Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016
A. Mathur and A. Roychoudhury (Eds.)

doi:10.3233/978-1-61499-617-0-107

Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention

Jan-Willem Bullée [a], Lorena Montoya [a], Marianne Junger [a] and Pieter H. Hartel [a]
[a] *University of Twente, Enschede, The Netherlands*

Abstract. The objective of this study is to evaluate the effectiveness of an information campaign to counter a social engineering attack via the telephone. Four different offenders phoned 48 employees and made them believe that their PC was distributing spam emails. Targets were told that this situation could be solved by downloading and executing software from a website (i.e. an untrusted one). A total of 46.15 % of employees not exposed to the intervention followed the instructions of the offender. This was significantly different to those exposed to an intervention 1 week prior to the attack (9.1 %); however there was no effect for those exposed to an intervention 2 weeks prior to the attack (54.6 %). This research suggests that scam awareness-raising campaigns reduce vulnerability only in the short term.

Keywords. Awareness, Decay, Scam, Social Engineering, Retention, Telephone, Time, Training

1. Introduction

Since 2008 a scam has been carried out by employees claiming to belong to Microsoft's technical department [1]. A phone call is received unexpectedly at home; the caller introduces himself and proceeds to inform the home owner that there is a virus on the PC or that the PC is distributing spam emails. To verify the claim from the caller, the victim is persuaded to open a remote desktop session to review some warnings in the system log files. In order to resolve the problem, the caller advises the victim to buy a small software tool to prevent loosing valuable data. The solution can be bought on their website and payment is possible via either credit card or PayPal. When the victim next checks the bank account, he/she discovers that the savings have disappeared. The victim thinks that he/she is securing the system whilst in fact the opposite has taken place.

Since 2011, the Dutch Fraud Help Desk (an organisation that collects fraud data) has received 4000 reports of this Microsoft technical support scam in The Netherlands. In 2014, there were 856 people who filed a complaint, and 88 (10.28 %) of them admitted to have paid the scammers. From January until September 2015 there were already 1099 complaints filed, of which 154 (14 %) involved payment. This constitutes a significant increase in both *i*) the number of filed complaints (z = 31.396, p = .000) and *ii*) the number of victims (z = 30.130, p = .000) for a short period of time. These numbers indicate that people are vulnerable to social engineering via the telephone.

Information security has been treated as a technical problem for many years, resulting mainly in technical solutions [2] and overlooking the human aspect [3]. Since information technology becomes more integrated into our daily activities, security experts propose that social engineering will be the greatest threat to any security system [2]. One example of social engineering is the technical support scam [4].

This paper therefore explores: *i*) the extent to which people are susceptible to telephone-based social engineering attacks when they are persuaded to go to a website and download a software and, *ii*) the effectiveness of an intervention to reduce the effects of social engineering over time.

1.1. Informing people to change behaviour

The Elaboration Likelihood Model (ELM) of Persuasion describes how information is processed and can be tailored to the receivers [5]. According to the ELM, people process information via either the peripheral or the central route. The peripheral route of information processing is used when there is minimal attention to the message and can involve superficial cues, such as the attractiveness of the message presented. One may like the sound of a person's voice, or that person might have gone to the same university as one did. The central route, on the other hand, involves persuasion on the basis of the message's content, such as voting for the political party with the best arguments [6]. Consistent with the ELM theory, attitudes obtained via the central route last longer, are less vulnerable to contra-argumentation and are better predictors of human behaviour. Furthermore, the effect of persuasive communication increases if the message is relevant to the audience and if surprises and repetitions are used [5].

Studies about leaflets have successfully increased the knowledge of the general public [7], as well as more specific groups such as patients [8], parents [9], and customers [10]. Experts argue that both training and education can help protect users against phishing [11]. It is noted that the currently available intervention materials can be effective as long as the user actually reads the material [11].

Gadgets can be used as subtle reminders of a campaign and are mentioned in the theory of Situational Crime Prevention as elements that 'remove excuses' [12]. Although the literature on reminder cues is limited, research suggests that these are effective [13]. In previous work we showed that exposing university personnel to both an information leaflet and a subtle reminder contributes to a significant reduction in the success rate of a social engineering attack [14].

1.2. Retention

In 1885 Herman Ebbinghaus demonstrated the existence of memory decay over time [15]. In addition, he described the 'forgetting curves', which refer to the amount of new information one is able to learn with each repetition of the same content. The amount of new information learned after each repetition decreases less steeply, meaning that more and more information stays in one's memory [15]. Retention can relate to knowledge but it can also relate to skill and is not limited to a single context as shown in the examples below.

Knowledge Ebbinghaus showed, using a list of 3 letter nonsense syllables (starting and ending with a consonant and a resonant in the middle), that over time, more syllables are forgotten [15]. Since the publication of this work, other research areas have looked into this topic as well, such as in the fields of aeronautics and medicine.

The aeronautical knowledge of 60 pilots was tested with a multiple-choice test, with items randomly selected from the Federal Aviation Administration (FAA) private pilot item bank of questions. A negative correlation was found between test scores and number of months since each pilot's last flight review (r = -.44, df = 18, t = 1.96, $p < .05$). This means that pilots who recently completed their flight reviews were associated with higher scores, compared to those with a longer time since the review [16].

In the field of medicine it was shown that the knowledge regarding Cardiopulmonary Resuscitation (CPR) dropped significantly over a period of 10 weeks. In this test 19 health care professionals (i.e. nurses) were tested via a 26 open item CPR theoretical questionnaire [17].

Skill The flight manoeuvres of a group of 192 pilots were tested in a full-motion flight simulator 6 and 12 months after training. During the test the pilots had to perform 12 emergency manoeuvres and 25 normal manoeuvres. The results showed there was a significant decay in performance between the 6 and 12 month group [18].

18 medical students were assessed on their CPR performance at three points in time: a) a pre-test to establish the baseline score, b) a training phase, c) a post-test and d) a re-test after 10 weeks. The test scores between the post- and re-test differed significantly, confirming skill decay [19].

In the context of a phishing test, the skill retention of adult subjects was measured 7 days after an information campaign [11]. During the test, the subjects had to classify 6 emails (as phishing emails or not) at 3 points in time (i.e. pre-test, post-test and re-test). This study did not find a significant decay of performance in classifying phishing emails.

This suggests that skill after training remains stable on the short term, but not on the long term. A further question to be answered is: how do the effects of training decay between 1 and 10 weeks?

1.3. Research Question

The objective of this research was to find out: "*How susceptible are people to a technical support scam?*". The following hypothesis was formulated: **H1)** "Time influences the relation between compliance and intervention."

2. Method

The sample consisted of 48 subjects of both sexes who worked in one particular building on the campus of the University of Twente. All subjects were scientific personnel of 9 research groups. Only approached were those who *i*) had an office work space and *ii*) were present to answer the telephone.

2.1. Subject Selection

Professors, secretaries, support and laboratory staff were excluded from the experiment in order to minimize disruption of primary activities. The pool of subjects therefore consisted of PhD-candidates, Post-Doc researchers as well as Assistant and Associate professors. The sample consisted of 34.29 % of all possible targets; the nationality distribution was comparable to the overall nationality distribution of the faculty, while those in the experimental sample were slightly younger (38 vs. 41 years).

2.2. Researchers

The researchers (i.e. the "offenders") consisted of 4 bachelor students (2 female and 2 male). The age of the researchers ranged between 21 and 24, the average age was 22.25 years (SD = 1.26). All researchers were Dutch nationals. There was no restriction with regards to approaching subjects of the same gender.

Procedure One-third of the potential subjects was exposed to an information campaign two weeks before the experiment whilst another one-third was exposed one week before. The research departments were randomly selected and all their staff was exposed to the intervention.

The intervention consisted of two parts: *i*) a leaflet informing staff about what constitutes a scam and describing how scammers operate, how to detect them and what to do and *ii*) a reminder in the form of a semi-transparent card holder with the university logo on one side and the text "Beware of scams. Verify all requests. Report all incidents." on the other side.

The leaflets were designed using story telling to ensure that non experts could understand it as well [20]. The leaflet represents the information medium and the card holder represents a cue to remember the message. Departmental secretaries were responsible for distributing the materials and they were unaware that this was part of an experiment. The leaflet was distributed via email, whereas the card holder was distributed in person. All subjects were approached via telephone between 0930h and 1700h, on an normal Monday during term time.

The researchers were randomly assigned to a target, however if the researcher recognised a target, this target person was randomly assigned to another researcher. Each researcher approached the subject using the following script:

> Hi this is `[name]`. We discovered that the PC you are using is distributing spam emails. This is caused by a malicious program that is running in the background. Did you notice that your PC was a bit slower lately? There is nothing to be ashamed of, there are other people who have the same problem. I already helped 3 people to fix this earlier this morning. Luckily this is easy and quick to solve. Do you have 2 or 3 minutes time, so that we can remove it together right away? Please click the link that appears in the chat window. URL: `http://removespam.utwente.info`. To proceed to the download, please enter the validation code; this is your complete employee number. The complete number can be found on the back of your employee card. Please save the file to your Desktop and execute it. After the program is finished, could you read out the completion code?

All targets were subjected to the same script and request. After the target indicated that the downloaded file was installed, the debriefing procedure was started. During the debriefing procedure the target was told that this was an experiment, and asked some demographic information, employment length, some computer characteristics and their reasons for or against downloading and installing the software. Finally, the importance of not sharing any information about the experiment with colleagues was explained; all subjects acknowledged this and agreed not to disclose any information. This was checked during the debriefing and none of the subjects stated having had prior knowledge of the experiment.

2.3. Variables and Analysis

The variables used in the analysis were: compliance, intervention, age, offender and sex. The dependent variable compliance measured whether the subject complied with the request of the offender to download and install the software package. The dichotomous variable was dummy coded as 0 = did not comply, 1 = did comply. The independent variable intervention measured whether the subject was exposed to the intervention (0 = not exposed to the intervention, 1 = exposed to the intervention 1 week before, 2 = exposed to the intervention 2 weeks before). The independent continuous variable age measured the age in whole years at the moment of the attack. The independent categorical variable offender measured who performed the attack (1 = researcher1, . . . , 4 = researcher4). The independent dichotomous variable sex was measured for both the subjects and the researchers and was dummy coded (0 = female, 1 = male). The hypothesis was tested using cross-tabulation and χ^2.

3. Results

A total of 48 subjects were approached. No 'target sex' effect on compliance ($\chi^2 = .470$, $df = 1$, $p = .493$), 'offender sex' effect on compliance ($\chi^2 = .176$, $df = 1$, $p = .675$), 'offender' effect on compliance ($\chi^2 = 4.253$, $df = 3$, $p = .354$) and 'target age' effect on compliance ($OR = .997$, $p = .905$) were found and therefore these issues are not further mentioned.

The debriefing procedure was used to verify that the subjects were coded correctly (i.e. had received an intervention or had not received an intervention). The subjects who recalled receiving the intervention material were coded as intervention group whilst those who could not recall having received any intervention material were coded as control group.

3.1. H1: *"Time influences the relation between compliance and intervention."*

The compliance for the control group was 46.15 % compared to 9.09 % for those exposed to the information campaign 1 week prior to the measurement. The compliance of those exposed to the campaign 1 week prior was 9.09 % compared to 54.55 % for those exposed to the campaign 2 weeks prior to the measurement. The compliance for the control group was 46.15 % compared to 54.55 % for those exposed to the campaign 2 weeks prior to the measurement. A difference was found between the control and the 1 week group, furthermore a difference was found between the 1 week and 2 week group. However no difference was found between the control and the 2 week group. Hypothesis 1 is therefore accepted. Refer to Table 1 for descriptive statistics.

Table 1. Number of observations and percentages per intervention condition over time

		Intervention			
		No	1 week	2 weeks	Total
Complied	No	14 (53.85%)	10 (90.91%)	5 (45.45%)	29 (60.42%)
	Yes	12 (46.15%)	1 (9.09%)	6 (54.55%)	19 (39.58%)
Total		26 (100%)	11 (100%)	11 (100%)	48 (100%)

Group control = 1 week (χ^2 = 4.659, df = 1, p = .031);
Group control = 2 week (χ^2 = 0.218, df = 1, p = .641;
Group 1 week = 2 week (χ^2 = 5.238, df = 1, p = .022);

4. Discussion

This study investigated whether an information campaign influences the compliance with a telephone request to download and install software available on the internet, over time.

An information campaign consisting of *i*) informing employees about the dangers of telephone scams and *ii*) distributing a card holder with a reminder text was effective in the short term to reduce the vulnerabilty of employees to follow a stranger's request to perform actions on their PC.

In total 9.09 % of the employees exposed to an information campaign (1 week prior to the attack) compared to 46.15 % in the control group complied with the request to download and execute software available on the internet. Those not exposed to the campaign (1 week prior) have 8.13 higher odds of complying with the offenders request. These findings are in line with the results Bullée et al. [14] in which university personnel was approached by strangers and asked to hand over their keys.

The employees exposed 2 weeks prior showed no difference to the control group. The CPR studies of Madden [19] and Broomfield [17] both showed a significant decay since the training, however they measured their decay over a period of 10 weeks time.

One explanation for the difference could be the modality of information that is transferred, (i.e. visual leaflet). The effect of different modalities on memory has been shown in an experiment where the subjects had to remember and recall a list of words or auditory representations. The results showed that the auditory representations had both a significant better *i*) recall and *ii*) recall order of the presented stimuli [21]. Glenberg showed that this auditory modality effect is also present in long term memory, this means that auditory stimuli were better remembered in the long term compared to their visual counterparts [22].

An second alternative explanation could be in the process of creating a memory. There are 3 processes that constitute memory processing: *i*) Encoding, *ii*) Consolidation and *iii*) Retrieval. Encoding is the process of forming mental representations of the materials one wants to put in memory. The process of encoding is enhanced by elaboration (interpretation of the materials and connecting them to other materials) and trying to repeat it to oneself [23]. Attention is important as well; when attention is divided as encoding will be weaker and later attempts to remember are likely to fail [24, p. 202]. The consolidation process modifies the mental representation in such a way that it becomes stable in memory. Consolidation of the declarative memory (explicit memory containing experiences and information) can be affected by sleep [25], caffeine intake [26] and age [27]. Finally, retrieval is important to access the knowledge in the brain via cues. The context (e.g. physical surrounding) in which a memory is created is important for retrieval. The theory of optimistic bias states that people believe that positive events are more likely to occur to them than to other people [28] and that negative events are more likely to occur to other people than to themselves. In the context of the information campaign, a possibility is that the subjects could not identify themselves with the material because they thought that it was not applicable to them, since there are others who were more vulnerable. In both cases the subjects will not have the appropriate attention to properly encode the material to make it last in the memory.

A third explanation could be that the information campaign is too abstract and therefore an ambiguous memory cue is created for the material. Once the subject is ‘attacked’ there is no proper recollection of the cue to memory and he/she fails to recollect the materials in the information campaign. This could explain the difference between the 1 and 2 week groups as the cues are simply forgotten over time. It would be too simple to say that the subjects forgot about the information campaign since there were questions to control for this, since the subjects stated they recalled having received and read the materials.

Limitations This study has 2 limitations: *i*) The current study has a limited number of observations, therefore only a limited number of variables could be tested. *ii*) All subjects were from the same organisation, replication in other organisations would be needed.

Acknowledgements

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the author’s views and the Union is not liable for any use that may be made of the information contained herein. In addition, we would also like to thank Christian Orriëns, Koen de Jong, Evelien Kroon, and Hilde Jansen for their valuable contribution to this research.

References

[1] C. Arthur, “Virus phone scam being run from call centres in india,” 18 July 2010 2010. [Online]. Available: http://www.theguardian.com/world/2010/jul/18/phone-scam-india-call-centres

[2] M. Rouse. (2006) Definition Social Engineering. [Online]. Available: http://www.searchsecurity.techtarget.com/definition/social-engineering

[3] H.-S. Rhee, C. Kim, and Y. U. Ryu, “Self-efficacy in information security: Its influence on end users’ information security practice behavior,” *Computers & Security*, vol. 28, no. 8, pp. 816 – 826, 2009.

[4] D. Harley, M. Grooten, S. Burn, and C. Johnston, “My pc has 32,539 errors: how telephone support scams really work,” *22nd Virus Bulletin International Conference (VB2012)*, 2012.

[5] R. E. Petty and J. T. Cacioppo, “The elaboration likelihood model of persuasion,” in *Communication and Persuasion*. Springer, 1986, pp. 1–24.

[6] ——, *Attitudes and Persuasion–classic and Contemporary Approaches*. W.C. Brown Company Publishers, 1981.

[7] S. Stubbings, K. Robb, J. Waller, A. Ramirez, J. Austoker, U. Macleod, S. Hiom, and J. Wardle, “Development of a measurement tool to assess public awareness of cancer,” *Br J Cancer*, vol. 101, no. S2, pp. S13–S17, 2000.

[8] J. Barlow, “Knowledge in patients with rheumatoid arthritis: a longer term follow- up of a randomized controlled study of patient education leaflets,” *Rheumatology*, vol. 37, no. 4, pp. 373–376, 1998.

[9] F. Ghaderi, A. Adl, and Z. Ranjbar, “Effect of a leaflet given to parents on knowledge of tooth avulsion.” *European journal of paediatric dentistry : official journal of European Academy of Paediatric Dentistry*, vol. 14, no. 1, pp. 13–6, 2013.

[10] S. M. Shim, S. H. Seo, Y. Lee, G. I. Moon, M. S. Kim, and J. H. Park, "Consumers'knowledge and safety perceptions of food additives: Evaluation on the effectiveness of transmitting information on preservatives," *Food Control*, vol. 22, no. 7, pp. 1054–1060, 2011.

[11] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Transactions on Internet Technology*, vol. 10, no. 2, pp. 1–31, 2010.

[12] D. B. Cornish and R. V. Clarke, "Opportunities, precipitators and criminal decisions: A reply to wortley's critique of situational crime prevention," *Crime prevention studies*, vol. 16, pp. 41–96, 2003.

[13] I. Flight, C. Wilson, and J. McGillivray, "Turning intention into behaviour: The effect of providing cues to action on participation rates for colorectal cancer screening," *Colorectal Cancer-From Prevention to Patient Care. Shanghai: InTech*, pp. 67–86, 2012.

[14] J. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *Journal of Experimental Criminology*, vol. 11, no. 1, pp. 97–115, 2015.

[15] H. Ebbinghaus, *Memory: A Contribution to Experimental Psychology*. Teachers College, Columbia University, 1913, no. 3.

[16] S. Casner, D. Heraldez, and K. Jones, "Retention of aeronautical knowledge," *International Journal of Applied Aviation Studies*, vol. 6, no. 1, pp. 71–98, 2006.

[17] R. Broomfield, "A quasi-experimental research to investigate the retention of basic cardiopulmonary resuscitation skills and knowledge by qualified nurses following a course in professional development," *Journal of Advanced Nursing*, vol. 23, no. 5, pp. 1016–1023, 1996.

[18] S. M. L. Hendrickson, T. E. Goldsmith, and P. J. Johnson, "Retention of airline pilots' knowledge and skill," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 50, no. 17, pp. 1973–1976, 2006.

[19] C. Madden, "Undergraduate nursing students acquisition and retention of CPR knowledge and skills," *Nurse Education Today*, vol. 26, no. 3, pp. 218 – 227, 2006.

[20] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12. New York, NY, USA: ACM, 2012, pp. 6:1–6:17.

[21] A. Drewnowski and B. B. Murdock, "The role of auditory features in memory span for words." *Journal of Experimental Psychology: Human Learning and Memory*, vol. 6, no. 3, pp. 319 – 332, 1980.

[22] A. M. Glenberg, "A retrieval account of the long-term modality effect." *Journal of Experimental Psychology: Learning, Memory, and Cognition*, vol. 10, no. 1, pp. 16 – 31, 1984.

[23] F. I. Craik and R. S. Lockhart, "Levels of processing: A framework for memory research," *Journal of verbal learning and verbal behavior*, vol. 11, no. 6, pp. 671–684, 1972.

[24] E. Smith and S. Kosslyn, *Cognitive Psychology: Mind and Brain*, ser. Pearson Education. Pearson Prentice Hall, 2008.

[25] A. Ashworth, C. M. Hill, A. Karmiloff-Smith, and D. Dimitriou, "Sleep enhances memory consolidation in children," *Journal of Sleep Research*, vol. 23, no. 3, pp. 304–310, 2014.

[26] S. E. Favila and B. A. Kuhl, "Stimulating memory consolidation," *Nature Neuroscience*, vol. 17, no. 2, pp. 151–152, 02 2014.

[27] L. Cahill, B. Prins, M. Weber, and J. L. McGaugh, "β-adrenergic activation and memory for emotional events," *Nature*, vol. 371, no. 6499, pp. 702–704, 10 1994.

[28] N. D. Weinstein, "Unrealistic optimism about future life events." *Journal of personality and social psychology*, vol. 39, no. 5, p. 806, 1980.