PASSWORD USAGE IN HUNGARY AND SLOVAKIA AMONG USERS OF SMART DEVICES

JELSZÓHASZNÁLAT MAGYARORSZÁGON ÉS SZLOVÁKIÁBAN AZ OKOSESZKÖZ HASZNÁLÓK KÖRÉBEN

MANDIĆ Dorottya[1] – KISS Gábor[2]

Abstract

The number of IoT devices is increasing and more and more people are buying different smart devices, but they do not know how to use them safely. That is why we thought it important to conduct a survey among smart device users, which examines what smart device users use in relation to password use. For example, do they use the same password in several places, how long are the symbols used, how often do they change their password, whether the password they use contains meaningful words or personal information and whether the password contains uppercase and lowercase letters, numbers and special characters. In addition, the survey also deals with showing how popular smart devices are among the participants in the survey in Hungary and Slovakia. The purpose of this study is to present the results of the survey conducted in Hungary and Slovakia among smart device users regarding the use of passwords.

Keywords

password, smart devices, security, IoT, password usage

Absztrakt

Egyre jobban nő az IoT eszközök száma, és egyre többen vásárolnak úgy okoseszközöket, hogy nem tudják hogyan kellene az okoseszközöket biztonságos használni. Ezért fontosnak gondoltunk elvégezni egy felmérést az okoseszköz használók körében, mely azt vizsgálja, hogy az okoseszköz használók a jelszóhasználatra vonatkozóan milyen jelszavakat használnak, például ugyan azt a jelszót használják-e több helyen, milyen hosszú a jelszavakat használnak, milyen gyakran változtatják meg a jelszót, a jelszó amit használnak tartalmaz-e értelmes szót vagy személyes információt, valamint, hogy a jelszó tartalmaz-e kis és nagybetűket számokat, speciális karaktereket. Ezen kívül a felmérés azzal is foglalkozik, hogy bemutatja, hogy Magyarországon és Szlovákiában a felmérésben résztvevők válaszai alapján mennyire népszerűek az okoseszközök. Jelen tanulmány Magyarországon és Szlovákiában végzett felmérés eredményeit szeretné bemutatni a jelszóhasználatra vonatkozóan az okoseszköz használók körében.

Kulcsszavak

jelszó, okoseszközök, biztonság, IoT, jelszóhasználat

[1] mandic.dorottya@uni-obuda.hu | ORCID: 0000-0002-3384-5590 | PhD Student, Óbuda University Doctoral School on Safety and Security Science| PhD hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola
[2] kiss.gabor@bgk.uni-obuda.hu | ORCID: 0000-0002-0447-937 | associated professor, Óbudai University|egyetemi docens, Óbudai Egyetem

INTRODUCTION

The use of smart devices has already become a part of our daily life and more and more people are using various smart devices in their everyday life [1]. Due to the rapid spread of IoT devices it is important to deal with the security of the devices [2], [3], [4]. Among the users there are smart device users who do not take measures to use smart devices more safely. For example ,,many people use a password that is weak and easy to guess." Since more complicated passwords would be much more difficult to remember so they often prefer a password that is easy to guess and that they do not forget [5], [6]. IoT devices often do not have strong passwords so they are vulnerable to attacks and even if users change the password, they often choose a password that is easy to guess [7].

According to Statista's report the five most used passwords for IoT devices in 2021 were ,,admin", ,,root", ,,nc11", ,,user" and ,,enable"[8]. Unfortunately, users often use their smart devices in their everyday life without having sufficient knowledge to be able to use their smart devices safely [9], [10], [11]. There are also smart device users who don't even change the default password, such as ,,123456" or use a password that contains meaningful words or personal information as their date of birth or the name of their favorite pet [12]. According to the NordPass report the most common password in 2019 was ,,12345", followed by ,,123456" in 2020-2021 and ,,password" in 2022 [13]. However, it may also happen that the same password is used in several places. Since this way they do not have to remember several passwords and it is enough to remember the given password. The use of simple passwords is not safe as they can be easily guessed, which attackers can easily take advantage of [14].

On the Security.org page we can see how long it takes to crack a password when passwords of different lengths and content are used [15]. According to Security.org, it takes 2 seconds to crack a 7-character password if it only contains ,,uppercase and lowercase letters" and numbers and if the password does not contain numbers, it takes even less time as 1 second is enough to crack the password. If the password contains both ,,uppercase and lowercase letters", numbers and symbols, 4 seconds are enough to crack the password. If the password contains 8 characters, as well as lower and uppercase letters, in this case 28 seconds are enough to crack the password. If the password contains ,,uppercase and lowercase letters" and numbers, 2 minutes are required. If the password also contains symbols, it takes 5 minutes to crack the password. However, according to Security.org's report, if the password we use contains at least 12 characters and the password contains upper and lower case letters, in this case, according to the report, 6 years may be necessary [16].

According to the Cybernews 2024 report passwords such as ,,123456", ,,123456789", ,,qwerty", ,,password" and ,,12345" were among the top five most used passwords worldwide. Despite the fact that we can find different suggestions on how and why it is important to use strong and unique passwords, as well as why it is recommended to use a password manager. Many people still use weak and easy-to-guess passwords, which even a novice cybercriminal can easily hack [17].

In this survey, we investigated the lengths of passwords that users use among smart device users in Hungary and Slovakia for example whether the password they use contains meaningful words and personal information and whether the password contains small and capital letters, numbers, and special characters and whether the same password is used in

several places. In the research, we looked for the answer to whether there is a difference between the two countries regarding the use of passwords among smart device users, especially when a meaningful word is used as a password.

RESEARH METHODOLOGY

In the research, we looked for the answer to whether there is a difference in the use of passwords between the two countries among smart device users especially if a meaningful word is used as a password. The study examines the password usage habits of smart device users in Hungary and Slovakia, whether smart device users use lower- and upper-case letters, numbers, special characters, personal data, meaningful words and whether they use the same password in several places, the length of the passwords and how often they change the password they use. This survey examines the password usage of smart device users. A total of 194 people in Hungary and Slovakia took part in the survey. The survey was conducted online in both countries and the data was analyzed using the SPSS statistical program. We used the Mann-Whitney U test, and we compared the differences in password usage according to gender in Hungarian and Slovakia.

THE RESULT OF THE SURVEY

A total of 194 people in Hungary and Slovakia took part in the survey. The survey was conducted online in Hungary and Slovakia. A total of 135 people participated in Hungary of which 107 were men (79.3%) and 28 were women (20.7%). A total of 59 people took part in the survey in Slovakia of which 25 were men (42.4%) and 34 were women (57.6%).

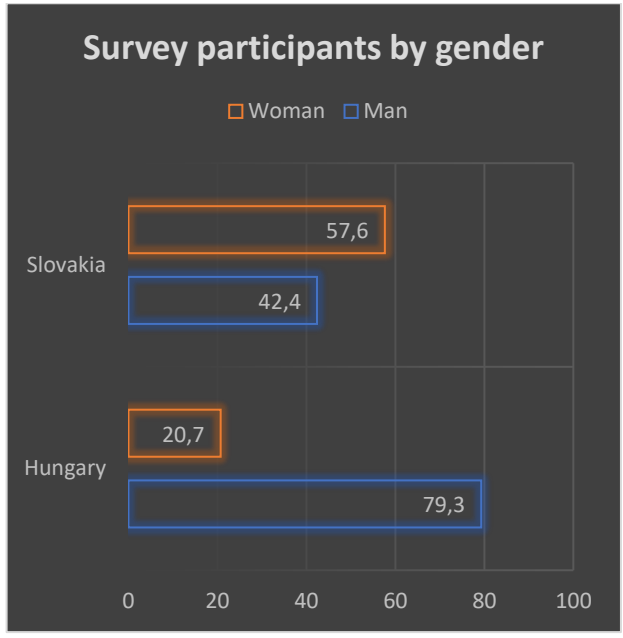

Figure 1: Shows the survey participants in Hungary and Slovakia by gender represented in a diagram. (Source:Created by the author)

On the (Fig.1) diagram, we can see that in Hungary more men took part in the survey than women and in Slovakia more women took part in the survey than men.

Age	Hungary		Slovakia	
	Freq.	**Perc.**	***Freq.***	**Perc.**
18-24 years old	100	74.1%	43	72.9%
25-34 years old	24	17.8%	9	15.3%
35-50 years old	11	8.1%	7	11.9%

Table 1: Age of survey participants in Hungary and Slovakia. (Source:Created by the author)

In (Table 1), we can see that among the participants in the survey in Hungary (74.1%) of the 18-24 year olds took part in the survey, (17.8%) of the 25-34 year olds and (8.1%) of the 35-50 year olds. In Slovakia (72.9%) of 18–24-year-olds participated in the survey (15.3%) of 25–34-year-olds and (11.9%) of 35–50-year-olds. We can see that the 18–24-year-old age group took part in the survey in both Hungary and Slovakia.

Education attainment	Hungary		Slovakia	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Elementary school	10	7.4%	0	0%
High School	82	60.7%	42	71.2%
College	28	20.7%	16	21.7%
University	10	7.4%	1	1.7%
Others	5	3.7%	0	0%

Table 2: Educational level of the participants in the survey in Hungary and Slovakia. (Source:Created by the author)

In Table 2, we can see that 10 (7.4%) of the participants in the survey answered that they had a primary school education 82 (60.7%) had a secondary school education and 28 (20.7%) answered that they had a college degree and 10 (3.7%) answered that they had a university degree and 5 (3.7%) answered that they had other degrees. In Slovakia 42 (71.2%) of the survey participants answered that they had high school education and 16 (21.7%) answered that they had college education and only 1 of the respondents (1.7%) answered that they have a university degree. In the survey, we also examined how many of the respondents who use smart devices have an IT degree in Hungary and Slovakia. Based

on the survey in Hungary (33.4%) answered that they had an IT degree and (66%) answered that they did not. In Slovakia (41.4%) of survey participants answered that they had an IT degree and (58.6%) answered that they did not. When asked whether the participants in the survey use smart devices, we can see in (Figure 2) that in Hungary (98.5%) answered that they use smart devices and only (1.5%) answered that they do not. In Slovakia (98.3%) of the participants in the survey answered that they use a smart device and (1.7%) answered no. We can see that based on the responses of the participants in the survey in Hungary and Slovakia more than 98% of the respondents answered that they use at least one smart device. Figure 2. shows how many of the survey participants answered that they use smart devices.

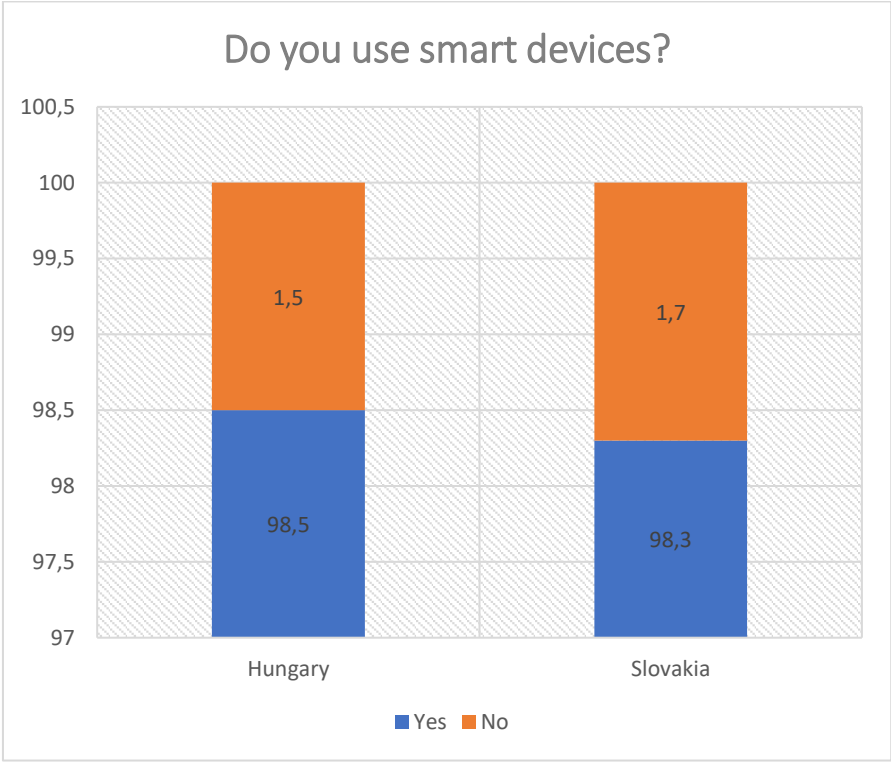

Figure 2: Based on the answers of the participants in the survey, whether they use smart devices in Hungary and Slovakia. (Source:Created by the author)

Smart devices use by gender	**Hungary**		**Slovakia**	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Man	106	79.7%	24	42.1%
Women	27	20.3%	33	57.9%

Table 3: Smart device users by gender in Hungary and Slovakia. (Source:Created by the author)

If we look at the number of people who answered that they use smart devices by gender, then based on the survey in (Table 3), we can see that in Hungary 106 of the men (79.7%) answered that they use smart devices and 27 of the women (20.3%) answered that they use reasoning tools based on the survey. In Slovakia based on the survey 24 (42.1%) of the men and women 33 (57.9%) answered that they use smart devices.

How long is the password that you use?	**Hungary**		**Slovakia**	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Less than 8 characters.	4	3%	27	45.8%
8-10 characters.	71	53.4%	0	0%
12 or more characters.	58	43.6%	31	52.5%

Table 4: The answers of the participants in the survey about what long passwords are used in Hungary and Slovakia. (Source:Created by the author)

In (Table 4.), we can see that in Hungary 4 (3%) of the participants in the survey answered that they use less than 8 characters as a password, 71 respondents (53.4%) answered that the password they use uses 8-10 characters and 58 (43.6%) answered that they use 12 or more characters as a password. Median=2 U=1452 z= -0.114 p=0.910 r=0.010 In Slovakia 27 (45.8%) respondents answered that they use a password that contains less than 8 characters and 31 (52.5%) answered that the password they use contains 12 or more characters. Based on the survey, we can see that more people in Slovakia answered that they use 12 or more characters as passwords than in Hungary. Most of the participants in the survey in Hungary answered that they use 8-10 characters as passwords. Median= 3 U=336 z=-1.390 p=0.165 r= 0.198

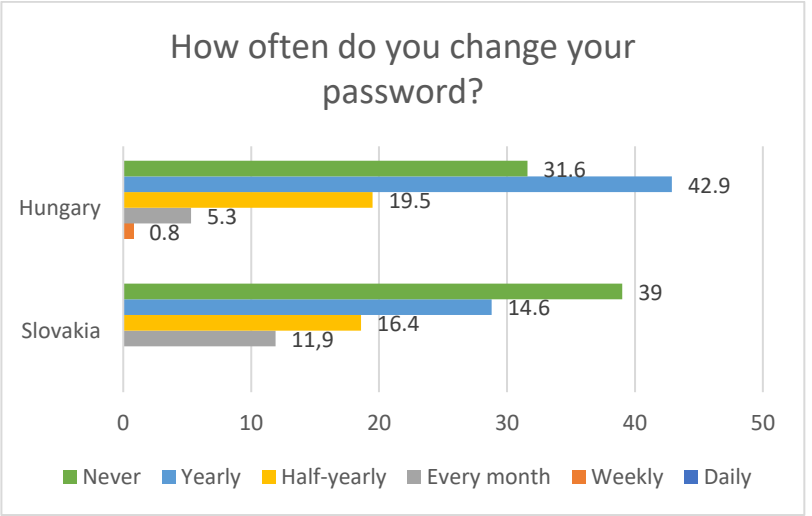

Figure 3: Frequency of password changes by participants in the survey in Hungary and Slovakia. (Source:Created by the author)

Figure 3. shows that (0.8%) of the participants in the survey in Hungary answered that they change their password on a weekly basis, (5.3%) change it every month, (19.5%) every semester and (42.9%) every year, (31.6%) answered that they never change their password. Median=5 U=1435 z= -0.206 p=0.837 r=0.018 In Slovakia, (11.9%) of survey participants answered that they change their password every month, and (16.4%) answered that they change their password every six months, (14.6%) answered that they change the password they use every year and (39%) answered that they never change the password they use. Median= U=331 z=-1.346 p=0.178 r=0.192

Password usage habits	**Hungary**		**Slovakia**	
	Freq.	**Perc.**	***Freq.***	**Perc.**
Password contains upper- and lower-case letters, numbers, and special characters.				
Yes	125	94%	35	59.3%
No	8	6%	23	39%
The password contains personal data.				
Yes	30	22.9%	20	33.9%
No	101	74.8%	38	64.4%
The password contains a meaningful word.				
Yes	69	51.9%	38	64.4%
No	64	48.1%	20	33.9%
Use the same password in several places.				
Yes	86	64.7%	40	67.8%
No	47	35.3%	18	30.5%

Table 5: *Password usage habits based on the responses of survey participants in Hungary and Slovakia. (Source:Created by the author)*

We can see that 125 (94%) of the participants in the survey in Hungary answered that they use a password that contains upper- and lower-case letters, numbers and special characters. Only 8 answered (6%) that the password they use does not contain ,,uppercase and lowercase letters", numbers and special characters. Median=1 U= 1249 z= -2.955 p=0.003 r= 0.268 30 (22.9%) of the survey participants answered that the password they use contains personal information and 101 (74.8%) answered that the password they use does not contain personal information. Median=2 U=1326 z= - 0.606 p=0.545 r=0.055 When asked if the password contains meaningful words 69 (51.9%) answered that the pass-

word they use contains meaningful words and 64 answered (48.1%) that it does not. Median= 2 U= 973 z= -3.169 p=0.002 r=0.288 When asked whether they use the same password in several places 86 (64.7%) answered that they use the same password in several places and (35.3%)of 47 answered no. Median=1 U=1463 z= -0.047 p=0.963 r=0.004 In Slovakia 35 respondents (59.3%) answered that they use a password that contains ,,uppercase and lowercase letters", numbers and special characters and 23 respondents (39%) answered no. Median=1 U=270 z= -2.640 p=0.008 r=0.377 When asked whether the password they use contains personal information 20 (33.9%) answered yes and 38 (64.4 %) answered that the password they use does not contain personal information. Median=2 U=249.5 Z=-3.108 p=0.002 r=0.444 When asked whether the password contains a meaningful word 40 (67.8%) answered that the password also contains a meaningful word (33.9%) answered no. Median=1 U=343.5 z=-1.316 p= 0.188 r= 0.188 In the survey 86 people (64.7%) answered yes to the question of whether they use the same password in several places and 47 (35.3%) answered that they do not use the same password in several places. Median=1 U=405.5 z=-0.137 p=0.891 r=0.019

Mann-Whitney U test

,,The Mann-Whitney U Test is a statistical test used to determine if 2 groups are significantly different from each other on your variable of interest." [18] ,, A significant level of 0.05 indicates a 5% risk of concluding that a difference exists when there is no actual difference."[19]

MANN-Whitney U test	Hungary	Slovakia
	P	p
The password contains upper- and lower-case letters, numbers and special characters.	0.003	0.008
The password contains personal data.	0.545	0.002
The password contains a meaningful word.	0.002	0.188
The same password used in several places.	0.963	0.891
The password changes.	0.834	0.178
The password length.	0.837	0.165

Table 6: A Mann Whitney U test result for password usage in Hungary and Slovakia. (Source:Created by the author)

We can see in (Table 6.) the Mann-Whitney U test in the case of password use when a meaningful word is used as a password, the p value in Slovakia is much higher than in Hungary.

CONCLUSIONS

We can say that based on the survey, the use of smart devices is popular in both Hungary and Slovakia as more than 98% of the participants answered that they use at least one smart device in both countries. As for password length, according to the survey, more people in Slovakia use passwords with 12 or more characters than in Hungary. When asked whether they use ,,upper and lower-case letters", numbers and special characters in the password, according to the survey in Hungary, more people use upper- and lower-case letters, numbers and special characters than in Slovakia. In the case of passwords fewer people use personal information in Hungary than in Slovakia. The Mann-Whitney U test shows that the p value in Slovakia is higher than in Hungary in the case of password use when a meaningful word is used as a password. On the basis of this we can say that people living in Slovakia are exposed to a greater risk of attacks than people living in Hungary. According to Kaspersky's report as to, how to create a strong password, it is important to pay attention to the following. For example the password should be at least 10-12 characters long, but the longer the password the better. It is important to avoid easily guessed passwords such as,,12345" password, since the password can be cracked in seconds by a ,,brute force" attack. It is important that the password contains lowercase and uppercase letters, numbers, special characters, as this makes it more difficult to crack the password[20]. According to Keeper's 2023 report a strong password consists of 16 characters and contains uppercase letters, numbers and special characters and does not contain personal information and the same password should not be used in multiple places [21]. The Americas Cyber Defense Agency (CISA) reports that using simple passwords is not secure, so you should never choose a password that can be easily guessed along with your date of birth as easy-to-guess passwords can be easily cracked [22]. One way for IoT devices to be protected is to use these hard-to-guess passwords [23]. In addition, it is very important to always change the default passwords on our IoT devices [24].

REFERENCE

[1] Dorottya Mandić, „Az okoseszközök veszélyei", Biztonságtudományi Szemle *5*:3, pp. 37–45, p. 9, 2023.

[2] Blessing, Elisha & Potter, Kaledio & Klaus, Hubert., „Security and Privacy in IoT: Considerations for securing IoT devices.", 2024, [Online]. Available: https://www.researchgate.net/publication/377853082_Security_and_Privacy_in_IoT_Considertions_for _securing_IoT_devices

[3] Kollár Csaba, „Társadalom és információbiztonság. A humán információbiztonság a digitális korban", International Research Institute, (2016) 488p.pp.189-194.,6p.. doi: 10.18427/IRI-2016-0023.

[4] Kollár Csaba „IoT a gyakorlatban, az információbiztonság fókuszában I.: Az IoT működése, fejlődési tendenciái", Bolyai Szemle 2017:1pp.41-54.,14p. (2017)

[5] X. Su, B. Wang, C. Choi, and D. Choi, „Case study on password complexity enhancement for smart devices", in 2017 *14*th IEEE Annual Consumer Communications &

Networking Conference (CCNC), Las Vegas, NV: IEEE, jan. 2017, p. 1–5. doi: 10.1109/CCNC.2017.8013419.

[6] S. A. Baho and J. Abawajy, „Analysis of Consumer IoT Device Vulnerability Quantification Frameworks", Electronics, 12(5), p. 1176, feb. 2023, doi: 10.3390/electronics12051176.

[7] R. J. and V. S. M., „Security Challenges Prospective Measures In The Current Status of Internet of Things (IoT)", in 2022 International Conference on Connected Systems & Intelligence (CSI), Trivandrum, India: IEEE, aug. 2022, p. 1–8. doi: 10.1109/CSI54720.2022.9923984.

[8] „Most common passwords used in Internet of Things (IoT) devices over a 45 day period worldwide in 2021". [Online]. Available: https://www.statista.com/statistics/1298495/frequently-seen-passwords-in-iot-devices/

[9] S. Sanaullah and B. Liu, „Information Security Challenges in the Internet of Things (IoT) Ecosystem", in 2022 International Symposium on Electrical, Electronics and Information Engineering (ISEEIE), Chiang Mai, Thailand: IEEE, feb. 2022, p. 124–129. doi: 10.1109/ISEEIE55684.2022.00029.

[10] D. Mandić and G. Kiss „Az okoseszközök és vírusvédelem használata Magyarországon és Szerbiában", 30th Anniversary conference of the safety and security enineering education: A biztonságtechnikai mérnök képzés 30évi jubileumi konferenciája, Budapest, Magyarország (2023) 127p. pp. 64-75.,12p., ISBN:9789634493297

[11] D. Mandić and J. Simon, „Biztonságosak-e az okosotthonokban használt okoseszközök",Biztonságtudományi Szemle 4:4pp.59-67.,9p(2022)

[12] K. Andras, „Life is Short. Have another Affair - Password Security", p. 121–130, 2015.

[13] „Top 200 most common passwords of the year 2019-2022". [Online]. Available: https://s1.nordcdn.com/nord/misc/0.78.0/nordpass/top-200-2023/200-most-common-passwords-en.pdf

[14] D. K. Davis, M. M. Chowdhury, and N. Rifat, „Password Security: What Are We Doing Wrong?", in 2022 IEEE International Conference on Electro Information Technology (eIT), Mankato, MN, USA: IEEE, Maj 2022, p. 562–567. doi: 10.1109/eIT53891.2022.9814059.

[15] „How Secure Is My Password?" [Online]. Available: https://www.security.org/how-secure-is-my-password/

[16] „How Long Does It Take for a Hacker to Crack a Password?" [Online]. Available: https://tech.co/password-managers/how-long-hacker-crack-password

[17] „Most common passwords: latest 2024 statistics". [Online]. Available: https://cybernews.com/best-password-managers/most-common-passwords/

[18] „Mann-Whitney U Test". [Online]. Available: https://www.statstest.com/mann-whitney-u-test/#Assumptions_for_a_Mann-Whitney_U_Test

[19] „Interpret the key results for Mann-Whitney Test". [Online]. Available: https://support.minitab.com/en-us/minitab/help-and-how-to/statistics/nonparametrics/how-to/mann-whitney-test/interpret-the-results/key-results/

[20] „Internet of Things security challenges and best practices". [Online]. Available: https://usa.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security

[21] „What Makes a Strong Password?" [Online]. Available: https://www.keepersecurity.com/blog/2023/08/31/what-makes-a-strong-password/

[22]„Use Strong Passwords”. [Online]. Available: https://www.cisa.gov/secure-our-world/use-strong-passwords
[23]„Best Practices for IoT device security”. [Online]. Available: https://bytebeam.io/blog/iot-security-how-to-protect-your-connected-devices/
[24]„Best Practices in Securing Passwords for IoT Devices”. [Online]. Available: https://iotmktg.com/best-practices-in-securing-passwords-for-iot-devices/