Principles of Persuasion in Social Engineering and Their Use in Phishing

Ana Ferreira[1,2(✉)], Lynne Coventry[3], and Gabriele Lenzini[1]

[1] Interdisciplinary Centre for Security Reliability and Trust - University of Luxembourg, Luxembourg, Luxembourg
ana.ferreira@uni.lu
[2] Institute of Cognitive Science and Assessment - University of Luxembourg, Luxembourg, Luxembourg
[3] Psychology and Communication Technology, Northumbria University, Newcastle upon Tyne, UK

Abstract. Research on marketing and deception has identified principles of persuasion that influence human decisions. However, this research is scattered: it focuses on specific contexts and produces different taxonomies. In regard to frauds and scams, three taxonomies are often referred in the literature: Cialdini's principles of influence, Gragg's psychological triggers, and Stajano *et al.* principles of scams. It is unclear whether these relate but clearly some of their principles seem overlapping whereas others look complementary. We propose a way to connect those principles and present a merged and reviewed list for them. Then, we analyse various phishing emails and show that our principles are used therein in specific combinations. Our analysis of phishing is based on peer review and further research is needed to make it automatic, but the approach we follow, together with principles we propose, can be applied more consistently and more comprehensively than the original taxonomies.

Keywords: Social engineering · Principles of persuasion · Phishing emails

1 Introduction

Social engineering consists of persuasion techniques to manipulate people into performing actions or divulging confidential information [1]. How persuasion works is well known in other domains such as marketing where, for instance, Cialdini [2] identifies six principles which are used to influence buyers to purchase goods they may not even like or need to buy. However, less known are the principles of deception usually applied by social engineers to steal confidential information. Uebelacker *et al.* [3] assume that Cialdini's principles work in social engineering as well, but argue that some principles work better depending on the victim's personality traits. Akbhar [4] analyses 207 phishing emails according to what Cialdini's

G. Lenzini—This research is supported by FNR Luxembourg, project I2R-APS-PFN-11STAS.

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2015, LNCS 9190, pp. 36–47, 2015.
DOI: 10.1007/978-3-319-20376-8_4

principles are used therein. However, Cialdini is not the only author to suggest principles of persuasion that can be used in social engineering. Gragg, from reading the literature on persuasion and social-engineering, extracts seven *psychological triggers* [5] which, he claims, make social engineering successful; Stajano *et al.*, from investigating the behaviour of street hustlers, draw seven *principles of scams* and show how these can be used to breach security [6]. All these principles and triggers may be related. Indeed, Gragg's triggers seem to work in some of Cialdini's principles [7]. Still, is unclear what basic principles constitute a clear and complete basis for social-engineering and whether what makes social-engineering persuasive should be found only among Cialdini's, Gragg's and Stajano *et al.* work, or somewhere else.

Contribution. This paper proposes a reviewed list of principles of persuasion that works in social engineering. The list is obtained by comparing and merging Cialdini's, Gragg's and Stajano *et al.*'s principles. In addition, this paper investigates what combination of principles is most commonly used in phishing, a research that can help identify effective and directed countermeasures against this widespread and insidious type of socio-technical attacks.

2 Motivation

Most research about protecting users from phishing emails is about methods to check manually or automatically for keywords, grammatical inconsistencies, typos, or information misplacement [8–10]. All these methods can help the user, but they have not yet changed the fact that people are still falling for phishing emails [10]. Why is phishing so effective? One reason is that phishing e-mails use more or less explicitly deception and persuasion strategies. Some of such strategies, adopted in areas such as marketing, were extensively studied by Cialdini, who grouped them into six basic categories which he called *the six basic principles of influence* [2]. These principles — even if we do not recognize them as such — are used ubiquitously in human interactions to influence and to persuade people to do, act, and think the way one wants. Influence is not only used maliciously but it can also be used ethically to nudge people into a positive behaving; however, surprisingly, it is less effective for this positive purpose unless it is strategically twisted to work [11].

Persuading people and influencing their decisions seems to be not only a matter of human interactions but also of contextual variables. Successful influence is increasingly governed, rather than by cognition, by the context and by the psychological environment where information is presented [11]. In understanding this, social engineers are ahead: they know that to influence and persuade more efficiently they have not only to inform people but also make small shifts in their approach to link their message to deep human motivations. If we were able to identify both the principles of influence and those small shifts, we would be able to understand why these principles make social engineering so persuasive and successful. Moreover, if a small set of agreed principles is developed, studying why human interactions are susceptible and how people react when those principles are in place can be done more orderly and systematically.

3 Methods

We study how Cialdini's [2], Gragg's [5], and Stajano *et al.*'s [6] principles relate one another and from it we produce a reviewed list of more uniform and more general principles of persuasion in social engineering. To relate principles we define three relations, indicated as $=$, $\subset$, and $\sim$. A ssuming that Pa and Pb are two distinct principles, we write that:

$Pa = Pb$, if Pa's and Pb's descriptions use the same keywords or expressions with equivalent meaning and for all scenarios that we can describe where Pa is *successful*, also Pb is, and vice versa. For a principle, to be successful in a scenario means that the application of the principle is what makes the deception work in that scenario. If $Pa = Pb$, they can be used interchangeably.

$Pa \subset Pb$, if for all scenarios where Pa is successful then Pb is also successful, but not vice versa. There are scenarios where Pb is successful but where Pa does not work, so Pa is more specific than Pb.

$Pa \sim Pb = (Pa \cap Pb)$ AND $(Pa \not\subseteq Pb)$ AND $(Pa \not\subseteq Pb)$, if Pa and Pb cannot be used interchangeably because there are scenarios where Pa is successful but Pb is not, and vice versa. Then Pa is used to express concepts that partially overlap with principle Pb, but is not a refinement of it.

We use these relations to relate Cialdini's, Gragg's and Stajano *et al.*'s principles, as well as Gragg's and Stajano *et al.*'s principles. Once the relationships are established, we are able to either maintain or combine existing principles and propose a list, which we call *Principles of Persuasion in Social Engineering*. Specifically, we add a new principle for each quotient class defined by the equivalence relation $=$; we have a new principle for each maximal element in the order relation $\subset$. Clusters which are mixed and that include $Pa \sim Pb$ need to be further inspected: we either split Pa from Pb and have two principles or merge Pa and Pb into a new one.

4 Principles of Persuasion in Social Engineering

To easily refer to Cialdini's, Gragg's and Stajano *et al.* principles, we tag each of the principles with the initial letter of the principle author — C for Cialdini, G for Gragg, and S for Stajano *et al.*— and a number, from 1 to 6 or 7, respectively; thus, we have the following IDs: $C1, \ldots, C6$, for Cialdini's principles, $G1, \ldots, G7$ for Gragg's, and $S1, \ldots, S7$ for Stajano, as in the table at the beginning of the next page.

Relating Cialdini's, Gragg and Stajano *et al.'s* Principles. Due to space constraints we can only sketch our findings. We report in Fig. 1 only a few of the obtained relations which shows that (upper part) *Authority* ($C1$ and $G1$) = *Social compliance* ($S1$), which means that the three principles are interchangeable. We can then state that they actually constitute one *Principle of Persuasion in Social Engineering* that we call *Authority* (AUTH).

Figure 1 also shows that (bottom part) *Diffusion responsibility* ($G2$) $\subset$ *Herd* ($S2$) $\subset$ *Social proof* ($C2$), which means that *Social proof* ($C2$) is the most

	C	*G*	*S*
1	Authority	Authority	Social compliance
2	Social proof	Diffusion responsibility	Herd
3	Linking & Similarity	Deceptive relationship	Deception
4	Commitment & Consistency	Integrity & Consistency	Dishonesty
5	Scarcity	Overloading	Time
6	Reciprocation	Reciprocation	Need & Greed
7	-	Strong Affect	Distraction

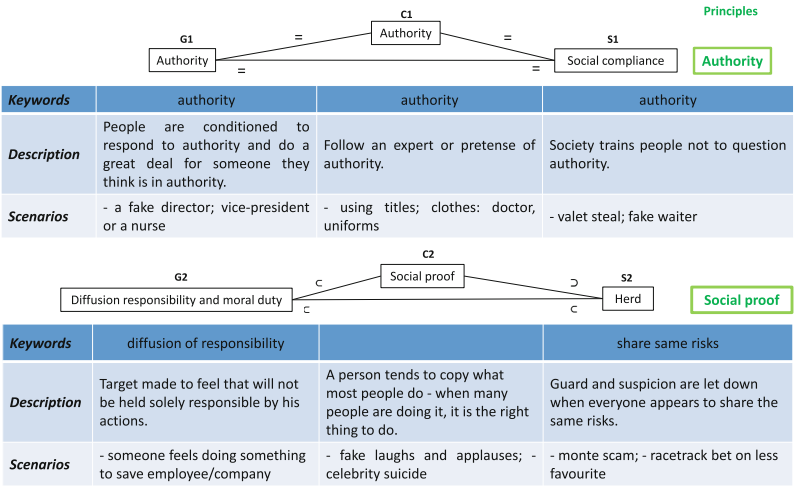

Fig. 1. Example of two relations between the principles.

general including the other two. Since, these three principles also form an independent cluster, we can then state another, more comprehensive, *Principle of Persuasion in Social Engineering*, which we call *Social Poof* (SP). Figure 1 also lists the keywords that characterize the principle (row "Keywords"), quotes the description given by the principle's authors (row "Description") and reports (row "Scenario") the scenarios they gave in describing that principle.

All the relations are represented as a Venn diagram reported in Fig. 2 as well as the proposed five *Principles of Persuasion in Social Engineering*, namely:

***Authority* (AUTH).** Society trains people not to question authority so they are conditioned to respond to it. People usually follow an expert or pretense of authority and do a great deal for someone they think is an authority.

***Social Poof* (SP).** People tend to mimic what the majority of people do or seem to be doing. People let their guard and suspicion down when everyone else appears to share the same behaviours and risks. In this way, they will not be held solely responsible for their actions.

***Liking, Similarity & Deception* (LSD).** People prefer to abide to whom (they think) they know or like, or to whom they are similar to or familiar with, as well as attracted to.

***Commitment, Reciprocation & Consistency* (CRC).** People feel more confident in their decision once they commit (publically) to a specific action and need to follow it through until the end. This is true whether in the workplace, or in a situation when their action is illegal. People have tendency to believe what others say and need, and they want to appear consistent in what they do, for instance, when they owe a favour. There is an automatic response of repaying a favour.

***Distraction* (DIS).** People focus on one thing and ignore other things that may happen without them noticing; they focus attention on what they can gain, what they need, what they can lose or miss out on, or if that thing will soon be unavailable, has been censored, restricted or will be more expensive later. These distractions can heighten people's emotional state and make them forget other logical facts to consider when making decisions.

The representation of the obtained relations in Venn diagrams (see Fig. 2) shows that these are quite clear for some principles (i.e., those numbered C1, C2 and C3) and more complex for others, so the later required clarification.

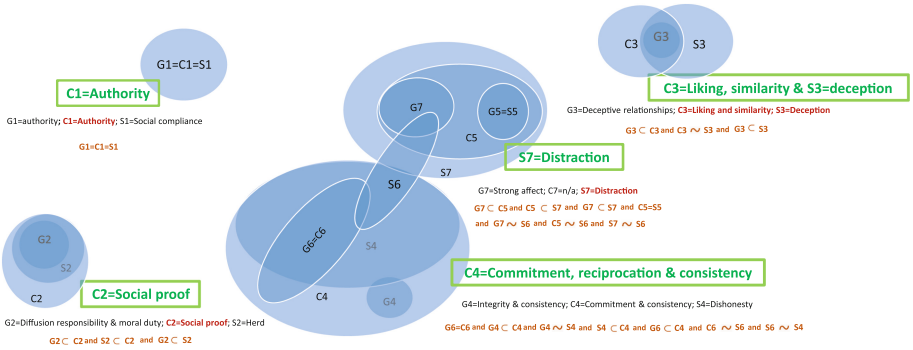

Fig. 2. The Venn diagram showing all relationships among the considered principles.

To assert that *Dishonesty* ($S4$) $\subset$ *Commitment & Consistency* ($C4$), as shown in the diagram, we needed to exclude that *Dishonesty* ($S4$) $\sim$ *Commitment & Consistency* ($C4$). Going back to the description and examples of both principles, it is possible to confirm that *Dishonesty* ($S4$) $\subset$ *Commitment & Consistency* ($C4$) since the *Dishonesty* ($S4$) principle mainly refers to the fact that people are committed by an illegal action and feel *induced/forced* to finish that transaction and be consistent with the first illegal action they took. This is exactly what the principle of commitment and consistency refers to, but for all types of actions, not only those which include illegal content.

To verify if *Reciprocation* ($C6$) $\sim$ *Commitment & Consistency* ($C4$) or *Reciprocation* ($C6$) $\subset$ *Commitment & Consistency* ($C4$) we analyse again the description and scenarios regarding reciprocation by both Gragg *et al.* and Cialdini and conclude that they all fit in Cialdini's *Commitment & Consistency* ($C4$) principle. *Reciprocation* ($C6$) is described as the returning of a favour that someone has made. The receiver feels obliged (committed) to return that favour at some point in time. These examples fit with *Commitment & Consistency* ($C4$) principle as it describes that someone asks something of us, but also the opposite, when we do something that makes us commit and be consistent with the consequences of that previous action. So we believe that, in fact, Cialdini's principle *Commitment & Consistency* ($C4$) integrates the principle *Reciprocation* ($C6$), reducing these to a single principle. However, in this specific case, we leave reciprocation as part of the final principle's name because it is easier to understand its inclusion since it was always identified as a separate principle in other research works.

To clarify if *Scarcity* ($C5$) $\subset$ *Distraction* ($S7$), we acknowledge that the *Scarcity* ($C5$) principle is described by people focusing on what they can potentially lose, or miss out on, like limited availability of time, money, goods, etc. The situations are described in a way that focuses people's attention on the lack of those specific things, ignoring all other facts. This is exactly what the principle of *Distraction* ($S7$) described by Stajano *et al.* is about. Making people focus attention on one specific thing while other things go unnoticed and not included in the reasoning.

One final clarification relates to the *Need & Greed* ($S6$) principle which Stajano *et al.* defines as including most cases under the *Dishonesty* ($S4$) principle, so *Need & Greed* ($S6$) $\sim$ *Dishonesty* ($S4$). But what about the other cases inside *Need & Greed* ($S6$), are they all included in the principle of *Distraction* ($S7$) or not? In fact, according to the *Need & Greed* ($S6$) description, people focus attention on what they can gain and forget the other rational facts. This is part of the *Distraction* ($S7$) principle, so the other cases of *Need & Greed* ($S6$) are all included in *Distraction* ($S7$).

5 Persuasion in Phishing Emails

We validated our Principles of Persuasion in Social Engineering by verifying which of them are used in phishing e-mails.

Data Collection and Phishing Elements. We have collected examples of phishing emails from our own mailboxes and from real examples found on the Internet. The inclusion criteria was phishing emails only (we have ignored *SPAM* emails) and, when possible, completed with images, logos and colors, since these can make a difference in the success rate [10]. This type of analysis had to be done manually by a human — there is no tool to automatically associate phishing email elements together with text, images and colors to principles of persuasion — so it was not possible to have a bigger sample at this point.

We organized the collected emails according to their goal, namely (1) *Data Theft*: banking, financial, helpdesk or account deactivation emails asking for confidential or personal information (these emails include attacks such as Man-In-The-Middle, session hijacking, and impersonation); (2) *Malware*: emails with attachments or emails with fake websites such as pharmaceuticals (these websites or attachments can contain Trojan horses, virus, system reconfiguration and malicious software); and (3) *Fraud*: emails offering large sums of money and prizes (this email includes attacks such as the 419 or the Nigerian scams). We have analysed a sample of 52 different phishing emails: 30 from the *Data Theft* category, 15 from *Malware* and 7 from *Fraud*.

There are patterns that recur in phishing emails (e.g., text, images, and colors). We have identified and transcribed them to the table in Fig. 3.

For each element of the phishing email we counted the *Principle(s) of persuasion in Social Engineering* that are used therein. If the same principle(s) appears in consecutive email elements, we counted it(them) as appearing only once.

We have only used phishing emails written in English. Considering other languages is out of scope in this work, but the analysis and comparison between different languages raises interesting questions if some differences are to be found, related to that language/culture.

		Principles of Social Engineering				
		AUTH	SP	LSD	CRC	DIS
Pattern elements found within the phishing emails	Identification (eg. name, email, address, telephone, and similar)	if it is a company, bank or government related		it gives false detailed information to look real		
	Details of the service (eg. invoice numbers, requested service details, payment details, and similar)			it gives false detailed information to look real		
	Visual cues and restrictions (eg. colors, font, capital letters, big images, exclamation and interrogation marks, time restriction, urgent, must be done, and similar)					focus the attention on these elements
	Logos	if it is a company, bank or government related		false but similar images to look real		focus the attention on the elements of the logo
	Description of something that concerns the user such as: user's actions, requests, inactivity, and similar	if users actions do not agree with poicies and agreements stipulated by the company on the email		it gives false information about what the user did or did not to look real	if it implies that the user must perform an action in return	
	as well as information about the user such as: known contacts in CC, referring to friends, colleagues and family, and similar		gives information about how others feel and think about the author of the email	it gives false detailed information regarding the email author to look familiar and real		
	Elements that ask the user to perform an action such as: click here, update the form, confirm the form, your tickets are in the attachment, confirm personal details, and similar	press or advise the user to perform an action			ask the user to perform an action in return of what was stated before	focus the attention on specific actions, documents and links present in the email
	Actions performed by others such as customers complaints, or others expect your input		other people performed actions that affect the user	it gives false detailed information regarding others to look real		
	Elements in the first person stating "I am this and that"			it gives false detailed information regarding the email author to look familiar and real		
	Elements in the first person describing behaviour around others		gives information about how others feel and think about the author of the email	it gives false detailed information regarding the email author to look familiar and real		
	Asking commitment from the user: "Can I trust you?", "Can you do this for me?", and similar				ask the user to perform an action in return of what was stated before	focus the attention on specific actions or requests
	Referring to other elements outside the ambit of the email to look more reliable such as: "You need to have acrobat Reader to read the atached file", and similar			false but similar information about existing products to look real	using existing real information about other companies is consistent to what the user normally sees in real sites	

Fig. 3. Common elements extracted from phishing emails.

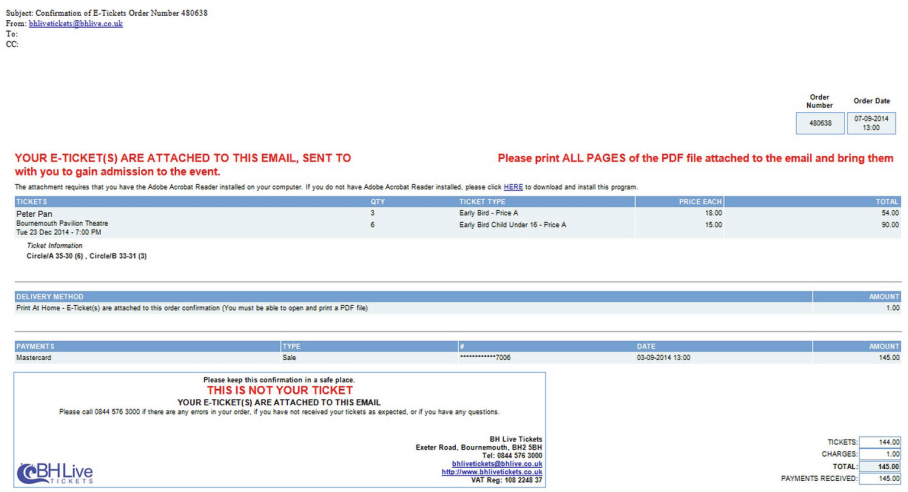

Fig. 4. Peter Pan malware phishing email.

Analysis. We provide an example (e.g., the "Peter Pan phishing email" in Fig. 4) of how we have analysed the phishing emails. As mentioned, we identified the various elements present in the phishing email and counted the *Principle(s) of Persuasion in Social Engineering* therein (see Fig. 5).

The final results are reported in Fig. 6. The graph on the top shows the number of elements that express a specific principle while the graph at the bottom depicts the number of elements that integrate two principles, for the three categories of analysed phishing emails.

	AUTH	SP	LSD	CRC	DIS	Other factors
bhlivetickets@bhlive.co.uk	1		1			color; smaller font
Confirmation of e-tickets order number 480638; Order Date 07-09-2014 13:00			1			smaller font
YOUR E-TICKET(S) ARE ATTACHED TO THIS EMAIL, SENT TO	1		1		1	color; capital letters; bold face
Please print ALL PAGES of the PDF file attached to the email and bring them with you to gain admission to the event	1			1	1	color; capital letters; bold face
The attachment requires that you have Acrobat Reader installed on your computer. If you do not have Adobe Acrobat Reader installed, please click HERE to download and install this program.			1	1		smaller font
A table with clear description of the type of tickets, quantity, seating information, place with date and time of the show and prices per item			1			smaller font
A table with clear description of the delivery method- Print at Home-E-Ticket(s) are attached to this order confirmation (you must be able to open and print a PDF file)	1		1	1		smaller font
A table with clear description of the payment including credit card last numbers			1			smaller font
Please keep this confirmation in a safe place	1			1		smaller font; in a rectangle
THIS IS NOT YOUR TICKET YOUR E-TICKET(S) ARE ATTACHED TO THIS EMAIL	1			1	1	bigger font; in a rectangle
Please call number if there are any errors in your order, if you have not received your tickets as expected, or if you have any questions.			1	1		smaller font
BHLiveTICKETS Logo	1		1		1	color; bigger font
BHLiveTICKETS full contact information including: address, telephone number, email, website and VAT Reg. number	1		1			smaller font; bold face; color

Fig. 5. Analysis of the elements of a phishing email and the principles of persuasion in social engineer those elements express.

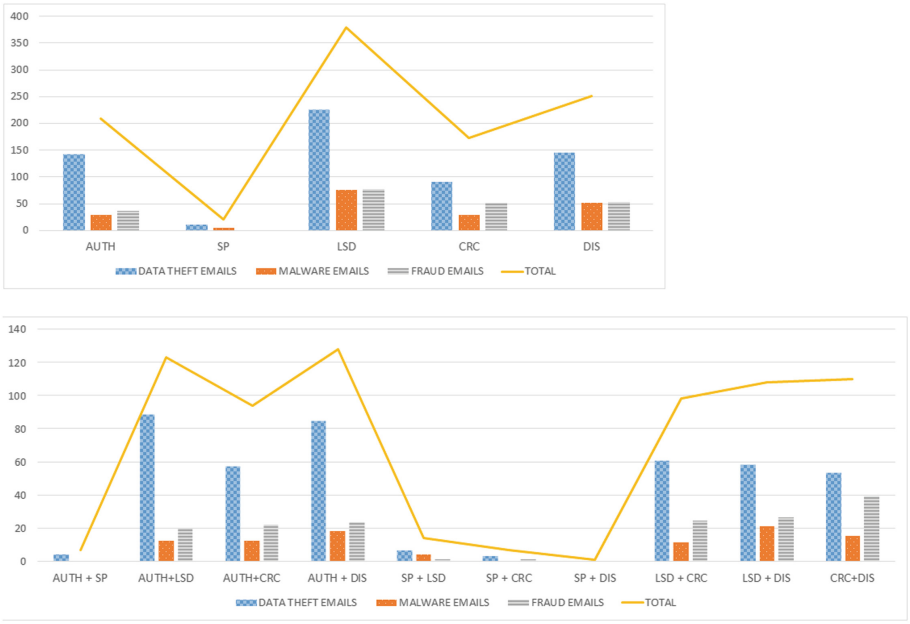

Fig. 6. Number of phishing email elements that express the principles of persuasion in social engineering (authority-AUTH; Social proof-SP; Liking, similarity and deception-LSC; Commitment, reciprocity and consistency-CRC; Distraction-DIS).

Succinctly, the results show that the most common principle of social engineering is the principle of *Liking, Similarity & Deception* (LSD), followed by the principle of *Distraction* (DIS). The next third most common principles are *Authority* (AUTH) for data theft emails and malware, and *Commitment, Reciprocation & Consistency* (CRC) for malware and fraud emails.

When the principles are applied together, the most common pair is AUTH-LSD, followed by AUTH-DIS for data theft emails. For malware emails, the most common pair of principles is LSD-DIS followed by AUTH-DIS, while for the fraud category, the most common pair of principles is CRC-DIS followed by LSD-DIS. Also, some elements of phishing emails include three principles of social engineering and the most common from our analysis are AUTH-CRC-DIS, followed by AUTH-LSD-DIS for both data theft and malware phishing emails. For the fraud category, the three most present principles are AUTH-CRC-DIS, followed by LSD-CRC-DIS.

6 Discussion

Our research shows that previous work had many overlaps in terms of principles and techniques of persuasion and deception in different contexts. We believe in the importance of further study into how these principles relate and are used in social engineering. We believe it will prove useful to have a common list

and description of such principles and their identification in social engineering attacks, such as phishing emails. We proposed such a list in this paper which can be reused by other researchers as a common approach for future work. We tested this list by identifying its five principles of persuasion in social engineering in various phishing emails. It was clear that those principles are commonly present in the majority of the elements that constitute phishing emails. However, more analyses need to be performed to verify whether the identified principles are not exclusive (there may be others not yet identified), and also if they are not only present in phishing emails but also in other types of social engineering attacks.

Not surprisingly, the principle of social engineering that is mostly used in all types of phishing emails is the principle of *Liking, Similarity & Deception* (LSD). From all five principles, this is the one that relates more to the way humans interact socially when they try to connect with others by finding characteristics that are more agreeable and similar to them. Humans tend to believe in what other humans do or say, unless they suspect something is really wrong or that some behaviour is completely unexpected.

The second most common used principle is *Distraction* (DIS) we think because it complements the principle of *Liking, Similarity & Deception* (LSD). The human brain is adept at working with images and visual cues have some advantage to any type of verbal expression. However, distraction factors can also be very effective in verbal expression (e.g., open attached file) and so, adding elements that are at the same time familiar, known, and close to what users think is real, together with some extra elements that complement and confirm those characteristics will, it seems, be very effective in the practice of phishing emails. These results confirm the fact that principles of persuasion are not alone. Interfaces, their content and the way they are designed and how the information is presented also have a large impact on users' decisions so more research is required into the effectiveness of persuasive design in the domain of security as well as in the detection and analysis of phishing emails.

Although the principles of *Liking, Similarity & Deception* (LSD) and of *Distraction* (DIS) alone can be important to detect problems in emails we believe that the way they are used together makes them more successful. For instance, when both the principle of *Liking, Similarity & Deception* (LSD) and the principle of *Distraction* (DIS) are paired with the principle of *Authority* (AUTH), which is the majority of times for data theft emails, we can see that this is not a coincidence. Humans respond to authority and requests to make things right, so the principles of *Liking, Similarity & Deception* (LSD) and of *Distraction* (DIS) work better when they contain some authority elements as well. This is also true for malware emails but there are some differences in fraud emails. For fraud emails it seems that the principle of *Authority* (AUTH) is not as common. Instead, the principle of *Commitment, Reciprocation & Consistency* (CRC) is used more because this type of email tends to be more personal and more informal so they replace the sense of authority with the next best possible principle that makes users commit and be consistent with what they are asked. In this case, the emails are very personal, are written in the first person in what appears to be someone who knows the user and seems to have some type of

relation within him/her. Asking favours from the user in these circumstances appears more normal. These results show that principles of social engineering are commonly used together so further research is needed to understand in more detail what pairs are used and with what goals. Again, we believe that it will be harder to automatically identify the combination of all these principles so we need new tools that can help us do this.

It is however surprising that the principle of *Social Poof* (SP) is the least used with very low counts. It would be expected, mainly in fraud emails, that these strategies of social awareness, belonging to a group and sharing the same risks could be exploited more frequently. Although we are social beings, when making our decisions, we probably focus more on ourselves, our experiences and how we see the world. We think social engineers target their attacks to appeal to the individual and how important and relevant his/her own actions are to the matter at hand.

While this work identifies which combinations of principles are applied to phishing emails further work is required to explore whether any combinations are more effective in persuading people to act than others. The analysis did not have access to the success rate of the different types of combinations. Now that we have the principles, the next step would be to analyse the success rates of the different combinations.

Other Social Engineering Elements in Phishing. In addition to our principles, phishing emails use more tricks to deceive people and convince them of the authenticity of the email's content. These include, for instance, the repetition of information; the use of bigger and smaller font; the use of bold face; the use of different text colors; or the use of tables. These elements are all about the way information is displayed as specific visual cues can, in fact, influence users' decisions (e.g., Gestalt principles [12,13]), and are very effective when used in phishing emails. These can probably generate other principles besides the ones studied here and so need to be analysed in future work.

Limitations. There was no previous work that could guide us in the analysis and merging of existing research on principles of persuasion, so we defined a methodology that could, as objectively as possible, focus on text and description provided for each principle. Also, the analysis performed on the phishing emails could not be automated. Although there is software to identify phishing emails, there is no software to verify which principles of social engineering, the elements present in those emails, express. This also explains the small sample since it would not be possible to perform an exhaustive analysis, with a bigger sample, in the available time.

7 Conclusion

By studying the relations among existing principles of influence (Cialdini), psychological triggers (Gragg) and principles of scams (Stajano *et al.*), we propose a synthesized list of principles of persuasion that constitute a basis for principles

of social-engineering. We found that our principles are largely used in phishing emails where they mainly appear in specific pairs or triplets. Although the principles of persuasion in social engineering obtained in this paper are not usually used alone (e.g., together with other visual cues and interface dynamics), we consider that the proposed list can help researchers to better recognise and understand how, in what situations and for what purpose those principles are used. With this knowledge, we intend to study and design countermeasures which can be better equipped to target and minimize the success of specific types of social engineering attacks.

References

1. Mitnick, K., Simon, W.: The Art of Deception. Wiley Publishing Inc., New York (2002)
2. Cialdini, R.B.: Influence: The Psychology of Persuasion (Revision Edition). Harper Business, Dunmore (2007)
3. Quiel, S., Uebelacker, S.: The social engineering personality framework. In: Proceedings of 4th Workshop on Socio-Technical Aspects in Security and Trust (STAST 2014), Vienna, Austria, 18 July 2014, pp. 24–30 (2014)
4. Akbar, N.: Analysing persuasion principles in phishing emails. Ph.D. dissertation, Master Thesis, University of Twente, The Netherlands, October 2014
5. Gragg, D.: A multi-level defense against social engineering. Technical Report, SANS Institute - InfoSec Reading Room (2003)
6. Stajano, F., Wilson, P.: Understanding scam victims: seven principles for systems security. Commun. ACM **54**(3), 70–75 (2011)
7. Scheeres, J.W., Mills, R.F., Grimaila, M.R.: Establishing the human firewall: reducing an individual's engineering attacks. In: Proceedings of the 3rd International Conference on Information Warfare and Security (ICIW), Omaha, USA, 24–25 April 2008
8. Fette, I., Sadeh, N., Tomasic, A.: Learning to detect phishing emails. In: Proceedings of the 16th Interenational Conference on World Wide Web (WWW 2007), Banff, AB, Canada, 8–12 May 2008, pp. 649–656. ACM (2007)
9. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., Hong, J.: Teaching Johnny not to fall for phish. ACM Trans. Internet Technol. **10**(2), 1–31 (2010)
10. Blythe, M., Petrie, H., Clark, J.A.: F for fake: four studies on how we fall for phish. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2011), Vancouver, BC, Canada, 7–12 May 2011, pp. 3469–3478. ACM (2011)
11. Martin, S.J., Goldstein, N., Cialdini, R.B.: The Small BIG: Small Changes that Spark Big Influence. Grand Central Publishing, New York (2014)
12. Arnheim, R.: The gestalt theory of expression. Psychol. Rev. **56**, 156–171 (1945)
13. Geremek, A., Greenlee, M., Magnussen, S.: Perception Beyond Gestalt: Progress in Vision Research. Psychology Press, New York (2013)