



Can individuals' neutralization techniques be overcome? A field experiment on password policy

Mikko Siponen^{a,*}, Petri Puhakainen^b, Anthony Vance^c

^a University of Jyväskylä, Faculty of Information Technology, P.O. Box 35, FI-40014, Finland

^b Prime Minister's Office, Helsinki, Finland

^c Temple University, USA

ARTICLE INFO

Article history:

Received 3 January 2017

Revised 26 December 2018

Accepted 5 March 2019

Available online 21 September 2019

Keywords:

Information security policy

Passwords

Neutralization

Information security

ABSTRACT

Individuals' lack of adherence to password security policy is a persistent problem for organizations. This problem is especially worrisome because passwords remain the primary authentication mechanism for information systems, and the number of passwords has been increasing. For these reasons, determining methods to improve individuals' adherence to password-security policies constitutes an important issue for organizations.

Extant research has shown that individuals use neutralization techniques, i.e., types of rationalizations, to disregard organizational information-security policies. What has not been determined from extant information security research is whether these neutralizations can be changed through educational training interventions. We argue that training based on principles of cognitive dissonance theory is a promising method for reducing individuals' use of neutralization techniques. We contribute by showing empirically that training based on cognitive dissonance theory can reduce the use of neutralization techniques when such training is designed to counter such techniques.

Using a quasi-experimental design at an organization, individuals received training on neutralization techniques in the context of password security. Using a quasi-experimental design, we found that individuals who received our training treatment exhibited substantially less intent to use neutralization techniques and were significantly more likely to use secure passwords. Additionally, a follow-up measurement three weeks after the training session showed that the experimental treatment retained its effectiveness, i.e., the experimental group exhibited substantially less intent to use neutralization techniques and a greater likelihood of using strong passwords in the future. Additionally, intent was significantly greater in the experimental group. Implications for practice and future research are discussed.

© 2019 Elsevier Ltd. All rights reserved.

1. Introduction

Authentication is a cornerstone of information security and a frontline defense against security breaches (Schneier, 2000; Zhang et al., 2009). Despite advances in biometric and visual forms of authentication mechanisms (Renaud and De Angeli, 2009), passwords remain by far the dominant means of authentication (Florêncio and Herley, 2010; Keith et al., 2009). In fact, people today have increasing numbers of passwords as they create more and more website accounts, from memberships to merchant accounts. To ensure that passwords are used securely, organizations commonly espouse password-security policies, which typically require

individuals to develop difficult-to-guess passwords that are unique for each system (Potter, 2010). Besides that, passwords should be complex and consist of random characters (TeamsID, 2015). It also is important to ensure that passwords are unique to each system because the most common mechanism for determining passwords is obtaining a password file (Tatli, 2015). This can happen through malware, which exploits vulnerabilities in operating systems or applications (Geer, 2005; Tatli, 2015). If individuals reuse the same password across different systems, a hacker who gets the password file of reused passwords can gain access to several different systems (Florêncio and Herley, 2010). The problem is compounded by literally billions of passwords that having been released through large-scale data breaches at Yahoo, MySpace, LinkedIn, and elsewhere (McMillan, 2016; Perloth, 2017). Unsurprisingly, an estimated 81% of organizational data breaches are facilitated by weak or stolen passwords (Verizon, 2017).

* Corresponding author.

E-mail addresses: mikko.t.siponen@jyu.fi (M. Siponen), Petri.Puhakainen@vnk.fi (P. Puhakainen), anthony@vance.name (A. Vance).

It has been widely reported that when faced with complex rules while creating passwords, many individuals ignore information security policies in favor of weaker, more memorable passwords and/or refuse to change their passwords (Herley, 2009; Siponen et al., 2010). Even when password policies are enforced, individuals frequently attempt to circumvent such policies, such as by reusing passwords across multiple systems or weakening a policy's effectiveness by leaving written passwords in visible places (Siponen et al., 2010). Therefore, it is no surprise that individuals' compliance with password policy is a top concern for security managers, but password enforcement alone is not a good-enough solution (Siponen and Vance, 2010). Technical enforcement to require complex passwords cannot capture reuse from one system to another, and it has been reported that individuals come up with passwords that meet enforcement minimums, but are still weak (Karjalainen et al., 2019; Tatli, 2015), e.g., using a company's name in a foreign language plus some letters, or using two common terms, but slightly misspelling them, as passwords can elude password enforcement.

Research in information security behavior has addressed the issue of unsecure password behaviors by adopting theories from criminology or health behavior. One promising theory involves neutralization techniques, which are specific types of rationalizations (Kaptein and van Helvoort, 2018; Sykes and Matza, 1957). Research indicates a major contributor to information security policy violations in general, and password security policies specifically (Barlow et al., 2013, 2018; Silic et al., 2017; Siponen and Vance, 2010). While it is known that such rationalizations can help explain violations, it is not known how such rationalizations can be overcome through security educational training interventions (Siponen and Vance, 2010). We define security educational training as formal instructor-led training that (a) informs individuals of security risks and security policies that mitigate them, and (b) instructs individuals in the skills necessary to comply with policies (D'Arcy et al., 2009). The issue here is whether one is examining (un)secure behavior vs. examining how to change unsecure behavior to secure behavior. In health behavior, such divisions between behavior and change are called theories of behavior vs. theories of behavioral change (Velicer and Prochaska, 2008). In criminology, it is known that theories explaining crime may not be able to explain why offenders stop offending (Bushway et al., 2003). Neutralization techniques are a case in point. Neutralizations are evoked to avoid moral guilt (Sykes and Matza, 1957). If this is the case, can we overcome neutralizations easily merely by making people feel guilty (Sykes and Matza, 1957)? Plus, feeling guilt is precisely the reason why neutralizations were introduced in the first place (Sykes and Matza, 1957). Another important consideration is that some neutralization techniques can indicate criminal activity (Maruna and Copes, 2005).

This article's objective is to examine whether it is possible to change or reduce individuals' neutralizations to minimize unsecure passwords by changing individual behaviors. Neutralization techniques also can be context-specific (Maruna and Copes, 2005). Given this, we also examine which neutralization techniques can be overcome in the context of password selection. To address these issues, a two-group field experiment ($n = 80$) was designed involving information security policy educational training for individuals at a large multinational organization. The individuals in the experimental treatment received specific training on neutralization techniques, including rules against misuse for failing to comply with the password security policy.

The study experiment's results indicate that training on neutralization techniques substantially decreases individuals' intent to violate the password security policy, as well as their intent to use strong passwords in the future. Additionally, a follow-up survey 3 weeks after the experiment found that members of the exper-

imental group still had substantially less intent to use neutralization techniques than they did before the experimental treatment, as well as a greater intent to follow the password policy. Thus, this study contributes by demonstrating that the use of neutralization techniques can be reduced via educational training and that individuals' intent to follow password security policies can be strengthened.

The rest of this manuscript proceeds as follows. The second section reviews extant literature on information security behavior. The third section describes the study's theoretical underpinnings, namely neutralization techniques and educational training interventions. The fourth section describes the experimental design. The fifth section describes the experimental analysis, while the sixth section discusses these results. Finally, implications for information security practice and future research are discussed.

2. Unsecure behavior, behavioral change, and the research gap

In this section, following research in criminology and health behavior (Bushway et al., 2003; Loeber and Le Blanc, 1990; Velicer and Prochaska, 2008), we separate two areas of research on information security behavior. The first area focuses on theories/models that aim to explain behavior (not change), then we discuss behavioral change, before finally examining the research gap.

2.1. Information security research on explaining/predicting (un)secure behavior

Several extant studies examine to what extent theoretical models taken from social psychology, psychology (Herath and Rao, 2009; Johnston and Warkentin, 2010; Ng et al., 2009; Pahnla et al., 2007; Siponen et al., 2007, 2010), criminology (D'Arcy et al., 2009; Siponen and Vance, 2010), and moral psychology (Myrsky et al., 2009) explain or predict individuals' compliance with information security policies or their intention to comply. These studies correlate independent variables (e.g., sanctions or neutralizations) with dependent variables, measuring intent or actual unsecure behavior. These studies show empirically which factors explain/predict unsecure behaviors (or intent). However, studies in this category do not attempt to improve behavior (i.e., change unsecure behavior to secure behavior) or change intent to perform unsecure behaviors into intent to behave securely because they merely examine (un)secure behavior, not how to change unsecure behaviors into secure behaviors. Examining change from non-compliance to compliance, or from unsecure to secure behaviors, is important because the reasons why individuals do not comply with information security, or display unsecure behaviors, can differ from why individuals change their behaviors. The difference between examining mere 'behavior' vs. 'behavioral change' is noted in extant health-behavior research and criminology. In health behavior, it is noted how "Historically, theories of behavior were concerned primarily with stability of behavior... in such theories, stable constructs are emphasized, such as...attitudes" (Velicer and Prochaska, 2008, p. 77). Prochaska noted how many health theories "had much more to say about why people don't change, rather than how people can change" (Velicer and Prochaska, 2008, p. 77). In criminology, it is noted that "we know very little about changes in individuals' rates of offending" (Loeber and Le Blanc, 1990, p. 376). Different mechanisms may explain why one engages in a crime and why he or she stops committing the crime (Bushway et al., 2003). Next, we focus on reviewing extant information security studies that examine changing unsecure behavior to secure behavior, which also is the present study's focus.

2.2. Information security research on examining how to change insecure behavior to secure behavior

To examine change, IS scholars have tested interventions through educational training programs (e.g., Puhakainen and Siponen, 2010; Straub and Welke, 1998) or messages such as fear appeals (e.g., Anderson and Agarwal, 2010; Johnston and Warkentin, 2010; Johnston et al., 2015) aimed at ensuring individuals' compliance with information security procedures. Typical settings for such change studies contain an intervention and a posttest (Johnston et al., 2015). Theories used in these interventions vary. While Straub and Welke (1998) did not provide the theoretical details behind their educational training intervention, they reported that security training significantly influenced managers' security planning behavior.

Like Straub and Welke (1998), Puhakainen and Siponen (2010) use action research to focus on changing individuals' behavior in the context of a small company where individuals did not encrypt their emails. Puhakainen and Siponen (2010) modified different persuasion techniques to the context of secure email use.

While the aforementioned studies by Straub and Welke (1998) and Puhakainen and Siponen (2010) offered qualitative evidence on the relevance of their educational training intervention, other studies (Anderson and Agarwal, 2010; Barlow et al., 2013; Johnston and Warkentin, 2010; Johnston et al., 2015) used quantitative evidence obtained through self-reporting surveys. Other differences are that while Straub and Welke (1998), Puhakainen and Siponen (2010), and Johnston et al. (2015) carried out their action research within business organizations, Agarwal and Anderson (2010) and Johnston and Warkentin (2010) used university students and faculty. Also, while Straub and Welke (1998) and Puhakainen and Siponen (2010) used face-to-face training with real people (and two-way communication), Agarwal and Anderson (2010), Johnston and Warkentin (2010), and Johnston et al. (2015) utilized one-way communication, such as fear appeal messages.

For example, Agarwal and Anderson (2010) studied how message qualities can influence home computer individuals' information security attitudes and norms using 101 undergraduate students as their sample. The students were assigned to two groups in a computer lab: One reviewed a website with a positive information security message, while the other reviewed a website with a negative information security message. The positive message stressed the benefits of taking information security precautions, while the negative message stressed the consequences from not taking such precautions. The participants then filled out a questionnaire. While the results failed to show a positive relationship between these two interventions and attitudes, they did indicate that a positive message leads to a descriptive norm.

In another example, Johnston and Warkentin (2010) examined the effects of fear appeals on intent to use anti-spyware tools, with university students and faculty used as their sample. A fear appeal is a persuasive message aimed at changing people's behavior—or intent to behave, like in this study—through scaring them by listing terrible things that could happen if they do not behave as suggested in the fear-appeal message (Johnston and Warkentin, 2010). These experimental groups consisted of 200 faculty and students, with the control group consisting of 30 respondents. The groups completed a pretest before the treatment and a posttest immediately after the treatment. The message was designed based on protection motivation theory. The researchers found that message elements that contained response efficacy, social influence, and self-efficacy exerted a positive influence on individuals' intent to adopt anti-spyware tools. Following Johnston and Warkentin (2010), Johnston et al. (2015) examined the effect of fear

appeals and the role of personalized threats with respect to a USB stick in a government office in Finland.

Barlow et al. (2013) examined change of intent to act in a secure manner by comparing how deterrence and rationalization-based messages affect individuals' reported intent to violate information security policies.

2.3. Research gap: can we reduce neutralizations to change behavior?

Siponen and Vance (2010) showed that the intent to violate information security policy correlates with neutralizations. Similarly, Siponen et al. (2012) showed that the intent to engage in unauthorized copying of software correlates with neutralizations. These studies examine behavior (or intent to behave)—but not change. Hence, they do not show whether/how we can change the minds of those who neutralize. As a result, the question of how researchers and practitioners can best change people's use of neutralization techniques remains as a significant research gap (Siponen and Vance, 2010). While Barlow et al. (2013) provided useful information on how rationalizations and deterrence-based messages can be articulated to change intent to act in a secure manner, measuring whether the respondents had used neutralizations when they were behaving in an insecure manner went beyond the scope of their paper. Similarly, Barlow et al. (2018) found that antineutralization communications—brief written statements that specifically address neutralization techniques—reduced intentions to violate the policy. However, they did not investigate the ability of educational training to counteract neutralization techniques. In summary, we do not yet know whether educational training can actually reduce individuals' use of neutralization techniques to violate information security policies.

We argue that not just any educational training intervention or message framing would change the minds of those using neutralizations. According to Sykes and Matza (1957), neutralizations are evoked so that offenders can put guilt aside: "This guilt, and its potential for producing a negative self-image, helps dissuade us from engaging in criminal or deviant acts most of the time. Therefore, in order to participate in deviant behavior under such conditions, we must find ways to rationalize the action or neutralize the guilt associated with it" (Maruna and Copes, 2005). If Sykes and Matza (1957) are correct—that neutralization is introduced to avoid guilt and negative self-image—then arguably, it is not necessarily an easy task to change the behaviors of those who neutralize their actions (Maruna and Copes, 2005). However, to date, we lack understanding of how practitioners and researchers can change their use of neutralization techniques in an IS context, as recognized by Siponen and Vance (2010). Also, we lack understanding as to which counter-rationalization tactics (if any) are effective in reducing the use of neutralization techniques. This study is aimed at taking a first step in this direction by examining the effects of an educational training intervention on individuals' intent to use neutralization arguments in the context of passwords.

3. Theoretical framework

3.1. Neutralization techniques

Neutralization techniques were advanced by Sykes and Matza (1957). They originally put forward five such techniques, namely denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties. Later scholars extended the theory by offering more techniques on neutralization. Minor (1981) added "the defense of necessity," Coleman (1994) advanced an argument based on entitlement, Lanier and Henry (1998) suggested "relative acceptability," and Cromwell and Thurman (2003) advanced the technique of

defense by comparison. The neutralization techniques provided by Sykes and Matza, and others (Collins, 1994; Cromwell and Thurman, 2003; Minor, 1981) have been applied in several contexts, such as deer poaching (Eliaison and Dodder, 1999), hate crimes (Byers et al., 1999), rule-breaking in military environments (Pershing, 2003), drug use (Priest and McGrath III, 1970), corporate crime (Piquero et al., 2005), and workplace theft (Hollinger, 1991). In the IS area, Lim (2002) found that the metaphor of the ledger is invoked by individuals to justify cyberloafing. Siponen and Vance (2010) found that neutralization techniques strongly predicted individuals' intent to violate information security policies by sharing passwords, failing to protect sensitive data, and neglecting to secure their work computer. Morris and Higgins (2009) found that neutralization techniques strongly predicted the intent to commit software piracy. Harrington (1996) found that denial of responsibility, one type of neutralization technique, was strongly correlated with computer-abuse intent. Similarly, Willison (2006) suggested that neutralization techniques affect information security behavior in general.

3.1.1. Denial of responsibility

Denial of responsibility refers to a situation in which people who engage in rule-breaking deny responsibility for their actions (Rogers and Buffalo, 1974; Sykes and Matza, 1957). A deviant who applies denial of responsibility views himself or herself as a billiard ball being helplessly propelled through different situations (Sykes and Matza, 1957). Hence, the person rationalizes that the action in question is beyond his or her control (Piquero et al., 2005). For example, a denial-of-responsibility argument in the context of information security could be that individuals justify their non-compliance by claiming that they are not well-versed on the company's password guidelines (Siponen and Vance, 2010).

3.1.2. Denial of injury

Denial of injury focuses on minimizing the harm caused by an act. With denial of injury, the delinquent justifies an action by reasoning that no one will get hurt (Sykes and Matza, 1957). For example, potential car thieves may regard auto theft as "just borrowing," which does not hurt anyone (Sykes and Matza, 1957, p. 667). Byers et al. (1999) reported that people committing hate and property crimes justified their actions using denial of injury by arguing that no harm or damage was actually done. Similarly, in an information security context, individuals can, for example, justify their behavior by claiming that it is acceptable to use simple passwords at work if no one gets hurt (Siponen and Vance 2010).

3.1.3. Defense of necessity

Defense of necessity is based on the justification that if the rule-breaking is viewed as necessary, one should not feel guilty when committing the action (Minor, 1981, p. 298). In this regard, the offender can put aside feelings of guilt by believing that an act was necessary and that there was no other choice (Piquero et al., 2005). For example, Eliaison and Dodder (1999, p. 248) found that deer poachers neutralized their actions through the defense of necessity by claiming that poaching is not wrong because their families are hungry and that they must acquire food through poaching. A defense-of-necessity neutralization in the context of information security could be that individuals justify the use of simple passwords at work by rationalizing that they do not have time to memorize complex passwords (Siponen and Vance, 2010).

3.1.4. Condemnation of the condemners

Condemnation of the condemners refers to a justification in which one neutralizes his or her actions by blaming those who are the target of the action (Byers et al., al.,1999). For example, one might break a law because the law is unreasonable (Siponen and

Vance, 2010). Eliaison and Dodder (1999, p. 248) reported that deer poachers neutralized their actions through this technique by claiming they hunt because game wardens themselves hunt illegally or because the poachers hate game wardens. In the case of information security, a condemnation-of-the-condemners neutralization is to claim that information security policies are unreasonable (Siponen and Vance, 2010).

3.1.5. Appeal to higher loyalties

An appeal to higher loyalties takes place when someone justifies norm-breaking by claiming loyalty to someone or something (Byers et al., 1999) or acts on behalf of someone (Sykes and Matza, 1957). In an organizational context, an individual may appeal to organizational values or hierarchies (Piquero et al., 2005). In the context of compliance with information security procedures, individuals could utilize the argument of an appeal to higher loyalties by arguing that he or she must violate corporate security procedures to get his or her work done (Puhakainen and Siponen, 2010; Siponen, 2006; Siponen and Vance, 2010).

3.1.6. Entitlement

The argument based on entitlement, originally advanced by Coleman (1994), suggests that people have a right to engage in certain behaviors. For example, an individual may feel that he or she is entitled to receive gains from norm-breaking behavior. Elison (2003) reported that an argument based on entitlement was used by fishermen who fished without a permit. In the context of information security behavior, individuals could justify their behavior by saying that they should be free to choose any password they want.

3.1.7. Relative acceptability

Henry and Eaton (1999) advanced the concept of relative acceptability. This technique is used to remove blame for one's actions by pointing out that others are even "worse than me." For example, Lanier and Henry (2004) reported on police officers who justified the beating of a suspect by claiming some other officers would have been even more brutal. In the context of the present study, individuals could justify their use of weak passwords by alleging that other individuals' passwords are much weaker than theirs.

3.1.8. Defense by comparison

Cromwell and Thurman (2003) advanced the technique of defense by comparison. The argument of this defense is that the person is excusing his or her actions by suggesting that while the action might not be good, the person could have acted even worse (but did not). Cromwell and Thurman (2003) found that offenders use this for shoplifting. In the context of the present study, a person using this argument might say that the use of weak passwords at work is not a big deal compared with other issues, such as being lazy on the job.

3.2. Cognitive dissonance theory

Learning can be defined as a persistent change in the learner's performance—an individual's information security behavior in this case (Driscoll and Driscoll, 2005). Educational training interventions have long been a recognized means of improving individuals' security behavior in information security (Straub, 1989; Straub and Welke, 1998). Effective educational training requires the use of proper methods for designing and delivering the training (Puhakainen and Siponen, 2010). In the present study, the theory of cognitive dissonance (Festinger, 1957) was selected as the theoretical basis for planning and executing the educational training intervention. Festinger's (1957) theory holds that there is a tendency for individuals to seek consistency in their beliefs and

perceptions. When there is an inconsistency between one's attitudes or behaviors (i.e., dissonance), one must change his or her attitudes or behavior to eliminate or reduce the dissonance. Festinger's (1957) theory conceptualizes dissonance as a negative drive state—such as hunger or thirst. Consequently, an individual is motivated to reduce it.

The theory of cognitive dissonance (Festinger, 1957) is a well-suited point of departure for educational training interventions that aim to diminish learners' use of neutralization techniques. In our experiment, the objective is to create dissonance between individuals' current behaviors and their ideas (provided during the training) regarding secure behavior, as described in the host organization's information security policies. According to Festinger (1957), such training should lead to changes in the learner's attitudes and eventually in his behavior. A similar view is shared by Neighbour (1992), who makes the generation of appropriate dissonance into a major feature of teaching.

In our experiment, the objective is to reduce learners' use of neutralization techniques through cognitive inconsistencies. This is expected to lead to increased intent to comply with the host organization's information security policies. This view is shared by Elliot and Devine (1994) and Dechawatanapaisal and Siengthai (2006). According to Elliot and Devine (1994), cognitive inconsistencies have been shown to motivate people to actively attempt to alter their behaviors in an effort to attain consonance between attitude and behavior. Moreover, Dechawatanapaisal and Siengthai (2006) found that people's unpleasant psychological states might be moderated in the learning process to enable their cognitive dissonance conditions to become a motivating factor that elicits attitudinal and behavioral change. According to Dechawatanapaisal and Siengthai (2006), cognitive dissonance may help arouse people to depart from the status quo. In such situations, people are willing to consider the need for change and are energized to be able to absorb the new knowledge.

Despite its possible usefulness, existing information security education and training research has not used the theory of cognitive dissonance. However, Festinger's (1957) theory has proven useful in other fields of IS to design interventions that aim for behavioral changes. For example, Cosolvo et al. (2009) used it to design strategies for technologies that support behavioral change in everyday life, and Ma et al. (2009) used it to design an approach to learn programming concepts by novice programmers.

3.3. Educational training and hypotheses

Information security education and training has long been a recognized means of improving individuals' security behavior (Straub, 1989; Straub and Welke, 1998). The use of effective training for this purpose requires the use of a proper learning method (Puhakainen and Siponen, 2010).

Learning can be defined as a persistent change in a learner's performance, e.g., in an individual's information security behavior (Driscoll and Driscoll, 2005). Educational training interventions in information security eventually should aim for such behavioral changes. In changing an individual's behavior, his cognitive processing has a key role. Here, an individual's cognitive processing refers to his active critical processing of information that he receives, e.g., during information security training. This contains the idea that the recipient's relevant knowledge acquisition requires him to understand the received information in a meaningful way. This enables the recipient's integration of new knowledge into what he already knows. Extant research suggests that cognitive processing of persuasive information is necessary for long-lasting attitudinal and behavioral changes (Gardner, 2006; Greenwald, 1968; McGuire, 1968). Similarly, constructivism stresses activating learners' own thinking processes. In addition, it empha-

sizes critical reflection of learners' own knowledge and interpretive and conversational forms of evaluation (Karjalainen and Siponen, 2011). Educational training approaches based on constructivism are viewed as preferred approaches for educating and training white-collar individuals in organizations (Karjalainen and Siponen, 2011; Puhakainen and Siponen, 2010). Consequently, constructivism was selected as the pedagogical paradigm behind the host organization's password training.

Given the above theoretical support, we offer the following hypotheses:

H1a: Educational training interventions that evoke cognitive dissonance will reduce use of (a) "denial of responsibility," (b) "denial of injury," (c) "defense of necessity," (d) "condemnation of the condemners," (e) "appeal to higher loyalties," (f) "entitlement," (g) "relative acceptability," and (h) "defense by comparison" neutralization techniques.

H2: Educational training interventions that evoke cognitive dissonance will increase intent to use strong passwords.

4. Methodology

To test whether an educational training intervention could be used to reduce individuals' use of neutralization techniques, we conducted a field experiment at a regional office in the United Arab Emirates (UAE) of a multinational company in the energy sector. The office had 98 employees on the payroll. Although our field experiment was conducted at one office of the multinational company, the corporate information security manager indicated that problems with password policy compliance were experienced throughout the company.

Field experiments, like laboratory experiments, have the advantage of strong internal validity afforded by precision and control (Dennis and Valacich, 2001). On the other hand, because field experiments are conducted in natural settings, independent variables more closely assume true-to-life values, i.e., "approximate a natural spectrum of events" (Bouchard, 1976; Straub et al., 1993, p. 137).

4.1. Planning the educational training intervention

Password education and training was provided as part of general training sessions dealing with the host organization's information security instructions. The researchers were responsible for planning and delivering the educational training intervention. The first step in planning the password education and training was determining the training's desired goal. A few months before the educational training intervention, an author of the paper visited the information security manager and the UAE office for the purpose of interviewing employees' understanding of their information security practices. The author also interviewed the IT staff in the UAE office, who claimed that password security was not a problem, because they had automated password controls in place that ensured that employees selected passwords complied with the password policy. However, although automated password controls are important, they have limitations. First, they typically do not detect individuals' reuse of passwords across an organization's internal applications and cannot detect reuse of passwords across external applications. Second, they commonly do not detect the use of biographical information that makes passwords vulnerable to targeted password cracking attacks (Picolet, 2017). Finally, although automated password controls can be made more strict to eliminate loopholes, making password policies overly stringent can have a negative effect on usability which can introduce a range of negative consequences (Florêncio et al., 2016), such as writing down passwords in insecure places. For this reason, a combination of automated password controls and effective password security training is needed.

Indeed, interviews with employees indicated problems like those described above. The automatic controls could not capture various terms, such as employees' own names written verbatim or with slight variation. This was especially the case for names and terms from different languages and cultures. Moreover, the automatic controls could not capture password reuse across applications. Based on analysis of the employee interviews, the host organization's information security manager and the researchers decided that the prevailing practice of using weak passwords should be remedied due to the risks it posed. Consequently, the primary goal of the educational training intervention was defined as increasing individuals' intent to use strong passwords.

The second step in planning the educational training intervention was analyzing whether employees' current passwords were weak in the first place to ensure that the educational training intervention focuses on relevant problems (Siponen and Vance, 2014). As mentioned earlier, one of the authors participated in an audit of the company before the educational training intervention. During the audit, it was discovered through interviews with employees that most were aware of the existence of a password policy, but could not recall its contents or its requirements for creating strong passwords. Instead, employees had strong—and often insecure—assumptions regarding their own password practices (e.g., “no one knows my mother's maiden name”). Many employees believed it was difficult to create complicated, yet memorable passwords. For this reason, they commonly rationalized that it was acceptable to use a piece of personal data—such as one's own name, spouse's name, or child's name—as the basis for one's password because it is easy to remember.

4.1.1. Developing and implementing educational training intervention

The third step of the planning phase was designing an educational training intervention for password security, which contained four components. The first was designed as an instructor-led introduction to the topic of proper use of user IDs and passwords, which included helping individuals understand what constitutes a strong password. The objective was to activate learners' existing knowledge about the subject matter. In particular, individuals should be aware of the existence of the company's password policy and its rules regarding the use of strong passwords. This first component was the same for both the experimental and control groups.

In accordance with constructivism, the second component was designed as a collaborative group discussion regarding the characteristics of the learners' own passwords that they used within the company's systems. This component was for both the control and experimental groups, and its goal was twofold. First, it aimed to make the component personally relevant to the learners and, in this way, motivate them toward critical reflection on their current password practices (Puhakainen and Siponen, 2010). Making the issue personal is important in creating dissonance, as according to Wu and Ahn (2010), conflicting information should be an individual-centered and subjective construct. Moreover, practical exercises that accompanied the lectures diminished the learners' cognitive load (Clark, 2003). However, we did not develop practical exercises in which the learners created passwords. Rather, learners were to discuss, in small groups, the traits of their own passwords and whether they used passwords that are easy to remember, but difficult to guess or crack by an attacker.

Second, we used this approach to increase dissonance between the individuals' current password practices and their ideas regarding strong passwords. According to Ma et al. (2009), when learners appear to misunderstand a concept, cognitive dissonance can be used to challenge their current understanding and motivate them to change that understanding. In accordance with this view, our educational training intervention should create dissonance be-

tween individuals' current password practices and the new ideas (from the educational training) regarding secure (i.e., strong) passwords. However, according to Ma et al. (2009), cognitive conflict alone is unlikely to be sufficient to effect change in understanding. They claim that students must be encouraged to create new models. Consequently, the goal of the second phase of educational training was to clarify the advantages of using strong passwords and point out obvious threats in individuals' existing practices in using weak passwords.

In the third component, the goal was to address learners' use of neutralization techniques explicitly by creating dissonance between individuals' prevailing ideas on password security and proper use of strong passwords. This component only applied to the experimental group. The instructor was to demonstrate the possible consequences to the organization and to the learners themselves if weak passwords were used. The goal was to make the subject matter important to each individual, which, in turn, should motivate the learners' critical cognitive processing regarding their existing password practices (cf., Petty and Cacioppo, 1986; Petty and Cacioppo, 1981; Puhakainen and Siponen, 2010). Furthermore, the purpose of the task was to build a cause-and-effect mental model to enhance long-lasting learning (Clark, 2003).

Finally, in the fourth component, the instructor introduced the use of mnemonics, both to the experimental and control groups, through examples and demonstrations. However, in the case of only the experimental group, the mnemonics dovetailed with the neutralization techniques as a counter-argument to show that a fast method to create passwords that are easy to remember, but difficult to guess or crack, exists. This was done to create dissonance by addressing individuals' concerns that strong passwords take too much time to generate and are difficult to remember.

4.2. Instrumentation

Consistent with Siponen and Vance (2010), we operationalized neutralization as a second-order formative construct comprised of first-order reflective constructs for each neutralization technique. This is because several distinct dimensions of neutralization exist (Cromwell and Thurman, 2003) that together describe a different facet of the overall neutralization construct (Jarvis et al., 2003). We adapted aspects from Siponen and Vance (2010) to the context of passwords. We also created new items for the following two constructs: justification by comparison and entitlement. The instrumentation items are reported in Appendix 1.

Instrument validation is reported in Appendix 2, including reliability and construct validity, in terms of the correlation of the latent variable scores and the square root of the average variance extracted (AVE) calculated. These scores were calculated using the partial least squares statistical package SmartPLS (Ringle et al., 2005). As expected, some of the neutralization techniques were highly correlated because they were all different expressions of the same overarching theoretical mechanism: neutralization (Siponen and Vance, 2010). Still, Appendix 2 provides an acceptable pattern of discriminant validity (Gefen and Straub, 2005). We also conducted a multicollinearity test in which we regressed intent on each of the neutralization techniques in the same model. The variance inflation factor (VIF) scores for each neutralization technique were below the threshold of 10 recommended by Hair et al. (1998), indicating a low likelihood of multicollinearity.

4.3. Validating the survey instrument used in the experiment

Given that we adapted previously tested items (Siponen and Vance, 2010) to our context, two preliminary tests were performed to evaluate (1) content validity and (2) factorial validity of the survey instrument (Boudreau et al., 2001). First, to evaluate content

Table 1
Experimental design.

		T ₁		T ₂	T ₃
Group 1	N	O ₁	X ₁	O ₂	O ₃
Group 2	N	O ₁	X ₂	O ₂	O ₃

N = non-equivalent group; T = time; O_i = Observation at time *i*; X₁ = Control treatment; X₂ = experimental treatment.

validity, 14 information security managers and subject-domain experts took the survey and provided feedback. Second, to test factorial validity of the survey instrument, 23 university students completed the survey. Reliability was tested using Cronbach's α , and discriminant and convergent validity was assessed using principal component analysis. After both pretests, items were dropped or revised. This validated instrument was used in the field experiment, which included the pre-test and two post-test surveys, described in the next sections. Please note that the pre-test of the field experiment should not be confused with the validity testing of the survey instrument.

4.4. Main data collection

The experimental sample frame consisted of the 98 employees on the payroll of the UAE office. Participants were recruited as part of management-sponsored training sessions on the company's information security policy, including sick leave, holidays, day-long meetings with customers, and business trips. The training sessions reviewed the organization's information security policies, including principles of secure password selection. The sessions were held in the training room of the organization, just like any other training sessions or meetings at the organization. The educational training material was reviewed by the information security manager, who also saw the issue of bad-password practice as a key information security procedure compliance issue at the company. One of the authors of this study led the 90-minute-long training session. This author was not known to the UAE office employees.

4.5. Experimental design

The experiment followed a nonequivalent group design (NEGD) comprising control and experimental groups and pre- and posttests. Additionally, a second posttest (posttest₂) was administered three weeks after the educational training session to observe any attenuation in effects of the educational training intervention. For group sizes, 21 participants were assigned to the control group, while 66 were assigned to the experimental group. Of those in the experimental group, 62 responded to the pre and post surveys. The design of the experiment is summarized pictorially in Table 1.

We asked the company to assign employees to the groups randomly. A secretary at the company who was assigned to do that informed the authors that some employees already had scheduled meetings during the educational training time. Thus, having the secretary assign employees randomly to the groups would have resulted in a lower participation rate, as well as offer an excuse for some employees not to participate. Given that information security is a weak-link phenomenon (Siponen and Vance, 2014; Willison and Warkentin, 2013), we deemed it important to maximize the participation rate.

As a result, all employees of the organization were invited to participate, but were free to choose which educational training session to attend based on their work schedules. Following this selection approach, 87 out of 98 employees participated. Technically, the participation rate was 88%, but practically, the participation

rate was 92.5% because at least 4 people were on holiday, away on business trips, or sick during the training times.

It also is noteworthy that the employees did not know which sessions were the control and treatment groups. Because we conducted pretests for both groups, we were able to compare differences between the two (Trochim and Donnelly, 2006). No significant differences were found, either in terms of an overall neutralization measure or in terms of measures of individual neutralization techniques. There also was no significant difference in reported use of strong passwords or intent to use strong passwords. Although these results cannot rule out a selection threat, they at least show that no obvious differences existed between groups prior to conducting the experiment.

Both experimental and control groups received the same information security education material on the organization's password policies and the need for strong passwords. Furthermore, both experimental and control groups attended nearly identical information security educational training sessions, except that the experimental group received education addressing each of the neutralization techniques reviewed in the previous section, as well as why these techniques are not justifiable excuses for selecting weak passwords. Thus, the manipulation or treatment was password educational training based on cognitive dissonance theory, which offered counter-arguments for neutralization techniques. The control group did not receive this specific manipulation.

Before the educational training session, participants completed the experimental pretest instrument, which measured neutralization techniques, current use of complex passwords, and intent to use complex passwords in the future. Immediately after the session, participants completed the experimental posttest, consisting of the same instrument taken in the pretest. Thus, it was possible to compare differences in neutralization techniques and intent to use strong passwords both between the experimental groups and within the experimental groups using the pretest and posttest results. The data collection was anonymous. The pretests and posttests were numbered so that they could be connected, and both were given to the employees before the educational training session. This practice was explained to all participants, and they were ensured that their identities could not be determined through their answers, thereby preserving anonymity.

The pretest and posttest instruments were identical for both the experimental and control groups. When the participants came to the educational training sessions, they were asked to fill out the pretest. After the session and before they left the training room, they were asked to fill out the posttest. This procedure applied to both experimental and control groups. By doing this, we endeavored to maximize control (and minimize the effect of extraneous variables), in that the pretests and posttests for both experimental and control groups were filled out under exactly the same circumstances. A second person, who was not the lecturer, administered the distribution and collection of both the pretests and posttests for both groups. Also, the educational training intervention for both groups was provided by the same lecturer to rule out the lecturer's style or characteristics as being a possible influence on results.

5. Analysis

In accordance with our non-equivalent group design, we employed a reliability-corrected analysis of co-variance (ANCOVA) technique to control for the pretest scores of each group (Trochim and Donnelly, 2006). Using this approach, a typical ANCOVA model is created in which the experimental group is entered as a dummy variable, and the pretest score for a variable is entered as a covariate. This approach controls for possible differences between the two groups because they are non-equivalent

Table 2
ANCOVA results for comparison of control and experimental groups.

Hypothesis	F-score	η^2	Supported?
H1a: Educational training that evokes cognitive dissonance will reduce use of the <i>denial-of-responsibility</i> neutralization technique.	3.48*	0.040	Yes
H1b: Educational training that evokes cognitive dissonance will reduce use of the <i>denial-of-injury</i> neutralization technique.	6.99**	0.086	Yes
H1c: Educational training that evokes cognitive dissonance will reduce use of the <i>defense-of-necessity</i> neutralization technique.	4.60*	0.057	Yes
H1d: Educational training that evokes cognitive dissonance will reduce use of the <i>condemnation-of-the-condemners</i> neutralization technique.	4.22*	0.053	Yes
H1e: Educational training that evokes cognitive dissonance will reduce use of the <i>appeal-to-higher-loyalties</i> neutralization technique.	5.08*	0.062	Yes
H1f: Educational training that evokes cognitive dissonance will reduce use of the <i>entitlement</i> neutralization technique.	0.14 n.s.	0.001	No
H1g: Educational training that evokes cognitive dissonance will reduce use of the <i>relative-acceptability</i> neutralization technique.	2.53 n.s.	0.036	No
H1h: Educational training that evokes cognitive dissonance will reduce use of the <i>defense-by-comparison</i> neutralization technique.	0.23 n.s.	0.005	No
H2: Educational training that evokes cognitive dissonance will increase <i>intention to use strong passwords</i> .	7.48**	0.096	Yes

* $p < .05$; ** $p < .01$; n.s. not supported.

(i.e., randomization was not used in group assignment). However, the pretest score is first corrected using the formula $x_{adj} = \bar{x} + r(\bar{x} - x)$, in which x_{adj} is the adjusted pretest value, \bar{x} is the original pretest value, and r is the reliability score, in this case, Cronbach's α (Trochim and Donnelly, 2006). This technique corrects bias in the ANCOVA due to measurement error in the pretest and the initial nonequivalence between groups (Trochim and Donnelly, 2006).

The results in Table 2 show that all but hypotheses H1f (entitlement neutralization), H1g (relative-acceptability neutralization), and H1h (defense by comparison) were supported. Although it is natural to assume that these neutralization techniques were not effective, our experimental design does not allow us to definitively compare the effectiveness of individual neutralization techniques since all were used in the same treatment condition. However, we can conclude that educational training intervention did reduce the use of neutralization techniques overall.¹

An examination of effect sizes for each of the significant hypothesis tests shows an η^2 between 0.040 and 0.096, indicating a small-to-medium and medium-to-large effect sizes, where 0.01, 0.06, and 0.14 correspond to small, medium, and large effect sizes respectively for ANOVA following Cohen (1988). A post-hoc power analysis shows an obtained power between 0.357 and 0.721. While this level of power may not have been sufficiently high to detect effects for three of our nine hypotheses (relating to defense by comparison, relative acceptability, and entitlement), the effect sizes for the remaining six hypotheses were large enough to be detected in our hypothesis tests. Therefore, we conclude that our sample size was low, but adequate for the purposes of this field experiment.

Table 3
Results from posttest and follow-up posttest.

Construct	Pretest mean - Posttest ₂ mean	Posttest ₁ mean - Posttest ₂ mean
Relative acceptability	-0.9 N.S.	-1.7 N.S.
Defense of comparison	-3.4**	0.4 N.S.
Condemn the condemners	-4.4***	-1.0 N.S.
Entitlement	-3.4*	-0.8 N.S.
Denial of injury	-3.7*	0.6 N.S.
Appeal to higher loyalties	-5.4***	-0.6 N.S.
Defense of necessity	-3.7**	0.7 N.S.
Denial of responsibility	-2.8***	-0.3 N.S.
Neutralization	-4.7***	-0.4 N.S.
Current use of strong passwords	3.0***	1.4 N.S.
Intent to use strong passwords in the future	2.3***	0.3 N.S.

Note: *** $p < .001$; ** $p < .01$; * $p < .05$; N.S. non-significant.

5.1. Follow-up posttest

For a more stringent test of the effectiveness of our intervention, we administered a second posttest (denoted posttest₂) three weeks after the first posttest (posttest₁). By allowing time to pass between the intervention and posttest₂, we were able to observe to what extent the effect of the educational training had attenuated. The posttest₂ was identical to posttest₁, except that posttest₂ was administered online, while posttest₁ was paper-based and filled out in person.

Only members of the experimental group were invited to take the online posttest₂, since only this group received the educational training. Of the 63 members of this group, 20 completed posttest₂. To test for the possibility of a nonresponse bias, we compared the first 10 respondents with the last 10 respondents using an independent sample t -test, since it is commonly held that late respondents are a good surrogate for nonrespondents (Armstrong and Overton, 1977). The results of this test showed that there were no significant differences between early and later responders, indicating a low likelihood of nonresponse bias.

We performed the same comparisons as the within-group analysis discussed previously (see Table 3). However, not all respondents to posttest₂ chose to identify themselves, making a link to their previous pretest and posttest₁ responses impossible. For this reason, an independent-sample t -test (rather than a paired-sample t -test) was performed. Table 3 shows the difference in means between the pretest and posttest₂ and between posttest₁ and posttest₂. The differences in means between the pretest and posttest₂ were all significant, indicating that our educational training intervention still demonstrated a significant effect three weeks later. Furthermore, there was no significant difference between the means for posttest₁ and posttest₂, indicating that no significant attenuation in the effect of the educational training occurred after three weeks.

6. Discussion

This paper studied educational training interventions aimed at de-neutralizing neutralization techniques in the context of password security. Using a two-group, quasi-experimental design ($n = 80$), we found that individuals who received our educational training (experimental group) used neutralization techniques substantially less often and had significantly greater intent to use secure passwords than the control group. Next, we highlight two important new contributions. First, our quasi-experiment suggests that an educational training intervention designed to address neutralization techniques is an effective method to decrease and improve individuals' compliance through information security procedures, at least in the context of password selection. While the role of neutralization is recognized as affecting individuals' compliance

¹ We thank an anonymous reviewer for this insight.

with information security procedures (Siponen and Vance, 2010), this is the first study that examined whether an educational training intervention can decrease individuals' use of neutralization techniques.

Second, our results suggest that the effect of educational training interventions can continue beyond the intervention for at least three weeks. Given that previous studies have implemented a posttest right after an intervention, to our understanding, this is the first study that has offered quantitative evidence of individuals' intent and behavior after the education or training intervention.

6.1. Implications for practice

We now highlight six implications for practice based on our findings. Overall, based on our results, we suggest that rather than simply announcing information security policies or educating individuals about the content of these policies, organizations should use carefully designed information security educational training to increase individuals' compliance with information security policies and measure the effect of the educational training. By "carefully designed," we mean educational training should be crafted to justify and explain why individuals should follow the procedures described in the policies. Based on our findings, we recommend the following considerations for practice.

First, the information security educational training programs within organizations should tackle the defense-of-necessity argument by explaining why it is not acceptable to use simple passwords at work, even if the individuals claim they do not have time to come up with complex passwords or have no time to learn complex passwords. A key argument as to why the defense of necessity is not acceptable, other than compliance with relevant information security procedures is part and parcel of the individuals' duties at work, is that increasing the difficulty of guessing passwords is not difficult. In fact, our results suggest that in addition to the aforementioned arguments, information security educational training should include a demonstration and exercise with a discussion on how to select a strong password that is difficult to guess, but easy to remember.

Second, information security educational training needs to address the condemnation-of-condemners argument by explaining that even though some other person may use a simple password, this does not give other individuals the right to use simple passwords. Individuals must be told that if excuses such as "because others do not comply, why should I comply?" are accepted, then no one should need to do anything because we always can find someone who does not do something. In the same vein, if such an argument were accepted, everything becomes acceptable because no matter what the action is, we can always find someone who does not comply with it.

Third, regarding arguments on justification by comparison and denial of injury, individuals need to realize through demonstrations within information security educational training that an easy-to-guess password may cause a serious security breach. Here, we suggest practical demonstrations showing how fast an easy password can be guessed and what kind of damage can be caused when individuals' passwords are stolen.

Fourth, regarding the argument based on an appeal to higher loyalties, holding that it is OK to use simple passwords if it helps get the job done, the trainer needs to emphasize two issues. The first is that selecting a password that is difficult to guess, but easy to remember, is not necessarily time consuming. Second, it should be stressed in the educational training that compliance with relevant information security procedures is an important work duty.

Fifth, as for the argument on denial of responsibility, individuals need to learn that ignorance of the password policy is not professional and that adherence to security procedures, such as the password policy, is part of their work responsibilities. Simultane-

ously, organizations need to ensure that their password policy is properly introduced during mandatory information security educational training. Sixth, regarding entitlement, individuals must be told that they indeed have a right to choose any password—as long as it is difficult to guess.

6.2. Implications for research

We next highlight five implications for research based on our findings. First, future research should study the impact of educational training on other violation types. While our findings provide relatively strong support for training on password practices, future research should study whether such training is successful for increasing individuals' compliance with other types of information security procedures as well.

Second, future research should consider the long-term effects of educational training interventions. Our study used two posttests after the intervention, one right after the intervention and the other three weeks later. While this is more than in recent similar studies (Johnston and Warkentin, 2010; Anderson and Agarwal, 2010; Johnston et al., 2015), which used just one posttest immediately after the intervention, future research should study the effects from educational training interventions in the long term because the ultimate objective of information security training should be long-term security (Siponen and Baskerville, 2018). For this purpose, we call for longitudinal case studies lasting from months to years.

Third, there is a need to examine the effect of different techniques, and to compare the effects of different techniques on individuals' compliance, such as fear appeals (Johnston and Warkentin, 2010) and educational training based on neutralization techniques.

Fourth, while we used self-reports to gauge actual behavior and intent in the sense that they were anonymous (and we used a control group), there is also a need for "objective" measures to gauge actual behavior.

Fifth, research should include online educational training. While our training suggests that face-to-face information security educational training with discussions was effective in de-neutralizing individuals' use of neutralization techniques and increasing their intent to behave, we do not know whether online educational training with less interaction between the trainer and individuals would be equally successful. Hence, future research should study this aspect.

6.3. Limitations of the study

The participants in our study were not randomly assigned to the groups through an independent third party. In our case, if we had done so, it would have resulted in a low rate of participation, as explained earlier. Low participation is problematic because (in the case of low participation) we cannot know whether the results apply to non-participants. To illustrate why this is the case, let us presume that the participation rate for information security educational training in an organization is 30%, and therefore 70% do not participate. In this case, we are left with having to guess whether the 70% who did not participate have any ability or desire to follow information security standards on passwords. In information security, the issue of non-participants is especially important because information security is a "weak link" phenomenon, meaning that the attackers need to find the weakest links (Willison and Warkentin, 2013). In our case, the weakest links are the weakest passwords. It is possible that the weakest passwords belong to those individuals who avoid information security educational training (i.e., non-participants).

To ensure a high participation rate, which in our case was 92.5%, the individuals were free to choose which educational train-

ing session to attend based on their work schedules. Importantly, the individuals—or anyone at the company—did not know which groups were control and treatment groups. Both groups looked the same to the individuals. As a result, we see no selection biases involved in our selection approach. It is important to point out that the objective of the random assignment was to ensure that the groups are identical and that scholars did not select the participants for each group. In our case, with respect to the latter, we had no influence on the allocation of participants to groups because the participants self-selected the groups based on their schedules. For the former, there were no significant differences between pretest results across the experimental and control groups. Nonetheless, we acknowledge that the nonequivalent groups in this study are a limitation, and we call for future research to examine neutralization techniques using a random assignment design.

Finally, our field experiment examined intent to create strong passwords, rather than actual password-creation behavior. In this sense, our paper resembles many other studies on the topic of information security in organizations (Cram et al., 2017). Nevertheless, future research is needed to study actual password behavior objectively (Crossler et al., 2013).

7. Conclusion

Previous research suggests that individuals' compliance with a password security policy is a key concern in practice. Also, extant research has pointed out that the neutralization technique, which includes types of rationalizations or excuses, explains individuals' noncompliance with information security procedures. However, what is not known in previous information security research is whether these neutralizations can be changed by an information security educational training intervention.

We examined this question empirically by using a quasi-experimental design ($n=80$). In this design, we found that individuals who received our educational training intervention (the experimental group) exhibited substantially less frequent use of neutralization techniques and exhibited significantly stronger intent to use secure passwords. Additionally, a follow-up measurement 3 weeks after the educational training session showed that the experimental educational training retained its effectiveness, i.e., the experimental group exhibited a substantially lower tendency to use neutralization techniques and greater intent to use strong passwords in the future. Implications for practice suggest that educational training that counters the arguments based on neutralization techniques is effective in improving individuals' compliance with password procedures. Five directions for future research were outlined earlier based on our findings.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The Finnish Funding Agency for Innovation (Business Finland) and several companies funded this study.

Appendix 1. Instrumentation for measuring neutralization techniques, current (actual) use of passwords and intention to use. Constructs are listed in an alphabetical order

Construct	Code	Item	Source
Appeal to higher loyalties	loyal1	It is all right to use simple passwords at work if you get your work done.	Siponen and Vance (2010)
	loyal2	It is OK to use simple passwords if you carrying out an important job by your manager.	New item based on Siponen and Vance (2010)
	loyal3	It is all right to use simple passwords at work if it helps to get the job done.	Siponen and Vance (2010)
	loyal4	It is all right to use simple passwords at work if you complete the task given by management.	Siponen and Vance (2010)
Condemnation of the condemners	condemn1	It is okay to use simple passwords at work because everyone uses simple passwords at times.	New item based on McGregor (2008)
	condemn2	It is okay to use simple passwords at work because this is what everyone at work does.	New item based on McGregor (2008)
	condemn3	It is okay to use simple passwords at work because even the managers use simple passwords.	New item based on McGregor (2008)
Current behavior	current1	I currently use complex passwords for work systems.	New item
	current2	I presently use complex passwords for work systems.	New item
Defense of necessity	necess1	It is OK to use simple passwords at work if you do not have time to learn complex passwords.	New item based on Siponen and Vance (2010)
	necess2	It is OK to use simple passwords at work if you do not have time come up with complex passwords.	New item based on Siponen and Vance (2010)
	necess3	It is OK to use simple passwords at work if it is too difficult to remember complex passwords.	New item based on Siponen and Vance (2010)
Denial of Injury	injury1	It is OK to use simple passwords at work if no harm is done.	Siponen and Vance (2010)
	injury2	It is OK to use simple passwords at work if no damage is done to the company.	Siponen and Vance (2010)
	injury3	It is OK to use simple passwords at work if no one gets hurt.	Siponen and Vance (2010)
Denial of Responsibility	response1	It is OK to use simple passwords at work if you aren't sure what the company's password guidelines are.	Siponen and Vance (2010)
	response3	It is OK to use simple passwords at work if the password guidelines are not advertised.	Siponen and Vance (2010)
Entitlement	entitlement1	I have the right to use simple passwords at work.	New item based on McGregor (2008)
	entitlement2	Employees should have the right to use any password at work they choose.	New item based on McGregor (2008)
	entitlement3	I should be free to choose any password I want.	New item based on McGregor (2008)

(continued on next page)

(continued)

Construct	Code	Item	Source
Intention	intention1	I intend to use complex passwords for work systems.	Venkatesh et al. (2013)
	intention2	I plan to use complex passwords for work systems.	Venkatesh et al. (2013)
Justification by comparison	compare1	The use of simple passwords at work is not a big deal compared with other things.	New item based on McGregor (2008), Cromwell and Thurman (2003)
	compare2	The use of simple passwords at work is not as bad as being lazy on the job.	New item based on McGregor (2008), Cromwell and Thurman (2003)
	compare3	Using simple passwords at work is not as bad as wasting time.	New item based on McGregor (2008), Cromwell and Thurman (2003)
Relative Acceptability	relative1	Some employees use much simpler passwords than I do.	New item based on Henry and Eaton (1999)
	relative2	There are some employees whose passwords are much simpler than mine.	New item based on Henry and Eaton (1999)
	relative3	Compared to others, my passwords are not too simple.	New item based on Henry and Eaton (1999)

Appendix 2. Instrument Validation in terms of reliability and correlation of the latent variable scores with the square root of average variance extracted (AVE) on the diagonal

Construct	CR	α	1	2	3	4	5	6	7	8	9
Intention (1)	0.92	0.82	0.92								
Accept (2)	0.86	0.75	0.28	0.82							
Compare (3)	0.84	0.63	-0.41	0.10	0.85						
Condemn (4)	0.97	0.95	-0.62	-0.02	0.56	0.97					
Entitle (5)	0.72	0.66	-0.45	-0.01	0.45	0.51	0.70				
Injury (6)	0.97	0.96	-0.52	-0.10	0.53	0.75	0.50	0.96			
Loyal (7)	0.96	0.92	-0.61	-0.03	0.64	0.86	0.60	0.78	0.96		
Necessity (8)	0.94	0.91	-0.69	-0.15	0.63	0.84	0.55	0.75	0.86	0.92	
Response (9)	0.92	0.83	-0.45	-0.09	0.53	0.75	0.48	0.78	0.74	0.73	0.92

CR = Composite reliability; α = Cronbach's alpha

References

- Anderson, C.L., Agarwal, R., 2010. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Q.* 34 (3), 613–643.
- Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R., 2013. Don't make excuses! discouraging neutralization to reduce IT policy violation. *Comput. Secur.* 39 (Part B), 145–159.
- Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R., 2018. Don't even think about it! the effects of antineutralization, informational, and normative communication on information security compliance. *J. Assoc. Inf. Syst.* 19, 689–715.
- Bouchard, T.J., 1976. Field research methods: interviewing, questionnaires, participant observation, systematic observation, unobtrusive measures. *Handbook Industr. Organ. Psychol.* 1, 363.
- Boudreau, M.-C., Gefen, D., Straub, D.W., 2001. Validation in information systems research: a state-of-the-art assessment. *Mis Q.* 1–16.
- Bushway, S.D., Thornberry, T.P., Krohn, M.D., 2003. Desistance as a developmental process: a comparison of static and dynamic approaches. *J. Quant. Criminol.* 19 (2), 129–153.
- Byers, B., Crider, B.W., Biggers, G.K., 1999. Bias crime motivation a study of hate crime and offender neutralization techniques used against the Amish. *J. Contemp. Crim. Justice* 15 (1), 78–96.
- Clark, R., 2003. Building Expertise: Cognitive Methods for Training and Performance Development. Washington DC, International Society for Performance Improvement.
- Coleman, J., 1994. Neutralization Theory: An Empirical Application and Assessment PhD Thesis. Oklahoma State University.
- Collins, M.D., 1994. Neutralization theory: An empirical application and assessment PhD Thesis. Oklahoma State University Stillwater.
- Consolvo, S., McDonald, D.W., Landay, J.A., 2009. Theory-driven design strategies for technologies that support behavior change in everyday life. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, pp. 405–414.
- Cromwell, P., Thurman, Q., 2003. The devil made me do it: use of neutralizations by shoplifters. *Deviant Behav.* 24 (6), 535–550.
- Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R., 2013. Future directions for behavioral information security research. *Comput. Secur.* 32 (1), 90–101.
- D'arcy, J., Hovav, A., Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf. Syst. Res.* 20 (1), 79–98.
- Dechawatanapaisa, D., Siengthai, S., 2006. The impact of cognitive dissonance on learning work behavior. *J. Workplace Learn.* 18 (1), 42–54.
- Dennis, A.R., Valacich, J.S., 2001. Conducting experimental research in information systems. *Commun. Assoc. Inf. Syst.* 7 (1), 5.
- Driscoll M.P. and Driscoll M.P. (2005) Psychology of learning for instruction.
- Eliason, S.L., 2003. Illegal hunting and angling: the neutralization of wildlife law violations. *Soc. Animals* 11 (3), 225–243.
- Eliason, S.L., Dodder, R.A., 1999. Techniques of neutralization used by deer poachers in the western united states: a research note. *Deviant Behav.* 20 (3), 233–252.
- Elliot, A.J., Devine, P.G., 1994. On the motivational nature of cognitive dissonance: dissonance as psychological discomfort. *J. Pers. Soc. Psychol.* 67 (3), 382.
- Festinger, L., 1957. A Theory of Cognitive Dissonance. Stanford University Press, Stanford.
- Florêncio, D., Herley, C., 2010. Where do security policies come from? In: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, p. 10.
- Florêncio, D., Herley, C., van Oorshot, P., 2016. Pushing on string: the 'Don't care' region of password strength. *Commun. ACM* 59 (11), 66–74.
- Gardner, H., 2006. Changing minds: the Art and Science of Changing Our Own and Other People's Minds. Harvard Business Review Press.
- Geer, D., 2005. Malicious bots threaten network security. *IEEE Computer* 38 (1), 18–20.
- Greenwald, A.G., 1968. Cognitive learning, cognitive response to persuasion, and attitude change. *Psychol. Found. Attitudes* 147–170.
- Harrington, S.J., 1996. The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS Q.* 257–278.
- Henry, S., Eaton, R., 1999. Degrees of Deviance: Student Accounts of Their Deviant Behavior. Sheffield Publishing, Salem.
- Herath, T., Rao, H.R., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* 18 (2), 106–125.
- Herley, C., 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In: *Proceedings of the 2009 workshop on New security paradigms workshop*. ACM, pp. 133–144.
- Hollinger, R.C., 1991. Neutralizing in the workplace: an empirical analysis of property theft and production deviance. *Deviant Behav.* 12 (2), 169–202.
- Jarvis, C.B., Mackenzie, S.B., Podsakoff, P.M., 2003. A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *J. Consum. Res.* 30 (2), 199–218.
- Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. *MIS Q.* 34 (3), 549–A544.
- Johnston, A.C., Warkentin, M., Siponen, M., 2015. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *Mis Q.* 39 (1), 113–134.

- Kaptein, M., Van Helvoort, M., 2018. A model of neutralization techniques. *Deviant Behav.* 1–26.
- Karjalainen, M., Siponen, M., 2011. Toward a new meta-theory for designing information systems (IS) security training approaches. *J. Assoc. Inf. Syst.* 12 (8), 518–555.
- Karjalainen, M., Siponen, M., Sarker, S., 2019. Towards a theory of information systems security behaviors of organizational employees: a dialectical perspective. *Inf. Syst. Res.* 30 (2), 351–710.
- Keith, M., Shao, B., Steinbart, P., 2009. A behavioral analysis of passphrase design and effectiveness. *J. Assoc. Inf. Syst.* 10 (2), 2.
- Lanier, M.M., Henry, S., 1998. *Essential Criminology*. Westview, Boulder, CO.
- Lanier, M., Henry, S., 2004. *Essential Criminology*. Westview Press, Boulder.
- Lim, V.K., 2002. The it way of loafing on the job: cyberloafing, neutralizing and organizational justice. *J. Organ. Behav.* 23 (5), 675–694.
- Loeber, R., Le Blanc, M., 1990. Toward a developmental criminology. *Crime Justice* 375–473.
- Ma, L., Ferguson, J., Roper, M., Ross, I., Wood, M., 2009. Improving the mental models held by novice programmers using cognitive conflict and jeliot visualisations. In: *ACM SIGCSE Bulletin*. ACM, pp. 166–170.
- Maruna, S., Copes, H., 2005. What have we learned from five decades of neutralization research? *Crime Justice* 221–320.
- Mcguire, W.J., 1968. Personality and attitude change: an information-processing theory. *Psychol. Found. Attitudes* 171–196.
- McMillan R (2016). Yahoo Hackers Were Criminals Rather Than State-Sponsored, Security Firm Says, *Wall Street Journal* (<https://www.wsj.com/articles/yahoo-hackers-were-criminals-rather-than-statesponsored-security-firm-says-1475081065>, accessed 10/3/2019).
- Minor, W.W., 1981. Techniques of neutralization: a reconceptualization and empirical examination. *J. Res. Crime Delinquency* 18 (2), 295–318.
- Morris, R., Higgins, G., 2009. Neutralizing potential and self-reported digital piracy. *Crim. Justice Rev.* 34, 173–195.
- Myrri, L., Siponen, M., Pahlila, S., Vartiainen, T., Vance, A., 2009. What levels of moral reasoning and values explain adherence to information security rules? an empirical study. *Eur. J. Inf. Syst.* 18 (2), 126–139.
- Neighbour, R., 1992. *The Inner apprentice: an Awareness-Central Approach to Vocationaltraining For General Practice*. Kluwer, Lancaster.
- Ng, B.-Y., Kankanhalli, A., Xu, Y., 2009. Studying users' computer security behavior: a health belief perspective. *Decis. Support Syst.* 46 (4), 815–825.
- Pahlila, S., Siponen, M., Mahmood, A., 2007. Employees' behavior towards is security policy compliance. In: *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, p. 156b–156b.
- Perloth, N., 2017. All 3 Billion Yahoo Accounts Were Affected by 2013 Attack, *The New York Times* (<https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html>, accessed 10/3/2019).
- Pershing, J.L., 2003. To snitch or not to snitch? Applying the concept of neutralization techniques to the enforcement of occupational misconduct. *Sociol. Perspect.* 46 (2), 149–178.
- Petty, R.E., Cacioppo, J.T., 1981. Attitudes and persuasion: Classic and contemporary approaches. Brown, Dubuque.
- Petty, R.E., Cacioppo, J.T., 1986. The elaboration likelihood model of persuasion. In: Berkowitz, L. (Ed.), *Advances in experimental social psychology* 19, pp. 123–205.
- Picolet, J., 2017. *Hash Crack: Password Cracking Manual (v2.0)*. CreateSpace, Seattle, Washington.
- Piquero, A.R., Macdonald, J., Dobrin, A., Daigle, L.E., Cullen, F.T., 2005. Self-control, violent offending, and homicide victimization: assessing the general theory of crime. *J. Quant. Criminol.* 21 (1), 55–71.
- Potter, B., 2010. Common sense for your network. *IT Prof.* 12 (3), 11–13.
- Priest, T.B., McGrath III, J.H., 1970. Techniques of neutralization: young adult marijuana smokers. *Criminology* 8, 185.
- Puhakainen, P., Siponen, M., 2010. Improving employees' compliance through information systems security training: an action research study. *Mis Q.* 34 (4), 757–778.
- Renaud, K., de Angeli, A., 2009. Visual passwords: cure-all or snake-oil? *Commun. ACM* 52 (12), 135–140.
- Rogers, J.W., Buffalo, M., 1974. Neutralization techniques: toward a simplified measurement scale. *Pac. Sociol. Rev.* 313–331.
- Schneier, B., 2000. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons Inc, New York, pp. 100–115 ISBN: 0-471-25311-1 4.
- Silic, M., Barlow, J.B., Back, A., 2017. A new perspective on neutralization and deterrence: predicting shadow IT usage. *Inf. Manag.* 54 (8), 1023–1037.
- Siponen, M., 2006. Six design theories for IS security policies and guidelines. *J. Assoc. Inf. Syst.* 7 (1), 19.
- Siponen, M., Pahlila, S., Mahmood, A., 2007. Employees' adherence to information security policies: an empirical study. In: *New Approaches for security, Privacy and Trust in Complex Environments*. Springer, pp. 133–144.
- Siponen, M., Pahlila, S., Mahmood, M.A., 2010. Compliance with information security policies: an empirical investigation. *Computer* 43 (2), 64–71.
- Siponen, M., Vance, A., 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Q.* 34 (3), 487–502.
- Siponen, M., Vance, A., 2014. Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *Eur. J. Inf. Syst.* 23 (3), 289–305.
- Siponen, M., Vance, A., Willison, R., 2012. New insights into the problem of software piracy: the effects of neutralization, shame, and moral beliefs. *Inf. Manag.* 49 (7), 334–341.
- Siponen, M., Baskerville, R., 2018. Intervention effect rates as a path to research relevance: information systems security example. *J. Assoc. Inf. Syst.* 19 (4), 247–265.
- Straub, D., Carlson, P.J., Jones, E.H., 1993. Detering cheating by student programmers: a field experiment in computer security. *J. Manag. Syst.* 5 (1), 33–48.
- Straub, D.W., 1989. *Detering computer abuse: The effectiveness of deterrent countermeasures in the computer security environment* PhD Thesis.
- Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. *Mis Q.* 441–469.
- Sykes, G.M., Matza, D., 1957. Techniques of neutralization: a theory of delinquency. *Am. Sociol. Rev.* 22 (6), 664–670.
- Tatli, E., 2015. Cracking more password hashes with patterns. *IEEE Trans. Inf. Forensics Secur.* 10 (8), 1656–1665.
- TeamsID (2015) Announcing our worst passwords of 2015. Retrieved January 18, 2016, 2016, from <https://www.teamsid.com/worst-passwords-2015/>.
- Trochim, W., Donnelly, J., 2006. *The Research Methods Knowledge Base*. Atomic Dog, Cincinnati, OH.
- Velicer, W.F., Prochaska, J.O., 2008. Stage and non-stage theories of behavior and behavior change: a comment on schwarzer. *Appl. Psychol.* 57 (1), 75–83.
- Venkatesh, V., Brown, S.A., Bala, H., 2013. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MISQ.* 37 (1), 21–54.
- Verizon (2017). 2017 Data Breach Investigation Report: Understand Your Cybersecurity Threats (https://enterprise.verizon.com/resources/reports/2017_dbir.pdf, accessed 10/3/2019).
- Willison, R., 2006. Understanding the offender/environment dynamic for computer crimes. *Inf. Technol. People* 19 (2), 170–186.
- Willison, R., Warkentin, M., 2013. Beyond deterrence: an expanded view of employee computer abuse. *MIS Q.* 37 (1), 1–20.
- Wu, L., Ahn, H.A., 2010. Making sense of conflicting health information: an exploratory study. *Proc. Am. Soc. Inf. Sci. Technol.* 47 (1), 1–9.
- Zhang, J., Luo, X., Akkaladevi, S., Ziegelmayer, J., 2009. Improving multiple-password recall: an empirical study. *Eur. J. Inf. Syst.* 18 (2), 165–176.

Mikko Siponen is a professor in the Department of Computer Science and Information Systems at the University of Jyväskylä. He holds a Ph.D. in philosophy from the University of Joensuu, Finland, and a Ph.D. in Information Systems from the University of Oulu, Finland. His research interests include IS security, IS development, computer ethics, and philosophical aspects of IS. Mikko has published 58 articles in journals such as *MIS Quarterly*, *Journal of the Association for Information Systems*, *Information & Management*, *European Journal of Information Systems*, *Information & Organization*, *Communications of the ACM*, *IEEE Computer*, *IEEE IT Professional*, and others. He has received over 10 million EUR of research funding from corporations and numerous funding bodies. He has been a track chair for the International Conference on Information Systems and the European Conference on Information Systems three times. His other editorial board experiences include positions with *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Information & Management*, and *Communications of the Association for Information Systems*. He has more than 8300 google scholar citations.

Petri Puhakainen is an information security consult. He holds a Ph.D. in Information Processing Science from the University of Oulu, Finland, and the degrees of L.Sc. (Tech.) and M.Sc. (Tech.) in Computer Science from the Helsinki University of Technology. His research interests include IS security behavior, IS security awareness and training, and IS security maturity. Dr... Puhakainen has been involved in the field of information systems and IS security for over 25 years as a security director, senior consultant, teacher, and researcher.

Anthony Vance is an Associate Professor of Information Systems in the Marriott School of Management of Brigham Young University. He has earned Ph.D. degrees in Information Systems from Georgia State University, USA; the University of Paris—Dauphine, France; and the University of Oulu, Finland. He received a B.S. in IS and Masters of Information Systems Management (MISM) from Brigham Young University, during which he was also enrolled in the IS Ph.D. preparation program. He currently is an associate editor at *MIS Quarterly* and serves on the editorial board of the *Journal of the Association for Information Systems*. His previous experience includes working as a visiting research professor in the Information Systems Security Research Center at the University of Oulu. He also worked as an information security consultant and fraud analyst for Deloitte. His work is published in outlets such as *MIS Quarterly*, *Journal of Management Information Systems*, *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Journal of the American Society for Information Science and Technology*, and *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI)*. His research focuses on behavioral and neuroscience applications to information security.