National Password Security Survey: Results

K. Helkala[1] and T.H. Bakås[2]

[1]Norwegian Defence Cyber Academy and Gjøvik University College
[2]Norwegian Centre for Information Security
e-mail: kirsi.helkala@gmail.com, tone@norsis.no

Abstract

Research, especially in the early 21st century, has shown that education is needed to change people's behaviour regarding password generation, management and storage. As our daily routines and duties have become more dependent on electronic services in the last decade, one could think that qualitative education is nowadays given to users. To verify this assumption we conducted a nation-wide, demographic survey in Norway with a sample of 1003 respondents at the age of 18 to 64. The results show that the education or proper guidance seldom is given leading to the outdated users' behavior.

Keywords

Password security, Information security awareness

1. Introduction

Password authentication has existed several decades and it is likely to remain one of the top authentication mechanisms also in the future (Kuhn and Garrison, 2009, Bonneau and Preibusch, 2010). The latest biannual survey on security incidences, data criminality and countermeasures among Norwegian industry conducted by The Security Council of Norwegian Industry (NSR, 2012) reveals that organizations are increasing their usage of information technologies. For example, from 2008 to 2012 the use of mobile phones to receive emails has increased from 54% to 71%, use of social media for internal information exchange from 0% to 16% and for external information exchange from 3% to 39%. All these accounts are password protected.

It is common to think that everybody has knowledge of how to create, store and manage passwords without education. However, research shows the opposite (Horcher and Tejay, 2009, Katz, 2005, Sasse et al., 2001). As the use of the electronic information technologies increases, one could think that basic training is given to children, in-depth education within studies and repetition guidance in accordance with needs of the working environment. This would lead to increasing information security awareness, including password security. We were eager to learn how the situation is in practice and launched a nationwide password survey in Norway. YouGov Norway, a leading Internet based market research institute in the Nordic region (YouGov, 2013), collected the data. The survey was sent to a natural representation of employees at the age of 18 to 64. A total number of 1003 respondents answered the questionnaire.

2. Related Work

As password authentication is an old method, there are plenty of surveys available, such as pure password surveys e.g. (CSID, 2012), information security awareness surveys e.g. (Talib et al., 2010), password policy surveys e.g. (Florêncio and Herley, 2010) or a nation wide security incidences, data criminality and countermeasures surveys e.g. (NSR, 2012).

The results of NSR survey (NSR, 2012) showed that the amount of given education has decreased from 2010 and only four tenth of newly employed have gotten security training. Talib et al. (Talib et al., 2010) executed a survey about information security awareness within home and work environments. As the survey mainly concentrated on users' understanding of security threats, passwords were also included. 45% of the respondents who had not gotten any security awareness training used passwords containing letters, digits and special characters and the passwords were minimum 8 characters long. 61% of the respondents also kept the passwords to themselves.

Florêncio and Herley studied password policies of 75 different websites (Florêncio and Herley, 2010). They found that sites that accept advertising and purchase-sponsored links have a negative correlation with password strength. Shay et al. studied user attitudes after password policy change in Carnegie Mellom University (Shay et al., 2010). The new policy required the minimum of eight characters and at least one character from each character sets: lower case letters, upper case letters, digits and symbols. The passwords were also compared against dictionaries. Results showed that the users found the new policy annoying but believed it to provide better security. The new passwords were created by modifying the old ones and the use of words and names was the most often used password creation strategy.

Hoonakker et al. (Hoonakker et al., 2009) made a password survey from a human factor perspective in a large organization. The results showed that in average a user had nine password accounts, 18% of the respondents used the same password always, 50% reused sometimes, and in average passwords were renewed seven times a year. A password security survey on Symantec Security Response blog (Haley, 2010) found that 44% of the respondents had more than 20 password protected accounts, 45% had few passwords circulating on their accounts and 63% changed their passwords less than once a year. Kumar (Kumar, 2011) studied usability of passwords in practice among students and staff in University at New Delhi. 60% of the respondents had more than six password accounts, 79% reused their passwords and only 30% used different passwords in different accounts. CSID made a demographical survey about password habits of American consumers (CSID, 2012). 61% of the consumers reused their passwords, 54% had less than five passwords, 44% changed their password less than once a year and 21% had experienced a compromise of an online account.

Previously mentioned pure password surveys are very general and do not separate different user groups based on the background information of respondents. They also fail to look at connections. In our study, we have looked at differences between age, gender, occupation and educational groups and identified reasons for behaviour.

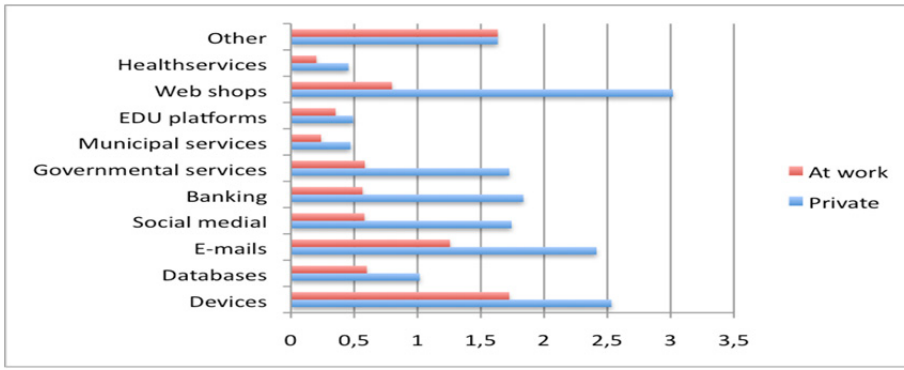

Figure 1: Number of passwords.

3. Results of Questionnaire

We had a total of 1003 respondents. 57% were men, 43% female, 28% were at age 18-34 years, 41% at age 35-49 years and 31% at age 50-64 years. 10% were Executives, 8% Managers, 14% Project managers, 14% Head of departments, 52% Regular employees and 2% were other workers. Questions are listed in Appendix.

3.1. Total numbers of passwords

We found the minimum number of private passwords as 17.3 passwords per person and work related 8.5 passwords per person. *This leads to minimum number of passwords per person to 25.* Figure 1 shows the average number of the password-protected accounts vs. services. The devices included PCs, tablets and phones.

3.2. Education of good passwords

59% of the subjects stated that they had gotten education or guidance on how to generate good passwords. 28% of these had gotten guidelines either from newspapers or websites, 22% at work, 12% during studies and 11% from friends or colleagues. From all respondents, 6% did not remember and *35% stated that they had not gotten any guidance*. This is rather high percentage when considering that password security guidance is often given in security awareness training e.g (Junglemap, 2013). However, the results support a finding in (NSR, 2012) that only four tenths of

	Executive	Manager	Project Manager	Head of Depart.	Regular Employee	Other
Studies	11 %	9 %	16 %	15 %	11 %	6 %
At work	13 %	24 %	39 %	24 %	19 %	0 %
Friends	16 %	16 %	9 %	13 %	10 %	22 %
Websites	**28 %**	**32 %**	**35 %**	**23 %**	**27 %**	**44 %**
Other	3 %	1 %	7 %	1 %	3 %	6 %
Not remem.	7 %	10 %	3 %	8 %	7 %	6 %
Not gotten	**42 %**	25 %	23 %	34 %	**38 %**	28 %

Table 1: Password education vs. occupations.

newly employed had gotten training. With 95% confidence, 35±5% of the respondents at age 18-34 years, 35±5% at age 35-49 and 33±5% at age 50-64 had not gotten education meaning that there is no statistical difference between age groups.

Comparison of password education and occupations is shown in Table 1. *Websites and newspapers are the main source of password education*. *The shocking result was that as high as 42% of executives had not received education*. This might have consequences. Executives have access to most of the assets of the organization. If these assets are password protected, the protection given by the executive might be low. The untrained executives might also oversee the need of education for others.

When asked which websites were used 60% of the respondents did not remember and 1% did not want to say. 10% of those who remembered mentioned VG, 7% Dagbladet and 6% Aftenposten (Norwegian newspapers). 5% of users named The Norwegian Broadcasting Corporation (NRK). Among IT-magazines mostly used was Digi by 12%, ITavisen and Computerword by 1-2% and general information site DinSide by 6% of users. However, none of these sites has a static guidance available. 3% of the respondents listed guidance given by the services themselves. A static

		Password Type (Helkala, 2011)		
		Word	**Mixture**	**Non-Word**
NorSIS (NorSIS, 2012)	**Recommended**	Not mentioned	Yes	Yes
	Min length		20	9
	Character sets		From examples: Uc, lc and sc	From examples: Uc, lc, and d
	Examples		A sentence with a modified letter	First characters from a song
	Other info	Do not reuse, do not share, association helps memorization, change passwords regularly, do not let programs remember passwords and log out after use. Additional information about hacking methods.		
Hardware (Benediktsson, 2012)	**Recommended**	Not	Not mentioned	Yes
	Min length			8, better if 12
	Character sets			Uc, lc, d and sc
	Examples			First characters taken a sentence
	Other info	Avoid using the same character in a password, avoid using characters in the same order that they are found on a keyboard, do not reuse, change regularly. Additional information about hacking methods.		
NSM (NSM, 2002)	**Recommended**	Password type has not been given.		
	Min length	14		
	Character sets	Uc, lc, d and sc		
	Examples	Not given		
	Other info	Do not reuse, change after 90 days, log out, min age for a password one day and if written down, the note has to be stored in a secure place.		

Table 2: Password guidelines by NSM, NorSIS and Hardware.

guidance site is found in IT-magazine Hardware and official security sites of The Norwegian National Security Authority (NSM) and The Norwegian Centre for Information Security (NorSIS), but only 1% of the respondents had found Hardware and 4% NSM and NorSIS. The guidelines are listed in Table 2.

3.3. Description of a good password

After learning where the users got their password guidelines, we were interested to know what they have actually learned. Therefore, we asked them to describe what a good password is in their own words. From all respondents 10% did not want to reveal their description and 4% did not know. The rest 86% had an opinion. We compared those who had gotten guidance and who had not by used character sets and minimum length of passwords, Table 3. *The users with guidance include special characters in their passwords more often than the users without guidance*. There is no statistical difference on the minimum length. However, a good password is more than characters and length. The respondents had considered the following.

Personal information: 19% of the respondents with an opinion considered personal information as worth of mentioning. 35% of these had not gotten guidance and 65% had received guidance. Large majority in *both groups stated that personal information should not be used* and there was no statistical difference between groups (guidance: 95±4% and without guidance: 89±8% with 95% confidence).

Words: 20% of the subjects with an opinion discussed about words. 73% of these had gotten guidance and 27% had not. The use of single words either alone or together with digits, is a bad habit. However, use of several modified words or use of sentences adds robustness against password cracking (Helkala et al. 2012). Due to the small number of users without guidance in this case, we can conclude only with 90% confidence that *the users without guidance more often use pure words* (38±11% of the respondents without guidance and 21±6% with guidance). Modified words where some letters are replaced with other letters, digits or special characters are

		NO GUIDANCE	GUIDANCE
CHARACTER SET	Had no opinion/ Did not want to reveal/ Did not know	38%	19%
	Had an opinion	62% 1 Char set: 1,3% 2 Char sets: 30% 3 Char sets: 56% 4 Char sets: 13±4% (95% conf.)	81% 1 Char set: 0,3% 2 Char sets: 23% 3 Char sets: 54% 4 Char sets: 23±4% (95% conf.)
MIN LENGHT	Had no opinion/ Did not want to reveal/ Did not know	89%	78%
	Mentioned	11% Average: 7,6 ±0,4 (95% conf.)	22% Average: 8,1 ±0,4 (95% conf.)

Table 3: Guidance/No guidance vs. Character sets and length (1 set: digits, 2 sets: digits and one set of letters, 3 sets: digits and both letter cases, 4 sets: all characters.)

used by 2% of the respondents without guidance and 4% with guidance. 53% of the respondents without guidance and 65% with guidance stated that words should not be used. However, the education shows in *variation of password structures*. 8% of the users with guidance gave memorization tricks such as passphrase and 9% use full sentences. For non-educated, the percentages are 0% and 6%, respectively.

Summa summarum, according to majority of respondents "*A good password is a mixture of letters and digits*." This statement is not corresponding to the Norwegian security authorities (NSM, 2009, NorSIS, 2012) or NIST (NIST, 2009). The description is not a surprise taking into account that more than half of the respondents have not had guidance or have received it from websites. The private devices together with web shops, email, social media and cloud accounts constitutes at least half of the private password accounts and when the top traffic sites such as Google, Facebook, Yahoo! and Youtube accept weak passwords as min length between 6-8 characters and only one character sets (Florêncio and Herley, 2010) it is no wonder that a good password description is as it is. When asked if the users follow their own "good password" description 25% of the respondents claimed that all their passwords are good ones, 38% stated that most of them are, 24% said that some of them are good, 8% did not have any good ones and 5% did not know.

As an alternative for own password creation, passwords can be gotten from online password generators e.g. (GRC 2013). However, there is no guarantee that generated passwords are not further used in either direct attacks or indirect attacks by adding hashes of the passwords on online hash lists. The respondents were asked to comment these generators. Results showed that 46% of the respondents had never heard of them and 10% thought that they were good tools for password generation. 13% of the respondents do not use them because they do not know who has access to the generated passwords and 16% do not use them because the generated passwords are hard to remember. 13% did not have an opinion and 3% had some other opinion.

3.4. Confidential Information Protected by Extra Good Passwords

We do not claim that all passwords should be good or strong ones. The accounts that do not contain private and confidential information such as sport activity blogs do not need strong protection. Therefore, we were interested to see how end-users themselves rank the different services based on the accounts' security need, and if they use stronger passwords in these accounts. Figure 2 shows that more than *90% of the respondents stated that bank accounts need to be well protected, more than 70% said the same about email-accounts, and more than 65% considered devices and governmental services* like online social security service as accounts that need stronger password protection. *However, only 31% of the respondents always use stronger passwords in the services they thought should be protected by better passwords*, 27% use usually, 19% sometimes, 19% do not use and 5% do not know.

3.5. Reuse and remembering of Passwords

In our study, *12% of the respondents always reuse their passwords, 62% reuse sometimes* and 15% seldom. 9% of the subjects stated that they never reuse their

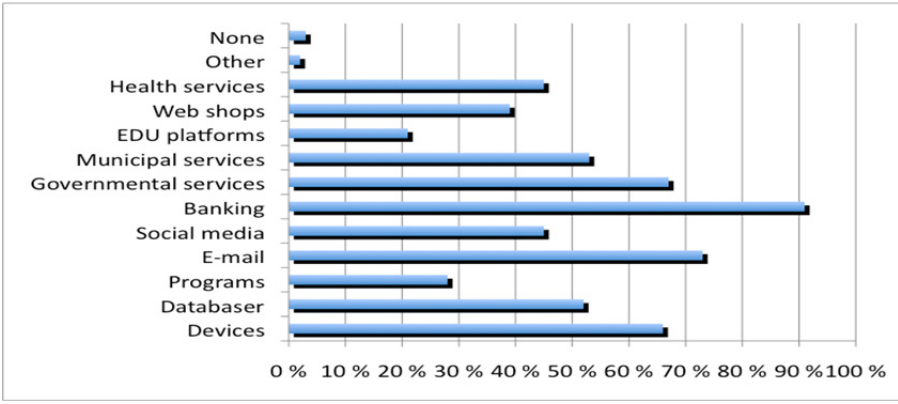

Figure 2: Services that should be protected by extra good passwords

passwords and 2% do not know. The percent of reuse is high. However, there is a difference between genders. We found that *males reuse less passwords than females* ("do not reuse" with 95% confidence: men 12±3% and female 6±2%). There is no statistical difference between ages. Figure 3 shows reuse percentages vs. gender and age. 43% of the respondents claimed to remember all their passwords, 33% use reset option for the passwords their cannot recall, 20% write them down, 1% remember only the login passwords and otherwise trust the browser to remember the rest and 3% use some other methods. We also wanted to know where the passwords are written down. *51% of those who write passwords down have a note either at home or at work place*, 23% store passwords on a text file either on PC or phone, 11% use software for storing, 13% have other methods, 6% carry a note with them and 3% do not know. Differences among genders were found. *With 90% confidence men trust their memory more than females when it comes password remembering and with 95% confidence females more often use a reset option* (remember all passwords: men 46±3% and female: 38±4%, use reset option: men 29±4% and female: 39±5%).

3.6. Sharing Passwords

Among our respondents, *63% do not share their passwords, 31% share with a spouse or partner,* 7% with their children, 4% with colleagues, 2% with IT, 2% with

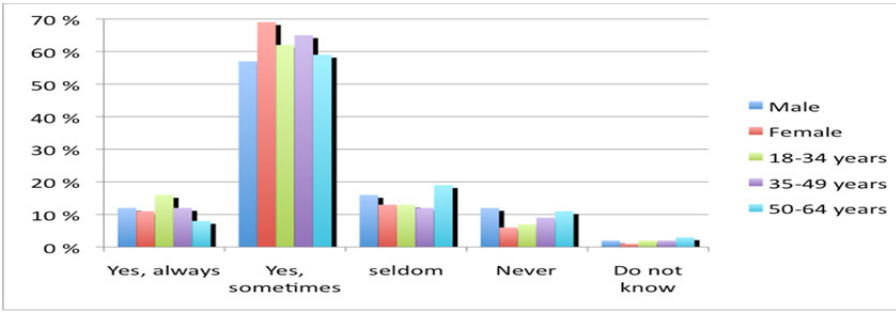

Figure 3: Reuse of passwords among gender and age groups

friends, 1% with bank and 1% with boss. There is no statistical difference between different genders or different age groups. We were also keen on knowing which accounts users trusted for others to use when they shared their passwords. *An interesting finding is that passwords, which protect devices, are earlier stated to be the stronger passwords, however, they are also the most often shared passwords*, see Figure 4. The next shared passwords belong to programs and web shop accounts. The data indicates that females share their private passwords more than males. However, the difference is not statistical significant. It can also be noted that users share their work passwords less than private ones.

4. Conclusion and Future Work

We conducted a nationwide survey of password security with sample of 1003 respondents in Norway. We found that in average a person has minimum of 25 passwords. Not enough qualitative education or guidance is given. Password guidance is left with commercial companies, which are mostly concerned about the easiness of passwords, not the strength of passwords. The good guidelines for passwords given by information security authorities are not among the websites where users search guidance. In the users' opinion the general description of good password is "*A good password is a mixture of letters and digits*." Passwords are very often reused. The users do understand which accounts contain confidential and private information. However, they do not use any better password to protect them. Passwords are shared but mostly with close family members. Even if the password authentication method is old, it is not going to change soon. In order to keep the users updated, we need to invest in education and guidance from the root to top level.

The general results of the password survey have gotten media attention in Norway such as (Thorvaldsen, 2012) and NorSIS had already used the results in national security strategy meetings to wake up governmental departments to realise the real knowledge level of the Norwegian companies and inhabitants. Also meetings with vendors to help them give better password guidance as well as change their policies are to be arranged. NorSIS organizes awareness training amongst Norwegian companies and uses media to reach a bigger population of inhabitants. A national

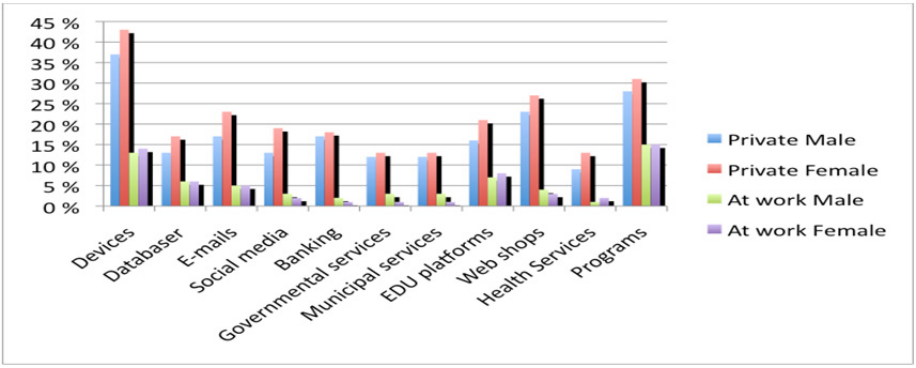

Figure 4: Shared passwords

campaign "The National Security Month" was arranged together with other security experts in October 2012, and a bigger campaign in 2013 is under planning. The campaign will contain commercials in national radio channels, articles in national newspapers and media, awareness training for Norwegian SMEs and speeches for Norwegian companies as charity from Norwegian security experts. The password security will be part of the campaign. The security awareness is also promoted during the year in each of those over a hundred speeches given by NorSIS.

5. References

Benediktsson, A., (2012) "Passordhåndtering", www.hardware.no/artikler/passordhaandtering/78112 (Accessed 8.1.2013)

Bonneau, J. and Preibusch, S. (2010), "The password thicket: technical and market failures in human authentication on the web", In Proc. of WEIS 10

CSID (2012), "Comsumer survey: Password habits, September 2012", www.csid.com/wp-content/uploads/2012/09/ CS_PasswordSurvey_FullReport_FINAL.pdf (Accessed 8.1.2013)

Florêncio, D. and Herley, C. (2010), "Where Do Security Policies Come From?" In Proc. of Symposium on Usable Privacy and Security (SOUPS 2010)

Gibson Research Corporation Web Site (GRC) (2013), "Perfect passwords", www.grc.com/passwords.htm (Accessed 12.1.2013)

Haley, K. (2010), "Symantec - Password Survey Results", www.symantec.com/connect/blogs/ password-survey-results (Accessed 8.1.2013)

Helkala, K. (2011), "Password Education Based on Guidelines Tailored to Different Password Categories" Journal of Computers, Vol. 6, Nr 5, Academy Publisher, Finland.

Helkala, K., Svendsen, N.K., Thorsheim, P. and Wiehe, A. (2012), "Cracking Associative Passwords". In Proc. 17th Nordic Conference, NordSec 2012, LNCS Vol.7617, p. 153-168.

Hoonakker, P., Bornoe, N. and Carayon, P. (2009), "Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users", In Proc. of the Human Factors and Ergonomics Society 53rd Annual Meeting, p. 459-463.

Horcher, A.-M. and Tejay, G.P. (2009), "Building A Better Password: The Role of Cognitive Load in Information Security Training", In Proc. of IEEE International Conference on Intelligence and Security Informatics, ISI, p. 113–118.

Junglemap Corporation Web Site, 2013, junglemap.com/ (Accessed 15.1.2013)

Katz, F.H. (2005), "The Effect of a University Information Security Survey on Instruction Methods in Information Security". In Proc. of the Information Security Curriculum Development Conference, p 43–48.

Kuhn, T.B. and Garrison, C. (2009), "A survey of passwords from 2007 to 2009". In 2009 Information Security Curriculum Development Conference, InfoSecCD'09, p. 91–94.

Kumar, N. (2011), "Password in Practice: An usability survey", Journal of Global Research in Computer Science, Vol. 2, No. 5, pp.107-112.

Nasjonal sikkerhetsmyndighet Corporation Web Site (2002), "Veiledning til $ 5-26: Utarbeidelse av brukerinsturks*"*, (Accessed 8.1.2013)

NorSIS , 2012, "Passordvett", www.norsis.no/veiledninger/Passord.html (Accessed 8.1.2013)

NIST Special Publication 800-118 (2009), "Guide to Enterprise Password Management", csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf

Næringslivets sikkerhetsråd (NSR) (2012), "Mørketallsundersøkelse 2012", www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/moerketall_2012.pdf

Sasse, M.A., Brostoff, S. and Weirich, D. (2001), "Transforming the "weakest link"-human/ computer interaction approach to usable and effective security", BT Technol,19(19)p.122-131.

Shay, R., Komanduri S., Kelley, P.G., Leon, P.G., Mazurek, M.L., Bauer, L., Christin, N. and Cranor, L.F. (2010), "Encountering Stronger Password Requirements: User Attitudes and Behaviors", In Proc. of the Symposium on Usable Privacy and Security (SOUPS 2010).

Talib, S., Clarke, N.L, and Furnell, S.M. (2010), "An Analysis of Information Security Awareness within Home and Work Environments*",* In Proc. of ARES 10, p. 196-203.

Thorvaldsen, L. (2012), "Majoriteten av Norge tror at det vet hva som er et godt passord", dagbladet.no/2012/12/05/nyheter/innenriks/datasikkerhet/passord/24685246/ (Access 20.1.13)

YouGov Corporation Web Site (2013), www.yougov.no/ (Accessed 14.1.2013)

Appendix - Questions

With products/services we mean *devices, cloud services/databases, e-mails, social media, banking, governmental services, municipal services, web shops, health services and other.*

1. How many of the following products and /or services that require a password do you have in your private life and at work? *Product/Services.*
*2.*Have you received guidance for password creation? Where or from who? *While studying; At work; From friends/colleagues; Websites/newspapers; Other; Not remember; Not gotten.*
3. You answered that you received education/guidance from websites/newspapers. Can you specify on which website? *A list of Norwegian sites; Other; Not remember; No.*
4. Describe what you think is a good password and how you create it? (Open).
5. Do your passwords meet your own "good password" description? *All of them; Most of them; Some of them; None of them; Not know.*
6. Which of the following products and/or services provide information that you believe should be kept secret and therefore need extra protection? *Products/Services.*
7. Do you use "better" passwords in the services that you think should be extra protected? *Always; Usually; Sometimes; No; Not know.*
8. Do you reuse your passwords? *Always; Sometimes; Seldom; Never, Not know.*
9. Which of the following statements is best suited to describe how you remember your passwords? *I always remember them; I write them down; I reset them if not remembering; I have checked "remember me" boxes and only remember my login password; Other.*
10. Where do you write passwords down? *On a note I store at home/work; On a note I bring with me; In a text file on my PC/Phone; A computer program for storing; Other; Not know.*
11. What do you think of password generators available on the Internet? *Never heard; A good tool for generating passwords; A scary tool. Do not use them because do not know who has*

access to the generated passwords; Do not use them because generated passwords are hard to remember; Other; Not know.

12. Do you share any of your passwords with any of the following? *Spouse/Partner; Own children; Friends; Colleagues; Boss; Police; Bank; Supplier; IT; Anyone; Do not share.*

13. Do you think it is okay to share any of the following passwords with others, either private and/or work? *Products/Services*