JYX JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

This is a self-archived version of an original article. This version may differ from the original in pagination and typographic details.

Author(s): Siponen, Mikko; Puhakainen, Petri; Vance, Anthony

Title: Can Individuals' Neutralization Techniques Be Overcome? : A Field Experiment on Password Policy

Year: 2020

Version: Accepted version (Final draft)

Copyright: © 2019 Elsevier Ltd.

Rights: CC BY-NC-ND 4.0

Rights url: https://creativecommons.org/licenses/by-nc-nd/4.0/

Please cite the original version:

Siponen, M., Puhakainen, P., & Vance, A. (2020). Can Individuals' Neutralization Techniques Be Overcome? : A Field Experiment on Password Policy. Computers and Security, 88, Article 101617. https://doi.org/10.1016/j.cose.2019.101617

Journal Pre-proof

Can Individuals' Neutralization Techniques Be Overcome? A Field Experiment on Password Policy

Mikko Siponen , Petri Puhakainen , Anthony Vance

PII: S0167-4048(19)30164-6
DOI: https://doi.org/10.1016/j.cose.2019.101617
Reference: COSE 101617

To appear in: *Computers & Security*

Received date: 3 January 2017
Revised date: 26 December 2018
Accepted date: 5 March 2019

Please cite this article as: Mikko Siponen , Petri Puhakainen , Anthony Vance , Can Individuals' Neutralization Techniques Be Overcome? A Field Experiment on Password Policy, *Computers & Security* (2019), doi: https://doi.org/10.1016/j.cose.2019.101617

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2019 Published by Elsevier Ltd.

Can Individuals' Neutralization Techniques Be Overcome? A Field Experiment on Password Policy

MIKKO SIPONEN

UNIVERSITY OF JYVASKYLA, FACULTY OF INFORMATION TECHNOLOGY,

P.O. BOX 35, FI-40014 UNIVERSITY OF JYVASKYLA, FINLAND.

MIKKO.T.SIPONEN@JYU.FI<MAILTO:MIKKO.T.SIPONEN@JYU.FI>

PETRI PUHAKAINEN

PRIME MINISTER'S OFFICE

PETRI.PUHAKAINEN@VNK.FI<MAILTO:PETRI.PUHAKAINEN@VNK.FI>

ANTHONY VANCE

TEMPLE UNIVERSITY

ANTHONY@VANCE.NAME<MAILTO:ANTHONY@VANCE.NAME>

LÄHETETTY IPHONESTA

Journal Pre-proof

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.

Keywords: Information security policy, passwords, neutralization, information security.

Journal Pre-proof

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 & De Angeli, 2009), passwords remain by far the dominant means of authentication (Florêncio & 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 (Thomas et al., 2017; Florêncio & 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; Perlroth, 2017). Unsurprisingly, an estimated 81 percent of organizational data breaches are facilitated by weak or stolen passwords (Verizon 2017).

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 & 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., 2010; 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 & van Helvoort, 2018; Sykes & 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 & 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 & 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 & 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 & Matza, 1957). If this is the case, can we overcome

Journal Pre-proof

neutralizations easily merely by making people feel guilty (Sykes & Matza, 1957)? Plus, feeling guilt is precisely the reason why neutralizations were introduced in the first place (Sykes & Matza, 1957). Another important consideration is that some neutralization techniques can indicate criminal activity (Maruna & 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 & 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 three weeks after the experiment found that members of the experimental 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, BEHAVIORIAL CHANGE, AND THE RESEARCH GAP

In this section, following research in criminology and health behavior (Bushway et al., 2003; Loeber & Le Blanc, 1990; Velicer & 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.

Journal Pre-proof

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 & Rao, 2009; Johnston & Warkentin, 2010; Ng et al., 2009; Pahnila et al., 2007; Siponen et al., 2007; Siponen et al., 2010), criminology (D'Arcy et al., 2009; Siponen & Vance, 2010), and moral psychology (Myyry 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 & 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 & Prochaska, 2008, p. 77). In criminology, it is noted that "we know very little about changes in individuals' rates of offending" (Loeber & 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 Unsecure Behavior to Secure Behavior

To examine change, IS scholars have tested interventions through educational training programs (e.g., Puhakainen & Siponen, 2010; Straub & Welke, 1998) or messages such as fear appeals (e.g., Anderson & Agarwal, 2010; Johnston & 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

Journal Pre-proof

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 & Agarwal, 2010; Barlow et al., 2013; Johnston & 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

Journal Pre-proof

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 & 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 unsecure 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 & 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 & 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 (Sykes & 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 (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 (Henry and Eaton 1999; Collins, 1994; Cromwell & Thurman, 2003; Minor, 1981) have been applied in several contexts, such as deer poaching (Eliason & Dodder, 1999), hate crimes (Byers et al., 1999), rule-breaking in military environments (Pershing, 2003), drug use (Priest & 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 & Buffalo, 1974; Sykes & Matza, 1957). A deviant who applies denial of responsibility views himself or herself as a billiard ball being helplessly propelled through different situations (Sykes & Matza, 1957). Hence, the person rationalizes

Journal Pre-proof

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 & 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 & Matza, 1957). For example, potential car thieves may regard auto theft as “just borrowing,” which does not hurt anyone (Sykes & 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 & 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, Eliason 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 & 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.,1999). For example, one might break a law because the law is unreasonable (Siponen & Vance, 2010). Eliason 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 & Vance, 2010).

3.1.5 Appeal to Higher Loyalties

Journal Pre-proof

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 & 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 & Siponen, 2010; Siponen, 2006; Siponen & 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 (2014) 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 & Driscoll, 2005). Educational training interventions have long been a recognized means of improving individuals' security behavior in information security (Perry 1985; Straub, 1989; Straub & Welke, 1998). Effective educational training requires the use of proper methods for designing and delivering the training

Journal Pre-proof

(Puhakainen & 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.

Journal Pre-proof

3.3 Educational Training and Hypotheses

information security education and training has long been a recognized means of improving individuals' security behavior (Perry 1985; Straub, 1989; Straub & Welke, 1998). The use of effective training for this purpose requires the use of a proper learning method (Puhakainen & 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 & 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 emphasizes critical reflection of learners' own knowledge and interpretive and conversational forms of evaluation (Karjalainen & Siponen, 2011). Educational training approaches based on constructivism are viewed as preferred approaches for educating and training white-collar individuals in organizations (Karjalainen & Siponen, 2011; Puhakainen & 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

Journal Pre-proof

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 & 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 unsecure 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

Journal Pre-proof

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 & 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 unsecure—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.

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 & 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

Journal Pre-proof

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 between 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., Cacioppo et al.,1986; Petty et al., 1981; Puhakainen & 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

Journal Pre-proof

(Cromwell & 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 & 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 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

Journal Pre-proof

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 ($posttest_2$) 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.

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*; X_1 = Control treatment; X_2 = experimental treatment

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 & Vance, 2014; Willison & 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 four 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 & 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, administrated 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.

Journal Pre-proof

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 & 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 (i.e., randomization was not used in group assignment). However, the pretest score is first corrected using the formula $x_{adj} = \bar{x} + r(x - \bar{x})$, 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 & Donnelly, 2006). This technique corrects bias in the ANCOVA due to measurement error in the pretest and the initial nonequivalence between groups (Trochim & 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].

Journal Pre-proof

[1] We thank an anonymous reviewer for this insight.

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 *denial-of-responsibility* neutralization technique.	3.48*	.040	Yes
H1b: Educational training that evokes cognitive dissonance will reduce use of the *denial-of-injury* neutralization technique.	6.99**	.086	Yes
H1c: Educational training that evokes cognitive dissonance will reduce use of the *defense-of-necessity* neutralization technique.	4.60*	.057	Yes
H1d: Educational training that evokes cognitive dissonance will reduce use of the *condemnation-of-the-condemners* neutralization technique.	4.22*	.053	Yes
H1e: Educational training that evokes cognitive dissonance will reduce use of the *appeal-to-higher-loyalties* neutralization technique.	5.08*	.062	Yes
H1f: Educational training that evokes cognitive dissonance will reduce use of the *entitlement* neutralization technique.	.14 n.s.	.001	No
H1g: Educational training that evokes cognitive dissonance will reduce use of the *relative-acceptability* neutralization technique.	2.53 n.s.	.036	No
H1h: Educational training that evokes cognitive dissonance will reduce use of the *defense-by-comparison* neutralization technique.	0.23 n.s.	.005	No
H2: Educational training that evokes cognitive dissonance will increase *intention to use strong passwords*.	7.48**	.096	Yes
* $p < .05$; ** $p < .01$; n.s. not supported			

An examination of effect sizes for each of the significant hypothesis tests shows an η^2 between .040 and .096, indicating a small-to-medium and medium-to-large effect sizes, where .01, .06, and .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 .357 and .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.

Journal Pre-proof

5.1 Follow-up Posttest

For a more stringent test of the effectiveness of our intervention, we administered a second posttest (denoted $posttest_2$) three weeks after the first posttest ($posttest_1$). By allowing time to pass between the intervention and $posttest_2$, we were able to observe to what extent the effect of the educational training had attenuated. The $posttest_2$ was identical to $posttest_1$, except that $posttest_2$ was administered online, while $posttest_1$ was paper-based and filled out in person.

Only members of the experimental group were invited to take the online $posttest_2$, since only this group received the educational training. Of the 63 members of this group, 20 completed $posttest_2$. 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 $posttest_2$ chose to identify themselves, making a link to their previous pretest and $posttest_1$ 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 $posttest_2$ and between $posttest_1$ and $posttest_2$. The differences in means between the pretest and $posttest_2$ 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 $posttest_1$ and $posttest_2$, indicating that no significant attenuation in the effect of the educational training occurred after three weeks.

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

Journal Pre-proof

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 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

Journal Pre-proof

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. Simultaneously, 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.

Journal Pre-proof

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 & Warkentin, 2010; Anderson and Agarwal, 2010; Jonhnston 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 & 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 & 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 & 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).

Journal Pre-proof

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

Journal Pre-proof

compliance with password procedures. Five directions for future research were outlined earlier based on our findings.

ACKNOWLEDGEMENTS

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

REFERENCES

ANDERSON CL and AGARWAL R (2010) Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly 34*(3), 613-643.

BARLOW JB, WARKENTIN M, ORMOND D and DENNIS AR (2013) Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security 39, Part B*, 145-159.

BARLOW JB, WARKENTIN M, ORMOND D and DENNIS AR (2018) Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems 19*, 689-715.

BOUCHARD TJ (1976) Field research methods: Interviewing, questionnaires, participant observation, systematic observation, unobtrusive measures. *Handbook of industrial and organizational psychology 1*, 363.

BOUDREAU M-C, GEFEN D and STRAUB DW (2001) Validation in information systems research: a state-of-the-art assessment. *Mis Quarterly*, 1-16.

BUSHWAY SD, THORNBERRY TP and KROHN MD (2003) Desistance as a developmental process: A comparison of static and dynamic approaches. *Journal of Quantitative Criminology 19*(2), 129-153.

BYERS B, CRIDER BW and BIGGERS GK (1999) Bias Crime Motivation A Study of Hate Crime and Offender Neutralization Techniques Used Against the Amish. *Journal of Contemporary Criminal Justice 15*(1), 78-96.

COLEMAN J (1994) *Neutralization Theory: An Empirical Application and Assessment*. PhD Thesis, Oklahoma State University.

COLLINS MD (1994) *Neutralization theory: An empirical application and assessment*. PhD Thesis, Oklahoma State University Stillwater.

CONSOLVO S, MCDONALD DW and LANDAY JA (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*, pp 405-414, ACM.

CROMWELL P and THURMAN Q (2003) The devil made me do it: Use of neutralizations by shoplifters. *Deviant Behavior 24*(6), 535-550.

D'ARCY J, HOVAV A and GALLETTA D (2009) User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research 20*(1), 79-98.

DECHAWATANAPAISAL D and SIENGTHAI S (2006) The impact of cognitive dissonance on learning work behavior. *Journal of Workplace Learning 18*(1), 42-54.

DENNIS AR and VALACICH JS (2001) Conducting experimental research in information systems. *Communications of the association for information systems 7*(1), 5.

DRISCOLL MP and DRISCOLL MP (2005) Psychology of learning for instruction.

Journal Pre-proof

ELIASON SL (2003) Illegal Hunting and Angling: The Neutralization of Wildlife Law Violations. *Society & Animals 11*(3), 225-243.
ELIASON SL and DODDER RA (1999) Techniques of neutralization used by deer poachers in the western United States: A research note. *Deviant Behavior 20*(3), 233-252.
ELLIOT AJ and DEVINE PG (1994) On the motivational nature of cognitive dissonance: Dissonance as psychological discomfort. *Journal of personality and social psychology 67*(3), 382.
FESTINGER L (1957) *A Theory of Cognitive Dissonance*. Stanford University Press, Stanford.
FLORÊNCIO D and HERLEY C (2010) Where do security policies come from? In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, p 10, ACM.
FLORÊNCIO D, HERLEY C and VAN OORSHOT P (2016) Pushing on String: The 'Don't Care' Region of Password Strength. *Communications of the 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.
GREENWALD AG (1968) Cognitive learning, cognitive response to persuasion, and attitude change. *Psychological foundations of attitudes*, 147-170.
HARRINGTON SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. *MIS quarterly*, 257-278.
HERATH T and RAO HR (2009) Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems 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*, pp 133-144, ACM.
HOLLINGER RC (1991) Neutralizing in the workplace: An empirical analysis of property theft and production deviance. *Deviant Behavior 12*(2), 169-202.
JARVIS CB, MACKENZIE SB and PODSAKOFF PM (2003) A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of consumer research 30*(2), 199-218.
JOHNSTON AC and WARKENTIN M (2010) Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly 34*(3), 549-A544.
JOHNSTON AC, WARKENTIN M and SIPONEN M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *Mis Quarterly 39*(1), 113-134.
KAPTEIN M and VAN HELVOORT M (2018) A Model of Neutralization Techniques. *Deviant Behavior*, 1-26.
KARJALAINEN M and SIPONEN M (2011) Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems 12*(8), 518-555.
KEITH M, SHAO B and STEINBART P (2009) A behavioral analysis of passphrase design and effectiveness. *Journal of the Association for Information Systems 10*(2), 2.
LANIER MM and HENRY S (1998) *Essential Criminology*. Westview, Boulder, CO.
LANIER MM, HENRY S and DESIRE'JM A (2014) *Essential criminology*. Perseus Books Group.
LIM VK (2002) The IT way of loafing on the job: cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior 23*(5), 675-694.
LOEBER R and LE BLANC M (1990) Toward a developmental criminology. *Crime and justice*, 375-473.
MA L, FERGUSON J, ROPER M, ROSS I and WOOD M (2009) Improving the mental models held by novice programmers using cognitive conflict and Jeliot visualisations. In *ACM SIGCSE Bulletin*, pp 166-170, ACM.

Journal Pre-proof

MARUNA S and COPES H (2005) What have we learned from five decades of neutralization research? *Crime and justice*, 221-320.
MCGUIRE WJ (1968) Personality and attitude change: An information-processing theory. *Psychological foundations of attitudes*, 171-196.
MINOR WW (1981) Techniques of Neutralization: a Reconceptualization and Empirical Examination. *Journal of Research in Crime and Delinquency 18*(2), 295-318.
MORRIS R and HIGGINS G (2009) Neutralizing Potential and Self-Reported Digital Piracy. *Criminal Justice Review 34*, 173-195.
MYYRY L, SIPONEN M, PAHNILA S, VARTIAINEN T and VANCE A (2009) What levels of moral reasoning and values explain adherence to information security rules? an empirical study. *European Journal of Information Systems 18*(2), 126-139.
NEIGHBOUR R (1992) The inner apprentice: an awareness-central approach to vocationaltraining for general practice, Lancaster: Kluwer.
NG B-Y, KANKANHALLI A and XU Y (2009) Studying users' computer security behavior: A health belief perspective. *Decision Support Systems 46*(4), 815-825.
PAHNILA S, SIPONEN M and MAHMOOD A (2007) Employees' behavior towards IS security policy compliance. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, pp 156b-156b, IEEE.
PERSHING JL (2003) To snitch or not to snitch? Applying the concept of neutralization techniques to the enforcement of occupational misconduct. *Sociological Perspectives 46*(2), 149-178.
PICOLET J (2017) *Hash Crack: Password Cracking Manual (v2.0)*. CreateSpace, Seattle, Washington.
PIQUERO AR, MACDONALD J, DOBRIN A, DAIGLE LE and CULLEN FT (2005) Self-control, violent offending, and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology 21*(1), 55-71.
POTTER B (2010) Common Sense for Your Network. *IT professional 12*(3), 11-13.
PRIEST TB and MCGRATH III JH (1970) Techniques of neutralization: young adult marijuana smokers. *Criminology 8*, 185.
PUHAKAINEN P and SIPONEN M (2010) Improving employees' compliance through information systems security training: an action research study. *Mis Quarterly 34*(4), 757-778.
RENAUD K and DE ANGELI A (2009) Visual passwords: cure-all or snake-oil? *Communications of the ACM 52*(12), 135-140.
ROGERS JW and BUFFALO M (1974) Neutralization techniques: Toward a simplified measurement scale. *Pacific Sociological Review*, 313-331.
SCHNEIER B (2000) Secrets and Lies: Digital Security in a networked world. *New York. John Wiley & Sons Inc. ISBN: 0-471-25311-1 4*, 100-115.
SILIC M, BARLOW JB and BACK A (2017) A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management 54*(8), 1023-1037.
SIPONEN M (2006) Six design theories for IS security policies and guidelines. *Journal of the Association for Information systems 7*(1), 19.
SIPONEN M, PAHNILA S and MAHMOOD A (2007) Employees' adherence to information security policies: an empirical study. In *new approaches for security, privacy and trust in complex environments* pp 133-144,Springer.
SIPONEN M, PAHNILA S and MAHMOOD MA (2010) Compliance with information security policies: an empirical investigation. *Computer 43*(2), 64-71.
SIPONEN M and VANCE A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly 34*(3), 487-502.

Journal Pre-proof

SIPONEN M and VANCE A (2014) Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems 23*(3), 289-305.
SIPONEN M, VANCE A and WILLISON R (2012) New insights into the problem of software piracy: The effects of neutralization, shame, and moral beliefs. *Information & Management 49*(7), 334-341.
STRAUB D, CARLSON PJ and JONES EH (1993) Deterring cheating by student programmers: A field experiment in computer security. *Journal of Management Systems 5*(1), 33-48.
STRAUB DW (1989) *Deterring computer abuse: The effectiveness of deterrent countermeasures in the computer security environment*. PhD Thesis.
STRAUB DW and WELKE RJ (1998) Coping with systems risk: security planning models for management decision making. *Mis Quarterly*, 441-469.
SYKES GM and MATZA D (1957) Techniques of neutralization: A theory of delinquency. *American sociological review 22*(6), 664-670.
TEAMSID (2015) Announcing Our Worst Passwords of 2015. Retrieved January 18, 2016, 2016, from https://www.teamsid.com/worst-passwords-2015/.
TROCHIM W and DONNELLY J (2006) *The Research Methods Knowledge Base*. Atomic Dog, Cincinnati, OH.
VELICER WF and PROCHASKA JO (2008) Stage and Non-stage Theories of Behavior and Behavior Change: A Comment on Schwarzer. *Applied Psychology 57*(1), 75-83.
WILLISON R (2006) Understanding the offender/environment dynamic for computer crimes. *Information Technology & People 19*(2), 170-186.
WILLISON R and WARKENTIN M (2013) Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly 37*(1), 1-20.
WU L and AHN HA (2010) Making sense of conflicting health information: an exploratory study. *Proceedings of the American Society for Information Science and Technology 47*(1), 1-9.
ZHANG J, LUO X, AKKALADEVI S and ZIEGELMAYER J (2009) Improving multiple-password recall: an empirical study. *European Journal of Information Systems 18*(2), 165-176.

Journal Pre-proof

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)

Journal Pre-proof

	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)
intention	intention1	I intend to use complex passwords for work systems.	Venkatesh et al. (2003)
	intention2	I plan to use complex passwords for work systems.	Venkatesh et al. (2003)
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)

Journal Pre-proof

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)	.92	.82	**.92**								
Accept (2)	.86	.75	.28	**.82**							
Compare (3)	.84	.63	-.41	.10	**.85**						
Condemn (4)	.97	.95	-.62	-.02	.56	**.97**					
Entitle (5)	.72	.66	-.45	-.01	.45	.51	**.70**				
Injury (6)	.97	.96	-.52	-.10	.53	.75	.50	**.96**			
Loyal (7)	.96	.92	-.61	-.03	.64	.86	.60	.78	**.96**		
Necessity (8)	.94	.91	-.69	-.15	.63	.84	.55	.75	.86	**.92**	
Response (9)	.92	.83	-.45	-.09	.53	.75	.48	.78	.74	.73	**.92**
CR = Composite reliability; α = Cronbach's alpha											

Journal Pre-proof

Author Bios

Mikko Siponen
University of Jyväskylä
Department of CS and IS
40100 Jyväskylä, Finland
Tel. +358 505588128
mikko.t.siponen@jyu.fi

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

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

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

Journal Pre-proof

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.

Journal Pre-proof