André Melzer
Georges Steffgen

FLSHASE / University of Luxembourg

Social Engineering by Chocolate – Reciprocity Increases the Willingness to Communicate Personal Data

ADaCoR Industry Workshop – Luxembourg, April 19-21, 2016

Data Security and Social Engineering

"The attack vector is a combination of psychological and technical ploys"

S. Abraham & I. Chengular-Smith (2010, p.184)

- Successful **anti-malware technology** cause criminals to attack IT systems *indirectly*
  - Planting **malicious code** on websites
  - "Spearfishing", "whaling": sending **phishing e-mails**
  - Tricking people into revealing **passwords**

"No matter how secure a system is, there's always a way to break through. Often, the human elements of the system are the easiest to manipulate and deceive."

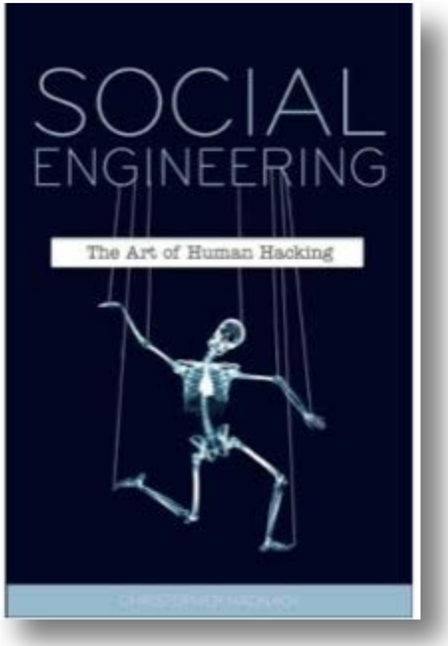
C. Hadnagy (2011, p.vx)

Social Engineering

> *“(…) social engineering is the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives.”*

C. Hadnagy (2011, p. 10)

- Social engineering attacks often address people’s basic motivations or processes
  - **Curiosity**, empathy, excitement, superstition: subject lines in emails, celebrities, games,…
  - **Greed**: supposedly easy way to gifts, rewards,…
  - …



SOCIAL ENGINEERING

The Art of Human Hacking

Social Engineering: Psychological Persuasion

- Persuasion:
  messages using powerful social mechanisms aimed at **changing/revealing** opinions, attitudes, or behavior in others

- Reciprocation: “Tit-for-tat”
  - Giving something away → inherent **expectation** that when others treat you well you respond in kind
  - Basic **norm** of human culture; **all** members of the society are trained **from childhood** to abide by the rule or suffer serious **social disapproval**

Social Engineering: Reciprocity

- Rule of **reciprocation** used by social engineers: *Give something before asking for a return favor!*

  This **rule**…

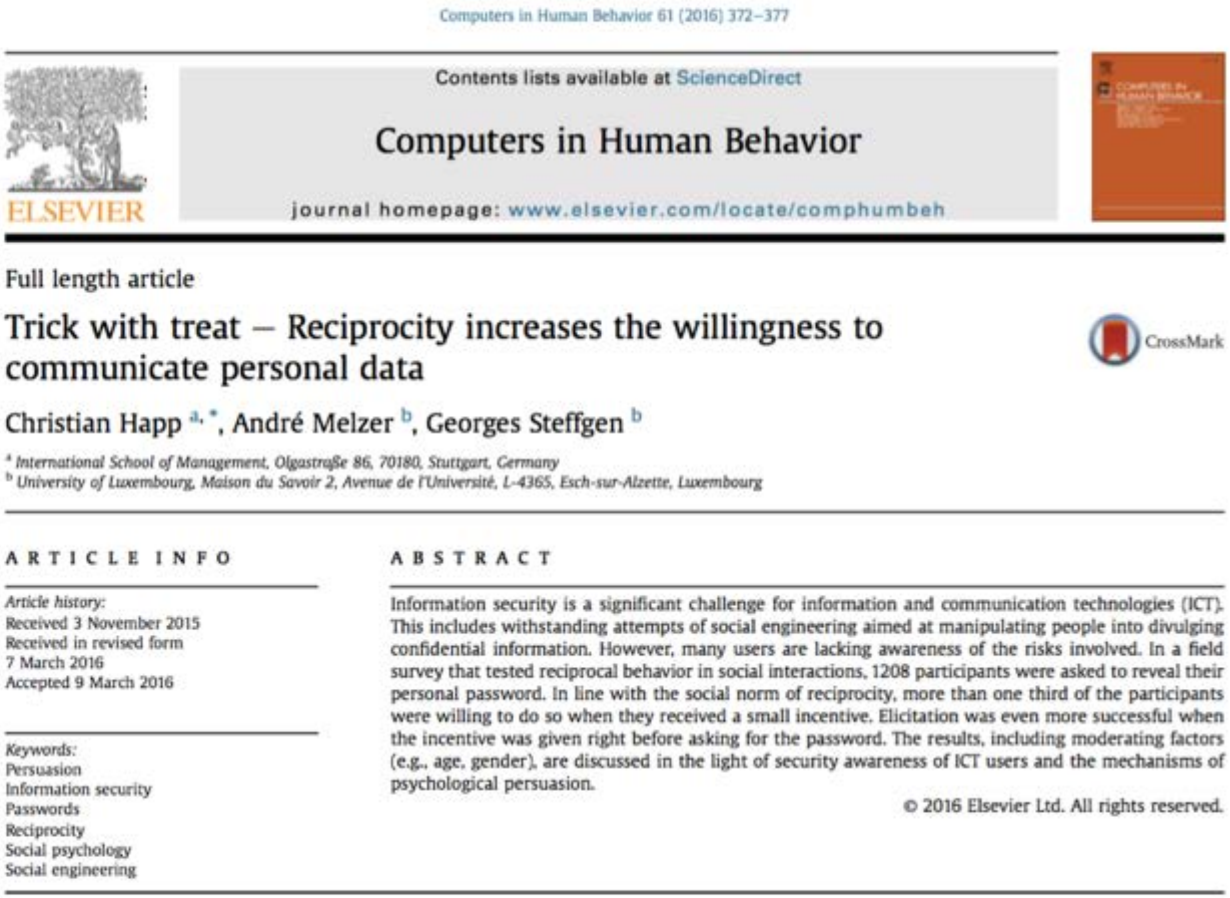
  …is extremely **powerful** → may overwhelm the influence of other factors that normally determine (rational) behavior

  …applies even to **uninvited** first favors

  …can spur **unequal exchanges** → to get rid of the uncomfortable feeling of indebtedness, people often agree to a request for a **substantially larger** favor than originally received

  …is **moderated** by time: the shorter the delay between the benefit and the opportunity to reciprocate the more successful the benefit

“Social Engineering by Chocolate” — The “Easter Eggs” Field Study



Computers in Human Behavior 61 (2016) 372–377

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Full length article

Trick with treat – Reciprocity increases the willingness to communicate personal data

Christian Happ [a, *], André Melzer [b], Georges Steffgen [b]

[a] International School of Management, Olgastraße 86, 70180, Stuttgart, Germany
[b] University of Luxembourg, Maison du Savoir 2, Avenue de l'Université, L-4365, Esch-sur-Alzette, Luxembourg

ARTICLE INFO

Article history:
Received 3 November 2015
Received in revised form
7 March 2016
Accepted 9 March 2016

Keywords:
Persuasion
Information security
Passwords
Reciprocity
Social psychology
Social engineering

ABSTRACT

Information security is a significant challenge for information and communication technologies (ICT). This includes withstanding attempts of social engineering aimed at manipulating people into divulging confidential information. However, many users are lacking awareness of the risks involved. In a field survey that tested reciprocal behavior in social interactions, 1208 participants were asked to reveal their personal password. In line with the social norm of reciprocity, more than one third of the participants were willing to do so when they received a small incentive. Elicitation was even more successful when the incentive was given right before asking for the password. The results, including moderating factors (e.g., age, gender), are discussed in the light of security awareness of ICT users and the mechanisms of psychological persuasion.

Social Engineering by Chocolate

(*cont'd*; Happ, Melzer, & Steffgen, 2016)

- Which conditions make people communicate (i.e. reveal) private information, e.g. their current computer password?
  → follow-up study to similar survey from **2008**

- Social engineering effect moderated by time delay?

  → Participants were rewarded with chocolate pralines in Easter wrapping either…

…at the end of the survey (control condition, n=426),

…at the beginning of the survey (n=407), or

…before asked to tell their password (n=373)

Social Engineering by Chocolate

(*cont'd*; Happ et al., 2016)

- Seven student interviewers presented a 2-minute-questionnaire (15 items) to **1.208** participants in Luxembourgish, German, or French in Lux-City, Esch-sur-Alzette, Diekirch

…numbers and types of passwords in use?

…knowledge of other passwords (e.g., colleagues)?

…willingness to communicate password to colleagues, IT department, stranger/interviewer?

…what is your current password?

…did you tell the truth? (control question)

…what‘s your name, phone number, date of birth?

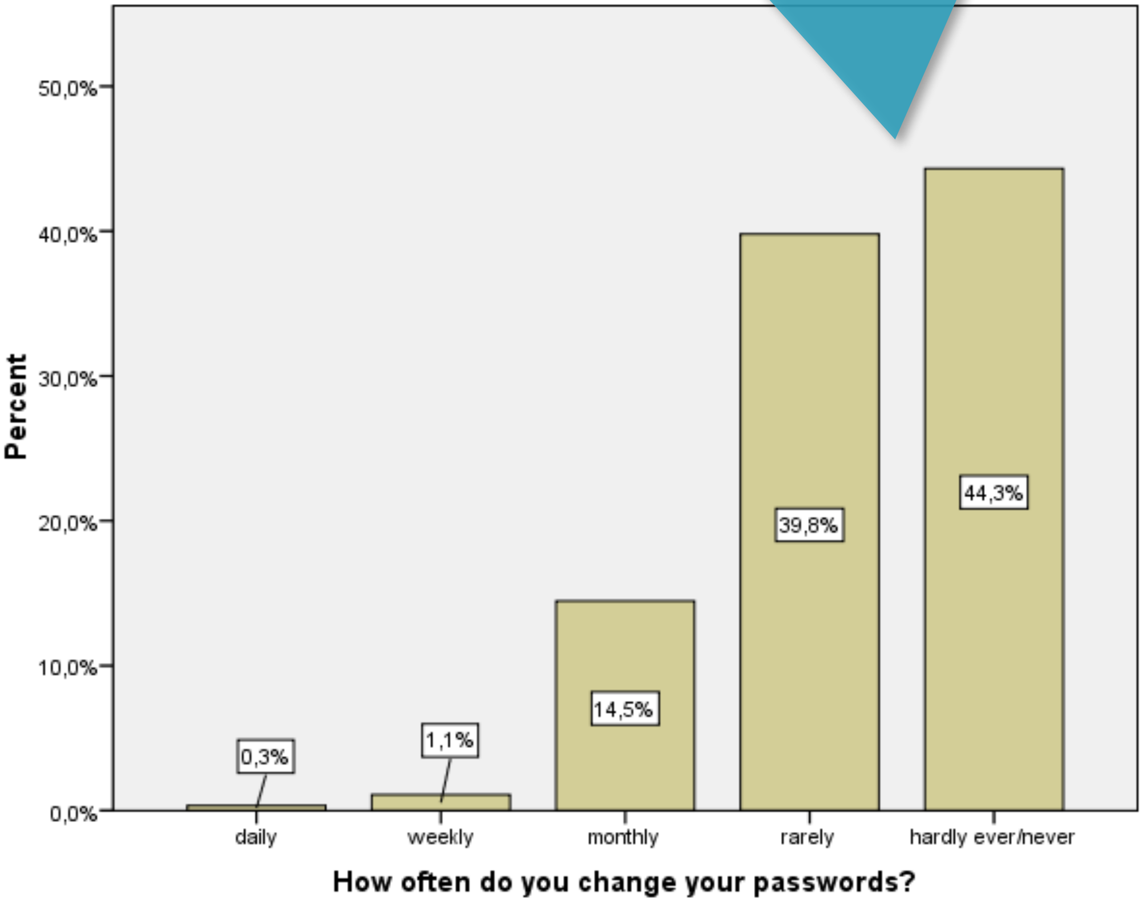
…do you recall past sensitization campaign(s) in LUX?

Social Engineering by Chocolate

(*cont'd*; Happ et al., 2016)

- Results: Password use
  - **94.1**% (n=1,146) use passwords at work
  - **55.1**% use the password for ≥2 domains

Most participants **never** or **hardly ever** change the password



Social Engineering by Chocolate

(*cont'd*; Happ et al., 2016)

UNIVERSITÉ DU LUXEMBOURG

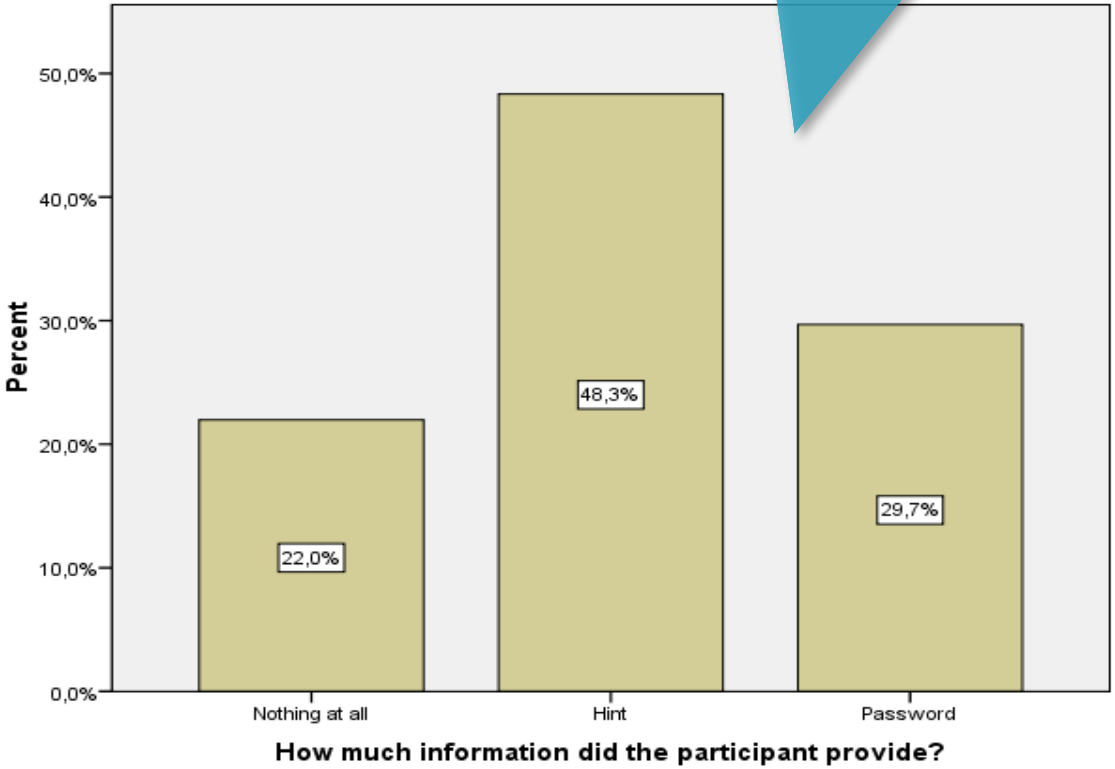
- Password ⇔ Stranger
  - **22.0%** no password, no hint
  - **78.0%** some information

- Age

  (12-74 years, *M*=31, *SD*=13)

  - **Younger** people revealed passwords more readily → especially likely to fall victim to social engineering

Most participants revealed at least **some information** about their password



Social Engineering by Chocolate

(*cont'd*; Happ et al., 2016)

- Sensitive data revealed to interviewer
  - **83.1**% date of birth
  - **88.4**% name
  - **49.6**% phone number
- Telling the truth
  - **18.4**% "lied about password"
  - **11.6**% "lied about hints"
- Sensitization campaign
  - **27.1**% heard of a campaign
  - **17.3**% recalled ≥ 1 name of a campaign
  - **22.0**% recalled ≥ 1 name or event of a campaign

Social Engineering by Chocolate

(*cont'd*; Happ et al., 2016)

- “Chocolate effect”

  (only n=724 participants who confirmed having responded truthfully; in %)

	At the beginning (n=258)	**Before password** (n=211)	**End of survey** (n=255)
Passwords	43.5		29.8
	39.9	47.9	
Hints	47.7	40.3	53.3
Total	*87.6*	*88.2*	*83.1*

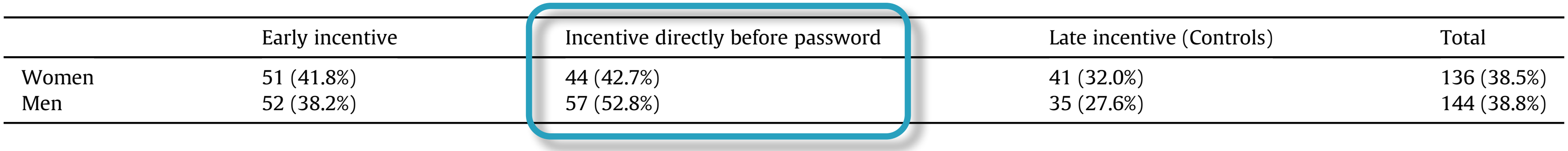
Effect of the **social norm of reciprocity**

Effect of **time delay**

Social Engineering by Chocolate

(*cont'd*; Happ et al., 2016)

- "Gender effect" only with regard to immediacy!
  (men were 1.23 times more likely to fall for the incentive when the chocolate was given right before asking for their password)

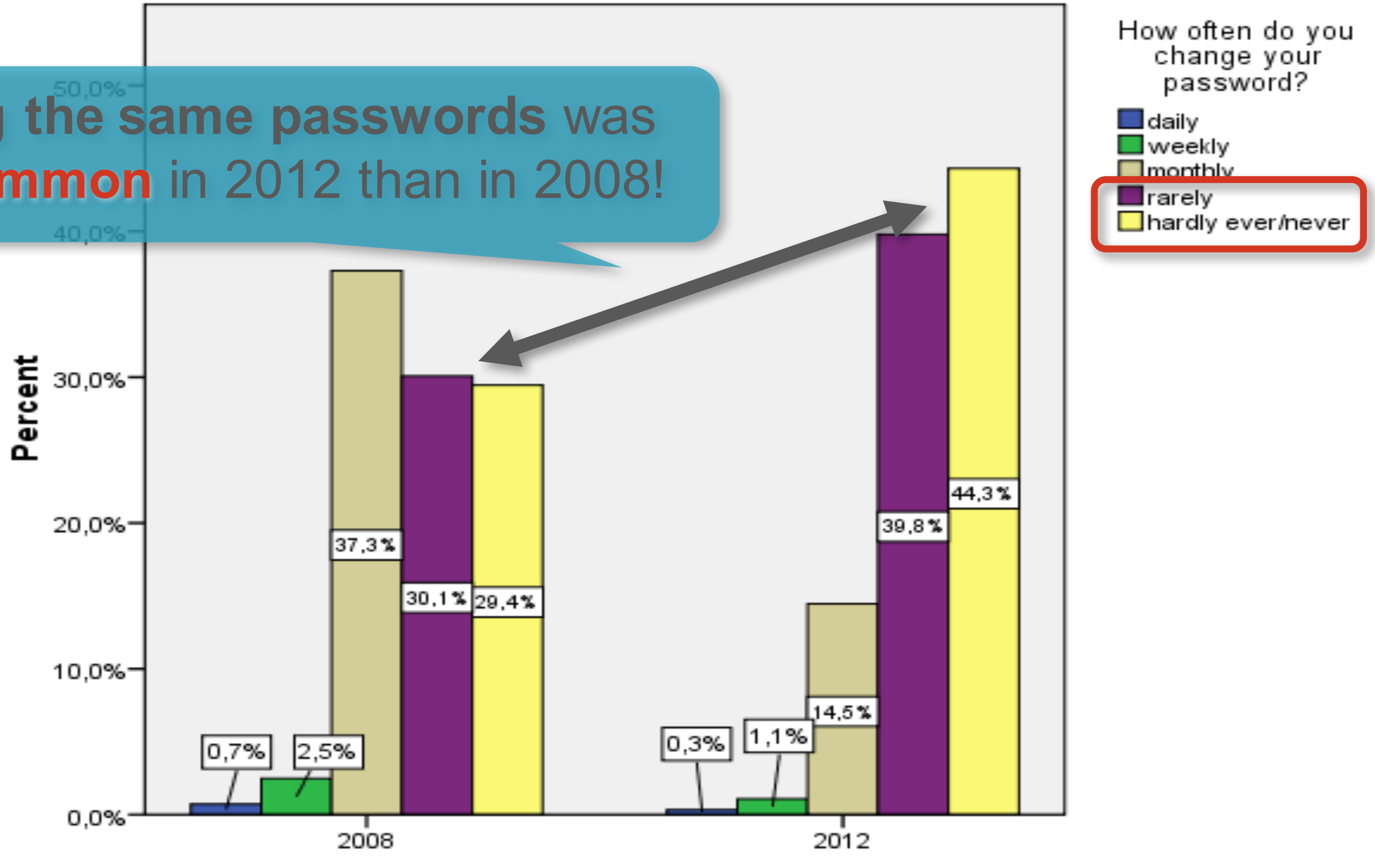


	Early incentive	Incentive directly before password	Late incentive (Controls)	Total
Women	51 (41.8%)	44 (42.7%)	41 (32.0%)	136 (38.5%)
Men	52 (38.2%)	57 (52.8%)	35 (27.6%)	144 (38.8%)

Social Engineering by Chocolate

(cont'd)

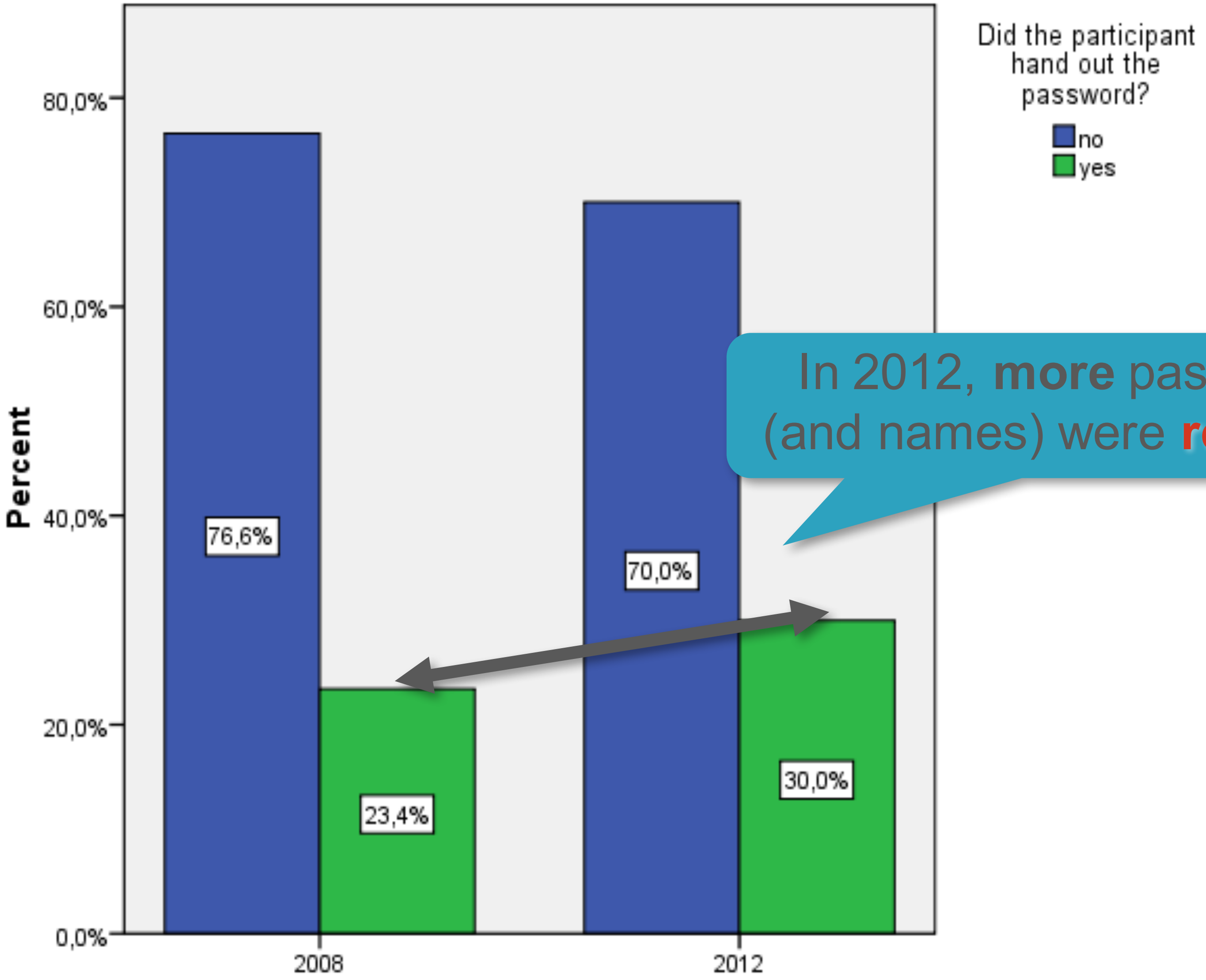
- Although people use more passwords now, they use the same password for multiple domains **more often** than in 2008



Keeping the same passwords was **more common** in 2012 than in 2008!

Social Engineering by Chocolate

(cont'd)



In 2012, **more** passwords (and names) were **revealed**!

Social Engineering by Chocolate: Summary

- Almost **9** out of 10 people reveal some password relevant information to a stranger
- Effect of social engineering:
  successful misuse of the **social norm of reciprocity**;
  even more efficient when induced *immediately* before asking the critical question

Social Engineering by Chocolate: Summary

- Almost half of the participants never change their password; even more than half uses passwords for multiple domains
  → sloppy handling of passwords

- Higher willingness to reveal the password and stronger effect of social engineering in 2012

→ Security awareness of IT users remains an urgent issue —especially with regard to younger people

- Thank you very much for your attention.

Dr. André **MELZER**

Research Unit INSIDE

Institute for Health and Behaviour

University of Luxembourg
Campus Belval
11, Porte des sciences
L-4366 Esch-sur-Alzette
Grand-Duchy of Luxembourg

andre.melzer@uni.lu

References

Abraham, S. & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implication. *Technology in Society, 32,* 183-196.

Bakhshi, T., et al. (2008). Social engineering: assessing vulnerabilities in practice. *Information Management & Computer Security, 17*(1), 55-63.

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

Freedman, J. L. & Fraser, S. C. (1966). Compliance without pressure: The foot-in-the-door technique. *Journal of Personality and Social Psychology*, *4,* 195-203.

Hadnagy, C. (2011). *Social Engineering: The art of human hacking.* Indianapolis, IN: John Wiley & Sons Ltd.

Happ, C., Melzer, A., & Steffgen, G. (2015). Trick with Treat – Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior, 61,* 372-377. http://dx.doi.org/10.106/j.chb.2016.03.026

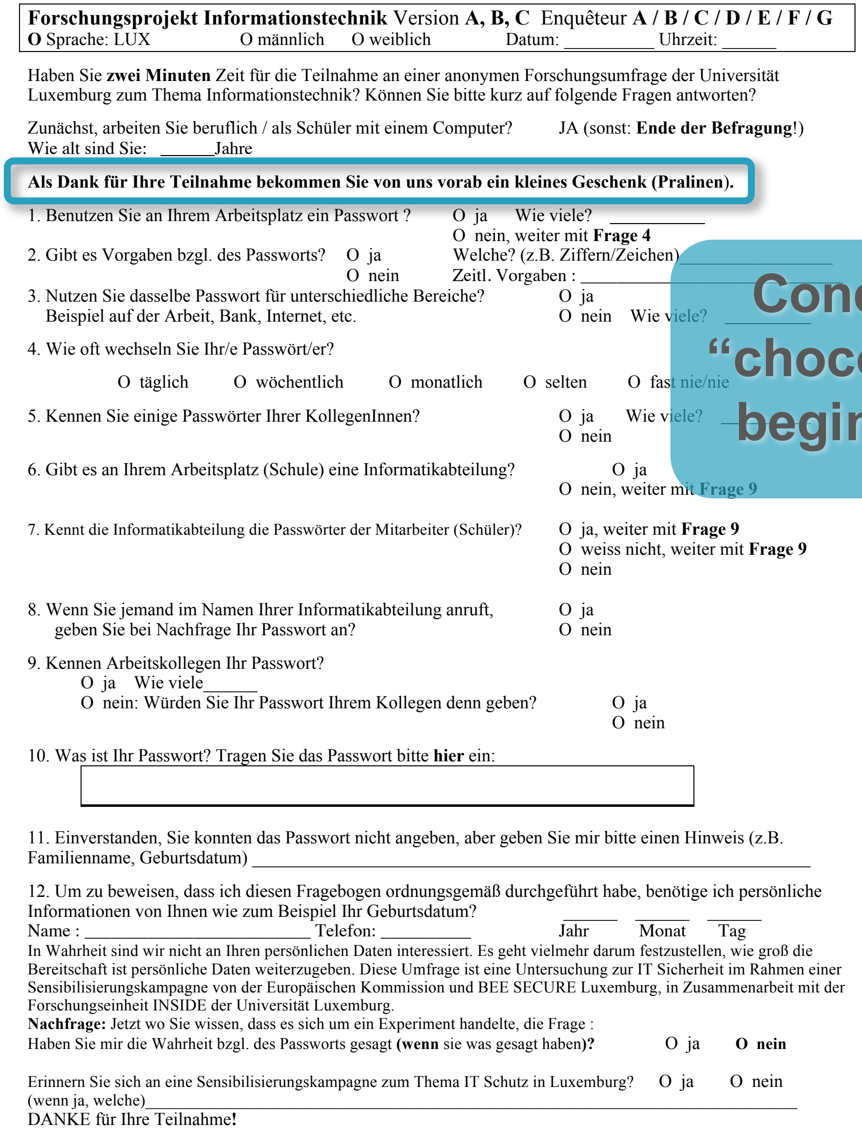
Levine, R. (2003). The power of persuasion: how we're bought and sold. Hoboken, NJ: John Wiley & Sons.

Orgill, G.L., et al. (2004, October). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *SIGITE '04, October 28-30, 2004, Salt Lake City, Utah, USA,* pp. 177-181.

Pattinson, M., et al. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28.

Provos, N, Abu Rajab, M., & Mavrommatis, P. (2009). Cybercrime 2.0: When the cloud turns dark. *Communications of the ACM, 53*(4), 43-47. DOI:10.1145/1498765.1498782

The "Easter Egg" Questionnaire



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

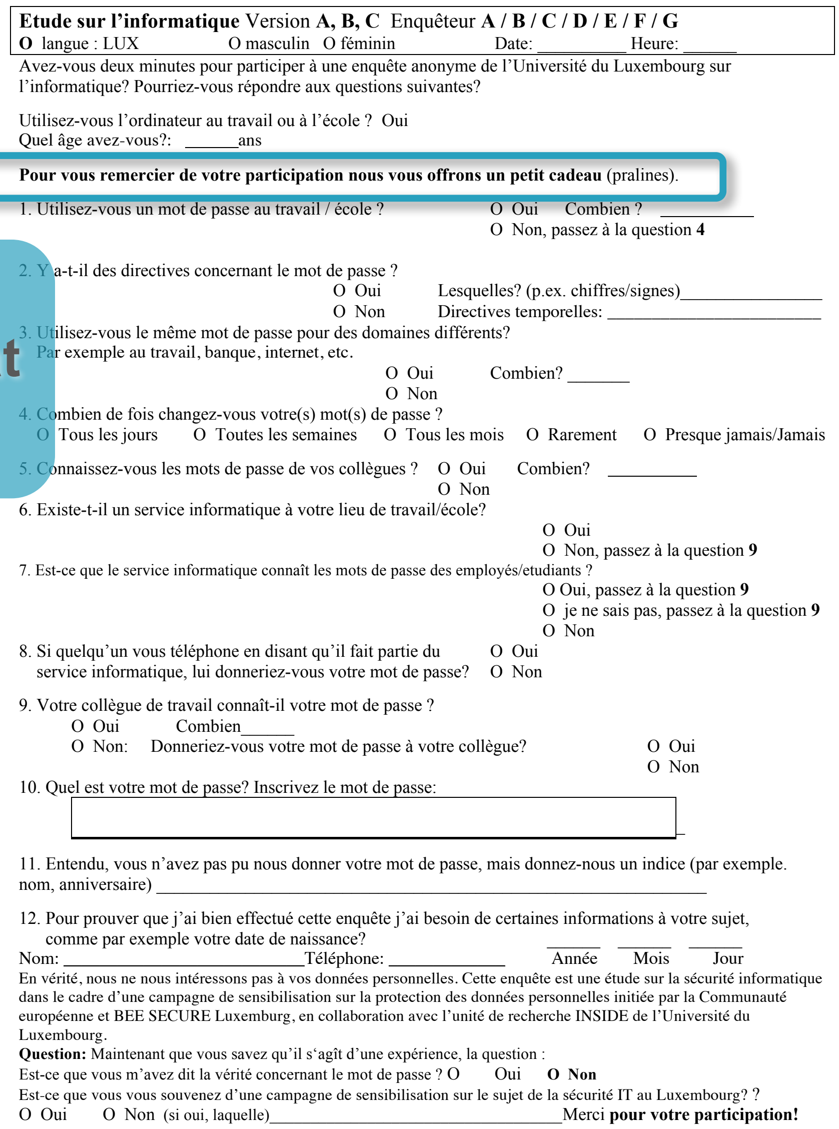
10. Was ist Ihr Passwort? Tragen Sie das Passwort bitte **hier** ein:

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**!**

Condition "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 O Oui
service informatique, lui donneriez-vous votre mot de passe? 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!**