NATIONAL UNIVERSITY OF PUBLIC SERVICE
Doctoral School of Public Administration Sciences

Eszter Diána Oroszi

Improving security awareness level of users throug gamification methods

Doctoral (PhD) thesis

THESIS BOOKLET

Supervisor:

Dr. Ferenc Leitold

Budapest, 2023

CONTENT

1. THE AIM OF THE DISSERTATION, ACTUALITY OF THE TOPIC

An organisation's primary line of defence against information security attacks is its employees. As many statistics highlight, exploiting the human factor is a common - and successful - tool for attackers. There is a myriad of techniques for exploiting the human factor, and these methods have been described in detail by international authors and several national experts in their studies, establishing that social engineering methods pose a real threat to organisations. These attack techniques are constantly evolving and new ones are emerging.

Many public organisations around the world rely on digital government services, which increases the information security risks in this sector. Public sector organisations are particularly vulnerable to overload/DoS attacks, website defacement, phishing and malicious code threats, unauthorised access and data leakage and theft, due to their role and operations. International research also confirms that the public sector was one of the sectors most affected by cybersecurity incidents in 2022. This makes it essential to improve the information security of public sector organisations, of which security awareness training for employees is an essential part. All the national laws and standards relevant to information security presented in this thesis require information security education for users.

Reducing the risks posed by the human factor is therefore in the interest of every organisation, and it is essential to increase users' security awareness and sensitise them to the subject by improving and applying appropriate methods. Training methods may have different effectiveness for different organisations and user groups, and it is important to evaluate their effectiveness before use.

Both the literature review and my own experience have confirmed that commonly used educational methods alone are no longer sufficient to effectively improve awareness level of users, as both the techniques of attack and the needs of users have changed a lot over the last 10 years.

For these reasons, I set the goal to investigate which methods can be used to effectively improve users' security awareness level, to acquire a security-aware attitude and to encourage participants to do a security-aware behaviour, in line with nowadays' requirements and current trends. As a potential solution to this problem, I identified the currently popular gamification methods and investigated their applicability to the improvement of security awareness level. I was curious to find out which security awareness solutions are effective in increasing employees' security awareness, which methods are preferred by users, what kind of user experience they provide for participants, and whether gamification solutions can be used in a workplace environment to improve security awareness level of employees, and if so, with what effectiveness, and who and how can use them. In this research I have also focused on how the workplace environment, workplace characteristics, and specifically the nature of the organisations influence the level of security awareness of users, the success and effectiveness of the methods used.

Several international and national experts have also published research on the effectiveness of security awareness improvement methods, and their results show that it is worth further exploring the issue, since, as several authors have shown, preferred solutions may not yet be effective in practice. Nevertheless, the applicability of gamification in security awareness training has been investigated in relatively few scientific publications: a search on 26 June 2023 on Scopus for the terms "awareness" and "gamification" yielded 104 relevant results, narrowing the subject to "Computer Science" yielded 13 publications, and a search on Academia.edu for "security awareness gamification" yielded 959 publications, including 62 journal articles and 1 conference paper. For all these reasons, I found it important to investigate both the literature and the practice of security awareness gamification.

2. SUMMARY OF THE RESEARCH AND THE DISSETRATION

For the preparation of the dissertation, I conducted both a literature review and my own research. In many of the studies and surveys I drew on my own practical experience and on the results of surveys from other sources, as well as on feedback from awareness-improvement actions and observations made specifically in the security awareness escape room and in the delivery of board game programmes.

The first step of the research was to explore the relevant international and national literature on Social Engineering, security awareness and related education, training and improvement opportunities, including gamification.

Based on the results of the literature review, four hypotheses were defined and examined in separate chapters. I have chosen a questionnaire survey with practical elements as the most appropriate data collection method to verify the hypotheses, which I will present in detail in the examination of the first hypothesis. In addition, I have considered my previous surveys relevant to the topic as well as my practical experience.

The data collected through the questionnaire survey will be presented and analysed in the examination of each hypothesis, with each chapter presenting the data used in the research in relation to the specific topic. Overall, I have worked with the data indicated in Figure 1.

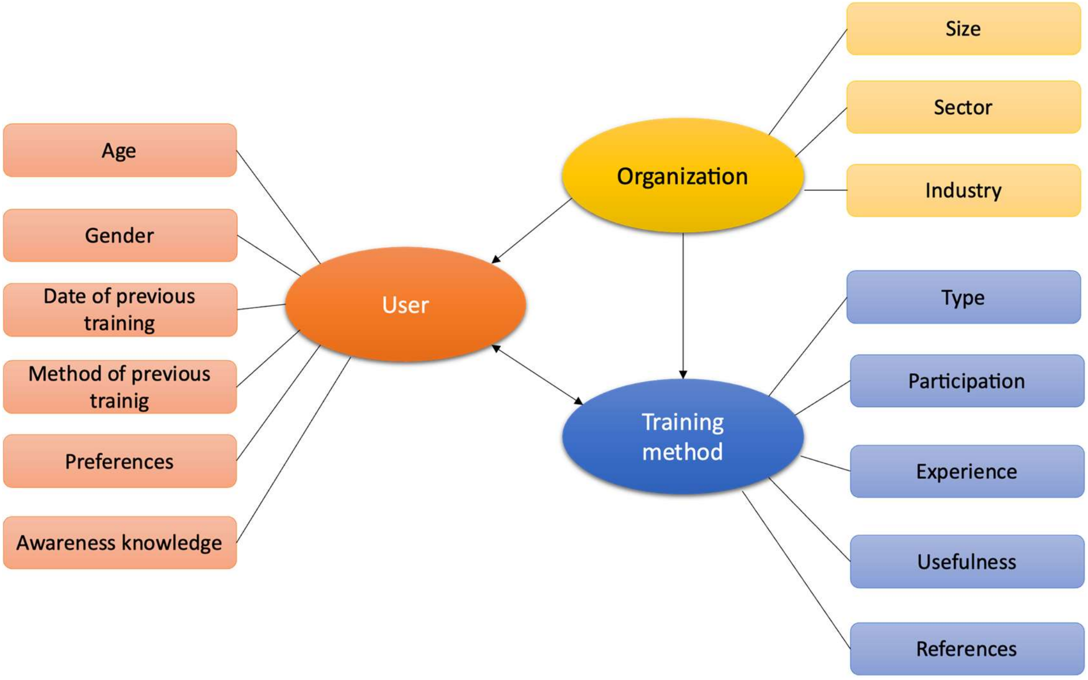

Figure 1: Data collected and used in the research (source: own editing)

In the figure, the colours indicate each of the constituent groups, such as organisational, user characteristics and training method. The arrows between the groups represent their interaction. By analysing the data, I have applied general descriptive statistical methods and cluster analysis.

I have divided my dissertation into the following chapters:

- **Chapter 2**: *Literature review,* in which I present the methodology and results of the first phase of the research in detail and describe the security awareness development methods that are also reflected in the research and identify the requirements and best practices related to them.
- **Chapter 3**: *Examining the effectiveness of security awareness improvement methods in the light of user experience*, in which I present the chosen data collection method and the practical research conducted for the dissertation, and its results, such as the effectiveness of each of the methods examined, and compare its relationship with user preference experience and usefulness.
- **Chapter 4**: *The applicability of gamification to enhance users' security awareness level in the workplace environment* is the title of this thesis, in which I specifically discuss the research findings that demonstrate the relevance of gamification in information security improvement.
- **Chapter 5**: In *The applicability of the Security Awareness Escape Room in a workplace environment for improving users' security awareness* I highlight a specific solution from Chapter 4, using the results of a previous research to investigate whether the method can be applied in a workplace environment to improve security awareness.
- **Chapter 6**: In *The applicability of a security awareness board game in a workplace environment to increase users' security awareness* I highlight a specific solution from Chapter 4, including the steps to develop such a solution, and examine whether it can be applied to improve security awareness in a workplace environment.
- **Chapter 7**: *Conclusion*, in which I summarise the results and conclusions of the related research, as well as the potential for further use and extension of the methodologies and tools developed.

3. TESTED HYPOTHESES

The aim of my dissertation was to compare the effectiveness of different security awareness development methods, to draw conclusions about which method is most applicable for which kind of developments, in which topics and work environments, thus helping organizations to plan information security awareness improvement actions and to increase their effectiveness. Within the education types examined, I was particularly interested in the applicability of gamification solutions in a domestic context, in organisations of different sizes, operating in different sectors, and in relation to two gamification programmes I developed, the security awareness escape room and the security awareness board game.

In preparing my dissertation, I sought to answer questions such as

- which security awareness methods are the most effective, including how gamification approaches are used,
- which method transfers the most knowledge to the participants in the different improvement actions,
- which method will achieve at least a minimum level of knowledge increase for most users (i.e. increase the number of users who will gain at least one new knowledge following the programme),
- in the long term (e.g. one month later), which training method is most likely to retain the knowledge learnt and which training will provide long-lasting knowledge,
- which methods are preferred by users when they have to decide whether or not to participate in some kind of training and whether this has an impact on the learning,
- how users rate each security awareness programme in terms of user experience, enjoyment and how this affects the improvement of their level of security awareness,
- how users rate each security awareness programme in terms of usefulness and how this affects the improvement of their security awareness level,
- is there a correlation between the knowledge acquired and the user's preference and the degree of user experience provided by the programme,
- which are the most existing security awareness skills, and
- which ones have improved the most following participation in the security awareness programme,

- can we use gamification methods, including the security escape room and the security awareness board game in the workplace,
- how and which method should we choose when planning our next security awareness action?

Based on these questions, I have defined four hypotheses presented below, which are partially interdependent, and examined in detail in the chapters of this dissertation.

Hypothesis H1: "For Hungarian organisations, both in the private and public sector, security awareness improvement methods that are enjoyable for users will increase security awareness knowledge both in the number of new knowledge elements and number of security-aware employees than solutions that users prefer or find useful."

To prove this hypothesis, I developed a practical survey methodology to compare the effectiveness of security awareness methods, which is presented in Chapter 3 of this thesis. My aim with this study was to demonstrate that security awareness methods that are enjoyable for users increase users' security awareness knowledge to a greater extent and are able to increase the knowledge of more users than methods that users prefer or find unhelpful.

Based on the results, I found that user preference does not affect the effectiveness of training, i.e. the fact that a user does not prefer a training method does not mean that he or she will not learn from it, and vice versa: a preferred training method is not necessarily effective. I identified a weak positive relationship between users' perceived usefulness and effectiveness, suggesting that training methods that users perceive as useful are marginally more effective in increasing both the number of security awareness knowledge and the number of more security aware users. Likewise, a weak positive relationship was found when examining how user experience influences the number of new security awareness knowledge after attending a training course, but a strong relationship was identified in increasing the number of more security-aware users. This suggests that user experience can influence the effectiveness of a security awareness programme. That is, those who participate in a programme that they enjoy are more likely to learn from the training than those who receive less enjoyable training.

Hypothesis H2: "Gamified solutions and gamification methods can be used in information security training actions in Hungarian organisations, both private and public sector, and can increase the security awareness of employees and the number of users who have acquired at least one new security awareness knowledge element."

To prove the hypothesis, I used the results of the survey used for H1. My aim with this study was to prove that users indeed consider gamified programs to be the most enjoyable in terms of security awareness development, and that gamification methods have the potential to improve security awareness both in terms of increasing knowledge and increasing the number of more security-aware users.

The results have confirmed that gamification methods as the most enjoyable solution can be applied to any organisation, regardless of its nature and size, and can be applied to any user group, regardless of the age and gender of the employees, based on the user experience. This will help to dispel misconceptions that these methods can be used to reach a narrower user group. My research has also shown that gamification methods can be at least as effective as traditional approaches in improving security awareness in the short term, but in the long term they are inferior to lecture-based training, and it is therefore worth using a mixed programme approach.

Hypothesis H3: "A security awareness escape room, as a new training method developed by me can increase the security awareness knowledge of employees of private and public sector organisations in Hungary and increase the number of users enriched with new security awareness knowledge."

My aim in this study was to prove that the security awareness training room I developed in 2014 can improve security awareness both in terms of increasing knowledge and increasing the number of more security-aware users. I applied the research developed for hypothesis H1 and examined the results of this research specifically in relation to the escape room as an element used in it. The results show that, according to the percentage of users who have acquired at least one new security awareness element, the security escape room is the 3rd best security awareness improvement tool of the 6 methods tested, and thus has the potential to improve security awareness and is most effective in raising awareness, especially among the 50-59 age group and the under-30s. The results are very mixed across sectors in terms of the effectiveness of the security awareness escape room in increasing security awareness: in the public sector it is less effective in this test item, while in the private sector it is the most effective solution for increasing awareness level of employees. All of this suggests that the skills previously identified as common gaps (document shredding, social media, phone and smart device security awareness) are greatly improved following this programme, and that the method is particularly suitable for delivering targeted konwledge through its ease of customisation.

Hypothesis H4: "A security awareness board game, as a new training method that I have developed has the potential to increase the security awareness knowledge of employees of private and public sector organisations in Hungary and to increase the number of users who have gained new security awareness knowledge."

In this study, my aim was to prove that the security awareness board game I developed in 2021-2022 can improve security awareness level of users both in terms of increasing knowledge and increasing the number of more security-aware users. For this purpose, I used the research developed for hypothesis H1 and examined its results specifically in relation to the board game as an element used in it. The results show that, based on the proportion of users who have acquired at least one new security awareness knowledge element, the security awareness board game is the 2nd best security awareness tool among the methods tested, and it means that it has the potential to improve security awareness, being most effective for sensitising those under 30 and those aged 30-39. In the public sector, increasing security awareness is considered the most effective method of education, while in the private sector it is the least effective way to increase awareness. Generally the board game programme has also led to a small but significant improvement in knowledge previously identified as generally lacking (document shredding, social media usage, phone and smart device security awareness), an area where it may be appropriate to improve the customisation of the game, for example by specifically marking cards for pre-sorting.

4. THESES AND NEW SCIENTIFIC RESULTS

The aim of my dissertation was to prove that experience-based training solutions, gamification methods can improve security awareness both in increasing the number of security awareness knowledge and in increasing the number of more security-aware users (i.e., who gain at least 1 new knowledge after the training). In addition, I have developed two gamified educational tools, a security awareness escape room, and a security awareness board game, which I have demonstrated to be effective in security awareness improvement method.

Based on the above, the following scientific results can be concluded:

I. With the survey method I developed for this research, I was able to measure users' evaluations of specific programmes, such as preference, usefulness and enjoyment, not only through traditional questionnaires, but also through practical participation in different programmes. To these I was able to relate the results to changes in their security awareness and identify the relationship between user ratings and programme effectiveness. **With these findings, I proved the thesis that, for Hungarian organizations, both private and public sector, security awareness programs that users enjoy increase security awareness knowledge to a greater extent and increase security awareness knowledge of more employees than preferred or perceived useful methods.**

II. From the point of view of user experience, gamification methods were clearly the best option based on my research. Accordingly, I measured the openness of users to gamification on the one hand, and the effectiveness of these methods on the other hand, also by means of the survey used in the first point. **My research proved the thesis that gamified solutions and gamification methods can be applied in information security awareness training actions in Hungarian organisations, both in the private and public sector, and that they are able to increase the security awareness level of employees and the number of users who have acquired new security awareness knowledge.**

III. To improve security awareness level of users, I developed a **security awareness escape room** methodology in 2014, which I have been actively using since then to train users on information security awareness. This solution has received a lot of positive feedback, but its effectiveness has not yet been measured in any other way, so its applicability has not been proven. **Through this research I have validated**

the thesis that the security awareness escape room developed by me in 2014, as a new security awareness improvement solution, has the potential to improve security awareness level of employees both in terms of increasing knowledge and increasing the number of more security-aware users.

IV. To improve security awareness, I also developed a **security awareness board game** between 2021-2022, which was published and is available as an educational solution for both organisations and individuals. This solution has received a number of positive feedbacks, but its effectiveness has not yet been measured in any other way, so its applicability has not been proven. **Through this research I have validated the thesis that security awareness board game developed by me in 2021-2022, as a new security awareness improvement solution, can improve security awareness level of employees both in terms of increasing knowledge and increasing the number of more security-aware users.**

5. PRACTICAL USE OF THE RESEARCH RESULTS

In my dissertation, I have shown that gamification methods, including escape rooms and board games, can improve security awareness level of employees, both to increase new knowledge and to increase the number of more security-aware users (i.e. participants who have gained at least 1 new knowledge after the program). The two gamification solutions I tested (the security awareness escape room and the security awareness board game) were found to be highly effective in the short term, but in the longer term, although effective in improving participants' knowledge, they ended up at the bottom of the ranking. It should be noted, however, that both of the gamified methods I have presented primarily promote regular use, with the board game, for example, specifically aimed at providing frequent educational opportunities or even board game club-like use. The research findings presented, and the experiences described in detail in this thesis, may be useful in helping organisations designing information security awareness programmes to select the most appropriate methods for their needs - as it is important to recognise that there is no one best solution for everyone.

New methods that follow current trends, such as gamification, will most likely always be popular, so it is worth keeping up with the times and opening up to new possibilities, but it is important to evaluate which solutions are the most enjoyable and effective for our organisation and employees. As my research has repeatedly and surprisingly highlighted, there can be huge differences even in the effectiveness of gamification methods, even just in terms of the sector in which they operate. What proved to be the most effective solution in the public sector came last among market companies - and vice versa. Therefore, prior evaluation, preferably testing with key users is very important, in which even the survey method I used and presented in my dissertation, can be of great help.

6. FUTURE RESEARCH DIRECTIONS AND IMPOVEMENT OPPORTUNITIES

The research for this dissertation has also provided me with very interesting and enlightening results, which I plan to use as a basis for further developments, both in terms of further survey options and the gamification tools developed:

- My aim is to do further investigations about gamification methods, which are more effective in the short term, can have a positive impact on other traditional training methods, and whether the use of gamified methods to stimulate interest has an impact on the success of traditional methods.
- In the present research, this was not possible primarily due to the sample size, but it may also be interesting to investigate how the gained knowledge are actually applied in practice (e.g. during a Social Engineering audit), and what correlation can be observed between long-term recall of theoretical knowledge and practical application.
- Specifically with regard to the board game, its positive reception and its effectiveness in security awareness development confirmed that there is a case for further development of the game as described in detail in this thesis, for improving the existing game and adding new features, and for developing more specialised versions (for home and management).

7. LIST OF PUBLICATIONS

OROSZI, Eszter Diána, *Információbiztonsági stratégia és vezetés* [Information security strategy and management], EIV képzés tananyag (egyetemi jegyzet), 2014

OROSZI, Eszter, *A humán erőforrás védelme – védelem a humán erőforrás ellen* [Protecting human resources – protection against human resources] In. MUHA, Lajos – LEITOLD, Ferenc – SZÁDECZKY, Tamás – OROSZI, Eszter – SOM, Zoltán – LEITOLD, Ferenc (szerk.) Információ és adatvédelem a közigazgatásban, 2014, p. 27-37.

OROSZI, Eszter, *A biztonságtudatossági szint mérésének lehetőségei* [Opportunities to measure security awareness level] In. GULYÁS, Éva – MARÓTI, Dávid – MÁTHÉ, Réka Zsuzsánna – SOMOGYI, Renáta – SŐREG, Krisztina – SZINAY, Ildikó (szerk.) Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola 2014/15-ös Kutatói Fórumának tanulmánykötete, 2015, p. 169-183.

OROSZI, Eszter, LEITOLD, Ferenc, *Social Engineering methodologies – Identifying and analysing human risks* In. CEE eGov Days 2014 eGovernment: Driver or Stumbling Block for European Integration, 2014 Alexander Balthasar, Handrik Hansen, Balázs König, Robert Müller-Török, Johannes Pichler (Eds.) ISBN: 978-3-85403-300-4, p. 127-138.

OROSZI, Eszter Diána, *Kártékony programok terjedése social engineer szemmel* In. Dunakavics, 2015 III. Évfolyam VIII. szám, felelős szerkesztő: Dr. András István, ISSN: 2064-5007, p. 5-14.

LEITOLD, Ferenc, HADARICS, Kálmán, OROSZI, Eszter, GYŐRFFY, Krisztina, *Measuring the information security risk in an infrastructure* In. 2015 10th International Conference on Malicious and Unwanted Software (MALWARE), 2015, p. 93-100.

OROSZI, Eszter, GYŐRFFY, Krisztina, *Information Security for e-government social media marketing and citizen interaction* In. CEE eDem and eGov Days 2016, Multi-Level (e)Governance: Is ICT a means to enhance transparency and democracy, 2016, p. 225-236.

LEITOLD, Ferenc, ARROTT, Anthony, HADARCSI, Kálmán, OROSZI, Eszter, *Automating visibility into user behaviour vulnerabilities to malware attack* In. Virus Bulletin 2016, Proceedings of the 26th Virus Bulletin International Conference, VB 2016 Denver 5-7 October 2016 Martjin, Grooten (szerk.) p. 1-8.

OROSZI, Eszter Diána, *Social Engineering technikák* [Social Engineering techniques] In. BODÓ, Attila Pál - OROSZI, Eszter Diána - SÁGI, Gábor János - SZAPPANOS, Gábor - SZARVÁK, Anikó - ZÁMBÓ, Nóra - DEÁK, Veronika (szerk.) Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában résztvevő személy számára, 2018, ISBN: 978-615-5870-52-1 p. 76-118.

OROSZI, Eszter Diána, *Security awareness escape room – a possible new method in improving security awareness of users* In. Cyber Science Cyber Situational Awareness for Predictive Insight and Deep Learning, C-MRiC.ORG, 2019 Onwubiko C., Bellekens X., Erola A., Jaatun M.G., Nogueira C. (Eds.) ISBN: 978-0-9932338-4-5"

OROSZI, Eszter Diána, *Biztonságtudatossági szabadulószoba, mint új programelem az információbiztonsági képzésekben* [Security awareness escape room – a possible new method in improving security awareness of users] In. Dunakavics, 2020. VIII. Évfolyam III. szám, felelős szerkesztő: Dr. András István, ISSN: 2064-5007, p. 51-62.

OROSZI, Eszter Diána, *Social Engineering a koronavírus tükrében, avagy a rendkívüli helyzetet kihasználó támadási technikák és megelőzésük* [Socia Engineering in the light of COVID-29 – attack techniques exploiting the emergency situation and prevetive actions] In. Dunakavics, 2020. VIII. Évfolyam V. szám, felelős szerkesztő: Dr. András István, ISSN: 2064-5007, p. 51-62.

OROSZI, Eszter Diána, *Using gamification to improve security awareness level of users - Security awareness escape room as an effective and unique element of trainings* In. ISACA Journal Volume 4, 2020 (2020. July), Jannifer Hajigeorgiou (szerk.), ISSN 1944-1967

OROSZI, Eszter Diána, *Make Security Awareness an Experience,* ISACA Now Blog, 2020.09.25 (https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/make-security-awareness-an-experience, utolsó elérés: 2023.04.09)

OROSZI, Eszter Diána, *Exploitable Traits as Vulnerabilities: The Human Element in Security,* In. ISACA Journal Volume 5, 2021, Jannifer Hajigeorgiou (szerk.), ISSN 1944-1967, p.16-21

OROSZI, Eszter Diána, *Boardgames as Security Awareness Improvement Tools* In. HOF, Hans-Joachim – POPESCU, Manuela – FONGEN, Anders (szerk.) SECURWARE 2021 :

The Fifteenth International Conference on Emerging Security Information, Systems and Technologies, 2021, p. 19-23.

OROSZI, Eszter Diána, *Patching Security Awareness: Human Traits as Vulnerabilities,* ISACA Now Blog, 2021.10.15 (https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2021/patching-security-awareness-human-traits-as-vulnerabilities, utolsó elérés: 2023.04.09)

LACZKÓ, Anikó, OROSZI, Eszter Diána, *Vigyázz – Kész - Rajt! Hamarosan indul a kibervédelmi hónap!* [Ready – Stady Go! Let's start Cybersecurity Month!] (tanulmány) https://silentsignal.hu/docs/S2_kibervedelmi_honap_kampanyelemek_tanulmany_20220805.pdf, utolsó elérés: 2023.03.26), 2022

OROSZI, Eszter Diána, *Taking a Risk-Based Approach to Pen Testing*, ISACA Industry News, 2022.10.24 (https://www.isaca.org/resources/news-and-trends/industry-news/2022/taking-a-risk-based-approach-to-pen-testing, utolsó elérés: 2023.04.09)

BARNA, Bianka Rita; KOLLÁR, Csaba; **OROSZI, Eszter Diána**: *A social engineering helye az információbiztonsági auditban.* [Social Engineering in the information security audit] In. Biztonságtudományi Szemle, 5. évfolyam, 1. szám (2023), ISSN 2676-9042, p. 25-41.

Conference presentations:

- *Social Engineering – amikor fellebben a fátyol* [Social Engineering – when the veil lifted], Hacktivity 2011, Budapest, 2011.09.18
- *„Social Media Engineering", avagy játék határok nélkül?* [Social Media Engineering – games without borders?], Ethical Hacking konferencia2014, Budapest, 2014.05.22
- *Magánélet és biztonság – avagy biztonságtudatosság a munkahelyen innen és túl...*[Privacy and security – security awareness in the workplace and beyond], ITBN konferencia 2014, Budapest, 2014.09.24
- *Kibertámadások a kibertéren kívül – avagy a pokolba vezető út is jószándékkal van kikövezve* [Cyber attacks outside the cyberspace – the road of the hell is paved with good intentions], HISEC konferencia 2014, Budapest, 2014.11.18
- *„Hacking with human" – avagy a pokolba vezető út is jószándékkal van kikövezve* [Hacking with human - the road of the hell is paved with good intentions], Ethical Hacking konferencia 2015, Budapest, 2015.05.08

- *Beléptető rendszerek biztonsága – Valós védelem vagy hamis biztonságérzet?* [Security of entrance systems – real protection or false sense of security?], Ethical Hacking 2016, Budapest, 2016.05.12
- *Kibertámadások a kibertéren kívül - A biztonságtudatosság szerepe és jelentősége a technológiai informatikai rendszerek elleni támadások kezelésében* [Cyber atacks outside the cyberspace – the role and importance of security awareness against attacks on OT systems], Védelem és irányítástechnikai fórum 2016, Velence, 2016.06.01
- *Biztonságtudatossági szabaduló szoba, mint a felhasználók biztonságtudatosságának új fejlesztési eszköze* [Security awareness escape room – a possible new method in improving security awareness of users], ISACA második szerdai előadás, Budapest, 2017.05.10
- *A „humán hackelés" művészete, avagy az emberi tényező, mint a biztonság leggyengébb láncszeme* [The art of human hacking – human factor, as the weakest link in the chain of security], BM OKF konferencia 2017, Budapest, 2017.10.26
- *Kibertámadások a kibertéren túl, avagy az információbiztonság humán oldala* [Cyber attacks outside the cyberspace – human side of information security], Kihívások a nemzetbiztonságban konferencia 2017, Budapest, 2017.10.27
- *A biztonságtudatosság fejlesztésének új lehetőségei* [New methods to improve security awarneess], BM OKF konferencia 2018, Budapest, 2018.10.11
- *Social Engineering támadások megelőzése, avagy a tudatosítás lehetőségei munkahelyi környezetben* [Peventing Social Engineering attacks – improving security awareness in the workplace], Alkotmányvédelmi Hivatal, Awareness konferencia 2019, Budapest, 2019.03.06
- *Az információbiztonság humán faktora* [The human factor in information security], Nemzetközi Katonai Információbiztonsági Konferencia, 2019, Balatonkenese, 2019.05.23
- *A biztonság humán faktora, avagy az emberi tényező kihasználható tulajdonságai* [The human factor of security – exploitable traits and habits of human factor], Alkotmányvédelmi Hivatal, Awareness konferencia 2020, Budapest, 2020.03.04
- *Biztonságtudatossági játékok, avagy a felhasználók információbiztonsági ismereteit fejlesztő módszerek hatékonyságának értékelése* [Security awareness games – evaluating the effectiveness of security awareness improvement methods], ISACA Második Szerda, 2022.01.12

- *A biztonság nem játék... de játszva fejleszthető!* [Security is not a game... Buti t can be improved by gamification!], Hétpecsét Információvédelem Menedzselése CI. Szakmai Fórum, Budapest, 2022.05.18
- *Időutazás a Social Engineering auditok korában, avagy mi változott az elmúlt 10 év alatt?* [Time travel in the age of Social Engineering audits. what has changed in the last 10 years?], ISACA Konferencia 2022, Budapest, 2022.06.16.
- *Szirének hálójában – avagy hívószavak a szervezetet érintő információbiztonsági kockázatok (költség)hatékony kezeléséhez* [In the Siren's web – actions for (cost) effective management of information security risks tot he organization], MLBKT Kongresszus 2022, Siófok, 2022.10.19
- *Szirének szigete - avagy tévutak és csábító lehetőségek a kockázatmenedzsmentben* [The Island of Sirens – missteps and temptations in risk management], WITSEC Konferencia 2022, Budapest, 2022.10.26
- *Szirének hálójában - avagy a szervezetünket érintő információbiztonsági kockázatok teljeskörű feltérképezésének fontossága* [In the Siren's web – the importance of mapping information security risks tot he organization], EIVOK-30 Tudományos – Szakmai Konferencia, Debrecen, 2022.11.03
- *Kárral szemben – Úton a SIREN fedélzetén* [Facing damage – On the road on board of the SIREN], Silent Signal Szakmai Nap, Budapest, 2023.03.28
- *Adataink őrzői – és a végtelen kockázatok* [Guardians of our data – Infinite risks], ISACA Konferencia 2023, Budapest, 2023.06.01.

8. CURRICULUM VITAE

Eszter Diána Oroszi graduated from the Corvinus University of Budapest in 2009 with a BSc in Business Informatics and in 2011 with an MSc in Business Informatics. In 2008 she joined Kancellár.hu Zrt. as an intern and later as an information security consultant. Already at that time he was particularly interested in measuring and developing human factor security awareness, his thesis written in 2008 collects and describes in detail the Social Engineering techniques, and his MSc thesis describes the methodology of Social Engineering audits.

Eszter was admitted to the Doctoral School of Public Administration of the National University of Public Service in 2014, where she started to research the development of security awareness in line with her previous theses. Her main research interest is the investigation of the application of gamification in the field of security awareness development, the exploration and creation of methods to develop the level of security awareness in an effective and enjoyable way for users. In 2014, he was the first to introduce the first security awareness escape room in Hungary, which he turned into a methodology and has been continuously developing ever since, and in 2022, with the support of his current workplace, Silent Signal Ltd., her security awareness board game was published, and the creation of the company's online security awareness game is also attributed to her.

In addition to her consulting work, Eszter has also worked as an internal information security expert for 6 years in both public and private sector companies, which has also greatly contributed to her research work. In addition, she has been a lecturer at the National University of Public Service since 2014 for the advanced training course Electronic Information Security Manager. Nowadays she works as Head of Information Security Consulting department of Silent Signal Ltd.

She is a regular speaker at national professional conferences and regularly publishes in international professional publications.