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.

1. Introduction and theory

> 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. xv)

In the light of recent reports on hidden data collections (e.g., Wikileaks) and hacking of personal information, one would expect people worldwide to be concerned and alarmed about their online security. However, many people still reveal a great deal of private information on social network sites like Facebook and Twitter. The choice of private online passwords follows this reckless behavior. The 25 most common (i.e., by definition worst) passwords of 2013 prove that people are still not very creative (SplashData News, 2013). "Password" lost its long-time top position in password choices to "123456", followed by "12345678", both failing as substantial improvements to password security. However, poor passwords are only the tip of the iceberg. Below lies a much-undeveloped understanding of who to share this information with. The present study explored whether and under which conditions people are willing to share their personal information (i.e., their password) with a total stranger.

Many people still underestimate the importance of online security behavior and fall prey to those using psychological strategies aimed at tricking people to reveal personal details. Social engineering is the art of manipulating people into performing actions or divulging confidential information (Hadnagy, 2011), involving a broad range of approaches. Many of these approaches are borrowing from applied social psychology, including strategies of persuasion and its underlying mechanisms (Cialdini, 2001). In this regard, the norm of reciprocity (i.e., the feeling of being obliged to return a favor) is only one prominent example. As previous studies have shown (e.g., Whatley, Webster, Smith, & Rhodes, 1999), most people feel this sense of obligation after someone treats them kindly. This social norm of reciprocity has been researched for many decades (e.g., Berkowitz, 1972; Cialdini, 2001). To our knowledge, however, no experimental studies on this phenomenon have been reported in the context of online security and password use.

* Corresponding author.
E-mail addresses: happ.christian@ebc-hochschule.de (C. Happ), andre.melzer@uni.lu (A. Melzer), georges.steffgen@uni.lu (G. Steffgen).

http://dx.doi.org/10.1016/j.chb.2016.03.026
0747-5632/

1.1. Information security and security at the workplace

Today, ensuring information security is a major topic and a significant challenge both for suppliers and users of ICT. Organizations have increased their expenses on both physical and IT security technologies (e.g., Gordon, Loeb, Lucyshyn, & Richardson, 2004). Despite this increased expenditure, organizations encounter a number of security incidents as a result of staff errors and misdemeanors (Chan, Woon, & Kankanhalli, 2005). Contrary to the general perception that organizations are mainly vulnerable to external threats, a majority of misuse is in fact committed by their own employees. Survey reports suggest that 78% of computer attacks occur in the form of viruses (Gordon et al., 2004), which are activated through e-mail attachments that have been opened by employees or plugging in unauthorised USB devices (PriceWaterHouseCoopers, 2013).

In addition to employee computer abuse in the organization (Galletta & Polak, 2003), the lack of information security awareness has been identified as a contributing factor for information security incidents (e.g., Pattinson, Jerram, Parsons, McCormac, & Butavicius, 2012). In general, the assurance of information security requires a multifaceted approach encompassing technical and social factors (e.g., Dhillon & Backhouse, 2001; Straub & Welke, 1998) to ward off both technical and psychological ploys (cf. Abraham & Chengalur-Smith, 2010). In particular, the threat posed by techniques of Social Engineering is continuously present both at work and at home.

1.2. Social engineering

Social Engineering (SE) is broadly defined as a set of techniques used to manipulate people into performing actions or disclosing confidential information (Mitnick & Simon, 2002). Social engineering aims at gaining access to seemingly secure systems by obtaining information from a person rather than breaking into the system through electronic or algorithmic techniques (Orgill, Romney, Bailey, & Orgill, 2004).

Social engineers have been characterized as excellent psychologists that exploit typical human behavioral patterns as vulnerabilities using specific classes of attacks (Stajano & Wilson, 2011). These may include, among other psychological traits, carelessness and distractibility, fear, greed, social compliance, and the desire to help.

Social engineering is generally on the rise (e.g., Abraham & Chengalur-Smith, 2010; Hadnagy, 2011), and it threatens not only companies and government agencies, but also individuals. Social engineering is only possible because people are permanently susceptible to social tactics such as deception, manipulation, and intimidation. Additionally, savvy threat agents know how to use this to their advantage and have dedication, time, and motivation on their side (cf. Hadnagy, 2011). It is often the case that employees do not even realize that they have been target of an attack that has just disclosed private information. This makes the human being the weakest link of the security chain (Orgill et al., 2004; Scheeres, 2008). In fact, tricking only one member of an organization may be sufficient to circumvent security controls of highest technological standards (Abraham & Chengalur-Smith, 2010). A common trick in social engineering is based on social compliance and the universal mechanism of reciprocity.

1.3. The norm of reciprocity

The reciprocity norm (e.g., Cialdini, 2001; Gouldner, 1960) is a basic psychological principle, which can be found in all cultures. Reciprocity refers to the social expectation that people are strongly motivated to repay what another person has provided ("tit-for-tat"), including returning benefits for benefits, and responding with either indifference or hostility to harm. Ultimately, the norm of reciprocity has survival value (Aronson, 2007). It is an important feature of social interactions and an essential aspect in social exchange theory (Thibaut & Kelly, 1959).

All members of society are trained from childhood on to either abide by the rule or suffer serious social disapproval (Cialdini, 2001). People are taught that returning kindness is simply the right thing to do (Kolyesnikova & Dodd, 2008). On a broader scope, these obligations and helping behaviors are beneficial for societies (Ridley, 1997; Wright, 1994). People feel under pressure when they are given a small gift or a favor. This is utilized in advertising where a gift is proffered with the expectation of producing a desire to reciprocate, for example by purchasing a product (e.g., Kolyesnikova & Dodd, 2008), making a donation, or becoming more receptive to a line of argument (Whatley et al., 1999). More generally, the salience of the norm of reciprocity causes the beneficiary to feel obligated, resulting in increased compliance to subsequent benefactor requests (Gouldner, 1960; Regan, 1971). In other words, accepting a favor from another person reduces one's freedom and measures of obligation often reflect feelings of 'having to do something' (e.g., Abrahams & Bell, 1994).

The rule of reciprocity applies even to uninvited first favors (Cialdini, 2001), thereby restricting people's choice to decide whom they want to owe and putting a part of the decision in the hands of others. Studies also reveal that people often comply with requests from those who have done us small favors (Berkowitz, 1972; Boster, Rodriguez, Cruz, & Marshall, 1995; Burger, Horita, Kinoshita, Roberts, & Vera, 1997), and that reciprocity can even spur unequal exchanges. To get rid of the uncomfortable feeling of indebtedness, people often agree to a request for a substantially larger favor than the one originally received. Against this backdrop, it is not surprising that this powerful norm is popular in social engineering attacks (Cialdini, 2001), because reciprocity may also take the form of a mutual exchange of information and knowledge (Tamjidyamcholo, Bin Baba, Tamjid, & Gholipour, 2013).

Research has demonstrated several moderating and mediating factors that affect the norm of reciprocity. This includes, for example, the time delay between the benefit and the opportunity to reciprocate (Burger et al., 1997), indicating that a timeframe exists for returning acts of kindness, with shorter delays between favor and the opportunity to reciprocate being typically more successful.

Two techniques are often cited when using the norm of reciprocity in the context of advertising and marketing: the foot-in-the-door-technique (FINT) and the door-in-the-face-technique (DITF). FINT refers to the fact that people are willing to do more or even greater favors to someone they have already done a (simpler) favor to (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, which represents the request that was originally intended. 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 schema they have built. This simple favor can be as easy as a question, which people hardly ever refuse to answer.

A similar approach is the "door-in-the-face" technique (e.g., Goldman, 1986), where 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. Having said "no" as a