Dr. André Melzer

University of Luxembourg

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

"Password-Based Protection of Privacy and Personal Data: friend or foe?"

CPDP 2017 — Brussels, January 27, 2017

UNIVERSITÉ DU LUXEMBOURG

Data Security and Social Engineering (SE)

"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*, e.g. by 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)

How SEs Try to Reach Their Goals...

- Exploiting basic human psychological traits (Melzer, in preparation)

1. **"Third-person effect"**
   People acknowledge the risk, but tend to feel immune to attacks

2. **"Food is the first thing. Morals follow on."**
   People follow basic needs, like fear, greed etc.

3. **Human information processing is limited**
   Only a limited amount of information can be processed simultaneously

4. **Humans are social beings**
   People adhere to socially shared norms

Psychological Persuasion: Reciprocity

- Social mechanism: "Tit-for-tat" strategy

- Give something → recipient is **expected** to respond in kind

- Basic **norm** of human culture:
  abide by the rule …or suffer serious **social disapproval**

- Can spur **unequal exchanges**

- **Moderated** by time: reciprocity is more successful with shorter delays between the benefit and the opportunity to reciprocate

"Social Engineering by Chocolate"
(Happ, Melzer, & Steffgen, 2016)

ELSEVIER

Full length article

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

CrossMark

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

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.

SMILE
SECURITY MADE IN LETZEBUERG

Europäische Kommission

Social Engineering by Chocolate
(*cont'd*; Happ et al., 2016)

- Which **conditions** make people reveal private information, including their current **computer password**?

- Seven student interviewers presented a **2-min** questionnaire

    …numbers and types of passwords in use?

    …willing to communicate password to e.g. colleagues, IT department, strangers?

    …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)

- Participants (N=**1.208**) 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 effect?

Effect moderated by time delay?

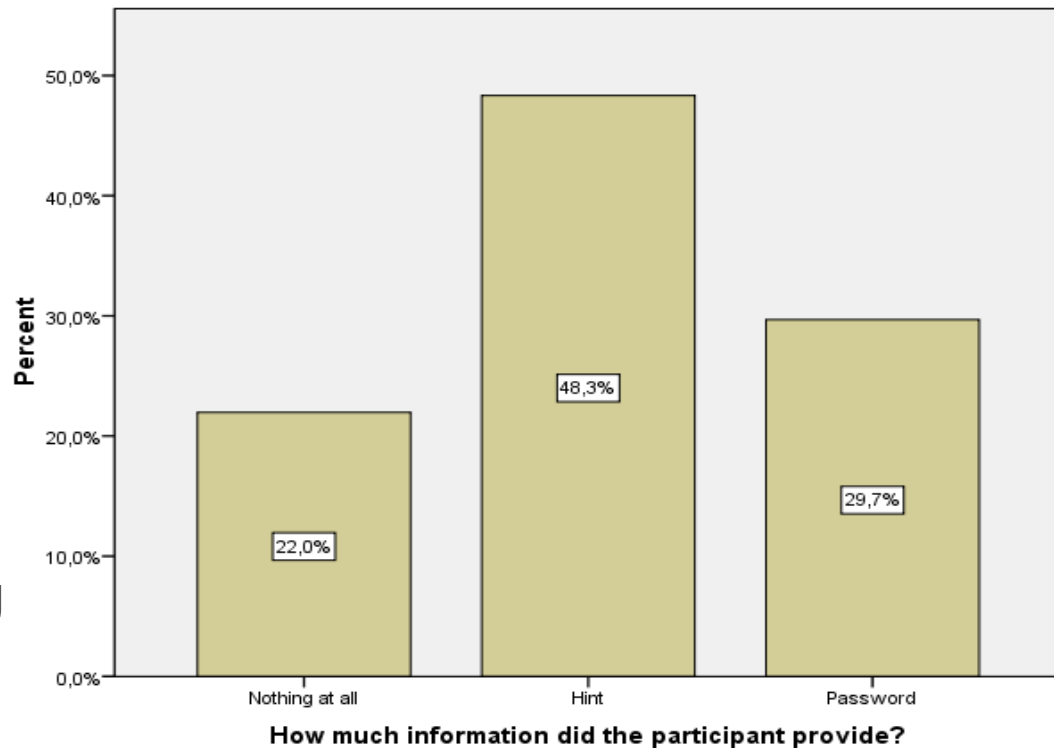# Social Engineering by Chocolate

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

- Password → Stranger

  - **78.0**% some information (e.g., password, date of birth, name)

  - **22.0**% <u>no</u> password/hint

- Age

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

  - **Younger** people revealed passwords more readily; they are especially likely to fall victim to social engineering

How much information did the participant provide?

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 **time delay**

Effect of the **social norm of reciprocity**

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

Concluding Thoughts

*"[…] nowadays it seems that it is not a matter of "**if**" you will get hacked, but "**when**"."*

C. Hadnagy (2011, p.339)

- "Third person effect" → perception of immunity
  Are you really **less prone** to become victim than others?

- Increasing security awareness of IT users remains an urgent issue—especially with regard to younger people

*"It is about creating a culture or a set of standards that each person is **committed** to utilizing in his or her entire life. […] it is the way one approaches being secure as a whole."*

C. Hadnagy (2011, p.338)

Thank You Very Much For Your Kind 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

http://www.zazzle.com/social+engineering+tshirts