UNIVERSITY OF LUXEMBOURG
Integrative Research Unit on Social and Individual Development (INSIDE)

IT Security

An Empirical Study on the Willingness of People to Communicate Personal Data

Research Report

Christian Happ, André Melzer,

Lucien Rasmus Volkert & Georges Steffgen

August 2012

SMILE
SECURITY MADE IN LETZEBUERG

Europäische Kommission

Table of contents

Acknowledgement

The authors of this report wish to thank the Luxembourg Ministry of the Economy and Foreign Trade and its employees working for SMILE, as well as the City of Luxembourg for their cooperative work.

The authors also received active support from students of the Bachelor of Science in Psychology at the Université du Luxembourg, Simone Bung, Ann-Kathrin Dax, Felicitas Eichner, Nathalie König, Georges Lemmer, Jessica Storoni, Steve Thill and Lucien Rasmus Volkert. Thanks in particular to all the members of the public who took part in the survey - without their help the study would not have been possible.

Survey conducted within the framework of the 'Eastereggs and Toothbrushes' project, co-financed by the European Commissions' Fundamental Rights and Citizenship Program.

Abstract

The following report presents the results of an empirical study conducted in 2012. At the request of and in cooperation with the Luxembourg Ministry of the Economy (SMILE), the University of Luxembourg's research unit INSIDE carried out a survey on peoples' willingness to communicate personal data. The main aim was to determine the number of people revealing their current computer password, on the basis of three different conditions: participants were either given a small reward (chocolate in Easter box) at the beginning of the survey, right before they were asked to name their password, or at the end of the survey. The original questionnaire from a previous study in 2008 was only slightly changed to allow for the comparison of results from the two measuring times. Six interviewers questioned a total of 1206 people in the Luxembourgish cities Esch-sur-Alzette (n=198), Diekirch (n=63), and Luxembourg City (n=945). In addition to information regarding their own password and their knowledge of other passwords, the survey measured participants' willingness to communicate their password as well as other personal data. Statistical analysis of the results revealed that 29.7% of the people (n=358) were willing to communicate their password to a stranger, the interviewer. An additional 48.3% disclosed extensive information and hints that would have been sufficient to reveal their password. Only less than a quarter of those questioned (22.0%) did neither reveal their password nor any hints on it. People were more willing to indicate their password when they were rewarded for participating in the survey (Chi^2=11.91; p<.01). Furthermore, the results were compared with findings from the preceding study conducted in 2008 (Steffgen & Melzer, 2008). Most notably, this comparison revealed that people seem even more likely to disclose personal information nowadays than they did in 2008. In sum, the results provide further evidence that additional measures need to be taken to improve the security awareness of users of new information and communication technologies.

1 Theory

There are many psychological theories, which form the basis of this study on social engineering. This short overview will briefly introduce three important psychological mechanisms that social engineering draws on.

1.1 "Foot in the door" and "door in the face"

Social engineering is the art of manipulating people into performing actions or divulging confidential information. Early research to the topic of the so-called "foot in the door" technique (FINT) shows that people are willing to do more or even greater favours to someone they have already done a (simpler) favour for (e.g., Freedman & Fraser, 1966). Practically, this strategy includes starting with a little request in order to gain eventual compliance with a related larger request. The principle involved is that a small agreement creates a social bond between two people; a basic human reality that social scientists call "successive approximations". The other person has to justify their agreement to him/herself by being nice or liking the requester. In a future request, they then feel obliged to act consistently with their internal explanation they have built. This simple favour can be as easy as a question, which people hardly ever refuse to answer. With regard to social engineering, Cialdini (2001) recommends, "*to be very careful about agreeing to trivial requests, because that agreement can influence our self-concepts.* [...] *it can make us more willing to perform a variety of larger favors that are only remotely connected to the little one we did earlier"* (p. 65f).

A similar approach is the "door-in-the-face" technique (DITF; e.g., Goldman, 1986). In DITF, the persuader attempts to convince the respondent to comply by making a large request that the respondent will most likely turn down. The respondent is then more likely to agree to a second, more reasonable request, compared to the same reasonable request made in isolation

(this strategy is therefore also known as “rejection-then-retreat technique”). A hard request, followed by a smaller one leads to higher acceptance of this smaller favour than in baseline conditions.

Although DITF has a different approach than FINT, both are persuasion techniques known to successfully increase the likelihood that a respondent will agree to the second request (see Cialdini, Vincent, Lewis, Catalan, Wheeler & Darby, 1975).

In the present study, therefore, the interview started with FINT by asking easy questions to set stage for the request of the password. However, for participants who refused to answer the question about their personal password, the DITF technique was used and further questions were asked. Here, participants were expected to give some hints regarding their password, because they should feel obliged to.

1.2 Reciprocity

The reciprocity norms (e.g., Cialdini, 2001, Gouldner, 1960) are a basic psychological principle, which can be found in many cultures. The norm of reciprocity is the social expectation that people try to repay, in kind, what another person has provided (“tit-for-tat”), including returning benefits for benefits, and responding with either indifference or hostility to harm. Thus, the norm of reciprocity ultimately has survival value (Aronson, 2007).

All members of the society are trained from childhood to abide by the rule or suffer serious social disapproval (Cialdini, 2001). Hence, people feel under pressure when they are given a present or a favour. As the norm of reciprocity requires that we repay in kind what another has done for us, it is used in advertising whereby a small gift of some kind is proffered with the expectation of producing a desire on the part of the recipient to reciprocate in some way, for example by purchasing a product, making a donation, or becoming more receptive to a

line of argument. Whatley, Webster, Smith & Rhodes (1999) found support for both public and private reasons for reciprocation, as the presence of a favour appeared to increase compliance in both public and private conditions. In addition, public compliance was even greater than private compliance. Moreover, the rule of reciprocation applies even to uninvited first favours, which reduce people's ability to decide whom they wish to owe and puts the choice in the hands of others. In addition, reciprocation can even spur unequal exchanges. To get rid of the uncomfortable feeling of indebtedness, people often agree to a request for a substantially larger favour that originally received. Against this backdrop, it is not surprising that the powerful rule of reciprocation ("give something before asking for a return favour") is popular in social engineering attacks (Cialdini, 2001).

In the present study, by offering some chocolate, which was intended to put participants under the pressure to give something in return, reciprocation was induced. In this case, "giving something in return" refers to revealing personal sensitive information.

1.3 Mood

Peoples' mood influences their behaviour. According to the "feelings as information model", people use their moods and emotions as indicators of whether or not they have performed adequately (Schwarz & Clore, 1988). When individuals experience positive affective states, they assume they have performed sufficiently. As a consequence, they withdraw effort. In contrast, when individuals experience negative affect states, they assume not having performed adequately, which leads them to amplify their efforts on a given task. According to Schwarz's (1990) cognitive tuning model, positive mood causes people to believe that the immediate environment is safe and no further action is necessary (for evidence, see Bless, Bohner, Schwarz, & Strack, 1990; Worth & Mackie, 1987). Schwarz & Bless (1991) found that a positive mood even transports an „everything-is-fine" attitude, which leads participants

to accept greater risks and to base their judgement on initial heuristics without careful analysis of the situation in hand.

In the present study a reward was given to induce a positive mood state in the recipients. This positive mood was then thought to influence people's perception of the situation. Perceiving a situation as reflecting a "safe" setting, it should become more likely that they reveal personal information.

2 Description of the study

2.1 Issues addressed

Ensuring information security is a major topic and a significant challenge both for suppliers and users of new information and communication technologies. The wide range of possible applications offered on the Internet, for instance, also comprises a large number of dangers and risks. With increasing professionalization and technically advanced methods, cyber criminals present a particular threat. A computer with an inadequate level of security can easily fall prey to criminals who can gain access to the personal data stored on it. However, information security is by no means confined to technical measures. Rather, potential risks are increased by the fact that many computer users are often unaware of the risks involved and fail to implement the most important IT security rules. In this sense, passwords are an important part of the problem. Passwords are the easiest way for cyber criminals to get access to people's IT system. Irrespective of all (possible) high technical precautions, knowing a person's password allows cyber criminals to access and misuse personal data. Revealing passwords may also open entire company networks to cyber criminals.

CASES (Cyberworld Awareness and Security Enhancement Structure) – a unit set up by the Luxembourg Ministry of the Economy and Foreign Trade to improve information security – has found that many users do not exercise due care when dealing with their passwords (e.g., Steffgen & Melzer, 2008). Though CASES still exists, most of the activities in the domains of raising awareness, communication, but also resource centre as IT emergency response team are now managed by SMILE, a dedicated GIE (Economic Interest Group). SMILE thus set out to determine, via this study, the extent to which people were willing to communicate personal data in specific circumstances.

A social engineering research analysis (extracting data by using psychological tricks) was performed in Luxembourg with more than 1200 persons interviewed in public. It was tested whether it is really so easy to obtain private data from people. The simulated attack took into account not only methods used by cybercriminals but also methods, which are perfectly legal and used by companies via commercial Internet sites, for example. This social engineering study was performed Easter 2012 in Luxembourg, using chocolate in Easter box to attract and recreate a situation similar to the situations faced in Cyberspace. The concrete objective of the survey was to extract private data from people on the street and get them to reveal it to an interviewer – a stranger – within two minutes. If research showed how easy it was to obtain private data from adults on a public street, how easy would it be with children in cyberspace? The research result would then help to make decision takers and the public become more aware of the problem of 'social engineering' methods used to extract data from people. It would also be helpful in developing pedagogical materials aimed at training children and adults in security skills, as well as developing material for successful and targeted raising awareness campaigns aimed at parents, children, the general public, and decision takers on this subject for 2012. As has already been shown in the previous study in 2008, many people give their password to a stranger after receiving a chocolate bar of a value of 3.80 Euros. The present study therefore also investigated changes over time, that is, whether people's awareness of the importance of information security has changed from 2008 to 2012.

2.2 Scientific method

A study group was formed to carry out the research. The 2008 questionnaire was re-evaluated, partly rephrased and slightly changed (see below). Second- and third-year Psychology students from the University of Luxembourg were recruited as interviewers and trained by the study group, who also managed them throughout the study. The research unit INSIDE of the

University of Luxembourg was responsible for drafting a research plan, analysing the data and presenting the main results in this report. The interviews were conducted in French, German, and Luxembourgish.

2.2.1 Measuring instrument: The 2012 questionnaire

This questionnaire was first used in the 2008 study (Steffgen & Melzer, 2008). It was adapted to the Luxembourgish context and translated from English into French and German. The questionnaire was brief such that it would not take longer than 3 minutes. It covered the extent and type of password use, knowledge of other passwords as well as the participant's willingness to communicate his/her password to (a) colleagues, (b) a possible IT-department, and (c) the interviewer/ a stranger. This most important part of the questionnaire was measured with the question if the participant is willing to write down their personal password on the questionnaire. If participants were not willing to do that, the interviewer asked for hints regarding the password. The questionnaire also included demographic and personal data as well as a question regarding the awareness of sensitization campaigns in Luxembourg and if participants were telling the truth, therefore controlling for his/her tendency to answer in a socially desirable way.

For the 2012 study, time constraints had again a determining influence on the scope and content of the questionnaire. In total, it consisted of 15 items. However, in order to use the questionnaire more efficiently, the following minor changes were made to the 2008 questionnaire:

- "Password hints" and their relevance turned out to be hard to define and code. In this questionnaire we only coded if hints were given at all.

- A filter question was needed, as there is not always an IT department affiliated with individual work places. Therefore, answering the question how people respond to "calls from the IT-department" might cause confusion.
- Participants' suggestions for mostly used passwords were eliminated due to coding problems.
- The order of questions was slightly changed to expedite the interview.
- At the end of the interview, participants were asked if they had told the truth about how they deal with their sensitive data. This makes the exclusion of unwanted social desirable answers easier.
- Extensive effort has been put into many recent campaigns on information security. Therefore, participants were asked if they recall any of these campaigns (yes/no and name).

2.2.2 Sample description

As is the case with questions and wording used in the present study, minor changes were also made with regard to the procedure in the 2008 study. This was done to ensure a data set, which reveals information more explicitly.

- Giving out chocolate at the end of the interview could not influence participants' answering behaviour in 2008 as all answers were already given when the reward was handed out. However, we decided to investigate the effect of reward more closely. Therefore, we varied the specific moment during the interview when participants received their treat: Has a chocolate reward right before the relevant information is asked (i.e., what is your password?) a stronger influence than at the beginning of the interview?
- As SMILE also targets adolescents' Internet use, this age group was no longer excluded from the recruiting.
- Answering behaviour of the participants might differ in different cities, as there are differences in Internet use. Therefore, we interviewed not only people in Luxembourg City, but also, according to population density, participants from the smaller cities of Diekirch and Esch-sur-Alzette.

The 2012 sample consisted of *N*=1208 participants. Two participants were excluded because they did not report their age. In consequence the analyses are based on *N*=1206 participants. Most participants were interviewed with the German questionnaire (*n*=815; 67.6%) the remaining interviews were carried out with the French questionnaire (*n*=391; 32.4%).

Gender was nearly counterbalanced with *n*=649 (53.8%) male and *n*=557 (46.2%) female participants. The age of the participants ranged from 12 to 74 years. The mean age was 30.52 years and the standard deviation was 13.25 years. The median was 27 years, indicating that half of the sample was younger than 27 years and the other half older.

2.2.3 Design and implementation of the study

The study consisted of a 3x3-factor quasi-experimental design. This means that for the Social Engineering factor there were 3 reward conditions (i.e., chocolate given to participants) tested in 3 different locations (i.e., cities). In the first condition, chocolate was given to the participant at the very beginning of the interview (*n*=407; 33.7%). In the second condition, participants received the reward immediately before being asked for their password (*n*=373; 30.9%), and in the third condition chocolate was handed out at the end of the interview (*n*=426; 35.3%).

With regard to location, 945 (78.4%) participants were interviewed in Luxembourg City, 63 (5.2%) in Diekirch and 198 (16.4%) in Esch-sur-Alzette. These numbers correspond to the density of population in these three cities and were therefore specified in advance.

Interviews were conducted in the morning (from 8 am on: *n*=419 34.7%), at noon (*n*=291; 24.1%), afternoon (*n*=381; 31.5%), and in the evening (until 7 pm: *n*=115; 9.5%).

All participants were interviewed between March 26 and April 10, 2012. Seasonally caused, the chocolate reward was given in the form of an Easter box of chocolates. The interviewers were wearing a bag of the University of Luxembourg that had the University of Luxembourg logo clearly visible printed on it. They addressed pedestrians asking them to participate in what was introduced as a "study on IT conducted by the University of Luxembourg". The interviewers used standardized questionnaires and were trained and briefed before they started work. The interviewers approached people in the city and asked them if they were willing to take part in the short interview. After agreeing, participants could chose between the German and the French version of the questionnaire (see Appendix). The interview then lasted between 2 and 3 minutes. Afterwards participants were thanked and interviewers approached a new person. The only condition for taking part was that participants used a computer at work or in school regularly.

2.2.4 Statistical analysis of the data

Data were entered and coded anonymously and then analysed with SPSS 17 for Windows. Missing values were deleted pairwise. This means if some participants have not answered to some questions, they were only excluded for these questions and not for the whole questionnaire. Following control measures and plausibility tests, a descriptive-statistical analysis was performed on the data to prepare the present report (Section 3). Next, both the distribution of participants' answers to specific questions and comparison of means (e.g., *chi-squared* tests, t-tests) were taken into consideration to explore group differences (significance testing; Section 4). In contrast to a t-test that compares two (group) means, a chi-squared test compares if the number of occurrences is equally likely in all conditions. For example, if the willingness to give away the password (yes or no) differs between the three chocolate groups to the extent that more people reveal their password in one specific condition, the test may become significant. Finally, variables that have been collected in both waves (2008 and 2012) are analysed (Section 5).

3 Results of the 2012 survey

In the following the results of the data analysis will be presented.

3.1 Descriptive analysis

In this section we will report the results of the descriptive analyses. Percentages are always calculated on the total number of valid answers.

3.1.1 Password use

Of 1206 interviewed persons, 1146 (95.1%) reported that they use a password at work. 60 persons (4.9%) do not use a password and were therefore excluded from further analyses on the use of passwords. Of those using a password, 397 (34.6%) reported that they have no guidelines for their passwords. In contrast, 749 (65.3%) participants reported that they have to respect certain guidelines concerning their passwords. 514 password users (44.9%) reported that they use more than one password for multiple domains. 632 participants (55.1%) reported that they use one password for at least two domains. While most participants admitted that they do not change their password at all (*n*=530; 44.5%), those who do change their password do this only infrequently (*n*=476, 39.8%). Some change their password on a monthly basis (*n*=173; 14.5%). Hardly anyone reported changing his or her password weekly (*n*=13; 1.1%) or daily (*n*=4; 0.3%, see Figure 1).

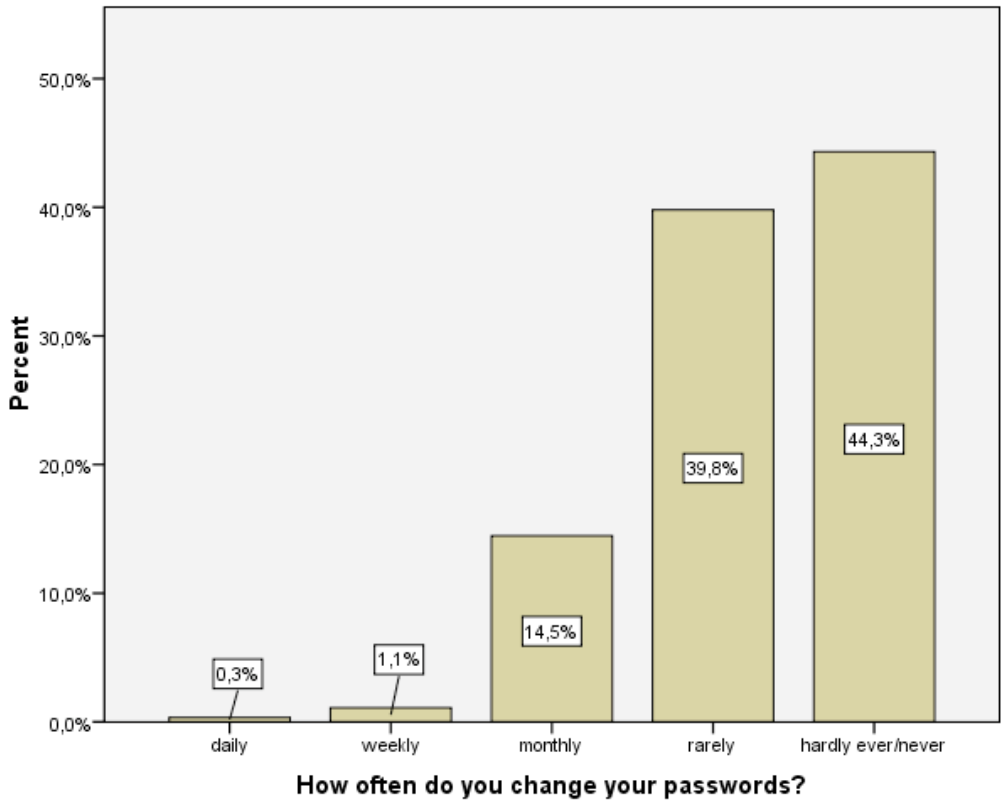

Figure 1: Frequency of password change

3.1.2 Participants' knowledge of colleagues' passwords

The majority of participants (821, 68.2%) reported that they do not know the passwords of their colleagues. However, 382 participants (31.8%) indicated that they know at least one password of their colleagues.

3.1.3 Participants' trust towards IT-department

963 (79.9%) participants stated that there is an IT-department in their company. Of those, 371 (38.5%) participants are sure that their IT-department knows their password(s). In contrast, 206 participants (21.4%) are not sure if this is true for their IT-department. The remaining 386 participants (40.1%) claimed that their IT-department does not know the passwords of the employees, and 322 of them (83.4%) would not name their password if they were called by

their IT-department, whereas 76 participants (16.6%) would be willing to reveal their password on the phone.

3.1.4 Colleagues' knowledge of participant's passwords

941 participants (78.4%) reported that they have not informed their colleagues about their passwords. In contrast, 260 participants (21.6%) reported that (at least one) colleague(s) know(s) at least one password of the participant.

3.1.5 Handing out the password to a colleague

A great number of participants (726; 76.0%) would not reveal their password to colleagues, but 229 (24.0%) would.

3.1.6 Handing out the password the interviewer

836 participants (70.3%) refused to disclose their password to the interviewer. Surprisingly, 358 participants (29.7%) did reveal their password. When those who did not disclose their password were asked for a hint, 579 (an additional 48.3% of the total sample) gave at least one hint. Only 257 participants (22.0%) refused to reveal their password or a hint for it (see Figure 2).

Taken together, a total of 937 (78.0%) participants that were interviewed revealed some personal information concerning their password.

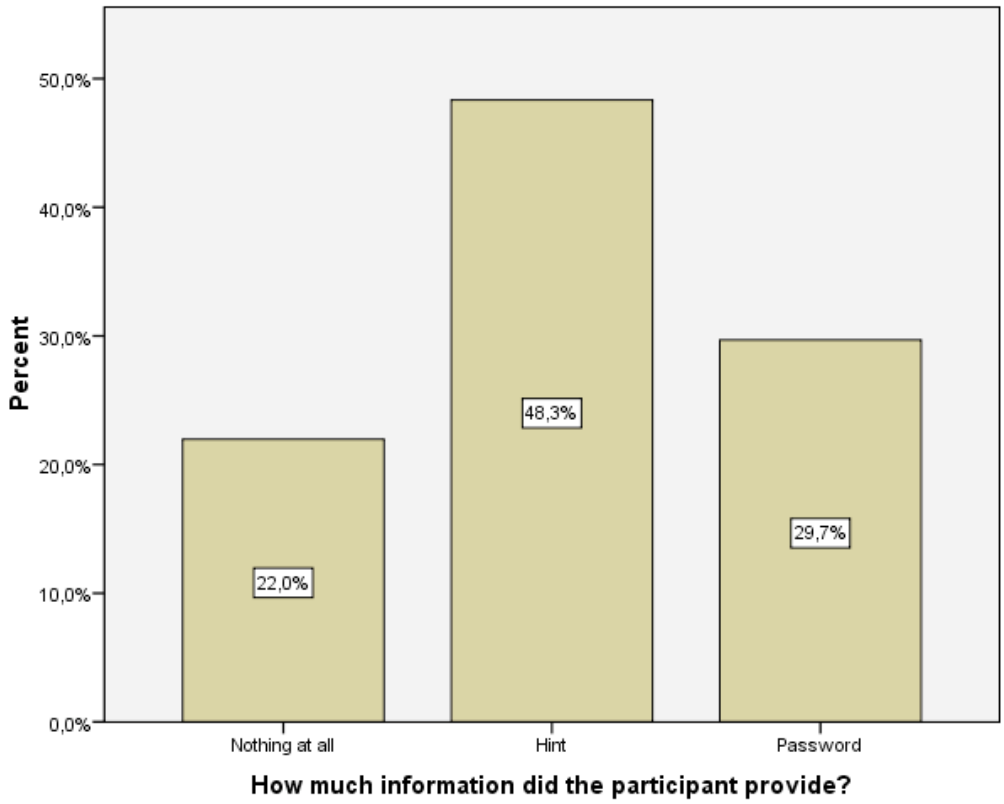

Figure 2: Information provided by participants

3.1.7 Communication of sensitive data

At the end of the interview, participants were asked to reveal some personal information to confirm the validity of the questionnaire. While 1000 (83.1%) participants revealed their date of birth, 204 (16.9%) did not hand out this particular information. Most of the participants also revealed their names (1064; 88.4%), but only approximately half of the interviewees communicated their telephone number (596; 49.6%).

3.1.8 Telling the truth

Finally, participants were given the chance to admit that they had not told the truth regarding their password information. Of those who gave out at least some hints or even the entire password, 133 participants (11.1% of the total sample) indicated that they had not told the truth. 66 of the 358 participants who revealed their password reported that they communicated

incorrect information (18.4% of those who told the password). Additionally, 67 participants "lied" when they gave hints regarding their password (11.6% of 579).

Given that the truth item renders the opportunity to exclude dishonest participants (please keep in mind that this is still a self-report item), the following distribution results: 292 (27.3%) were password tellers, 512 (47.9%) were hint tellers, and 265 (24.8%) gave no information at all. Please note that these alterations do *not* lead to changes in the general pattern of handling sensitive information (see Figure 2 in Section 3.1.6).

3.1.9 Recalling sensitization campaigns

As was already mentioned above, the interview also included a part where participants were asked for their awareness of recent campaigns on Internet safety in Luxembourg. A general question (yes/no) was followed by an open question (*"If yes, what do you remember?"*). Therefore, all given answers are freely memorized. 327 participants (27.1%) reported that they heard at least about one campaign, but 879 participants (72.9%) reported that they were not aware of any previous campaign.

When then asked for details, 209 participants (17.3%) were able to remember at least one campaign name, and 265 participants (22.0%) remembered at least one name or an event that dealt with sensitization.

More specifically, 101 participants (8.4% of all participants) associated the term "toothbrush" with a sensitization campaign. There were similar results regarding a different recent campaign involving condoms *(*53 participants, 4.4%). The organization name "CASES" was named by 15 participants (1.2% of the total sample), whereas 81 participants (6.7%) were able to name the term "BEE-Secure".

4 Significance testing

In the following section, the results of the statistical analyses of the different factors associated with handing out the password will be presented. The level of significance was set at alpha = 5%.

4.1.1 Demographic data

Gender of the subject: There was no significant difference between men and women regarding handing out their passwords (see Table 6; $p>.05$).

Language: There was a statistically significant main effect of language of the participants and handing out the password ($Chi^2(1,1206)=4.90$; $p<.05$). French speaking participants were less likely to hand out their password (25.8%) than German-speaking participants (32.3%). The same is true to the interviewers' use of Luxembourgish ($Chi^2(1,863)=44.19$; $p<.001$). When Luxembourgish was used, only 20.4% of the participants handed out their password whereas 43.1% of the participants handed out their password when the interview was conducted in a different language.

Age: The correlation was highly negatively significant ($r=-.13$; $p<.001$), indicating that younger persons handed out their password more readily than older participants. To see if the correlation was due to differences between adolescents and adults, a *t*-test was performed. It was found that adolescents (under 18 years old) were more inclined to hand out their password than adults (aged 18 or older), $t(246.54)=-3.48$; $p<.01$. Next, it was tested whether there were age differences among the group of adults. To observe differences for younger and older adults, a one-way Analysis of Variances (ANOVA) was conducted, which revealed that there were significant mean differences ($F=6.59$; $p<.001$), but only for the under 18-year-olds.

Between the adult age groups (18-30; 31-50 and 51+) there were no significant mean differences (see Table 1).

Table 1: Number of participants in the different age groups

Age group	<18	18-30	31-50	>50	Total
N	192	498	395	121	1206
$\mathbf{N_{pw\text{-}given}}$	80	153	101	27	361
$\mathbf{N_{pw\text{-}given}/\ N}$	41.7%	30.7%	25.6%	22.3%	30.0%

4.1.2 Manipulated variables

Time of day: There was no statistical effect for the time of day and giving out the password ($p>.05$). Apparently, participants did not respond differently at different times of the day.

Place: A statistically significant difference was revealed between the location and handing out the password ($Chi^2(1,1206)=28.42$; $p<.001$). In Luxembourg City, 33.8% of the participants revealed their password whereas in Diekirch only 13.3% of the participants and in Esch-sur-Alzette only 16.7% handed out their password. It has to be kept in mind, however, that the number of participants interviewed was different among the three cities.

Time of handing out the chocolate: There was a highly significant difference between the time of handing out the chocolate and handing out the password ($Chi^2(1,1206)=11.91$; $p<.01$). When the chocolate was given in the beginning, 31.5% of the participants handed out their password. 35.8% revealed their password when the chocolate was given directly before asking for it, but only 24.4% of the participants handed out their password when the chocolate was given at the end of the questionnaire.

4.1.3 Password use

Password directives: Directives regarding the password did not significantly influence if participants revealed their password to the interviewer ($p>.05$).

Password use for multiple domains: There was a statistically significant difference between the use of the password for multiple domains and handing out the password to the interviewer ($Chi^2(1,1146)=5.46$; $p<.05$). If participants did not use their password for multiple domains, 26.7% of the participants handed out their password. In contrast, if participants used their password for multiple domains, 33.1% of the participants handed out their password.

Subject's knowledge of colleagues' passwords: When participants reported that they knowing the password(s) of their colleagues, they revealed their own password more readily ($Chi^2(1,1203)=20.59$; $p<.001$). If the participants did not know the password(s) of their colleagues, 25.9% disclosed their password. In contrast, if the participants knew the passwords of their colleagues, 39.2% of the participants handed out their password.

IT-Department: There was no difference between the presence of an IT-Department and handing out the password to the interviewer ($p>.05$).

IT-Department's knowledge of participants' password: There was a highly significant difference between the IT-Department's knowledge of passwords and handing out the password to the interviewer ($Chi^2(1,964)=55.51$; $p<.001$). If the IT-Department did not know the password of the subject, 17.6% of the participants handed out their password. In contrast, if the IT-Department knew the password of the subject, 42.7% handed out the password. If the participants did not know whether or not the IT-Department knows the subject's password, 28.6% of the participants handed out their password.

Handing out the password to the IT-Department if called: There was a highly significant difference for revealing the password depending on whether or not participants were willing to inform the IT-department about their password ($Chi^2(1,398)=8.93$; $p<.01$). If the participants would not give their password to the IT-Department, only 14.4% handed out the password to the interviewer. If the participants would give their password to the IT-Department, 29.2% handed out their password to the interviewer.

Colleagues knowledge of the subject's password: There was a very highly significant difference between those whose password is known by colleagues and those whose password is a secret also for colleagues ($Chi^2(1,1201)=27.65$; $p<.001$). If colleagues did not know the password of the participant, only 26.4% of the participants gave their password to the interviewer. If the participants' colleagues knew the password of the participants, 43.7% gave out their password to the interviewer.

Handing out the password to a colleague: There was a very highly significant statistical difference those who know also colleagues' passwords and those whose password those who do not ($Chi^2(1,955)=17.91$; $p<.001$). In case the participants would not give their password to a colleague, 23.5% of the participants handed out their password to the interviewer. In case the participant would give the password to a colleague, 38.0% of the participants handed out the password to the interviewer.

4.1.3.1 Correlations between "handing out the password" and other variables

In a final step, it was analysed whether participants' reported willingness to hand out their password was associated with other variables.

Number of passwords: The correlation was positive and significant ($r=.07$; $p<.001$). Apparently, people's willingness to communicate passwords increases with the number of passwords in use.

Changing the password: The correlation was negative and highly significant (r=-.12; p<.001). With regard to attempts to increase the awareness for issues of IT security, it is important to look at this result from both sides of the correlation. On the one hand, the fewer participants change their password the more likely they are to hand out the password to the interviewer. However, participants seem to be less likely to disclose their password if they change passwords often.

Colleagues' knowledge of subject's password: There was significant positive correlation between the colleagues' knowledge of the subject's password and handing out the password (r=.08; p<.05).

For handing out the password, no significant correlation was found with **Number of domains for one password**, **Number of colleagues' passwords** and **Usefulness of the comment** (ps>.05).

5 Tests between the two waves 2008 and 2012

In this section, the results of the comparative tests between the two waves 2008 and 2012 will be reported.

5.1 Sample differences

Language: In 2008, there were significantly more French-speaking participants (*N*=447; 43.0%) than in 2012 (*n*=391; 32.4%), $Chi^2(1,2246)=26.62$; $p<.001$. In 2012, significantly more interviews were conducted in Luxembourgish (*n*=349; 28.9%) than in 2008 (*N*=229; 22.0%), $Chi^2(1, 1903)=75.68$; $p<.001$.

Gender: There was no significant difference between the 2008 and 2012 sample concerning the gender ($Chi^2(1, 2246)=3.42$; $p>.05$, see Figure 3). In 2008, 50.1% of the participants were female (*n*=521) and 49.9% (*n*=519) were male. In 2012, 46.2% of the participants were female (*n*=557) and 53.8% were male (*n*=649).

Test conditions (handing out the chocolate): In 2008, the interviewers gave no chocolate at all (*n*=503), at the beginning (*n*=271), or at the end of the questionnaire (*n*=266). In 2012, a reward was given at the beginning of the questionnaire (*n*=407), immediately before asking for the password (*n*=373), or at the end of the questionnaire (*n*=426). Therefore, a total of four different reward conditions were tested.

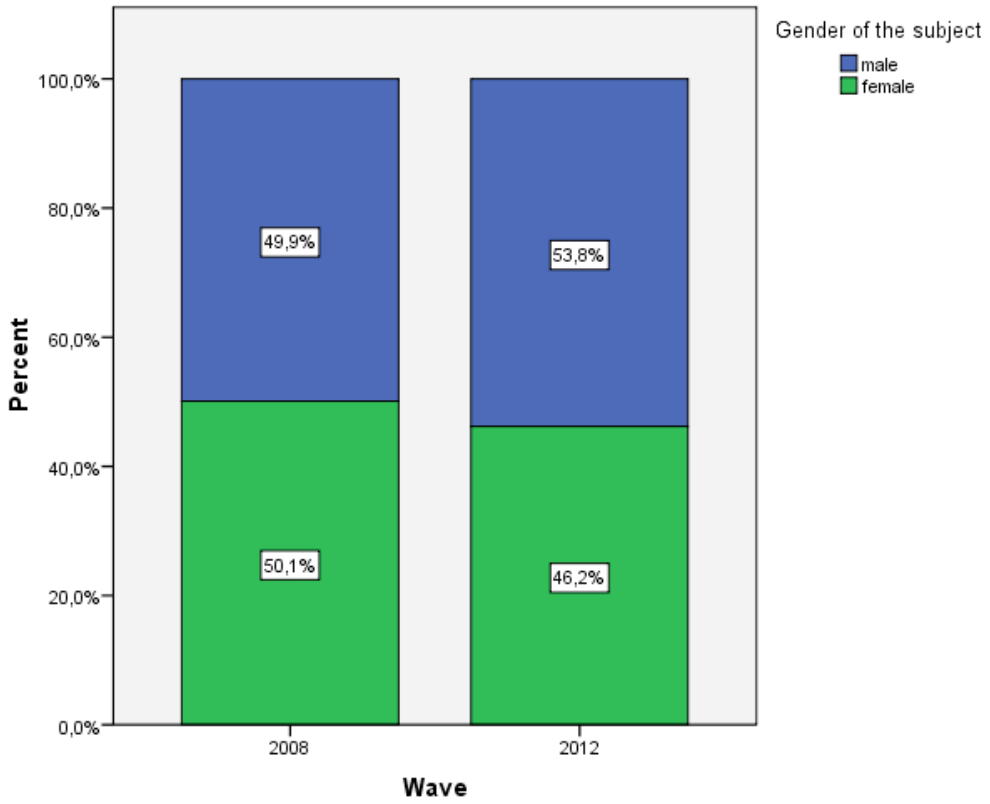

Figure 3: Distribution of the participants' gender

5.2 Password information

Password use: In 2012, there were significantly more people who stated that they use a password (n=1146; 95.0%) than in 2008 (n=961; 92.4%) (Chi^2(1,2246)=6.61; p<.05; see Figure 4). Similarly, the participants reported to use more passwords (M=4.14) in 2012 than in 2008 (M=3.26). This difference was statistically significant (t(2049.52)=-4.55; p<.001).

In 2012, more people reported that they use their passwords or one password for multiple domains (n=632; 55.1%) than in 2008 (n=337; 32.8%) (Chi^2(1,2174)=6.61; p<.001). Yet, the amount of domains accessed with one password decreased from M=6.09 in 2008 to M=4.74 in 2012. This difference is statistically significant (t(1125.35)=5.38; p<.001).

Finally, there was no statistically significant difference in the frequency of changing the password in 2008 (M=4.21, SD=1.57) and 2012 (M=4.27, SD=0.77; t(1462.04)=-1.12; p>.05; see Table 2). This means that on the average participants rarely changed their password.

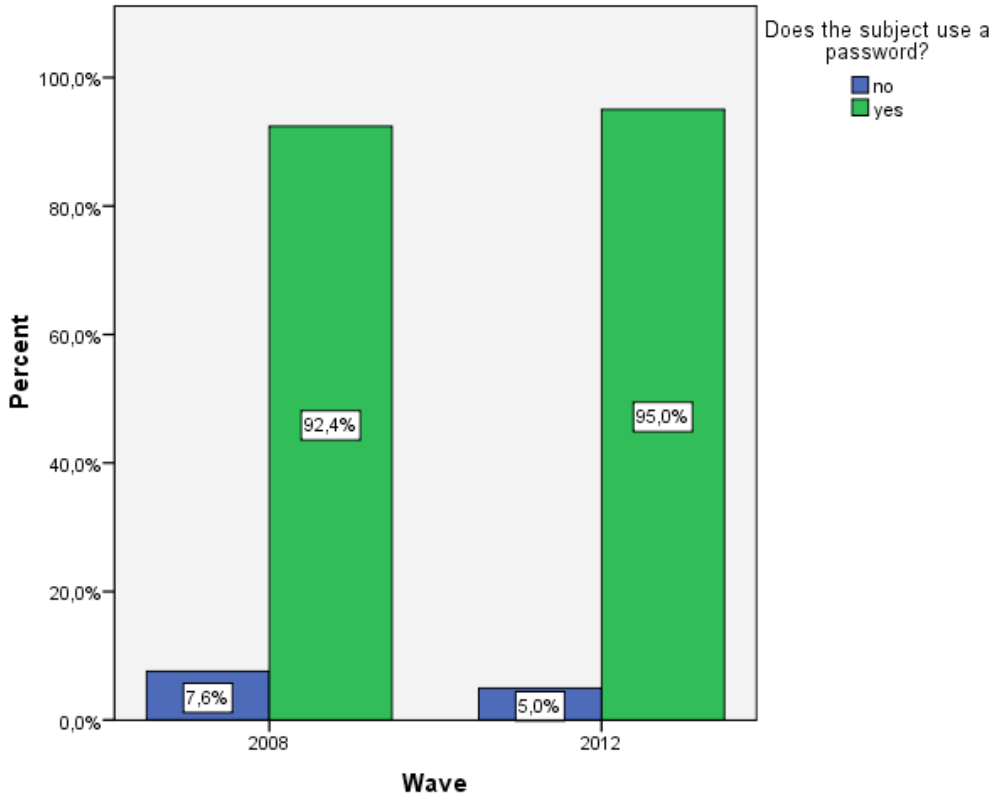

Figure 4: Participants' password use

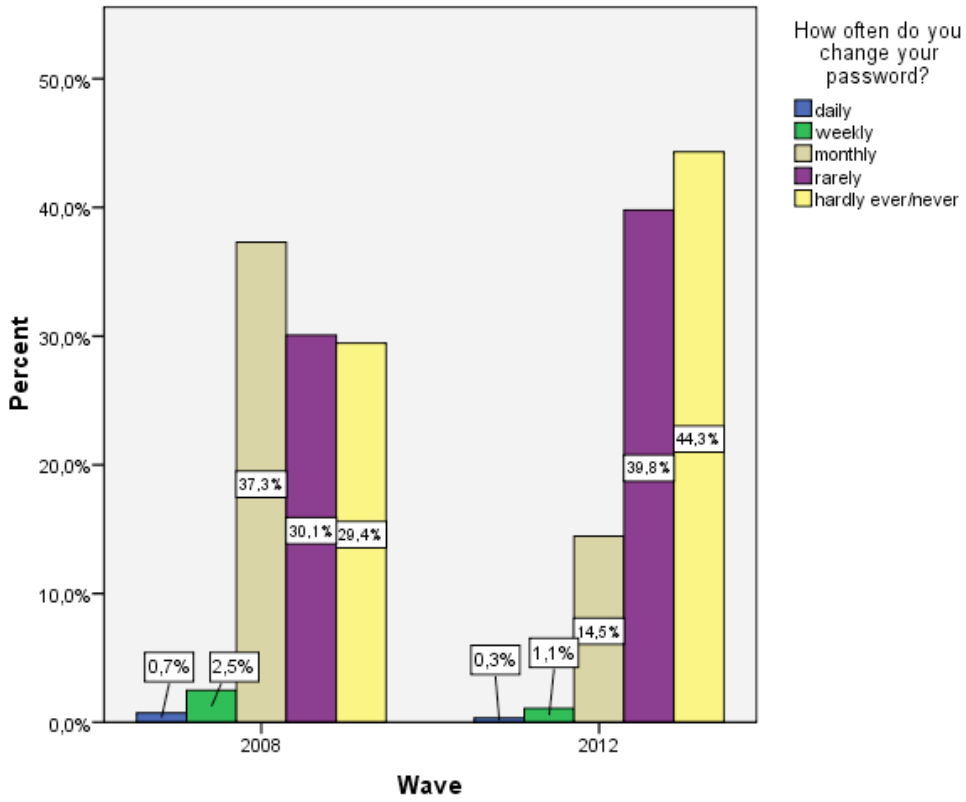

Figure 5: Frequency of changing the password

5.2.1 Subgroup analysis: Gender and changing the password:

Table 2 illustrates the frequency of password changes for male and female participants in the 2008 and 2012 studies as well as the overall numbers in both waves.

Table 2: Changing the password subgroup analysis

	2008		2012		Total
	Male	Female	Male	Female	
How often do you change your password?	4.11	4.30	4.23	4.31	
Total	4.21		4.27		4.08

5.3 Second party knowledge of password

Participants' knowledge of colleagues' passwords: In 2012, more participants reported that they know the passwords of their colleagues (n=382; 31.8%) than in 2008 (n=264; 25.5%). This difference was statistically significant ($Chi^2(1,2237)=10.48$; $p<.01$; see Figure 6). There was no significant mean difference in the number of colleagues' passwords the participants knew ($t(278.44)=1.64$; $p>.05$).

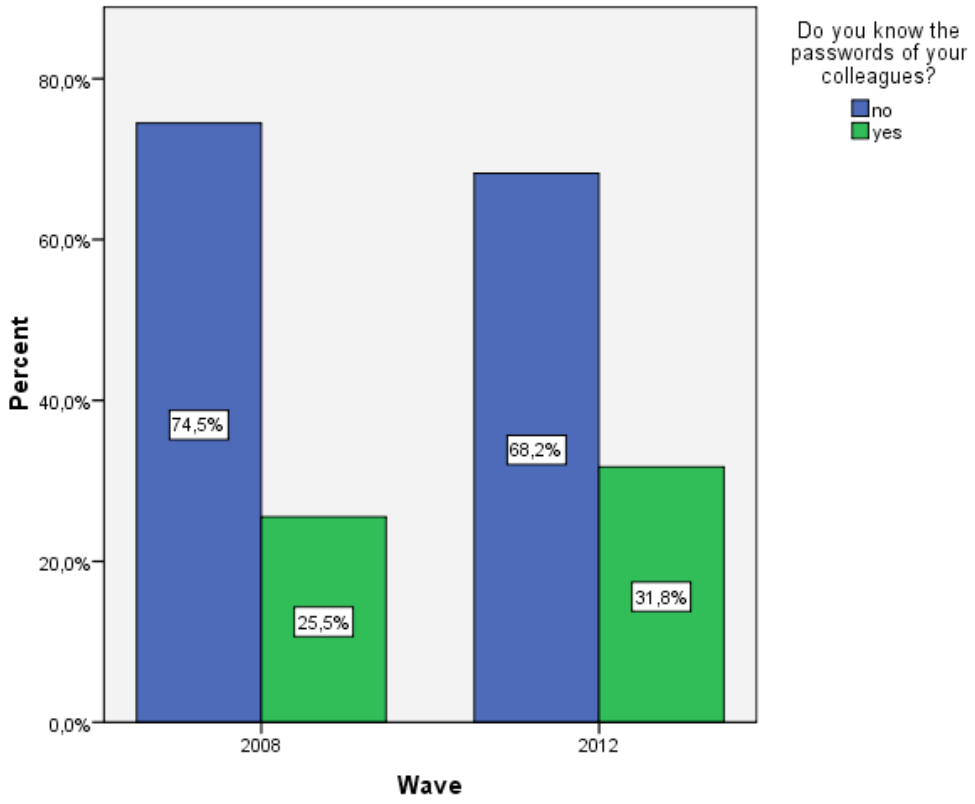

Figure 6: Participant's knowledge of colleagues' passwords

5.3.1 Subgroup analysis: Gender and knowledge of colleagues' password(s)

In Table 3, the number of female and male participants is listed, who reported knowing their colleagues' passwords.

Table 3: Subgroup analysis for participants' reported knowledge of their colleagues' passwords

		Male	Female	Total
2008	**N**	515	519	1034
	$\mathbf{N_{know\_colleagues}}$	129	135	264
	$\mathbf{N_{know\_colleagues}/\ N}$	25.0%	26.0%	25.5%
2012	**N**	647	556	1203
	$\mathbf{N_{know\_colleagues}}$	180	202	382
	$\mathbf{N_{know\_colleagues}/\ N}$	27.8%	36.3%	31.8%
Total	**N**	1162	1075	2237
	$\mathbf{N_{know\_colleagues}}$	309	337	646
	$\mathbf{N_{know\_colleagues}/\ N}$	26.6%	31.3%	28.9%

Handing out the password if called by the IT-Department: There was no statistically significant mean difference between 2008 and 2012 with regard to handing out the password if participants were called by the IT-department ($Chi^2(1,1409)=2.48$; $p>.05$). In 2008, 779 participants (77.1%) reported that they would not hand out their password and in 2012, 322 (80.9%) participants reported to not to do so.

Colleagues' knowledge of participant's password: There was no statistically significant difference between 2008 (n=250, 24.7%) and 2012 (n=260, 21.6%) regarding the number of participants who reported that colleagues know their password ($Chi^2(1,2212)=2.93$; $p>.05$; see Figure 7).

Handing out the password to a colleague: The tendency to hand out passwords to colleagues decreased from 2008 (n=219; 28.9%) to 2012 (n=229; 24.0%). This difference was statistically significant ($Chi^2(1,1713)=5.28$; $p<.05$).

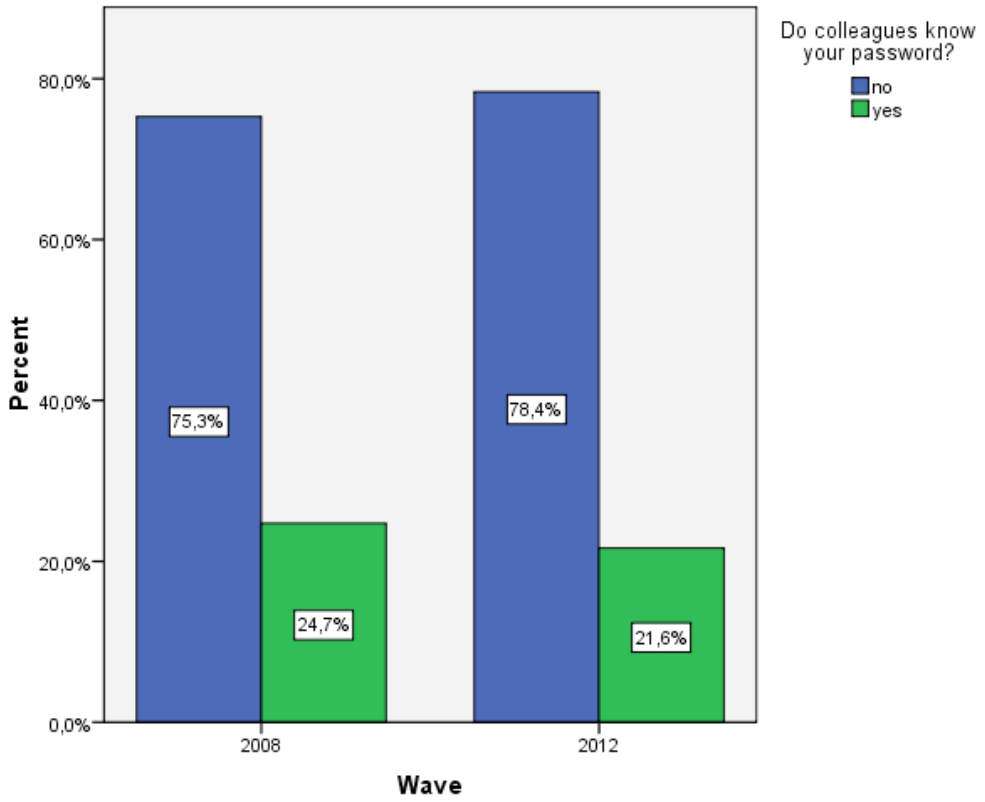

Figure 7: Two wave analysis for colleagues' knowledge of participants' passwords

5.3.2 Subgroup analysis: Gender and colleagues knowledge of participants' password(s)

In Table 4, the number of female and male participants is listed, who reported that their colleagues know their passwords.

Table 4: Subgroup analysis for colleagues' knowledge of participants' passwords

		Male	Female	Total
2008	**N**	501	510	1011
	$\mathbf{N_{know\_participant's}}$	108	142	250
	$\mathbf{N_{know\_participant's}}$/ **N**	21.6%	27.8%	24.7%
2012	**N**	646	555	1201
	$\mathbf{N_{know\_participant's}}$	118	142	260
	$\mathbf{N_{know\_participant's}}$/ **N**	18.3%	25.6%	21.6%
Total	**N**	1147	1065	2212
	$\mathbf{N_{know\_participant's}}$	226	284	510
	$\mathbf{N_{know\_participant's}}$/ **N**	19.7%	26.7%	23.1%

5.4 Confidence

Handing out the password: In 2008, 23.4% (*n*=239) of the participants handed out their password to the interviewer. In 2012, even 30.0% (*n*=358) of the participants handed out their password to the interviewer. This difference was significant in a statistical sense ($Chi^2(1,2215)=12.08$; $p<.01$: see Figure 8).

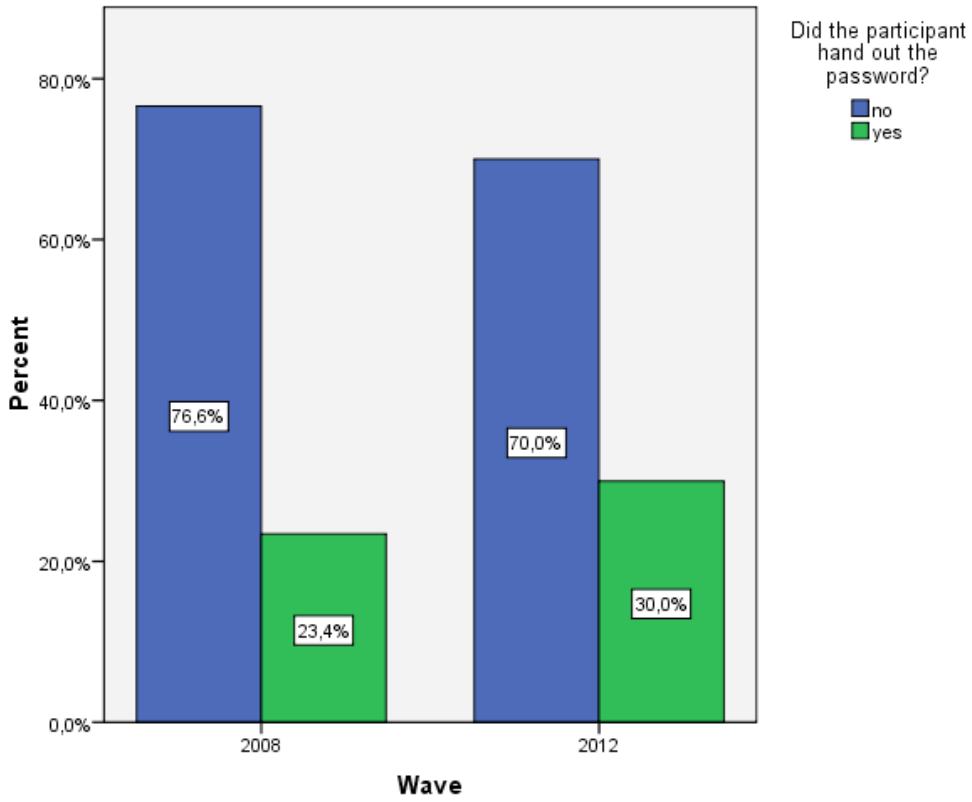

Figure 8: Wave analysis for communicating the password

Giving hints to the password: In contrast to participants' willingness to reveal their password, people were less willing to provide a hint to their password in 2012 (n=651; 54.0%) than in 2008 (n=659; 63.4%) ($Chi^2(1,2246)=20.24$; $p<.001$, see Figure 9).

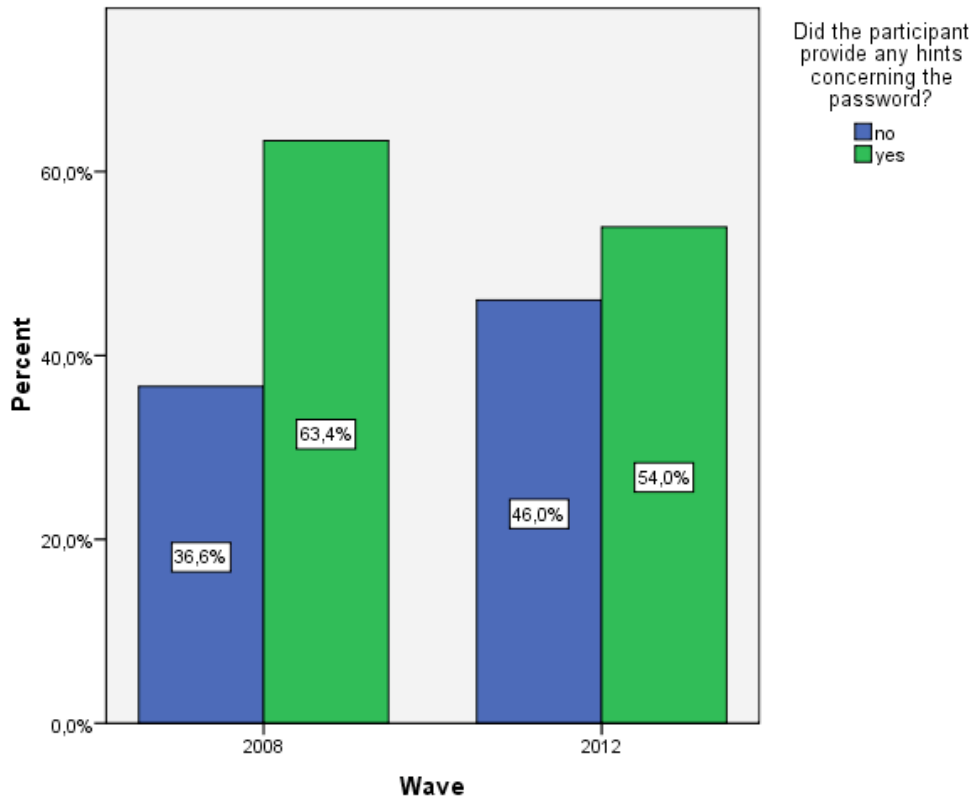

Figure 9: Providing hints subgroup analysis for the two waves

Handing out the date of birth: In contrast to passwords, people were significantly less willing to report their date of birth to the interviewer in 2012 (n=1000; 83.1%) than in 2008 (n=927; 92.1%) (Chi^2(1,2211)=39.67; p<.001).

Telling the name: In 2012 (n=1064; 88.4%), more people told their name to the interviewer than in 2008 (n=827; 79.9%). This difference was highly significant (Chi^2(1,2239)=30.41; p<.001).

Telling the telephone number: In 2012 (n=596; 49.6%), significantly less people handed out the telephone number than in 2008 (n=601; 58.0%) (Chi^2(1,2238)=15.89; p<.001).

5.5 Handing out the password: Subgroup-analyses

5.5.1 Different conditions

In 2008, there were three test conditions ("no chocolate – no reward", "chocolate at the beginning", and "chocolate at the end"). In 2012, the conditions were "chocolate at the beginning", "chocolate before the critical question", and "chocolate at the end". The number (Table 5) and percentage (Figure 10) of participants in the different test conditions, who revealed their password to the interviewer, are illustrated below.

Table 5: Number and percentage of participants, who gave passwords to interviewers in the two studies

		No reward	Chocolate at the beginning	Chocolate before the critical question	Chocolate at the end	Total
2008	**N**	496	265	/	260	1021
	$N_{pw\text{-}given}$	102	72	/	65	239
	$N_{pw\text{-}given/}$ N	20.6%	27.1%	/	25.0%	23.4%
2012	**N**	/	405	366	423	1194
	$N_{pw\text{-}given}$	/	126	127	105	358
	$N_{pw\text{-}given/}$	/	31.1%	34.7%	24.8%	30.0%
Total	**N**	496	670	366	683	2215
	$N_{pw\text{-}given}$	102	198	127	170	597
	$N_{pw\text{-}given/}$ N	20.6%	29.6%	34.7%	24.9%	26.9%

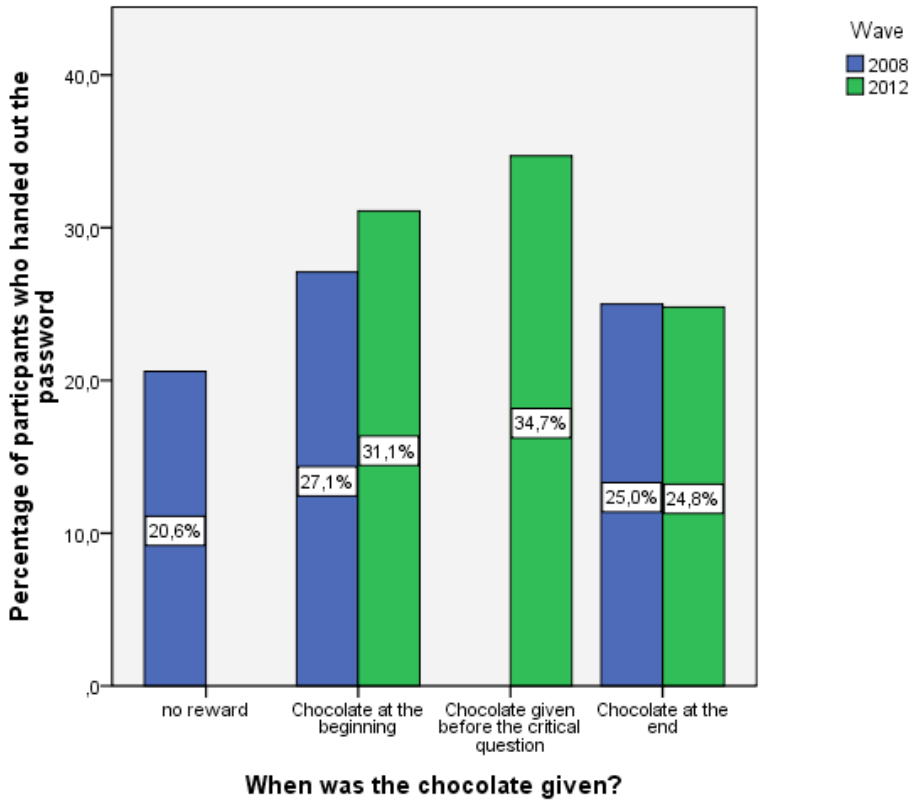

Figure 10: Time of giving the chocolate and handing out the password

5.5.2 Gender and handing out the password

Table 6 summarizes how many men and women revealed their password in 2008 and 2012.

Table 6: Subgroup analysis for gender and wave

		Male	Female	Total
2008	**N**	512	509	1021
	$N_{pw\text{-}given}$	113	126	239
	$N_{pw\text{-}given}$/ N	22.1%	24.8%	23.4%
2012	**N**	641	553	1194
	$N_{pw\text{-}given}$	197	161	358
	$N_{pw\text{-}given}$/ N	30.7%	29.1%	30.0%
Total	**N**	1153	1062	2215
	$N_{pw\text{-}given}$	310	287	597
	$N_{pw\text{-}given}$/ N	26.9%	27.0%	27.0%

5.5.3 Gender and giving hints to the password

Table 7 summarizes how many men and women revealed hints regarding their password in 2008 and 2012.

Table 7: Subgroup analysing providing hints to the password

		Male	Female	Total
2008	**N**	512	509	1021
	$N_{hint-given}$	328	326	654
	$N_{hint-given}$/ N	64.1%	64.0%	64.1%
2012	**N**	641	553	1194
	$N_{hint-given}$	360	287	647
	$N_{hint-given}$/ N	56.2%	51.9%	54.2%
Total	**N**	1153	1062	2215
	$N_{hint-given}$	688	613	1301
	$N_{hint-given}$/ N	59.7%	57.7%	58.7%

6 Conclusions

The analysis of the survey data revealed worrying results. 29.7% of all participants that were interviewed revealed their password to the interviewer. In addition, another 48.3% gave a helpful hint to their password. This means that almost four out of five people revealed some personal information to a person they do not know. Moreover, it appears that social engineering was successful in the present study. Giving chocolate as a reward affected participants' behaviour such that they were more willing to reveal their personal data. Furthermore, when the reward was handed in the beginning (32%) or immediately before asking for passwords (36%), participants were more likely to reveal their password than in the control condition (24%).

When asked for other personal information, most participants communicated their birth date and name. However, less than 50% were willing to reveal their phone number. Apparently, people are willing to give important personal information to a stranger in the street, although they seem to differentiate between different kinds of information. Generally, both men and women act similar alike. Younger people, however, handed out their password more readily. Surprisingly, people were more willing to reveal their passwords in the urban area of Luxembourg City compared to other cities in Luxembourg, which may reflect a more conservative view on Internet security in rural areas.

Today, many people use passwords (94.1%). They are also aware of password guidelines, which they need to follow (65.4%). Nevertheless, almost half of the participants *never* change their password and more than half of them uses the same password for multiple domains. These numbers are alarming because they illustrate that passwords are not handled with care. This is further supported by findings that many participants report that their colleagues know

their password(s) (78.4%) or that they are familiar with passwords of their colleagues (31.8%). Results also show that participants that answered German questionnaires were more ready to disclose their password than when interviewed using French questionnaires. The least number of passwords was obtained when using the Luxembourgish version. However, these finding are hard to interpret as not all interviewers were fluent in Luxembourgish and the questionnaire was only available in French and German.

Password were also more likely to be revealed if participants used their password for multiple domains, if they were familiar with their colleagues' passwords, and if the IT-Department or their colleagues already know it. Participants with multiple passwords and those who hardly ever change their passwords also appear to be more vulnerable of disclosing personal information. Although the popularity of passwords is still high in 2012 their overall number has increased, and they are being used more frequently for multiple domains than in 2008. This may be due to the still extending Internet use with different accounts for an ever-increasing number of applications and networks.

While participants in this study reported to know their colleagues' passwords more often than in 2008, they also reported that colleagues know their own password less often. This hints at a subjective feeling of security that participants had with regard to their own data, even though it is quite common to share passwords with colleagues. The general willingness to write down their password explicitly was even higher in 2012 than in 2008 (30.0% vs. 23.4%). Although the mean age of the 2012 sample was lower than in 2008, still 27% of all participants (18 years or older) revealed their password when adolescents were excluded. Hence, the social engineering effects found in 2008 were replicated and were shown on an even stronger level. Due to the fact that 11% of the participants stated that they had not been telling the truth regarding password information, the decrease in the number of people who provided a hint to

their password in 2012 compared to 2008 cannot be interpreted as a positive sign that awareness for IT security issues has increased.

This is also mirrored by the finding of a low awareness of sensitization campaigns in Luxembourg. Only one out of four persons reported having heard about sensitization campaigns. Even fewer people were able to name a campaign or event related to this issue. Recent campaigns were only remembered by small fractions of the sample.

What conclusions can be drawn from these findings? Even though further research is necessary to explore the cognitive mechanisms in people, it was clearly demonstrated that many participants are willing to communicate their password to a person that they have never met before. Psychologically speaking, this may be explained by the foot-in the-door technique as the interview starts with easy questions that set stage for requesting the password (Cialdini, 2001). For those participants who actively refused to reveal their password on the interviewer's initial attempt, the door-in-the-face technique might be more relevant. Having said "no" as a response to the first question causes a feeling of obligation in the participants that leads them to reveal at least some hints (Cialdini, 2001).

Both the 2012 and the 2008 studies strongly support previous in from the literature that participants' compliance or willingness to reveal personal information may be raised easily by offering a small but attractive reward (i.e., chocolate). It turned out that this reward was especially effective when provided shortly before asking the critical question to name the password. Accepting the chocolate may serve as a kind of social pressure that motivates the recipient to repay the benefactor as soon as possible, thereby illustrating the power of the norm of reciprocation in social situations. In the case of our studies, this social pressure leads many participants to disclose sensitive personal information. Alternatively, taking the reward puts participants in a good mood causing them to erroneously assume that they are in a social setting, which is "safe" for them to reveal personal information.

The present study illustrates how easy it is to obtain access to extensive personal information. Apparently, a combination of basic knowledge about the mechanisms in social situations and a decent and friendly appearance when addressing potential victims, which is further supported by a logo of a well-respected institution, turns out to be sufficient to lower people's barriers in such a way that they disclose personal information. Our findings therefore support the urgent need to intensify approaches aimed at raising the security awareness of IT users. However, our findings also indicate that many participants already have a basic awareness of IT security issues but are lacking the appropriate behavioural strategies to withstand social engineering attacks. Future campaigns should therefore also pay attention to communicating and training adequate behaviour aimed at dealing with such attacks, including saying "no" in situations of social pressure.

Our findings also have a somewhat worrying age-related aspect: If it is so easy to obtain private data from adults on a public street, how easy will it be with children in cyberspace? This should make decision takers and the public become more aware of the problem of social engineering methods used to extract data from young people. Our findings therefore support efforts to develop pedagogical material that foster and develop competences within children, parents and educational staff that will improve their knowledge and behaviour in cyberspace. Despite all efforts following the results in 2008, the present results prove that campaigns targeting Internet security awareness are still important and should even be intensified in order to change people's behaviour effectively.

6.1 References

Aronson, W. A. (2007). Social Psychology 6th Edition. New Jersey: Pearson Education, Inc.

Bless, H., Bohner, G., Schwarz, N., & Strack, F. (1990). Mood and persuasion: A cognitive response analysis. *Personality and Social Psychology Bulletin, 16,* 331-345.

Cialdini, R.B. (2001). Influence: Science and practice. Boston, MA: Pearson Education, Inc.

Cialdini, R.B.; Vincent, J.E., Lewis, S.K., Catalan, J., Wheeler, D., & Darby, B. L. (1975). Reciprocal concessions procedure for inducing compliance: the door-in-the-face technique. *Journal of Personality and Social Psychology, 31*, 206–215.

Freedman, J.L. & Fraser, S.C. (1966). Compliance without pressure: The foot-in-the-door technique. *Journal of Personality and Social Psychology, 4*, 195-202.

Goldman, M. (1986). Compliance employing a combined foot-in-the-door and door-in-the-face procedure. *The Journal of Social Psychology, 126 (1),* 111-116.

Gouldner, A.W. (1960). The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review, 25,* 161-178.

Schwarz, N. (1990). Feelings as information: Informational and motivational functions of affective states. In R. Sorrentino & E. T. Higgins (Eds.), *Handbook of motivation and cognition: Foundations of social behavior* (Vol. 2, pp. 527-561). New York: Guilford Press.

Schwarz, N., & Clore, G. L. (1988). How do I feel about it? The informative function of affective states. In K. Fiedler & J. P. Forgas (Eds.), *Affect, cognition, and social behavior* (pp. 44-62). Toronto, Ontario, Canada: Hogrefe & Huber.

Schwarz, N., & Bless, H. (1991). Happy and mindless, but sad and smart? The impact of affective states on analytic reasoning. In J. Forgas (Ed.), *Emotion and social judgments* (pp. 55–71). Oxford, England: Pergamon Press.

Steffgen, G. & Melzer, A. (2008*). IT Security – An Empirical Study on the Willingness of People to Communicate Personal Data. Condensed Report* (Unpublished Report). University of Luxembourg, Luxembourg.

Whatley, M. A, Webster, J. M., Smith, R. H., & Rhodes, A. (1999). The Effect of a Favor on Public and Private Compliance: How Internalized is the Norm of Reciprocity. *Basic and Applied Social Psychology, 21(3),* 251-259.

Worth, L. T., & Mackie, D. M. (1987). Cognitive mediation of positive mood in persuasion. *Social Cognition, 5,* 76-94.

7 List of figures

8 List of Tables

9 Appendix

9.1 German Questionnaire (chocolate at beginning)

Forschungsprojekt Informationstechnik Version **A, B, C** Enquêteur **A / B / C / D / E / F / G**
O Sprache: LUX O männlich O weiblich Datum: _____ Uhrzeit: _____

Haben Sie **zwei Minuten** Zeit für die Teilnahme an einer anonymen Forschungsumfrage der Universität Luxemburg zum Thema Informationstechnik? Können Sie bitte kurz auf folgende Fragen antworten?

Zunächst, arbeiten Sie beruflich / als Schüler mit einem Computer? JA (sonst: **Ende der Befragung**!)
Wie alt sind Sie: _____Jahre

Als Dank für Ihre Teilnahme bekommen Sie von uns vorab ein kleines Geschenk (Pralinen).

1. Benutzen Sie an Ihrem Arbeitsplatz ein Passwort ? O ja Wie viele? _____
   O nein, weiter mit **Frage 4**
2. Gibt es Vorgaben bzgl. des Passworts? O ja Welche? (z.B. Ziffern/Zeichen)_____
   O nein Zeitl. Vorgaben : _____
3. Nutzen Sie dasselbe Passwort für unterschiedliche Bereiche? O ja
   Beispiel auf der Arbeit, Bank, Internet, etc. O nein Wie viele? _____
4. Wie oft wechseln Sie Ihr/e Passwört/er?

   O täglich O wöchentlich O monatlich O selten O fast nie/nie

5. Kennen Sie einige Passwörter Ihrer KollegenInnen? O ja Wie viele? _____
   O nein
6. Gibt es an Ihrem Arbeitsplatz (Schule) eine Informatikabteilung? O ja
   O nein, weiter mit **Frage 9**
7. Kennt die Informatikabteilung die Passwörter der Mitarbeiter (Schüler)? O ja, weiter mit **Frage 9**
   O weiss nicht, weiter mit **Frage 9**
   O nein
8. Wenn Sie jemand im Namen Ihrer Informatikabteilung anruft, O ja
   geben Sie bei Nachfrage Ihr Passwort an? O nein
9. Kennen Arbeitskollegen Ihr Passwort?
   O ja Wie viele_____
   O nein: Würden Sie Ihr Passwort Ihrem Kollegen denn geben? O ja
   O nein
10. Was ist Ihr Passwort? Tragen Sie das Passwort bitte **hier** ein:

    _____

11. Einverstanden, Sie konnten das Passwort nicht angeben, aber geben Sie mir bitte einen Hinweis (z.B. Familienname, Geburtsdatum) _____
12. Um zu beweisen, dass ich diesen Fragebogen ordnungsgemäß durchgeführt habe, benötige ich persönliche Informationen von Ihnen wie zum Beispiel Ihr Geburtsdatum?
    _____ _____ _____
    Name : _____ Telefon: _____ Jahr Monat Tag

In Wahrheit sind wir nicht an Ihren persönlichen Daten interessiert. Es geht vielmehr darum festzustellen, wie groß die Bereitschaft ist persönliche Daten weiterzugeben. Diese Umfrage ist eine Untersuchung zur IT Sicherheit im Rahmen einer Sensibilisierungskampagne von der Europäischen Kommission und BEE SECURE Luxemburg, in Zusammenarbeit mit der Forschungseinheit INSIDE der Universität Luxemburg.
Nachfrage: Jetzt wo Sie wissen, dass es sich um ein Experiment handelte, die Frage :
Haben Sie mir die Wahrheit bzgl. des Passworts gesagt **(wenn** sie was gesagt haben**)?** O ja **O nein**

Erinnern Sie sich an eine Sensibilisierungskampagne zum Thema IT Schutz in Luxemburg? O ja O nein
(wenn ja, welche)_____
DANKE für Ihre Teilnahme**!**

9.2 French Questionnaire (chocolate at beginning)

Etude sur l'informatique Version **A, B, C** Enquêteur **A / B / C / D / E / F / G**
O langue : LUX O masculin O féminin Date: _____ Heure: _____

Avez-vous deux minutes pour participer à une enquête anonyme de l'Université du Luxembourg sur l'informatique? Pourriez-vous répondre aux questions suivantes?

Utilisez-vous l'ordinateur au travail ou à l'école ? Oui
Quel âge avez-vous?: _____ans

Pour vous remercier de votre participation nous vous offrons un petit cadeau (pralines).

1. Utilisez-vous un mot de passe au travail / école ? O Oui Combien ? _____
   O Non, passez à la question **4**

2. Y a-t-il des directives concernant le mot de passe ?
   O Oui Lesquelles? (p.ex. chiffres/signes)_____
   O Non Directives temporelles: _____

3. Utilisez-vous le même mot de passe pour des domaines différents?
   Par exemple au travail, banque, internet, etc.
   O Oui Combien? _____
   O Non

4. Combien de fois changez-vous votre(s) mot(s) de passe ?
   O Tous les jours O Toutes les semaines O Tous les mois O Rarement O Presque jamais/Jamais

5. Connaissez-vous les mots de passe de vos collègues ? O Oui Combien? _____
   O Non

6. Existe-t-il un service informatique à votre lieu de travail/école?
   O Oui
   O Non, passez à la question **9**

7. Est-ce que le service informatique connaît les mots de passe des employés/etudiants ?
   O Oui, passez à la question **9**
   O je ne sais pas, passez à la question **9**
   O Non

8. Si quelqu'un vous téléphone en disant qu'il fait partie du service informatique, lui donneriez-vous votre mot de passe? O Oui O Non

9. Votre collègue de travail connaît-il votre mot de passe ?
   O Oui Combien_____
   O Non: Donneriez-vous votre mot de passe à votre collègue? O Oui O Non

10. Quel est votre mot de passe? Inscrivez le mot de passe:
    _____

11. Entendu, vous n'avez pas pu nous donner votre mot de passe, mais donnez-nous un indice (par exemple. nom, anniversaire) _____

12. Pour prouver que j'ai bien effectué cette enquête j'ai besoin de certaines informations à votre sujet, comme par exemple votre date de naissance?
    _____ _____ _____
    Nom: _____Téléphone: _____ Année Mois Jour

En vérité, nous ne nous intéressons pas à vos données personnelles. Cette enquête est une étude sur la sécurité informatique dans le cadre d'une campagne de sensibilisation sur la protection des données personnelles initiée par la Communauté européenne et BEE SECURE Luxemburg, en collaboration avec l'unité de recherche INSIDE de l'Université du Luxembourg.

Question: Maintenant que vous savez qu'il s'agît d'une expérience, la question :
Est-ce que vous m'avez dit la vérité concernant le mot de passe ? O Oui **O Non**
Est-ce que vous vous souvenez d'une campagne de sensibilisation sur le sujet de la sécurité IT au Luxembourg? ?
O Oui O Non (si oui, laquelle)_____Merci **pour votre participation!**