Guidelines for Security Education, Training and Awareness: a literature review

Olivier de Casanove, Florence Sèdes

Guidelines for Security Education, Training and Awareness: a literature review

Olivier de Casanove[1], Florence Sèdes[1]

[1]Université Toulouse III - Paul Sabatier, 118 route de Narbonne, 31400 Toulouse, France

Abstract

Security standards help to create security policies, but they are often very descriptive, especially when it comes to security awareness. Information systems security awareness is vital to maintain a high level of security. SETA programmes (Security Education, Training and Awareness) increase information systems security awareness and play an important role in finding the strategic balance between the prevention and response paradigms. By reviewing the literature, we identify guidelines for designing a SETA programme following a PDCA (Plan Do Check Adjust) cycle.

Keywords

Flexible automation, Prevention, PDCA, information systems security, Awareness, SETA, Guidelines, Review

1. Introduction

Security awareness is very difficult to define. Tsohou et al. [1] even conclude their paper saying that the absence of concrete definition creates frustration among security experts; this could be a reason why security awareness remains a problem. In this article we will consider that the objective of security awareness is to reduce the share of security incidents caused by humans. It is difficult to estimate how many of the security breaches are caused by humans. To give an idea of the problem, M.G. Lee [2] estimates, using a dataset from the United Kingdom Commissioner's Office, that 46.2% of security breaches resulting in a privacy violation are due to human error by well-meaning insiders.

To decrease the proportion of security incidents caused by well-meaning users, we need to educate them. As stated in [3] "Accountability must be derived from a fully informed, well-trained and aware workforce." Some information system security standards define objectives to promote a security culture and to raise awareness. Some of the most famous standards addressing this concern are the ISO/IEC 27000 family [4] and COBIT [5]. These standards often follow a Plan Do Check Adjust (PDCA) cycle. PDCA is a method for control and continuous improvement of processes or tools. As the IT world is ever-evolving, a continuous improvement method such as PDCA is suitable for information systems security. PDCA is also a great tool for flexible automation. Unfortunately, many information system security standards are very descriptive [6]. They set goals to reach but rarely offer advice on how to reach them; there is a

C&ESAR 2021: Automation in Cybersecurity

olivier.decasanove@irit.fr (O. d. Casanove); florences.sedes@irit.fr (F. Sèdes)

https://www.irit.fr/~Florence.Sedes/ (F. Sèdes)

need for guidelines.

In this paper we will review the literature to identify guidelines on security education, training and awareness (SETA) programme. It should be noted that some authors do not agree with considering education and training as security awareness [1]. These guidelines are presented in four sections, each of which corresponds to a step in the PDCA cycle. Then, we discuss the future of SETA programmes and security awareness. Finaly we conclude.

2. Plan the SETA programme

Planning the SETA programme is important to avoid pitfalls. Article L4121-2 of French Labour Code [7] provides guidelines on how to approach prevention in general: "Plan prevention by integrating, in a coherent whole, technique, work organisation, working conditions, social relations and the influence of environmental factors." In other words, when designing a SETA programme, the context must be taken into consideration. This statement is consistent with [8] which states that prevention and response paradigms in security should go hand by hand. The response paradigm, in information system security, encompasses all the techniques, tools and protocols to manage an incident and this is a part of the context in which the SETA programme will be used. The role of SETA programmes can be defined as the mitigation of risks coming from the user that cannot be avoided. A SETA programme is designed to make people adopt safer behaviour than they had. This means that people will still make mistakes, but if we are successful, they will make fewer. The most effective way to change security behaviours is to make people adopt a security culture [9]. To adopt a new culture, it is advised to generate an intrinsic motivation [10]. In other words, SETA programmes should increase empowerment. A SETA programme designed to generate intrinsic motivation is more likely to be successful over a long period of time. Because SETA programme is part of a continuous process, it is important to work with what we already have. In order not to start from scratch, we need to assess all the tools available and currently used to raise security awareness. Once the assessment is complete, we need to decide how to run the programme.

First, we need to understand who is the source of the message [9]. Depending on their hierarchical level, the programme will not have the same degree of complexity. For example, if the message is from executives, the objective will be to teach non-technical ideas, for example *how to have good digital hygiene?* As executives have less understanding of the production environment than team leaders, their messages should not be about technical matters. It is the role of the team leaders to translate the non-technical messages into technical messages that are relevant to what their team is facing. For example, the team leader can turn the previous non-technical message into *How use the shared mailbox to safely?* If executives try to impose technical topics or if team-leaders try to convey non-technical messages, this will lead to interference and a SETA programme poorly run.

Secondly, we must understand how we want to communicate. There are two forms of communication that the SETA programme should adopt [10][3]:

- *Persuasive communication/education:* it answers the question "why" in the user's mind. It should increase people's insight and motivation.

- *Active participation/training:* it answers the question "how" in the user's mind. It should develop skills and competence.

Both are equally important; people will not be satisfied if the only reason given for improving security is "just do it" and they cannot do anything if they do not know how. A good programme is a combination of active training and persuasive communication [10] There are five themes to conduct a security awareness campaign [11].

- *Deterrence messages* associate sanction to a bad action. This assumes that people are rational and will choose the best option for them, which will not be the one with the expected penalty. Empirical evidence that SETA programmes are suitable for deterrence messages can be found in [12]. This finding is confirmed by the literature review [13]. Deterrence messages can also be considered in the literature as fear messages. Fear is one of the most used messages in the industry. For example, the ANSSI, the French information systems security agency, has asked information systems security managers to stop scaring people [14].
- *Morality messages* attempt to evoke our own moral principles to avoid bad decisions. Empirical evidence that moral reasoning has an impact on security behaviour can be found in [15]. The authors also argue that appropriate punishment activities are important for moral reasoning to be effective. Punishment activities obviously cannot be carried out during a SETA programme.
- *Regret messages* assume that people can anticipate the emotional consequences of their choices before making a decision. This anticipation would encourage people to make the right choice. Empirical evidence of the positive effect of regret on security behaviour is found in [16] but is not distinguished from deterrence or morality. Regret is theoretically a lever to influence behaviour but no significant evidence is found in [17].
- *Incentive messages* assume that giving rewards for doing the right thing helps people improve. This can be seen as the opposite of regret messages. Empirical studies show that rewards for compliance with security policies and procedures are not associated with the individual's perceived mandatoriness of the established set of policies and procedures [18] or with actual compliance [19]. A survey also concludes that rewards do not directly influence security behaviour [13]. However, [20] finds theoretical evidence of positive effects on security behaviour and [16] finds empirical evidence that the incentive has a positive effect. Financial rewards also have a positive effect on security behaviour according to [21].
- *Feedback messages* assume that people will change their behaviour if they receive feedback on their actions, this can be positive or negative reinforcement. In [22], West explains that classical feedback mechanisms do not work in information systems security; the consequence of a bad action is often delayed, and the consequence of a good one is to not be under attack, in other words nothing happen. Reinforcement learning is therefore not effective.

Finally, a SETA programme should be audience-specific. Unfortunately, little work has been done to study the relationship between public types and other factors, such as the theme of a SETA programme. However, one paper finds that there might be a correlation between

personality traits and the effectiveness of a theme [11]. The most relevant advice found regarding the public is to divide the population by groups of interest. This recommendation is found several times in the literature, whatever the date of publication of the study. [23][24][3].

The plan step does not have much room for automation because most of the work is about making decision about how to run the program. These choices must be made by humans. However, if the SETA programmes are carefully done and documented at each iteration, the assessment could be partially automated considering all information is already available.

Summary To plan a SETA programme we should assess available resources, understand who is the source of the message and which theme we will use to communicate. It should be noted that each programme is specific to its context but there is not many ressources on this subject. Automation is not an option at this step, but some time could be saved during the assessment step by having a good knowledge management.

3. Do the SETA programme

There are many different media for conveying a SETA programme and choosing the right one is an important decision. The choice of media depends on multiple factors:

- *The population we are targeting:* as mentioned in the previous section, there is little literature about developing a SETA programme for a specific population.
- *The why or the how:* some media are more suited for persuasive communication, and others for active participation. [3] lists the possible media according to the question they answer.
- *The price:* [3] details which media are cheap and which are expensive.

As mentioned in the previous section, we need to use media that allow us to answer the question of how (active training) and why (persuasive communication). There are other factors that can be taken into consideration, but they are not as important as the previous ones: (i) Is the medium suitable for multi-messaging? (ii) will the medium allow your message to be self-disseminated? You can find these secondary characteristics by media in [3].

Catch The Flag (an event where security enthusiasts have to find as many "flags" possible. The "flags" are secrets hidden in softwares, hardwares or intentionally vulnerable websites) and other types of competitions used for information systems security training are not suitable media for SETA programmes. These exercises ([25] for a list of examples) are intended to improve specific information systems security skills, which is not the purpose of a SETA programme. Our goal is to make users adopt safer behaviour.

It is well known that gamification helps to learn and remember. Consequently, the programme should be as gamified as possible. Our programme will be more attractive and the audience will be larger. In addition, people will remember the message more easily.

At this stage, we may have selected several media for our programme. If we have a choice of media and cannot use all of them in our campaign, we should focus the media that best suits our needs taking into account these four features [3]:

- *Ease of use:* How easy is it to access, deploy, update and maintain the SETA programme?

- *Scalability:* Can the material be used for different sized audiences and in different locations?
- *Support:* Will support for the programme be internal or external ? Is it easy to find help to use the material?
- *Accountability:* What statistics can be used to measure the effectiveness of the programme ? How comprehensive are these measures?

Finally, we will have to focus on the governance part. In order to have as little impact as possible on production, we should communicate the plan to all stakeholders [13][3]. This means the people we are training, but also their immediate superior and other people they work with who are not involved in the programme. During the session, the trainees will not be able to maintain production; everyone working with them must be prepared for the consequences. In addtion the SETA programme should be organised in short sessions [24]. Providing social interactions during a session increases the effectiveness of the SETA programme [13][26][9]. The direct implication of this is that e-learning and other MOOCS are not relevant. At the end of the programme, giving goodies is a good way to spread our message and reinforce the commitment [24]. When we carry out the programme, the most important thing is the public's willingness to participate [26]. In his literature review on the place of human element in information systems security, Dhillon et al. [27] mention that user empowerment is a strong lever to increase security awareness.

During this step, automation is not an option because of the trainees' need for social interaction. In addition the creation of the media needs creativity and this is something difficult to automate. Using use cases and frameworks could be a way to reduce the need for creativity. The only part that could be automated is the communication to the coworkers, warning that one member of their team is attending an awareness campaign.

Summary For the awareness campaign to be effective, it should be a combination of both active training and persuasive education. The media of the campaign must be chosen in consequence. The choice of the media also depends on factors like the population we are aiming for and the budget we have. Awareness campaigns must always provide social interaction for the attendees. Attendees' coworkers should be warned that attendees will not be available to maintain production. The warning process must be automated.

4. Check the SETA programme

The check step is important for the continuous improvement of the SETA programme. In order to evaluate our programme, we will need to collect data. They can be feedback, questionnaires or notes taken during the session. We can distinguish three types of evaluation:

- *Measure of behavioural intention:* This is the most represented type of evaluation in the literature. It posits that actual system, method or tool use can be estimated using many other measures, and that the behavioural intention to use is a good estimator of actual usage. For example, if we run a campaign to promote password managers, the higher the user's intention to use them, the more successful the campaign is.

Table 1
Frequency of Special Characters

Evaluation method	References
Measure of behavioural intention	[28][29][30]*[31]
Knowledge test	[32][33][34]
Ulterior incident rate	[3]

* is a literature review about behavioural intention in information systems security.

- *Knowledge oriented:* People who have less understanding of security concepts are more likely to be victims of an attack. Therefore, assessing the knowledge gained after the SETA programme can be an indicator of the effectiveness of the programme.
- *Ulterior incident rate:* This method consists of measuring the incident rate ulterior to the campaign. For example, if we run a campaign against bad password management and the rate of incidents related to bad password management decreases after the campaign, we can consider the campaign successful.

Khan et al. [26] identify that information systems security awareness lags behind other domains such as ecological or public health awareness. They propose to imitate techniques from other fields to improve information systems security awareness. For example, in public health, a reference model is the EPPM (Extended Parallel Process Model) [35][36]. This model works well with messages fear-based (deterrence messages), which are effective for SETA programmes. A model of this type could be useful in information security awareness. This model also has the advantage of explaining why some campaigns may backfire.

Whatever solution we choose to evaluate our programme, we need to think about automating the evaluation [3][33]. Some SETA programmes can be huge; the process of collecting the data and then interpreting it can be time consuming. Obviously, some types of data are better suited for automation than others. For example, if you are collecting only hand notes of the session this will be much harder to automate than analysing online questionnaires filled by the participants.

Summary At this step, we need to choose a way to evaluate our programme. As the SETA programme will grow, it will be harder to evaluate it without automation. Some evaluation methods are most suited for automation than others; this should be taken into consideration when choosing the method to evaluate our programme.

5. Adjust the SETA programme

The real added value of PDCA applied to SETA programmes is at this step. The adjust step will permit designing a better future iteration; the next campaign will be easier to start. By using PDCA, we prevent flows from occurring in our SETA programmes in the first place, or once they do, we stop them from continuing.

We can subdivide the adjust step in three other steps. They should be done in that exact order.

1. Take a look back at the campaign. The feedback collected can help to improve the way the SETA programme is run. [37] provides guidelines for making information systems security more user-friendly. These guidelines are relevant to a SETA programme and can be used to improve it. In addition, see if we avoided common pitfalls. Awareness campaigns often fail for the same reasons according to [38].
2. By collecting feedback we should have a better understanding of the needs of the public. We should adapt the environment to the new needs identified during the programme. As said in section 2, prevention is there to mitigate risks that cannot be avoided. With the feedback collected, it is an opportunity to avoid new risks.
3. Finally, is the campaign consistent with the new policies and environment? The IT environment is an ever-evolving place, it is important to check if the messages provided are not obsolete. If so, we will need to update them or add new ones if we have new technology in our environment.

Data visualisation is the key to automate this step. While the final decision will be human, we can save some time by presenting all the input (the information gathered during the plan step), output (the metrics collected during the check step) and other data of our campaign in an efficient way. Humans have many biases and it is difficult to process statistics; data visualisation is the solution to reduce errors and save some time, leading to flexible automation.

Once we have our improved programme, we should consider launching a new campaign. This cycle is the single-loop learning of the prevention paradigm described in [8]. Since we are considering SETA programme as a continuous process, a new campaign should be launched regularly.

Summary The improvement process of the SETA programme could be divided in three steps: did our SETA programme avoid common traps and what are the feedback on our program? Could we avoid new risks given the information collected during the programme? Finally is the campaign consistent with the new policies and environment? With a good data visualisation of all the data and metrics collected during the programme, we can reduce improvement errors and save some time, leading to flexible automation. A new campaign must be planned at the end of the previous one.

6. Discussion

Prevention is an important aspect of security and helps reduce the number of security events. In addition, the more users have a better understanding of information system security, the less detection systems used in the industry, like intrusion detection systems or security information management systems, will have false positive due to the drop of users misuses and errors.

While many tools in information system security are automated, non-technical security measures are exceptions to this rule. The PDCA cycle permits automating the running process of SETA programmes. This kind of automation remains very flexible, which is very needed in security. The full automation of a SETA programme is impossible due to the need for social interaction to make awareness campaigns effective and the complexity of the task. Therefore,

flexible automation for SETA programmes may be a solution toward automation of non-technical security measures without making compromise on their effectiveness.

We believe this work can help information system security actors to design better prevention programmes but not only. This work can also be used by researchers who want to study the various topics related to prevention. They can find in this paper guidelines to create effective programmes to convey messages, leading to more efficient prevention campaign and more significant results.

Finally, prevention is one of three main principles used to fight epidemic threats at Internet scale like worms [39]. We made this work with fighting those kinds of threats in mind. With a detection system that detects epidemic threats soon enough, we can then create effective SETA programmes and stop, or at least lower, the impact of those attacks.

7. Conclusion

Security awareness is a major concern. Despite this, there is very little work done to understand how to create good awareness campaigns. The theme of deterrence is dominant in security awareness, probably because of the relationship between information systems security and criminology.

Another problem with current security awareness is the lack of datasets. Many models have been compared to find which one that best explains the behaviour of the studied population, but none of them were compared with the same dataset. As a result, it is difficult to conclude that one model is better or worse than any other.

SETA programmes are useful tools for improving security awareness. They should be considered as a part of a security culture. However, there is a lack of methodology on how to implement them in the state of the art. This is the problem we try to address in this paper. By reviewing the literature, we identify guidelines for designing a SETA programme following a PDCA cycle. The application of PDCA to SETA programmes is a way to partially automate the SETA programme and to give prescriptive recommendations.

References

[1] A. Tsohou, S. Kokolakis, M. Karyda, E. Kiountouzis, Investigating Information Security Awareness: Research and Practice Gaps, Information Security Journal: A Global Perspective 17 (2008) 207–227. URL: https://doi.org/10.1080/19393550802492487. doi:10.1080/19393550802492487.

[2] M. G. Lee, Securing the human to protect the system: human factors in cyber security, Stevenage, UK, 2012, pp. 4A1–. doi:10.1049/cp.2012.1519.

[3] M. Wilson, J. Hash, Building an Information Technology Security Awareness and Training Program, Technical Report, 2003. URL: https://csrc.nist.gov/publications/detail/sp/800-50/final. doi:10.6028/NIST.SP.800-50.

[4] ISO, Iso 27000 framework, 2018. URL: https://www.iso.org/standard/73906.html.

[5] ISACA, Cobit framework, 2019. URL: https://www.isaca.org/resources/cobit.

[6] Y. Barlette, V. V. Fomin, The Adoption of Information Security Management Standards: A Literature Review, IGI Global, 2010, pp. 69–90. URL: www.igi-global.com/chapter/information-resources-management/54471. doi:10.4018/978-1-61520-965-1.ch104.

[7] Legifrance2016, Article l4121-2, 2016. URL: https://www.legifrance.gouv.fr/codes/section_lc/LE\GITEXT000006072050/LEGISCTA000006160774/.

[8] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prevention and response, Information & Management 51 (2014) 138–151. URL: http://www.sciencedirect.com/science/article/pii/S0378720613001171. doi:10.1016/j.im.2013.11.004.

[9] R. von Solms, B. von Solms, From policies to culture, Computers & Security 23 (2004) 275–279. URL: http://www.sciencedirect.com/science/article/pii/S0167404804000331. doi:10.1016/j.cose.2004.01.013.

[10] M. T. Siponen, A conceptual foundation for organizational information security awareness, Information Management & Computer Security 8 (2000) 31–41. URL: https://doi.org/10.1108/09685220010371394. doi:10.1108/09685220010371394.

[11] M. Kajzer, J. D'Arcy, C. R. Crowell, A. Striegel, D. Van Bruggen, An exploratory investigation of message-person congruence in information security awareness campaigns, Computers & Security 43 (2014) 64–76. URL: http://www.sciencedirect.com/science/article/pii/S0167404814000327. doi:10.1016/j.cose.2014.03.003.

[12] J. D'Arcy, A. Hovav, D. Galletta, User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research 20 (2009) 79–98. URL: https://doi.org/10.1287/isre.1070.0160. doi:10.1287/isre.1070.0160.

[13] S. Abraham, Information Security Behavior: Factors and Research Directions., in: AMCIS, volume Proceedings - All Submissions, 2011, p. 462. URL: https://aisel.aisnet.org/amcis2011_submissions/462.

[14] L. M. Informatique, L'anssi demande aux rssi de ne plus faire peur, 2016. URL: https://www.lemondeinformatique.fr/actualites/lire-assises-de-la-securite-2019-l-anssi-demande-aux-rssi-de-ne-plus-faire-peur-76715.html.

[15] L. Myyry, M. Siponen, S. Pahnila, T. Vartiainen, A. Vance, What levels of moral reasoning and values explain adherence to information security rules? An empirical study, European Journal of Information Systems 18 (2009) 126–139. URL: https://doi.org/10.1057/ejis.2009.10. doi:10.1057/ejis.2009.10.

[16] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly 34 (2010) 523–548. URL: https://www.jstor.org/stable/25750690. doi:10.2307/25750690.

[17] C. Wright, P. Ayton, Focusing on what might happen and how it could feel: can the anticipation of regret change students' computing-related choices?, International Journal of Human-Computer Studies 62 (2005) 759–783. URL: https://www.sciencedirect.com/science/article/pii/S1071581905000327. doi:10.1016/j.ijhcs.2005.03.001.

[18] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler, R. W. Boss, If someone is watching,

I'll do what I'm asked: mandatoriness, control, and information security, European Journal of Information Systems 18 (2009) 151–164. URL: https://doi.org/10.1057/ejis.2009.8. doi:10.1057/ejis.2009.8.

[19] S. Pahnila, M. Siponen, A. Mahmood, Employees' Behavior towards IS Security Policy Compliance, IEEE, 2007, pp. 156b–156b. doi:10.1109/HICSS.2007.206.

[20] T. August, T. I. Tunca, Network Software Security and User Incentives, Management Science 52 (2006) 1703–1720. URL: https://www.jstor.org/stable/20110643.

[21] S. Goel, K. J. Williams, J. Huang, M. Warkentin, Can Financial Incentives Help with the Struggle for Security Policy Compliance?, Information & management (2021) 103447–. doi:10.1016/j.im.2021.103447.

[22] R. West, The psychology of security, Commun ACM (2008) 34–40.

[23] S. Bauer, E. W. N. Bernroider, K. Chudzikowski, Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks, Computers & Security 68 (2017) 145–159. URL: http://www.sciencedirect.com/science/article/pii/S0167404817300871. doi:10.1016/j.cose.2017.04.009.

[24] M. Thomson, R. von Solms, Information security awareness: educating your users effectively, Information Management & Computer Security 6 (1998) 167–173. URL: https://doi.org/10.1108/09685229810227649. doi:10.1108/09685229810227649.

[25] L. J. Hoffman, T. Rosenberg, R. Dodge, D. Ragsdale, Exploring a national cybersecurity exercise for universities, IEEE Security Privacy 3 (2005) 27–33. doi:10.1109/MSP.2005.120.

[26] B. Khan, K. S. Alghathbar, M. K. Khan, Information Security Awareness Campaign: An Alternate Approach, in: T.-h. Kim, H. Adeli, R. J. Robles, M. Balitanas (Eds.), Information Security and Assurance, Communications in Computer and Information Science, Springer, Berlin, Heidelberg, 2011, pp. 1–10. doi:10.1007/978-3-642-23141-4_1.

[27] G. Dhillon, J. Backhouse, Current directions in IS security research: towards socio-organizational perspectives, Information Systems Journal 11 (2001) 127–153. URL: https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2575.2001.00099.x. doi:https://doi.org/10.1046/j.1365-2575.2001.00099.x.

[28] D.-L. Huang, P.-L. Patrick Rau, G. Salvendy, F. Gao, J. Zhou, Factors affecting perception of information security and their impacts on IT adoption and security practices, International Journal of Human-Computer Studies 69 (2011) 870–883. URL: http://www.sciencedirect.com/science/article/pii/S1071581911001029. doi:10.1016/j.ijhcs.2011.07.007.

[29] A. C. Johnston, M. Warkentin, Fear Appeals and Information Security Behaviors: An Empirical Study, MIS Quarterly 34 (2010) 549–566. URL: https://www.jstor.org/stable/25750691. doi:10.2307/25750691.

[30] B. Lebek, J. Uffen, M. Neumann, B. Hohler, M. H. Breitner, Information security awareness and behavior: a theory-based literature review, Management Research Review 37 (2014) 1049–1092. URL: https://doi.org/10.1108/MRR-04-2013-0085. doi:10.1108/MRR-04-2013-0085.

[31] J. Shropshire, M. Warkentin, S. Sharma, Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, Computers & Security 49 (2015) 177–191. URL: http://www.sciencedirect.com/science/article/pii/S0167404815000036. doi:10.1016/

j.cose.2015.01.002.

[32] L. Drevin, H. Kruger, A.-M. Bell, T. Steyn, A Linguistic Approach to Information Security Awareness Education in a Healthcare Environment, in: M. Bishop, L. Futcher, N. Miloslavskaya, M. Theocharidou (Eds.), Information Security Education for a Global Digital Society, IFIP Advances in Information and Communication Technology, Springer International Publishing, Cham, 2017, pp. 87–97. doi:10.1007/978-3-319-58553-6_8.

[33] H. A. Kruger, W. D. Kearney, A prototype for assessing information security awareness, Computers & Security 25 (2006) 289–296. URL: http://www.sciencedirect.com/science/article/pii/S0167404806000563. doi:10.1016/j.cose.2006.02.008.

[34] H. Kruger, L. Drevin, T. Steyn, A vocabulary test to assess information security awareness, Information Management & Computer Security 18 (2010) 316–327. URL: https://doi.org/10.1108/09685221011095236. doi:10.1108/09685221011095236.

[35] K. Witte, Putting the fear back into fear appeals: The extended parallel process model, Communication Monographs 59 (1992) 329–349. doi:10.1080/03637759209376276.

[36] K. Witte, Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale, Journal of Health Communication 1 (1996) 317–342. URL: https://doi.org/10.1080/108107396127988. doi:10.1080/108107396127988.

[37] J. R. C. Nurse, S. Creese, M. Goldsmith, K. Lamberts, Guidelines for usable cybersecurity: Past and present, in: 2011 Third International Workshop on Cyberspace Safety and Security (CSS), 2011, pp. 21–26. doi:10.1109/CSS.2011.6058566.

[38] M. Bada, A. M. Sasse, J. R. C. Nurse, Cyber Security Awareness Campaigns: Why do they fail to change behaviour?, arXiv:1901.02672 [cs] (2019). URL: http://arxiv.org/abs/1901.02672, arXiv: 1901.02672.

[39] D. Moore, G. M. Voelker, S. Savage, Quantitative network security analysis, Cooperative Association for Internet Data Analysis (CAIDA), NSF-01-160 7 (2002).