Play the Game!
Analogue Gamification for Raising Information Security Awareness

Margit SCHOLL
Department Business, Computing, Law, Technical University of Applied Sciences (TUAS) Wildau
Wildau, Brandenburg 15745, Germany
margit.scholl@th-wildau.de

ABSTRACT

Government digital agendas worldwide want to help develop the digital transformation in businesses and public administrations, while acknowledging the digital changes taking place in society and the need to integrate information security (IS). Although information communication technology (ICT) shapes our lives, we tend to have an insufficient knowledge of the risks involved, of information security (IS), and of the General Data Protection Regulation (GDPR); this is compounded by carelessness in handling data and insufficient IS awareness (ISA). Backed by a clear conceptual approach, information security awareness trainings (ISAT) are also essential for everyone. However, classical trainings are not currently working. Psychologically based research shows that a systemic approach might be helpful. This is where analogue game-based learning (GBL) comes into play.

Keywords: Digitization, ICT, IS, GDPR, ISA, ISAT, GBL, security sensitization.

1. INTRODUCTION

Modernization in our society and a more dynamic way of working is inconceivable without the use of the latest digital information communication technology (ICT) systems. An ICT system is an ensemble of hardware, software, networks, and all the design and qualification processes involved in work and organization (GI, 2015: 9). However, ICT and digitization increasingly permeate all aspects of today's society. The societal impacts of modern ICT include the digital divide, altered work structures in institutions, the rationalization and creation of new jobs, changed communication and social behavior, the emergence of virtual communities, etc. (GI, 2015: 8). The digital agendas of governments around the world want to lay the foundations for digital transformation (DT) and ensure added value for their countries. The European Digital Agenda (BMWi, 2014) is seeking to keep abreast of digital networking and the digital changes in society. However, as the German Informatics Society (GI) points out in article 7 of its "Ethical Guidelines," the design and implementation of ICT systems, including any control and monitoring techniques, should be combined with user involvement (GI, 2015: 6).

The next section briefly summarizes the main scientific knowledge about the human side of IS and information security awareness trainings (ISAT) as well as some of the ethical responsibilities in informatics. Because Serious Games have great potential in the field of ISAT, section 3 discusses several examples of analogue game-based learning scenarios for practice. Section 4 gives the conclusions generated by the previous findings.

2. HUMAN SIDE OF INFORMATION SECURITY AND ETHICS

According to the BSI, information security awareness (ISA) should address the following threats and vulnerabilities (BSI, 2016): insufficient knowledge of regulations, insufficient ISA, and carelessness in handling information. Tsohou et al. (2012) conclude from recent global security surveys that ISAT are not currently working. One reason might be a "technocratic" view of risk communication, meaning the tendency for technical experts to tell people what they think and ought to know (Steward and Lacey, 2012). A second reason might be policies "ending up as long lists of dos and don'ts located on web pages most employees only access when they have to complete their mandatory annual 'security training' and which has little to no effect on their security behavior" (Kirlappos et al., 2013). And a third reason is that a training aimed at addressing security awareness gaps is not sufficient to ensure compliance with a security culture (Fagade and Tryfonas, 2016).

Psychological research shows that in addition to the classical theoretical approach to knowledge transfer and the marketing-oriented approach of emotionalization, a systemic approach to team-based communication is needed (Pokoyski, 2009; Khan et al., 2011; Beyer et al., 2016). Scholl et al. (2016) point out that ISATs need a "methodology 3.0": social participation in a communicative team process is a key component in this third stage of emotionally based awareness-raising activities. This is because IS and IT are about more than just technology (Kruger et al., 2007). ICT systems involve human actors, and users do not always behave the way they are supposed to (Aytes and Terry, 2004). The adverse characterization of people in the field of IS (Scholl et al., 2018) has now been rethought, because there are fundamental strategic IS deficits in institutions themselves.

Politics and informatics have ethical responsibilities with regard to DT. For example, members of the GI are expected to expand their expertise to understand the rights and interests of the various stakeholders (GI, 2015: 4). This also includes the readiness to take part in interdisciplinary discussions (GI, 2015: 4). According to article 8, members of the GI who teach computer science should also instruct learners about their individual and shared responsibility, while at the same time serving as role models (GI, 2015: 6). Acting together needs both individual and group reflection (GI, 2015: 14).

3. ANALOGUE GAMIFICATION FOR A DIGITALLY BASED LIFE

ISA learning methods should clarify threats, vulnerabilities, attacks, and possible damage as well as the main values of IS and data protection. The three basic values are confidentiality, integrity, and availability. Additional values include authentication, commitment, and reliability (BSI, 2016). In many organizations, ISA and the training of relevant competences (ISAT) are often limited to knowledge-transfer measures. Based on psychologically based research (Pokoyski, 2009; Helisch, 2009; Hauke and Pokoyski, 2018) on creating lasting sensitization and promoting security-related behaviors Albrechtsen, 2007; Helisch, 2009; Khan et al., 2011), the game-based learning (GBL) methodology is becoming more important for ISA. The so-called "3.0 Systemic Approaches" of Scholl et al. (2016) were implemented and tested at the Technical University of Applied Sciences (TUAS) Wildau (Fuhrmann et al., 2017). Major campaigns for large companies like T-Systems, Alliance, BMW, and HP were also completed with an analogue "Security Parcours" (https://web.eco.de/news/unterwegs-auf-dem-security-parcours/) or individually organized, as was the case with Deutsche Post (TAKE AWARE, 2018).

Serious Games have great potential to make valuable contributions to socially relevant areas such as education, health, and society (Göbel, 2017; Institute of Play, 2015). For this reason, game-based learning is receiving increasing recognition as an effective teaching and learning method that improves motivation and triggers behavioral changes (Bösche and Kattner, 2011). Emotionalizing must address people's specific concerns. Psychological studies (Hauke and Pokoyski, 2018) show that people need to "understand"—through emotional engagement—that they are themselves affected. Analogue GBL is especially effective as a means of stimulating motivation and should be explicitly used for ISAT, because learners can directly see the consequences of their actions and get a sense of their knowledge level in dialogue.

Adapted, analogue GBL scenarios in the English-speaking "Security Arena" are part of the final results of the project "SecAware4job" (Fuhrmann et al., 2017). The serious games can be purchased through our Cologne-based project and cooperation partner known_sense. The themes of the learning scenarios are listed below and complemented with learning tasks and goals (see table 1).

Learning scenario	Learning task	Learning goals
Clear Desk	Identify which items and information on the desk should be securely locked	Create awareness of a tidy work space and importance of safeguarding sensitive information
Data Security	Assemble phrases from two parts	Repeat and deepen knowledge
Internet Services	Assess the sample services and apps for eight risks	Know and discuss the risks of common Internet and App services
Phishing	Recognize phishing emails	Explain criteria for detecting phishing emails
Security on the Go	Identify typical hazard scenarios in public space and assign appropriate protective measures	Identify safeguards for IS in public space and while traveling
Social Media	Recognize critical published images and information on social networks	Create awareness of safe behavior on social networks
Password Hacking	Guess passwords for a fictitious Facebook profile	Generate sensitivity to secure passwords and knowledge about hash values
Network Domino	Use game elements to lay out network architectures that meet the given requirements for security and functionality	Deepen knowledge of the operation of network components and sensible secure organization (infrastructure)
Incident Management	Cluster information security, privacy, and compliance incidents and assign to hotlines	Get to know sample IS, privacy, and compliance incidents, and relevant reporting points
Social Engineering	Recognize the exploitation of human traits (social barriers) such as helpfulness and curiosity	Create awareness of the techniques of social engineering and social gateways

Table 1: Analogue GBL scenarios of the "Security Arena" from the TUAS Wildau project "SecAware4job" (Fuhrmann et al., 2017; Scholl, 2018)

The research project SecAware4job sets out to develop and examine as many creative learning and teaching methods as possible to enable students, employees, and guests to more easily understand the complex of information security with all its facets (regulatory framework, norms and standards, protective measures, concepts, etc.) and make this issue more visual. The applied methodological framework is a learning station format (*Stationenlernen*) that goes back to circuit training in sports. It is enhanced by elements of other learning methodologies such as game-based learning (GBL), blended learning, and authentic learning (Fuhrmann et al., 2017).

Fig. 1 Security Arena Game "Security on the Go," developed by known_sense, adapted for the TUAS Wildau, played by students, employees, guests, and pupils. © TUAS Wildau & known_sense

Each learning station is presented in a playful manner and consists of a five-minute introduction to a special topic (for

example, “security on the go” in public spaces) that also integrates a dialogue between participants. There follows a phase of authentic learning in which the participants as a team solve real problems from everyday (professional) life. The teams of about ten people each receive points and discuss the solution, enabling immediate learning within a maximum of five minutes. All in all, one learning station needs approximately fifteen minutes. Playing four stations in parallel as a competition, it takes only one hour to sensitize about forty people. The completion of the learning stations is the prelude to addressing a topic in greater depth, involving as many interactive methods as possible. By way of repetition, these analogue learning stations can be complemented by digital learning games in blended learning formats.

In the following, three game examples are described in more detail. The first game is “Security on the Go” (see fig. 1). The game consists of an infographic map as a playing area. It is played in two rounds. The first round includes 14 risk cards in orange that describe the various security risk scenarios shown on the map, with players asked to assign the cards to the appropriate situation shown. In the second round 14 defense cards in blue must be correctly matched with the orange card. The following questions might potentially be used to help engage people in team discussions and activities and generate interactive play:

- How do I perceive the behavior of my fellow passengers with regard to cell phone use?
- How can I obtain products for encrypting information?
- What does the term “shoulder surfing” mean?

The second game is “Social Engineering” (see fig. 2), an attack focusing on human beings, which is often not well known. Research shows that social engineers use tricks and manipulation of the so-called six social gateways and bluff people into giving them access to information. The participants in the game have to locate cards—describing real situations concerning the six gateways—on the specific field at the playing area. Some of the cards apply to multiple gateways and map fields—what is important is the interactive discussion and exchange of experiences between all players.

Fig. 2 Security Arena Game “Social Engineering,” developed by known_sense, adapted for the TUAS Wildau, played by students, employees, guests, and pupils. © TUAS Wildau & known_sense

The third game is “Social Media” (see fig. 3). Here the underlying idea is that the Internet does not forget, which prompts such questions as “Should I post this picture or not?” “Should I post this text or not?” In the discussion the people need to demonstrate their knowledge of social media and the relevant laws and regulations.

Fig. 3 Security Arena Game “Social Media”, developed by known_sense, adapted for the TUAS Wildau, played by students, employees, guests, and pupils. © TUAS Wildau & known_sense

4. CONCLUSION

The aim of this paper is to explain concepts for analogue GBL scenarios. Designing ISAT with analogue scenarios, emotionalization, and team-based exchange—as mentioned above—is extremely important for the motivation and successful sensitization of human actors in the field of IS. Depth psychological studies show that emotionalizing and motivation are important factors in creating short-term scenarios in real-life situations using authentic learning (AL) and problem-based learning (PBL). Our own extensive experience with such learning materials and methods in projects and events suggests that ISA and the knowledge associated with it could be improved in almost all participants, and behavioral changes triggered.

As a supplement, completion and deepening of the analogue learning scenarios we also have developed and programmed eight digital game-based learning scenarios (see fig. 4)—available only in German. These digital scenarios are listed at the project website and can be used at no charge. However, digital GBL scenarios are not the focus of this paper.

Fig. 2 Digital web-based serious games developed by the project team “SecAware4job”. © TUAS Wildau
See project website: http://secaware4job.wildau.biz/#lernszenarien

Analogue and digital serious games should be used in combination to raise IS. As part of our ongoing research projects, we will perform a systematic evaluation with both GBL methodologies to get more durable results. Nevertheless, there is no simple linear cause-and-effect relationship between institutional safeguards and knowledge, attitudes, and real behavior. ISA remains a critical issue. Therefore, ISAT and programs must be developed with a user-centered approach. Moreover, a clear set of IS principles needs to be identified and communicated (Kirlappos et al., 2013). Learning in IS should be developed by integrating target-oriented, interactive analogue/digital GBL scenarios and team-oriented methods as an ongoing process.

Games of the Security Arena can be bought via our project partner, the Cologne company known_sense: http://www.known-sense.de. Further research projects with and for universities, educational institutions, companies, and/or public administrations are requested by the TUAS Wildau and can be arranged with Professor Scholl: https://www.th-wildau.de/scholl.

References

[1] Albrechtsen, E. (2007), "A qualitative study of users' view on information security," **Computers & Security**, 26, pp. 276–289.

[2] Aytes, K., and Terry, C. (2004), "Computer security and risky computing practices: A rational choice perspective," **Journal of Organizational and End User Computing**, 16, pp. 22–40.

[3] Bundesministerium für Wirtschaft und Energie (BMWi)/Federal Ministry of Economics and Energy (2014), "International Dimension: EU – Digital Agenda," Bonn. Available from: http://www.bmwi.de/Redaktion/EN/Dossier/digitisation.html (accessed: 2017-05-29).

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security (2016), "ORP.3: Sensibilisierung und Schulung/Sensitization and training." Bonn. Available from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html (accessed: 2018-01-17).

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security (2008), "BSI-Standard 100-1. Information Security Management System." Version 1.5. Bonn. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.html (accessed: 2018-01-20).

[6] Bösche, W., and Kattner, F. (2011), "Fear of (serious) digital games and game-based learning? Causes, consequences and a possible countermeasure," **International Journal of Game-Based Learning**, 1(3), pp. 1–15.

[7] DSV-Gruppe, EnBW, <kes>, known_sense, nextsolutions, Pallas (editors) (2006), "Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen." Cologne & Munich. Available from: http://known-sense.de/de/Produkte/Security_Studien_2/ (accessed: 2018-03-06).

[8] Fagade, T., and Tryfonas, T. (2016), "Security by compliance? A study of insider threat implications for Nigerian banks," in Tryfonas, T. (ed.), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2016, Lecture Notes in Computer Science, vol. 9750, Cham: Springer, pp. 128–139.

[9] Fuhrmann, F., Scholl, M.C., Edich, D., Koppatz, P., Scholl, L.R., Leiner, K.B., and Ehrlich, E.P. (2017), **Informationssicherheitsbewusstsein für den Berufseinstieg.** Abschlussbericht Projekt SecAware4job. Aachen: Shaker, DOI: 10.2370/9783844054668. Available from: http://secaware4job.wildau.biz (accessed: 2018-01-20).

[10] Gesellschaft für Informatik e.V. (GI)/The society for computer science (2015), "Unsere Etischen Leitlinien," Berlin, version 07/2015.

[11] Göbel, S. (2017), "Autorenumgebung für Serious Games-StoryTec: Eine Autorenumgebung und narrative Objekte für personalisierte Serious Games," TU Darmstadt, Dissertation.

[12] Haucke, A., and Pokoyski, D. (2018), "Mea culpa – Schuld, Scham und Opferrolle bei Social Engineering," **kes** 1, pp. 6-8

[13] Helisch, M., and Pokoyski, D. (eds.) (2009), **Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung**, Wiesbaden: Vieweg+Teubner.

[14] Institute of Play (2015), "Q Design Pack School." Retrieved from http://www.instituteofplay.org/wp-content/uploads/2013/09/IOP_QDesignPack_School_1.0.pdf (accessed: March 3, 2016).

[15] Khan, B., Alghathbar, K.S., Nabi, S.I., and Khan, M.K. (2011), "Effectiveness of information security awareness methods based on psychological theories," **African Journal of Business Management**, 5(26), pp 10862–10868.

[16] Kirlappos, I., Beautement, A., and Sasse, M.A. (2013), "'Comply or die' is dead: Long live security-aware principal agents," in Adams, A.A., Brenner, M., and Smith, M. (eds.), **Financial Cryptography and Data Security**, Lecture Notes in Computer Science. vol. 7862. Heidelberg: Springer, pp70-82.

[17] Kruger, H., Drevin, L., and Steyn, T. (2007), "Email security awareness: A practical assessment of employee behavior," in Futcher, L., and Dodge, R. (eds.), **Fifth World Conference on Information Security Education, IFIP** – International Federation for Information Processing, vol. 237. Boston, MA: Springer, pp. 33–40.

[18] Pokoyski, D. (2009), "Security Awareness: Von der Oldschool in die Next Generation – eine Einführung, in Helisch, M., and Pokoyski, D. (eds.), **Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung**, Wiesbaden: Vieweg+Teubner, pp. 1–8.

[19] Scholl, M. (2018 in press), "Information Security Awareness in Public Administrations," in Comite, U., **Public Management and Administration**, Open Access: INTECH d.d.o. Rijeka (InTechOpen).

[20] Scholl, M., Fuhrmann, F., and Scholl, L.R. (2018), "Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices," in **Proceedings of the 51th Hawaii International Conference on System Sciences (HICSS)**, Big Island, Hawaii, pp. 2235–2244. Available from: http://hdl.handle.net/10125/50168.

[21] Scholl, M., Fuhrmann, F. and Pokoyski, D. (2016), "Information security awareness 3.0 for job beginners," in Varajão, J.E., Cruz-Cunha, M.M., Martinho, R., Rijo, R., Bjørn-Andersen, N., Turner, R., and Alves, D. (eds.), **Proceedings of the Conference on ENTERprise Information Systems (CENTERIS)**, pp. 433–436.

[22] Stewart, G., and Lacey, D. (2012), "Death by a thousand facts: Criticising the technocratic approach to information security awareness," **Information Management & Computer Security**, 20, pp. 29–38.

[23] Tsohou, A., Karyda, M., Kokalakis, S., and Kiountouzi, E. (2012), "Analyzing trajectories of information security awareness," **Information Technology & People**, 25, pp. 327–335.