AARMS Vol. 21, No. 2 (2022) 5–14.

10.32565/aarms.2022.2.1

Recommendations for Safety-Conscious Smart Device Use by Military Professionals

Marco KOLLER[1]

Security-conscious behaviour is of paramount importance, both in the field of information security and in various public institutions. Thus, in the public administration, especially in the various armed bodies, the training of personnel in this direction is of strategic importance, as a person with low security awareness can endanger the security of the entire organisation. Human security issues may even have national security or intelligence relevance.

Keywords: *information security, smart devices, awareness, SWOT analysis, game theory*

Introduction

The internet has played a major role in globalisation, with everything available at the click of a mouse. In addition to the above, smart devices are another major contributor to this process. As these devices become more widespread and become an integral part of our daily lives, service providers, companies, governments and others can extract useful information about a person or group of persons. The significance of cyberspace from a military perspective is best illustrated by the fact that NATO officially declared it an operational area at the Warsaw Summit in 2016, thus making it an area of not only security importance for the subject, but also an area of national security challenges for states.

At the intersection of the interests and the certainty of the individual and the state are the general security in cyberspace of public organisations, public administrations and, in particular, of those working in the fields of defence and law enforcement, and their presence as users in everyday life. The European Court of Human Rights has also ruled that it is now difficult to separate private and professional life, so that the monitoring of behaviour and communications in the workplace necessarily involves an intrusion into the private lives of the individuals concerned.[2] This is particularly true when a person working in a public administration carries out some of his or her private and work-related online

[1] PhD student, University of Public Service, Doctoral School of Military Sciences, e-mail: marcoakoller@gmail.com

[2] Emberi Jogok Európai Bírósága: C-222/20. sz. ügy: Az előzetes döntéshozatal iránti kérelemről a Bíróság eljárási szabályzata 98. cikkének (1) bekezdése alapján készített összefoglalás.

activities on the same smart device. Some applications, be it social networking sites, news sites, video-sharing sites, maps, ask for access to various data: the contact details of all our partners, who we communicate with, how long and how regularly, our text messages and emails, our location when using GPS. If such data is accessed by an individual or organisation with malicious intent, they can use it to map workplace relationships within an organisation, potentially gaining access to sensitive information. In addition to the above, an application that can be installed on a device may even contain a virus of some kind, allowing hackers to take control of the phone. The article will provide recommendations for military professionals (a term that will be defined later) to protect not only general user security, but also the security of their own organisation.

The aim of the research

The aim of this publication is to present, based on interviews with experts in the fields of information security, data security, security awareness and IT, the most learnable user standards that will enable people beyond the average user, and those who choose to work in the military professional world, to live their daily lives more securely, thus protecting their own organisations in the world of smart devices.

Research methodology

In addition to the international and national literature and legislation, the publication is based on an interview already published[3] in the international literature, which has been restructured to suit the author's research. The answers to the questions were evaluated through logical analysis and levelling and in a planned way, based on a SWOT analysis.

Conceptual background

SWOT analysis

The term SWOT is an acronym formed from the initials Strengths, Weakness, Opportunity and Threats. SWOT analysis is a strategic planning tool used to assess the strengths, weaknesses, opportunities and threats of a focus of study. In conducting a SWOT analysis, in addition to identifying the individual factors, it is equally important to identify the relationship between the factors and how they are interrelated.[4]

---

[3] Flynn Wolf et al.: An Empirical Study Examining the Perceptions and Behaviours of Security-Conscious Users of Mobile Authentication. *Behaviour and Information Technology,* 37, no. 4 (2018). 320–334.

[4] Pató Gáborné Dr. Szűcs Beáta et al.: Beszállító értékelés vizsgálata SWOT analízis segítségével. *Vállalkozás-fejlesztés a XXI. században,* 6 (2016). 253–270.

Military professional

For the purposes of this study, the definition of the military professional (hereinafter: professional) is best defined as a soldier in the Penal Code. For the purposes of this Act, a soldier is a member of the Hungarian Defence Forces, the police, the Parliamentary Guard, the prison service, the professional disaster management service and the civilian national security services.[5]

In other words, the group presented in the present study is the law enforcement agencies, the professional staff of the Hungarian Defence Forces and the staff of the Military National Security Service. However, given that the research presents a general security awareness recommendation based on expert interviews, the research can also be applied to other government sectors or general users. Furthermore, the advantages and disadvantages of security awareness are outlined based on the SWOT analysis.

Information security

By information security, we mean the requirements and knowledge that cover both the technical-technological background and the management systems.[6] Basically, three categories can be identified in information security:

- physical protection
- logical protection
- human security, administrative protection

For the purpose of this study, physical protection, which refers to signalling systems, live systems, mechanical protection, etc., and *logical protection*, which refers to the protection of an electronic information system by means of information technology tools and procedures, are not highlighted.[7] The *administrative protection* which includes regulations and education is the basis of my present research, this study can be included in the interpretative framework of administrative protection so to speak. In other words, the focus should be on protection by strengthening the human factor, by strengthening the 'weakest' link, so to speak, and by reflexively inculcating security-conscious behavioural elements that can contribute to a higher level of information security.

Security awareness

There is no universally accepted concept of security awareness, but several Hungarian and international studies have attempted to define its components. Some authors emphasise

---

5 Paragraph (1) of Article 127 of Act C of 2012 on the Criminal Code.

6 A Nemzeti Elektronikus Információbiztonsági Hatóság.

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

the individual aspects of the concept.[8] Others emphasise the organisational aspects of the concept, with information security awareness being part of the culture of the organisation, a way of thinking and behaviour that ensures that employees of organisations recognise the legitimacy of security measures out of commitment, comply with them and communicate and enforce them to others.[9] According to Legárd, awareness does not follow from the knowledge of the user, but is a learned behaviour, a set of rules in which the user limits his/her own actions when using different IT systems, in this case smart devices.[10] It can be concluded from the above that training is a prerequisite for this kind of awareness.

Information security concerns of professionals

The importance of security-conscious user behaviour is almost beyond doubt. For general users, i.e. ordinary citizens, security awareness is also of explicit relevance, if only to protect their own data and values. In addition, particular attention should be paid to strengthening the security-conscious behaviour of professional staff, as defined in the study, since the various data belonging to these individuals or to representatives of other public bodies may be of extreme importance to certain public or non-public actors. Therefore, security-conscious user behaviour is important, and it is necessary to be selective about the type of access that certain applications grant. In some cases, the malicious intent behind the application is conscious, in others it is not so easy to judge, but it can be telling if a flashlight application requests access to our GPS coordinates, phone book and so on.[11] However, in many cases even realistic requests for permission can be risky, as in the case of a fitness app used for running, it is realistic if it wants to collect our real-time location data. However, it was just such an app that accidentally revealed the secret location of some U.S. military bases, as the soldiers stationed there were also using the app, so that the location of objects in 'no man's land' could be easily identified based on the running workouts they did on and around the base.[12]

The emphasis on security consciousness is also important because, although a public organisation can spend billions on securing its internal network, put in place the necessary physical and logical protection, and even within the administrative protection, put in place the regulations to ensure its own information security, if it is not accompanied by a sufficiently prepared human resource, there will always be a 'gap in the shield'. However, it is important that successful and effective security awareness programmes are put in place so that security conscious behaviour becomes a normal part of everyday life for professionals.

---

8 Ildikó Legárd: Célpont vagy! – a közszolgálat felkészítése a kiberfenyegetésekre. *Hadmérnök,* 15, no. 1 (2020). 95.

9 Legárd (2020): op. cit.

10 Legárd (2020): op. cit.

11 Péter Bányász: Az okos mobil eszközök biztonsága. *Hadmérnök,* 13, no. 2 (2018). 360–377.

12 Pál Fehér-Polgár – Pál Michelberger: A sajáttulajdonú mobil eszközök információbiztonsági kockázatai. *International Journal of Engineering and Management Sciences,* 3, no. 4 (2018). 176–185.

According to Legárd, it is also important for the government to maintain a high level of security awareness, because if citizens feel safe, they can live their lives more efficiently, pay their taxes and fulfil their obligations as a sign of satisfaction.[13] Following the above logic, a high level of security awareness among public employees, and specifically among professionals is a priority for the State.

Analysis of expert interviews

When selecting the interviewees, it was important to interview experts from several fields, due to the interdisciplinary nature of the topic, in order to get a more comprehensive picture of the safe use of smart devices by general users. Therefore, we selected experts from the fields of IT, data security and caution. Based on the above, written interviews were conducted with six experts, taking into account the pandemic situation caused by Covid-19.

- *Dr. Atilla András Péterfalfvi* – National Authority for Data Protection and Freedom of Information, President
- *Veronika Koncz* – Constitution Protection Office – Security Awareness Expert
- *Lénárd Zsákai* – Ministry of the Interior, Department of European Cooperation, Senior Specialist, Székely Family Ltd., Security Research and Proposals Coordinator
- *Zoltán Székely* – Székely Family Kft., Co-Founder, Information Security Expert
- *András József Üveges* – Defence Systems Designer (MsC), PhD in Defence Electronics
- *István Ilia* – Arxadoris Ltd., Managing Director, IT Expert

The interview questions were sent to me by Professors Flynn Wolf and Ravi Kuber, which were adapted to the specifics of this research, as I mentioned above. The questionnaire covered the following topics. In total, 23 questions were asked in the written interviews and, in addition, the experts briefly described their attachment to the topic and their professional background.

Questions about owning smart devices

All experts own some kind of smart device, the most common being the smart phone or tablet. The majority of experts (four out of six) use IOS on their smart phones, but some versions of Android were also mentioned. In the case of the other systems outlined, it seemed to me that they require a higher level of IT expertise than a simple user-friendly IOS system. The choice of those using a plain Android system tended to be based on familiarity and convenience, while the choice of those using an IOS system was mostly driven by higher security and lower vulnerability. These results suggest that for a simple user choice, it may be more appropriate to choose IOS without IT knowledge.

[13] Legárd (2020): op. cit.

Questions about security authentication

In the case of the issues raised in this topic, the answers of the experts varied, with two cases of dual authentication in addition to simple password authentication, of which two cases of preference for biometric identification were highlighted. Based on the above and the available literature, the dual authentication mechanism, which provides the highest level of security, does not impose a significant additional burden on the average user in everyday life and its everyday use may be recommended. The responses clearly indicated that experts in the field of finance, i.e. banking and financial applications, clearly use separate authentication, which is different from what is commonly used. However, in terms of security awareness, the need for separate authentication for business-related logins, i.e. separate authentication procedures and codes for private and work-related authentication, was also raised. There were experts who use separate authentication (password) for each application. In case of a potential threat such as a device security authentication being copied by another person, the majority agreed that in such a case either the access code or the device itself would be replaced.

Based on the responses and the literature, it is certainly worthwhile to distinguish between corporate and private sector passwords and authentication methods, especially for the actors (professionals) targeted in the study.

Information and data security issues

From the experts' responses, it can be concluded that trusted authentication on mobile devices is definitely necessary, but that the storage of really sensitive data on such devices should be avoided. Opinions differ as to whether it is possible to guarantee full security, but the information available so far suggests that even with full security awareness, 100% security cannot be guaranteed, but can and should be strived for.

Experts believe that they are more security-aware than the average user, as evidenced by the fact that they have not been victims of identity theft, have not lost their smart devices, and know what steps to take to protect their personal data in the event of a security incident. A remarkable circumstance is that the experts who experienced a security incident in their immediate environment received a kind of impulse that encouraged them to further learning and higher security awareness. Thus, based on the conclusions drawn from the above, the presentation of such an act in the context of a security awareness lecture or an interactive case study could have a stimulating effect on the security awareness of users.

The definition of attitudes towards new technologies has arisen in the context of information and data security, because, while they offer many new and useful opportunities, they may also present risks. There is almost a basic consensus among the experts that they seek expert help for new technologies that they are not familiar with (except, of course, for those experts who work in the IT field, who carry out their own testing). The need to seek the views of other users was also raised. Based on the above experience, the most obvious solution for the average user, as well as for professionals, seems to be to develop a concept

for a new technology, be it a device or software, by browsing through various tech forums where both technology experts and user opinions are available.

This topic asked which generation might be the most security-conscious, whether there is a generational difference, given today's digital world. In most cases, expert opinion suggests that it is entirely individual as to who is security conscious. The majority of experts believe that Generation Y is the most security conscious because they are already at home and not so lost in the digital world, but there was some expert opinion that it is precisely because of the generational advantage in technical knowledge of digital nativity that the younger Generation Z is more security conscious.

User security awareness issues

This topic investigated whether security-conscious behaviour can have disadvantages that put individual users at a disadvantage. The experts were divided on this point, with some considering that there was no disadvantage to security consciousness, while others saw freedom as the price of informality. Another cardinal theme was the issue of raising awareness of security. The basic premise of this, according to the interviews, is that the only way to address information security challenges is to reduce the risk of the 'human factor', and the only way to do this is through awareness raising and sensitisation, which can contribute to prevention. Raising awareness should start by emphasising the importance of this. People must feel the importance of information security. The aim should be to develop basic habits and to make clear why users should be concerned about certain phenomena. Starting with the right registration for data security, continuing with the right settings, and then raising awareness of the risks inherent in daily use. Effectiveness could be greatly enhanced if users/population were to be familiarised with the concepts (at their own level) from an early age. Education should possibly start in the first grade of primary school, as these children already have smart devices. The above leads to the conclusion that education, which has a huge role to play, is clearly the key to developing good habits and habits of mind. In my opinion, it is also necessary for professionals to be given training and education in how to handle their own devices in a safety-conscious way in their everyday lives.

Analysis and presentation of strategic safety-conscious behaviour

Based on a SWOT analysis of the interviews with the experts, the following can be concluded about safety-conscious behaviour.

- Strengths: minimising risks, relatively cheap
- Weaknesses: comes at the price of freedom, does not provide full security
- Opportunities: education, training
- Threats: inattention, obsession, excessive suspicion

The aim of the expert interviews was to identify, through the experts' opinions and their own safety awareness behaviour, a form of behaviour, a strategy, as it were, and its development directions, which can be used by the professional and the public institution employing him/her, and which can also be used as a guide for other users.

From the above, it can be concluded that the strength of safety-conscious behaviour is that it is cheap and effective to minimise the risks arising from the use of smart devices. Considering that it does not require the creation of special software or other physical things, security awareness as a means of protection is considered cheap and not a special skill that cannot be learned, so its strengths include learnability.

A weakness is that it does not provide full protection, as it is not possible to fully comply with the measures required by the organisation and to train the professional if he or she is attacked by software and hardware outside his or her control. Furthermore, constant vigilance can lead to a lack of freedom for the user, or even to frustration or a loss of focus over time, which can result in an information security incident due to negligence.

An opportunity has been identified in the field of security awareness to organise different security awareness training and education, and within this, to organise training that is interactive and can create a deep impression, thus contributing to the shaping of specific security awareness mechanisms into skills.

One of the risks is that security awareness can give the user a feeling of being over-protected, which can lead to a loss of self-awareness, after which an information security incident can occur. A further risk is that training that is not interactive enough is not very effective, which only consumes the time of professionals and the money of the public organisation concerned.

Based on the above analysis, it is clear that there is a need for security awareness training, but in a way that the user can interpret it in depth, and also for reminder lectures to check compliance with the mechanisms taught, and in this direction, it may be useful for professional staff to have a non-routine, non-'bloody' check, with the assistance of the Military National Security Service and the National Defence Service, to provide feedback to staff. The interviews showed that it is important to keep abreast of new technologies and to constantly improve IT knowledge at user level, which can contribute to the conscious use of certain applications and tools and to increasing knowledge in this area.

Conclusions

Safety-conscious behaviour reduces various risks, but it does not provide complete protection. The emphasis on security awareness is important because even without adequate physical or logical protection, or even administrative protection, there can be a security deficit due to low security awareness among users.

It is important that effective safety awareness programmes are put in place to make safety-conscious behaviour a normal part of everyday life for professionals. The expert interviews suggest that programmes should be proactive, so that the awareness is embedded in the memory in a more tangible way. Self-training in this area is important,

as is the organisation of regular safety awareness lectures, both for ordinary citizens and professionals, and special attention should be paid to the second category.

This is also important for the government, as maintaining a high level of security awareness among professionals is of paramount importance, as building and maintaining awareness is one of the protective lines of defence of the state's sensitive infrastructure.

Safety awareness training should be interactive, aiming to develop this behaviour to a skill level.

Using dual authentication on your own device for different applications is useful. It is recommended to use different passwords for each application, specifically for business or private use.

References

Bányász, Péter: Az okos mobil eszközök biztonsága. *Hadmérnök*, 13, no. 2 (2018). 360–377.

Fehér-Polgár, Pál – Pál Michelberger: A sajáttulajdonú mobil eszközök információbiztonsági kockázatai. *International Journal of Engineering and Management Sciences*, 3, no. 4 (2018). 176–185. Online: https://ojs.lib.unideb.hu/IJEMS/article/view/5079

Glavanits, Judit: Az állami cselekvés játékelméleti megközelítése. In Csaba Svéhlik (ed.): *Paradigma- és stratégiaváltási kényszer a gazdaságban: VI.* Mór, KHEOPS, 2011. 135–142.

Kiss, Attila – Csaba Krasznay: A felhasználói viselkedéselemzés kiberbiztonsági előnyei és adatvédelmi kihívásai. *Információs Társadalom*, 18, no. 1 (2017). 55–71. Online: https://doi.org/10.22503/inftars.XVII.2017.1.4

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

Munk, Sándor: Információs szolgáltatásokat nyújtó hálózatok alapjai. *Hadmérnök*, 6, no. 2 (2011). 227–243.

Nagy, Tamás: *Játékelmélet.* Miskolc, Miskolci Egyetem, s. a. Online: www.uni-miskolc.hu/~matente/oktatasi%20tananyagok/JATEKELMELET.pdf

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

Szűcs, Beáta, Pató Gáborné, Dr. – Evelin Kopácsi – Barbara Kreiner: Beszállító értékelés vizsgálata SWOT analízis segítségével. *Vállalkozásfejlesztés a XXI. században*, 6 (2016). 253–270.

Wolf, Flynn – Ravi Kuber – Adam J. Aviv: An Empirical Study Examining the Perceptions and Behaviours of Security-Conscious Users of Mobile Authentication. *Behaviour and Information Technology*, 37, no. 4 (2018). 320–334. Online: https://doi.org/10.1080/0144929X.2018.1436591

Legal references

Act C of 2012 on the Criminal Code.

A Nemzeti Elektronikus Információbiztonsági Hatóság. Online: http://kifu.gov.hu/kifu/sites/default/files/NFM_Ibtv_NEIH_2013_12_18.pdf

Emberi Jogok Európai Bírósága: C-222/20. sz. ügy: Az előzetes döntéshozatal iránti kérelemről a Bíróság eljárási szabályzata 98. cikkének (1) bekezdése alapján készített összefoglalás. Online: https://curia.europa.eu/juris/showPdf.jsf;jsessionid=1F496C43E8E38F9528651BA20E9E028C?docid=228843&pageIndex=0&doclang=HU&mode=req&dir=&occ=first&part=1&cid=7613359