu et al. 2017). However, the use of micro-expressions has also been criticized for not being sufficiently effective in practice (Burgoon 2018).

Studies on linguistic characteristics of verbal accounts have been performed. Some studies presented an optimistic account of the possibilities for computer programs to discern features in a text that would help to distinguish lies from truths (Hancock and Gonzales 2013). Applications have been presented for distinguishing lies from truth in political speeches (Hauch et al. 2014) and in the ENRON bankruptcy (Keila and Skillicorn 2005).

A meta-analysis on computer programs for lie detection found that only one factor was important in computer-mediated communication (CMC): liars used more words, whereas in interviews or person-to-person interactions, liars use fewer words (Hauch et al. 2014). All other factors that were studied were nonsignificant (i.e., word quantity; content word diversity; type-token ratio; six-letter words; average word length; verb quantity; sentence quantity; average sentence length) (Hauch et al. 2014). Overall, it seems that lie detection – even for law enforcement professionals – is difficult with uncertain results. However, recent studies found that both arm and mouse movement can be used to detect deception (Sartori et al. 2018). Several experiments already showed that key-stroke dynamics could be used to obtain a similar effect (Sartori et al. 2018). For instance, computer users who lie use more backspaces and execute more edits.

In conclusion, while humans will probably remain poor lie detectors, machines could help us to catch liars.

Who Is More Vulnerable to Social Engineering?

Previous sections provided some insight into the success of different social engineering attacks. Additional factors are often included in order to get a better understanding of who are particularly vulnerable. Performing a social engineering attack in an organization provides a snapshot of the current state of affairs. Including sociodemographic variables in the analysis helps to understand the organization better; employees are not a homogeneous group of entities and are diverse regarding, e.g., sex and age (Pfeffer 1985). Another reason to perform subgroup analyses relates to countermeasures. Knowing who is most vulnerable to an attack can help to focus an awareness campaign and distribute it resource efficient. A campaign that is tailored for, e.g., the elderly looks different than a campaign that is for both elderly and teenagers. Similarly, when, e.g., males are most vulnerable to an attack, the males should receive an awareness training, and those who already perform the desired behavior can be left alone. Characteristics that often reoccur are the sociodemographic variables of sex and age; those will be discussed in more detail. We will

focus on social engineering via email, due to the number of empirical studies available.

Sex

In the context of social engineering via email, we believe that there is no reason to assume that females and males perform differently. Since email is an integrated part of our life, it is to be expected that both females and males have a similar experience with phishing and therefore are equally equipped to identify phishing attempts (Moody et al. 2017).

We will zoom in on 12 studies that investigated the relationship between sex and the success of email phishing in a field experiment. All subjects were persuaded to either click a link or provide data. There were seven studies that investigated a student population (Jagatic et al. 2007; Halevi et al. 2013; Wright et al. 2014; Benenson et al. 2017; Goel et al. 2017; Moody et al. 2017; Carella et al. 2018) four investigated employees (Holm et al. 2013; Flores et al. 2015; Bullée et al. 2017a; van der Meer 2017), and one used civilians as population (Oliveira et al. 2017). The reason that there are more student populations investigated is that they have an increased risk of victimization (Sheng et al. 2010). Out of the 12 studies, there were 4 found that females were more at risk than males, whereas eight found no main effect of sex. However, there could be a moderator effect; four out of seven studies that investigated students found females to be most at risk (Carella et al. 2018; Halevi et al. 2013; Jagatic et al. 2007; Wright et al. 2014). Those who investigated staff or civilians did not find such an effect. In sum, there seems to be no main effect for sex on victimization; however, a moderating variable could explain these findings.

Age

Everybody can be targeted by a social engineering attack, both young and old. Previous research linked age to risky behavior. Findings on offline risks suggest that adolescents take more risks than adults (Hirschi and Gottfredson 1983; Massie et al. 1995; Steinberg 2007). Since the adolescent's brain is still in development, they tend to engage (on average) in riskier behavior (Reyna and Farley 2006; Sheng et al. 2010). Sensation seeking, thrill seeking, impulsivity, and other risky behavior are part of the ongoing learning about the world. Furthermore, younger people tend to learn less from experience than older people do, whereas older people resist risky behavior on intuition (Reyna and Farley 2006). However, for online behavior, this relationship with age is less clear (Baumgartner et al. 2010). In the context of cybercrime, it was argued that younger people are more at risk since they have fewer years of education, fewer years on the internet, less exposure to training materials, and fewer risk aversions (Sheng et al. 2010).

We present the findings of four experimental studies that control for possible differences by age in exposure (Holm et al. 2013; Bullée et al. 2017a; Moody et al. 2017; Oliveira et al. 2017). The result was that one study found that older people, rather than younger people, were the group most at risk (Holm et al. 2013). The other three studies did not find a main effect of age. Two studies reported that there was an

Table 1 Summary table of presented literature on phishing studies and sociodemographic predictors

Most at risk							
N	Goal	Population	Modality	Sex	Age	Success[a]	Ref
50	Click link	Student	Email	Female	–	54	Carella et al. (2018)
100	Enter data	Student	Email	Female	–	17	Halevi et al. (2013)
94	Enter data	Student	Email	Female	–	16	Jagatic et al. (2007)
41	Enter data	Student	Email	Female	–	2	Wright et al. (2014)
2099	Click link	Staff	Email	No effect	–	9	Flores et al. (2015)
53	Click link	Staff	Email	No effect	Older	8	Holm et al. (2013)
483	Click link	Staff	Email	No effect	–	36	van der Meer (2017)
975	Click link	Student	Email	No effect	–	20	Benenson et al. (2017)
7225	Click link	Student	Email	No effect	–	13	Goel et al. (2017)
595	Click link	Student	Email	No effect	No effect	41	Moody et al. (2017)
295	Enter data	Staff	Email	No effect	No effect[b]	19	Bullée et al. (2017a)
158	Click link	Mix[c]	Email	No effect[b]	No effect[b]	43	Oliveira et al. (2017)

[a]Success shows the success of social engineering in the control group
[b]No main effect, however, was an interaction effect that was found
[c]Mix refers to a mix of both students and staff

interaction effect with a third variable: (i) younger employees with few years of service in the organization are most at risk (Bullée et al. 2017a) and (ii) older females were the groups most at risk (Oliveira et al. 2017).

In conclusion, research on the effects of age and sex in social engineering research showed mixed outcomes. Therefore, a general conclusion is difficult since many studies found no relationships. However, when a relationship is found, it is usually reported that females and younger age groups seem to be at higher risk for falling victim to social engineering experiments. For a summary of the studies, refer to Table 1.

Concerning the success of social engineering, it is impossible to give precise numbers: as was shown in Table 1, the percentage of success depends very much on the wording and the form of the deceptive message as well as the context.

Section "Why Is Social Engineering Successful?" explains why victimizing humans using social engineering is relatively easy.

Why Is Social Engineering Successful?

Research on information security, trust, and disclosure has also studied how easy it is to get online users to disclose personal information. We also draw on the disclosure literature to explain the ease with which people tend to fall for social engineering. Both the perspective of target characteristics and offender tactics are discussed.

Target Characteristics

Humans Have Great Difficulties in Recognizing Lies

In general, it is difficult for people to recognize a lie. Many scholars argue that humans are predisposed to trust others. Rousseau et al. (1998) defined trust as "*a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or the behavior of another"* (Rousseau et al. 1998). Trust determines how an individual approaches other people (Kosfeld et al. 2005). Humans tend to conform and are relatively trustworthy by nature: trust has an evolutionary survival value, e.g., children need to trust others in order to be able to learn (Morgan and Laland 2012). In line with this approach, most researchers in deception research believe that adults start with the presumption of truth (Burgoon and Levine 2010). In general, having trust in others has positive outcomes for individuals (Dohmen et al. 2011).

Since humans start with the assumption of truth, it probably will always be difficult for them to detect fraud (Burgoon and Levine 2010). Bond and DePaulo (2006) conducted a meta-analysis on 206 studies regarding the people's accuracy in distinguishing a lie from the truth. They found that people achieve an average of 54% correct lie-truth judgments, correctly classifying 47% of lies as deceptive and 61% of truths as nondeceptive. Although there are none or only weak relations found between behavior and lying, liars tend to make a more negative impression and are tenser (DePaulo et al. 2003).

Research on Online Disclosure

Disclosure or self-disclosure is the process of communicating information about oneself verbally to another person (Cozby 1973). Besides having relatively high trust, humans seem to have low thresholds for disclosing personal information and do this relatively often. Most of the studies on disclosure are in the context of psychology and mental health. These studies showed that self-disclosure has positive mental health outcomes (Dindia 2002; Cozby 1973).

However, in addition to having positive outcomes, personal information can also be abused (Acquisti et al. 2015). The outcome of a literature review shows that users are "sensitive" to the default setting; users tend to keep the preprogrammed settings (Acquisti et al. 2015). Moreover, it was also found that the perception of having control over your personal information reduces privacy concerns and increases disclosure (Acquisti et al. 2015). Studies show that being active online, for instance on social media, can lead to victimization of cyberbullying and cyberstalking

(Mishna et al. 2009; Wachs et al. 2015). Furthermore, the loss of personally identifiable information (PII) can have severe consequences for both individuals and organizations. Individual consequences can include identity theft, embarrassment, or blackmail. Consequences for an organization may include a loss of public trust, legal liability, or remediation costs (McCallister 2010). Research has been done to investigate the degree to which users are prepared to disclose personal information online and the context in which disclosure increases or decreases (for a review, see Junger et al. 2017).

John et al. (2011) presented four experiments in which they measured disclosure of deviant behavior. In three experiments, users disclosed more personal information on unprofessional looking websites compared to professional looking websites (John et al. 2011, p. 868). In a fourth experiment, where users had to think about privacy, the effect of context (i.e., type of website) was absent, and all disclosure rates were comparable among groups.

John et al. (2011, p. 868) concluded that their results "stand in contrast to the considerable body of privacy research that is premised on the assumption of rational choice." Rational choice states that people make trade-offs between privacy and other concerns, implying that disclosure is the result of this rational weighing of costs and benefits, in which objective costs – such as an unprofessional looking website – should prevent or at least decrease disclosure.

A specific aspect of context is the person to whom one discloses information. Olson et al. (2005) stated that it is not so much the nature of the information disclosed that matters, but the person to whom information is disclosed. When that other person is trusted, users easily disclose (Joinson et al. 2010). No other studies studied this aspect of information disclosure.

Acquisti et al. (2015) conclude that disclosure levels are highly malleable. For instance, users are sensitive to default settings: they tend to stick to the pre-programmed default settings. These are easily manipulated by website design; some websites frustrate or confuse users into disclosing personal information. Also, the perception of having control over one's personal information reduces concerns over privacy and increases disclosure (Acquisti et al. 2015).

Lack of Knowledge

Users have insufficient knowledge and lack of strategies to identify vulnerabilities and scams (Purkait 2012). They do not know the methods attackers use to execute their crimes (Jansen and Leukfeldt 2015). In an experimental study of warnings before downloading a pdf file, many subjects explained that they trusted the antivirus program or thought that pdf files were always safe (Krol et al. 2012).

An experiment by Grazioli and Wang (2001) studied the determinants of success or failure in determining if a website was fraudulent or not. They concluded that subjects were all equally good at inspecting the website or at perceiving cues of deception. However, failure was caused because the generation of hypotheses, based on perceived cues, cannot be assessed. The authors concluded that "priming subjects to facilitate hypothesis generation is useless unless we provide them with adequate knowledge to assess the primed hypothesis" (Grazioli and Wang 2001, p. 201). The

authors think this is good news, overall, because, when provided with more knowledge, users should be able to act more wisely. Acquisti et al.'s (2015) conclusion is that many users were unaware of the fact that the information requested from them by researchers could be abusive: "People are often unaware of the information they are sharing, unaware of how it can be used, and even in the rare situations, when they have full knowledge of the consequences, of sharing, uncertain about their preferences." Due to their lack of knowledge, users follow their "default" option, which is trust, obedience, and disclosure of information.

The previous section discussed the lack of knowledge as a major cause of victimization. A refinement of lack of knowledge is lack of knowledge of consequences. Users may lack insight into the severity of the consequences if they fill in their personal information on a spoofed website (Purkait 2012; West 2008). It seems plausible that victims are not aware of the potential consequences of a fraudulent scheme. However, not all researchers found that lack of knowledge is a major cause of victimization.

A study interviewing scam victims reported that the victims often have significant knowledge about the subject of the scam content (Lea et al. 2009, p. 137). For example, background knowledge of shares and stocks may increase the likelihood of falling for an investment scam. Alternatively, people who have experience with winning a price in legitimate lotteries might be more likely to fall for a lottery scam, compared to those who do not have such an experience (Lea et al. 2009, p. 137). The underlying cognitive process is the overconfidence bias (refer to section "Cognitive Biases"). Another finding in the literature against the idea that victims are not aware of consequences comes from experimental research. Training that installs fear for consequences is not ineffective in preventing phishing (Zielinska et al. 2014).

Goal Hierarchy: Users Are Not Motivated?

Security is often not the main concern for users. They may prefer convenience, or they are tricked for financial motives or other basic human motives (West 2008). Förster et al. (2007) state – in line with Goals System Theory – that goals are organized in a hierarchical network. Many authors have argued that – during their work – security warnings, for instance, interrupt users and are therefore considered a nuisance, keeping them away from their primary goal, which is to get their job done (Krol et al. 2012). Similar findings were reported by Krol et al. (2012), who found that pop-up warnings are usually disrupting users from their primary task. Due to their disruptive nature, users tend to skip them to continue with their primary task. This may explain why priming or warnings showed these varying effects on security behavior.

Junger et al. (2017) investigated the disclosure of banking details to an interviewer in a shopping district. Their finding was that participants who were confronted with a warning "not to share banking details with anyone," disclosed equally compared to those who did not receive such warning (Junger et al. 2017). Among other things, "goal hierarchy" could explain their findings. The mind of the subjects was on their primary task (i.e., shopping) and completed the second task (i.e., survey) without paying too much attention to privacy considerations.

Cognitive Biases

Humans use heuristics, or rules of thumb, to make decisions in relatively complex situations (Benson 2016). Benson (2016) identified four types of situations in which humans tend to use heuristics: (i) Information overload, (ii) lack of meaning, (iii) the need to act fast, and (iv) how to know what needs to be remembered for later.

(i) *Information overload.* Too much information does not help in making decisions. Therefore, shortcuts help to select the bits of information that are most likely going to be useful in some way.
(ii) *Lack of meaning.* The world around us is confusing, and therefore we need to bring some sense and direction to it.
(iii) *Need to act fast.* Humans are constrained by time and information, but we cannot let that paralyze us. Accordingly, we need shortcuts to make decisions rapidly.
(iv) *What should we remember?* Not everything is equally important. The humans need to make constant bets and trade-offs around what we try to remember and what we forget.

For more information on cognitive biases, refer to Hilbert (2012). Acquisti et al. (2017) suggested seven types of biases relevant for online disclosure: anchoring, framing effects, self-control, loss aversion, optimism bias, postcompletion errors, and status quo bias. Below we present a brief overview of the biases most relevant to the vulnerability to social engineering.

- *Anchoring* is the tendency to rely heavily on one piece (usually the first) of information (Acquisti et al. 2017). People tend to disclose more information in surveys that start with intrusive privacy questions, compared to questionnaires that gradually augment the privacy sensitivity of the questions (Acquisti et al. 2017).
- *Framing effects* People's decisions are influenced by how information is presented (Acquisti et al. 2017). It was found that respondents' cybersecurity recommendations to their best friend were significantly influenced by personal experience.
- *Self-control* In behavioral economics, people are said to discount the value of the later reward (Acquisti et al. 2017). Several studies found a link with cybercrime victimization (Bossler and Holt 2010).
- *Optimism bias* People believe that negative events are less likely to happen to them than to others and that positive events are more likely to happen to them than to others (Weinstein 1980).
- *Social proof* is our tendency to look to others for cues on what to use and how to behave (Nolan et al. 2008). A Facebook experiment showing people the number of their friends that used security features led to 37% more viewers to explore the promoted security features compared to raising awareness about security issues (Das et al. 2014).

- *Overconfidence* is the tendency to overestimate performance or judgment and occurs in hard tasks or when failure is likely (Moore and Schatz 2017). One specific case of overconfidence is the illusion of control; this is the case where one believes to have control when in fact they do not (Langer 1975).

Offender Strategies

Smart Attackers

Stajano and Wilson (2011) presented the seven principles that attackers use to victimize targets, based on their knowledge of fraud. They derive their principles from an analysis of the BBC TV program *The Real Hustle.* In this program, a variety of scams and "short cons" were recreated to warn members of the public and prevent them from falling for the same scams (Stajano and Wilson 2011).

(i) *The Distraction Principle.* When users are distracted by what grabs our interest, social engineers will profit, and many will not notice.
(ii) *Social Compliance Principle.* People are trained not to question authority. Social engineers exploit this tendency "suspension of suspiciousness" to make us do what they want. CEO-fraud heavily relies on this principle (Stajano and Wilson 2011, p. 72)
(iii) *Herd Principle.* What others are doing can strongly influence behavior (Goldstein et al. 2008). Herd behavior describes how individuals in a group can collaborate and do things that compromise their security (e.g., see Junger et al. 2017).
(iv) *Dishonesty Principle.* Users' dishonesty makes them vulnerable. Fraudsters can use anything illegal.
(v) *Kindness Principle.* People are fundamentally nice and willing to help others. Social engineers shamelessly take advantage of it.
(vi) *Need and Greed Principle.* Our needs and desires make us vulnerable. Once social engineers know what we want, they can easily manipulate us.
(vii) *Time Principle.* When under time pressure, people use different decision strategies, and social engineers use this method a lot, e.g., in phishing emails.

Difficulty of Social Engineering Research

To better understand social engineering, different investigative methodologies can be used. This section discusses three methods: (i) case studies, (ii) interviews and surveys, and (iii) experiments. For each method, the advantages and disadvantages are presented.

Case Studies

Case studies are reports on a single instance of a scenario and are often used in popular media (e.g., newspaper or social media) to report on social engineering. There are books on social engineering that contain many case studies, e.g. (i) *The Art of Deception: Controlling the Human Element of Security* (Mitnick and Simon 2002), (ii) *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker* (Mitnick et al. 2011), (iii) *Hacking the Human: Social Engineering Techniques and Security Countermeasures* (Mann 2008), and (iv) *Social Engineering: The Art of Human Hacking* (Hadnagy and Wilson 2010).

Traditional crimes are analyzed from the perspective of both the offender and the victim. In computer-related crimes, finding the offender for research purposes is difficult, especially when the target is unaware of being victimized (Bullée et al. 2017b). The four books mentioned afore are therefore particularly interesting since these are authored by offenders who use social engineering. Case studies can be used in crime scripts to obtain a better understanding of the execution of a crime and particular for the design of specific interventions (Cornish 1994). The use of crime scripts has been demonstrated for various crimes: drug manufacturing (Chiu et al. 2011), illegal waste activity (Thompson and Chainey 2011), resale of stolen vehicles (Tremblay et al. 2001), serial sex offences (Beauregard et al. 2007), and also for social engineering (Bullée et al. 2017b).

Case studies give an insight into the crime and where to apply interventions. Moreover, it is a useful method to generate hypothesis and theories, whereas case studies are less useful for hypothesis testing (Flyvbjerg 2006). Furthermore, a disadvantage is that case studies often lack rigor; in the past, investigators have often been sloppy and included biased views to influence findings and conclusions (Yin 2009, p. 14). Finally, since case studies can be complex and extensive, it is often difficult to properly summarize a case study without losing valuable information (Flyvbjerg 2006).

In the context of social engineering, a disadvantage of this methodology is that it neither provides an insight into the success nor the prevalence of the crime. One reason is that often only success stories are reported. Also, these individual case studies do not constitute a representative sample of victims (Ross et al. 2014). Although case studies can have great value, one should consider the negatives as well. How researchers can examine the prevalence or success of social engineering will be discussed in the next sections.

Surveys (Interviews and Reports)

Surveys are a convenient method for collecting data (Mathiyazhagan and Nandan 2010) and obtaining insights into social engineering and crimes in general. In a relatively short time, a large audience can be reached for a reasonably low cost (Jones et al. 2013). Asking people about past experiences contributes to insights on the prevalence of a crime, and asking people how they would react in a particular

situation can provide insights into the success of a crime. However, asking people directly for their experience will produce a biased outcome, since many surveys do not control for the opportunity (i.e., a question of whether people received an attempt of the fraud) (Ross et al. 2014). It is evident that not being exposed to a criminal attempt will never produce a victim; there are only a few surveys that take this into account (e.g., Titus et al. 1995). Other factors that one should take into account when conducting a survey include: (i) the respondent could be unaware of being victimized, (ii) misremembered the account, (iii) forgot that it happened, or (iv) feels too ashamed to report (Ross et al. 2014). Finally, self-selection bias is a limitation that should be taken into account. In any given community, some individuals are more likely than others to complete a survey or questionnaire (Stanton 1998; Wright 2005).

Asking people how they expect they will behave in a specific scenario can contribute insights on the success rate of a crime. Note that people tend to provide socially desirable responses that can bias the survey outcomes. Often, "good behavior" is over-reported, whereas "bad behavior" is under-reported (Crowne and Marlowe 1960). This phenomenon is also known in political science and refers to the inconsistency in voter opinion polls and election outcomes (Payne 2010).

This discrepancy was investigated in the context of fear of crime, using the following design: First, the researchers asked the respondents how the participant would react if a stranger ringed their door at night. In a later stage, the researchers would visit their respondents at their home, ring their door, and observe their behavior. The outcome was a statistically significant difference between the verbal expected reaction and their behavioral reaction ($p = 0.001$) (Van Dijk and Nijenhuis 1979).

Two social engineering studies also used this approach. The first study involved social F2F social engineering, and the goal was to obtain office keys from the targets. The respondents were asked, based on steps in a scenario, how they would react. Of the 31 respondents, 1 (3.23%) expected to be compliant with the request of the offender. The results of the field experiment showed that 68 (58.62%) of the 116 subjects did comply with the request of the offender (Bullee 2017).

The second study was executed via the telephone; the goal was to make people download and install software from an untrusted source. In a survey, 49 respondents were asked how they thought they would react. The result was that none of them would comply with the request of the offender, whereas the results of the field test showed that 14 (40%) downloaded and installed the software (Bullee 2017).

Experiments

The limitations of the survey methodology relate to the difficulty of people remembering an account of a crime. By using experiments, the behavior of the subjects can be observed in a controlled environment (Siedler and Sonnenberg 2010). Furthermore, the experimenter often can repeat the experiment until sufficient observations are collected to answer the research question. Another advantage of experiments is

the ability to manipulate one or more variables. The researcher can precisely control the manipulation of variables by specifying the exact conditions of the experiment (Christensen 2007). However, conducting an experiment on cybercrime and social engineering requires careful planning and consideration, e.g., how to introduce the study to subjects. People who are aware of the goal of the experiment could be biased in their behavior. It is unlikely that they would perform the same behavior (e.g., have similar levels of suspicion) outside of the experiment; this could influence the ecological validity of the study (Furnell 2007; Parsons et al. 2013).

Not so much as a disadvantage as something to keep in mind is the research design of an experiment. Each design has associated threats to both internal (i.e., history, maturation, testing, instrumentation, statistical regression, selection biases, experimental mortality, and selection-maturation interaction) and external (i.e., the reactive or interaction effect of testing; the interaction effects of selection biases with the experimental variable; reactive effects of experimental arrangements; multiple-treatment interference) validity (Campbell and Stanley 1963). Due to the context and the operationalization of a social engineering experiment, the choices of research designs can be reduced.

Finally, since social engineering experiments typically involve humans (e.g., employees), ethical considerations must be taken into account (Belmont Report 1979). Particularly challenging is the use of deception (refer to section "Email") since it conflicts with ethical principles (Code of Federal Regulations 2005).

Summary

This chapter started with the scenario of a traveler who was tricked into disclosing credit card information. The offender used social engineering via the telephone, one of the modalities to perform an attack. Field experiments showed that using social engineering as an attack vector, depending on the context, makes many victims.

Victimization, from the victim's point of view, is caused by three factors: (i) people have difficulty in detecting a lie, (ii) people "suffer" cognitive biases (e.g., assuming that all communication is honest), and (iii) a lack of knowledge to identify scams and foresee consequences. On the other hand, offenders are aware of these weaknesses and are not afraid to use this in their attacks. The seven attack principles described by Stajano and Wilson (2011) illustrates this point.

We discussed campaigns that successfully reduced victimization by social engineering. The PhishGuru comic and interactive web application NoPhish made people more resistant to email phishing. To counter Verification Code Forwarding Attack (VCFA) via text message, a warning message in the verification message proved a substantial reduction in victimization.

Despite examples of successful interventions, we need more research on how to prevent social engineering, and which are the principles of successful interventions. Several issues have been noted in previous studies. Although interventions to counter social engineering can have significant effects, the study of Bullée et al. (2016) also found a decay effect of similar strength. It means that over time, the

knowledge (or the skill to act on the knowledge) evaporates to the level of the control group. It is our opinion that this phenomenon requires further investigation and is a suggestion for future research.

We have three suggestions for future research. First, as mentioned in the previous paragraph: "How can 'boosters' be utilized to counter the decay effect?" The effect of the intervention was only present in the short term. Therefore, a suitable follow-up study could involve the use of "quick" booster interventions to counter the decay effect. This was already tested in the context of cardiopulmonary resuscitation (CPR) skill retention (Sutton et al. 2011).

Second, in many cases, the field studies were performed only once. All the experiments were snapshots of the organization. The results tell something of the state of affairs at one particular moment. An interesting future work could be to do a longitudinal study where subjects are tested multiple times. It would be particularly interesting to see how being "victimized" in such a test influences the behavior in future tests. The suggestion involves a longitudinal study: "What are the effects of repeated attempts on victimization?" or "What is the effect of being victimized on the behavior in future tests?"

Third, in the context of information security behavior, limited research has been conducted on cultural influences. The majority of studies have been conducted in Western countries, occasionally in Asia, whereas the rest of the world has been overlooked. Cross-cultural research is relevant since culture is likely to have a direct influence (Crossler et al. 2013).

Cross-References

- ▶ Computer Hacking and the Hacker Subculture
- ▶ Data Breaches and GDPR
- ▶ Hactivism: Conceptualization, Techniques, and Historical Review
- ▶ Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime
- ▶ Identity Theft: Nature, Extent, and Global Response
- ▶ Organized Crime and Cybercrime
- ▶ Phishing and Financial Manipulation
- ▶ Spam-Based Scams
- ▶ Technology as a Means of Rehabilitation: A Measurable Impact on Reducing Crime
- ▶ Technology Use, Abuse, and Public Perceptions of Cybercrime
- ▶ The General Theory of Crime
- ▶ The Psychology of Cybercrime

References

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society, 32*(3), 183–196.

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., et al. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys, 50*(3), 44:1–44:41.

Alnajim, A., & Munro, M. (2009). An anti-phishing approach that uses training intervention for phishing websites detection. In *ITNG 2009 – 6th international conference on information technology: New generations* IEEE Computer Society Washington, DC, USA (pp. 405–410).

Arthur, C. (2010). *Virus phone scam being run from call centres in India*. [Newspaper Article]. Retrieved from http://www.theguardian.com/world/2010/jul/18/phone-scam-india-call-centres.

Baumgartner, S. E., Valkenburg, P. M., & Peter, J. (2010). Unwanted online sexual solicitation and risky sexual online behavior across the lifespan. *Journal of Applied Developmental Psychology, 31*(6), 439–447.

Beauregard, E., Proulx, J., Rossmo, K., Leclerc, B., & Allaire, J.-F. (2007). Script analysis of the hunting process of serial sex offenders. *Criminal Justice and Behavior, 34*(8), 1069–1084.

Belmont Report. (1979). *The Belmont report: Ethical principles and guidelines for the protection of human subjects of research.* The Commission. Washington (DC)

Benenson, Z., Gassmann, F., Landwirth, R. (2017). Unpacking spear phishing susceptibility. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10323 LNCS* Springer, Cham (pp. 610–627).

Benson, B. (2016). *Cognitive bias cheat sheet.* Retrieved 23-sep-2018, from https://betterhumans.coach.me/cognitive-bias-cheat-sheet-55a472476b18

Bond, C. F., & DePaulo, B. M. (2006). Accuracy of deception judgments. *Personality and Social Psychology Review, 10*(3), 214–234.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38*(3), 227–236.

Bosworth, S., Kabay, M., & Whyne, E. (2014). *Computer security handbook* (6th ed.). New York: Wiley.

Bullee, J. H. (2017). *Experimental social engineering.* Unpublished doctoral dissertation, University of Twente, Netherlands.

Bullée, J. H., & Junger, M. (2019). *Are interventions against social engineering effective, not effective, or do they have adverse effects? A meta-analysis of 27 studies.* (Manuscript in preparation).

Bullée, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. H. (2015). The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *Journal of Experimental Criminology, 11*(1), 97–115.

Bullée, J. H., Montoya, L., Junger, M., & Hartel, P. H. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. In A. Mathur & A. Roychoudhury (Eds.), *Proceedings of the inaugural Singapore cyber security r&d conference (sg-crc 2016), Singapore, Singapore* (Vol. 14, pp. 107–114). Amsterdam: IOS Press.

Bullée, J. H., Montoya, L., Junger, M., & Hartel, P. H. (2017a). Spear phishing in organisations explained. *Information and Computer Security, 25*(5), 593–613.

Bullée, J. H., Montoya, L., Pieters, W., Junger, M., Hartel, P. H. (2017b). On the anatomy of social engineering attacks – a literature-based dissection of successful attacks. *Journal of Investigative Psychology and Offender Profiling, 15*(1), 1–26.

Burgoon, J. K. (2018). Microexpressions are not the best way to catch a liar. *Frontiers in Psychology, 9*, 1–5.

Burgoon, J. K., & Levine, T. R. (2010). Advances in deception detection. In *New directions in interpersonal communication research* (pp. 201–220). SAGE Publications.

Campbell, D. T., & Stanley, J. C. (1963). *Experimental and quasi-experimental designs for research*. Boston: Houghton Mifflin Company.

Caputo, D., Pfleeger, S., Freeman, J., & Johnson, M. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security and Privacy, 12*(1), 28–38.

Carella, A., Kotsoev, M., Truta, T. (2018). Impact of security awareness training on phishing click-through rates (Vol. 2018-January, pp. 4458–4466).

Castle, S. (2007). *Thief woos bank staff with chocolates – then steals diamonds worth £14m.* Retrieved 06-aug-2018, from https://www.independent.co.uk/news/world/europe/thief-woos-bank-staff-with-chocolates-then-steals-diamonds-worth-16314m-5332414.html

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy and Security, 1*(3), 18–41.

Chiu, Y.-N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *British Journal of Criminology, 51*(2), 355–374.

Christensen, L. (2007). *Experimental methodology.* Boston: Pearson/Allyn & Bacon.

Code of Federal Regulations. (2005). *Title 45: Public welfare, Department of Health and Human Services, part 46: Protection of human subjects.* U.S. Government Printing Office. Washington (DC)

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*, 151–196.

Cozby, P. C. (1973). Self-disclosure: A literature review. *Psychological Bulletin, 79*(2), 73–91.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., et al. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90–101.

Crowne, D. P., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology, 24*(4), 349.

Das, S., Kramer, A. D., Dabbish, L. A., & Hong, J. I. (2014). Increasing security sensitivity with social proof. In *Proceedings of the 2014 ACM SIGSAC conference on computer and communications security – CCS '14.* ACM Press.

DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., & Cooper, H. (2003). Cues to deception. *Psychological Bulletin, 129*(1), 74–118.

Dindia, K. (2002). *Self-disclosure research: Knowledge through meta-analysis*. Mahwah: Lawrence Erlbaum Associates Publishers.

Dohmen, T., Falk, A., Huffman, D., & Sunde, U. (2011). The intergenerational transmission of risk and trust attitudes. *The Review of Economic Studies, 79*(2), 645–677.

Ekman, P. (2001). *Telling lies: Clues to deceit in the marketplace, politics, and marriage*. New York: W.W. Norton.

Evans, J. R., Michael, S. W., Meissner, C. A., & Brandon, S. E. (2013). Validating a new assessment method for deception detection: Introducing a psychologically based credibility assessment tool. *Journal of Applied Research in Memory and Cognition, 2*(1), 33–41.

Flores, W., Holm, H., Nohlberg, M., & Ekstedt, M. (2015). Investigating personal determinants of phishing and the effect of national culture. *Information and Computer Security, 23*(2), 178–199.

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative Inquiry, 12*(2), 219–245.

Förster, J., Liberman, N., & Friedman, R. S. (2007). Seven principles of goal activation: A systematic approach to distinguishing goal priming from priming of non-goal constructs. *Personality and Social Psychology Review, 11*(3), 211–233.

Fraudehelpdesk.nl. (2018a). *Aanzienlijke schade whatsapp-fraude.* Retrieved 04-apr-2019, from https://www.fraudehelpdesk.nl/aanzienlijke-schade-whatsapp-fraude/

Fraudehelpdesk.nl. (2018b). *Forse toename whatsapp-fraude.* Retrieved 04-okt-2018, from https://www.fraudehelpdesk.nl/nieuws/forse-toename-whatsapp-fraude/

Furnell, S. (2007). Phishing: Can we spot the signs? *Computer Fraud and Security, 2007*(3), 10–15.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished? Internet security and human vulnerability. *Journal of the Association of Information Systems, 18*(1), 22–44.

Goldstein, H. J., Martin, S., & Cialdini, R. B. (2008). *Yes! 50 scientifically ways to be persuasive*. New York: Simon & Schuster.

Gots, J. (2011). *Hacker for the hell of it: The adventures of Kevin Mitnick.* Retrieved 24-sep-2018, from https://bigthink.com/think-tank/hacker-for-the-hell-of-it-the-adventures-of-kevin-mitnick

Graves, R. (1992). *The Greek myths.* Penguin Books. London

Grazioli, S., & Wang, A. (2001). Looking without seeing: Understanding unsophisticated consumers' success and failure to detect internet deception. In *ICIS 2001 proceedings* (Vol. 23). https://aisel.aisnet.org/icis2001/23.

Hadnagy, C., & Wilson, P. (2010). *Social engineering: The art of human hacking*. New York: Wiley.

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd international conference on world wide web* (pp. 737–744). New York: ACM.

Hancock, J. T., & Gonzales, A. (2013). Deception in computer-mediated communication. In *Pragmatics of computer-mediated communication.* De Gruyter. Berlin

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat – reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior, 61*, 372–377.

Hauch, V., Blandón-Gitlin, I., Masip, J., & Sporer, S. L. (2014). Are computers effective lie detectors? A meta-analysis of linguistic cues to deception. *Personality and Social Psychology Review, 19*(4), 307–342.

Hilbert, M. (2012). Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making. *Psychological Bulletin, 138*(2), 211–237.

Hirschi, T., & Gottfredson, M. (1983). Age and the explanation of crime. *American Journal of Sociology, 89*(3), 552–584.

Holm, H., Flores, W., Ericsson, G. (2013). Cyber security for a smart grid – what about phishing?

Internet Complaint Center (IC3). (2018a). *2017 internet crime report.* Retrieved 23-sep-2018, from https://pdf.ic3.gov/2017_IC3Report.pdf

Internet Complaint Center (IC3). (2018b). *Internet crime schemes.* Retrieved 23-sep-2018, from https://www.ic3.gov/crimeschemes.aspx#item-1

Internet Movie Database. (2002). *Catch me if you can.* Retrieved 26-sep-2018, from https://www.imdb.com/title/tt0264464/

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94–100.

Jakobsson, M. (2018). Two-factor in authentication – the rise in SMS phishing attacks. *Computer Fraud & Security, 2018*(6), 6–8.

Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. In *2015 workshop on socio-technical aspects in security and trust.* IEEE.

Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology, 32*(6), 584–593.

Jensen, M., Dinger, M., Wright, R., & Thatcher, J. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597–626.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*(5), 858–873.

Joinson, A., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction, 25*(1), 1–24.

Jones, T. L., Baxter, M. A. J., & Khanduja, V. (2013). A quick guide to survey research. *Annals of the Royal College of Surgeons of England, 95*(1), 5–7.

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66*, 75–87.

Keila, P. S., & Skillicorn, D. (2005). Detecting unusual and deceptive communication in email. In *Centers for advanced studies conference* Queen's University Press, Ontario (pp. 17–20).

King, R. (2011). *Emc's rsa security breach may cost bank customers $100 million.* Retrieved 05-aug-2016, from http://www.bloomberg.com/news/articles/2011-06-08/emc-s-rsa-security-breach-may-cost-bank-customers-100-million

Kosfeld, M., Heinrichs, M., Zak, P. J., Fischbacher, U., & Fehr, E. (2005). Oxytocin increases trust in humans. *Nature, 435*(7042), 673–676.

Krol, K., Moroz, M., & Sasse, M. A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. In *2012 7th international conference on risks and security of internet and systems (CRiSIS).* IEEE.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007a). Protecting people from phishing: The design and evaluation of an embedded training email system. In *Conference on human factors in computing systems – proceedings* ACM New York, NY, USA (pp. 905–914).

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L., et al. (2007b). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *ACM International Conference Proceeding Series, 269*, 70–81.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2008). Lessons from a real world evaluation of anti-phishing training. In *Ecrime researchers summit, 2008* IEEE, New York, NY, USA (pp. 1–12).

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., & Blair, M., et al. (2009). School of phish: A real-world evaluation of anti-phishing training. In *SOUPS 2009 – proceedings of the 5th symposium on usable privacy and security.* ACM. New York, NY, USA

Kunz, A., Volkamer, M., Stockhardt, S., Palberg, S., Lottermann, T., & Piegert, E. (2016). Nophish: Evaluation of a web application that teaches people being aware of phishing attacks. In *Gi-jahrestagung.* "Gesellschaft für Informatik e.V.", Bonn, Germany.

Langer, E. J. (1975). The illusion of control. *Journal of Personality and Social Psychology, 32*(2), 311.

Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science, 3*(1), 1–10.

Lastdrager, E. E., Carvajal Gallardo, I., Hartel, P., & Junger, M. (2017). How effective is anti-phishing training for children? In *Thirteenth symposium on usable privacy and security (soups 2017).* Santa Clara: USENIX Association.

Lea, S., Fischer, P., & Evans, K. (2009). *The psychology of scams: Provoking and committing errors of judgement: Prepared for the office of fair trading*. (Tech. Rep.). University of Exeter School University of Exeter, School of Psychology. Exeter

Majid, A. (2018). *Ik voelde me zo dom. Eén knop en alles was weg.* Retrieved 04-oct-2018, from https://www.volkskrant.nl/nieuws-achtergrond/-ik-voelde-me-zo-dom-een-knop-en-alles-was-weg-~bbadb2d6/

Mann, I. (2008). *Hacking the human: Social engineering techniques and security countermeasures*. Aldershot: Gower.

Massie, D. L., Campbell, K. L., & Williams, A. F. (1995). Traffic accident involvement rates by driver age and gender. *Accident Analysis & Prevention, 27*(1), 73–87.

Mathiyazhagan, T., & Nandan, D. (2010). Survey research method. *Media Mimansa, 4*(1), 34–45.

McCallister, E. (2010). *Guide to protecting the confidentiality of personally identifiable information*. Diane Publishing. Collingdale, PA

McGoogan, C. (2016). *Whatsapp users targeted with £100 Sainsbury's scam – how to protect yourself.* Retrieved 22-nov-2016, from http://www.telegraph.co.uk/technology/2016/10/25/whatsapp-users-targeted-with-100-sainsburys-scam%2D%2D-how-to-protec/

Mishna, F., McLuckie, A., & Saini, M. (2009). Real-world dangers in an online reality: A qualitative study examining online relationships and cyber abuse. *Social Work Research, 33*(2), 107–118.

Mitnick, K., & Simon, W. (2002). *The art of deception: Controlling the human element of security.* New York: Wiley.

Mitnick, K., Simon, W., & Wozniak, S. (2011). *Ghost in the wires: My adventures as the world's most wanted hacker.* New York: Little, Brown.

Moody, G., Galletta, D., & Dunn, B. (2017). Which phish get caught an exploratory study of individuals' susceptibility to phishing. *European Journal of Information Systems, 26*(6), 564–584.

Moore, D. A., & Schatz, D. (2017). The three faces of overconfidence. *Social and Personality Psychology Compass, 11*(8), e12331.

Morgan, T. J. H., & Laland, K. N. (2012). The biological bases of conformity. *Frontiers in Neuroscience, 6*, 87.

Nolan, J. M., Schultz, P. W., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2008). Normative social influence is underdetected. *Personality and Social Psychology Bulletin, 34*(7), 913–923.

Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., & Muradoglu, M., et al. (2017). Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 chi conference on human factors in computing systems* (pp. 6412–6424). New York: ACM.

Olson, J. S., Grudin, J., & Horvitz, E. (2005). A study of preferences for sharing and privacy. In *CHI '05 extended abstracts on human factors in computing systems – CHI '05.* ACM Press.

Pars, C. (2017). *Phree of phish – the effect of anti-phishing training on the ability of users to identify phishing emails.* (Unpublished Master Thesis).

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2013). In L. J. Janczewski, H. B. Wolfe, & S. Shenoi (Eds.), *Security and privacy protection in information processing systems: 28th ifip tc 11 international conference, sec 2013, Auckland, New Zealand, July 8–10, 2013. Proceedings* (pp. 366–378). Berlin/Heidelberg: Springer.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers and Security, 52*, 194–206.

Payne, J. G. (2010). The Bradley effect: Mediated reality of race and politics in the 2008 us presidential election. *American Behavioral Scientist, 54*(4), 417–435.

Pfeffer, J. (1985). Organizational demography: Implications for management. *California Management Review, 28*(1), 67–81.

Purkait, S. (2012). Phishing counter measures and their effectiveness – literature review. *Information Management & Computer Security, 20*(5), 382–420.

Radar. (2019). *Fikse toename van oplichting via whatsapp.* Retrieved 04-apr-2019, from https://radar.avrotros.nl/uitzendingen/gemist/item/fikse-toename-van-oplichting-via-whatsapp/

Ramzan, Z. (2010). Phishing attacks and countermeasures. In P. Stavroulakis & M. Stamp (Eds.), *Handbook of information and communication security* (pp. 433–448). Berlin/Heidelberg: Springer.

Reyna, V. F., & Farley, F. (2006). Risk and rationality in adolescent decision making: Implications for theory, practice, and public policy. *Psychological Science in the Public Interest, 7*(1), 1–44.

Richmond, R. (2011). *The rsa hack: How they did it.* Retrieved 06-mrt-2019, from https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science, 9*(4), 427–442.

Rouse, M. (2006). *Definition social engineering.* TechTarget. Retrieved 23-oct-2013, from http://www.searchsecurity.techtarget.com/definition/social-engineering

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review, 23*(3), 393–404.

Sartori, G., Zangrossi, A., Monaro, M. (2018). Deception detection with behavioral methods. In *Detecting concealed information and deception* (pp. 215–241). Elsevier.

Savage, M. (2012). *The rsa breach: One year later.* Retrieved 04-sep-2016, from http://searchsecurity.techtarget.com/magazineContent/The-RSA-breach-One-year-later

Schneier, B. (2000a). *Crypto-gram, October 15, 2000.* Retrieved 10-oct-2018, from https://www.schneier.com/crypto-gram/archives/2000/1015.html

Schneier, B. (2000b). *Secrets & lies: Digital security in a networked world* (1st ed.). New York: Wiley.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the sigchi conference on human factors in computing systems* (pp. 373–382). New York: ACM.

Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M., & Memon, N. (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security, 65*, 14–28.

Siedler, T., & Sonnenberg, B. (2010). *Experiments, surveys and the use of representative samples as reference data*. (Tech. Rep. No. 146). German Council for Social and Economic Data (RatSWD). Berlin

Solon, O. (2017). *Frank Abagnale on the death of the con artist and the rise of cybercrime.* Retrieved 26-sep-2018, from https://www.wired.co.uk/article/frank-abagnale

Stajano, F., & Wilson, P. (2011). Understanding scam victims: Seven principles for systems security. *Communications of the ACM, 54*(3), 70–75.

Stanton, J. M. (1998). An empirical assessment of data collection using the internet. *Personnel Psychology, 51*(3), 709–725.

Steinberg, L. (2007). Risk taking in adolescence: New perspectives from brain and behavioral science. *Current Directions in Psychological Science, 16*(2), 55–59.

Sutton, R. M., Niles, D., Meaney, P. A., Aplenc, R., French, B., Abella, B. S., et al. (2011). Low-dose, high-frequency cpr training improves skill retention of in-hospital pediatric providers. *Pediatrics, 128*(1), e145–e151.

The Federal Bureau of Investigation. (2015). *Business email compromise.* Retrieved 04-aug-2016, from https://www.ic3.gov/media/2015/150827-1.aspx

The SANS Institute. (2012). *Cyber security newsletter (social engineering – hacking your mind).* Retrieved 23-aug-2016, from https://www.uab.edu/it/home/images/Module02-SocialEngineering-Newsletter.pdf

Thompson, L., & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal on Criminal Policy and Research, 17*(3), 179–201.

Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency, 41*(1), 54–72.

Tremblay, P., Talon, B., & Hurley, D. (2001). Body switching and related adaptations in the resale of stolen vehicles. Script elaborations and aggregate crime learning curves. *British Journal of Criminology, 41*(4), 561–579.

van der Meer, J. (2017). *Wie is precies de zwakste schakel?* Unpublished master's thesis, Erasmus Universiteit.

Van Dijk, J., & Nijenhuis, N. (1979). Ja zeggen, nee doen? een onderzoek naar de overeenkomst tussen verbale attitudes en feitelijk gedrag bij angstgevoelens tav criminaliteit. *Tijdschrift voor Criminologie, 21*(6), 257–273.

Verschuere, B., Köbis, N. C., Bereby-Meyer, Y., Rand, D., & Shalvi, S. (2018). Taxing the brain to uncover lying? Meta-analyzing the effect of imposing cognitive load on the reaction-time costs of lying. *Journal of Applied Research in Memory and Cognition, 7*(3), 462–469.

Vrij, A., Fisher, R. P., & Blank, H. (2015). A cognitive approach to lie detection: A meta-analysis. *Legal and Criminological Psychology, 22*(1), 1–21.

Wachs, S., Junger, M., & Sittichai, R. (2015). Traditional, cyber and combined bullying roles: Differences in risky online and offline activities. *Societies, 5*(1), 109–135.

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of Personality and Social Psychology, 39*(5), 806–820.

West, R. (2008). The psychology of security. *Communications of the ACM, 51*(4), 34–40.

Wright, K. B. (2005). Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication, 10*(3), 00–00.

Wright, R., Jensen, M., Thatcher, J., Dinger, M., & Marett, K. (2014). Influence techniques in phishing attacks: An examination of vulnerability and resistance. *Information Systems Research, 25*(2), 385–400.

Wu, Z., Singh, B., Davis, L. S., & Subrahmanian, V. S. (2017). Deception detection in videos. *arxiv:1712.04415v1.* Retrieved from http://arxiv.org/abs/1712.04415v1

Yin, R. (2009). *Case study research: Design and methods*. Thousand Oaks: SAGE.

Zielinska, O. A., Tembe, R., Hong, K. W., Ge, X., Murphy-Hill, E., & Mayhorn, C. B. (2014). One phish, two phish, how to avoid the internet phish: Analysis of training strategies to detect phishing emails. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58*(1), 1466–1470.