

Results upon two samples of university students on safety consciosness in smartphone usage

Pál Fehér-Polgár

Óbuda University, Keleti Károly Faculty of Business and Management,
feherpolgar.pal@kgk.uni-obuda.hu

Abstract: At the 2022 MEB conference I have shown my preliminary results from a research on safety consciosness in smartphone usage of university students. I have conducted research on a group of university students in spring 2022 with the repeated usage of a scientific questionnaire that I have created and used in 2016. In 2016 I have created a questionnaire and made a survey on the safety consciosness of the smartphone users in the group of university students and have shown my results in conference papers and have shown interesting results. This year I have repeated the survey on a different set of students in order to measure their safety consciosness and I will show the results in this paper. The groups differ in many points, thus we can not directly create a comparison of the results, but with the usage of literature review I will be able to show the current state of the topic. In this paper I will present my detailed results from the two groups, updated upon the feedback gathered at 2022 MEB conference.

Keywords: safety consciosness; university students' IT safety consciosness; DOSPERT; Modifeied DOSPERT questioner

1 Introduction

In 2022, we will be surrounded by modern technology at all levels. Smart devices in our hands, in our homes, in our cars.[2][4][7] We use them in our personal and professional lives.[9] They've played a prominent role before, but it was during the closures of pandemic COVID-19 that we were confronted again with how many areas of our lives these devices can help us to be.[6]

However, as in the other areas of life, we cannot ignore the issue of security.[5]

According to the European Union Agency for Network and Information Security [1] the top 3, high category risks for smartphone users are:

- Data leakage resulting from device loss or theft
- Unintentional disclosure of data.
- Attacks on decommissioned smartphones

In this research I have concentrated on the first two risk sources.

2 Methodology

In 2016, I composed a comprehensive study on smartphone usage patterns and their impact on safety. I developed a questionnaire in a multi-step process. I tested it on a small sample, modified it, and then used it on a larger sample.

2.1 Structure of the questionnaire

The questionnaire consists of 42 questions, of which I created a total of 87 variables for statistical processing. Question groups were:

- Demographic questions
- Smartphone usage
- Security related questions

In 2016, students from three faculties of Óbuda University (Bánki Donát Faculty of Mechanical and Safety Engineering, Kandó Kálmán Faculty of Electrical Engineering, Keleti Károly Faculty of Business and Management) formed my research sample and I have presented the detailed results in several scientific publications.

In the spring of 2022, I conducted a research with the reuse of this questionnaire again because I was curious to see how my current students would respond to this questionnaire.

3 Data and results

3.1 Limitations

My aim was to build a sample that would make the results comparable with previous results. But unfortunately, neither the sample size nor the proportion of groups in

the sample (in terms of gender, age and the degree course studied by the students) allow for a comparison of results without strong statistical constraints.

3.2 Findings

3.2.1 Software security awareness

All the answerers responded their phone that they mainly use is a smart phone.

Software usage behaviour of the answerers' is a crucial part of the usage of smartphones.[3] The respondents have answered that their phones are not rooted. Rooted operating systems could mean a higher level of risk of potential malware attacks. Thus this usage pattern can be translated as security aware usage. Also almost all the respondents (94%) answered that they are continuously updating their smartphones operating system and software.

Also I have asked about the sources of their installed applications. Again, almost every respondent (87%) answered they are using only the official sources (google play, app store, huawei appgallery, galaxy store...) for installing applications.

3.2.2 Security aware usage of the smart phone

I have asked 'Do you restrict the access to your phone in any way?'[4][5][8] 100% of the respondents has answered yes. Mainly they use screen locks with pin in most cases but many use biometric authentication with finger prints or Face ID. Only a very small fraction, 2 respondents answered that they use 2 factor authentication for their phones.

3.2.3 Security awareness of the used networks

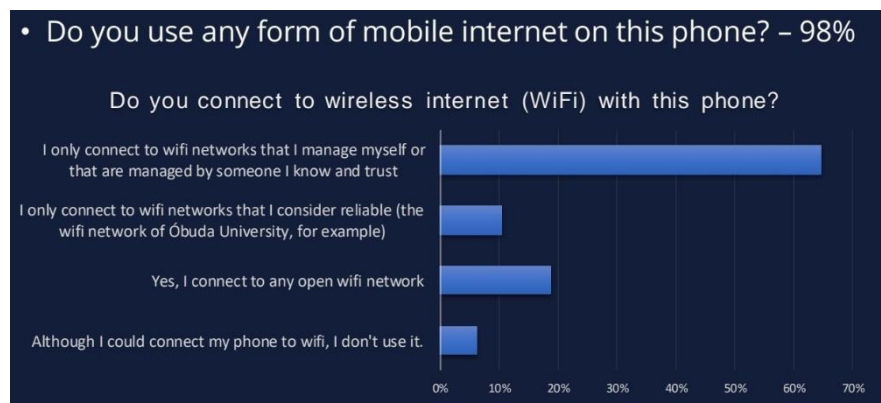


Figure 1.
Network usage of the answerers

3.2.4 Security awareness of the stored data



Figure 2.

Storing important data on the answerer's smartphone (source: own research)

In the questionair I have asked the answerers about the stored data on their smartphones. A high percentage of the answerers have answered yes, and they store a vide variety of data on their phones.

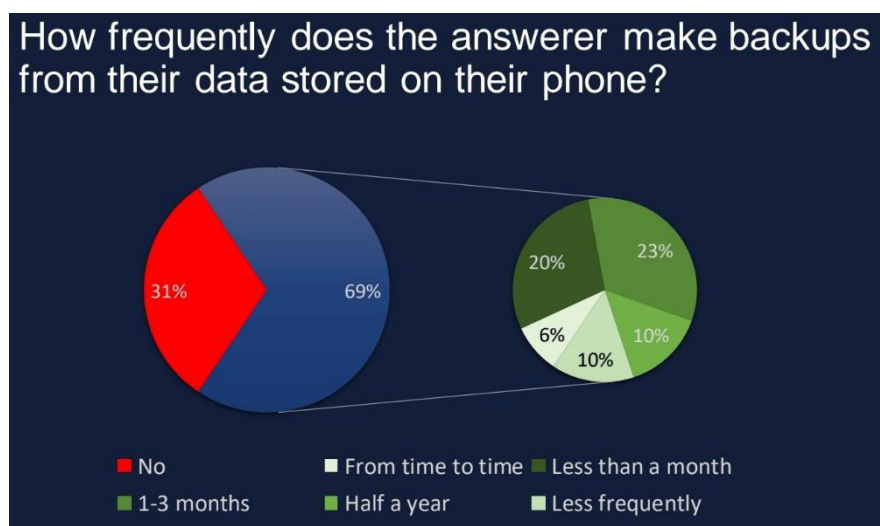


Figure 3.

Making backups from data stored on the answerer's smartphone (source: own research)

If we store data then it is a crucial question if they make backups from their data. Almost a third part of the respondents said they are not making any backups from their data stored on their smartphones.

Conclusions

Although direct comparison could not have been conducted between the samples, there can be seen some interesting outcomes from this research.

First of all the smartphone penetration has grown to 100% in the sample.

Although almost all the respondents have answered that they store important data on their smart phones their usage patterns still show possible risks for losing or compromising stored data.

References

- [1] enisa European Network and Information Security Agency. (2013) Top Ten Smartphone Risks. <https://web.archive.org/web/20120527090937/http://www.enisa.europa.eu/activities/application-security/smartphone-security-1/top-ten-risks> (Utolsó letöltés (webarchív-on archivált változattól) 2022. november 15.)
- [2] O. Dobos, I. M. Tóth, Á. Csiszárík-Kocsir, M. Garai-Fodor and L. Kremmer, "How Generation Z managers think about the agility in a world of digitalization," 2022 IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI), 2022, pp. 000207-000212, doi: 10.1109/SAMI54271.2022.9780683.
- [3] KESZTHELYI András, Paradigmaváltás - biztonság - emberi tényező, Taylor : gazdálkodás- és szervezéstudományi folyóirat , vol. 7, no. 1-2, pp. 406-412, 2015. http://acta.bibl.u-szeged.hu/36354/1/vikek_018_019_406-412.pdf
- [4] KESZTHELYI András, About passwords, Acta Polytechnica Hungarica , vol. 10, no. 6, pp. 99-118, 2013. DOI:10.12700/APH.10.06.2013.6.6 http://acta.uni-obuda.hu/Keszthelyi_44.pdf
- [5] Keszthelyi and P. Michelberger, "From the IT authorisation to the role- and identity management," 2012 4th IEEE International Symposium on Logistics and Industrial Informatics, 2012, pp. 173-178, doi: 10.1109/LINDI.2012.6319483.
- [6] K. Lazányi, "Generation Z and Y – are they different, when it comes to trust in robots?," 2019 IEEE 23rd International Conference on Intelligent Engineering Systems (INES), 2019, pp. 000191-000194, doi: 10.1109/INES46365.2019.9109508.
- [7] Lazányi, K., Vincze, A., & Szikora, P. (2021). The digital skills in the Hungarian higher education during the first wave of Covid-19. Higher education policies for developing digital skills to respond to the Covid-19 crisis: European and global perspectives, 4-18.

- [8] P. Szikora and B. Ali, "Information Security in the 21st Century - Smart Phones in Focus," 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), 2018, pp. 000255-000260, doi: 10.1109/SISY.2018.8524767.
- [9] Szikora, P., & Lazányi, K. (2022). The End of Encryption?—The Era of Quantum Computers. In *Security-Related Advanced Technologies in Critical Infrastructure Protection* (pp. 61-72). Springer, Dordrecht.