Can the Cognitive Dissonance (CD) concept help to mitigate phishing susceptibility in healthcare?

Prosper Kandabongee Yeng Yeng, Muhammad Ali Fauzi, Arnstein Vestad, Bian Yang, Katrien De Moor, Christian Jacobsen

Submitted to: Journal of Medical Internet Research
on: October 27, 2024

Table of Contents

Can the Cognitive Dissonance (CD) concept help to mitigate phishing susceptibility in healthcare?

Prosper Kandabongee Yeng Yeng[1] PhD; Muhammad Ali Fauzi[2] PhD; Arnstein Vestad[3]; Bian Yang[3]; Katrien De Moor[2]; Christian Jacobsen[4]

[1]Norwegian University of Science and Technology Gjøvik NO
[2]Norwegian University of Science and Technology H403 Teknologivegen 22 2815 Gjøvik NO
[3]Norwegian University of Science and Technology Teknologivegen 22, 2815 Gjøvik NO
[4]Aidn Oslo NO

Corresponding Author:
Prosper Kandabongee Yeng Yeng PhD
Norwegian University of Science and Technology
Teknologivegen 22,
Gjøvik
NO

Abstract

Background: Phishing attacks are a pervasive global threat across multiple sectors, especially healthcare, where attackers exploit psychological factors to increase susceptibility among healthcare staff. Cognitive dissonance, a psychological concept describing the discomfort experienced when an individual holds conflicting beliefs or attitudes, may serve as a critical factor influencing the adherence to cybersecurity practices. Similar to how hunger motivates actions to alleviate discomfort, cognitive dissonance prompts individuals to seek internal consistency, potentially influencing their response to phishing attempts.

Objective: This study examines the role of cognitive dissonance in reducing phishing susceptibility among healthcare staff. Through a controlled, in-the-wild phishing simulation, cognitive dissonance was assessed as an independent variable to understand its impact on staff compliance with security practices.

Methods: A two-stage controlled experiment design was used, including self-reported assessments and real-world security practice observations. A total of 830 participants, comprising doctors and nurses from a major hospital in Norway, participated in the experiment. Participants were divided into control, experimental, and neutral groups, with susceptibility rates recorded at 65% in the control group, 44% in the experimental group, and 53% in the neutral group. Statistical analysis, specifically Pillai's Trace assessment, was used to evaluate differences in actual behavior, perceived severity, and cues to action.

Results: Significant differences were observed in participants' responses, suggesting that cognitive dissonance may influence susceptibility to phishing attacks by affecting their perception of risk and cues to action.

Conclusions: This study highlights the potential of leveraging cognitive dissonance as a psychological tool to reduce phishing susceptibility in healthcare. Practical recommendations are provided to help healthcare institutions apply cognitive dissonance strategies in cybersecurity training to foster more resilient security practices among staff.

(JMIR Preprints 27/10/2024:68051)
DOI: https://doi.org/10.2196/preprints.68051

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Can the Cognitive Dissonance (CD) concept help to mitigate phishing susceptibility in healthcare?

Abstract

Background:

Phishing attacks are a pervasive global threat across multiple sectors, especially healthcare, where attackers exploit psychological factors to increase susceptibility among healthcare staff. Cognitive dissonance, a psychological concept describing the discomfort experienced when an individual holds conflicting beliefs or attitudes, may serve as a critical factor influencing the adherence to cybersecurity practices. Similar to how hunger motivates actions to alleviate discomfort, cognitive dissonance prompts individuals to seek internal consistency, potentially influencing their response to phishing attempts.

Objective:

This study examines the role of cognitive dissonance in reducing phishing susceptibility among healthcare staff. Through a controlled, in-the-wild phishing simulation, cognitive dissonance was assessed as an independent variable to understand its impact on staff compliance with security practices.

Methods:

A two-stage controlled experiment design was used, including self-reported assessments and real-world security practice observations. A total of 830 participants, comprising doctors and nurses from a major hospital in Norway, participated in the experiment. Participants were divided into control, experimental, and neutral groups, with susceptibility rates recorded at 65% in the control group, 44% in the experimental group, and 53% in the neutral group. Statistical analysis, specifically Pillai's Trace assessment, was used to evaluate differences in actual behavior, perceived severity, and cues to action.

Results:

Significant differences were observed in participants' responses, suggesting that cognitive dissonance may influence susceptibility to phishing attacks by affecting their perception of risk and cues to action.

Conclusions:

This study highlights the potential of leveraging cognitive dissonance as a psychological tool to reduce phishing susceptibility in healthcare. Practical recommendations are provided to help healthcare institutions apply cognitive dissonance strategies in cybersecurity training to foster more resilient security practices among staff.

Keywords: Cognitive dissonance, Phishing simulation, Healthcare, Psychological incentive, Health belief model, Protection motivation theory

Introduction

The healthcare sector plays a vital role in meeting societal needs, and technological advancements have significantly impacted healthcare services through terms like health

informatics and eHealth [1]. However, the integration of technology in healthcare has also introduced risks and challenges, with cybersecurity issues posing a significant challenge to the eHealth infrastructure. Incidents of security and privacy breaches in healthcare have been reported at alarming rates [2], including a cyber security report in 2021 that revealed the National Health Service (NHS) in the UK being targeted with 357 million malicious emails. On average, each employee received around 89,353 targeted emails in that year [3]. Phishing attacks, in particular, have seen a surge, especially within the healthcare sector, during the COVID-19 pandemic [4], with estimates of recent increases in phishing attacks ranging from 600

Phishing attacks exploit the human element of security vulnerability, relying on deceptive messages to trick individuals into divulging sensitive information or installing malicious software within targeted infrastructures [5, 6]. Phishing attacks encompass various forms, including emailbased, SMS-based (Smishing), and voice-based (Vishing) attacks. These attacks primarily exploit the human aspect of security weaknesses, often referred to as the weakest link in the security chain [7, 5].

To combat phishing and other malicious attacks, the implementation of cybersecurity strategies and practices has become essential for organizations exposed to such threats. Cybersecurity practices involve the development, adoption, and adherence to organizational security policies for IT infrastructures, with the aim of achieving confidentiality, integrity, and availability (CIA) requirements [8, 9]. These security practices involve human-centred aspects that rely on individuals' awareness and compliance with security measures [10]. While technical measures like email filtering can efficiently detect phishing emails, a small proportion may still reach users' inboxes, where human judgment is required to take appropriate security measures [5, 11, 12, 13]. Hence, users of IT infrastructures, including healthcare staff such as doctors and nurses, are expected to follow prescribed security measures or policies [14].

The human factor in cybersecurity can be likened to the vulnerability of the ”Bribed to open the gate of the great wall of China” story [15, 16, 17]. In ancient times, the Chinese built a strong and tall wall that was difficult to scale, breakthrough, or tunnel beneath. However, the enemy successfully invaded China three times by bribing the gatekeepers. Similarly, an eHealth infrastructure may have robust technical controls such as firewalls, DMZ, anti-viruses, and intrusion detection and prevention systems, but if the ”human firewall” is weak, the infrastructure becomes vulnerable, rendering the technical security controls ineffective [18, 19, 20].

The act of responding to phishing emails includes decision-making processes, wherein individuals are often confronted with challenging choices between equally enticing alternatives, such as whether to click on the links contained within the emails. This predicament can give rise to cognitive dissonance, wherein an individual simultaneously holds two contradictory beliefs [21]. For instance, while being aware that the received email originates from an external organization, the email may entice the person with financial incentives contingent upon clicking the embedded link. In order to justify their actions, individuals frequently employ neutralization techniques or rationalizations, particularly when engaging in deviant behaviors like clicking on the link. Such rationalizations are believed to stem from a motivation to reduce cognitive dissonance [21, 22]. Numerous studies have indicated that this process of rationalization can contribute to the adoption of risky cybersecurity practices [23, 24, 25]. Motivated by these observations, our study empirically examines the use of cognitive dissonance theory as an

intrinsic motivational method to reduce phishing susceptibility in the healthcare sector.

Previous studies have explored other approaches to reduce phishing susceptibility in healthcare, considering variables like disposition to trust, risk-taking propensity, gender effects [26], the theory of planned behavior, and trust theories [27]. These studies found positive relationships between attitude, subjective norms, perceived behavioral control, collective felt trust, and self-reported compliance behavior [27]. However, some well-known psychological theories such as cognitive dissonance (the presence of conflicting cognitions or thoughts) [28] and perception constructs related to the Health Belief Model [29] and Protection Motivation Theory [30] have not been thoroughly examined in phishing simulation studies within the healthcare sector.

This experiment aims to determine if healthcare staff's perception and behaviour, when exposed to cognitive dissonance, will make them less susceptible to phishing simulation attacks.

The following sections present the theoretical background, including related works, the adopted theory, study framework, and hypotheses. This is followed by a description of the study's methodology, presenting the design and implementation. The results are then presented in the results section, followed by a discussion and conclusion.

Study background

Cognitive dissonance serves as one of the initial psychological challenges individuals must address when confronted with the decision to comply with cybersecurity practices. Just as hunger motivates actions aimed at reducing hunger, cognitive dissonance motivates efforts to alleviate the discomfort and achieve internal consistency [31]. In this study, an intervention based on the cognitive dissonance theory is explored due to its involvement in human decision-making, judgments, and evaluations, and its influence on faster and more accurate decision-making processes[21].

People often employ rationalization methods to neutralize their cognitive dissonance before engaging in security policy violations [32]. However, the implementation of anti-neutralization methods can disrupt this process by instilling feelings of guilt and shame [33], discouraging individuals from violating security measures [23, 34]. Furthermore, some offenders may underestimate the constructs within the Health Belief Model (HBM) and Protection Motivation Theory (PMT), as observed in cases like smokers [35].
Considering cognitive dissonance as a practical tool to induce attitude and behaviour change [36], its adoption as a psychological incentive holds significant potential in reducing susceptibility to phishing attacks. By leveraging cognitive dissonance and its associated processes, organizations can effectively encourage individuals to prioritize and adhere to secure behaviours.

Psychological incentives in relation to a phishing attack

To reduce security violations from the human aspect, researchers have assessed various multidisciplinary behavioural theories to motivate users [37, 38, 38, 39]. Motivations for information security-conscious care behaviour can be considered as a state of having an interest in complying with the security measures [37, 38]. These motivations have been categorised into intrinsic and extrinsic motivations [38]. Intrinsic motivation tends to induce motivations from the individuals themselves without using external factors. It is a behaviour that is based on self-

rewarding with inherent satisfaction. This type of motivation is independent of external reward and provides the freedom for employees to take their own internal decisions including their own aspirations. Alternatively, extrinsic motivation is influenced by external rewards such as financial rewards or punishment towards inducing the individuals to comply with conscious care security behaviour. Many phishing-related attacks rely upon their victims undertaking specific behavioural actions including opening malicious links. The probability of the targets clicking on the link depends on a broad range of psychological motivations including perception, cognition, trust, and their cognitive dissonance resolution [40, 28]. The cyber adversaries themselves weave in psychological concepts to trick their targets into clicking the links [41]. To enhance the perception of healthcare staff towards reducing phishing susceptibility, this study therefore assessed cognitive dissonance theory in an experiment to determine if antrationalization in the experiment group contributes to less phishing susceptibility among healthcare staff. Further explanation of perception and cognitive dissonance is provided in the next section.

Perception and cognitive dissonance as an incentive towards mitigation of phishing attack

Cognitive dissonance is a psychological discomfort that sets in when for instance, a person knows of a good security measure but tends to (consciously) circumvent that. In order for the person to be able to carry on with the unethical or the illegality, the cognitive dissonance is usually resolved with rationalization methods [28]. It involves pairs of cognition or elements of knowledge and whether these pairs are relevant or irrelevant to each other. Two relevant elements of knowledge, are either consonant or dissonant (in disagreement or incongruent) to each other. Two elements of knowledge are consonant pairs if one agrees with the other, else they are dissonant pairs if one element of the pairs opposes the other. The presence of the discrepancy between dissonant pairs of cognition creates a psychological discomfort called cognitive dissonance. This dissonance motivates the individual to reduce cognitive discrepancy. A higher magnitude of dissonance creates higher motivations to reduce discomfort.

Cognitive dissonance can be resolved in two ways. First, by deciding not to pursue the desires and resolved not to engage in the unpleasant desire. An example includes a person who decided not to violate an information security (IS) policy. Secondly, others may rationalize violating the policy with numerous excuses. In cognitive dissonance resolution, the elements of knowledge that are in disagreement can be removed, and new elements of knowledge that are in agreement are added. Furthermore, the importance of the disagreements between the cognition pairs is reduced or the importance of the agreements between the cognitive pairs is increased. For instance, if a healthcare person who often shares his password with his colleagues happens to know that password sharing violates the hospital’s security policy, he will experience dissonance since the elements of knowledge that password sharing violates security policy is dissonant with the cognition’s that he shares his passwords with others.

The person can reduce the discomfort by changing his behaviour to stop sharing his access credential with others. This will be in line with the cognition that sharing passwords violates the security policy. Alternatively, the healthcare staff can reduce the discomfort by rationalizing to continue to share his password by changing his cognition about the harmful effect of sharing his passwords with

others, with the excuse that password sharing does not violate the hospital's IS policy, thereby eliminating the dissonant cognition [40]. Additionally, he may add positive elements of sharing his passwords which is an addition of consonant cognition. He may also reduce the importance of dissonant cognition by holding the belief that harm from password sharing is negligible. Furthermore, the staff who shares his password with others could increase the importance of consonant cognition by considering the significant contribution of password sharing including saving a life. To encourage consonant pairs cognition of healthcare staff to comply with phishing-related security practices, we examined the concept of discouraging rationalization approach as a strategy to reduce cognitive dissonance. We, therefore, opine that healthcare staff phishing susceptibility will be comparatively reduced if they are treated with anti-rationalization methods. Specifically, we hypothesized that

- H1: In a control experiment, healthcare staff in the experiment group who are treated with anti-neutralization methods will be less susceptible (low click rate) to the simulated phishing attack as compared to healthcare staff in the control and neutral group.
- H2 Healthcare staff in the experiment group will have better self-reported phishing security knowledge (H2a), attitude (H2b) and behaviour (H2c) as compared to the control group.

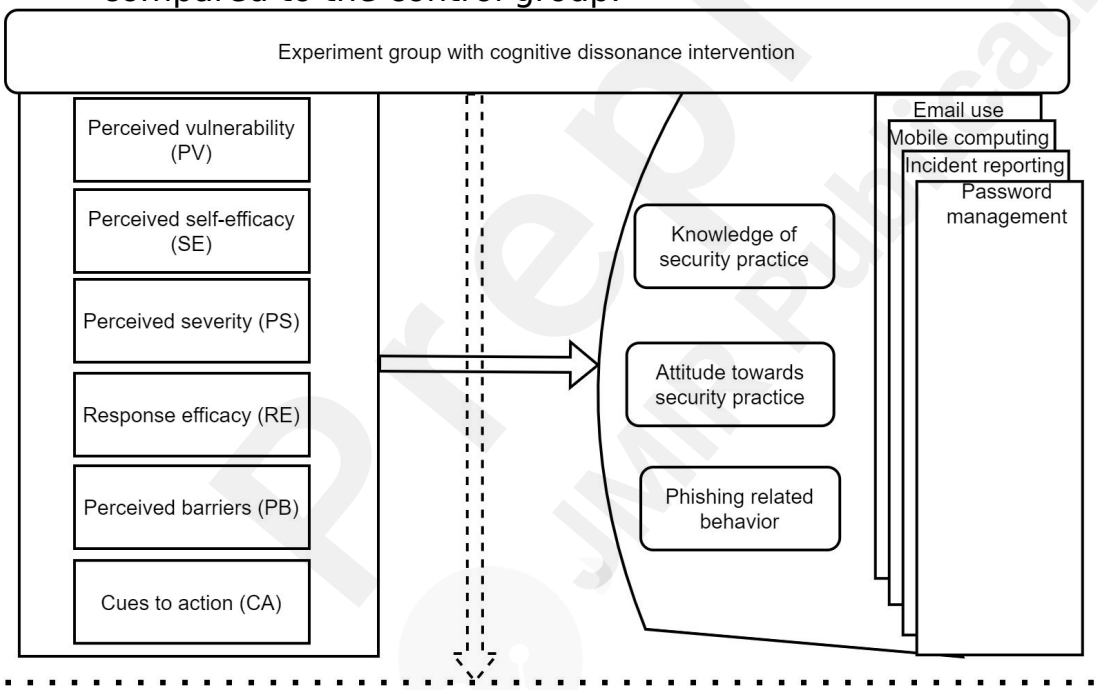

Figure 1: Experiment-model for Psychological incentive

The effect of the cognitive dissonance on perception

In a phishing attack, adversaries tend to manipulate the psychological attributes of their targets into clicking malicious links [42]. Therefore, it is imperative to explore for incentives that can be used to improve the conscious care behaviour of the healthcare staff to be cautious when they are faced with deceptive messages from phishing attackers [43, 44]. In this study, we, therefore, propose that if healthcare staff are treated with the anti-rationalization concept in

cognitive dissonance, their perception of phishing susceptibility will be significantly better (or less risky) than their peers in the control group of the experiment. Specifically, perceived vulnerability (PV), perceived severity (PS), perceived self-efficacy (SE), perceived response efficacy (RE), Cues to action (CA) and perceived barriers (PB) are the psychological constructs that were used in health belief model (HBM) and protection motivation theory (PMT). These constructs are deemed suitable for achieving the objective of this experiment [45].

The view in HBM is that people usually perceive the severity of a disease. So, their perception of the effectiveness of the recommended treatment and their ability to follow recommended actions inform them about their health behaviour choices [46, 47, 47]. HBM has since been adopted in observing information security practices [48, 49]. The HBM has the following construct; PV, PS, perceived benefit(PBf), PB, cues-to-action (CA), and SE.

PMT on the other hand consists of threat and coping appraisal constructs that are used in decision-making especially when people are under stressful situations [50, 51, 52]. The threat appraisal consists of PV and PS while, the coping appraisal consists of response-efficacy (RE), SE, and response cost (RC). RE is the perception of the effectiveness of the recommended action while RC is the cost component of the recommended measures. PV is the susceptibility risk of being a victim of a cyber attack. PS is the perception of the magnitude of the adverse impact if a cyber attack should occur. PB are the obstacles that are to be overcome when following the recommended security practice, while SE is the assessment of one’s ability to carry out the required security practice. Additionally, CA is internal or external stimuli including training, pain, and knowledge of the situation, that influences an individual to adapt to the recommended solution. Some common drawbacks that have been associated with PMT are limitations to measure attitude, habitual behaviour, and environmental or economic factors. Based on this background, the following hypotheses were formed;

- H3: PV of participants in the experiment group has lesser phishing susceptibility risk as compared to that of the control group.
- H4: PS of participants in the experiment group has lesser phishing susceptibility risk as compared to that of the control group.
- H5: SE of participants in the experiment group has lesser phishingsusceptibility risk as compared to that of the control group.
- H6: RE of participants in the experiment group has lesser phishingsusceptibility risk as compared to that of the control group.
- H7: PB of participants the in the experiment group has lesser phish-ing susceptibility risk as compared to that of the control group.
- H8: CA of participants in the experiment group has lesser phishingsusceptibility risk as compared to that of the control group.
- H9: password handling in phishing attacks of participants in the ex-periment group has lesser phishing susceptibility risk as compared to that of the control group.
- H10: Incident reporting management in phishing attacks of partici-pants the in the experiment group has lesser phishing susceptibility risk as

compared to that of the control group.
- H11: Incident reporting management in phishing attacks of partici-pants the in the experiment group has lesser phishing susceptibility risk as compared to that of the control group.
- H12: Incident reporting management in phishing attacks of partici-pants in the experiment group has lesser phishing susceptibility risk as compared to that of the control group.
- In the subsequent subsections, a review of the related work was conducted to provide guidance for this study.

Related work on incentives in a phishing simulation study in healthcare

In efforts toward mitigating phishing susceptibility in healthcare, Abdelhamid [26] investigated health concerns, disposition to trust, risk-taking propensity and the effect of gender on phishing susceptibility. A total of 200 online participants were required to read scenarios and indicate their intention to click a phishing simulated link in the healthcare context. In the findings, health concerns, disposition to trust and risk-taking tendency were predictors of higher phishing susceptibility. Abdelhamid et al., the study provided knowledge on the self-reported behaviour of the targets in the context of trust and risk-taking tendencies however, the actual phishing security behaviour of these participants was not considered. This provided an aspect of the bases for adding a simulated phishing attack layer in our current experiment.
In a related study, an IT service provider conducted a spear phishing simulation attack among various staff in various sectors including healthcare and finance staff who were its clients [53]. In the simulated attack, the participants were tested on whether they would click on a hyperlink in a malicious email, submit a form with personal information and click on other hyperlinks after accessing a website form. Of a total of 1174 targets, 240 accessed the phishing website representing a 20.4% of success rate. Moreover, the healthcare industry was the largest group of victims who interacted with the phishing website and submitted a form providing both their usernames and password. These findings by Slonka et al., buttressed the high susceptibility of phishing attacks among healthcare staff which serves as a motivation for our study. Besides, Slonka et al., the method included the collection of passwords and user names from the participants, which added extra depth to their attack, however, to reduce the security risk, complexities and ethical requirements, the targets in our phishing simulation attack were challenged with a simulated malicious link.

Gordon et al. also evaluated the effectiveness of a phishing training program in a large hospital in the US [54], having sent a total of 20 email campaigns to a total of 5416 healthcare staff. Two groups thus, offenders and non-offenders, emerged. Offenders were those participants who clicked on at least five simulated phishing emails in the 15th campaign, while the non-offenders did not click or clicked on less than the five simulated phishing emails. It was found that the click rates decreased for each group over 20 campaigns. The offenders were subsequently trained. Gordon et al., the study provided a susceptibility gap that guided the training of the participants who were identified in the simulation to pose more threat in terms of phishing susceptibility. However, their study, [54] did not include the assessment of various factors including psychological, social

and cultural factors that have an influence on security behaviour [48]. Another relevant study incorporated constructs from the Theory of Planned Behaviour and trust theories aimed to assess the factors that influence clicking behaviour [27].

In the study, a simulated hoax phishing email was sent to 397 healthcare staff who participated in the study. Later, a survey was conducted with the participants where their self-reported phishing security practice in the aspect of the theory of planned behaviour (TPB) and collective felt trust constructs were assessed. A structural equation modelling was used to assess the gaps between the actual security practice of the participants and their self-reported security behaviour on phishing. The results revealed that attitude, subjective norms and perceived behavioural control and collective felt trust predicted self-reported compliance behaviour. Collective felt trust is about the perception of employees on how they are trusted by management [55]. On the aspect of perceived behavioural control, it is about people's perception of others in terms of their ease or difficulty in performing a given task [56], while subjective norms are about the perception of one's behaviour based on the significant influence of others [57]. In effect, Jalali et al observed the behaviour of participants in relation to their actual phishing attack behaviour and their self-reported behaviour. Similarly, [26, 53, 54, 27], performed the observational study, however, our study delved into a comparative study to assess the effect of the cognitive dissonance on mitigating phishing susceptibility.

Related work in the use of cognitive dissonance in assessing security practice

as those of deterrence sanctions.

Various studies [58, 54, 59, 5] have contributed knowledge towards reducing phishing susceptibility however, these studies' scope did not include the investigations of psychological aspects. Understanding the psychological aspect is very crucial in assessing phishing attack vulnerabilities in the human aspect since attackers tend to circumvent the users' psychological factors by tricking them to click on malicious links. In this regard, Jalali et al and other researchers such as Barlow et al and Payday et al included psychological constructs in their investigations. However, these studies [27, 40, 10], did not perform a comparative assessment to determine the efficacy Cognitive dissonance theory was developed by Festinger, around 1957 within the field of social psychology [21]. However, it has been found to be useful in marketing, education, management and information security [40]. A related study [40] therefore proposed the use of cognitive dissonance theory in mitigating insider threat neutralization, towards reducing cyber security risk behaviour. In this experiment, a honeypot was used in the study model, to bait insiders to attack the honey port, instead of attacking real data. The study model was centred on assessing the rationalization of insiders to neutralize their actions. In this model, a honeypot was used as bait to induce cognitive dissonance by luring insiders with the honey port. The honeypot also served as a tool to detect insider threats and activate social-technical interventions. The interventions include the neutralization mitigation mechanism (NMM) such as promoting policy, posting

instructions, alerting the conscience and assisting compliance. The NMM are being introduced prior to attacking, during the attack and after attacking the honeypot by participants. Insiders who still rationalized and attacked the honeypot, suggest that the NMM possibly failed to influence the attacker's behaviour.

Additionally, Barlow et al., analyzed denial of injury, the metaphor of the ledger and the defence of necessity aspects of rationalization for noncompliance with password security measures [10]. The focus was to examine whether IT security training that is focused on mitigating neutralization will improve compliance with security measures as compared to when IT security training is focused on deterrence measures. The findings showed that focusing on neutralization techniques is as effective of cognitive dissonance among healthcare staff in relation to their intended behaviour, actual behaviour and perception of phishing security practice. This gap is what has triggered this study.

Method

A two-stage controlled experiment was adopted in this paper where a total of 830 participants were invited from one of the largest hospitals in Norway to take part in the study. Based on convenience sampling, the participants were mainly doctors and nurses. These were randomly assigned into two groups thus, a control group and an experiment group as shown in Figure 1 The participants were then invited in May 2022 to answer a questionnaire in the first stage. A total of 82 (9.8%) participants took part in the first stage which involved the phishing susceptibility survey. Out of this, 42 of the participants were in the control group while 40 of them were in the experiment group. In the second stage of the study, a phishing simulation email was sent to 34 and 32 participants in June 2022 in the respective control and experiment groups. These were the participants who agreed to participate in the second stage which requires participants to identify a simulated malicious email in the phishing attack simulation exercise. Subsequently, the "malicious" email was then sent to the 753 participants called a neutral group who were neither in the control group nor the experiment group. The healthcare staff who participated in the first stage and the second stage were to be motivated with free lunch at the hospital canteen. Additionally, they will be in a draw where ten lucky winners will receive about USD 50.00 gift cards.

Ethical, privacy and security measures with in-the-wild study

In this experiment, a survey with a questionnaire instrument, and an in-the-wild-field study were combined. The hybrid was essential since the survey approach provided bases for the researchers to understand the intended phishing security behaviour of the participants, while the in-thewild-field study tested the actual phishing security practice (the clicking action) of the participants. In-the-wild-field study is a kind of phishing simulation study in which the researcher performs a phishing simulation attack on the participants [6]. Additionally, other phishing study-related methods include lab-based experiments and questionnaire-based studies. The lab-based phishing experimental studies are conducted in controlled laboratories whilst the survey-related phishing study requires the participants to report their phishing behaviour. Among these, the

in-the-wild field study is deemed effective because the simulated attacks are very similar to the real attacks except that the payload in this case is non-malicious. The issue is that in-the-wild-field study faces ethical dilemmas. Many ethical committees decline approvals for in-the-wild-field related studies with the view that deception in research contradicts informed consent and that it has possible harm to participants. However, this notion has been argued against with the point that when participants are aware that their phishing behaviour is being observed, they tend to behave differently [60, 61].

Furthermore, the research community also argued that deception in research is not ethically wrong if the reasons for withholding such information are valid for the study [60, 62]. They further explained that participants in the clinical sector do not care about deception in research if it is likely to educate them. It may be impossible to study some psychological constructs without withholding certain information about the true purpose of the study [61] in-the-wild-field study, however, certain processes need to be followed [61, 60]. Prior to the launching of the phishing study, a press release to administrators should be issued. Also, during the launching of the attack, data protection and the well-being of the participants need to be considered by providing debriefing and post-informed consent. Having followed these measures, this study also obtained ethical clearance from the targeted hospital, the Regional Committees for Medical and Health Research Ethics of Norway (REK) and the Norwegian Center for Research Data (NSD) an email-based phishing simulation was performed in this controlled experiment.

Survey instrument

This study was conducted having reviewed and developed various frameworks in psychological, social and cultural aspects [20, 19, 18, 48, 20, 18, 63, 18, 48]. In the first section of the questionnaire, we adopted Parson et al, the approach of the human aspect of the information security questionnaire [63]. This consists of 42 items which measured the knowledge, attitude and behaviour (KAB), risk in relation to phishing attacks on password management, email use, incident reporting and mobile device use. A 5-point Likert scale was used in this instrument. These areas of security practice are believed to be more prone to phishing attacks. Additionally, about 25 items in this instrument were measuring other psychological constructs such as PV, SE, CA, PB and RE. Figure A.8 in appendix Appendix A showed the structure of the questionnaire. The instrument was developed with an online secured Norwegian version of a survey system called Nettskjema [64]. The questionnaire was then duplicated into two, thus the control and the experiment group. The difference between them was that the experiment group of the questionnaire had a cognitive dissonance message item as shown in Figure B.5 in Appendix 1, and in the model in Figure 1. While the questionnaire of the controlled group was not infused with the cognitive dissonance message item. The instrument was then pretested with four PhD students and a professor who works in the space of cybersecurity. Issues including complex terminologies and the length of the cognitive dissonance message were identified and resolved. Measures were also taken against error variances [65]. Error variance can be caused by preexisting factors to introduce changes among the study groups, either than the treatment effect. In this

regard, the healthcare personnel were randomly assigned to reduce potential biases. Additionally, the questionnaire of the experiment group was incorporated with a cognitive dissonance message and they were asked not to share their questionnaire with others.

Attention checkers were among the survey items in the study and these required the participants to choose specified responses. Participants who failed to correctly answer two out of the three attention checkers imply that they failed to pay attention while answering the questionnaire. As a result, two records were discarded. This has been one of the most popular methods being used to improve the quality of survey responses without compromising the research findings [66, 67, 68, 69, 70].

Phishing simulation setup and experiment process

A phishing simulation tool, known as Gophish [71], was set up on a server as illustrated in Figure 2. It has a functionality where an attacker can simulate a phishing email and send it to a target. It is also able to record click events of the links in phishing emails.

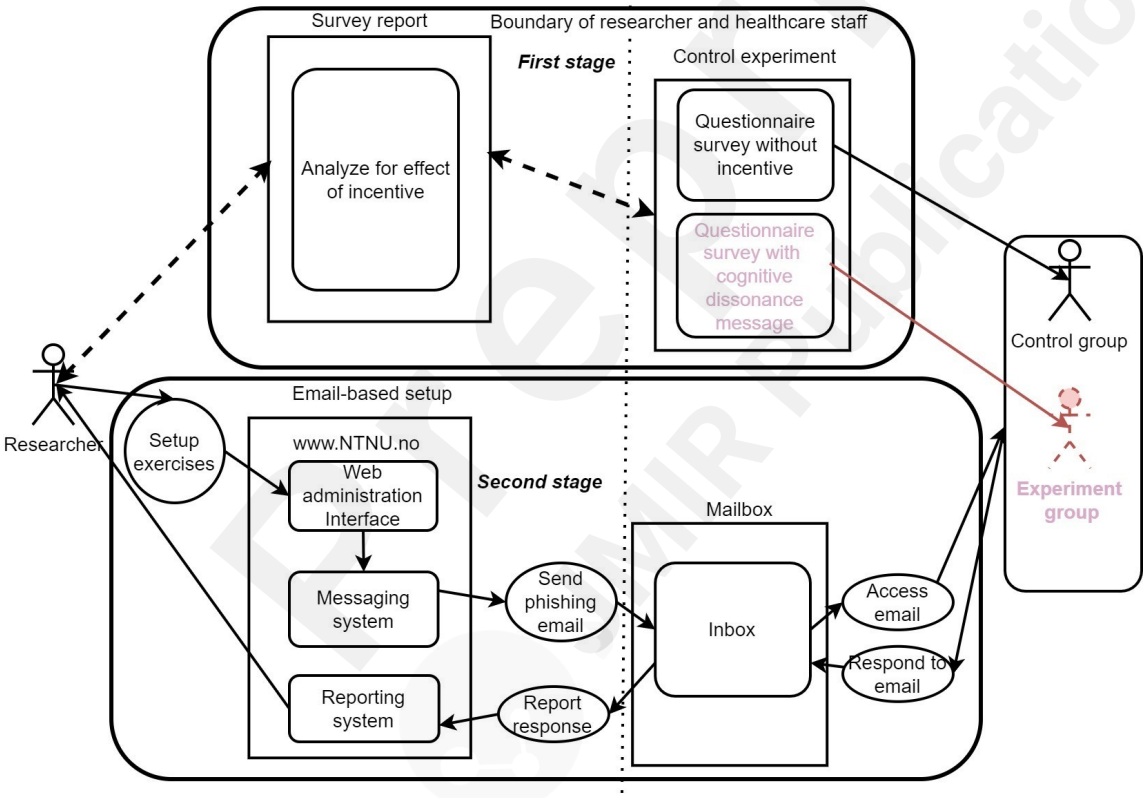

Figure 2: Experiment setup

In the initial setup, the simulated phishing email was tested with a staff of the target hospital however, that email was flagged as spam by the email filtering system of the service provider. Since the study goal was not to test the technical email security controls of the target facility, we collaborated with the providers, and they configured the email system to allow the phishing simulation email to land in the inbox of the targeted participants.

The use of link click event

In this experiment, the Gophish system recorded the sending details of the simulated malicious emails such as the sender's email address, date and time sent, and sending status. Additionally, the click details of the embedded link including email address, click status, date and time of click were also recorded. A rhetorical question that needs addressing is whether clicking on a link alone is an effective security assessment in this phishing simulated study.
Proponent argues that malware and rootkit could be embedded in a link such that clicking on that link could imply granting permission for the victim's computer to open, download and install the malware [72]. This can enable the victim's computer to be controlled by the attacker as part of a bot, botnet. Most ransomware attacks adopt this strategy where links or documents containing macros are embedded with the malware. So as soon as the link is clicked or the document is opened, it downloads and infects the victim's computer quickly within seconds to about 20 minutes. Within this time, the malware can search for all files in various media such as internal and external storage devices to be encrypted.

Aside from a click that can lead to compromising a system, there exist zero-day click attacks [73, 74]. In this kind of attack, the target system can be compromised without any click event from the victim. A common instance includes the Pegasus spyware which took advantage of the IMassage vulnerability in the iPhone 12 Pro.

On the other hand, the opponent discourages the use of a click event in a phishing simulation study with the view that it is not an effective measure. The reason is that web browsers in this era are mostly updated with security patches which prevent automatic downloads in the event of link clicks [75]. Additionally, attackers do request the victim's user credentials, and some sensitive information such as bank and payment card details to enable them to perform effective attacks.

While the opponent's point of view is true, it depends on the attacker's goal. For instance, if the goal of the attacker is not to steal payment card information or login credentials, that cyber-criminal will not phish for such information. Also, if the target's browser is not updated with the latest security updates, that person's risks of falling victim to installing malware become high if a malicious link is clicked. Aside from these, if there are zero-day vulnerabilities that are being exploited by cyber-criminals, clicking on malicious links can take advantage of that to compromise the system. Besides, common web vulnerabilities including cross-site scripting and cross-site request forgery require the victim to basically click on the malicious link.

Therefore, to avoid being a victim of the attack, the surest way is to avoid clicking on suspicious links while reporting such incidents to the appropriate incident response teams. To this end, the healthcare staff were tested with the ”link click” in this experiment. Related studies also adopted the ”link click” method and collected the click events of participants for analysis [5, 27].

Controlled experiment

The basic type of research studies in social science and psychology include an observational study, and a controlled experiment [76, 77]. The observational study involves the measure or a survey of participants of a sample without influencing them, whereas a controlled experiment involves assigning the participants to groups and applying some treatment to one of the groups (called the experiment or the treatment group), while the other group (called the control group) does not receive the treatment.

MANOVA is often used to assess the effect of the intervention in a controlled experiment because it creates a linear combination of all the dependent variables and tests to see if there are differences across the levels of the independent variables (levels of groups ie control group and experiment group) on that linear combination of the combined dependent variables [78]. If a difference is detected, some follow-up tests are performed to determine where the difference exists among the various dependent variables. It is also possible that there could be no difference across the group levels.

To assess the effectiveness of the cognitive dissonance in a control experiment, a minimum of two dependent variables are needed with interval or ratio levels which are commonly known as scales in SPSS. In this study, fourteen dependent scale variables were used which satisfied the number of dependent variable assumptions. Additionally, a minimum of one independent variable is required with at least two or more categorical groups. Our study also meets this condition with an independent group of two levels, ie control and experiment levels.
MANOVA assumes multivariate normality. The test also needs homogeneity of covariant metrics and the dependent variables cannot be multicolonial. Additionally, sufficient sample size is also needed in MANOVA.

Table 1: Rule of Thumb on Cronbach's Alpha [82, 83]

AlphaCoefficient Range	Strength of association
<0.6	Poor
0.6 to < 0.7	Moderate
0.7 to <0.8	Good
0.8 to <0.9	Very Good
0.9 to 1	Excellent

Essentially, there is a need to have the required sample size for each level of the independent variable. The rule of thumb requires 30 participants in each group level [79]. So the actual behaviour(AB,) variable, has the lowest participants of 30 and 32 participants in the respective control and experiment group levels which therefore indicates that the study met the minimum requirement.

Reliability assesses the extent that to which a group of items are assessing the same underlying construct [80, 81]. So, the coefficient of Cronbach's alpha value is often used and it is expected to be within the range of 0 and 1 [82]. The

average expected value is above 0.6 as shown in Table 1. However, these Alpha values are mostly dependent on the number of items measuring the construct [82, 83, 84, 85, 86]. According to [80, 82, 83], if the number of items measuring a construct is equal to or greater than 10 items, the Cronbach's alpha value is expected to record a coefficient of 0.6 or higher, else, the items might not be measuring the same construct. However, if the number of items measuring a particular construct is less than 10, Cronbach's alpha value could be as low as 0.2 to 0.4 [80, 85]. This means that the Cronbach's alpha value largely depends on the number of items measuring the targeted construct

Findings

The main objective of this study was to examine the effect of cognitive dissonance and other psychological factors toward mitigating phishing susceptibility in healthcare. This section, therefore, presents the analysis of the results covering the click rates, reliability, descriptive statistics, normality tests and the significance of the studies.

The click rates were 65% (22), 44%(14) and 53% (396) in the control, experiment and neutral groups respectively as shown in figure 3. As shown in Table 2, a total of 80 of the survey participants' records were analyzed, out of the 82. Two records were removed from the analysis because they did not pass attention checks that were placed in the questionnaire [66, 67, 68, 69, 70].

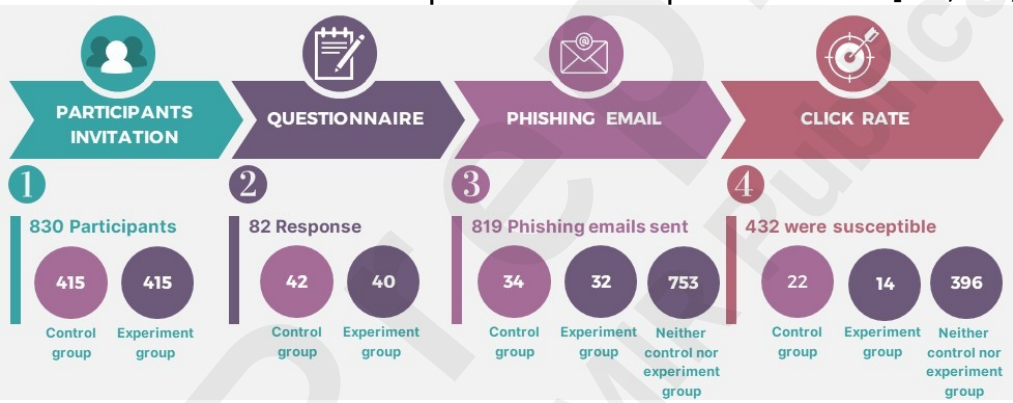

Figure 3: Response rate

Furthermore, among these participants, 72.5% were males while 27.5% were females. The age range between 31 to 40 of the participants had the highest proportion (28%) while over 60 years old participants formed the lowest proportion (11.3%). Regarding the roles of the participants, mainly doctors, nurses, and administrators took part in the study. Nurses were more than half the proportion of the total participants (50%), followed by doctors (38%) and administrators (7.5%). In terms of years of work experience, the participants with over twenty years of work experience were comparatively more (36.3%) as shown in Table 2. Meanwhile, the participants also shared their phishing security practice knowledge. Most of them (32.5%) had medium knowledge, and 28% of them had basic knowledge, while 15% indicated that they had no knowledge in phishing security practices. Additionally, the participants in the experiment group shared their opinion on the treatment effect of cognitive dissonance. Out of the 40 participants who were in the experiment group, the

majority of them thus, 38 (95%), agreed with the effectiveness of the treatment measure. To control for these confounding variables, the randomization [87] approach was used to assign the participants into the two groups in this study.

Table 2: Descriptive statistics of demographic variables)

Variable	Category	N	%
Gender	Male Female	58	72.5%
		22	27.5%
Age range	21-30	14	17.5%
	31-40	23	28.8%
	41-50	18	22.5%
	51-60	16	20.0%
	>60	9	11.3%
Position	Administrator	6	7.5%
	Nurse	40	50.0%
	Doctor	31	38.8%
	Others	3	3.8%
Yeas of experience	1-5	9	11.3%
	6-10	19	23.8%
	11-15	10	12.5%
	16-20	13	16.3%
	>20	29	36.3%
Knowledge in phishing attack	No knowledge	12	15.0%
	Basic	23	28.8%
	Medium	26	32.5%
	High	15	18.8%
	Very high	3	3.8%
	Professional	1	1.3%
Opinion in cognitive dissonance	N/A	40	50.0%
	Agree	38	95.0%
	Disagree	2	5.0%

Table 3: Reliability statistics

No	Construct	Cronbach's Alpha	N of Items
1	K	0.660	13
2	A	0.53	9
3	B	0.648	16
4	PV	0.654	3
5	PS	0.540	3
6	SE	0.655	6
6	RE	0.717	3
8	PB	0.476	4
9	CA	0.256	2
10	Password	0.349	6
11	Incident	0.792	9

12	Email	0.554	7
13	Mobile	0.65	12

4.1. Reliability, validity, and assumption assessment

Table 3 presents Cronbach's Alpha reliability. The highest value was 0.792 which corresponded to incident reporting, while the lowest value was 0.256 which corresponded to CA.

Based on the number of items, all the constructs met the required Cronbach's Alpha thresholds as shown in Table3.
The null hypothesis of normal distribution was tested with ShapiroWilk on the assumption that the dependent variables are normally distributed. From Table4, various dependent variables namely AB, A, PV, SE,PB, CA, password, incident, email and mobile were not normally distributed. This, therefore, informed the choice of some of the test and analysis methods that was adopted in this study.

Prior to performing the MANOVA, the appropriate correlations were conducted between all of the dependent variables (see in Table 5) with the aim to assess the assumption that most of the dependent variables in the MANOVA analysis would be correlated with each other in the moderate range between 0.20 - 0.60 correlation coefficient [88]. Based on the normality test as shown in Table 4 , a non-parametric correlation (Spearman's correlation) was performed as shown in Table 5. The results showed that

Table 4: Normality test (Shapiro-Wilk)

	Statistic	df	Sig.
AB	0.627	62	0.000
K	0.969	62	0.113
A	0.954	62	0.020
IB	0.968	62	0.110
PV	0.917	62	0.000
PS	0.884	62	0.000
SE	0.981	62	0.435
RE	0.814	62	0.000
PB	0.966	62	0.084
CA	0.828	62	0.000
Password	0.951	62	0.015
Incident	0.960	62	0.039
Email	0.887	62	0.000
Mobile	0.931	62	0.002

most of the dependent variables (65 out of 93 ie representing about 70%), were adequately correlated, indicating the appropriateness of a MANOVA in terms of multicoloniality.
As shown in Table 6, descriptive statistics were generated for the dependent variables across the group. From the results, the mean values of the risk of security practice of the various dependent variables in the control group were generally higher than that of the experiment group.

For a better and more effective assessment, Box's test of equality of covariance matrices was generated. Box's test is used to assess the null hypothesis that the observed covariance matrices of the dependent variables are equal across all groups. From the results, the established value of Box M was 153.081 at a significance level of p-value = 0.243, suggesting non-significant. According to the guideline of Huberty et al., the significant p-value should be p ¿ 0.005 [89] to signify the existence of the same in the covariance metrics across the group. Therefore, we fail to reject the null hypothesis that the observed covariance matrices of the dependent variables are equal across the control group and the experiment group.

Following this, a one-way multivariate analysis of variance (MANOVA) was performed to assess the hypothesis that there would be one or more

Table 5: Correlation

	AB	K	A	IB	PV	PS	SE	RE	PB	CA	PW	IR	E	M
AB	–													
K	-.371**	–												
A	-0.021	.500**	–											
IB	-0.050	.515**	.468**	–										
PV	0.010	0.133	.261*	.293**	–									
PS	0.227	-0.159	0.213	.297**	.383**	–								
SE	0.090	.440**	0.067	.432**	0.030	0.062	–							
RE	-0.090	.336**	.257*	.407**	.319**	0.148	.366**	–						
PB	0.113	-.328**	-0.209	-.401**	-0.147	-0.128	-.323**	-0.108	–					
CA	0.041	0.149	0.074	.337**	0.126	0.173	.537**	0.146	-.336**	–				
PW	0.041	.390**	.394**	.642**	0.217	.243*	0.158	0.172	-.264*	0.133	–			
IR	-0.175	.495**	.658**	.637**	.291**	.272*	0.156	.232*	-.330**	0.182	.383**	–		
E	-0.027	.538**	.402**	.655**	0.076	0.150	.431**	.356**	-0.204	.236*	.353**	.335**	–	
M	-0.208	.683**	.382**	.479**	0.050	-0.019	.505**	.350**	-.362**	0.148	0.210	0.133	.463**	–

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed). c. Listwise N = 62 PW=Password
E=Email use
M=Mobile device and SMS use IR=Incident reporting

mean differences between the control and the experiment groups among the dependent variables if the significance level of the p-value is less than 0.05. A statistically significant result of the MANOVA effect was obtained. Since Wik's lambda is used to interpret the results if all the assumptions of the MANOVA test are met, Pillais' Trace was rather used since there were uncertainties in some of the assumptions of our data, as shown in Table 4. The value of the Pillais' Trace was 0.442, F(14,47) = 2.660 and p-value = 0.006(p-value ¡ 0.05). This suggests the existence(s) of group difference(s) at the significance level [90]. The estimated multivariate effect size was at 0.442, which suggests that 44.2% of the variance in the derived dependent variable was accounted for by the group level. Essentially, based on Pillai's Trace results, there is a statistical significance difference across the levels of the independent variable on a lin-

Table 6: Descriptive statistics of dependent variables across groups

DV	Group	Mean	Std. Deviation	N
AB	Control	3.93	1.799	30
	Experiment	2.75	2.016	32
K	Control	1.82	0.412	30
	Experiment	1.81	0.494	32
A	Control	1.79	0.338	30
	Experiment	1.62	0.541	32
IB	Control	1.92	0.371	30
	Experiment	1.73	0.463	32
PV	Control	2.09	0.711	30
	Experiment	1.85	0.871	32
PS	Control	2.07	0.719	30
	Experiment	1.41	0.534	32
SE	Control	2.75	0.650	30
	Experiment	2.45	0.672	32
RE	Control	1.40	0.395	30
	Experiment	1.41	0.534	32
PB	Control	3.35	0.842	30
	Experiment	3.34	0.689	32
CA	Control	2.98	0.517	30
	Experiment	2.55	0.787	32
Password	Control	1.82	0.482	30
	Experiment	1.67	0.590	32
Incident	Control	2.39	0.708	30
	Experiment	2.07	0.766	32
Email	Control	1.60	0.430	30
	Experiment	1.49	0.523	32
Mobile	Control	1.65	0.355	30
	Experiment	1.65	0.471	32

ear combination of the dependent variables. To determine for the dependent variables that have a significant difference across the groups, a homogeneity test of variance was undertaken. The homogeneity of variance assumption was tested with Levene’s test of equality of error of variances for all the fourteen dependent variables across the control and experiment groups. It tests the null hypothesis that the error variance of the dependent variable is equal across the control and experiment groups. Based on test statistics, the homogeneity of variance assumption was considered satisfied, even though two (AB, CA) of the fourteen Levene’s F tests were statistically significant (p ¡ 0.05). Specifically, although Levene’s F test suggested that the variances associated with the actual behaviour, cues to action and sub-scales were not homogeneous, an analysis of the standard deviations as shown in 6 showed that none of the largest standard deviations is four times greater than the size of the corresponding smallest value. This indicates that the analysis of variance will be reliable [91].

Furthermore, various one-way ANOVA test were performed on each of the fourteen dependent variables. This was a further test in addition to the

MANOVA. As shown in Table 7, the ANOVA's of actual behaviour (AB), perceived severity and cues to action were statistically significant, with the respective effect sizes of 9.0%, 22.1% and 9.9%.

Table 7: Analysis of variance(ANOVA) results

	Sum of Squares	df	Mean Square	F	sig.	Partial Eta Squared	Noncent. Parameter	
AB	21.682	1	21.682	5.917	**0.018**	0.090	5.917	0.668
K	0.003	1	0.003	0.013	0.911	0.000	0.013	0.051
A	0.452	1	0.452	2.186	0.144	0.035	2.186	0.307
IB	0.572	1	0.572	3.223	0.078	0.051	3.223	0.423
PV	0.853	1	0.853	1.340	0.252	0.022	1.340	0.207
PS	6.753	1	6.753	17.020	**0.000**	0.221	17.020	0.982
SE	1.365	1	1.365	3.116	0.083	0.049	3.116	0.412
RE	0.001	1	0.001	0.003	0.959	0.000	0.003	0.050
PB	0.003	1	0.003	0.005	0.943	0.000	0.005	0.051
CA	2.950	1	2.950	6.574	**0.013**	0.099	6.574	0.713
Password	0.325	1	0.325	1.110	0.296	0.018	1.110	0.179
Incident	1.652	1	1.652	3.028	0.087	0.048	3.028	0.402
Email	0.183	1	0.183	0.792	0.377	0.013	0.792	0.141
Mobile	0.000	1	0.000	0.000	0.992	0.000	0.000	0.050

Discussion

Following the high susceptibility in phishing-related attacks [5], this study explored some psychological incentives toward mitigating the susceptibility in healthcare IT infrastructures. Specifically, a controlled experiment was conducted to determine the effectiveness of cognitive dissonance in preventing or mitigating the vulnerability among healthcare staff in terms of actual phishing attacks. Additionally, the effect of cognitive dissonance was assessed on perceptions and other security practices such as email use, mobile computing, incident reporting and password management. Furthermore, the influence of cognitive dissonance on self reported knowledge, attitude and behaviour was also assessed.

Principal findings

Having assessed the study to meet various assumptions relating to multivariate analysis (MANOVA), the data were subsequently analysed. In the control group, the click rate was 22 out of the 34 participants, which represents 65%. Meanwhile, the click rate in the experiment group was 14 out of the 32 participants representing 44%. Additionally, the click rate in the neutral group in the phishing simulation attack was 432 out of 819, thus representing 53%. The click rate in the experiment group was comparatively lower as compared to the experiment group as shown in Figure 3. Aside from this, the descriptive statistics of the dependent variables showed that the mean value of the phishing susceptibility risks was comparatively higher in the control group as shown in Table 6. Based on these the experiment group has recorded the lowest risk in terms of phishing susceptibility in the experiment group. However, this could be assessed better with MANOVA tests to determine the treatment effect of cognitive dissonance with the experiment group.

From Pillais' Trace assessment in MANOVA, the test also indicated the existence of group difference between the control group and the experiment group with the value of 0.442, F(14,47) = 2.660 at p-value = 0.006 (pvalue ¡ 0.05). A further assessment with ANOVA's test revealed significant group differences in the AB, PS and CA as shown in Table 7. This supports our study hypotheses of H1, H4 and H8 respectively. The self-reported behaviour of participants (IB), SE

and incident reporting also recorded a nearly significant difference across the groups with a p-value = 0.078, 0.083 and 0.087 however, none of these significantly supported their respective hypotheses. On the aspect of H1, most of the participants in the experiment group might have been influenced by the cognitive dissonance treatment to decide not to click the link. Guided with cues to action in phishing security practice, the participants in the experiment group might have first suspected the maliciousness of the email based on the phishing clues. So the thought of whether to click the link or not would set in. If the participant already knew that clicking suspicious emails violates security rules, and has the cognition of the treatment, he or she may resolve not to click the link. Whereas in the control group, most of the participants might have rationalized clicking the link since they were not exposed to the cognitive dissidence treatment.

Aside from these, the average click rate of the three groups was over 50%. This is deemed high and might have been influenced by the phishing campaign message as shown in appendix Appendix B. Because of the ongoing war between Ukraine and Russia, the phishing message was highly related to that. Moreover, due to the proximity of these countries, it might have been difficult for many participants to ignore the message which resulted in a high click rate. In anyways, these are the methods often used by cyber criminals to deceive their victims into clicking the malicious links
[92].

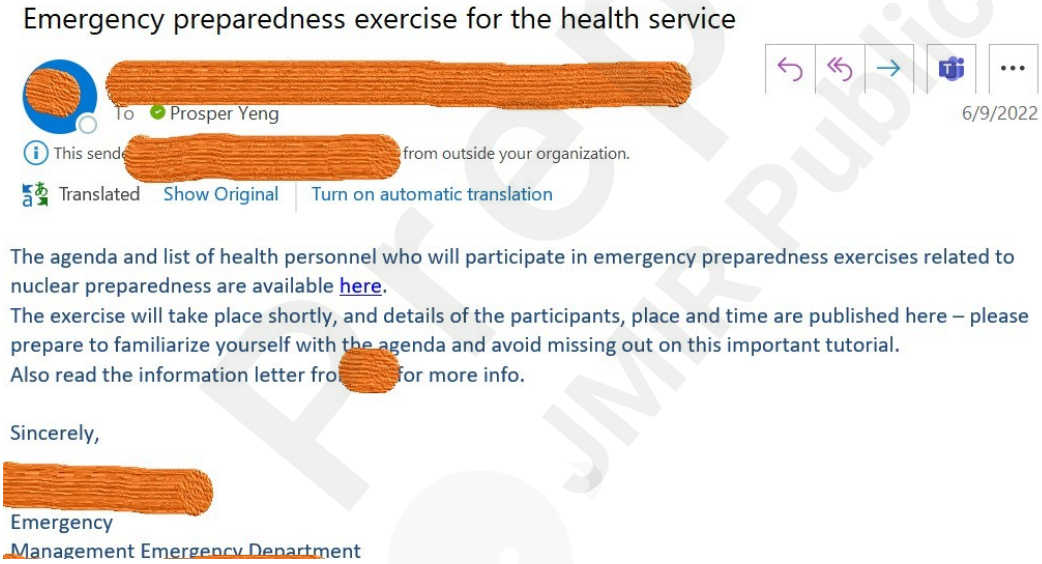

Figure 4: Phishing attack simulation message

While the investigation showed that cognitive dissonance has a positive influence in reducing the actual clicking risk (AB) of participants, the findings however did not show a meaningful effect on the self-reported intended behaviour (IB). A related study also discovered the insignificant relationship between self-reported phishing clicking behaviour and the actual clicking behaviour of participants [27]. This could mean that the IB risk of participants in the experiment group, differs from their AB risk. The reason could be that what users reports on their intended behaviour having been treated with cognitive dissonance might not be exactly translated into their actual practice. For instance, people may report that their behaviour to phishing susceptibility is

less risky but they may be susceptible to a real attack. Management should therefore be conscious of this and try to put in all necessary measures towards reducing phishing susceptibility.

Furthermore, this assessment also supported H4, on PS. The findings imply that cognitive dissonance exhibited a significant effect in the experiment group as compared to the control group with regard to perceived severity. This, therefore, translates that when healthcare staff are treated with cognitive dissonance, their perceived behavioural risk in phishing susceptibility is comparatively reduced. Related assessments in general cyber security researchers also found a significant positive effect of perceived severity towards enhancing cyber security practice in healthcare [93, 49]. It might be the case that through the lenses of cognitive dissonance, the participants in the experiment group reflected better on the severity of the impact of a possible cyber attack if the security measures are violated. That might have resulted in a low susceptibility rate in the experiment group.
Additionally, CA was also comparatively significant in the experiment group, which therefore supported hypothesis HB in this paper. Since CA are precursors or sources of knowledge that influences good behaviour, the effect of cognitive dissonance might have possibly influenced the cues to action by influencing the participants to add more positive pair of knowledge that is consonant to each other. For instance, one of the CA's items was that "I have been offered training/ courses in information security over the past two years". If the participants in the experiment group had better cyber security training that improved their phishing-related security knowledge, coupled with the treatment effect of cognitive dissonance, the combined efforts might have translated into less risky behaviour in the experiment group. Even though related studies did not show a significant effect between cues to action and self-reported general cyber security behaviour in related studies, [45, 47, 8].

Practical implication

This research highlights an average susceptibility rate of approximately 50% in the phishing simulation attack conducted at one of Norway's largest hospitals. Despite the presence of technical security measures that prevent or filter out malicious emails, there remains a significant risk of employees clicking on phishing emails if they manage to bypass these controls. This study serves as a wake-up call for hospital management to continually enhance their anti-phishing security measures, particularly in the human aspect.
Fortunately, the findings demonstrate a lower susceptibility risk of actual phishing click behavior among healthcare staff in the experiment group. Therefore, management should consider adopting cognitive dissonance as a strategy to mitigate phishing vulnerabilities in the human aspect. Moreover, the study reveals that perceived severity plays a significant role in reducing phishing susceptibility when combined with cognitive dissonance. Management can leverage this knowledge to emphasize the potential severity of phishing attacks and incorporate cue-to-action measures alongside cognitive dissonance. By combining social engineering-related training, education, and learning (TEL) techniques with psychological incentives like cognitive dissonance, hospital management can effectively reduce phishing susceptibility among healthcare staff.

To effectively instil psychological incentives in healthcare staff, management should explore the use of state-of-the-art training, education, and learning technologies, such as virtual reality (VR) and mixed reality (MR). These immersive technologies have proven to be more effective than traditional approaches, as they engage and motivate participants, reduce stress levels, and improve understanding and cognition. Additionally, immersive systems aid participants in developing patterns and enhance the retention of learned content in memory [94].

It is worth noting that despite inviting a significant number of participants, only a few of them actively participated in the study even after several follow-ups. Future research should explore alternative measures to increase participation rates. Additionally, the study was limited by the overall participation rate, which affected the ability to conduct certain analyses like structural equation modelling, which typically requires a minimum of 100 participants. Consequently, our analysis was constrained, preventing a comprehensive assessment of causality using structural equation modelling.

Conclusion

To address the susceptibility of healthcare staff to phishing attacks, a controlled experiment was conducted as part of an in-the-wild field study. The aim of the experiment was to investigate the effectiveness of cognitive dissonance and other psychological factors as intrinsic incentives for reducing phishing susceptibility.

A total of approximately 830 doctors and nurses were invited to participate in the study and were randomly assigned to either the control or experiment group. In the first stage, participants were asked to complete a
survey to self-report their phishing security practices. Subsequently, in the second stage, a phishing simulation attack was carried out. Out of the initial participant pool, 82 individuals (9.8%) completed the first stage, with 42 participants in the control group and 40 participants in the experiment group. A phishing simulation email was then sent to 34 participants in the control group and 32 participants in the experiment group.

To analyze the data and meet the requirements of multivariate analysis of variance (MANOVA), a Pillais' Trace assessment was conducted, resulting in a value of 0.442, F(14,47) = 2.660, and a p-value of 0.006 (pvalue ¡ 0.05). These findings indicated a statistically significant difference across some or all levels of the independent variables between the groups. Furthermore, separate one-way ANOVA tests were performed for each dependent variable, revealing a significant difference between the groups in terms of actual behavior (AB), perceived severity, and cues to action.

Based on these findings, it can be concluded that cognitive dissonance, in combination with other psychological factors such as perceived severity and cues to action, can serve as effective intrinsic incentives for reducing phishing susceptibility during real attacks. Future research should explore the utilization of state-of-the-art training, education, and learning tools, such as virtual and mixed realities, to promote the adoption of these psychological incentives among healthcare staff.

Table A.8: Nature of questionnaire

#	Item	Construct
1	I know that my password and username can be stolen by phishing attacks	
2	I think it is unnecessary to use two or more proofs (multi-factor authentication) such as passwords and codes on SMS to gain access to a website.	KAB with password management [95, 47, 96]
3	I prefer NOT to use two or more proofs (multi-factor authentication) such as passwords and code on SMS to access a website.	
4	I think it is necessary to report suspicious e-mails or SMS	
5	I do NOT report suspicious emails or SMS	
6	I know that I should not ignore my colleagues' poor information security practices at, for example, nursing home	KAB with incident reporting [95, 47, 96]
7	I know that it is not good information security practice to click on a link in an email from an unknown sender	
8	I know I can download malicious email attachments, especially from unknown senders	
9	I don't think there is anything wrong with downloading an email attachment without checking the sender	KAB with email use [95, 47, 96]
10	I always check the source or sender before I download an email attachment	
11	It is important to pay close attention to phishing attempts	
12	I do NOT pay close attention to phishing attempts	
13	I have the skills to identify malicious or suspicious links on the hospital mobile phone	
14	It is not a bad idea to send sensitive information via voice or SMS	KAB with mobile phone use [95, 47, 96]
15	I may sometimes send sensitive information via voice or SMS	
16	I can identify malicious phones in the hospital	
17	I feel that the chance of receiving an email with a virus attached is high.	
18	I feel that my chance of receiving malware via social media is high.	Perceived vulnerability [97, 47, 95]
19	I believe that my efforts to protect the organization's information will reduce illegal access.	
20	Loss of data as a result of hacking is a serious problem for me.	
21	If someone gets access to confidential information about me without my consent or that I know it is a serious problem for me.	Perceived severity [95, 47]
22	If my PC is infected by a virus as a result of a suspicious e-mail attachment being opened, this is a serious problem for me.	
23	I know how to identify phishing emails	
24	I can create strong passwords on my IT system	Self efficacy [7, 98, 47]
25	I can reveal voice-based phishing attempts	
26	Compliance with the information security practices in my organization helps to minimize security breaches	Perceived barrier
27	If I comply with good information security practices, the chance of an information security breach/attack will be reduced	
28	Good information security practices help to avoid security breaches.	
29	I have been offered training/courses in information security over the past two years	Cuest to action

Appendix A. Questionnaire

Appendix A.1. Questionnaire instrument

Appendix B. Cognitive dissonance message

Appendix B.1. Cognitive dissonance message for experiment group

Phishing attacks are a method that cybercriminals use to trick innocent users into clicking on links with the aim of stealing sensitive information or breaching privacy. Through phishing, cybercriminals can block access to health data or the entire network, and demand a ransom to unlock access. This is known as ransomware. The integrity of the patient's information can be deleted or changed, so one cannot trust that the information is correct when providing healthcare. Cyber-attacks can lead to a loss of trust from patients, large fines from regulatory authorities and, in the worst-case scenario, can lead to the loss of patients' lives. Based on this information, all employees in the health sector have to follow good routines within cyber security, to ensure that their actions and attitudes are free of risk. Although most people have good security awareness, sometimes they decide to break security requirements, where they have various excuses that justify the actions, such as ”nothing bad can happen”, ”no one will know or see it”, ”it is a one-off”, ”this is not malicious”. These are examples of behaviour that contribute to increasing the number of cyber attacks in the healthcare sector.

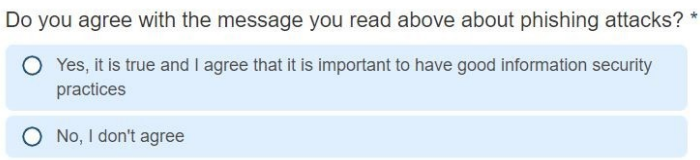

Figure B.5: Cognitive dissonance message for experiment group

References

[1] J. Van Gemert-Pijnen, O. Peters, H. C. Ossebaard, Improving ehealth, Eleven international publishing The Netherlands, 2013.

[2] T. D. Swig, Cybersecurity news and views:latest healthcare breaches and security news (April 2022).
URL hhttps://portswigger.net/daily

[3] J. Haworth, Uk government employees receive ‘billions’ of malicious emails per year – report (April 2022).
URL https://portswigger.net/daily-swig/uk-government-employees-receive-billions-ofmalicious-emails-per-year-report

[4] A. Georgiadou, A. Michalitsi-Psarrou, F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gounaris, G. Doukas, C. Ntanos, L. Landeiro Ribeiro, D. Askounis, Hospitals’ cybersecurity culture during the covid-19 crisis, in: Healthcare, Vol. 9, MDPI, 2021, p. 1335.

[5] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, L. Coventry, Phishing simulation exercise in a large hospital: A case study, Digital Health 8 (2022) 20552076221081716.

[6] B. Y. Prosper Yeng, Muhammad Ali Fauzi, P. Nimbe, Investigation into phishing risk behaviour among healthcare staff, MPDI Information 13 (8) (2022) 392. doi:https://doi.org/10.3390/info13080392.

[7] H.-S. Rhee, C. Kim, Y. U. Ryu, Self-efficacy in information security: Its influence on end users’ information security practice behavior, Computers & security 28 (8) (2009) 816–826.

[8] P. K. Yeng, M. A. Fauzi, B. Yang, Assessing the effect of human factors in healthcare cyber security practice: An empirical study, in: 25th Pan-Hellenic Conference on Informatics, 2021, pp. 472–476.

[9] I. SINGH, Y. SINGH, Cyber-security knowledge and practice of nurses in private hospitals in northern durban, kwazulu-natal, Journal of Theoretical and Applied Information Technology 100 (1) (2022).

[10] J. B. Barlow, M. Warkentin, D. Ormond, A. Dennis, 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 (8) (2018) 3.

[11] A. C. Johnston, M. Warkentin, M. Siponen, An enhanced fear appeal rhetorical framework, MIS quarterly 39 (1) (2015) 113–134.

[12] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness, MIS quarterly (2010) 523–548.

[13] C. L. Anderson, R. Agarwal, Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions, MIS quarterly (2010) 613–643.

[14] ISO, Iso 27799:2016(en), health informatics information security management in health

using iso/iec 27002 (November 2016). URL https://www.iso.org/standard/62777.html
[15] P. Ministry of Culture, The great wall of china (November 2009). URL http://en.chinaculture.org/focus/focus/2010expo_en/2010-04/19/content_376769_3.html
[16] L. E. Fisher, The great wall of China, Simon and Schuster, 1995.
[17] F. Kafka, The great wall of china., Commentary 2 (1946) 368.
[18] P. K. Yeng, B. Yang, E. A. Snekkenes, Healthcare staffs' information security practices towards mitigating data breaches: A literature survey, pHealth 2019 (2019) 239–245.
[19] P. K. Yeng, B. Yang, E. A. Snekkenes, Framework for healthcare security practice analysis, modeling and incentivization, in: 2019 IEEE International Conference on Big Data (Big Data), IEEE, 2019, pp. 3242– 3251.
[20] P. Yeng, B. Yang, E. Snekkenes, Observational measures for effective profiling of healthcare staffs' security practices, in: 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Vol. 2, IEEE, 2019, pp. 397–404.
[21] L. Festinger, A theory of cognitive dissonance, Vol. 2, Stanford university press, 1957.
[22] J. M. Jarcho, E. T. Berkman, M. D. Lieberman, The neural basis of rationalization: cognitive dissonance reduction during decisionmaking, Social cognitive and affective neuroscience 6 (4) (2011) 460– 467.
[23] J. B. Barlow, M. Warkentin, D. Ormond, A. R. Dennis, Don't make excuses! discouraging neutralization to reduce it policy violation, Computers & security 39 (2013) 145–159.
[24] M. Siponen, A. Vance, Neutralization: New insights into the problem of employee information systems security policy violations, MIS quarterly (2010) 487–502.
[25] A. Vance, M. T. Siponen, D. W. Straub, Effects of sanctions, moral beliefs, and neutralization on information security policy violations across cultures, Information & Management 57 (4) (2020) 103212.
[26] M. Abdelhamid, et al., The role of health concerns in phishing susceptibility: Survey design study, Journal of medical Internet research 22 (5) (2020) e18394.
[27] M. S. Jalali, M. Bruckes, D. Westmattelmann, G. Schewe, Why employees (still) click on phishing links: investigation in hospitals, Journal of medical Internet research 22 (1) (2020) e16775.
[28] E. Harmon-Jones, J. Mills, An introduction to cognitive dissonance theory and an overview of current perspectives on the theory. (2019).
[29] I. M. Rosenstock, The health belief model and preventive health behavior, Health education monographs 2 (4) (1974) 354–386.
[30] S. Prentice-Dunn, R. W. Rogers, Protection motivation theory and preventive health: Beyond the health belief model, Health education research 1 (3) (1986) 153–161.
[31] U. Hasan, Cognitive dissonance and its impact on consumer buying behaviour, IOSR Journal of Business and Management 1 (2012) 7–12.
[32] G. M. Sykes, D. Matza, Techniques of neutralization: A theory of delinquency, American sociological review 22 (6) (1957) 664–670.
[33] R. Willison, Understanding the perpetration of employee computer crime in the organisational context, Information and organization 16 (4) (2006) 304–324.
[34] M. Offei, F. K. Andoh-Baidoo, E. W. Ayaburi, D. Asamoah, How do individuals justify and rationalize their criminal behaviors in online romance fraud?, Information Systems Frontiers (2022) 1–17.
[35] M. A. Freeman, E. V. Hennessy, D. M. Marzullo, Defensive evaluation of antismoking messages among college-age smokers: the role of possible selves., Health psychology 20 (6) (2001) 424.
[36] V. Fointiat, Saying, but not doing: Induced hypocrisy, trivialization, and misattribution,

Social behavior and personality: An international journal 39 (4) (2011) 465–475.
[37] L. V. Brown, Psychology of motivation, Nova Publishers, 2007.
[38] B. Lebek, N. Guhr, M. Breitner, Transformational leadership and employees' information security performance: the mediating role of motivation and climate (2014).
[39] T. Herath, H. R. Rao, Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, Decision Support Systems 47 (2) (2009) 154–165.
[40] K. Padayachee, An insider threat neutralisation mitigation model predicated on cognitive dissonance (itnmcd), South African Computer Journal 56 (1) (2015) 50–79.
[41] J. Taylor-Jackson, J. McAlaney, J. L. Foster, A. Bello, A. Maurushat, J. Dale, Incorporating psychology into cyber security education: a pedagogical approach, in: International Conference on Financial Cryptography and Data Security, Springer, 2020, pp. 207–217.
[42] M. F. Cazares, D. Arevalo, R. O. Andrade, W. Fuertes, M. S´ anchez-´ Rubio, A training web platform to improve cognitive skills for phishing attacks detection, in: Intelligent Sustainable Systems, Springer, 2022, pp. 33–42.
[43] Y. Chen, K. Ramamurthy, K.-W. Wen, Organizations' information security policy compliance: Stick or carrot approach?, Journal of Management Information Systems 29 (3) (2012) 157–188. arXiv:https://doi.org/10.2753/MIS0742-1222290305, doi:10.2753/MIS0742-1222290305.
URL https://doi.org/10.2753/MIS0742-1222290305
[44] Y. Chen, W. Xia, K. Cousins, Voluntary and instrumental information security policy compliance: an integrated view of prosocial motivation, self-regulation and deterrence, Computers & Security 113 (2022) 102568.
[45] P. K. Yeng, M. A. Fauzi, B. Yang, A comprehensive assessment of human factors in cyber security compliance toward enhancing the security practice of healthcare staff in paperless hospitals, Information 13 (7) (2022) 335.
[46] V. L. Champion, C. S. Skinner, et al., The health belief model, Health behavior and health education: Theory, research, and practice 4 (2008) 45–65.
[47] B.-Y. Ng, A. Kankanhalli, Y. C. Xu, Studying users' computer security behavior: A health belief perspective, Decision Support Systems 46 (4) (2009) 815–825.
[48] P. K. Yeng, A. Szekeres, B. Yang, E. A. Snekkenes, Mapping the psychosocialcultural aspects of healthcare professionals' information security practices: Systematic mapping study, JMIR human factors 8 (2) (2021) e17604.
[49] N. Humaidi, V. Balakrishnan, M. Shahrom, Exploring user's compliance behavior towards health information system security policies based on extended health belief model, in: 2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e), IEEE, 2014, pp. 30–35.
[50] J. Mou, J. F. Cohen, A. Bhattacherjee, J. Kim, A test of protection motivation theory in the information security literature: A meta-analytic structural equation modeling approach, Journal of the Association for Information Systems 23 (1) (2022) 196–236.
[51] P. Ifinedo, Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory, Computers and Security 31 (1) (2012) 83–95.
[52] P. K. Yeng, B. Yang, E. A. Snekkenes, Healthcare staffs' information security practices towards mitigating data breaches: A literature survey, Studies in health technology and informatics 261 (2019) 239–245.
[53] K. J. Slonka, B. F. Shrift, Phishing our clients: A step toward improving training via social engineering., Issues in Information Systems 17 (1) (2016).

[54] W. J. Gordon, A. Wright, R. J. Glynn, J. Kadakia, C. Mazzone, E. Leinbach, A. Landman, Evaluation of a mandatory phishing training program for high-risk employees at a us healthcare system, Journal of the American Medical Informatics Association 26 (6) (2019) 547–552.
[55] S. Deutsch Salamon, Trust that binds: The influence of collective felt trust on responsibility norms and organizational outcomes, Ph.D. thesis, University of British Columbia (2003).
[56] P. Sparks, C. A. Guthrie, R. Shepherd, The dimensional structure of the perceived behavioral control construct 1, Journal of applied social psychology 27 (5) (1997) 418–438.
[57] D. Trafimow, K. A. Finlay, The importance of subjective norms for a minority of people: Between subjects and within-subjects analyses, Personality and social psychology bulletin 22 (8) (1996) 820–828.
[58] W. J. Gordon, A. Wright, R. Aiyagari, L. Corbo, R. J. Glynn, J. Kadakia, J. Kufahl, C. Mazzone, J. Noga, M. Parkulo, et al., Assessment of employee susceptibility to phishing attacks at us health care institutions, JAMA network open 2 (3) (2019) e190393–e190393.
[59] W. Priestman, T. Anstis, I. G. Sebire, S. Sridharan, N. J. Sebire, Phishing in healthcare organisations: Threats, mitigation and approaches, BMJ health & care informatics 26 (1) (2019).
[60] N. Athanassoulis, J. Wilson, When is deception in research ethical?, Clinical Ethics 4 (1) (2009) 44–49.
[61] R. Salah El-Din, To deceive or not to deceive! ethical questions in phishing research (2012).
[62] J. E. Sieber, Deception in social research i: Kinds of deception and the wrongs they may involve, IRB: Ethics & Human Research 4 (9) (1982) 1–5.
[63] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, C. Jerram, The development of the human aspects of information security questionnaire (hais-q) (2013).
[64] N. University of Oslo, Nettskjema: Surveys, registrations and orders (Mar. 2021). URL https://nettskjema.no/?lang=en
[65] E. Mullet, G. Chasseigne, Assessing information integration processes: A comparison of findings obtained with between-subjects designs versus within-subjects designs, Quality & Quantity 52 (4) (2018) 1977–1988.
[66] A. J. Berinsky, M. F. Margolis, M. W. Sances, Separating the shirkers from the workers? making sure respondents pay attention on selfadministered surveys, American Journal of Political Science 58 (3) (2014) 739–753.
[67] J. L. Huang, N. A. Bowling, M. Liu, Y. Li, Detecting insufficient effort responding with an infrequency scale: Evaluating validity and participant reactions, Journal of Business and Psychology 30 (2) (2015) 299–311.
[68] F. Y. Kung, N. Kwok, D. J. Brown, Are attention check questions a threat to scale validity?, Applied Psychology 67 (2) (2018) 264–283.
[69] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, T. Zwaans, The human aspects of information security questionnaire (hais-q): two further validation studies, Computers & Security 66 (2017) 40–51.
[70] S. D. Gosling, P. J. Rentfrow, W. B. Swann Jr, A very brief measure of the big-five personality domains, Journal of Research in personality 37 (6) (2003) 504–528.
[71] getgophish, Open-source phishing framework (January 2022). URL https://getgophish.com/
[72] D. P. Paul III, N. Spence, N. Bhardwa, C. D. PH, et al., Healthcare facilities: another target for ransomware attacks (2018).
[73] B. Marczak, J. Scott-Railton, N. Al-Jizawi, S. Anstis, R. Deibert, The great ipwn: Journalists

hacked with suspected nso group imessage ‘zero-click’exploit, Tech. rep. (2020).
[74] kaspersky, What is zero-click malware, and how do zero-click attacks work? (December 2022).
URL https://www.kaspersky.com/resource-center/ definitions/what-is-zero-click-malware

[75] D. Akhawe, A. P. Felt, Alice in warningland: a large-scale field study of browser security warning effectiveness, in: 22nd USENIX Security Symposium (USENIX Security 13), 2013, pp. 257–272.

[76] H. Coolican, Research methods and statistics in psychology, Psychology press, 2017.
[77] I. Asklund, E. Nystrom, M. Sj¨ ostr¨ om, G. Umefjord, H. Stenlund,¨ E. Samuelsson, Mobile app for treatment of stress urinary incontinence: a randomized controlled trial, Neurourology and urodynamics 36 (5) (2017) 1369–1376.
[78] A. French, M. Macedo, J. Poulsen, T. Waterson, A. Yu, Multivariate analysis of variance (manova) (2008).
[79] C. W. VanVoorhis, B. L. Morgan, et al., Understanding power and rules of thumb for determining sample sizes, Tutorials in quantitative methods for psychology 3 (2) (2007) 43–50.
[80] P. Julie, Spss survival manual-a step by step guide to data analysis using spss (2011).
[81] N. A. G. Arachchilage, S. Love, A game design framework for avoiding phishing attacks, Computers in Human Behavior 29 (3) (2013) 706–714.
[82] A. Shamsuddin, M. Shah, B. M. Shah, Perception of managers on the effectiveness of the internal audit functions: A case study in tnb, 2015.
[83] J. F. Hair, M. Page, N. Brunsveld, Essentials of business research methods, Routledge, 2019.
[84] J. Pallant, Spss survaival manual: a step by step guide to data analysis using spss (2010).
[85] S. R. Briggs, J. M. Cheek, The role of factor analysis in the development and evaluation of personality scales, Journal of personality 54 (1) (1986) 106–148.
[86] J. J. Vaske, J. Beaman, C. C. Sponarski, Rethinking internal consistency in cronbach’s alpha, Leisure Sciences 39 (2) (2017) 163–173.
[87] M. A. Pourhoseingholi, A. R. Baghestani, M. Vahedi, How to control confounding effects by statistical analysis, Gastroenterology and hepatology from bed to bench 5 (2) (2012) 79.

[88] L. S. Meyers, G. Gamst, A. J. Guarino, Applied multivariate research: Design and interpretation, Sage publications, 2016.

[89] H. E. Tinsley, S. D. Brown, Multivariate statistics and mathematical modeling, in: Handbook of applied multivariate statistics and mathematical modeling, Elsevier, 2000, pp. 3–36.

[90] K. S. Pillai, Some new test criteria in multivariate analysis, The Annals of Mathematical Statistics (1955) 117–121.

[91] D. Howell, Statistical methods for psychology . belmont, ca: Thomson learning (2007).

[92] A. K. Jain, B. Gupta, A survey of phishing attack techniques, defence mechanisms and open research challenges, Enterprise Information Systems 16 (4) (2022) 527–565.

[93] B. Samhan, Security behaviors of healthcare providers using hit outside of work: A technology threat avoidance perspective, in: 2017 8th International Conference on Information and Communication Systems (ICICS), IEEE, 2017, pp. 342–347.

[94] A. G. Gallagher, C. U. Cates, Virtual reality training for the operating room and cardiac catheterisation laboratory, The Lancet 364 (9444) (2004) 1538–1540.

[95] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, L. Xu, Gender difference and employees' cybersecurity behaviors, Computers in Human Behavior 69 (2017) 437–443.

[96] D.-H. Shih, B. Lin, H.-S. Chiang, M.-H. Shih, Security aspects of mobile phone virus: a critical survey, Industrial Management & Data Systems (2008).

[97] N. Mohamed, I. H. Ahmad, Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from malaysia, Computers in Human Behavior 28 (6) (2012) 2366–2375.

[98] P. Ifinedo, Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition, Information & Management 51 (1) (2014) 69–79.