PRO PUBLICO BONO – Public Administration, 2021/1, 108–127. • DOI: 10.32575/ppb.2021.1.7

Ildikó Legárd

EFFECTIVE METHODS FOR SUCCESSFUL INFORMATION SECURITY AWARENESS

Ildikó Legárd, PhD student, University of Public Service, Doctoral School of Public Administration Sciences, ildiko.legard@gmail.com

Information security awareness is becoming increasingly important these days. It is not enough to have a well-developed physical and logical protection of the system and stored data; the users of these systems have to keep up with technological development and have to be sufficiently aware or cautious when using these systems. Information Security Awareness Programs provide the most effective solution for the improvement of users' information security knowledge and digital competencies.

The aim of this study is to help organisations in finding and providing an effective way of knowledge transfer. The study identifies the key elements of the implementation of the awareness programs and highlights the importance of communication channels and methods. The essay summarises and shows the most effective techniques that experts can use in order to draw the user's attention toward information security, like real-life simulation scenarios, interactive games, themed awareness videos and other gamification techniques.

Keywords:
gamification, information security, information security awareness, IT-security, security awareness program

1. INTRODUCTION

The rapid increase in digitalisation, the tremendous development of ICT tools and services, the widespread use of the Internet, and rapid access have brought about the need for information security to keep data and information produced safe from various security threats and risks.

NATO's interpretation of information security (INFOSEC) by the Allied Joint Doctrine for Information Operations: 'As part of OPSEC (Operations Security) the goal of Information Security (INFOSEC) is to protect information (stored, processed or transmitted), as well as the host systems, against a loss of confidentiality, integrity and availability through a variety of procedural, technical and administrative controls. INFOSEC includes a range of measures that are applied on a routine basis under the auspices of security policy to protect information. (…) INFOSEC is an integral element of all military operations and encompasses Communications Security (COMSEC), Computer Security (COMPUSEC), Computer Network Defence (CND), an integral part of Computer Network Operations (CNO), and together with personnel, document, physical and procedural security, it must be considered at the earliest conceptual stages and throughout the planning of an operation.'[1]

Many experts agree that the weakest link in the field of information security is the human factor, namely the user. Social engineering is a type of threat that builds on influencing, manipulating and exploiting the vulnerability of the human factor. Social engineering attacks can be divided into two types of attack, depending on the methods used by the attacker: human-based and computer-based. The most popular forms of human-based attacks are: asking for aid or support, assistance (reverse social engineering), identity theft, thumbstone theft, shoulder surfing, dumpster diving and tailgating. Computer-based attacks are: phishing (for example scam, vishing, smishing, pharming, whailing), malicious programs (for example: viruses, trojans, scripts, keylogger, spyware, baiting, ransomware), attacks based on public Wi-Fi and attacks based on mobile apps.[2]

There are various types of measures under information security (for example modern preventive tools and security systems in place) and one of them is information security awareness.[3] According to Kruger and Kearney 'whilst information security generally focuses on protecting the confidentiality, integrity and availability of information, information security awareness deals with the use of security awareness programs to create

1 AJP-3.10 Allied joint doctrine for information operations, NATO/PfP unclassified publication, 2009.

2 Ildikó Legárd, 'Building an Effective Information Security Awareness Program', in *Central and Eastern European EDem and EGov Days 2020,* ed. by Thomas Hemker, Robert Müller-Török, Alexander Prosser, Dona Scola, Tamás Szádeczky and Nicolae Urs (Wien: Österreichische Computer Gesellschaft, 2020), 190.

3 Abigail N W Prah, Angela A Otchere and Kojo E Opan, 'The Perceived Effectiveness of Information Security Awareness', *Information and Knowledge Management* 6, no 7 (2016), 62.

and maintain security-positive behavior as a critical element in an effective information security environment'.[4]

This study is structured as follows. Next to the introduction, the second section reviews the conceptual framework including information security awareness and information security awareness programs. Section 3 identifies the key elements of the implementation of security awareness programs. Section 4 discusses and evaluates the main focus areas of the training material and the most effective ways and different information security awareness tools and techniques; presenting the role of a practice-oriented approach and gamification in security awareness and summarises the most important communication channels. Finally, the last section presents the main properties of the study.

This study utilises the qualitative method of research that is based on a secondary, in-depth analysis of literature. The aim of this method is to review, analyse and compare the most important concepts and theories in the field of information security awareness, especially effectiveness, the choice of methods, communication channels and gamification techniques.

2. CONCEPTUAL FRAMEWORK

This section presents the most important concepts: information security awareness and information security awareness programs.

2.1. Information security awareness

There is no generally accepted concept of information security awareness, but several Hungarian and international researchers have tried to define its components.[5] Hussain Aldawood and Geoffrey Skinner[6] emphasise individual aspects of information security awareness, while András Nemeslaki and Péter Sasvári[7] and Burcu Bulgurcu et al.[8] highlight its organisational aspects.

---

4 Hennie A Kruger and Wayne D Kearney, 'A prototype for assessing information security', *Computers & Security* 25, no 4 (2006), 289.

5 Ildikó Legárd, 'Célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre', *Hadmérnök* 15, no 1 (2020), 95; Ilirjana Veseli, *Measuring the Effectiveness of Information Security Awareness Program* (M. S. thesis, Gjøvik: Gjøvik University College, 2011), 87; Charlie C Chen, B Dawn Medlin and R S Shaw, 'A cross-cultural investigation of situational information security awareness programs', *Information Management & Computer Security* 16, no 4 (2008), 360–376.

6 Hussain Aldawood and Geoffrey Skinner, 'Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues', *Future Internet* 11, no 3 (2019), 1–16.

7 András Nemeslaki and Péter Sasvári, 'Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában', *Infokommunikáció és Jog* 4, no 60 (2014), 169–177.

8 Burcu Bulgurcu, Hasan Cavusoglu and Izak Benbasat, 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness', *MIS Quarterly* 34, no 3 (2010), 523–548.

Overall, the concept of information security awareness could be summarised as a set of knowledge, skills and behaviours that provides the users with the appropriate level of IT and information security knowledge, the skills that build on it and ensures its application, and the corresponding behaviour that appears as an internal need and recognises the importance of information security.[9] At the same time, information security awareness is part of an organisation's culture, a way of thinking and behaving that ensures that employees within the organisations are aware of and are ideally committed to the security objectives of their organisation and are enforcing security measures.[10]

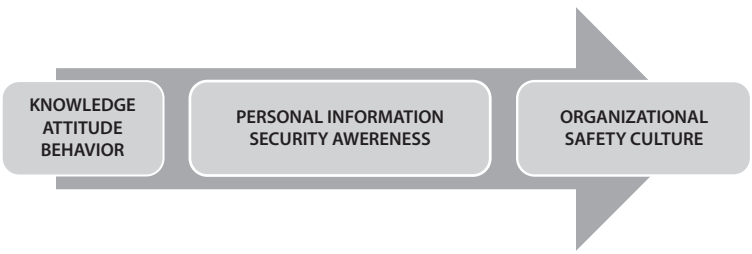

Figure 1 • *Security awareness (Source: Legárd, 'Building an Effective Information Security Awareness Program', 193.)*

Both NATO and the EU address the issue of awareness in their strategic documents.

The 2010 Strategic Concept 'Active Engagement, Modern Defence', which is a resolute statement on NATO's core tasks and principles, its values, the evolving security environment and the Alliance's strategic objectives, states: 'We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will: (…) develop further our ability to prevent, detect, defend against and recover from cyberattacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.'[11] To achieve this goal, NATO reinforces its capabilities for cyber education, training and exercises[12] and NATO and the EU are strengthening their cooperation on cyber defence, notably in the areas of information exchange, training, research and exercises.

In June 2019, the EU Cybersecurity Act (CSA) entered into force and ENISA became the European Union Agency for Cybersecurity, with a new permanent mandate. According to this act, in order to raise awareness and education, ENISA shall:

9 Legárd, 'Célpont vagy!', 95.

10 Nemeslaki and Sasvári, 'Az információbiztonság-tudatosság', 169.

11 *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization* (Brussels: NATO Public Diplomacy Division, 2010).

12 'Cyber defence', 23 May 2019.

(a) raise public awareness of cybersecurity risks, and provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including cyber-hygiene and cyber-literacy;
(b) in cooperation with the Member States, Union institutions, bodies, offices and agencies and industry, organise regular outreach campaigns to increase cybersecurity and its visibility in the Union and encourage a broad public debate;
(c) assist Member States in their efforts to raise cybersecurity awareness and promote cybersecurity education;

On 16 December 2020, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy presented a new EU Cybersecurity Strategy.[13] The EU's new Cybersecurity Strategy for the Digital Decade forms a key component of Shaping Europe's Digital Future that states: 'Improving education and skills is a key part of the overall vision for digital transformation in Europe.' A Digital Education Action Plan is essential to boost digital literacy and competences at all levels of education.[14]

2.2. Information security awareness programs

Effective protection against threats can be ensured by the security awareness of the users, which can be achieved through a well-organised and successful security awareness program.

Many international IT security standards refer to the implementation of an awareness program as a requirement for getting certifications, such as ISO 27001, COBIT, or ISO 9001: 2000.

Instead of the definition, previous studies concerning information security awareness programs focused on different aspects and purposes of the programs.[15]

Abigail N W Prah et al. state that information security awareness programs can be used by organisations to make their employees conscious of the security threats that could affect them and how they can be mitigated with security measures. The most important goal of the program is to positively affect the behaviour and attitudes of employees towards information security.[16] In their article, Mark Wilson and Joan Hash from the National Institute of Standards and Technology (NIST) define security awareness as follows: 'Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to

13 'The EU's Cybersecurity Strategy in the Digital Decade', 16 December 2020.
14 'Shaping Europe's Digital Future', 2020.
15 Legárd, 'Building an Effective Information Security Awareness Program', 192.
16 Prah et al., 'The Perceived Effectiveness', 62.

recognize IT security concerns and respond accordingly. (…) Awareness relies on reaching broad audiences with attractive packaging techniques.'[17]

Based on the various approaches, security awareness programs can be described as a continuous effort of raising the attention of stakeholders towards information security and its importance, stimulating security-oriented behaviours,[18] and ideally inducing stakeholders' compliance to security policies and guidelines.[19]

According to Wilson and Hash, there are three major steps in the development of an IT security awareness and training program: designing the program (including the development of the IT security awareness and training program plan), developing awareness and training material, and implementing the program. 'Awareness and training programs must be designed with the organization mission in mind. It is important that the awareness and training program supports the business needs of the organization and be relevant to the organization's culture and IT architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented.'[20]

David Lacey also states that the first step of developing an effective security program is to identify the requirements and the key problem areas, analyse the root causes and develop the programs that indicate corrective actions.[21]

Regarding relevant studies and best practices, I could set up a model of the key elements of the implementation and the most important five steps to ensure the success of security awareness programs and to help organisations to design their own specific program.[22]

17 Mark Wilson and Joan Hash, *Building an Information Technology Security Awareness and Training Program* (Gaithersburg, MD: National Institute of Standards and Technology, 2003), 8–9.

18 Thomas R Peltier, 'Implementing an Information Security Awareness Program', *Information Systems Security* 14, no 2 (2005), 37–48; ENISA, 'A new users' guide: how to raise information security awareness', 2008; Susan Hansche, 'Designing a Security Awareness Program: Part I', *Information Systems Security* 9, no 6 (2001), 14–23; David D Maeyer, 'Setting up an Effective Information Security Awareness Programme', in *ISSE/SECURE 2007 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/SECURE 2007 Conference (part 1),* 2007.

19 Aggeliki Tsohou, Maria Karyda and Ramzi El-Haddadeh, 'Implementation challenges for information security awareness initiatives in e-government', *ECIS 2012 Proceedings,* 2012, 179; Mikko T Siponen, 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security* 8, no 1 (2000), 31–41.

20 Wilson and Hash, *Building an Information Technology Security Awareness,* 11.

21 David Lacey, *Managing the Human Factor in Information Security. How to Win Over Staff and Influence Business Managers* (Wiley, 2009).

22 Legárd, 'Building an Effective Information Security Awareness Program', 193–194.

Figure 2 • *The key elements of the implementation of security awareness programs (Source: Legárd, 'Building an Effective Information Security Awareness Program', 194.)*

The study presents how an organisation can develop an information security program, and how it can pass on the right information to the right person in the right form.

3. TRAINING MATERIAL AND THE EFFECTIVE WAYS OF KNOWLEDGE TRANSFER (METHODS AND OPTIONAL COMMUNICATION CHANNELS)

The target user group for the program is either people without any previous training in the field of information security, or people who received training, but did not achieve a satisfactory result.

3.1. Training material

Information security awareness means that the employee:

- understands the meaning of definitions, exactly what we are talking about
- recognises what compromises the functioning of the information system
- helps prevention
- knows what to do in case of an IT incident[23]

[23] Nemeslaki and Sasvári, 'Az információbiztonság-tudatosság', 170.

Information security awareness consists of two main parts: in general, knowledge of IT and IT security and related skills, and on the other hand, knowledge of information security regulations and strategies.

But most important of all, if employees are aware of the security threats and how they can be mitigated, they can take appropriate action to prevent and correct security breaches. Therefore, the organisation as a whole can better prevent and mitigate these threats, especially social engineering attacks.

The training materials should be up-to-date, and should include the top threats identified in the most recent studies and analyses. In the following, the findings of several international organisations from 2020 are summarised:

The IOCTA is Europol's flagship strategic product highlighting the dynamics of cybercrime and the evolution of cybercrime threats. IOCTA 2020 states, that 'social engineering remains a top threat to facilitate other types of cybercrime. (…) However, despite the trend pointing towards a growing sophistication of some criminals, the majority of social engineering and phishing attacks are successful due to inadequate security measures or insufficient awareness of users'.[24]

Covid-19 Cybercrime Analysis Report by Interpol highlighted the below key threats:

- In one four-month period (January to April 2020) some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs – all related to Covid-19 – were detected by one of Interpol's private sector partners.
- Cybercriminals are increasingly using disruptive malware against critical infrastructure and healthcare institutions, due to the potential for high impact and financial benefit.
- The deployment of data harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans by cybercriminals is on the rise.
- Taking advantage of the increased demand for medical supplies and information on Covid-19, there has been a significant increase in cybercriminals registering domain names containing keywords, such as "coronavirus" or "Covid".
- An increasing amount of misinformation and fake news is spreading rapidly among the public.[25]

The European Union Agency for Cybersecurity (ENISA) calls attention to this problem in its document published at the end of 2020.[26]

[24] IOCTA, 'Internet Organised Crime Threat Assessment (IOCTA) 2020', 05 October 2020.
[25] 'COVID-19 Cybercrime Analysis Report', August 2020.
[26] 'ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected', 20 October 2020.

ENISA Threat Landscape – 15 Top Threats in 2020

Figure 3 • *ENISA Threat Landscape – 2020 (Source:* www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends*)*

Based on several studies of the last few years and the above presented recent papers, the security awareness program should provide adequate knowledge of the following actual threats:

Table 1 • *Threats identified as affecting security (Source: Compiled by the author.)*

Threats	Studies
Password usage and protection (e.g.): • choosing a good password • password management • password sharing • locking workstation	Aldawood and Skinner (2018); Aldawood and Skinner (2019); Illésy et al. (2014); Kruger and Kearney (2006); Nemeslaki and Sasvári (2014); Parsons et al. (2014); Pattinson et al. (2012); Prah et al. (2016); Som and Papp (2016); Stephanou et al. (2008); Szász and Kiss (2018)

Threats	Studies
E-mail (e.g.): • phishing • scam • pharming • whailing • spam • opening attachments and links	Aldawood and Skinner (2018); Aldawood and Skinner (2019); Bányász and Krasznay (2019) Deák (2019); Illésy et al. (2014); Kruger and Kearney (2006); Nemeslaki and Sasvári (2014); Parsons et al. (2014); Pattinson et al. (2012); Prah et al. (2016); Stephanou et al. (2008)
Internet (e.g.): • dangerous Website/URL • web-based attacks • web application attacks • public Wi-Fi security risks • (home) router security settings • online shopping and payment • update • misinformation • DDos • defacement • botnets • cryptojacking • installing unauthorised software • accessing dubious websites • inappropriate use of internet	Aldawood and Skinner (2018); Aldawood and Skinner (2019); Bányász and Krasznay (2019); Deák (2019); Illésy et al. (2014); Kruger and Kearney (2006); Nemeslaki and Sasvári (2014); Parsons et al. (2014); Prah et al. (2016)
Social networking site (SNS) (e.g.): • sharing sensitive, personal data • posting about work on SNS • games • malware • ransomware • misinformation and fake news	Aldawood and Skinner (2018); Aldawood and Skinner (2019); Bányász (2015); Bányász (2017); Bányász (2018); Bányász and Krasznay (2019); Deák (2017); Deák (2018); Parsons et al. (2014)
Mobile equipment (e.g.): • physical security (physical manipulation, damage, theft and loss) • public Wi-Fi security risks • mobile application license	Aldawood and Skinner (2018); Aldawood and Skinner (2019); Deák (2017); Deák (2019); Illésy et al. (2014); Kruger and Kearney (2006); Parsons et al. (2014)
Data and information handling (e.g.): • data breach • information leakage • cyber espionage • adherence to company policies • clean desks policy • plug-in storage devices • home office – VPN • private use of electronic communications in the workplace and use of a private mail system for work • installing unknown software	Aldawood and Skinner (2019); Bányász and Krasznay (2019); Deák (2019); Illésy et al. (2014); Nemeslaki and Sasvári (2014); Parsons et al. (2014)
Incident reporting: • reporting suspicious individuals • reporting bad behaviour by colleagues • reporting all security incidents	Kruger and Kearney (2006); Parsons et al. (2014); Prah et al. (2016)

3.2. Knowledge transfer methods and tools

The message of the program needs to be clear, meaningful, personal, memorable and contextualised. The specific, real-life examples and evidence can leave a lasting impression. The programs are more likely to be successful if the users feel that the subject matters and issues presented are relevant to their own needs.[27]

Aldawood and Skinner state that the traditional training methods, including onsite trainings and awareness camps, screensavers, posters, manual reminders and online courses are boring and tedious, leading to limited success. These methods tend to be very general and sometimes do not focus on the main objective of making staff remember the major manipulation techniques of hackers.[28] 'These traditional methods alone do not create sufficient safe culture among staff.'[29] Modern training methods, involving real-life simulation scenarios, interactive games, virtual labs, themed awareness videos and modules aim to provide awareness of social engineering and of how the social engineers actually perform an attack.[30]

The study of Kathryn Parsons et al. confirms the effectiveness of methods that provide useful knowledge and help with day-to-day tasks. They state that understandable, visible and 'convenient' security is the only way to ensure that users get useful knowledge in the field of IT security and also be motivated for the application of knowledge.[31] 'Training should be contextualized and should use case studies to improve both knowledge of what is expected and also understanding of why this is important'.[32]

Malcolm Pattinson et al. in their research of the detection of phishing e-mails, highlighted the effective role of scenario-based role-playing in awareness.[33]

Antónia Szász and Gábor Kiss confirm the efficiency of modern methods: 'It has been demonstrated that the educational method supported by decrypter programs that

---

27 Kathryn Parsons, Agata McCormac, Marcus Butavicius and Lael Ferguson, *Human Factors and Information Security: Individual, Culture and Security Environment* (Published by Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh South Australia, 2010), 32; Tony Stephanou and Rabelani Dagada, 'The impact of security awareness training on information security behaviour: The case for further research', in *Proceedings of the ISSA 2008 Innovative Minds Conference, ISSA 2008,* Gauteng Region (Johannesburg), 2008, 5.

28 Aldawood and Skinner, 'Reviewing Cyber Security', 7.

29 Jemal H Abawajy, 'User preference of cyber security awareness delivery methods', *Behaviour & Information Technology* 33, no 3 (2014), 1–12.

30 Aldawood and Skinner, 'Reviewing Cyber Security', 6; Hussain Aldawood and Geoffrey Skinner, 'Challenges of implementing training and awareness programs targeting cyber security social engineering', in *2019 Cybersecurity and Cyberforensics Conference (CCC)* (Melbourne, 2019), 113–115; Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson and Cate Jerram, 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security* 42 (2014), 165–176.

31 Parsons et al., *Human Factors and Information Security,* 54.

32 Parsons et al., 'Determining employee awareness', 174.

33 Malcolm Pattinson, Cate Jerram, Kathryn Parsons, Agata McCormac and Marcus Butavicius, 'Why do some people manage phishing e-mails better than others?', *Information Management & Computer Security* 20, no 1 (2012), 18–28.

facilitate student activity had a significantly greater impact on the students' information security attitudes, practices, and awareness than those methods applying only video demonstrations.'[34]

Gamification is becoming more widespread and can be used in many areas, such as education.[35]

Several studies have attempted to define gamification, but according to the most accepted definition, 'gamification is the use of game design elements and game mechanics in non game contexts'[36] with the aim of making the study process more interesting and effective.[37]

Based on researches in this field of information security, it can be concluded that gamification has a place in security awareness.

Sam Scholefield and Lynsay A Shepherd identified that gamification and gamification techniques were useful methods of raising security awareness and participants enjoyed playing these types of applications and suggested that they increased their knowledge on password security.[38]

Melanie Volkamer et al. developed a game based smartphone app, named NoPhish, to educate people in accessing, parsing and checking URLs, that is, enabling them to distinguish trustworthy and non-trustworthy websites. The outcomes of their research is that 'NoPhish helps users make better decisions with regard to the legitimacy of URLs immediately after playing NoPhish as well as after some times has passed'.[39] Based on experience, the application was further developed and its effectiveness was measured by a pre- and post-test. The next study concluded that the 'effectiveness of "NoPhish" in increasing users' security awareness and the ability of detecting phishing URLs could be proven'.[40]

---

34 Antónia Szász and Gábor Kiss, 'Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra', *Információs Társadalom* 18, nos 3–4 (2018), 82–104.

35 Tamás Kovács and László Várallyai, 'Gamifikáció, avagy a játékosítás szerepe napjainkban', *International Journal of Engineering and Management Sciences* 3, no 3 (2018), 171–180; Richárd Fromann and Andrei Damsa, 'Digitális pedagógia – A gamifikáció (játékosítás) motivációs eszköztára az oktatásban', *Új Pedagógiai Szemle* 3–4 (2016), 76–81; Diána Pacsi and Zoltán Szabó, 'A gamifikáció fejlődése és a magyar gamifikációs trend alakulása', *Studia Mundi – Economica* 4, no 1 (2017), 57–68.

36 Adrián Domínguez, Joseba Saenz-de-Navarrete, Luis de-Marcos, Luis Fernández-Sanz, Carmen Pagés and José-Javier Martínez-Herráiz, 'Gamifying learning experiences: Practical implications and outcomes', *Computer & Education* 63, no 1 (2013), 380.

37 Sebastian Deterding, Dan Dixon, Rilla Khaled and Lennart Nacke, 'From game design elements to gamefulness: defining gamification', in *Proceedings of the 15th International Academic MindTrek Conference,* 2011, 9–15; Fromann and Damsa, 'Digitális pedagógia', 76.

38 Sam Scholefield and Lynsay A Shepherd, 'Gamification Techniques for Raising Cyber Security Awareness', in *HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science,* ed. by Abbas Moallem (Cham: Springer, 2019), 191–203.

39 Gamze Canova, Melanie Volkamer, Clemens Bergmann and Roland Borza, 'NoPhish: An Anti-Phishing Education App', *International Workshop on Security and Trust Management,* 2014; Gamze Canova, Melanie Volkamer, Clemens Bergmann and Benjamin Reinheimer, 'NoPhish App Evaluation: Lab and Retention Study', *Workshop on Usable Security,* 2015.

40 Alexandra Kunz, Melanie Volkamer, Simon Stockhardt, Sven Palberg, Tessa Lottermann and Eric Piegert, 'NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks', in *Informatik 2016,* ed. by Heinrich C Mayr and Martin Pinzger (Bonn: Gesellschaft für Informatik e.V., 2016), 509.

3.3. Communication channels

The information security message can be disseminated through a number of different communication channels including formal and informal one-to-one communication, meetings with groups of employees, official correspondence such as letters, e-mails, telephone conversations, communication through discussion groups or chatting with individuals via internet. According to Sajjad ur Rehman et al., face-to-face communication is the most effective medium. The richest of these forms of communication is the one-to-one interaction.[41] We can also use corporate events (conferences, seminars, internal company meetings, road shows) as they can have a positive security influence to the persuasion process. We should attempt to use such methods as campaigns, newsletters, screensavers, DVDs, PR films or videos, trinkets, brochures and flyers to raise users' awareness.[42]

In summary, the following interpersonal, group and mass communication methods can be used in the awareness program:[43]

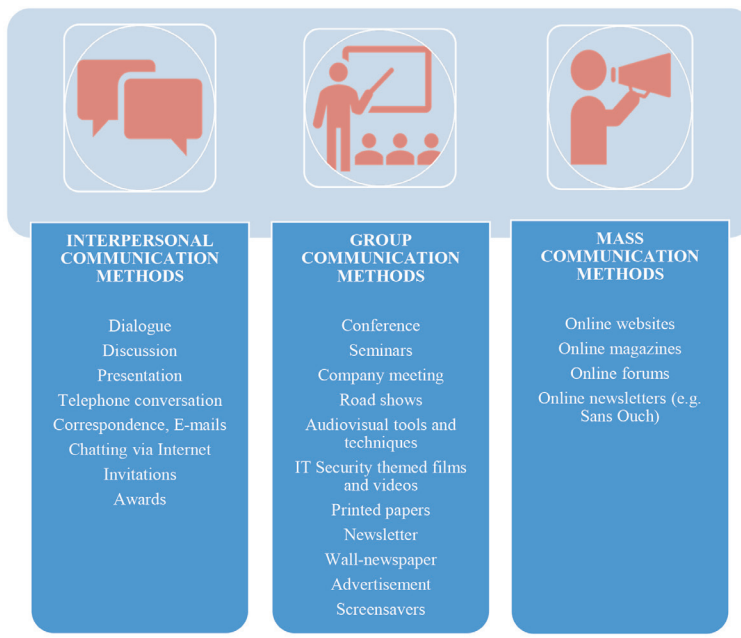

Figure 4 • *Communication channel, methods and tools (Source: Legárd, 'Célpont vagy!', 100–101.)*

41 Sajjad ur Rehman and Laila Marouf, 'Communication Channels and Employee Characteristics: An Investigation', *Singapore Journal of Library & Information Management* 37 (2008), 20–21.

42 Prah et al., 'The Perceived Effectiveness', 63; Parsons et al., *Human Factors and Information Security,* 32–33.

43 Legárd, 'Célpont vagy!', 99–101.

The language and communication should be understandable, visible and should avoid jargon and technical terminology. The program must be easy to use for all users on each level.[44]

It is very important to use marketing-oriented messages and the basic persuasion techniques such as: fear, humour, expertise, repetition, intensity and scientific evidence to seize attention, to establish credibility and trust, and to motivate action.[45]

The table below gives a concise evaluation of the matter.

Table 2 • *Summary table (Source: Compiled by the author.)*

Focus area		
Password usage and protection	Trainings on safe behaviour e.g. password safe keeping (E-learning/face-to-face)	Conferences Company meeting Seminars
	Gamification Applications	Newsletter
	Themed videos (from decrypter programs)	Seminars, road show
	Handout, posters,[46] screen savers[47]	(online) newsletter, wall-newspaper, online websites
	Password simulator	Seminars, road show
E-mail	Training (E-learning/face-to-face)	Conferences Company meeting Seminars
	Gamification applications[48]	Newsletter
	Handout, posters[49]	(online) newsletter, wall-newspaper, online websites
	Themed videos[50]	Seminars, road show, newsletter
	In case of suspicious/phishing e-mail	Dialogue (face-to-face/telephone conversation/e-mail)
	Phishing simulation – Simulate an attack via e-mail	Seminars, road show Test all employee

44 Tsohou et al., 'Implementation challenges'; Parsons et al., *Human Factors and Information Security,* 4.

45 Peltier, 'Implementing an Information Security Awareness Program'; Hansche, 'Designing a Security Awareness Program'; Maeyer, 'Setting up an Effective Information Security Awareness Programme'; Tsohou et al., 'Implementation challenges'; Maria Bada, Angela M Sasse and Jason R C Nurse, 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?', *International Conference on Cyber Security for Sustainable Society,* 2015, 5.

46 For details see www.ncsc.gov.uk/information/infographics-ncsc; www.kaspersky.com/blog/infographic-password-protection/1446/; www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

47 For details see www.enisa.europa.eu/media/multimedia/material

48 For example NoPhish App: Kunz et al., 'NoPhish: Evaluation'; 'Zero Threat' app: https://leolearning.com/leo-grc-academy

49 For details see https://nki.gov.hu/wp-content/uploads/2019/07/NKI_tajekoztato_a_spamakrol.pdf; www.itgovernance.co.uk/minimise-phishing-infographic; www.trendmicro.com/vinfo/us/security/news/cyber-attacks/spear-phishing-101-what-is-spear-phishing

50 For details see www.enisa.europa.eu/news/enisa-news/ecsm-2020; https://cybersecuritymonth.eu/press-campaign-toolbox/material/videos/clip6

Focus area		
Internet	Training (E-learning/face-to-face)	Conferences Company meeting Seminars
	Gamification applications[51]	Newsletter
	Handout, posters[52]	(online) newsletter, online websites, wall-newspaper, online websites
	In case of incident	Dialogue (face-to-face/telephone conversation/e-mail)
	Themed films and videos[53]	(online) Newsletter
Social media websites	Training (E-learning/face-to-face)	Conferences Company meeting Seminars
	Gamification applications	Newsletter
	Handout, posters[54]	(online) newsletter, online websites
	Screen savers	
Mobile equipment	Training (E-learning/face-to-face)	Conferences Company meeting Seminars
	Gamification applications[55]	Newsletter
	Handout, posters[56]	(online) newsletter, online websites
	Screen savers	
Data and information handling	Training (E-learning/face-to-face)	Conferences Company meeting Seminars
	Gamification applications[57]	Newsletter
	Handout, posters[58]	(online) newsletter, wall-newspaper
	In case of data privacy incident	Dialogue (face-to-face/telephone conversation/e-mail)
	Themed films and videos[59]	(online) newsletter
	Screen savers	
Incident reporting	Handout	Newsletter, wall-newspaper
	In case of incident	Dialogue (face-to-face/telephone conversation/e-mail)

51 No Phish App, Zero Threat app, Keep tradition secure app: https://keeptraditionsecure.tamu.edu

52 For details see www.interpol.int/Crimes/Financial-crime/Financial-crime-don-t-become-a-victim; www.enisa.europa.eu/topics/wfh-covid19/media/copy_of_infographic-cyber-seure-ecommerce/view

53 For details see www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats

54 For details see https://usa.kaspersky.com/resource-center/infographics/social-networking-dangers; www.sans.org/security-awareness-training/resources/posters/creating-cyber-secure-home

55 Keep tradition secure app.

56 For details see www.europol.europa.eu/publications-documents/mobile-malware-infographics; https://news.sophos.com/en-us/2013/12/19/infographic-anatomy-of-a-hacked-mobile-device

57 Zero Threat app; Keep tradition secure app.

58 For details see www.consilium.europa.eu/en/infographics/data-protection-regulation-infographics; www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data

59 For details see www.kaspersky.com/resource-center/definitions/data-breach

In all incidents or suspicious cases, the most important is the continuous communication with the user by phone, e-mail or by personal contact providing them with personal feedback.

Always use audiovisual tools and case studies for training and conferences and seminars for illustration and better understanding.

4. CONCLUSION

It is important to keep in mind that users are the first targets of social engineering attacks, so the human factor is the first line of defence against security threats. Therefore, security awareness programs are one of the greatest defences.

The aim of this study is to provide useful assistance for organisations in developing information security awareness programs that ensure an effective transfer of information security knowledge. The paper emphasises that if the users have adequate skills to detect, prevent and resolve breaches or incidents, the program can prevent and mitigate security threats and risks that an organisation might face.

This practical guide provides an overview on a scientific basis of the threats and focus areas that the program should be concerned with and details the risks in each area. Because the information security message can be disseminated through a number of different methods, the research compares traditional awareness programs with modern trainings and reviews effective solutions such as gamification techniques and applications. The study demonstrates that it is important to make any awareness program interesting and up to date to positively affect the behaviour and attitudes of employees towards information security.

The program needs to be understandable and meaningful to the users and should avoid jargon and technical vocabulary. The essay systematises the communication channels according to the level of communication, presents the personal, group and mass communication methods and tools.

The study also gives a comprehensive picture set of all the threats (focus areas), corresponding with useful training methods and communication channels.

The conclusion is that each organisation should develop and implement an awareness program focusing on their own specificities and needs, especially on their threats and risks. In order to realise a safety-conscious organisational culture through individual safety awareness, the program has to use repetition and transfer the main message using multiple techniques and communication channels.

REFERENCES

1. Abawajy, Jemal H, 'User preference of cyber security awareness delivery methods'. *Behaviour & Information Technology* 33, no 3 (2014), 1–12. Online: https://doi.org/10.1080/0144929X.2012.708787
2. *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.* Brussels: NATO Public Diplomacy Division, 2010. Online: www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf
3. AJP-3.10 Allied joint doctrine for information operations, NATO/PfP unclassified publication, 2009. Online: https://info.publicintelligence.net/NATO-IO.pdf
4. Aldawood, Hussain and Geoffrey Skinner, 'Challenges of implementing training and awareness programs targeting cyber security social engineering', in *2019 Cybersecurity and Cyberforensics Conference (CCC).* Melbourne, 2019, 111–117. Online: https://doi.org/10.1109/CCC.2019.00004
5. Aldawood, Hussain and Geoffrey Skinner, 'Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues'. *Future Internet* 11, no 3 (2019), 1–16. Online: https://doi.org/10.3390/fi11030073
6. Bada, Maria, Angela M Sasse and Jason R C Nurse, 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?' *International Conference on Cyber Security for Sustainable Society,* 2015, 1–11.
7. Bulgurcu, Burcu, Hasan Cavusoglu and Izak Benbasat, 'Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness'. *MIS Quarterly* 34, no 3 (2010), 523–548. Online: https://doi.org/10.2307/25750690
8. Canova, Gamze, Melanie Volkamer, Clemens Bergmann and Roland Borza, 'NoPhish: An Anti-Phishing Education App'. *International Workshop on Security and Trust Management,* 2014. Online: https://doi.org/10.1007/978-3-319-11851-2_14
9. Canova, Gamze, Melanie Volkamer, Clemens Bergmann and Benjamin Reinheimer, 'NoPhish App Evaluation: Lab and Retention Study'. *Workshop on Usable Security,* 2015. Online: https://doi.org/10.14722/usec.2015.23009
10. Chen, Charlie C, B Down Medlin and R S Shaw, 'A cross-cultural investigation of situational information security awareness programs'. *Information Management & Computer Security* 16, no 4 (2008), 360–376. Online: https://doi.org/10.1108/09685220810908787
11. 'COVID-19 Cybercrime Analysis Report', August 2020. Online: www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
12. 'Cyber defence', 23 May 2019. Online: www.nato.int/cps/en/natohq/topics_78170.htm
13. Deterding, Sebastian, Dan Dixon, Rilla Khaled and Lennart Nacke, 'From game design elements to gamefulness: defining gamification', in *Proceedings of the 15th*

International Academic MindTrek Conference, 2011, 9–15. Online: https://doi.org/10.1145/2181037.2181040
14. Domínguez, Adrián, Joseba Saenz-de-Navarrete, Luis de-Marcos, Luis Fernández-Sanz, Carmen Pagés and José-Javier Martínez-Herráiz, 'Gamifying learning experiences: Practical implications and outcomes'. *Computer & Education* 63, no 1 (2013), 380–392. Online: https://doi.org/10.1016/j.compedu.2012.12.020
15. ENISA, 'A new users' guide: how to raise information security awareness', 2008. Online: www.enisa.europa.eu/publications/archive/copy_of_new-users-guide
16. 'ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected', 20 October 2020. Online: www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020
17. Fromann, Richárd and Andrei Damsa, 'Digitális pedagógia – A gamifikáció (játékosítás) motivációs eszköztára az oktatásban'. *Új Pedagógiai Szemle* 3–4 (2016), 76–81.
18. Hansche, Susan, 'Designing a Security Awareness Program: Part I'. *Information Systems Security* 9, no 6 (2001), 14–23. Online: https://doi.org/10.1201/1086/43298.9.6.20010102/30985.4
19. IOCTA, 'Internet Organised Crime Threat Assessment (IOCTA) 2020', 05 October 2020. Online: www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
20. Kovács Tamás and László Várallyai, 'Gamifikáció, avagy a játékosítás szerepe napjainkban'. *International Journal of Engineering and Management Sciences* 3, no 3 (2018), 171–180. Online: https://doi.org/10.21791/IJEMS.2018.3.14.
21. Kruger, Hennie A and Wayne D Kearney, 'A prototype for assessing information security'. *Computers & Security* 25, no 4 (2006), 289–296. Online: https://doi.org/10.1016/j.cose.2006.02.008
22. Kunz, Alexandra, Melanie Volkamer, Simon Stockhardt, Sven Palberg, Tessa Lottermann and Eric Piegert, 'NoPhish: Evaluation of a web application that teaches people being aware of phishing attacks', in *Informatik 2016,* ed. by Heinrich C Mayr and Martin Pinzger. Bonn: Gesellschaft für Informatik e.V., 2016, 509–518.
23. Lacey, David, *Managing the Human Factor in Information Security. How to Win Over Staff and Influence Business Managers.* Wiley, 2009.
24. Legárd, Ildikó, 'Building an Effective Information Security Awareness Program', in *Central and Eastern European EDem and EGov Days 2020,* ed. by Thomas Hemker, Robert Müller-Török, Alexander Prosser, Dona Scola, Tamás Szádeczky and Nicolae Urs. Wien: Österreichische Computer Gesellschaft, 2020, 189–200. Online: https://doi.org/10.24989/ocg.338.15
25. Legárd, Ildikó, 'Célpont vagy! – A közszolgálat felkészítése a kiberfenyegetésekre'. *Hadmérnök* 15, no 1 (2020), 91–105. Online: https://doi.org/10.32567/hm.2020.1.7
26. Maeyer, David D, 'Setting up an Effective Information Security Awareness Programme', in *ISSE/SECURE 2007 Securing Electronic Business Processes Highlights*

of the Information Security Solutions Europe/SECURE 2007 Conference (part 1), 2007. Online: https://doi.org/10.1007/978-3-8348-9418-2_5

27. Nemeslaki, András and Péter Sasvári, 'Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában'. *Infokommunikáció és Jog* 4, no 60 (2014), 169–177.
28. Pacsi Diána and Zoltán Szabó, 'A gamifikáció fejlődése és a magyar gamifikációs trend alakulása'. *Studia Mundi – Economica* 4, no 1 (2017), 57–68. Online: https://doi.org/10.18531/Studia.Mundi.2017.04.01.57-68
29. Parsons, Kathryn, Agata McCormac, Marcus Butavicius and Lael Ferguson, *Human Factors and Information Security: Individual, Culture and Security Environment.* Published by Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh South Australia, 2010, 54. Online: https://apps.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf
30. Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson and Cate Jerram, 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)'. *Computers & Security* 42 (2014), 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003
31. Pattinson, Malcolm, Cate Jerram, Kathryn Parsons, Agata McCormac and Marcus Butavicius, 'Why do some people manage phishing e-mails better than others?' *Information Management & Computer Security* 20, no 1 (2012), 18–28. Online: https://doi.org/10.1108/09685221211219173
32. Peltier, Thomas R, 'Implementing an Information Security Awareness Program'. *Information Systems Security* 14, no 2 (2005), 37–48. Online: https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6
33. Prah, Abigail N W, Angela A Otchere and Kojo E Opan, 'The Perceived Effectiveness of Information Security Awareness'. *Information and Knowledge Management* 6, no 7 (2016), 62–73.
34. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), Article 10 Awareness-raising and education. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC
35. Rehman, Sajjad ur and Laila Marouf, 'Communication Channels and Employee Characteristics: An Investigation'. *Singapore Journal of Library & Information Management* 37 (2008), 13–43.
36. Scholefield, Sam and Lynsay A Shepherd, 'Gamification Techniques for Raising Cyber Security Awareness', in *HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science,* ed. by Abbas Moallem. Cham: Springer, 2019, 191–203. Online: https://doi.org/10.1007/978-3-030-22351-9_13
37. 'Shaping Europe's Digital Future', 2020. Online: https://doi.org/10.2759/091014

38. Siponen, Mikko T, 'A conceptual foundation for organizational information security awareness'. *Information Management & Computer Security* 8, no 1 (2000), 31–41. Online: https://doi.org/10.1108/09685220010371394
39. Stephanou, Tony and Rabelani Dagada, 'The impact of security awareness training on information security behaviour: The case for further research', in *Proceedings of the ISSA 2008 Innovative Minds Conference, ISSA 2008,* Gauteng Region (Johannesburg), 2008, 1–22.
40. Szász, Antónia and Gábor Kiss, 'Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra'. *Információs Társadalom* 18, nos 3–4 (2018), 82–104. Online: https://doi.org/10.22503/inftars.XVIII.2018.3-4.4
41. 'The EU's Cybersecurity Strategy in the Digital Decade', 16 December 2020. Online: https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade
42. Tsohou, Aggeliki, Maria Karyda and Ramzi El-Haddadeh, 'Implementation challenges for information security awareness initiatives in e-government'. *ECIS 2012 Proceedings,* 2012.
43. Veseli, Ilirjana, *Measuring the Effectiveness of Information Security Awareness Program*. M. S. thesis, Gjøvik: Gjøvik University College, 2011, 87. Online: www.semanticscholar.org/paper/Measuring-the-Effectiveness-of-Information-Security-Veseli/4105e146d3e0d13afe62960db6f1157722d824c9
44. Wilson, Mark and Joan Hash, *Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD: National Institute of Standards and Technology, 2003. Online: https://doi.org/10.6028/NIST.SP.800-50

Ildikó Legárd is currently a PhD student at the University of Public Service, Doctoral School of Public Administration Sciences in Budapest. She is an electronic information security manager in the public service. She graduated in history at Eötvös Lóránd University, Faculty of Humanities in 2004. In 2018, she qualified as an expert of public administration with specialisation in public management at the National University of Public Service, Faculty of Public Governance and International Studies. She has more than sixteen years of administrative experience, of which she has been specifically engaged in electronic information security for the past eight years. Her research focuses on the challenges of cyber security in public service with a particular attention on its human aspects, the development of users' information security awareness, and the scope and methodological criteria of awareness. She is interested in cyber warfare, too. She is on the register of program qualification experts of the University of Public Service and IT security expert for the "Angels of IT Security" self-development channel created within the Probono portal.