Victim Communication Stack: A flexible model to select the Human Attack Vector

Enrico Frumento, Federica Freschi
Cefriel Politecnico di Milano, Milan, Italy
Email: name.surname@cefriel.com

Angelo Consoli, Davide Andreoletti
University of Applied Sciences of Southern Switzerland
Manno, Switzerland
Email: name.surname@supsi.ch

September 15, 2017

Abstract

Information security has rapidly grown to meet the requirements of today services. A solid discipline has been developed as far as technical security is concerned. However, the human layer plays an increasingly decisive role in the managing of Information Technology (IT) systems. The research field that studies the vulnerabilities of the human layer is referred to as Social Engineering, and has not received the same attention of its technical counterpart. We try to partially fill this gap by studying the selection of the Human Attack Vector (HAV), i.e., the path or the means that the attacker uses to compromise the human layer. To this aim, we propose a multilayer model, named Victim Communication Stack (VCS), that provides the key elements to facilitate the choice of the HAV. This work has been carried out under the DOGANA European project.

This paper has been published in the Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES 2017), August 29 - September 1, 2017, Universit degli Studi Mediterranea di Reggio Calabria, Italy and the support of the DOGANA project (GA no. 653618)

1 Introduction

Information Technology (IT) plays a pivotal role in our society. Data are the fuel of the new economy and have therefore rapidly gained high financial value. The commerce of data has become an appealing source of revenue for cyber criminals, who steal them from companies and sell them on the black market. It has been estimated that the average lost for a breach of 1000 records of data is between $52000 and $87000 [1].

A relevant portion of data is generated by cheap and portable devices equipped with many functionalities (e.g., camera and GPS trackers), which results in advanced services increasingly tailored to the final users, e.g., location-based services [2] and user-specific advertising [3]. Thus, beside their economic value, the trade of data also raises severe privacy concerns. Due to these reasons, efficient security procedures are constantly needed to ensure that the likelihood of data breaches remains as low as possible.

Modern cyber-attacks can be roughly divided in two main categories: technical and non-technical ones. Traditional security countermeasures have mostly focused on the technical aspect of cyber-attacks, i.e., those that exploit the vulnerabilities of the devices. For instance, the IPsec protocol [4] has been developed to meet security requirements not satisfied by the original IP protocol.

However, the final user who manages IT systems presents vulnerabilities and is prone to errors. Moreover, various emerging phenomena (e.g., the *Bring your own device* (BYOD) paradigm [5]) further increase the power that final users have on their data. With great power comes great responsibility, and many unskilled or inattentive users might be unprepared to cope with new complex attacks. Given also that the human layer is widely considered as the weakest link of the security chain [6], it is of paramount importance to efficiently secure it.

The research field that studies how to attack the human layer is referred to as Social Engineering (SE). It is a broad discipline grounded in psychology and finds its natural application in the context of information security. SE is receiving more attention during the last years. For example, the ongoing DOGANA[1] project is aimed at doing a step forward in the research on SE.

SE attacks might not be limited to the cyberspace (e.g., shoulder surfing is the action of looking over the victim's shoulder to obtain confidential in-

[1] http://www.dogana-project.eu/ (Grant Agreement Number 653618)

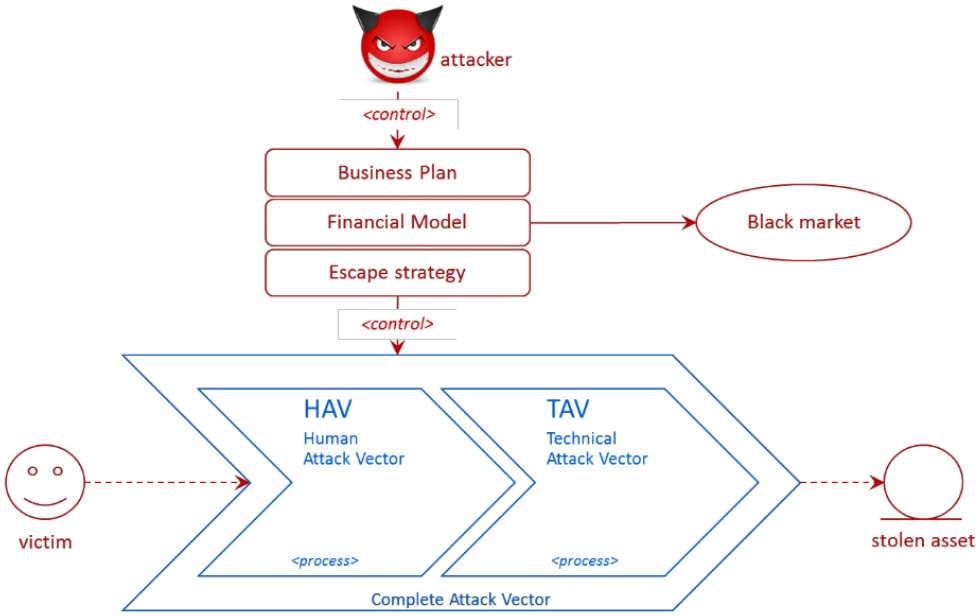

Figure 1: Complete Attack Vector and its relation with HAV, TAV and the business strategy

formation, not necessarily the digital ones, such as passwords and PINs [7]). However, despite its hybrid nature, we strongly believe that this discipline might benefit from the use of engineering approaches, e.g., modeling of the attack phases.

A foundamental part of a cyber attack is the choice of the attack vector, i.e., the path that the attacker uses to pursue her malicious goal. Modern attacks are formed by a combination of *human attack vectors* (HAV) and *technical attack vectors* (TAV). The former is created to compromise the human layer. The latter is created to compromise the devices. As the most disruptive attacks are motivated by financial goals, we depict in Figure 1 a schema representative of this scenario.

Examples of commonly used HAV include phishing, baiting and dumpster diving. As SE is still in its infancy with respect to its technical counterpart [8], we try to partially fill this gap by focusing on the choice of the HAV.

We propose a multilayer theoretical model, named Victim Communication Stack (VCS) Model, which is composed of 6 layers: *persona modelling*, *semantic*, *syntax*, *medium*, *device* and *context*. Details about each layer will

be given in Section 2. The model provides an effective way to create a victim template from which the most suitable HAV is derived. Both attackers and defenders are expected to benefit from the use of this model. On one hand, attackers will benefit from a more structured process for the selection of the HAV. On the other hand, defenders will be able to perform better analysis of the experienced attacks and accordingly propose tuned countermeasures.

The paper is structured as follows. In Section 2 the VCS model is described in detail. In Section 3 a review of the literature is presented. Section 4 is devoted to the presentation of various scenarios where the VCS model is used. Section 5 concludes the paper.

2 The Model

In this Section we describe the VCS model, which is used to choose the most suitable HAV. We take inspiration from the ontological model presented in [8], as it identifies the main entities involved in a SE attack. By entity we refer here to both the abstract ones (e.g., persuasion principles) to the more concrete ones (e.g., type of medium). Those entities have been mapped onto our model, which is composed of 6 layer, namely *Persona modelling*, *Semantic*, *Syntax*, *Medium*, *Device* and *Context*. This choice has been motivated by the high semantic and flexibility provided by multilayer models, such as the widely-used ISO/OSI [9]. The VCS model is depicted in Figure 2.

The users of the model (being the attacker choosing the HAV or the defender analyzing the attack) exploit the relation between adjacent layers, where each layer works based on information received from the upper one. In the following, the layers composing the model are described in details.

2.1 Persona modelling

The first layer of the model facilitates the selection of the victim, i.e., the type of person that most likely gives access to the desired asset, which is the attacker's ultimate goal. The modelling of the victim is done by projecting her profile over a set of different dimensions. The choice of the dimensions should take into account the impact that they have on the likelihood to be victim of a SE attack.

The dimensions that we propose in this work are:

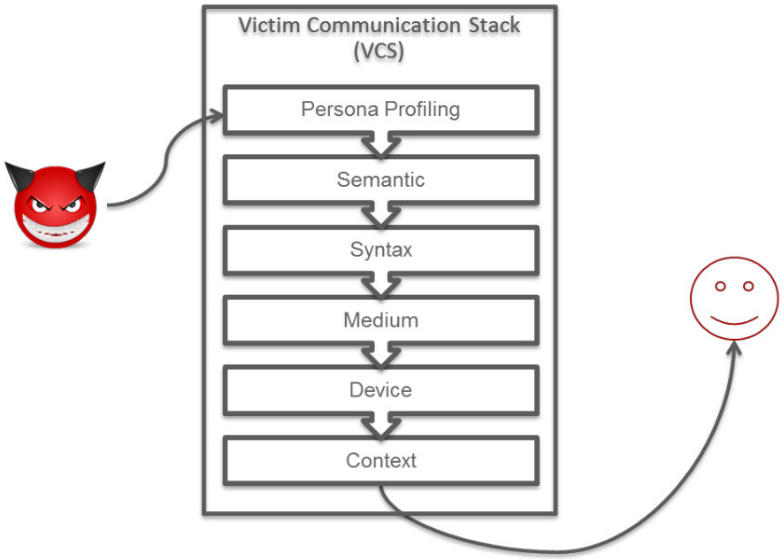

Figure 2: Victim Communication Stack (VCS) Model

- ***Personality***: this dimension concerns the identification of salient personality traits of the potential victim. The correlation between personality profiles and likelihood to be victim of a phishing attack has been shown in [10], where it has been proved that, the more extrovert a person is, the more likely she will open suspicious mail attachments. The use of personality templates (e.g., [11]) might help.
- ***Biographical Data***: age and gender are the most common examples, and have been studied in relation with the susceptibility to fall victim of a succesful attack.
- ***Social Role***: the role, being it both social (i.e., popular person) or related to the job (e.g., the boss).
- ***Cultural background***: this dimension can be very large, since it may include the religious background as well as the type of academic path. In particular, we consider important the relation that the potential victim has with the technology.

2.2 Semantic

The Semantic layer deals with the approaches that the attacker takes in order to *strike the right note* with her victim. From the higher layer, i.e., the Persona Modelling layer, the social engineer is able to make some assumptions about the mindset of the victim and infers her values and world view. Mind sets are unavoidable and implies a strong cognitive bias on one's reasoning [12]. The attacker exploits this intrinsic human characteristic to choose the most suitable persuasion technique to use. The 6 Cialdini's principles [13], namely *Reciprocity*, *Commitment and Consistency*, *Social Proof*, *Authority*, *Liking* and *Scarcity* are considered the basis of all the persuasion techniques.

2.3 Syntax

The syntax layer shapes the stylistic elements carrying the message. Stylistic choices may relate, for instance, to the style of the language (e.g., body language), to the graphic elements and to the linguistic register. This layer particularly depends on the upper one, as syntax and semantic are expected to be particularly consistent. Otherwise, it is more likely that the victim will have doubts about the malicious person [12]. For example, if the attacker tries to persuade her victim by saying only what she likes (i.e., Liking principle [13]) but her body language is inconsistent with the delivered message, it is easy for the victim to unmask her real purposes.

2.4 Medium

This layer concerns the choice of the medium to use to perform the attack. Some examples of media are: social media interactions, mail and chats, voice and physical presence, rogue mobile Apps and malevolent advertisements.

The decision of what is the best medium to employ strongly depends on the skills and self-confidence of the attacker. For example, the physical presence requires a better preparation (e.g., knowledge of the body language) and a different emotional control with respect to the far more impersonal e-mail medium.

2.5 Device

At this layer the attacker reasons about the device from which her victim will be attacked. For example, in case of phishing SMS, the device is likely to be a smartphone.

Notice that the proliferation of a vast amount of different types of devices has been accompanied with the evolution of increasingly pervasive interaction methods. The heterogeneity of the user interfaces is a non-negligible factor, as attacks may be crafted according to interaction that the victim has with the device. For example, the exposition to hundreds of notifications might lower the level of attention [14], and increase the likelihood to fall victim of a SE attack.

2.6 Context

It is arduous to clearly define what the context is. In the information security field the context has been defined as *every single piece of information that can categorize the situation of an entity in a given instant of time* [15].

Concerning the choice of the HAV, the context refers to the characteristics of the environment, the time and the place where the attack will be perpetrated, e.g., office during working hours. In this scenario, the context-aware computing paradigm [16] takes on particular importance, as a social engineer might leverage real-time context-related data, which are directly gathered from digital devices.

3 Related Work

This work tries to adapt the ontological model proposed in [8] to the selection of the most suitable HAV. To the best of our knowledge, this is the first attempt to provide a structured guideline for choosing the most suitable HAV based on victim templates. Therefore, there is not a reference literature for this specific topic. Consequently, we present the related work showing the relation of each layer of the model with the SE.

3.1 Persona modelling

A fundamental aspect of the persona modelling phase is the analysis of personality. The topic is very heterogeneous and not trivial to study. The

dominant papers in the field are [17] and [11]. The latter is an evolution of the former, and it is widely considered as a main reference model. It provides five dimensions of personality, namely *Openness to experience*, *Conscientiousness*, *Extraversion*, *Agreeableness*, and *Neuroticism*. The five-personality model has been widely used, e.g., to study job satisfaction[18] and leadership traits [19].

Studies on the relation between SE and personality traits have been presented in the literature [20, 21, 22]. For example, extraversion has proved to influence the tendency to reveal sensitive information [21].

Beside the personality traits, other factors have been studied in relation with the susceptibility to fall victim of a SE attack, such as the age [20, 23], the gender [24] and the cultural background [25, 26, 27].

3.2 Semantic

Persuasion techniques have received a lot of attention in the literature [28, 13, 29, 30]. They exploit intrinsic weaknesses of the human being, such as the unavoidability of cognitive biases. The topic is well described in [12].

The 6 Cialdini's principles briefly presented in Section 2 are a cornerstone of the theory of persuasion, and are extensively described in [13]. The importance of persuasion in relation with SE has been studied, mostly as far as phishing is concerned [31, 32].

3.3 Syntax

The stylistic choices refer to various elements, ranging from the body language to the linguistic register. The relation between body language and social engineering has been studied in [33]. Concerning attacks that require a written part (e.g., phishing e-mail) it has been shown that words should be chosen in order to increase the sense of urgency [34]. We assume that the same applies to the tone of voice (e.g., in vishing attacks), although none of the found sources have explored this issue.

We argue that the impact that this layer has on SE has not received the due attention in the literature. For example, to the best of our knowledge, a systematic study on the impact that the linguistic register has on the success of an attack (e.g., phishing) is still missing. The topic may represent a considerable step forward in the study of SE.

3.4 Medium

The number of possible media that a social engineer may utilize is very large. In order to make this choice as much effective as possible, the attacker might benefit from a deep understanding of the relation between victim's profiles and preferred medium. For instance, in [35] it has proved that age is a key factor in adopting a particular medium, e.g., elderly people likely do not use e-mails. Relation between SE and Social Networks (SN) has been studied, e.g., in [36]. SN proved to be one of the most favorable landscape for a social engineer, due to the numerous attack vectors that they present.

3.5 Device

Traditional SE attacks (e.g., e-mail phishing) may not require the victim to use a particular type of device. However, the incrasingly complex landscape of Human Machine Interfaces (HMI), as well as the multiplication of stimuli received by the victim, increases the power of the social engineer to craft attacks tailored to a particular device [14].

Devices play a particularly relevant role as far as information gathering is concerned. In fact, pervasive devices (e.g., IoT devices) have been widely used to obtain sensitive information about victims. For instance, smart TVs have been used to gather information concerning the psychological profiles of users [37]. Moreover, the attacker can leverage the ability of IoT devices to act in the physical space to further induce the victim into performing undesirable actions. The topic has been covered in [38].

3.6 Context

As documented in several studies (e.g., [39]) the context is relevant for a SE attacks and then as a part of the VCS, because it influences the attentive processes. Change of contexts changes the perceptions and reactions to attacks. Therefore, the choice of the context is mainly motivated by the level of attention that the victim is expected to have in a particular situation. As mentioned in Section 2.6, time and space are key dimensions that characterize the context, and are both related with the expected attention of the victim. For instance, it has been proved that attention is lowered in crowded places [40] and after many working hours [41].

4 From Theory to Practice

The VCS provides a victim instance that facilitates the choice of the most appropriate HAV. The attacker, based on the specific victim's profile that she obtains, performs a selection of the most suited components of the attack, layer by layer. However, due to the numerous variables that the problem presents, the passage from theory to practice (i.e., from the VCS instance to the actual HAV) is not straightforward. Therefore, in the following we provide some examples that help to understand this passage. A final discussion summarizes the benefit of the VCS. For the sake of simplicity, and without loss of generality, we describe scenarios where the TAV is not used.

4.1 Imaginary Scenario

In this section we put ourselves in the shoes of the attacker, starting from an imaginary but plausible scenario. The aim is to show the effectiveness of the VCS from her point of view.

A person with malicious goals finds out that a lot of valuable digital devices (e.g., smartphones and laptops) are used on a daily basis in the computer laboratory of the university campus. The attacker also finds that students are normally allowed to get inside the laboratory, if provided with a badge card. Her aim is to steal some of these objects and, at a later stage, to try to extract useful information from them.

We now show how the attacker can use the VCS to build a victim instance, from which the most suitable HAV can be easily derived.

- ***Persona profiling***: students are nearly always young and friendly people, with few worries about potential frauds.
- ***Semantic***: the attacker can gain the trust of her victim by employing the Reciprocity persuasion principle.
- ***Syntax***: the chosen linguistic register, as well as the body language, should be as much friendly as possible.
- ***Medium***: physical presence and normal chatting.
- ***Device***: no device is needed.

- ***Context***: when lecturers are finished (e.g., in the late afternoon), when it is normal that only few people are still at the university.

A possible HAV is the following. The attacker poses herself as a normal student and offers her victim a coffee under the pretext of getting useful information, e.g., about lectures and exams. After having gained her trust, she claims that her own badge card got lost, likely inside the computer laboratory. The attacker asks her victim to borrow her badge card for a while, she gets into the laboratory and pursues her goals. Notice the relevance of the chosen context, as the victim feels to be the only one able to help a person in need.

4.2 Analysis of the suffered attack

Here we show how the VCS model can be used to rigorously analyze suffered SE attacks. The aim is to decompose the HAV into its main components. We start from a real attack that have been carried out against US WhastApp users, in August 2015.

Attackers who claimed to be legitimate traders of authoritative companies (e.g., JPMorgan[2] and Goldman Sachs[3]) used WhatsApp to spread spam messages saying that the stoke price of the Avra Inc[4] company would have experienced a sudden increase in the following days. The fake campaign was effective, since the price increased by 640% from its opening price of $0.17 to its peak of $1.26[5]. As expected, the stock price crashed shortly thereafter.

In the following we use the VCS model to analyze the HAV relative to the described attack.

- ***Persona profiling***: the spam message has been sent to an unknown number of WhatsApp users, without any explicit selection criteria. The number of receivers was high and, from statistical considerations, we can easily conclude that the general background was far from cybersecurity.

- ***Semantic***: both the Liking and the Authority techniques have been used. In fact, by receiving an appealing message, victims feel to be

[2]https://www.jpmorgan.com/country/IT/en/jpmorgan
[3]http://www.goldmansachs.com/
[4]http://www.avraglobal.com/
[5]https://www.helpnetsecurity.com/2015/08/28/the-whatsapp-of-wall-street/

privileged (Liking persuasion principle). Authority is implicitly used as the messages apparently came from traders belonging to a renowned company (e.g., JPMorgan).

- ***Syntax***: the linguistic register is that of the everyday life, as it aims at increasing the level of trust. An example of message that has really been sent is[6]: *It's will with jpmorgan I remember you wanted me to tell you next time I have a good tip. AVRN is going up 300% next week. Dont tell me I didnt give you a heads up ;).*
- ***Medium***: the WhatsApp platform.
- ***Device***: any device supporting WhatsApp, e.g., mobile terminals.
- ***Persona profiling***: early hour in the Friday morning, to exploit the potential reduction of attention just before the week end.

4.3 Some final considerations

We envision two broad target categories of users of the VCS: the attacker and the defender.

As far as the former is concerned, the HAV is not rigidly derived from the victim template obtained using the VCS, which is just a theoretical model aimed at helping the attacker to rigorously organize the information found about her victims. HAVs are not well-defined entities and are therefore not easily categorizable. Thus, it is not possible to provide a precise method to extract the HAV from the VCS template. The creativity of the attacker plays a crucial role in this phase. The example described in Section 4.1 may help to understand this passage.

As far as the latter is concerned, the VCS helps the defender (e.g., the security manager of a company) to rigorously analyze the suffered attack by disassembling it into its main components (see Section 4.2). This approach allows the defender to understand the weaknesses of the human capital and, possibly, to propose tailored countermeasures, such as suitable awareness programs. Awareness programs are methods that the security manager of a company uses to raise the level of awareness of the employees in the field of information security. Examples of awareness methods are posters or lectures. They have been extensively studied during the DOGANA[2] project, mostly in relation with their effectiveness (e.g., by means of SWAT analysis). We

believe that the selection of the most suitable awareness method can strongly benefit from the use of the VCS model.

5 Conclusions

This study started from the observation that a reference model for the selection of the most appropriate HAV was never presented in the literature. In order to fill this gap, we proposed a layered model that helps to choose it by disassembling a SE attack into its main components.

We called the model Victim Communication Stack (VCS). The model encompasses all the main characteristic of a HAV, and is not limited to a particular scenario. The VCS model is expected to be beneficial for the attacker and for the defender. The former will more easily choice the main components of the HAV. The latter will be able to better analyze a) suffered attacks and b) the vulnerabilities of her human capital [42].

As a future work, we plan to study the applicability of the VCS model to various scenarios, such as the selection of the most suitable awareness method.

References

[1] Michele Maasberg and Charles Liu. Network effects and data breaches: Investigating the impact of information sharing and the cyber black market. 2015.

[2] Iris A Junglas and Richard T Watson. Location-based services. *Communications of the ACM*, 51(3):65–69, 2008.

[3] Victoria Bolotaeva and Teuta Cata. Marketing opportunities with social networks. *Journal of Internet Social Networking and Virtual Communities*, 2010:1–8, 2010.

[4] Russell Housley. Using advanced encryption standard (aes) counter mode with ipsec encapsulating security payload (esp). Technical report, 2003.

[5] Arnab Ghosh, Prashant Kumar Gajar, and Shashikant Rai. Bring your own device (byod): Security risks and mitigating strategies. *Journal of Global Research in Computer Science*, 4(4):62–70, 2013.

[6] Stephen Lineberry. The human element: The weakest link in information security. *Journal of Accountancy*, 204(5):44, 2007.

[7] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 13–19. ACM, 2007.

[8] Francois Mouton, Mercia M Malan, Louise Leenen, and Hein S Venter. Social engineering attack framework. In *Information Security for South Africa (ISSA), 2014*, pages 1–9. IEEE, 2014.

[9] Hubert Zimmermann. Osi reference model–the iso model of architecture for open systems interconnection. *IEEE Transactions on communications*, 28(4):425–432, 1980.

[10] Ibrahim Alseadoon, Taizan Chan, Ernest Foo, and Juan Gonzales Nieto. Who is more susceptible to phishing emails?: A saudi arabian study. In *ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012*, pages 1–11. ACIS, 2012.

[11] Robert R McCrae and Oliver P John. An introduction to the five-factor model and its applications. *Journal of personality*, 60(2):175–215, 1992.

[12] Richards J Heuer. *Psychology of intelligence analysis*. Lulu. com, 1999.

[13] Robert B Cialdini and Nathalie Garde. *Influence*, volume 3. A. Michel, 1987.

[14] Claudia Roda. *Human attention in digital environments*. Cambridge University Press, 2011.

[15] Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In *International Symposium on Handheld and Ubiquitous Computing*, pages 304–307. Springer, 1999.

[16] Manish J Gajjar. *Mobile Sensors and Context-Aware Computing*. Morgan Kaufmann, 2017.

[17] Hans Jurgen Eysenck and SGB Eysenck. The eysenck personality inventory. 1965.

[18] Timothy A Judge, Daniel Heller, and Michael K Mount. Five-factor model of personality and job satisfaction: a meta-analysis., 2002.

[19] Timothy A Judge, Joyce E Bono, Remus Ilies, and Megan W Gerhardt. Personality and leadership: a qualitative and quantitative review. *Journal of applied psychology*, 87(4):765, 2002.

[20] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 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*, pages 373–382. ACM, 2010.

[21] Tzipora Halevi, James Lewis, and Nasir Memon. A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web*, pages 737–744. ACM, 2013.

[22] Arun Vishwanath. Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. *Journal of Computer-Mediated Communication*, 20(5):570–584, 2015.

[23] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, page 3. ACM, 2009.

[24] JG Mohebzada, A El Zarka, Arsalan H BHojani, and Ali Darwish. Phishing in a university community: Two large scale phishing experiments. In *Innovations in Information Technology (IIT), 2012 International Conference on*, pages 249–254. IEEE, 2012.

[25] Mariam Al-Hamar, Ray Dawson, and Lin Guan. A culture of trust threatens security and privacy in qatar. In *Computer and Information*

Technology (CIT), 2010 IEEE 10th International Conference on, pages 991–995. IEEE, 2010.

[26] Abdullah Alnajim and Malcolm Munro. Effects of technical abilities and phishing knowledge on phishing websites detection. In *Proc. the IASTED International Conference on Software Engineering (SE 2009), Innsbruck, Austria, ACTA Press*, pages 120–125, 2009.

[27] Jingguo Wang, Tejaswini Herath, Rui Chen, Arun Vishwanath, and H Raghav Rao. Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4):345–362, 2012.

[28] Vivian Parker Makosky. Identifying major techniques of persuasion. *Teaching of Psychology*, 12(1):42–43, 1985.

[29] Gerald R Miller and Michael Burgoon. *New techniques of persuasion.* Harper & Row New York, 1973.

[30] Noah J Goldstein, Steve J Martin, and Robert Cialdini. *Yes!: 50 scientifically proven ways to be persuasive.* Simon and Schuster, 2008.

[31] Nurul Akbar. Analysing persuasion principles in phishing emails. 2014.

[32] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. Principles of persuasion in social engineering and their use in phishing. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 36–47. Springer, 2015.

[33] Christopher Hadnagy. *Unmasking the social engineer: The human element of security.* John Wiley & Sons, 2014.

[34] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 905–914. ACM, 2007.

[35] Steve Beger Scott McDaniel. Do different age groups prefer different channels?, 2016.

[36] Abdullah Algarni, Yue Xu, Taizan Chan, and Yu-Chu Tian. Social engineering in social networking sites: how good becomes evil. In *Proceedings of the 18th Pacific Asia conference on information systems (PACIS 2014)*. The Association for Information Systems (AIS), 2014.

[37] L. Kelion. Lg investigates smart tv 'unauthorised spying' claim, 2013.

[38] McAfee. Social engineering in the internet of things (iot), 2016.

[39] Annelies Vredeveldt and Timothy J Perfect. Reduction of environmental distraction to facilitate cognitive performance. *Frontiers in psychology*, 5, 2014.

[40] Fang Fang and Sheng He. Crowding alters the spatial distribution of attention modulation in human primary visual cortex. *Journal of Vision*, 8(9):6–6, 2008.

[41] Peter Joseph Jongen, Keith Wesnes, Björn van Geel, Paul Pop, Evert Sanders, Hans Schrijver, Leo H Visser, H Jacobus Gilhuis, Ludovicus G Sinnige, Augustina M Brands, et al. Relationship between working hours and power of attention, memory, fatigue, depression and self-efficacy one year after diagnosis of clinically isolated syndrome and relapsing remitting multiple sclerosis. *PloS one*, 9(5):e96444, 2014.

[42] E Frumento and R Puricelli. An innovative and comprehensive framework for social driven vulnerability assessment. *Magdeburger Journal zur Sicherheitsforschung*, 2:493–505, 2014.