Passwords to Absolutely Avoid

A survey in Greece

George E. Violettas
ICT Dept., Technical Training College
TTC
Riyadh, Kingdom of Saudi Arabia
georgevio@gmail.com

Kyriakos Papadopoulos
Christos Tasioudis
IT Dept., Alexander Technological Educational Institute
of Thessaloniki (ATEITH)
Thessaloniki, Greece

***Abstract*—This paper is describing the password habits of web users, particularly in Greece. A survey was conducted online to ask users questions about the length of the password they use today, in how many web sites they use the same password, whether they use personal data while constructing their passwords and if they ever used as a password some of trivial words. They were also asked whether they reveal their password(s) to friends and/or family and if they ever realized that their password was exposed or revealed to an attacker and the measures they took after that. Additionally, an extended literature review about password habits and effectiveness regarding length and complexity is included. At the end of the paper, for first time in Greece, there is a list of the 100 passwords that Greek users should absolutely avoid using due to the ease of guessing or weak complexity, short length or simply because they exist in every dictionary used for password attacks in the wild.**

Keywords—password; security; survey; web sites;

I. Introduction

During the academic year 2011-12, as part of a Bachelor Thesis for the Aristotle Technical Institute of Thessaloniki, Greece, supervised by the first author, an online survey was conducted for first time in the country about the password habits of Greek web users. The survey asked questions about the length of the passwords used, their strength and structure. There were also questions about the users' habits, i.e. how do they secure their passwords, how do they create them, and when and to whom they reveal them. The survey attempted to identify the users' ability to distinguish a strong from a weak password. Also there are suggestions on creating a strong password, safekeeping it and storing it.

According to the survey findings and extended literature and online research, a catalog of the weakest passwords that the Greek users should absolutely avoid was constructed.

II. Literature Review

Even though passwords are by far the most common security measure we have, not much scientific research has been conducted until today about user habits regarding their passwords.

The most complete survey by far was in [1], conducted over a three months period and included over half a million users. The findings of the survey were fascinating: the average user has 6.5 passwords, each of which is shared across 3.9 different sites. Each user has about 25 accounts requiring passwords and uses an average of eight passwords per day. An important finding was that the users are using a password of an average bit strength of 40.54 bits. It must be stated here that it is a totally different matter if this password could be found in a dictionary. If yes, its recovery is a matter of minutes using password recovery programs like John the Ripper [1]; if no, brute force attack must be used which increases the time frame exponentially. For this reason, the evaluation of passwords in this study is based on simple criteria like length and usage of digits, symbols and uppercase without considering other practices and techniques such as dictionary attacks [2].

Another recent (2013) study [3] evaluated passwords using 14 different meters/scores. Almost 3,000 users used the scoring board (from 0 to 100) to test their own, self-created passwords. The study had some noteworthy results:

- Users change their behavior in the presence of a password-strength meter.
- The most substantial changes in user behavior were elicited by stringent meters, although there is a limit to the stringency that a user can tolerate.
- The meters currently in use on popular websites are not aggressive enough in encouraging users to create strong passwords.

The most important conclusion is that the existence of such meters leads users to create significantly longer passwords including more symbols, digits and uppercase letters, without compromising their memorability and usability.

In [4] the authors built a password estimator comparing the search space versus the number of cracked passwords by various techniques such as dictionary attacks, brute force, probabilistic context free grammars, and Markov chains.

One conclusion from this paper is that it is helpful for users to base their password on their own native language to increase the password strength without additional effort. This is

George Violettas wishes to thank Technical Trainers College in Riyadh, Saudi Arabia for the full financial and moral support he got for this paper.

The findings of the paper are the effort of Kyriakos Papadopoulos and Christos.Tasioudis as part of their bachelor thesis for the Alexander Technological Educational Institute of Thessaloniki under the supervision of George Violettas.

A great thanks goes to Michelle Gately for proofreading the document.

especially helpful in languages with non-Latin alphabet, e.g. Greek, it is a very good idea to use a Greek word in the so called Greekglish writing[1] as one's password.

It is also concluded that passwords are usually comprised of pronounceable sub-strings and/or sequences of keys that are close on the keyboard.

The authors used a recursive algorithm checking the probability of appearance of each character given the previous characters. They state that dictionary attacks and mangling techniques are efficient when the search space is below 10^8. This could be easily interpreted that even if the user is using a dictionary word for her password, if this is "salted" (with uppercase, digits, symbols and adequate length) it is beyond the efficient time space of a dictionary attack.

It is also proven in the same paper that a Markovian chain approach search is by far more efficient than a brute force attack regarding passwords.

The results are that no technique alone is sufficiently discovering given passwords: a combination of Markov-chains, mangling, dictionaries are the tools known today that a possible attacker will use to successfully obtain the password of a given user.

In [5] the authors argue that even weak passwords measuring about 20 bits of entropy -if they are protected by the "three strikes" rule- are strong enough for a single account. They also discovered that for large institutions (e.g. banks, financial institutes, etc.) it is the secrecy, complexity and length of the user ID combined with a password meeting some complexity criteria that makes it very difficult for the attacker(s) to find random weak accounts in such institutions because the search space for any account with one given password is large.

In [6] the authors set the password problem to its correct dimension: "…While passwords seem to be a simple technology, it seems unfair to suggest that authentication is the simplest internet security problem…". They continue by enumerating the most important reasons-barriers that prohibit us to move beyond ubiquitous alphanumeric passwords.

They also discuss some important facts and findings:

- Large-scale usage of passwords on the internet is not well studied, except of course the very detailed survey in [7].
- An understudied problem is the impact on memorability and usability when end-users must remember many different passwords
- Low value, casual transactions may well still use ordinary passwords in ten years or even twenty (although at the introduction of the paper the authors claim that passwords suffer from a number of problems that suggest their reign should be coming to an end). In another paragraph they state that even for 2019 they expect the adoption of password alternatives to continue to be difficult to justify.

III. The survey

The survey for the paper in hands was conducted online. Specifically, many of the commonly used social networks were used, such as Facebook, MSN and college forums. Also extended e-mail lists were used targeting groups such as the Greek Informatics Union members.

Constructing a security questionnaire such as this is not an easy task since a lot of different aspects have to be considered. Parameters such as the anonymity, honesty and practicality had to be taken into consideration. At the end, thirteen questions were formed, so the users wouldn't be intimidated or bored to complete them. Also, the possible answers were all pre-drafted in drop-down menus, for the same above reasons.

Seven hundred and ninety five people participated to the survey conducted from March 8, until September 30, 2012 and it was available online at http://tinyurl.com/pass-questions. The survey was posted on various online sites. There is an open question, still, if people were hesitant to document their password habits and uses for security reasons. Although all possible measures were taken to guaranty the anonymity of the participants, the response to the survey was not as robust as hoped. There was no statistics kept about age, sex, logging IP addresses etc. For this reason, it is not possible to compare the findings of this survey with demographics etc.

The survey strived to document aspects of the everyday usage of passwords on the internet, specifically issues such as:

- Passwords used in the past
- Habits of changing (or not) passwords
- Complexity of passwords
- Ability to distinguish a weak password
- Number of total passwords used
- Ways of remembering (or storing) a password
- Probability (and/or possibility) of revealing a password

Users were also asked to reveal one (or more) password(s) they used in the past but they changed it for security reasons (or concerns). This resulted to the creation of the list with the weakest passwords (to absolutely avoid) for the Greek users.

A. *Q1. Weak Passwords used in the Past, or still being used*

The first question of the survey was asking the users if they did use a weak (in their opinion) password in the past and if yes which one they used, and if they had to change it for security

[1] Greeklish is writing in Greek language using the Latin alphabet. It started with the early age of computers when non Latin language keyboards were not supported and many times writing in those languages resulting to unintelligible text. Greeklish is used especially from young people in the web today and is very much accused and blamed for leading people to use poor orthography.

reasons. On the list provided, users could choose one or more of the passwords listed, or none of the passwords mentioned.

A large percentage (32%) of the users answered that they never used such a password in the past. But, also very high was the percentage (27%) of people answering that they used “1234” as their password. The same percentage of people (27%) answered that they used their own name as a password. A sizeable percentage (14%) of people used “123”, while 13% of people used the name of a local sports team (“παοκ”) as a password. Obviously there is a bias here[2] but nevertheless, the result remains that the name of the user’s favorite football team scores very high in this question.

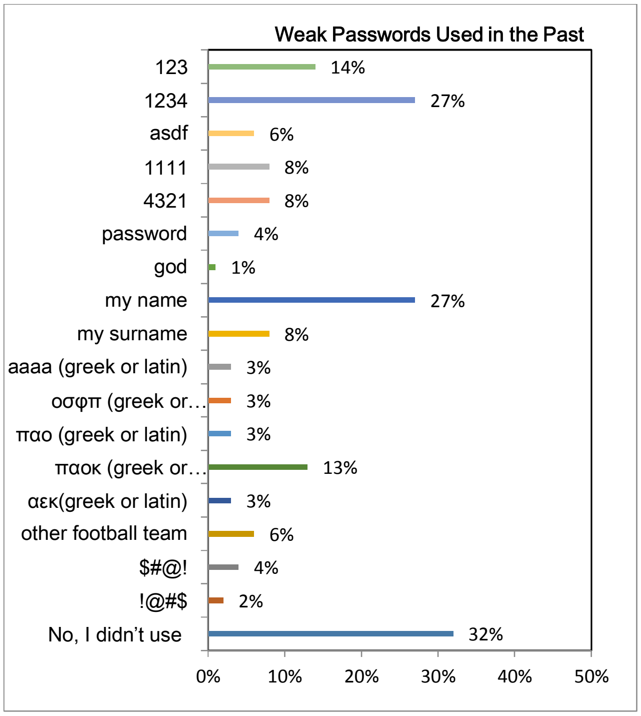

Fig. 2: Question No 1. Are you using or did you ever used any of the mentioned passwords or one that looks a lot like those?[3]

Summarizing the percentages of those who have answered that they used their football team name as a password yields a 31%, which is a very high number.

Also note that some of the passwords in Fig. 1 are sequential on the Latin keyboard. I.e. “$#@!” is the sequential Shift +4,3,2,1 characters, whilst the “!@#$” is the opposite.

B. Q2. Common/Not Safe Passwords

The vast majority of the users managed to identify correctly the most commonly used passwords that are considered to be totally unsafe today. Passwords like “123456” were identified as unsafe from nine out of ten users. The word “password” or the word “Mercedes” were also identified as unsafe from almost 60% and 40% respectively as common. It has to be mentioned here that the users in this question are just selecting the one or two passwords that are most obvious for them to be unsafe. That is why “123456” received an almost “perfect” score, since almost everybody “voted” for it. Not ticking on “xxxxxxx”, it doesn’t necessarily mean that the user doesn’t consider it unsafe; it just means that the user found “123456” much more unsafe than “xxxxxxxx” and clicked on just this one.

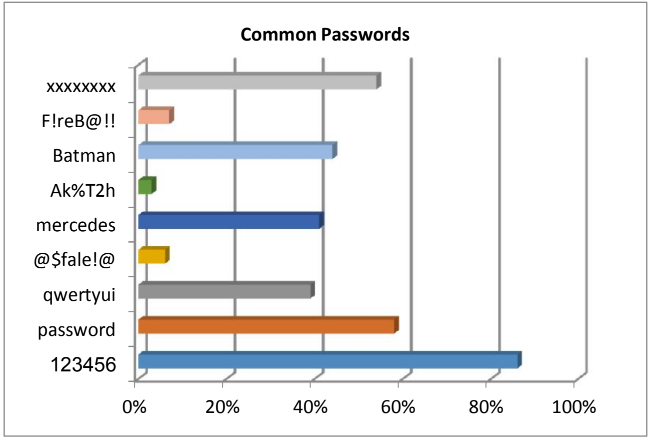

Fig. 1: Question No 4. Which of the above do you consider as common/not safe passwords to avoid?

It’s also worth mentioning here, that passwords such as “F!reB@!!” look complicated, and they really are, since they are using special characters and symbols extending the complexity of the password, but they are rather mistakenly identified as “safe” since their length is fewer than eight characters, which is widely considered to be the minimum length of a password today [8],[9],[10].

C. Q3. Freqeuency of password change

Although web sites like Microsoft [11] Google [12] or other big companies, suggest the users to change their passwords often, when the users were asked the question “how often do you change your password?” the results were rather disappointing: Just a 13% of the users change their password often, while on the other side, two out of five people (39%) have never changed their password!

The positive aspect about this question is that in another research study [13] conducted in 2006, with the same exact question, more than half of the users (52%) had never changed their password.

Considering the time passage, we can safely conclude that users today are more concerned about password issues than in the past, but the percentage of those “left behind” is still too high to ignore. Although today there are a lot of major web sites asking the users to change their password often [10],[11],[12] especially if those passwords fail to meet the security criteria, users tend to completely ignore this rule.

[2] The two authors-students responsible for conducting the online survey lived in Thessaloniki, where this particular football team is dominative. If the survey started from people living into Southern Greece (e.g. Athens) the result of this question would be in favor of a football team based there.

[3] Notice that the Greek words «οσφπ», «παο», «παοκ», «αεκ» are the names of some of the most popular football teams in Greece. The questions were asking the users if they ever used those names, either in Greek or in Latin writing.

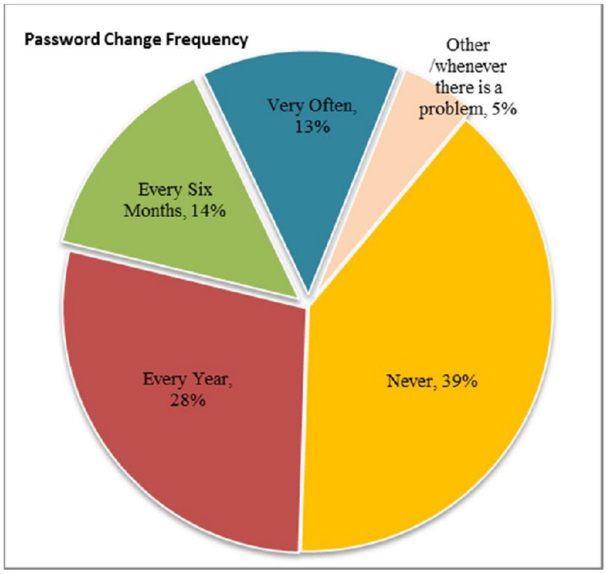

Fig. 3: Question No 3: How often do you change your password?

Only a very small percentage (a little more than one out of ten) of the users admit that they are changing their password(s) often, whereas four out of ten people (39%) never (!) change their password(s) as depicted in Fig.3. The rest of the users, are changing the password every year (almost three out of ten) or every six months (14%).

D. Q4. Complexity of Password

This question was meant to explore whether the users are aware of the complexity requirements of passwords. More specifically, the question asked if they are using symbols, numbers, or punctuation marks. The vast majority (almost eight out of ten users) answered positively, meaning that users today at least they know that passwords should have some of the above mentioned characters. Obviously the problem here is that looking back at the findings of Question No 2, nowadays users are not using the complexity rules that they know they have to!

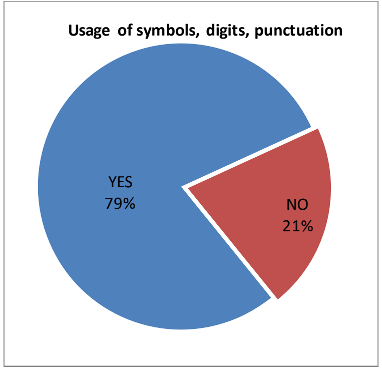

Fig. 4: Question No 4. Are you using symbols, numbers or punctuation marks in your password(s)?

E. Q5. Multitude of (different) passwords used

Users were asked how many different passwords they are using for webpages on the internet. The question was not more complicated intentionally, omitting the possibility of asking about local applications or computers. The answer is representative of the users' habits, i.e. if someone is using a lot of different passwords on the internet, she will tent to do the same for local applications and vice versa.

Almost half of the users (48%) were using two or three different passwords, so if someone knows one of those passwords, Trudy (the intruder) can access one third of the user's internet services, while Trudy can access all the services of the one third of the users that are using just one password! So the total number of users potentially under a serious security breach is 80%. Only 17% of the users are using a different password for every web page. Adding here the tendency of people to lie for such things, we have to seriously consider that the number of people using a different password for every service is even smaller!

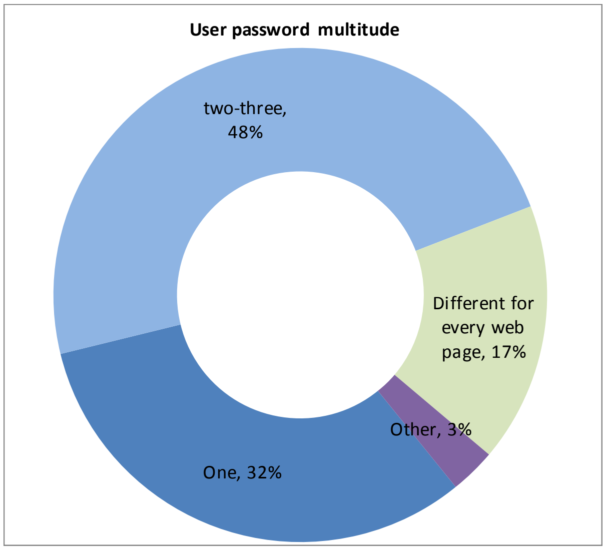

Fig. 5: Question No 5. How many different password(s) are you using for web pages?

The findings of this question are more or less in full accordance with the findings of past surveys [7],[14] mentioning in the first that each average user has 6.5 passwords, the latter three or less. It has to be mentioned here that password reuse can lead to some terrifying effects with great cost in real money such as the cases described here [15].

F. Q6 & Q7. Adequate length of password & your password length

The users were asked to comment on how many characters do they think that a safe password consist of. Almost seven out of ten people (68%) said that this number has to be greater than eight. Less than one out of ten (8%) said that four to five characters is a strong password. The good thing here is that (if the users are not lying or exaggerating) the findings of Question No 7 are almost identical with the findings of Question No 6.

Also it is noticeable that in [7] a great percentage (63% of lowercase passwords, 27% of digit only passwords, 8% alphanumeric passwords) of users are using a password of fewer than seven digits (Fig 9. bit strength less than 50); in the current survey only 25% of the users said that they are using those short passwords.

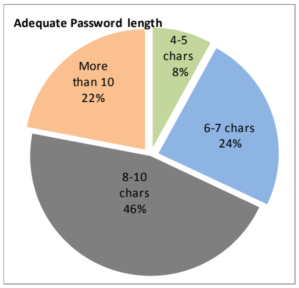

Fig. 6: Question No 6: How many characters do you think are needed for a "strong" password?

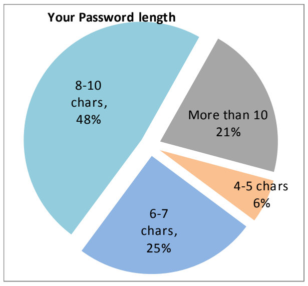

Fig. 7: Question No 7: How many characters long is your password?

G. Q8. Remembrance of a Password

The users were asked to comment on what they use to help them remember their password. This question is the main problem of the weak passwords today [16],[17]: eight out of ten users answered by memorizing. This is the problem: Memorizing the password means that it has to be memorable, so it is a word in dictionaries [7], or something familiar to the user, like his birthday, car's brand, children name etc., or the password has to follow some pattern, which if discovered, can lead straight to it.

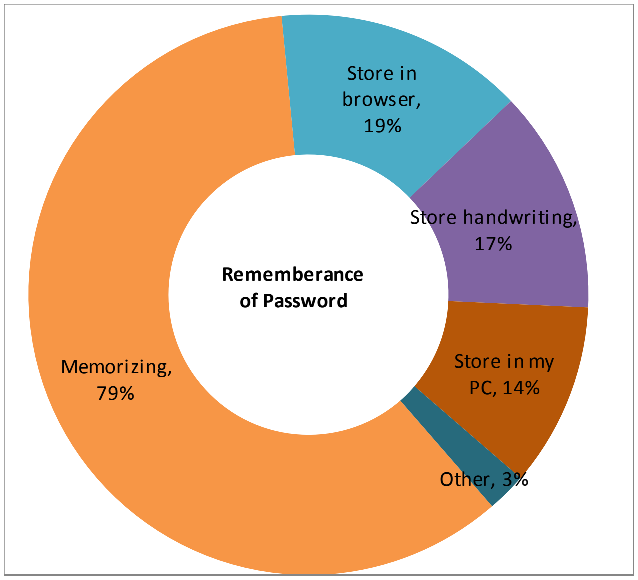

Fig. 8: Question No 8. What do you use to remember/store your password(s)?

The rest of the user's answers are even worse: 14% are storing passwords inside the computer, or even a 17% is storing them in handwritten notes (obviously somewhere close to the computer and easily discoverable)[4].

H. Q9. Usage of personal data into the password

The users were asked to answer if (and what) they are using information from their personal data as parts of their passwords, although every password guide is strongly discouraging them against such policy [11],[12]. Three out of ten people are using their birth date. The same date they publish in every social network they sign in! 26% of them are using their name as part of their password! Mobile phone number and address are used by one out of ten users respectively. Also easily accessible information such as name of spouse or children, pet's name and car brand get significantly high percentages; the same exact information that users "spread" all over social networks like Facebook etc.

So people with enough patience and some social engineering skills [18] can relatively easy discern those passwords.

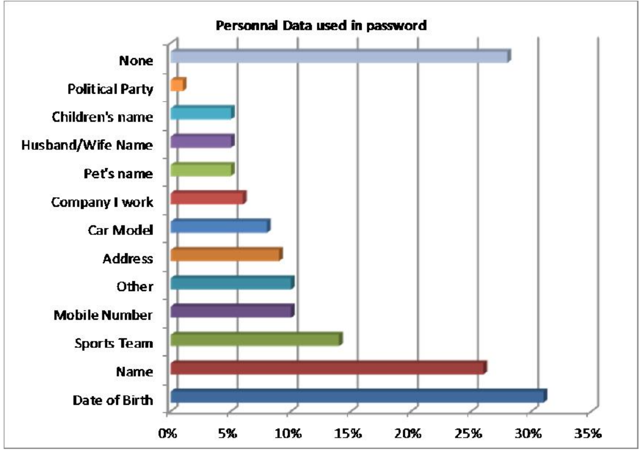

Fig. 9: Question No 9. Are you using any (or some) of the following as parts of your password(s)?

I. Q10 & Q11. Password Disclosure

There were two different questions about password disclosure to the users.

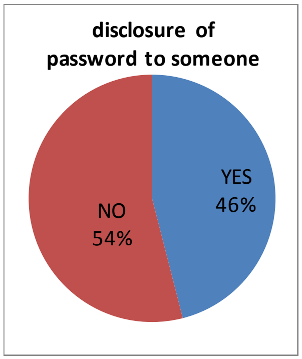

Fig. 10: Question No 10. Did you ever disclose your password(s) to someone you know to use them in your behalf?

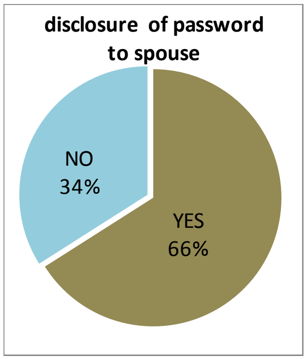

Fig. 11: Question No 11. Did you ever disclose your password(s) to your spouse

Question No 10 asked the users if they ever disclosed their password to someone they know, to use it on their behalf. Almost one out of two of them answered positively, meaning that regarding the half of the internet users, at least one other person knows (one of) their password. Combining this with the findings of Question No 5, 80% of the users revealed their one

[4] This looks a lot like the key under the front door carpet or under the pot twenty years ago…

and only, or at the best case the one out of three passwords they are using, to another person. I.e. combining 46% shared X 80% single/only password means 36.8% of the password related information is not secure.

Question No 11 is more interesting because two out of three users (66%) have revealed their password to their spouse. Combining this with the above, means that the vast majority of people today have given access to their very personal data to their spouse or another person they know!

J. Q12. Possible Password Interception

The percentage of people changing their password has to be viewed in conjunction with this next question, i.e. one out of three users believes that sometime, somehow their password for some application or service was intercepted or leaked.

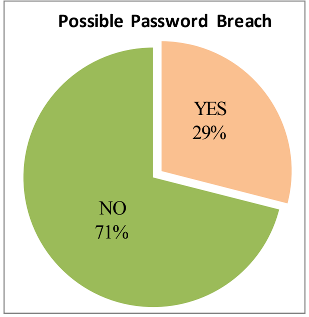

Fig. 12: Question No 12. Do you believe that your password for some service has been compromised?

This means that many people changed their password because they sensed that this password was somehow intercepted, although only 5% of people in the previous question answered that the changed their password because of a security problem!

K. Q13. Weak Passwords (not) to Use

This question is close related to questions No 1, 2, and 9. It is asking the users more or less the same thing: identify the passwords to avoid, i.e., find the passwords that a typical user of the internet today should absolutely avoid to use, because they are very easy to guess or to be compromised with little effort from the attacker.

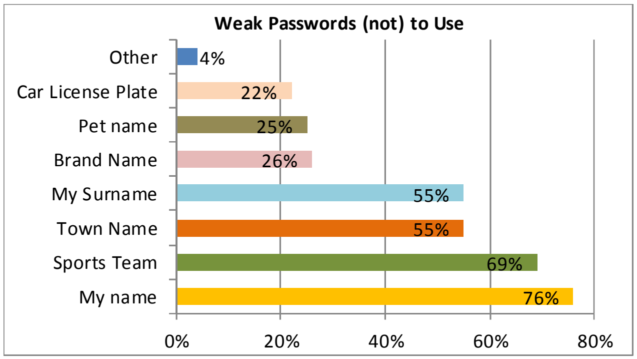

Fig. 13: Question 13. Which of the following passwords do you consider weak to use?

This question was asked in such different ways, because as it will be shown below, a matrix with those "top" passwords was constructed for the first time in Greece.

IV. Conclusions

A. The 100 Greeklish Passwords to Avoid

Our contribution was that combining the data from those questions above, a matrix was constructed with the most common passwords in the Greek language, which users should absolutely avoid nowadays.

	TOP 1-25	TOP 26-50	TOP 51-75	TOP 76-100
1	1234	aek-21	super3	Masoutis
2	123456	ΠΑΟΚ	qwerty	Marinopoulos
3	4321	ΑΕΚ	ΟΣΦΠ	osfp
4	654321	paok4	thessaloniki	Serres
5	1111	παοκ-θ4	athina	patra
6	123	Olympiakos7	volos	Carrefour
7	321	olympiakos	o-s-f-p	Multirama
8	!@#$	panathinaikos	A.E.K	μαρία
9	$#@!	θεος	Pao-13	Maria
10	password	pao	osfp	Giannis
11	!!!!	papadopoulos	giannis	Dimitris
12	αααα	george	nikos	Cyta
13	aaaa	giorgos	gewrgia	panagiwtis
14	QWERTY	vaso	xristos	sofia
15	theos	eirini	mazda	xristina
16	katerina	mercedes	savalas	ford
17	dimitra	nikolaou	karamanlis	honda
18	bmw	petridis	anna	opel
19	fiat	eleni	toyota	kostas
20	spiti	papandreou	Plaisio	e-shop
21	wind	germanos	vodafone	cosmote
22	Asdf	ασδφ	greece	Conn-x
23	volvo	Q-TELECOM	Tellas	forthnet
24	Audi	honda	nissan	Peugeot
25	Dunlop	michelin	Pirelli	Renault

Fig. 14: Top-100 passwords that the Greek users should absolutely avoid using

The above list contains the most common "version" of this particular password and all other "flavors" of this password should be avoided as well. E.g., the word "giorgos" in Greek means "George', so using your name as part of your password, even if it is something less common like "Pelopidas", is not making your password any stronger. The same applies if you published in social media your favoritism for a specific football team, even if this is not "Barcelona", it is not wise to use it as part of your password(s). It is also obvious that there are many more common Greek words that were not included into the above list, which under no circumstances should be considered full and complete. Hence the above matrix is just a guide and not an exact list.

Most of the Greek alphabet words in Fig. 14 are popular Greek football teams; Greek users should consider that using passwords written with the Greek alphabet, if the password is that easy as the above mentioned words, is not making it any harder to break despite the advice before (Section II) that users should consider using passwords in their native language [4].

B. *Rules for not "easy" passwords*

Users today already seem to know the basics about passwords. Summing up we can say that a "good" password should not use any of the following:

- Your name
- Spouse name
- Parent(s) name
- Pet's name
- Children names
- Names of beloved famous persons (e.g. your favorite football player)
- Telephone Number
- License Plate Number
- Public Service(s) Number(s) (E.g. VAT registration, ID Number etc.)
- Any kind of information that can be linked to you especially through social media (Facebook etc.)
- Repeated letters or phrases, or keyboard patterns like "qwerty"
- All the above written backwards or followed or leaded by one digit

Summarizing this, we have to add that if someone is trying to find the password of a particular person, he will start looking for the victim's personal data. So a password of the form "Isabella1977" looks strong enough, unless your wife's name is Isabella and she was born in 1977!

I. Conclusion

In general, it can be said that users today are more aware of the importance of the password strength and complexity than a few years ago. A big percentage of the users answering the questionnaire above never used an "easy" password or one of the classic passwords to avoid.

However, there is still a majority of users who are using two or three passwords or even just one for all their online services. If this is combined with a very high percentage of users who have revealed those passwords to at least one person they know, this consists a serious potential intrusion to their personal life and data.

Also, even today, public organizations should start a campaign to try to awaken as many users as they can to start using the basic steps and techniques described above, i.e. using more than two or three passwords, strengthen passwords by enriching them with letters, punctuation marks and symbols, extending their length to at least than 8 characters and not revealing them (especially to their partner!).

Maybe the Greek Union of Informatics should standardize the above and ask the Ministry of Education to insert it into courses of Informatics to all schools in Greece.

II. References

[1] Openwall, "John the Ripper password cracker," *John the Ripper password cracker*. [Online]. Available: http://www.openwall.com/john/. [Accessed: 12-Nov-2013].

[2] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, "Password cracking using probabilistic context-free grammars," in *Security and Privacy, 2009 30th IEEE Symposium on*, 2009, pp. 391–405.

[3] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, and L. Bauer, "How does your password measure up? The effect of strength meters on password creation," in *Proc. USENIX Security*, 2012.

[4] M. Dell'Amico, P. Michiardi, and Y. Roudier, "Password strength: an empirical analysis," in *INFOCOM, 2010 Proceedings IEEE*, 2010, pp. 1–9.

[5] D. Florêncio, C. Herley, and B. Coskun, "Do strong web passwords accomplish anything," *Proc Usenix Hot Top. Secur.*, 2007.

[6] C. Herley, P. C. van Oorschot, and A. S. Patrick, "Passwords: If we're so smart, why are we still using them?," in *Financial Cryptography and Data Security*, Springer, 2009, pp. 230–237.

[7] D. Florencio and C. Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 657–666.

[8] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012, pp. 523–537.

[9] NIST, "Electronic Authentication Guideline." Dec-2011.

[10] Yahoo, "Helpcentral Help | - SLN3012 - Create a secure, strong password," *Create a secure, strong password*, 2013. [Online]. Available: http://help.yahoo.com/kb/index?locale=en_US&page=content&id=SLN3012. [Accessed: 14-Nov-2013].

[11] Microsoft, "Change Passwords | Create Strong Passwords | Microsoft Security," *Create strong passwords*, 2013. [Online]. Available: http://www.microsoft.com/en-GB/security/online-privacy/passwords-create.aspx. [Accessed: 14-Nov-2013].

[12] Google, "Choosing a smart password - Accounts Help," *Choosing a smart password*, 2013. [Online]. Available: https://support.google.com/accounts/answer/32040. [Accessed: 14-Nov-2013].

[13] S. Riley, "Password security: What users know and what they actually do," *Usability News*, vol. 8, no. 1, 2006.

[14] S. Gaw and E. W. Felten, "Password Management Strategies for Online Accounts," in *Proceedings of the Second Symposium on Usable Privacy and Security*, New York, NY, USA, 2006, pp. 44–55.

[15] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," *Commun. ACM*, vol. 47, no. 4, pp. 75–78, 2004.

[16] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *Secur. Priv. IEEE*, vol. 2, no. 5, pp. 25–31, 2004.

[17] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2010, pp. 383–392.

[18] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. Wiley. com, 2001.