applied sciences

MDPI

Article

Age and Gender Impact on Password Hygiene

Aušrius Juozapavičius [1,*], Agnė Brilingaitė [2], Linas Bukauskas [2] and Ricardo Gregorio Lugo [3,4]

[1] General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A, LT-10322 Vilnius, Lithuania
[2] Cybersecurity Laboratory, Institute of Computer Science, Vilnius University, Didlaukio 47, LT-08303 Vilnius, Lithuania; agne.brilingaite@mif.vu.lt (A.B.); linas.bukauskas@mif.vu.lt (L.B.)
[3] Institute for Information Security and Communication Technology, Norwegian University of Science and Technology, NO-2802 Gjøvik, Norway; Ricardo.G.Lugo@ntnu.no
[4] Department of Welfare, Management, and Organization, Østfold University College, NO-1757 Halden, Norway
* Correspondence: ausrius.juozapavicius@lka.lt

Abstract: Password hygiene plays an essential part in securing systems protected with single-factor authentication. A significant fraction of security incidents happen due to weak or reused passwords. The reasons behind differences in security vulnerable behaviour between various user groups remains an active research topic. The paper aims to identify the impact of age and gender on password strength using a large password dataset. We recovered previously hashed passwords of 102,120 users from a leaked customer database of a car-sharing company. Although the measured effect size was small, males significantly had stronger passwords than females for all age groups. Males aged 26–45 were also significantly different from all other groups, and password complexity decreased with age for both genders equally. Overall, very weak password hygiene was observed, 72% of users based their password on a word or used a simple sequence of digits, and passwords of over 39% of users were found in word lists of previous leaks.

Keywords: passwords; password hygiene; data leak; password strength; gender impact

check for updates

Citation: Juozapavičius, A.; Brilingaitė, A.; Bukauskas, L.; Lugo, R.G. Age and Gender Impact on Password Hygiene. *Appl. Sci.* **2022**, *12*, 894. https://doi.org/10.3390/app12020894

Academic Editor: Agostino Forestiero

Received: 17 December 2021
Accepted: 13 January 2022
Published: 16 January 2022

1. Introduction

Cybercriminals target vulnerabilities that are easiest to exploit, and humans continue to constitute both a huge attack surface and the weakest component in any organisation [1]. Password authentication is the most common protection method in organisations' internet-based systems, mobile applications, and internal or local applications. Therefore, weak and reused passwords open doors even in the most hardened systems, and the security vulnerable behaviour of humans remains an active research subject. Compromised credentials represented 19% of initial attack vectors to organisations in 2020 [2], with identity theft reported representing 65% of all social engineering breach incidents [3]. Surveys show that in Germany, 33% of working adults rotate five to 10 passwords and 10% use the same one to two passwords for most/all online accounts [4]. In Japan, 21% of working adults rotate the same one to two passwords. Based on the global 2020 survey, 57% of employees use an employer-issued device to check e-mails and respond to them [5]. In addition, employees allow their friends and family members to check e-mails (33% worldwide and 52% in the US) and do online shopping (22% worldwide and 38% in the US) on their employer-issued devices. In contrast, only 58% of employees in Australia do not allow their friends and family members to check e-mails, do online shopping, do streaming or research, check social media, and perform other activities on their employer-issued devices [6,7].

1.1. Related Work

The relationship between gender and security risk remains inconclusive. Some statistical data show no difference in behaviour. For example, 67% of adult women and 66% of adult men restricted applications from accessing private data on their smartphones [8].

Other research showed that women understood the threat impact better than men, but they believed to be less vulnerable, expecting other people to implement security measures [9,10]. In another case, self-reporting results showed men having higher levels of knowledge of secure passwords and lower levels of conscientiousness [11]. A study of employees at a medium-sized American company observed no differences between gender-related security vulnerability risk when job-specific factors were taken into account [12]. Similarly, a study of spam messages on the Facebook platform found that in general, women were more likely to click on spam messages, but the results differed depending on a topic, with more men opening media- or pharma-spam [13].

Statistical data suggest a higher vulnerability of young and older people. For example, 60% of French teenagers (11–18 years) do not change passwords after choosing them [14]. On the other hand, the implementation of password hygiene training programmes for youth (13–16 years) show changes in password-setting behaviour [15]. Researchers found that there is a high percentage of reused passwords in both groups of older and younger respondents [16]. The researchers emphasise that public campaigns about password security have not been successful, as the problem continues to exist. Older adults are keen to protect themselves and understand the risk of not doing so, but they do feel anxiety, e.g., fear of forgetting the password [17]. A user becomes less security compliant when they are more security fatigued [18]. The fatigue is noticeable when security becomes superfluous. The enforcement of regular password changes does not increase security significantly and does not influence the creation of stronger passwords. Users cope with a password-changing policy by applying simple modifications to their current password and cycling through a dedicated set of passwords [19]. Researchers identified a large set of distinctive password pre-/post-fix patterns of various categories, for example, people, locations, digits, and culture-specific substitutions [20].

Little research exists on the analysis of password strength in the context of languages other than English. Doucek et al. [21] presented a password estimation engine based on the zxcvbn [22] algorithm for Czech and Slovak languages. They presented the methodology that can be used to adapt the zxcvbn algorithm for smaller European languages.

Previous research regarding the cyber hygiene of different age groups and genders has a few recurring limitations. As a rule, the studies are limited to several hundred data points, and they use self-reported user behaviour or insufficiently validated data such as gender or age from social media platforms where users have the freedom to misrepresent their demographic characteristics. The novelty of our work lies in the scale and validity of the data that we use in obtaining password strengths of all age and gender groups. It is primarily based on the large set (over 100,000) of user passwords that we managed to recover together with every user's accurate date of birth and gender.

1.2. Contribution

Our paper presents research on password hygiene based on a set of leaked data of Lithuanian users. The analysed dataset exceeded 100,000 records. According to Eurobarometer data [23], Lithuanian users represent an average European user from a cyber hygiene perspective; e.g., 65% of Lithuanian users changed their passwords for online services during the previous 12 months, while the European average is 67%. Nowadays, security breaches and data leaks are commonplace. In social media and advertisements of security companies, lists of top passwords are presented every half a year. In addition, yearly reports of the National Cyber Security Centre of Lithuania show rising numbers of cyber security incidents. Information technology (IT) as a mandatory subject for high school pupils in Lithuania was introduced in 1986. At that time, schools did not have a sufficient amount of computers, and teachers were struggling to ensure the development of practical skills. In 1995, the school graduation IT exam was introduced. The national association of IT teachers was established in 2000. In 2005, the IT subject was already taught from the 5th grade of secondary school. Therefore, we assume the varying exposure to IT of different generations to be visible in their password hygiene measurements.

The work aims to investigate password strength and identify the impact of age and gender properties using an extensive password dataset. We raise the following research questions in the context of the leaked dataset:

- Do older users have weaker passwords considering their lack of general IT education compared to younger generations?
- Has gender no impact on password strength, as previous studies did not find conclusive evidence of any significant differences?
- What is the password hygiene in general?

Our applied research has practical implications for service developers and providers. They should know and understand the distribution of security-related behaviour of their users. Corresponding technical measures should be adapted to ensure the security of systems and the privacy of their customers.

The paper is structured as follows. Section 2 covers the sample data and methodology of how leaked passwords were recovered. Section 3 provides statistical insights about the password strength from the perspective of age and gender differences. Section 4 discusses the implications of our findings and similarities with other research. Section 5 concludes the paper and offers directions for future work.

2. Materials and Methods

2.1. Dataset of Leaked Passwords

2.1.1. Data Leak and Ethical Concerns

In February of 2021, a car-sharing service CityBee acknowledged a leak of a misplaced database archive [24]. UAB Prime Leasing operates the service in Lithuania. The leaked archive dates back to 2018 and includes private data such as hashed passwords, names, driver's license ID, and other personally identifiable information. The quality of the data is exceptional due to the financial implications of the car-sharing service—the company has to validate its users before permitting the ride.

Ethics concerns may be raised due to the actual qualitative data used in this research paper. Several aspects eliminate any negative impact of the results on the individuals. First of all, the article does not reveal any personally identifiable data, and only aggregated statistical data are presented. Secondly, the data are sufficiently old (2018), and all affected users were already urged to change their passwords by the car-sharing company after the leak. The company publicly announced that the disclosure of the data would not impact the financial security of their customers [24]. The data were made publicly available by cybercriminals. They had the opportunity and better resources to obtain identical statistics as presented in our paper. In addition, some of the least secure passwords had been available on social media immediately after the disclosure.

The State Data Protection Inspectorate of Lithuania already imposed an administrative fine [25] on the company under the General Data Protection Regulation [26] due to "Insufficient technical and organisational measures to ensure information security". However, we argue that the general population and especially business companies should utilise the incident to their full advantage and improve their cyber security practices using the results presented here.

2.1.2. Data Description and Validity Checks

The leaked dataset contains 110,302 records in total. Each record includes a unique sequence ID, the user's first and last name, a password hash, the state-issued personal identification number (similar to the social security number used in the US), and an email. The sequence ID ranges from 1 to 111,052. Gaps in the sequence are small, and there are only 750 deleted records (below 1% of all records). Some of the first records were clearly used for testing purposes with incorrect hashes (5 records) and emails of the developers of the car-sharing company itself (17 records).

The Lithuanian personal identification number consists of 10 digits, revealing the person's gender and date of birth followed by a control digit. Furthermore, most male

Lithuanian names and surnames end with the letter *s*, giving us an additional criterion for the validity check. Records with empty, invalid (foreign or inconsistent), or duplicate personal codes were excluded from gender and age analysis.

We found over 91% of the 110,302 records containing a valid Lithuanian state-issued personal code revealing the user's gender and date of birth. Passwords were stored using a fast SHA1 hashing algorithm [27], giving us the possibility of recoveing most of them (92%) in a reasonable time. This created a unique opportunity to analyse password hygiene and habits of a large set of technologically savvy Lithuanian users of various ages and genders.

2.2. Password Recovery

Figure 1 presents the generalised workflow of password recovery. The central Hashing/Recovery executes the Brute Force method. Additionally, the component uses words transformed by the Transformations component. This component depends on the localised dictionary, anthology, word/character statistics, and data from known leaks. Recovered passwords are evaluated according to the password strength metrics. The Analytics component ends the workflow.

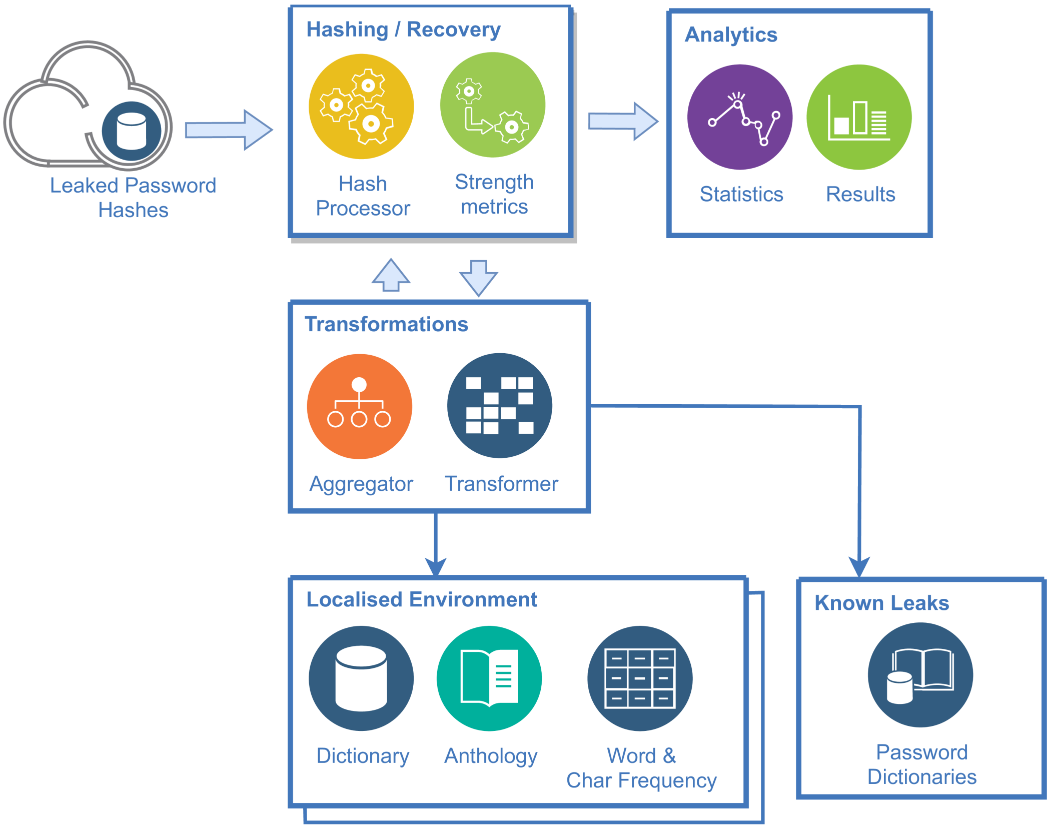

Figure 1. The flow of password recovery and analysis.

We used a computer with a single NVidia GeForce RTX 3070 video card and the `Hashcat` software package to recover 89,556 passwords (91.71%) out of 97,654 unique SHA1 hashes found in the leaked archive. This revealed passwords from 102,120 records out of 110,302 (92.6%). The hashing rate varied from 11 GH/s for brute-force attacks to 7.5 GH/s for dictionary attacks. It took around one week (180 h) to brute-force all passwords with 8 characters or less (45% of all unique hashes) using the complete Latin character set (2 × 26 letters), digits (10), and all printable special characters from the ASCII table, including space (33 characters). Ever-decreasing character sets were used to brute-force longer passwords of up to 14 characters in length. Based on the character frequency and pattern analysis of the already recovered passwords, we first eliminated some special characters, then all special characters, then upper-case letters, and finally, a digits-only set was used for lengths 13 and 14. This brute-force attack revealed an additional 33% of passwords and took 11 weeks (1900 h of computer time). In total, 78% of hashes were cracked using the brute-force attack. Further brute-force attacks become unfeasible; e.g., it would take 200 years to hash all 10-character-long combinations of the full character set (95 characters), and currently, even the most advanced hashing rigs would be unable to tackle SHA1 hashes of 11 or 12 character-long random passwords.

To recover longer passwords, we used a dictionary attack with various word-mangling rules added on top, such as appending up to 4 characters at the beginning or the end of each word, reversing words, or using other rule sets included in the default `Hashcat` package. Most of the default rules work well for the Lithuanian language with several minor improvements possible due to the following idiosyncrasies:

- Making l33tsp34k-like transformations: AaĄą → 4, EeĖė → 3, IiĮį→ 1, SsŠš→ 5, etc.;
- Changing letters to numbers based on their keyboard layout: Ąą→ 1, Čč→ 2, Ęę→ 3, Ėė→ 4, Įį→ 5, Šš→ 6, Ųų→ 7, Ūū→ 8, Žž→ 0;
- Simply dropping the diacritics: Ąą → Aa, ĖėĘę → Ee, Įį → Ii, ŲŪųū → Uu, and Žž → Zz.

Dictionary attacks with word-mangling rules work because usually, people create memorable passwords based on their social environment and native language [28]. We used several different dictionaries for this purpose. Table 1 presents their list, sizes, and the number of passwords found in each of them. It should be noted that some dictionaries—and therefore, the passwords found in them—overlap, because we wanted to measure the effectiveness of each of them. The table shows the number of passwords directly matching some word in the corresponding dictionary and the number of unique passwords not present in any other dictionary. In practice, the number of passwords recoverable from dictionaries is larger, because many passwords had fragments from the dictionaries; e.g., 37,452 passwords had fragments found in the Top500k dictionary, and 8789 users had their name as a part of their password. Overall, 30,265 unique passwords could have been extracted from all the dictionaries (the master dictionary) directly, although most of them (27,582) had been already found via the brute-force attack. However, the application of word-mangling rules revealed an additional 6815 passwords. Surprisingly, the rules applied to already recovered passwords gave an extra 81 passwords. Together, these simple dictionary attacks recovered an extra 10% of passwords and took just several hours of computer time.

Table 1. Dictionaries used and the corresponding number of matching passwords.

Dictionary	**Words**	**Passwords**	**Unique**	**Description**
Lithuanian words	83,256	1530	0	Microsoft's spell checker
↪ Latin version	81,093	3044	0	Same, with diacritic symbols removed
Anthology	144,716	1852	10	Most frequent words (without diacritics) from Lithuanian classic literature
CityBee users	145,401	3044	464	Names and e-mail patterns
Top500k Lithuanian passwords	523,267	21,152	1745	Breaches of 2019–2020
Extended Lithuanian leaks	1,944,927	24,045	4084	Names and passwords of previous breaches (388,327 words overlap with the Top500k dictionary)
Rockyou	14,344,392	8145	2797	Social games site's leak, 2009
All Lithuanian words	33,170,533	3823	154	Generated using Lithuanian language grammar rules (without diacritics)
Master dictionary	49,705,914	30,265		Unique words from all dictionaries together

Finally, we concluded the extraction with two of the so-called "combinator" attacks performed by adding together words from different (or the same) dictionaries. A simple combination of all our dictionaries uncovered around 3% of passwords in less than 6 h. The remaining 1% was obtained by using a more advanced combination technique called PRINCE, which combines an arbitrary number of words into passwords of a predefined length. If the words are sorted by their frequency with single letters concluding the dictionary, then asymptotically, this algorithm is equal to the usual brute forcing, but it uncovers passwords faster in the beginning. We stopped this attack after 7 days when the recovery speed dropped to less than one password per hour.

During the analysis after the run, passwords of 80,213 records were found to be composed of digits only or have fragments present in one of the dictionaries used. In other words, passwords of more than 72% of the users could be found using a combination of dictionary attacks, making them unsafe even for stronger hashing algorithms.

2.3. Strength Metrics

Password length alone is definitely not a good indicator of the password strength. Our intention was to choose a password strength meter that would be both accurate and easily implementable by any web or mobile service provider. The `zxcvbn` meter satisfied both the accuracy [29] and usability criteria. This low-budget password strength estimation method [22] uses a heuristic probability model employing the sum of two components—the number of patterns the attacker might know and the number of guesses the attacker has to make in the worst case scenario as multiplicative penalty.

$$\operatorname*{argmin}_{S \subseteq \mathbb{S}} D^{|S|-1} + |S|! \prod_{m \in S} m.guesses$$

where $|S|$ is the length of sequence $\mathbb{S}$, and D is a constant representing the number of the most common passwords the attacker already has in the dictionary.

A very important feature of the algorithm is the possibility of supplying custom-made dictionaries reflecting the predicted environment of the users. If a fragment of a password is found in one of the dictionaries, the score (number of predicted guesses) is negatively impacted, perfectly corresponding to the attack methods we used. In addition, the closer to the top of the dictionary a word is found, the lower the score. The implementation of the `zxcvbn` algorithm we used takes into account the possibility that a user chose a word from a dictionary unknown to us (a different language, a specific slang, or a dialect), so it lowers the score of random-looking passwords by giving each character a cardinality of 10; e.g., the number of guesses predicted by the algorithm to recover a 4-character-long password would be equal to 10,000. Therefore, we use a base-10 logarithm of the number of guesses to measure the password strength (denoted by `log10`). One additional convenient feature of this scale is an easy interpretation of the results, as the score of a randomly generated password is equal to its length (the number of its characters).

3. Results

3.1. Description of the Data

There was no apparent password policy in place because the lengths of the recovered passwords ranged from one to 28 characters (see Table 2). We discarded 536 records with zero-length passwords, assuming they belong to users who have not completed a full registration process. There were 100,317 records with valid Lithuanian personal codes and non-zero passwords (91% of the whole set), with 67,997 records belonging to male users and 32,320 records belonging to female users.

We failed to recover 8.5% of male user passwords, and this fraction remains almost the same (7%–9%) for all age groups. Alternatively, we did not recover 5.2% of female user passwords. Interestingly, the most advanced group consisted of the 20-year-old females with 10% of their passwords left unknown. All other female age groups have 8% or less of unrecovered passwords, with the fraction dropping down to 1% for the 49-year-old females.

Further analysis of password strength by age and gender is limited to 92,816 records with recovered non-zero passwords: 62,185 records of male users and 30,631 records of female users. It should be emphasised that the leaked archive dates back to 2018. Therefore, we calculated the users' age at the time.

Table 2. Distribution of password lengths (all 110,302 records).

Length	**All Records**		**Male**		**Female**		**Foreign/Unknown**	
	Count	**Proportion**	**Count**	**Proportion**	**Count**	**Proportion**	**Count**	**Proportion**
0	536	0.49%	322	0.45%	95	0.28%	119	2.54%
1	1	0.001%	1	0.001%				
3	24	0.02%	8	0.01%	9	0.03%	7	0.15%
4	253	0.23%	30	0.04%	115	0.34%	108	2.30%
5	607	0.55%	246	0.34%	174	0.52%	187	3.99%
6	5490	4.98%	3442	4.78%	1641	4.88%	407	8.68%
7	5578	5.06%	3484	4.84%	1760	5.24%	334	7.12%
8	38,594	34.99%	25,004	34.73%	11,509	34.24%	2,081	44.36%
9	17,659	16.01%	11,730	16.29%	5451	16.22%	478	10.19%
10	13,687	12.41%	9024	12.53%	4363	12.98%	300	6.40%
11	8727	7.91%	5705	7.92%	2841	8.45%	181	3.86%
12	5187	4.70%	3329	4.62%	1771	5.27%	87	1.85%
13	2732	2.48%	1730	2.40%	955	2.84%	47	1.00%
14	1597	1.45%	974	1.35%	599	1.78%	24	0.51%
15	770	0.70%	449	0.62%	313	0.93%	8	0.17%
16	357	0.32%	217	0.30%	137	0.41%	3	0.06%
17	155	0.14%	81	0.11%	72	0.21%	2	0.04%
18	99	0.09%	60	0.08%	37	0.11%	2	0.04%
19	34	0.03%	21	0.03%	11	0.03%	2	0.04%
20	20	0.02%	10	0.01%	10	0.03%		
21	6	0.01%	1	0.001%	5	0.01%		
22	3	0.003%	2	0.003%	1	0.003%		
24	1	0.001%	1	0.001%				
25	1	0.001%	1	0.001%				
26	1	0.001%			1	0.003%		
28	1	0.001%	1	0.001%				
Unknown	8182	7.42%	6130	8.51%	1738	5.17%	314	6.69%
Total	110,302	100.00%	72,003	100.00%	33,608	100.00%	4691	100.00%

3.2. Analysis of Dictionaries and Patterns

Dictionaries sorted by word frequency have a substantial impact on the recovery speed (see Figure 2), as the curves representing the fraction of found passwords against their position in the dictionary drop faster than an exponential. Half (50%) of 8145 passwords found in the Rockyou dictionary are within the first 5% of its words. Similarly, half of the matched passwords are within the first 15% of the Lithuanian Top500k dictionary and within the first 20% of the Lithuanian Anthology dictionary. This finding also illustrates the persistence of the password reuse problem because the Rockyou breach occurred in another country a decade ago, but passwords of more than 7% of unique CityBee hashes are present in the dictionary. Quite often, the same password is used by many users. There are 17,328 records (15.71% of all records) with shared passwords. As a consequence, 14,206 users (12.88% of all users) have their passwords in the Rockyou dictionary. In total, passwords of 40,229 users (39.39%) were found in at least one of the previously leaked databases.

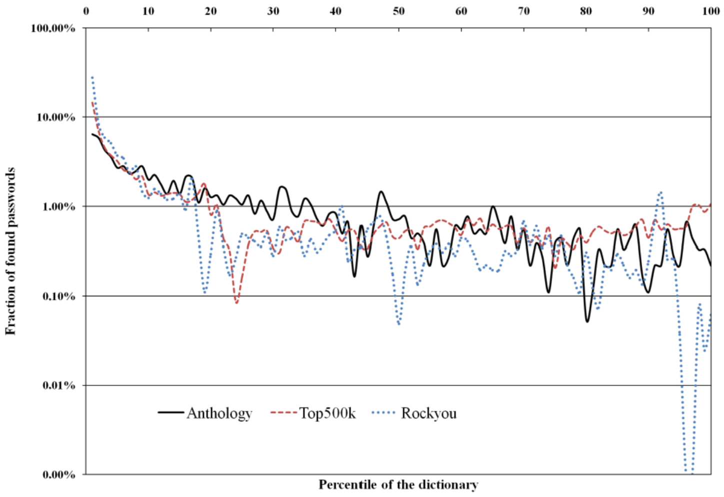

Figure 2. Distribution of matched passwords in sorted dictionaries.

Analysis of various patterns found in the recovered passwords is presented in Table 3. Each row independently lists a common pattern and the fraction of passwords observed among all recovered 102,120 passwords. Some patterns overlap. If a word from any dictionary listed in Table 1 is present somewhere in a password, then the password is assigned to the *word based* pattern class. All others except the *digit only* passwords are assigned to the *random* class. Therefore, the measurements of the two classes are imprecise. Manual inspection shows that up to 25% of the supposedly *random* passwords may have some semantic meaning, so it is difficult to determine the exact number of users who use password generators and managers.

Table 3. Pattern frequency of 102,120 recovered passwords (examples do not disclose real data).

Class	Fraction	Example	Description
random	21.45%	`9q7FZ!OTkE`	A sequence of random characters
digits only	4.00%	`1234500`	Any sequence of digits
↪ phone	0.75%	`860012345`	Possibly a phone number
↪ personal code	0.10%		State-issued code, 11 digits
date of birth	1.24%	`me19720101`	User's date of birth in any format
special symbol	2.58%	`password!`	At least one special character
spatial	0.11%	`1q2w3e`	Keyboard walks
lowercase only	23.82%	`apassword`	a–z letters only
uppercase only	0.09%	`PASSWORD`	A–Z letters only
ULS pattern	3.05%	`Password1`	One A–Z, then many a–z, then any non-letter
ULS+ pattern	12.21%	`Password!1`	One A–Z, then many a–z, then many non-letters
repeat	5.19%	`Pass121212`	Repeated groups of one or more characters
word based	74.55%	`Password123`	Some part is a dictionary word
↪ name/email	8.61%	`Someuser!1`	User's name or email
↪ reversed name	0.23%	`resUemoS123`	User's name in reverse
↪ l33t	≈ 1.5%	`P455w0rd`	L33tsp34k, somewhat ambiguous

We had enumerated all the possible key-spaces of eight-character-long passwords and shorter using the 95 printable ASCII characters (including space). Therefore, we could extract the frequency distribution of all characters (see Table 4). Letter *a* is the most popular character both among the recovered passwords (with the frequency of 10.12%) and in password dictionaries Rockyou (7.05%) and Top500k (10.64%). This is unusual, because the most frequent English letter is *e* (12.09%) followed by *t* (8.95%) and then *a* (8.50%) [30], and the most frequent Lithuanian letter is *i* (14%) followed by *a* (11.1%) [31]. The period was the most popular special character, which was similar to Rockyou and Top500k. Separately, we extracted the first digits of all numbers found in the passwords. The digit 1 exceeds the value of Newcomb–Benford's law (probability 0.376 instead of 0.301), as well as digits 7, 8, and 9. The order of all first digits by their diminishing frequency is 1203879564.

Table 4. Character count and frequency within 50,547 passwords of eight characters or less.

Char	Count	Freq %	Char	Count	Freq %	Char	Count	Freq %	Char	Count	Freq %
a	31,081	8.08	4	6012	1.56	V	2568	0.67	#	19	0.005
s	20,521	5.33	v	5753	1.49	C	2553	0.66	%	18	0.005
i	17,970	4.67	p	5583	1.45	N	2544	0.66	/	15	0.004
1	15,516	4.03	c	4768	1.24	I	2526	0.66	)	14	0.004
e	14,785	3.84	y	4749	1.23	U	2486	0.65	space	11	0.003
r	11,869	3.08	z	4641	1.21	J	2437	0.63	:	10	0.003
u	11,467	2.98	j	4589	1.19	H	2413	0.63	=	8	0.002
n	10,956	2.85	f	3482	0.90	O	2391	0.62	;	8	0.002
t	10,787	2.80	h	3478	0.90	F	2389	0.62	&	6	0.002
l	10,466	2.72	x	3236	0.84	Z	2375	0.62	(	5	0.0013
2	10,287	2.67	w	3071	0.80	X	2325	0.6	>	3	0.0008
k	10,215	2.65	A	3029	0.79	W	2313	0.6	\	3	0.0008
o	10,163	2.64	M	2866	0.74	Q	2289	0.59	'	2	0.0005
0	8864	2.30	S	2844	0.74	Y	2239	0.58	[	2	0.0005
m	8847	2.30	L	2724	0.71	.	151	0.04	~	2	0.0005
3	8202	2.13	K	2654	0.69	@	131	0.03	{	2	0.0005
9	7742	2.01	P	2630	0.68	-	87	0.02	]	2	0.0005
d	7727	2.01	R	2626	0.68	!	80	0.02	<	1	0.0003
5	6981	1.81	D	2624	0.68	*	75	0.02	|	1	0.0003
7	6367	1.65	q	2623	0.68	?	50	0.01	^	1	0.0003
b	6294	1.64	T	2619	0.68	_	44	0.01	"	1	0.0003
8	6283	1.63	E	2615	0.68	+	40	0.01	}	1	0.0003
g	6202	1.61	B	2605	0.68	$	24	0.01	`	0	0
6	6158	1.60	G	2597	0.67	,	19	0.005			

3.3. Age and Gender Analysis

Due to the sample size ($N = 92,816$), one could consider the distribution of the data to represent a normal population distribution [32]. Except for the peaks of randomly generated passwords of strength 8, both genders visually show normal distributions (Figure 3) but violate the Kolmogorov–Smirnov goodness-of-fit-test for normality (KS = 0.122 $p < 0.001$). Due to the number of cases, parametric analysis can be used since power, the low probability of type I errors, and a realistic effect size estimation are present with large samples [33]. Descriptive statistics is given in Table 5. Overall, the average strength of passwords (5.91 ± 2.16) corresponds to a six-character-long random password and should be considered as very weak, even though the average length of recovered passwords is 9.12 characters. Some differences between genders could be observed. The password strength of male users consistently exceeds the password strength of female users for every age group (see Figure 4). Males significantly had stronger passwords than females ($t = -17.66$, $p < 0.001$ Cohen's $d = 0.123$). This observation entails that 55% of males have stronger passwords than females, which is higher than chance alone (50%). On average, the difference of strengths measured as the base 10 logarithm of the number of guesses is 0.266. In other words, male users are more likely to use passwords almost twice as difficult to guess compared with those of female users ($10^{0.266} = 1.85$). As a result, we recovered 91.5% passwords of male users and 94.8% of female users.

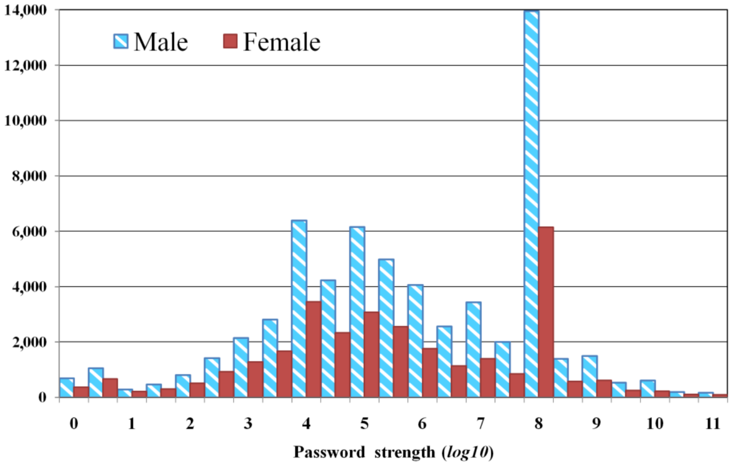

Figure 3. Histogram of password strengths.

Table 5. Descriptive statistics.

	Password Strength (log10)	
	Female	**Male**
Valid	30,631	62,185
Missing	0	0
Mean	5.731	5.997
Std. Error of Mean	0.013	0.009
Std. Deviation	2.191	2.142
Minimum	0.301	0.301
Maximum	17.260	16.284

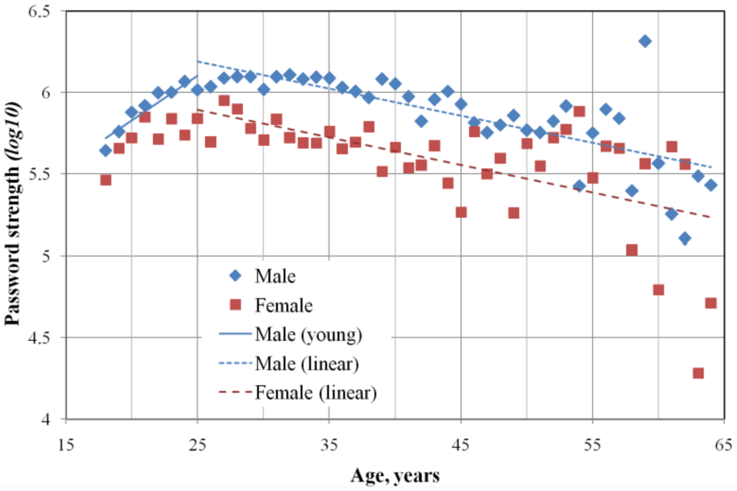

Figure 4. Password strength dependency on person's age.

Users between 25 and 35 years old had the strongest passwords. The average strength is reduced for younger users. This was not statistically significant for females, but it followed a well-pronounced linear path for male users (Male, 25 years or younger: $R = 0.044$, $F = 33.82$, $p < 0.001$, $\beta = 0.044$). For both genders above age 25, password complexity decreased with age equally (Male $R = 0.043$, $F = 86.31$, $p < 0.001$, $\beta = -0.043$; Female $R = 0.048$ $F = 51.03$, $p < 0.001$, $\beta = -0.048$). The difference in regression coefficients (Fisher's Z) to test if females and males as they get older differ in password strength was not significant, showing that older persons have increasingly less complex passwords irrespective of their gender.

The sample was separated into three distinct ranges (<26, 26–45, >45) to investigate further how age and gender influenced password complexity. The first segment was chosen based on our observation of the password strength development of young persons, while the age of 45 years was an approximate divider between persons who had exposure to IT during their school years and those who had not. Results show that age and gender have a significant interaction ($F = 9.92, p =< 0.001$) where the males aged 26–45 were significantly different from all other groups regardless of gender (see Figure 5).

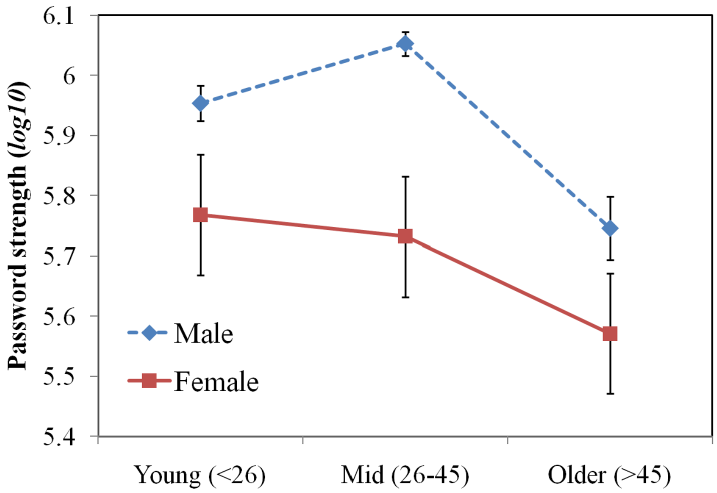

Figure 5. Password strength of different age groups.

4. Discussion

Our research answered the question about general cyber hygiene. The results showed weak password selection within most groups of users; i.e., most passwords were either short, based on a dictionary, using a limited set of characters, or found in leaked databases. Many human factors influence poor password hygiene. Service providers focus on attracting people via ease-of-use of systems. They do not want to scare new customers away by forcing them to create inconveniently complex passwords. In turn, customers rarely consider possible risks that arise from entire dataset theft. In addition, the *I have nothing important for hackers to take* mindset could explain the noticeable drop in password strength that we observed for young (in particular male) persons of ages 18 to 25. Concerning the research question about older users, our assumptions regarding the influence of their lack of general IT education on their password hygiene align with our findings. The analysis showed a decrease in users' password strength above 45 years old regardless of gender.

Based on the analysis between genders and their password choices, certain patterns and implications arise. Males generally have stronger passwords, and our results show that males between 26 and 45 have the strongest passwords. One trend that this study uncovered is that passwords regardless of gender become less complex as people get older, with the biggest difference being between males aged 26–45 and females over 45 (mean difference $\mu = 0.482 \pm 0.045$), translating to 3.03 times more complex passwords for males. A more worrisome finding is that females used the weakest passwords regardless of the age. This supports the findings of other researchers [34] that showed that females in Turkey and China had less complex passwords, although females in the UK had stronger passwords than their male counterparts. Petrie and Merdanyan [34] concluded that females in the UK might have more use of secured systems due to the digitisation of the society, whereas females in Turkey and China have less access to such systems. Regarding the research question about gender impact, our findings show a statistical difference in password-related behaviour between genders, although the effect is minimal. This aspect could explain ambivalent results in other studies of smaller samples.

It should be emphasised that adding a single random character to a password would increase its brute force time by two orders of magnitude. Every user, no matter the gender, has to be encouraged to use substantially stronger passwords because a large fraction of both genders in this research had shown especially risky behaviour, including passwords shorter than eight characters, extensive use of their own personal data while creating passwords (names, dates of birth, emails, and even personal codes), and an overall reliance on dictionary words. However, the largest cause for concern is password reuse. Nearly half of identified females (46%) and a slightly smaller fraction of males (40%) used passwords found in previously leaked databases, and about 16% of all users had a non-unique password. Apparently, this is not a culture-dependent behaviour, because analysis of a breached Chinese dataset (130,000 passwords) showed that trivial passwords such as `111111` or `123456` are in the list of the most common passwords of this culturally specific dataset [35]. Even their average password length (8.4 symbols) was similar to our findings (9.12 symbols). To mitigate the use of weaker passwords, one might consider informing users to use more complex passwords, but in our opinion, the only viable solution is to adopt password manager programs that generate strong and unique passwords for each different service. Websites and databases should also require more complex passwords through the use of algorithms such as `zxcvbn` that analyse password complexity. The adoption of these approaches would help secure data in case of breaches regardless of age and gender.

Our research also confirmed known user habits of password creation. The research of a small university staff and students showed that only 30% of users use special characters, while uppercase letters tend to be placed at the beginning, and numbers are placed at the end of a password [36], which is a pattern we called *ULS+*. In our research, only 2.58% of recovered passwords had a special symbol. It is possible that many more of the 8% of passwords that we failed to crack have these characters, but this will not change the statistics substantially. However, we only found 12.21% of our investigated passwords to use the *ULS+* pattern. On the other hand, we noticed the propensity of Lithuanian users to limit their alphabet to English letters, disregarding the opportunity to strengthen their passwords with specific Lithuanian characters. Table 1 lists two similar dictionaries: Lithuanian words and the Latin version of the same dictionary where diacritic marks were dropped from all letters. The results show that the first dictionary with correctly spelled words has a smaller number of passwords in it. Only 12 passwords having the Lithuanian letters with diacritics (ą, č, ž, and similar) were recovered in total, and none of them were from these two dictionaries. The use of ASCII-only symbols is a historical artefact of how information technology was developed. Early keyboards and operating systems had only English letters, and the post hoc implementation of various other character sets led to many complications in standardisation. In turn, this taught users to fall back to the simplified alphabet to avoid encoding errors in sensitive areas such as password creation. The same is true for other nationalities; e.g. an exceptionally small number of Rockyou words have specific Spanish letters.

Limitations and Strengths

The analysed data sample represents an active and technologically advanced part of the Lithuanian population. Thus, the findings related to cyber hygiene may overestimate the general population's behaviour. There were twice as many males in this study as females, which could cause skewed results, although the statistical analysis takes the differences into account, and every age group of up to 55 years old has at least 100 women. In addition, we cracked only 92% of all leaked hashes. The remaining passwords are stronger and therefore could influence our findings. However, the main conclusions are unlikely to change, because a larger fraction of males (8.51%) have unrecovered passwords compared to females (5.17%), which is consistent with the main findings. Even though the effect sizes in the statistical analysis are considered small, the number of cases can lead to strong generalisations of the findings and might better reflect the differences between genders regarding password complexity.

5. Conclusions and Future Work

Based on the analysis of over 100,000 passwords recovered from a high-quality leaked database, we determined that persons above 45 years old have the weakest passwords, and the strength decreases with age. One reason may be the lack of exposure to IT during their youth, although the exact reasons are left for further research. Although the effect size was small, females had significantly weaker passwords than males for all age groups. In general, the users' password hygiene could be considered very weak. Passwords of around 40% of users were found in previously leaked databases, including the old Rockyou dictionary.

Several additional conclusions arise from the analysed data. Firstly, users could be encouraged to use their entire national alphabet whenever possible—the introduction of special letters (ą, č, ñ, ø) considerably improves password strength. Nevertheless, words or word fragments must be avoided at all costs, no matter their language, spelling, or mangling. It is important to check newly generated passwords against collections of previously leaked passwords.

The strength of the hashing algorithm has little influence on the security of the hashed password because over 70% of user passwords are vulnerable to dictionary attacks. Neither the gender nor age of the user changes the statistics significantly. It might be impossible to persuade every person to use password managers and unique randomly generated passwords for every different application. Hence, the responsibility for password security mainly falls to service providers who should implement password strength meters and enforce password policies. The suggestion to force users to choose stronger passwords via specific means implemented by system developers has been raised before, as simple visual nudges do not influence them to choose longer or stronger passwords [37]. However, our results show that password alone is no longer a viable option, and the only reasonable alternative is multi-factor authentication.

The future directions of the work would be to investigate the development, usage, and policies on password enforcement mechanisms. The qualitative research of selected systems would provide insights into the user behavioural patterns from psychological and educational perspectives. Another possible direction is to research the impact of multi-factor authentication systems on future password complexity and develop methods to encourage more complex passwords. Finally, future research should delve into the underlying causes of the observed insecure user behaviour. In particular, trust in the technology and implications of trust to the complexity of passwords could be explored from the perspective of different age groups and genders.

Author Contributions: Conceptualization, A.J. and A.B.; methodology, A.J., L.B.; software, A.J.; validation, A.J., L.B., R.G.L.; formal analysis, A.J., L.B.; investigation, A.J., L.B., R.G.L.; resources, A.J.; data curation, A.J.; writing—original draft preparation, A.J., A.B., L.B., R.G.L.; writing—review and editing, A.J., A.B., L.B., R.G.L.; visualization, A.J., R.G.L.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: A.J. would like to acknowledge Aleksandras Kulik for his assistance during the password recovery.

Conflicts of Interest: The authors declare no conflict of interest.

Sample Availability: Samples of the aggregated research data are available from the authors.

References

1. Ponemon Institute LLC. *2020 Global Encryption Trends Study*. 2020. Available online: https://www.encryptionconsulting.com/wp-content/uploads/2020/04/2020-Global-Encryption-Trends-Study.pdf (accessed on 1 December 2021).
2. IBM Corporation. Cost of a Data Breach Report 2020. 2020. Available online: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf (accessed on 1 December 2021).
3. PurpleSec LLC. 2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends. 2021. Available online: https://purplesec.us/resources/cyber-security-statistics/ (accessed on 1 December 2021).
4. Statista. Common Password Habits of Online Adults in Selected Countries as of 2019. 2020. Available online: https://www.statista.com/statistics/1147830/common-password-habits-adults-country/ (accessed on 1 December 2021).
5. Statista. Which of These Personal Activities You Do on Your Employer-Issued Laptop and/or Smartphone? 2021. Available online: https://www.statista.com/statistics/1147849/share-adults-worldwide-employer-issued-device-personal-activities/ (accessed on 1 December 2021).
6. Statista. Which of These Activities Do You Allow Friends or Family to Do on Your Employer-Issued Laptop and/or Smartphone? 2021. Available online: https://www.statista.com/statistics/1148992/share-adults-worldwide-friends-family-use-employer-issued-device-personal-activities/ (accessed on 1 December 2021).
7. Statista. Share of Adults in Selected Countries Allowing Friends or Family to Use Their Employer-Issued Device for Personal Activities in 2020. 2021. Available online: https://www.statista.com/statistics/1147938/share-adults-worldwide-friends-family-use-employer-issued-device-personal-activities-country/ (accessed on 1 December 2021).
8. Statista. Share of People Who Have Restricted Applications on Their Smartphone from Accessing Personal Data in Finland in 2018, by Gender. 2018. Available online: https://www.statista.com/statistics/955247/people-restricting-smartphone-apps-data-access-gender-finland/ (accessed on 1 December 2021).
9. McGill, T.; Thompson, N. Gender Differences in Information Security Perceptions and Behaviour. In *Australasian Conference on Information Systems*; Sydney, Australia. University of Technology Sydney ePress. 2018. doi:10.5130/acis2018.co.
10. Anwar, M.; He, W.; Ash, I.; Yuan, X.; Li, L.; Xu, L. Gender difference and employees' cybersecurity behaviors. *Comput. Hum. Behav.* **2017**, *69*, 437–443. doi:10.1016/j.chb.2016.12.040.
11. Kennison, S.M.; Chan-Tin, E. Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Front. Psychol.* **2020**, *11*, 3030. doi:10.3389/fpsyg.2020.546546.
12. Sebescen, N.; Vitak, J. Securing the human: Employee security vulnerability risk in organizational settings. *J. Assoc. Inf. Sci. Technol.* **2017**, *68*, 2237–2247. doi:10.1002/asi.23851.
13. Redmiles, E.M.; Chachra, N.; Waismeyer, B., Examining the Demand for Spam: Who Clicks? In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, 21–26 April 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1–10. doi:10.1145/3173574.3173786.
14. Statista. Password Management by Teenagers in France in 2019. 2019. Available online: https://www.statista.com/statistics/1225114/password-management-by-teens-france/ (accessed on 1 December 2021).
15. Jiow, H.J.; Mwagwabi, F.; Low-Lim, A. Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education. *J. Media Lit. Educ.* **2021**, *13*, 67–78. doi:10.23860/JMLE-2021-13-1-6.
16. Merdenyan, B.; Petrie, H. Generational Differences in Password Management Behaviour. In Proceedings of the 32nd International BCS Human Computer Interaction Conference (HCI), Belfast, UK, 4–6 July 2018; BCS Learning & Development Ltd.: Swindon, UK, 2018. doi:10.14236/ewic/HCI2018.60.
17. Morrison, B.; Coventry, L.; Briggs, P. How do Older Adults feel about engaging with Cyber-Security? *Hum. Behav. Emerg. Technol.* **2021**, *3*, 1033–1049. doi:10.1002/hbe2.291.
18. Furnell, S.; Thomson, K.L. Recognising and addressing 'security fatigue'. *Comput. Fraud. Secur.* **2009**, *2009*, 7–11. doi:10.1016/S1361-3723(09)70139-3.
19. Habib, H.; Naeini, P.E.; Devlin, S.; Oates, M.; Swoopes, C.; Bauer, L.; Christin, N.; Cranor, L.F. User Behaviors and Attitudes Under Password Expiration Policies. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) , Berkeley, CA, USA, 12–14 August 2018; USENIX Association: Baltimore, MD, USA, 2018; pp. 13–30. Available online: https://www.usenix.org/conference/soups2018/presentation/habib-password (accessed on 1 December 2021).
20. Yu, X.; Liao, Q. Understanding user passwords through password prefix and postfix (P3) graph analysis and visualization. *Int. J. Inf. Secur.* **2019**, *18*, 647–663. doi:10.1007/s10207-019-00432-3.
21. Doucek, P.; Pavlíček, L.; Sedláček, J.; Nedomová, L. Adaptation of password strength estimators to a non-English environment—the Czech experience. *Comput. Secur.* **2020**, *95*, 101757. doi:10.1016/j.cose.2020.101757.
22. Wheeler, D.L. zxcvbn: Low-budget password strength estimation. In Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, USA, 10–12 August 2016; pp. 157–173.
23. European Commission. Special Eurobarometer 499: Europeans' Attitudes towards Cyber Security (Cybercrime) (v1.00). (2020). [Data Set]. Available online: http://data.europa.eu/88u/dataset/S2249_92_2_499_ENG (accessed on 1 December 2021).
24. Holroyd, M. Thousands of CityBee users have their personal data leaked online. *Euronews* **2021**. Available online: https://www.euronews.com/2021/02/17/thousands-of-citybee-users-have-their-personal-data-leaked-online (accessed on 1 December 2021).
25. Lithuanian Data Protection Authority (VDAI). Car Rental Company Fined for Data Breach under the General Data Protection Regulation. 2021. Available online: https://etid.link/ETid-927. (accessed on 1 December 2021).

26. Council of European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) . *Off. J. Eur. Union* **2016**, *59*, 1–88.
27. Eastlake 3rd, D.; Jones, P. *RFC 3174: US Secure Hash Algorithm 1 (SHA1)*; RFC 3174, September 2001. doi:10.17487/RFC3174.
28. Maoneke, P.B.; Flowerday, S.; Isabirye, N. The influence of native language on password composition and security: A socioculture theoretical view. *IFIP International Conference on ICT Systems Security and Privacy Protection*; Springer, Cham, 2018; pp. 33–46. doi:10.1007/978-3-319-99828-2_3.
29. Golla, M.; Dürmuth, M. On the accuracy of password strength meters. In *CCS '18, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018*; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1567–1582. doi:10.1145/3243734.3243769.
30. Jones, M.N.; Mewhort, D.J. Case-sensitive letter and bigram frequency counts from large-scale English corpora. *Behav. Res. Methods Instruments Comput.* **2004**, *36*, 388–396.
31. Grigas, G.; Juškevičienė, A. Letter Frequency Analysis of Lithuanian and Other Languages Using the Latin Alphabet. *Coactivity Philol. Educol./Santalka Filol. Edukologija* **2015**, *23*, 81–91. doi:10.3846/cpe.2015.271.
32. Ghasemi, A.; Zahediasl, S. Normality tests for statistical analysis: a guide for non-statisticians. *Int. J. Endocrinol. Metab.* **2012**, *10*, 486. doi:10.5812/ijem.3505.
33. Gelman, A.; Carlin, J. Beyond power calculations: Assessing type S (sign) and type M (magnitude) errors. *Perspect. Psychol. Sci.* **2014**, *9*, 641–651. doi:10.1177/1745691614551642.
34. Petrie, H.; Merdenyan, B. Cultural and Gender Differences in Password Behaviors: Evidence from China, Turkey and the UK. In *NordiCHI '16, Proceedings of the 9th Nordic Conference on Human-Computer Interaction, Gothenburg, Sweden, 23–27 October 2016*; Association for Computing Machinery: New York, NY, USA, 2016; NordiCHI '16. doi:10.1145/2971485.2971563.
35. Li, Y.; Wang, H.; Sun, K. A study of personal information in human-chosen passwords and its security implications. In Proceedings of the IEEE INFOCOM 2016—The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–14 April 2016; pp. 1–9. doi:10.1109/INFOCOM.2016.7524583.
36. Awad, M.; Al-Qudah, Z.; Idwan, S.; Jallad, A.H. Evaluating Password Behavior at a Small University. *J. Comput. Sci.* **2019**, *15*, 1–9. doi:10.3844/jcssp.2019.1.9.
37. Renaud, K.; Zimmerman, V.; Maguire, J.; Draper, S. Lessons Learned from Evaluating Eight Password Nudges in the Wild. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2017)*; USENIX Association: Arlington, VA, USA, 2017; pp. 25–37.