A systematic Gap Analysis of Social Engineering Defence Mechanisms Considering Social Psychology

P. Schaab[1], K. Beckers[1] and Sebastian Pape[2]

[1]Technische Universität München (TUM)
[2]Goethe Universität Frankfurt
e-mail: {peter.schaab, beckersk}@in.tum.de; Sebastian.Pape@m-chair.de

Abstract

Social engineering is the acquisition of information about computer systems by methods that deeply include non-technical means. While technical security of most critical systems is high, the systems remain vulnerable to attacks from social engineers. Social engineering is a technique that: (i) does not require any (advanced) technical tools, (ii) can be used by anyone, (iii) is cheap. Traditional penetration testing approaches often focus on vulnerabilities in network or software systems. Few approaches even consider the exploitation of humans via social engineering. While the amount of social engineering attacks and the damage they cause rise every year, the defences against social engineering do not evolve accordingly. Hence, the security awareness of these attacks by employees remains low. We examined the psychological principles of social engineering and which psychological techniques induce resistance to persuasion applicable for social engineering. The techniques examined are an enhancement of persuasion knowledge, attitude bolstering and influencing the decision making. While research exists elaborating on security awareness, the integration of resistance against persuasion has not been done. Therefore, we analysed current defence mechanisms and provide a gap analysis based on research in social psychology. Based on our findings we provide guidelines of how to improve social engineering defence mechanisms such as security awareness programs.

Keywords

social engineering, security management, persuasion, human-centred defence mechanisms

1. Introduction

Although security technology improves, the human user remains the weakest link in system security. Therefore, it is widely accepted that the people of an organization are the main vulnerability of any organization's security, as well as the most challenging aspect of system security (Mitnick and Simon, 2011). This is emphasized by many security consultants, as well as from genuine attackers, which accessed critical information via social engineering (Gragg, 2003). Early on Gulati (2003) reported that cyber attacks cost U.S. companies $266 million every year and that 80% of the attacks are a form of social engineering. A study in 2011 showed that nearly half of the considered large companies and a third of small companies fell victim of 25 or more social engineering attacks in the two years before (Dimensional Research, 2011). The study further shows that costs per incident usually vary

between $25 000 and over $100 000. Furthermore, surveys, like Verizon's 'Data Breach Investigation Report' (2012; 2013), show the impact of social engineering. Even though the awareness about the phenomenon of social engineering has increased, at least in literature, the impact has grown from 7% of breaches in 2012 to 29% of breaches in 2013 according to these studies. In addition, current security awareness programs are apparently ineffective (Pfleeger et al., 2014). These alarming numbers question whether the existing approaches towards awareness and defence of social engineering are fundamentally incomplete.

Frangopoulos et al. (2010) consider the psychological aspects of social engineering and relate them to persuasion techniques in their 2010 publication. In contrast to our work their work is not based on a literature review of behaviour psychology, but based on the expertise of the authors. Moreover, the scope of the authors is broader and consider physical measures, as well as security standards in their work. Our results classify existing research in IT security and persuasion in literature and contribute a structured gap analysis. In addition, Frangopoulos et al. (2012) transfer the knowledge of psychosocial risks, e.g. influence of headaches and colds on decisions, from a managerial and organisational point of view to the information security view.

Our hypothesis is that the psychological aspects behind social engineering and user psychology are not considered to their full extend. For instance, Ferreira et al. (2015) constitute psychological principles in social engineering and relate these principles to previous research of Cialdini (2009), Gragg (2003) and Stajano and Wilson (2011). However, these principles have to be the fundamental concern of any security defence mechanism against social engineering. Thus, we contribute a list of concepts that address social engineering defence mechanisms. We analyse in particular what IT security recommends in comparison to recommendations given by social psychology. The results of our analysis reveal fundamental gaps in today's security awareness approach. We provide a road map that shows how to address these gaps in the future. Our road map is an instrumental vision towards reducing the social engineering threat by addressing all relevant psychological aspects in its defence.

2. Methodology

Our research was guided by the methodology outlined in Fig. 1. We initialized the work with a working definition of social engineering (Sect. 3) and surveyed the state of the art from the viewpoint of computer science in particular with regard to IT security (Step 2) and separately from the viewpoint of social psychology (Sect. 4). We used the meta search engines Google Scholar and Scopus, which include the main libraries of IEEE, ACM, Springer, Elsevier and numerous further publishers. Based on the findings of our literature survey, we identified requirements and techniques from social sciences for defending against social engineering and map these to the defence mechanisms used in IT security today (Sect. 5). We outline the resulting gap and present a vision for overcoming these shortcomings of current IT security defences (Sect. 6). Finally, we conclude and provide directions for future research (Sect. 7).

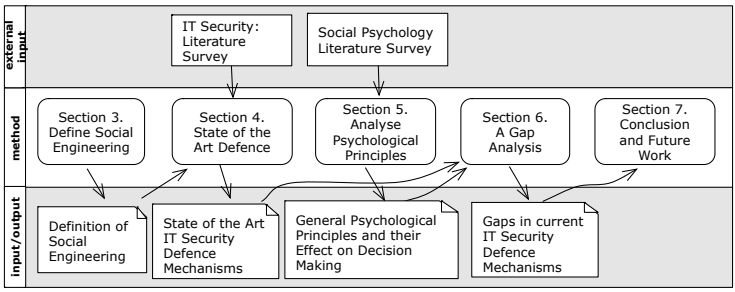

Figure 1: Methodology

3. Definition of Social Engineering

Although there is no agreed upon definition of social engineering, the common idea arising from the available definitions is that social engineering is the acquisition of confidential, private or privileged information by methods including both technical and non-technical means (Manske, 2009). This common idea is quite general, as it includes means of gaining information access such as shoulder surfing, dumpster diving, etc. However, it especially refers to social interaction as psychological process of manipulating or persuading people into disclosing such information (Thornburgh, 2004). Other than the former methods of accessing information, the latter are more complex and more difficult to resist, as persuasion is based on psychology. In this context, persuasion can be viewed as "any instance in which an active attempt is made to change a person's mind" (Petty and Cacioppo, 1996, p.4). The concept of 'optimism bias' states that people believe that others fall victim to misfortune, not themselves (Weinstein, 1980). Additionally, they tend to overestimate their possibilities to influence an event's outcome. Hence people think that they (i) will not be targeted by social engineering and (ii) are more likely to resist than their peers.

To actually raise resistance, we analyse how information security awareness can be increased. In alignment with Kruger and Kearny (2006) we define information security awareness as the degree to which employees understand the need for security measures and adjust their behaviour to prevent security incidents. Furthermore, in accordance with Veseli (2011) we focus on the information security dimensions attitude (how does a person feel about the topic) and behaviour (what does a person do) as they are an expression of conscious and unconscious knowledge (what does a person know).

4. An Analysis of Social Engineering Defence Mechanisms in IT Security

After having established the concept of social engineering, we analyse how the threat of social engineering is met in IT security. As the main vulnerability exploited by social engineering is inherent in human nature, it is the human element in systems that needs to be addressed. Thus, we concentrate on human based defence mechanisms. Predominantly three human based mitigation methods are proposed:

Policies, audits and security awareness programs, as indicated in Table 1. User awareness and security

Dimension		**Defence Mechanism**	**Description**
Knowledge	**Attitude**	Policy Compliance	- Foundation of information security - System standards and security levels - Guidelines for user behaviour
		Security Awareness Program	- Familiarity with security policy - Knowledge about sensitive, valuable information - Basic indicators, suspicious behaviour connected to social engineering attacks - (Recognition of being manipulated)
	Behaviour	Audit	- Test employee susceptibility to social engineering - Identify weaknesses of policy and security awareness program

Table 1: Defence mechanisms used in IT security

policies dominate the recommendations to defend social engineering (Scheeres, 2008).

Security Policies. Any information security is founded on its policy (Mitnick and Simon, 2011). Furthermore, policies provide instructions and guidelines how users should behave. It is especially hard to address social engineering in security policies, since people need to know how to respond to ambiguous requests (Gragg, 2003). By safe-guarding information, users should not come into uncertainty to decide whether certain information is sensitive or not. Necessarily these policies need to be enforced consistently throughout the system.

Security Awareness Programs. Upon establishment of a security policy all users need to be trained in security awareness programs to follow the policy, practices and procedures (Mitnick and Simon, 2011; Thornburgh, 2004). In general, the literature agrees upon the cornerstones of an awareness program. First of all, familiarity with the security policy needs to be established. It is important that everyone in the organization knows what kind of information is sensitive, hence particularly valuable for an attacker. Secondly, knowledge about social engineering is to be conveyed. This includes basics of social engineering, and how attacks work in detail. This should help employees to understand the reasons for related security policies that simply contains rules and usually not the reasoning behind it. The idea is that the understanding of why these polices were defined, will increase compliant behaviour among employees. In addition, the thought knowledge should reach beyond the rules in the policies and contain in particular indicators of social engineering attacks and what behaviour could be suspicious, such as requesting confidential information or to refuse provision of personal or contact information. Gragg (2003) demands the inclusion of additional training for key personnel to include inoculation, forewarning and reality check, see Section 5.

Audit. The conduction of audits is complementary to the above approaches (Thornburgh, 2004). It serves the purpose to test the susceptibility to social engineering attacks (Mitnick and Simon, 2011). Hence, it tests the effectiveness and identifies weaknesses of the other conducted methods (Winkler and Dealy, 1995). In this particular case, classic audits or penetration tests need an extension to social engineering penetration testing as done by Bakhshi et al. (2008). This extension is not trivial since it tests humans who can get upset and the work council needs to be involved.

5. Relevant Defence Mechanisms in Social Psychology

The intentions of security awareness programs are to inform about social engineering and sensitive information. It is assumed that by knowing about the threat of social engineering, users are less likely to be susceptible for such attacks. There is only a few researchers that have found this not to be sufficient, which appears to be ignored by most others. Gragg (2003) considers psychological principles of persuasion behind social engineering. Ferreira et al. (2015) have established a framework of psychological principles. These exhibit the ability to influence and potentially manipulate a person's attitude, believes and behaviour. Gragg therefore recommends techniques to build resistance against persuasion, borrowed from social psychology, to be included into awareness programs. An overview over these methods is given in

Dimension		**Defence Mechanism**	**Description**
Knowledge	**Attitude**	Persuasion Knowledge	- Information about tactics used in persuasion attempts and their potential influence on attitude and behaviour - Information about appropriate coping tactics
		Forewarning	- Warning of message content and persuasion attempt
		Attitude Bolstering	- Thought process strengthening security attitude
		Reality Check	- Demonstration of vulnerability to perceive risk of persuasion
	Behaviour	Inoculation	- Exposition to persuasive attempts and arguments of a social engineer - Provision of counter arguments to resist persuasion
		Decision Making	- Repeated exposition to "similar" decision making situations

Table 2: Defence mechanisms against persuasion borrowed from social psychology

Inoculation. A user gets exposed to persuasive attempts of a social engineer, he is put into a situation a social engineer would put him in. Thereby he is exposed to

arguments that a social engineer may use. Also he is given counter arguments that he can use to resist the persuasion. This works the same way as preventing a disease being spread by using inoculation and induces resistance to persuasion.

Forewarning. Forewarnings of message content and the persuasion attempt of the message triggers resistance to a social engineering attack. The intention is to not only warn about the persuasive attempt of a social engineer, but in particular to warn about the arguments being manipulative and deceptive. An example of this technique would be the warning about fraudulent IT support calls asking for user login and password.

Reality Check. As people tend to believe that they are invulnerable due to optimism bias, users need to realize that in fact they are vulnerable. Therefore, it has to be demonstrated to them, that they are vulnerable, to make them perceive the risks and training to be effective. However, any such effort has to be careful not to cause an amount of frustration that leads people to conclude their security efforts are useless. The balance between the demonstration of the vulnerability and the ensurance that people can make a difference in social engineering defence is vital for the success of defences.

Even though it appears that most programs are not extensive or limited in impact, it is unclear how much attention is given to these proposals in security practice. Nevertheless, research in the field of psychology over the past five decades has proven that inoculation is the most consistent and reliable method to induce resistance to persuasion (Miller et al., 2013). We are not aware of any study directly analysing the effects of inoculation to the resistance to social engineering. We are convinced that the principles behind inoculation are sound and we will analyse their effect on people in a future empirical study. In addition, Gragg (2003) has already adopted inoculation as a valuable mechanism for resistance to social engineering. Nevertheless, there exist further techniques in social psychology to train resistance to persuasion:

Persuasion Knowledge. Aim of security awareness programs is for users to experience resistance toward persuasion in case of a social engineering at- tack. This experience is increased if a user is concerned about being deceived (Friestad and Wright, 1994). Persuasion knowledge consists of information about tactics used in persuasive situations, their possible influence on attitudes and behaviour, their effectiveness and appropriateness, the persuasive agent's motives, and coping strategies (Fransen et al., 2015; Friestad & Wright, 1994). Activated persuasion knowledge usually either elicits suspicion about the persuasive agent's motives, or scepticism about arguments, and perceptions of manipulation or deception. Furthermore, it directs to options how to respond and selects coping tactics believed to be appropriate (Friestad and Wright, 1994). This positive relationship between persuasion knowledge and resistance to persuasive attempts is demonstrated by (Briñol et al., 2015): People are aware of persuasive attempts when having knowledge about persuasion and respond appropriately. This means educating users not only about common social engineering attack methods (e.g. phishing) but

particularly about psychological principles used in social engineering is an absolute necessity. As people also enhance their persuasion knowledge from experiences in social interactions, inoculation plays a vital role. Knowledge about coping tactics is, as indicated, essential to evaluate response options and to cope with persuasive attempts.

Attitude Bolstering. Awareness and knowledge of security policy, its implications and guidelines about e.g. confidential information are necessary to make use of attitude bolstering. The self or existing believes and attitudes are strengthened and therefore the vulnerability to persuasive attempts can be reduced (Fransen et al., 2015). In this process people generate thoughts that support their attitudes (Lydon et al., 1988). As demonstrated by Xu and Wyer (2012) it is possible to generate a bolstering mind-set that decreases the effectiveness of persuasive attempts. This is even possible when the cognitive behaviour leading to this bolstering mind-set has been performed in an unrelated, earlier situation.

Decision Making. Information is processed by using two different systems as explained by Kahneman (2003): intuition and reasoning. Decisions are made based on either one. Butavicius et al. (2015) found the preference for a decision making style has a link to the susceptibility to persuasion, i.e. phishing. Decisions based on heuristics or mental shortcuts are intuitive, impulsive judgements that are more likely to be influenced by persuasive attempts. But interestingly it seems that the style of decision making can be modified by training. This would imply that recurring exposure to different social engineering approaches helps in establishing effective strategies to cope with social engineering. Furthermore, it demonstrates that solely education about the threats of social engineering is not sufficient.

6. A Gap Analysis of Missing Defence Mechanisms in IT Security against Social Engineering

As indicated above, the available defence mechanisms can be classified into the dimensions attitude and behaviour, which in turn exert knowledge. Table 3 presents a mapping of defence mechanisms comparing suggestions in IT security against techniques known in social psychology. When comparing the dimension attitude, the limited scope of IT security becomes evident. As established in Section 4, in the dimension attitude IT security considers establishment of policy and security awareness programs. The purpose of security awareness programs is twofold. Firstly, it is concerned with getting users to know and adhere to the established policy. Secondly, security awareness program's scope is usually limited to the provision of basic knowledge about social engineering. In comparison social psychology offers distinctively more. Although some approaches may be at least partly covered. Forewarning can be seen as included in the education of social engineering basics, as malicious intention of social engineers certainly belongs to basic knowledge about social engineering. But persuasion knowledge goes beyond social engineering basics as it includes knowledge about persuasion strategies as well as counter tactics to rely on in any persuasive situation. For reliance on attitude bolstering good knowledge about security policy is necessary. Again IT security does the first step in user

education, but fails in the second step, the enhancement of this knowledge. The use of attitude bolstering, implies not only the knowledge about policy but its implications and a thought process initiated by each user that strengthens his attitude to e.g. keep sensitive information private. The necessity to perform a reality check can directly be deduced from the concept of 'optimism bias', as illustrated in Section 243. It might partially be covered in security awareness programs. A reality check might be done for e.g. spam mails. But as this particular reality check has a technical background and people tend to dismiss their possible failure by it being a technical detail and in the same time greatly underestimating personal susceptibility, it is important to demonstrate to them their failure in a non-technical environment as well.

Dimension		**IT Defence Mechanisms**	**Psychological Defence Mechanisms**
Knowledge	**Attitude**	Policy Compliance	-
		Security Awareness Program	Forewarning
		-	Persuasion Knowledge
		-	Attitude Bolstering
		-	Reality Check
	Behaviour	Audit	-
		-	Inoculation
		-	Decision Making

Table 3: Comparison of defence mechanisms suggested in IT security and social psychology

Table 3 presents another crucial finding. The dimension behaviour is under-represented in IT security. The only suggestion made for this dimension is to verify correct behaviour via audits. But IT security fails to actually enhance secure behaviour. Training correct behaviour as part of security awareness programs is, as indicated in Section 4, recommended by only a few authors and is usually at most done for spam mails. Even though this is the application of inoculation, this is only one possible social engineering attack and a particular technical one as well. Focus should again also be set on the persuasive nature of social engineering attacks. Hence trainings could for example include role plays. Additionally, it has been proven effective to alter the decision making process by conducting decision trainings where users make a "similar" decision in various appearances.

7. Conclusions and Future Work

Previously, we have discussed gaps in IT security. As indicated, both dimensions, attitude and behaviour, are represented inadequately in IT security when compared to recommendations from social psychology. To counter this gap. We envision a two-step improvement of available security awareness programs (as shown in Table 4). In a first step persuasion resistance trainings should be conducted. They should include a broad approach to social engineering including psychological principles and their effects, possible counter strategies, the initiation of attitude bolstering. As optimism bias is a strong enabler of successful social engineering, it would be desirable to

demonstrate users their susceptibility. This step is particularly promising, as it is feasible with little monetary effort. The second step is persuasive situation role plays. It is conceivable to include experiential exercises in this step as well as repeated decision trainings that force users to re-evaluate their knowledge and attitude by making a "similar" decision multiple times. This step is more effortful and it might suffice to only educate key personnel as it includes "live" training sessions guided by possibly costly trainers, actors or generally personnel capable of create persuasive situations.

Dimensions	**Future defence mechanisms**
Attitude	Persuasion resistance training
Behaviour	Persuasive situation role plays

Table 4: Envisioned training steps as part of security awareness programs

8. References

Bakhshi, T., Papadaki, M. and Furnell, S., 2008. A Practical Assessment of Social Engineering Vulnerabilities. In N. L. Clarke & S. Furnell, eds. *2nd International Conference on Human Aspects of Information Security and Assurance, {HAISA} 2008, Plymouth, UK, July 8-9, 2008. Proceedings*. University of Plymouth, pp. 12–23.

Briñol, P., Rucker, D.D. and Petty, R.E., 2015. Naïve theories about persuasion: Implications for information processing and consumer attitude change. *International Journal of Advertising*, 34(1), pp.85–106.

Butavicius, M. et al., 2015. Breaching the Human Firewall : Social engineering in Phishing and Spear-Phishing Emails. *Australasian Conference on Information Systems*, pp.1–11.

Cialdini, R.B., 2009. *Influence: the psychology of persuasion* EPub editi., New York: Collins.

Dimensional Research, 2011. *The Risk of Social Engineering on Information Security: A Survey of IT Professionals*, 2011

Ferreira, A., Coventry, L. and Lenzini, G., 2015. Principles of Persuasion in Social Engineering and Their Use in Phishing. In T. Tryfonas & I. Askoxylakis, eds. *Human Aspects of Information Security, Privacy, and Trust SE - 4*. Lecture Notes in Computer Science. Springer International Publishing, pp. 36–47. Available at:

Frangopoulos E.D.; Eloff, M.M.; Venter L.M., 2010. Psychological considerations in Social Engineering - The "ψ-wall" as defense, Proceedings of the IADIS International Conference Information Systems, pp. 1-20.

Frangopoulos, E.D., Eloff, M.M. and Venter, L.M., 2012. Psychosocial Risks: can their effects on the Security of Information Systems really be ignored? In N. L. Clarke & S. Furnell, eds. *6th International Symposium on Human Aspects of Information Security and Assurance, {HAISA} 2012, Crete, Greece, June 6-8, 2012. Proceedings*. University of Plymouth, pp. 52–63.

Fransen, M.L. et al., 2015. Strategies and motives for resistance to persuasion : an integrative framework. *Frontiers in psychology*, 6(August), pp.1–12.

Friestad, M. and Wright, P., 1994. The Persuasion Knowledge Model: How People Cope with Persuasion Attempts. *Journal of Consumer Research*, 21(1), pp.1–31.

Gragg, D., 2003. A multi-level defense against social engineering. *SANS Reading Room*.

Gulati, R., 2003. The Threat of Social Engineering and your defense against it. *SANS Reading Room*.

Kahneman, D., 2003. A perspective on judgment and choice: mapping bounded rationality. *The American psychologist*, 58(9), pp.697–720.

Kruger, H. A. and Kearney, W. D., 2006. A prototype for assessing information security awareness. Comput. Secur. 25, 4 , pp. 289-296.

Lydon, J., Zanna, M.P. and Ross, M., 1988. Bolstering Attitudes by Autobiographical Recall: Attitude Persistence and Selective Memory. *Personality and Social Psychology Bulletin*, 14(1), pp.78–86. Available at: http://psp.sagepub.com/content/14/1/78.abstract.

Manske, K., 2009. An Introduction to Social Engineering. *Information Security Journal: A Global Perspective*, 9(5), pp.1–7.

Miller, C.H. et al., 2013. Boosting the Potency of Resistance: Combining the Motivational Forces of Inoculation and Psychological Reactance. *Human Communication Research*, 39(1), pp.127–155.

Mitnick, K.D. and Simon, W.L., 2011. *The art of deception: Controlling the human element of security*, John Wiley & Sons.

Petty, R.E. and Cacioppo, J.T., 1996. *Attitudes and persuasion: Classic and contemporary approaches*, Boulder, CO, US: Westview Press.

Pfleeger, S.L., Sasse, M.A. and Furnham, A., 2014. From Weakest Link to Security Hero: Transforming Staff Security Behavior. *Journal of Homeland Security and Emergency Management*, 11(4), pp.489–510.

Sagarin, B.J. et al., 2002. Dispelling the illusion of invulnerability: The motivations and mechanisms of resistance to persuasion. *Journal of Personality and Social Psychology*, 83(3), pp.526–541.

Scheeres, J.W., 2008. *Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks*,

Stajano, F. and Wilson, P., 2011. Understanding Scam Victims: Seven Principles for Systems Security. *Commun. ACM*, 54(3), pp.70–75.

Thornburgh, T., 2004. Social Engineering: The "Dark Art." In *Proceedings of the 1st Annual Conference on Information Security Curriculum Development*. InfoSecCD '04. New York, NY, USA: ACM, pp. 133–135.

Verizon, 2012. Data Breach Investigations Report. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf [Accessed January 13, 2016].

Verizon, 2013. Data Breach Investigations Report. Available at: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf [Accessed January 13, 2016].

Veseli, I., 2011. *Measuring the Effectiveness of Information Security Awareness Program*. Gjøvik University College.

Weinstein, N.D., 1980. Unrealistic Optimism About Future Life events. *Journal of Personality and Social Psychology*, 39(5), pp.806–820.

Winkler, I.S. and Dealy, B., 1995. Information Security Technology?...Don't Rely on It A Case Study in Social Engineering. In *Fifth Usenix Security Symposium*. pp. 1–6.

Xu, A.J. and Wyer, R.S.J., 2012. The Role of Bolstering and Counterarguing Mind-Sets in Persuasion. *Journal of Consumer Research*, 38(5), pp.920–932. Available at: http://www.jstor.org/stable/10.1086/661112.