Erasmus University Rotterdam

MSc Economics & Business, specialization in Behavioral Economics

Nudging Secure Digital Behavior

Nudging the use of EduVPN

Agorasti Patronidou

Student Number: 613903

Supervisor: Sophie van der Zee & Rory O'Connor

Second assessor: Han Bleichrodt

July 2022

Abstract

In the past few years, cyberattacks have become more and more intricate and frequent, indicating the need for stronger and more sophisticated measures of cyber security (Dias et al., 2022). Organizations choose to prioritize cyber security by implementing and maintaining security tools such as Virtual Private Networks (VPNs), Multi-factor Authentication (MFA) systems, antivirus software, etc. Particularly, VPNs enable users to exchange data across different networks just as though their devices were directly connected to one private network. Although VPNs are clearly helpful and can be used to prevent certain types of cybercrime, users do not use them. The field experiment of this study utilizes the insights of Nudge Theory to promote the download and use of EduVPN among 1337 MSs' students at the Erasmus University Rotterdam. Based on the existing literature, students received an email combining information provision and a nudge. The nudges tested were social norms, priming, and self-commitment. All students who had not yet installed EduVPN by the seventh day of the experiment, received a simple, email-based reminder one week later, testing whether there are differences across the four initial nudge groups. The results suggest that the self-commitment nudge was effective in increasing the downloading rates of EduVPN. The insights from this study, apart from providing evidence of the effectiveness of self-commitment, can also be used to shape the future emails sent by the university and other organisations.

Keywords: Security, Secure Digital Behavior, VPN, Nudging

Dedication and Acknowledgements

This dissertation is dedicated to my family for their endless love, support and encouragement throughout my academic endeavors. They have always been a rock to lean on when things did not work out as planned.

I would also like to thank my supervisors; Sophie van der Zee and Rory O'Connor for making this project possible. The completion of this thesis could not have been achieved without the aid and cooperation of the Security Department of the Erasmus University Rotterdam and particularly Privacy Officer of the department, Floran Pikaar.

Contents

I. Introduction

Over the years, many companies and organizations have prioritized cyber security by implementing strategies to prevent their networks from being compromised and their accounts being hacked (Moor et al., 2015). Craigen et al. (2014) define cyber security as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". Undoubtedly, the high-speed evolution of the internet - although highly beneficial - has loomed serious risks and thus understanding how to securely use it is challenging but vital (Goutam, 2015). Educating and training individuals about cyber security, meeting compliance requirements, and staying ahead of any threats has proved useful, but it is just the first line of defense against cyberattacks (Sjouwerman, 2022; Lock & Freeform Dynamics, 2022).

Among other large organizations, even though not much broadcasted, educational institutions are often victims of cyber criminals (Chapman, 2019). Higher education institutions store not only personal data of students and employees, but also research datasets of great worth (Chapman, 2019). One of the most broadcasted hacks in the Netherlands involved Maastricht University (Fernadez Cras, 2022). Specifically, following a cyberattack in 2019, hackers demanded ransom payment in bitcoins in order to reinstate the servers of the university. Although the hackers were arrested nearly three years after the attack, the university's operations suffered, leading students to lose access to their accounts for a week during the period of the attack. The threat of criminal cyberattacks targeting educational institutions is especially high due to the pandemic, during and after which many people work or study online (Pranggono & Arabo, 2021). As a result, raising awareness for the importance of secure digital behavior can now be considered more vital than ever (European Union Agency for Cybersecurity & e-Governance Academy, 2021).

Technological advances have enabled the creation of tools like **Virtual Private Network (VPN)** which can be used to prevent certain types of cyberattacks (i.e., spyware, external hacking threats, phishing, crypto jacking, etc.) by supplying sufficient encryption to ensure the integrity of data (Singh & Gupta, 2016; 5 Cyber Threats That A VPN Can Handle, 2021). VPN is defined by Ferguson and Huston (1998) as a "private network constructed within a public network infrastructure, such as the global Internet". A VPN enables users to exchange data across different

networks just as though their devices were directly connected to one private network (What Is a VPN?, n.d.). VPNs provide users with the advantage of confidentiality, integrity, and availability through encrypted tunnels of communication (Rahimi & Zargham, 2011). Simply put, VPNs have two major advantages: First, they provide users with internal network institute access and second, they provide users with online security when browsing the internet (EduVPN: Index, n.d.). Therefore, organizations can improve their cyber-security by encouraging the use of VPN amongst employees and in the case of universities, amongst students (Singh & Gupta, 2016).

This study aims to encourage students at the Erasmus University Rotterdam to use the VPN system of the university, EduVPN. The ultimate goal is to increase secure digital behavior at the university. To test how the university can most effectively encourage the uptake of EduVPN amongst students, nudge theory is utilized. Particularly, the most promising nudges according to literature were tested in order to identify the most effective methods of communicating and promoting secure digital behavior to students. The tested nudges were **Social Norms**, **Priming**, and **Self-commitment**. In a separate analysis, this study tests whether there are differences across the initial treatment groups when the participants receive the same simple reminders. Thus, the research question of this study is formed as: "Which nudges are most effective in increasing students' uptake of EduVPN?".

Nudging is defined by Sunstein and Thaler as "any aspect of the choice architecture that alters people's behaviour in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid" (Thaler & Sunstein, 2008). Choice architects use nudges in order to promote a more desired behavior while supplying solutions to obstacles of the decision-making process (Loewenstein & Chater, 2017). In simple words, on occasions, individuals do not consider the option that benefits them the most (Acquisti, 2004). Thus, nudges aim to bring the desired choice to their attention while at the same time not limiting their choices (Sunstein, 2015).

The purpose of this study is to increase the number of students that willingly download and use EduVPN and thus engage in more secure behavior online. Studies addressing nudges for secure digital behavior are available, yet there is no clear evidence on the nudges that could be used to promote the active use of VPN in universities. Such insights will be relevant for all organizations

who wish their members to be secure online and will be especially important in the post-COVID world where many organizations continue to work remotely.

II. Literature review

A. Cyber security and the intention-behavior gap

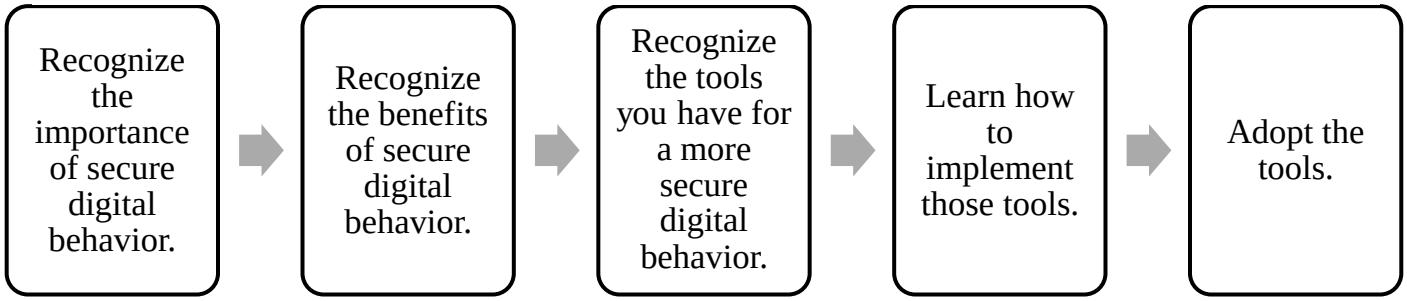
Cybercrime is defined as the crime committed with the use of a computer as a device to enact on unlawful activities (Dennis, 2019). There are various forms of cybercrime, including cyber stalking, intellectual property theft, phishing, and viruses (Goutam, 2015). Cyber criminals often target users' personal information, financial details, or even a combination of both, leading to significantly unpleasant outcomes for the victims (Wall, 2007). Cybercrime, because of its nature, is much more difficult to spot and to prosecute compared to conventional crime (Nykodym et al., 2005). Goutam (2015) states that cyber security is nowadays considered vital for individuals, families, organizations, governments, and educational institutions. Thus, it is of major importance to focus more on their prevention by learning to behave securely online.

A European Commission survey conducted in October 2019 examined Europeans' attitudes towards cyber security and reports that 93% of the respondents changed their online behaviors due to security concerns (European Commission & Kantar Belgium, 2020). Further, 67% of respondents are concerned about falling victims to online banking fraud (European Commission & Kantar Belgium, 2020). European internet users seem to care for their online security and are worried about falling victims of cyberattacks (European Commission & Kantar Belgium, 2020). However, a chasm is evident between users' intentions to behave securely online and their actual behavior, a phenomenon also known as intention-behavior gap (Jenkins et al., 2021).

Ly et al. (2013) argued that it is important to identify the factors that prevent individuals from following through with their intentions (i.e., behaving securely online) as these factors represent the areas where a nudging intervention can prove helpful in "pushing" them to the right direction. They proposed to create a decision map in order to identify these factors that prevent individuals from carrying on with their intentions concerning general decision making. Figure 1 illustrates the decision map users must follow in order to adopt tools for secure digital behavior

(Ly et al., 2013). First, users must recognize the importance of secure digital behavior. Next, they must recognize the benefits of secure digital behavior. The next steps are learning how to adopt tools for secure digital behavior, learning how to implement them, and lastly actually adopting those tools.

Figure 1 - Decision making process for secure digital behavior



Based on Ly, K., Mazar, N., Zhao, M., & Soman, D. (2013). A practitioner's guide to nudging. *Rotman School of Management Working Paper*, (2609347).

Veaudry (2022) conducted a qualitative study aiming to find the barriers individuals create for themselves, preventing them from behaving securely online. Lack of knowledge, cost, time and convenience were some of the barriers found. On some occasions, users may feel like their chances of becoming victims of a cyber-attack are lower than they actually are (Acquisti et al., 2017). Further, taking actions about your online security (e.g., downloading a VPN) takes time and effort (Acquisti et al., 2017). Williams et al. (2018) studied various characteristics that can influence the likelihood of engagement with secure digital behavior. Their results indicate that although tools to support secure digital behavior like VPNs, Multi Factor Authentication (MFA) methods, and Antivirus systems exist, the availability of such tools alone is not enough. Users must also be able and willing to implement them.

Consequently, the identified factors can prevent users from completing the decision steps of Figure 1. These factors also provide an explanation as to why; even though secure digital behavior is vital to prevent cyber-crimes, online users often do not follow through. Overcoming these restrictions can help individuals follow through with their intentions of adopting secure digital behavior tools (Ly et al., 2013). Consequently, interventions aiming to promote secure digital behavior should simultaneously acknowledge intentions, such as effort minimization, which can interfere with security intentions and actual behavior (Jenkins et al., 2021). Failure to bridge the intention-behavior gap in the context of secure digital behavior may have negative consequences by making a system vulnerable to cyber-crimes (Jenkins et al., 2021).

Currently, there is a plethora of tools users can download for online security. VPNs can be considered one of the basic tools users should have when combating cyber-attacks as downloading and using them is relatively easy and does not require any specialized knowledge, but they are also relatively cheap (Sharma & Kaur, 2020). Using a VPN on day-to-day use of the internet, can help prevent certain types of cyber-attacks by providing online privacy (Singh & Gupta, 2016; 5 Cyber Threats That A VPN Can Handle, 2021). However, even though users intent to behave securely online, VPN adoption as a measure of combating cyber-crime, is reported to be relatively low in Europe (European Commission & Kantar Belgium, 2020; Marvin, 2018). In the Netherlands alone, there is approximately only 10% VPN adoption (Kochovski, n.d.).

Ultimately, awareness and intention to behave securely online is not enough; for a real impact in reducing the risk of cyber-threats, behavior change is needed (Bada et al., 2019; How to Create Behavior Change with Security Awareness Training, n.d.). There is a collection of tools for behavior change such as nudges, implementation intentions, "upstream" interventions, and computerized high-repetition training (Papies, 2017). Nudges have been used in various contexts, such as health and exercising habits, as behaviour change interventions in order to bridge the intention-behavior gap and promote more desired actions (Papies, 2017; Kankane et al., 2018). Nudges have begun to be used in law and policy in many countries, with studies finding European citizens supporting this course of action (Reisch & Sunstein, 2016; Reisch et al., 2017).

B. Nudging

Individuals have two distinct modes of thinking (Kahneman, 2011). System 1 is the fast, automatic, emotional mode and System 2 is the slower, logical, calculating mode (Kahneman, 2011). Essentially, System 1 uses heuristics or mental shortcuts to associate pieces of information (Kahneman, 2011). Heuristics are the procedure under which decision-makers arrive at conclusions using what are often called "rules of thumb" (Kahneman, 2011). Although on some occasions heuristics can be helpful, on other occasions, heuristics may lead to "severe and systematic errors" (Tversky et al., 1982). Such systematic errors are also known as cognitive biases, which are "predictable deviations from rationality in judgment or decision-making" (Blanco, 2017). Consequently, on many occasions, people struggle to choose the rational option that would benefit them the most, which also applies on decisions concerning secure digital

behavior (Acquisti, 2004). In such instances, where individuals do not behave rationally, intervening with nudges could potentially aid a more desirable outcome (Sunstein, 2015).

Nudging is defined by Sunstein and Thaler (2008) as the choice architecture tool that adjusts people's behaviour in a foreseeable way without notably altering economic incentives or limiting any other options. Fundamentally, nudges offer *non-monetary incentives* to the decision-makers, in order to prompt them to a more desirable option (Johnson et al., 2012). There is a plethora of alternative nudges to choose from, according to the aim of the intervention (Johnson et al., 2012). Essentially, nudges work by activating automatic cognitive processes to encourage a particular set of choices (Zimmermann & Renaud, 2021). Consequently, nudges can be useful tools to induce desirable behavior (Sunstein, 2015).

Jung and Mellers (2016) highlight the two major advantages of using nudges. Firstly, a nudge intervention does not restrict other options while making others easier to adopt (Jung & Mellers, 2016). Secondly, nudge interventions help individuals to make more desired decisions, as decided by choice architects, while overcoming biases in the decision-making process (Jung & Mellers, 2016). Consequently, one could argue that nudges are persistent with the freedom of choice but also help individuals arrive to more rational decisions (Sunstein, 2015).

Despite their advantages, nudges have faced criticism regarding ethical concerns. Specifically, there are arguments both against the means of nudges (i.e., the techniques used to guide peoples' choices) as well as the aims of nudges (de Quintana Medina, 2021). Essentially, the objectors of nudges argue that nudging does not necessarily push people toward a better direction of choices but rather towards a direction that policy makers want people to make (White, 2013). In simple words, opponents of nudging argue that nudges can eliminate freedom of choice, alter our actions in a way that they are not our own, weaken rationality, and in the wrong hands be a powerful tool to exercise control over individuals' lives (Schmidt & Engelen, 2020).

Yet Sunstein and Thaler (2003) tied the idea of nudging with libertarian paternalism. Libertarian paternalists are those who attempt to steer people's choices in welfare-promoting directions without eliminating freedom of choice" (Sunstein & Thaler, 2003). Therefore, there are two sides to nudging, the paternalistic and the libertarian side (de Quintana Medina, 2021). The paternalistic side aims to change the behavior of individuals to what their judgement appoints to be best for them (Thaler & Sunstein, 2008). Simultaneously, the libertarian side aims to carry out

the aims of the paternalistic side without restricting individuals' original set of choices (Thaler & Sunstein, 2008; de Quintana Medina, 2021).

Additionally, Sunstein and Thaler (2003) argue that the assumption that individuals "always make choices that are in their best interests" is false. Organizations and agents are continuously tasked to make decisions affecting other individuals (Sunstein & Thaler, 2003). On that note there are not any policies alternative to being paternalistic (Sunstein & Thaler, 2003). Sunstein (2015) argued that if freedom of choice is a concern and thus the avoidance of interventions that threaten human agency is important, then mandates and bans should be the real topic of discussion - not nudges. Consequently, nudging can be considered as a powerful tool to aid people make good decisions for themselves without constricting their freedom.

Nevertheless, nudges are not a "one-size-fits-all" solution and their effectiveness depends on many factors such as the context, the timing, and the habits and preferences of the individuals being nudged (Brown, 2012; Caraban et al., 2019). For example, Johnson and Goldstein (2003) investigated the effects of default choices in organ donation and found that the default of opting out (i.e., being an organ donor is the default and if you do not wish to be an organ donor you have to opt out) increased the percentages of organ donors. Yet, Kankane et al. (2018) conducted an experiment in order to nudge users towards a better password management. When studying the defaults nudge[1], they found that users who knew that they were going to receive an auto-generated password soon by default, avoided the extra initiative of creating their own password (Kankane et al., 2018). Thus, the default nudge in this instance backfired. This example shows that the same nudge has different results in different circumstances. Still, nudges not inducing a desired behavior is not a negative outcome (Sunstein, 2017). Sunstein (2017) suggests that the ineffectiveness of nudges in some contexts and for some people, should be considered as a positive trait as it implies the preservation of freedom of choice. Particularly, he argues that if decision makers choose to ignore or reject a nudge, "it is because they know best" (Sunstein, 2017).

Considering that different nudge interventions are suitable for distinct types of decisions, there is a need to differentiate types of decisions. Specifically, Zimmermann and Renaud (2021)

[1] Defaults effect according to nudge theory explains the tendency of individuals to accept the default option (Altman, 2017). Therefore, defaults nudge is the behavior change tool where a decision maker follows the status quo (The Decision Lab, n.d.)

differentiate between infrequent choices (e.g., rarely made decisions) and frequent choices (e.g., repeated or regularly made decisions). For example, the decision of whether to allow for your health records to be used for research is an infrequent choice while deciding whether you will click on a link you received via email is a frequent choice (Zimmermann & Renaud, 2021). There is additionally a distinction between simple decisions (i.e., install a security update or not) and complex decisions (i.e., the choice of antivirus software). Thus, as some nudges work better depending on the frequency and the complexity of decisions, it is important to identify which type of decision is being nudged. Downloading EduVPN and using it at least once is a simple, infrequent choice. Zimmermann and Renaud (2021) find that with simple and infrequent decisions, a hybrid nudge (e.g., simple nudge and information provision) had the largest difference compared to the control group (e.g., no nudges).

Other studies to nudge secure digital behavior were recently conducted to address issues of online privacy, security, and stronger password management. Acquisti et al. (2017) lay down literature focusing on the aid of more beneficial privacy and security choices. They conclude that careful design of nudges and choice architecture is useful when it comes to helping users in a more secure behavior online. van Bavel et al. (2019) conducted an experiment inspired by Protection Motivation Theory[2] in which they gave advise to participants in order to minimize their exposure to digital risks. For this purpose, they used a coping message (e.g., a message that informs receiver of what to do in order to minimize the possibility of suffering from a cyberattack), a fear-based message (e.g., a message that scares the receiver of the consequences of not complying), and a combination of both (van Bavel et al., 2019). Their findings suggest that future efforts to promote secure digital behavior should incorporate a coping message or a coping message combined with a fear-based message (van Bavel et al., 2019). All these studies confirm the argument that users' decisions to engage in secure online behavior can be affected by the cognitive context users find themselves in (Williams et al., 2018).

The Erasmus University aims to improve the digital security of its employees and students. One tool to achieve this is EduVPN. Literature shows that Nudge Theory seems applicable in the context of promoting EduVPN as users seem unable to overcome the obstacles preventing them

[2] Protection Motivation Theory is a framework used to understand the impact of triggers causing fear-based feelings (Norman, Paul, et al. 2015).

from downloading and using it. Specifically, the IT desk of the Erasmus University Rotterdam supplied an overview of students who have downloaded and used EduVPN at least once. Out of 1671 MSc students in the Erasmus University Rotterdam, only 283 have downloaded and used at least once EduVPN, just before the experiment of the current study. This is just approximately 17% of MScs students. Nudging secure digital behavior could aid the efforts to promote the use of VPN among users.

C. Tested Nudges

In the field experiment of this study, we compare the effectiveness of different nudges to increase the uptake (i.e., download plus usage) of EduVPN among students at the Erasmus University Rotterdam. Students received information about EduVPN through informational email in combination with either no nudge (i.e., control condition), or one of three nudges (i.e., social norm, priming, or self-commitment). A week after receiving these first emails, all participants who have not yet downloaded EduVPN received a simple reminder email. All participants received emails containing information that EduVPN is available for download, a link they can follow to download EduVPN and some information on what having EduVPN means. The emails of participants of the treatment groups will contain additional information, compared to the control group, aiming to nudge them into downloading and using EduVPN. Each of these nudges is designed to utilize powerful cognitive biases in order to promote secure digital behavior.

Social Norm Nudge

Social norms are commonly approved rules of behavior that represent what individuals believe to be “appropriate behavior” (Bicchieri, 2016). Individuals tend to be strongly influenced by what other people do, often following what others around them are doing (Dolan et al., 2010). Further, individuals are most likely to seek the actions of others for acceptance when a situation is unclear or ambiguous (Cialdini, 2007). The power of social norms comes from the social penalties in the cases where an individual is not complying and from the social benefits in the cases where an individual is conforming (Dolan et al., 2010).

Social norm nudges exploit peoples' desire to fit in and to seek the approval of others (Nahmias et al., 2019). Norm nudges can prompt people to behave according to how other people behave, since humans are inclined by nature to model the behavior of others (Mol et al., 2021). There are two approaches when it comes to social norms: *injunctive norms* and *descriptive norms* (Cialdini, 2003). *Injunctive social norms* involve attitudes that are typically approved or disapproved by others (Cialdini, 2003). *Descriptive social norms* involve attitudes that are typically performed by others (Cialdini, 2003). Thus, the social norm nudge works by informing individuals that their behavior in a context, deviates from the behavior of the majority of others or deviates from what is socially approved (Cialdini, 2003).

A number of studies have utilized social norms in order to nudge individuals in various contexts. Cialdini (2003) used descriptive social norms in a sign, in order to promote recycling of towels in a hotel. Hotel guests increased their towel recycling when they saw the signs saying that most guests in the hotel recycle and that the earlier occupants of the room also recycled their towels (Cialdini, 2003). A recent study by Huitink et al. (2020) shows evidence of a positive effect of a social norm combined with the use of a designated space to place vegetables on shopping carts, on the number of vegetables bought.

John (2018) find that descriptive social norms are useful in increasing payment of local taxes in Central London. Specifically, they include message indicating that "over 95% of Lambeth residents pay their council tax" in the bill (John, 2018). Further, similar studies using the social norm nudge use personalized messages. For example, Kroll et al. (2019) use descriptive social norm nudge in a smart home app by showing the percentage of energy saving behaviors of similar household in order to promote energy-saving behavior. Although other studies utilize the social norm nudge using personalized messages aiming to compare the behavior of the recipient with the socially acceptable behavior of others, personalization is not always possible.

Coventry et al. (2014) introduces a structured approach in order to develop behavioral interventions. Their study includes a description with a worked example on how to develop a nudge to promote secure digital behavior when it comes to selection of wireless networks. Specifically, for the priming nudge, they propose: (a) telling users the percentage of people who lost data within the company because they used an unsecured network and (b) telling users the percentage of people

using the preferred secure network. Dolan et al. (2010), argue that for a successful social norm, choice architects should "relate the norm to the targeted audience as much as possible".

Hilton et al. (2014) in their experiment showed that the use of injunctive social norms increased preference for the desired behavior of choosing the train instead of the plain. Specifically, in the social norm conditions they included a message indicating that scientific data shows that trains are a more ecologically friendly option for transportation (Hilton et al., 2014). Further, they displayed a happy face (😊) next to the label "train" and a sad face (☹️) next to the label "plain" (Hilton et al., 2014). Such emoticons were used in other studies in order to show injunctive messages of approval and disapproval, showing significant results. Schultz et al. (2018) in a field experiment provided households with descriptive norms comparing them with other similar households in addition to a message of approval or disapproval, using emoticons.

In the context of online security, Herath and Rao (2009) investigated the employees' security behaviors and found evidence suggesting that social influence was one of the determinants affecting the adoption of security technologies. Specifically, social influence increased the employees' intentions to comply with security behaviors (Herath & Rao, 2009). Coventry et al. (2016), found that nudging with social framing is effective in reducing cookie acceptance in the condition of minority social norm. Therefore, the nudge of social norms seems to be effective in the context of secure digital behavior choices and thus should be effective in promoting the download and use of EduVPN.

H1: The use of the social norm nudge is expected to increase the number of students who use EduVPN, compared to the control group.

Priming Nudge

Priming is a nonconscious form of human memory where a change in the ability to identify or produce an item is observed, as a result of a specific prior encounter with the item (Tulving & Schacter, 1990). In simple words, priming is the phenomenon where if an individual is exposed to one stimulus, that stimulus influences the response of a following stimulus (Weingarten et al., 2016). Dolan et al. (2010) argue that the phenomenon of priming shows that people's behavior can be altered in the condition that they are first exposed to certain stimuli such as sights, words, or

sensations. Consequently, priming nudges are "subconscious cues which may be physical, verbal or sensational, and are changed to nudge a particular choice" (Wilson et al., 2016).

Numerous studies have shown that priming can induce desired behavior. Focusing on priming when using the stimuli of words, Dijksterhuis and Van Knippenberg (1998) asked one group of their participants to think about football hooligans and the other group to think about university professors. Both groups were then asked to answer trivia questions. Participants who thought of football hooligans answered less questions correctly compared to the second group, who kept the university professors in mind. Similarly, Wryobeck and Chen (2003) primed participants of their experiment by asking them to create a sentence out of words such as active and athletic, which made them significantly more likely to use the stairs instead of the elevators. Therefore, exposing people to specific words can subsequently promote certain desired behaviors.

Concerning privacy, Dawson et al. (2015) use priming in order to tested disclosure and showed evidence suggesting that primed participants shared significantly more information than the participants who were not primed. Specifically, when it comes to secure digital behavior, Parish et al. (2021) used the priming technique also known as the presentation effect in order to improve the security of graphical passwords by gradually revealing an image during password creation. Their analysis reveals that the priming technique enhanced the security of graphical passwords (Parish et al., 2021). Sharma (2017) find evidence suggesting that priming users to cyber-security risks reduces their tendency to take risks, suggesting that priming users can be an effective way to reduce cyber-security risks. Priming is a promising nudge in the context of secure digital behavior choices and thus should be effective in promoting the download and use of EduVPN.

H2: The use of the priming nudge is expected to increase the number of students who use EduVPN compared to the control group.

Self-commitment Nudge

People tend to delay or procrastinate when it comes to decisions that involve immediate costs and future, positive effects (O'Donoghue & Rabin, 1999). In the case of downloading and using EduVPN, the costs are immediate – time and effort to download the VPN –, but the rewards are future – being secure online. Dolan et al. (2010) argue that committing in a public manner increases

the costs of failure to take the committed action. Cialdini (2007) discusses our need as individuals to associate ourselves with the "mental picture" created of us and maintain this association over time. He then recommends that even when an individual engages in self-commitment by writing it down, that act can increase the probability of the individual actually fulfilling the task. A commitment intervention can be self-imposed or externally imposed, meaning that some people are willing to commit to their self while there is also the option to commit to someone else (Ly et al., 2013). Therefore, a self-commitment nudge, as used in this study, urges the individual to commit to themselves to do an action at a certain day and time.

Commitment devices have been shown to have meaningful results in many contexts. For example, Weijers et al. (2022) utilized the commitment nudge in order to increase online class attendance during COVID-19. Their evidence suggests that students who committed to attend online class did attend more often than the students who were in the control group (Weijers et al., 2022). Baca-Motes et al. (2013), studied the effect of commitment on hotel guests to behave environmentally friendly during their stay, showing that guests who committed were more likely to reuse their towels.

Specifically, studies on secure digital behavior have utilized commitment in order to promote more secure digital behavior. Frik et al. (2019) offered participants commitment devices by proposing to schedule future security tasks. This commitment device was able to increase the number of individuals who followed through with their intentions. Self-commitment devices are commitment arrangements that are self-imposed, meaning that individuals commit themselves to do something, by restricting other choices (Bryan et al., 2010). Therefore, providing participants of the current study with the recommendation to commit themselves into downloading and using at least once EduVPN, can increase the uptake of students who use EduVPN. All the studies mentioned, show that commitment devices can aid the purpose of this study.

H3: The use of the self-commitment nudge is expected to increase the number of students who use EduVPN compared to the control group.

Reminder Nudge

Nudging with the use or reminders is considered a simple and inexpensive way to promote a more desired behavior (Calzolari & Nardotto, 2017). Reminders are special types of messages aiming to inform individuals about upcoming tasks that need our attention (Dey & Abowd, 2000). Reminders are especially helpful in cases where individuals engage in activities where the costs are immediate, but the benefits are future (Calzolari & Nardotto, 2017). In such cases, reminders help an individual to remember an important task and at the same time help put forward the future benefits. Through this mechanism reminder nudge individuals to actually undergo with that task. In simpler words, reminders revamp individuals' attention to the opportunity they have for future gains (Calzolari & Nardotto, 2017).

Reminder nudges have been used in many studies and in various contexts such as retirement savings, healthcare as well as secure digital behavior. Specifically, Karlan et al. (2016), through a series of experiments in three distinct banks showed evidence that reminders increased banks' clients savings, helping them to reach their savings goals. Altmann and Traxler (2014), find evidence showing that message reminders increased the frequency of dental check-ups. Similarly, Gurol-Urganci et al. (2013) showed evidence that reminders through text messages increased the attendance rate of healthcare appointments. Bonham (2008) conducted an experiment where email reminders were found to significantly increase post-course assessments by students compared to students who did not receive reminders.

Calzolari and Nardotto (2017), through a field experiment show that **simple** weekly reminders increase participants' gym attendance. They also note that the participants' response to reminders was immediate, meaning that within a few hours individuals went through with the task they were reminded of, in this case gym attendance. Frascella et al. (2020), study the effectiveness of **email-based** reminders on the uptake of vaccinations and provide evidence supporting that email reminders are successful in increasing vaccine uptake in comparison with no email reminders.

Reminders were also used in the context of digital security. Frik et al. (2018) show evidence suggesting that reminders were effective in prompting individuals to engage in more secure digital behavior. Specifically, reminders reduced the participants intentions to ignore requests concerning security updates and requests about enabling the two-factor authentication method (Frik et al.,

2018). Reminders are promising nudges for the purposes of this study where the aim is to promote a more secure digital behavior for EUR students by increasing the number of students who use EduVPN.

Nonetheless, the university already occasionally sends reminders to particular emails. Yet, there is no clear "rule" on when these reminders are sent and rather it is on the discretion of the department responsible for sending the initial email. Therefore, testing the simple reminder nudge as an additional step to the three nudges is more relevant to the operations of the university. Specifically, since reminders are already occasionally sent after the original emails, testing whether the simple, email reminder nudge can be more effective when combined with the tested nudges (e.g., social norms, priming and self-commitment) can be a particularly interesting insight for the university. Thus, this study will not test the effectiveness of the reminder nudge but rather will test whether there are differences in effectiveness of the reminder nudge when first receiving either no nudges (e.g., control group) or the other three nudge interventions. Simply put, because the university already sends reminders, it is more relevant to test if simple email reminders have a particularly larger effect when paired with the initial intervention of sending informatory emails with nudges.

H4: One or more of the initial nudges are particularly more effective when followed by a simple reminder email.

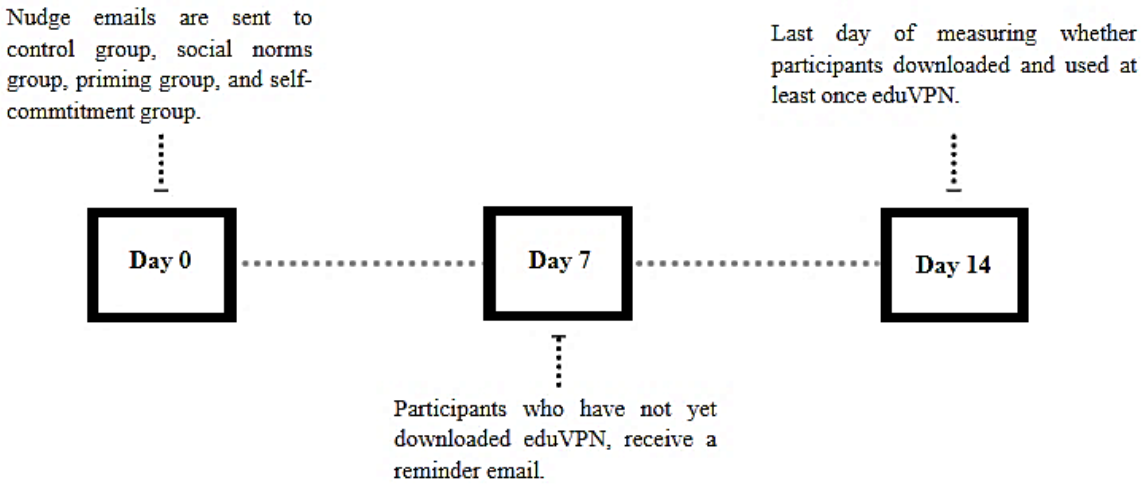
III. Methodology

A. Experimental design and procedure

Ethical approval was granted by the ethics committee of the Erasmus School of Economics, code ETH2122-0582. This study aims to test the effectiveness of four nudge methods, namely ***social norms***, ***priming***, ***self-commitment***, and ***reminders***, on increasing the uptake of EduVPN. For the purpose of this study a natural field experiment was conducted using MScs students at the Erasmus University Rotterdam. Students received emails signed by the Security Department of the university containing information about EduVPN. Initially, students were randomly assigned to one of four groups. The first group served as a control group, where no nudges were included in

the email, just the information about EduVPN. The three other groups served as treatment groups for nudges of *social norms*, *priming* and *self-commitment*. The treatment groups received the same information as the control group plus the corresponding nudges. Each of the groups received the emails created for the particular group on day 0. On day 7 simple reminder emails were sent to the students who by that day had not yet downloaded EduVPN. Figure 2 shows the timeline of the experiment. Essentially, the experiment is divided into two phases. Phase 1 (i.e., day 0 to day 7), where the nudges of social norms, priming and self-commitment are being tested. Phase 2 (i.e., day 7 to day 14), where the reminder nudge is being tested as a supplemental nudge to the three initial nudges.

Figure 2 - Timeline of experiment



Essentially, this study tested not only the suitability of nudges to promote the use of EduVPN within an educational institution but, also the effectiveness of the four individual nudge techniques. After the end of the experiment, participants were sent a debriefing email informing them that they had participated in an experiment. The debriefing email can be found in Appendix II. Further, the debriefing email contained a questionnaire aiming to provide additional insights concerning both the experiment of this study as well as insights on the decision to behave securely online. The questionnaire included additional questions that can be used in a future study. The questions used for the purposes of this study can be found in Appendix III.

B. Measurement of EduVPN users

The dependent variable for this study is the number of EduVPN users. Crucial for the measurement of the dependent variable are three points: First, none of the participants had downloaded or used EduVPN before the experiment. Second, we can detect which accounts use EduVPN and which do not. Third, we can determine which student received which treatment. Specifically, as the participants of this experiment are students who have not used EduVPN before, when a participant is seen by the security department to use the VPN (for the first time), we can actually infer that they have downloaded and used it at least once.

C. Sample

Participants are not aware of their participation in the experiment since this study concerns a natural field experiment. Warning them up front, could alter their behavior. The original sample of participants consist of 1671 MSc students from the Erasmus University Rotterdam (EUR). For the purposes of this experiment, we can only test students who have never downloaded or used EduVPN before. All of EUR students had access to EduVPN prior to the experiment, therefore not all students were eligible for participation. Thus, 283 students who had already downloaded and used EduVPN before the start of the field experiment were not eligible for participation. Further, the experimenter, 9 students who were aware of the experiment as well as 19 students whose emails bounces were also removed from the sample. The final sample consists of 1,359 MSc students who had not downloaded or used EduVPN before the experiment and were not aware of the experiment. The participants were randomly assigned to the four initial treatment groups. The control group consists of 342 participants, the social norms treatment consists of 338 participants, the priming treatment consists of 341 participants and the self-commitment treatment consists of 338 participants.

Essentially, the experiment of this study is divided into two parts. The first part of the experiment studies the effect of the three first nudges, priming, self-commitment and social proof on the uptake of EduVPN. For this part, a statistical power analysis was performed for sample size estimation for a Chi-squared test of independence with a small effect size of 0.1, the probability of finding significance where there is none was set to 0.05 (e.g., $\alpha=0.05$), the probability of not

finding significance when it is there was set to 0.80 (e.g., 1-β=0.80) and degrees of freedom equal to three (e.g., Df=3). This power calculation revealed a required total sample size of 1091, thus, approximately 275 participants per condition. The sample of 1,337 participants therefore will be adequate for the objective of the first part of this study.

For the second part of the experiment, which aims to test the effectiveness of reminders on the uptake of EduVPN as a complementary intervention to the first three nudges, the sample size depends on the number of participants who downloaded EduVPN during the first 7 days of the experiment. That is, the reminders were sent to the participants who by day 7 of the experiment had not yet downloaded EduVPN. Therefore, the sample size for the reminders was 1337 participants in total. Lastly, concerning the randomization process, for the purpose of this study students were randomly divided into four random subgroups. Each group received a different email, according to the nudge group they were assigned.

D. Materials

The experiment was conducted completely online using emails to convey all the information to participants. The emails of all the treatments were send both in English and in Dutch as this is the normal practice of the IT department when sending emails to students. The control group received a standard informatory email signed by the university's security department, containing basic information about what using EduVPN means, and a link to follow for downloading EduVPN. A sample of this email is shown in Appendix I. The three other groups received the same information as the control group with the addition of nudges to further encourage the downloading and usage of EduVPN. Zimmermann (2021) concludes that combining nudging with information provision is a promising strategy in order to promote making security-related decisions without having to enforce one particular choice.

Social Norm Nudge

The social norm nudge is based on the insights of Hilton et al. (2014). Specifically, the participants received emails that contained additional information on the percentage of people who find their digital security important (i.e., injunctive social norms). The information states that "88% of

people find their digital security important" (Economics of Cyber Security course, lecture 10, 2021-2022). Additionally, an emoticon was displayed next to the button of the link used to download EduVPN in order to show approval of this action. The email sent to the social norms treatment group can is shown in Appendix I.

Priming Nudge

Sharma (2017) primed participants to cyber-security risks which reduced their tendency to take risks when it comes to cyber-security. Providing participants with information regarding EduVPN and additionally including words such as "security", "cyber-crime", "cyber-security" can aid the target of priming participants. Therefore, participants receiving the treatment of priming received email containing text that includes a variety of security-related words, in addition to the part of the email informing them that EduVPN is available for students, which is the same as the control group. The email sent to the priming nudge treatment group can be seen in Appendix I.

Self-commitment Nudge

The commitment nudge is based on the insights of the study by Frik et al. (2019). Participants receiving the treatment of self-commitment, were prompted to schedule in their calendars when they would like to download EduVPN, in addition to the part of the email informing them what having EduVPN means and a link for download. In this way, students self-commit that they will download EduVPN on that particular day or time, which essentially is like setting an "appointment" for themselves to do so. In order to use the self-commitment nudge successfully, the assumption is made that although downloading and using EduVPN at least once is a relatively simple, easy, and quick task, students in multiple occasions do not proceed to do so. Reasons could be perhaps laziness or that students might read their emails from other devices other than their primary computer (i.e., from their phones). Consequently, prompting students to self-commit by scheduling when they would like to actually download EduVPN can overcome such obstacles. The email sent to the self-commitment nudge group can be seen in Appendix I.

Reminder Nudge

The decision to download EduVPN and use it a least once, is a one-time decision completely made by the user herself. Thus, in order to determine the timeframe under which the reminder email would be set, an experiment with a similar type of decision should be consulted (e.g., gym attendance). Calzolari and Nardotto (2017) reminded participants using weekly, repeated reminders and found that two days after the "reminder day", participants who received the reminders had a significantly higher probability of attending gym compared to participants who did not receive reminders. In the current study, the effectiveness of a reminder a week after the initial email will be tested. The reminder will not be repeated but rather sent only once, simply reminding participants who have not yet downloaded EduVPN to do so.

Concerning the content of the reminder emails, the study by Calzolari and Nardotto (2017) will be consulted again. In their study they used **simple reminders** to increase participants' gym attendance. Simple reminders do not contain any monetary incentives thus they allow the individual receiving them to give credit to themselves for performing the action they are reminded of (Calzolari & Nardotto, 2017). Such reminders are not only easy to send but are also inexpensive, making their use as a default policy a powerful tool (Calzolari & Nardotto, 2017). Therefore, on day 7 of the experiment all participants who had not yet downloaded EduVPN, received the same simple, email reminder regardless of which nudge group they were initially assigned to. In this way, the compatibility of the reminder as an additional method to induce the uptake of EduVPN can be tested. The email sent to participants of this treatment is shown in Appendix I.

E. Analysis

Social Norms, Self-commitment and Priming Analysis

In order to test the effect of social norm nudge (H1), the effect of priming nudge (H2) and the effect of self-commitment nudge (H3), a Chi-squared test of independence and a Fisher's Exact test were conducted. Both tests can be conducted for independent observations, for more than two groups (i.e., creating a 2x4 table). The Chi-squared test of independence assumes that the expected

frequencies in each cell should be greater than 5 in at least 80% of the cells and additionally no cell should have an expected frequency of less than one (Bewick et al., 2003). Even though this assumption is not met for all the nudges, the Fisher's Exact test will be also conducted as a robustness check (Grace-Martin, n.d.).

Reminders Analysis

In order to test whether there is a difference between the four treatment groups in the effectiveness of reminders (H4) a Chi-squared test and a Fisher's Exact test were conducted. Again, the data for the reminders have independent observations and more than two groups will be compared. The assumption of the expected value in each cell to be greater than 5 in at least 80% of the cells applies in this test (Bewick et al., 2003). It is important to note that the above test aims to underscore the differences between the four initial treatments when receiving reminders, rather than revealing the effectiveness of the reminder emails in increasing the EduVPN uptake. In other words, this analysis tests whether there are differences in EduVPN uptake between the control group, social norms, priming and self-commitment as a result of the reminders sent 7 days after receiving the initial email nudges. The results of this test reveal whether the reminder intervention can effectively be paired with one of the original nudges as an additional method to increase EduVPN uptake.

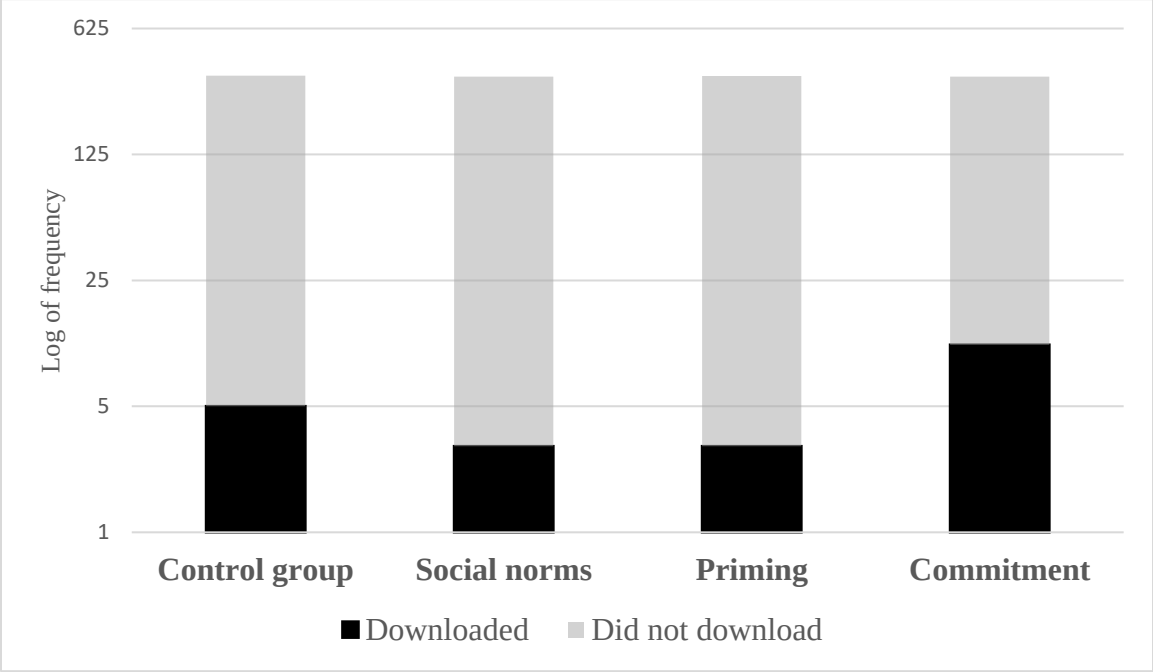
IV. Results

Social Norms, Priming, and Self-commitment Nudge Analysis

In order to test the effect of social norm nudge (H1), the effect of priming nudge (H2) and the effect of self-commitment nudge (H3), the participants choices were divided between '*downloaded and used EduVPN at least once'* and '*did not download EduVPN and used at least once'*. For this initial analysis, the data gathered from day 0 to day 7 were used. During this period, 22 participants in total downloaded and used at least once EduVPN. Among the 22 participants who downloaded and used at least once EduVPN, 5 participants were in the control group, 3 participants in social norms group, 3 participants in the priming group and 11 participants were in the self-commitment group. Figure 3 shows the logarithmic scale of frequencies of the participants who downloaded

and used EduVPN at least once per treatment. Although the results appear larger than they are in reality, as a result of the logarithmic scale, the important takeaway from Figure 3 is the differences in EduVPN uptake among the four treatment groups. The self-commitment nudge uptake rate on EduVPN is larger compared to the three other treatments.

Figure 3 – Logarithmic frequencies of participants who downloaded and did not download EduVPN per treatment



Note: The graph was created using a logarithmic scale of the frequencies of each treatment for the purposes of better visualization.

A Chi-Square Test of Independence was performed to assess the relationship between downloading and using EduVPN at least once and the different treatment groups. The test showed a significant relationship between the two variables, $\chi^2(3, N=1{,}359) = 8.03$, $p = .045$. The level of significance is at 5%. The assumption of the expected value in each cell to be greater than 5 did apply, as can be seen in Table 1 (Bewick et al., 2003). However, even though this assumption applies, a Fisher's exact test was additionally performed for the purposes of a robustness check. The Fisher's exact test also reveals that there are significant differences across the four conditions, $p=0.075$. Cramer's V, as a measure of effect size indicates that although significant, there is a small effect size (Cramér's $V = 0.0769$). The results of this initial analysis indicate that there is overall a deviation between the observed and expected frequencies of the variables tested.

In order to identify where the differences exist in the initial Pearson Chi-squared analysis, a post-hoc analysis is conducted (Beasley & Schumacker, 1995; Sharpe, 2015). Table 1 presents the adjusted residuals (e.g., z-scores[3]) that were calculated. The z-score calculated for the self-commitment nudge is equal to 2.749 which corresponds to the observed value of 11 participants who downloaded and used EduVPN at least once. The observed number of 11 downloads is statistically significantly different from the expected number of downloads which was 5.5, at 5% level of significance. In order to control for Type 1 error, the adjusted p-values (Table 1) are compared to the Bonferroni p-value[4], p=.00625 (MacDonald & Gardner, 2000). The results confirm the previous finding. Therefore, participants who received the self-commitment intervention downloaded and used EduVPN significantly more than expected, compared to the other treatments.

Table 1 – Expected Values and Adjusted Residuals for post-hoc Chi-squared testing

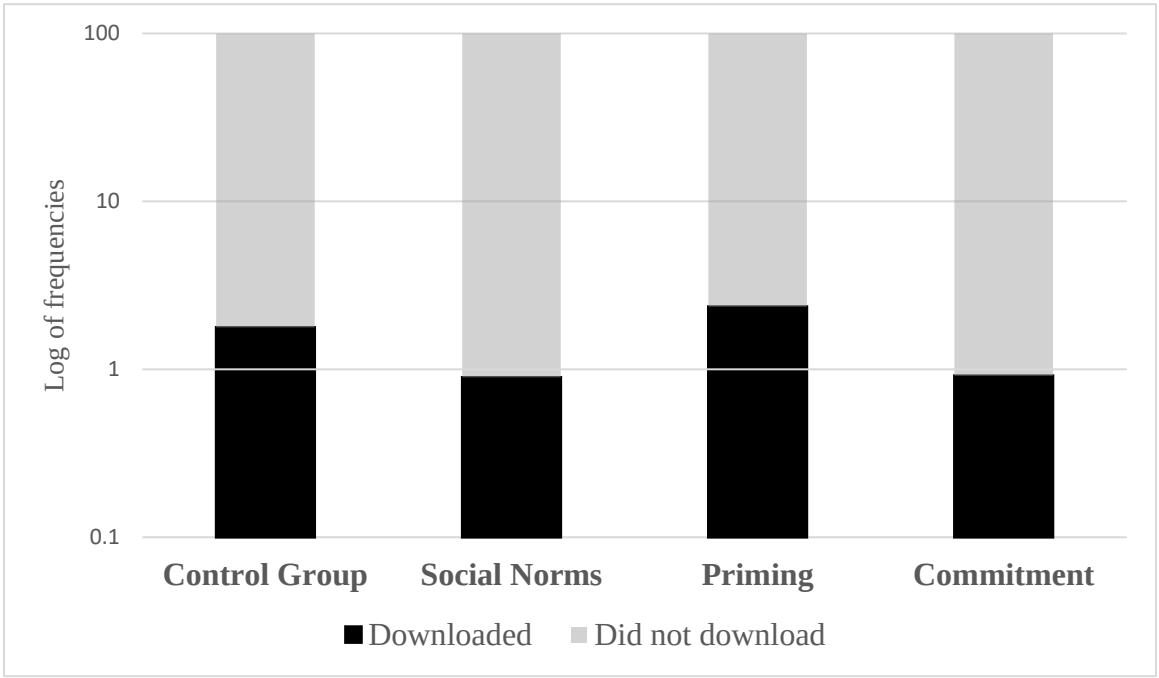
	Expected Values		**Adjusted Residuals**		**Adjusted p-values[5]**
	Downloaded EduVPN	**Did not download EduVPN**	**Downloaded EduVPN**	**Did not download EduVPN**	
Control Group	5.5	336.5	-0.266	0.266	.790
Social Norms Nudge	5.5	332.5	-1.229	1.229	.219
Priming Nudge	5.5	335.5	-1.250	1.250	.211
Commitment Nudge	5.5	332.5	2.749	-2.749	.0059

[3] An absolute z-score above 1.96 is statistically significant, at a 5% level of significance.
[4] The Bonferroni correction of p-value is calculated by dividing the p-value to the number of different hypotheses tested (Bonferroni, 1936).
[5] Adjusted p-values associated with the adjusted residuals.

Reminder Nudge Analysis

For the reminders analysis the data gathered from day 7 to day 14 were used. To test the effectiveness of the simple email reminders as an additional intervention a week after receiving each of the initial nudges. Based on this hypothesis the participants choices were again divided between '*downloaded and used EduVPN at least once'* and '*did not download EduVPN and used at least once'*. During this second part of the experiment, out of the 1,337 number of participants, 20 participants in total downloaded and used at least once EduVPN after receiving the reminders. Among the 20 participants, 6 participants were in the control group, 3 participants in social norms group, 8 participants in the priming group and 3 participants in the self-commitment group. Figure 4 shows the logarithmic scale of frequencies for the participants who downloaded and used EduVPN at least once after the reminders per treatment. The important takeaway from Figure 4 is the differences in EduVPN uptake after receiving the reminders among the four treatment groups. The control group and priming group have the highest EduVPN uptake rate, compared to social norms and self-commitment nudges.

Figure 4 - Logarithmic frequencies of EduVPN downloads after reminder emails per treatment.



Note: The graph was created using a logarithmic scale of the frequencies of each treatment for the purposes of better visualization.

A Chi-Square Test of Independence was performed to assess the relationship between downloading and using EduVPN at least once and the treatment groups. The test shows that there are not significant differences across the four conditions for the reminder nudge, $\chi^2(3, N= 1.337) = 3.4873$, $p = .322$. The Fisher's Exact Test was also revealing again that there are no significant differences across the four conditions for the reminders intervention, $p= .347$. Therefore, there is no significant difference between the expected and observed EduVPN downloads after receiving the reminder emails. This result indicates that there is not a difference in EduVPN downloading rates between the treatments after receiving the reminder. In simpler words, the intervention of sending the same reminders to all the different treatments did not produce significantly different rates of download. Thus, simple email reminders do not have a particularly larger effect when combined with the initial intervention of sending the nudges of social norms, priming and self-commitment

Debriefing questionnaire results

The questionnaire aims to identify a number of the factors that influenced the behavior of the participants when deciding to download EduVPN. In total, 6 of the participants completed the online questionnaire. Three of the participants were in the 18-24 age group, two were in the 25-34 age group and one participant was in the 55-64 age group. Three participants were male and three females. Four of the participants claimed that they had read the full email sent by the Security Department, while two claimed that they had not. However, all 6 participants answered that they had not discussed the content of the email with other students.

Out of the six participants only one downloaded and used EduVPN as a result of the email interventions, answering that they were persuaded by the information they had received in the email. This participant was in the priming treatment group and claimed that downloading EduVPN was extremely easy, they found it extremely useful and that they had also activated staring on sign-in as suggested in the email. The other five participants who answered the survey did not download EduVPN. Three of the participants were in the social norms treatment group, one was in the priming group and one in the self-commitment group.

All five participants answered different reasons as to why they did not download EduVPN. One participant claimed that they do not believe that using a VPN keeps them secure online. A second participant answered that they will graduate soon so they thought downloading EduVPN was unnecessary. Other participants answered that they use another personal VPN or that they did not even notice the original email they had received. The last participant answered that they are "never on campus" and that they have "access to Wi-Fi at home", which perhaps indicates of lack of cyber security knowledge. That is, it may be that they do not exactly understand the purpose of VPNs.

To measure if the participants of the survey are familiar with VPNs two questions were included. First, participants were asked what VPNs are for to which question three of the participants answered correctly "All of the above" and three chose different answers (Appendix III). Secondly, participants were asked what the acronym VPN stands for. All the participants answered correctly. Even though, as a result of the low sample size, the questionnaire cannot be used to derive robust results that can represent all the participants, it still provided some important insights, validating some of the concerns presented in the limitations section.

V. Discussion

Interpretation of results

The field experiment of the current study uses the insights of Nudge Theory, aiming to increase the uptake of EduVPN among students in EUR. Social norms, priming, and self-commitment were tested through sending emails which combined information and the corresponding nudges (i.e., phase one of the experiment). In a separate analysis, this study also tests whether there are differences across the four initial nudge groups when seven days later all participants, regardless of their initial distribution to the treatment groups, receive the same simple, email-based reminders. This test aims to reveal whether one or more of the nudges are particularly more effective when followed by a simple reminder email (i.e., phase two of the experiment).

Overall, through this experimental intervention, 42 participants downloaded and used EduVPN at least once. Specifically, 22 students had downloaded and used EduVPN during the

first week of the experiment (i.e., phase one) and 20 students during the second week of the experiment (i.e., phase two). The results suggest that the self-commitment nudge was effective in increasing the uptake of EduVPN, validating the hypothesis (H3) made at the beginning of the study. The nudges of social norms and priming were not found to have a significant effect on EduVPN downloading rates (H1, H2). Further, the intervention of sending the same simple reminders was not found to have significantly different rates of download across the different treatments (H4).

This study's result indicating that self-commitment nudge can be used in order to increase the uptake of EduVPN among students generates key implications. First, this paper presents evidence supporting that the self-commitment nudge is a powerful way to utilize commitment devices as a mechanism to induce a desired behavior. Consequently, the results of this study validate the recommendation made by Cialdini (2007), signifying that even when a person self-commits by writing it down, instead of externally committing, this act can increase the probability of the person fulfilling the task. Secondly, the results of this experiment provide evidence that self-commitment in combination with information provision is effective in increasing a desired behavior in the context of secure digital behavior. Self-commitment combined with information provision in emails can be considered a generally simple and inexpensive method to persuade individuals to act upon a recommendation made by an organization. Generally, self-commitment nudge can be used and established in emails sent by the university, especially when emails urge students to undertake one-time tasks. Lastly, this study provides indication that self-commitment nudge combined with information provision is an effective formula in order to promote infrequent choices. This finding validates the findings of Zimmermann and Renaud (2021) which suggest that a simple nudge combined with information provision is the most effective formula to encourage simple and infrequent decisions.

Limitations

A matter of concern would be potential spillover effects since students are participating in a natural field experiment, where there is little control to the experimenters. Specifically, there is a possibility of spillover effects of the information sent to different treatment groups to other treatment groups. For example, students who know each other but received different treatments

and thus different emails could discuss and transmit to each other the information they got from the emails. Such an occurrence could alter the effects of each treatment to EduVPN usage rates. This cannot be controlled for without compromising complete randomization of participants into the different treatments therefore potential spillover is considered a limitation of the experimental approach of this study. On this note, all six of the participants who answered the questionnaire stated that they had not discussed the content of the email with other students. Although six participants answering this does not eliminate the risk of spillover, it perhaps indicates that the rate may be lower than anticipated.

Another limitation is the timing of the study. The study was conducted in May 2022 just three months prior to the end of the educational year for MScs' students. It is possible that students who will graduate this year did not have any incentives to follow through with downloading and using EduVPN as online classes were already mostly done. Perhaps the same participants would have a different reaction, had the study was conducted during the beginning of the year. The follow-up questionnaire included a question addressing this issue. Specifically, the question asking the reasons as to why participants did not download EduVPN included the option "I will graduate soon so i thought it was unnecessary" and one of the participants claimed so. Again, although this answer does not provide evidence that this case applies for other participants as well, it does validate the concern that at least for one student the timing of the study did affect their choice of downloading EduVPN. On a related note, the low rate of answers to the follow-up questionnaire could perhaps result as well from poor timing of sending the debriefing email, where the questionnaire link was included.

Further, when choosing the most promising nudges for this particular study, it is important to consider that the objective is to increase the number of students who download and use at least once EduVPN, which is what is available for measure by the Security Department. Thus, the objective involves an infrequent choice. However, it is important to acknowledge that constant use of EduVPN is the ultimate goal when aiming to achieve secure digital behavior. On this note, even though the study measures the number of students who download and use EduVPN at least once, the emails prompt students to also activate "start on sign-in", which means EduVPN will automatically be activated upon sign-in on the device. Therefore, an ideal intervention would promote continuous use of EduVPN after downloading it for the first time, which is considered a

frequent choice. Alternatively, promoting download of EduVPN and simultaneously activation of starting at sign in, could be much easier as it is an infrequent, one-time choice. The questionnaire included a question asking participants who had downloaded EduVPN whether they had activated start on sign-in. The one participant who answered the questionnaire and downloaded EduVPN answered that they did activate start on sign-in, yet this is not an indication that the advice had an actual impact.

Lastly, a substantial limitation arises from the methodological difficulty of the reminder email. Specifically, the literature provided evidence of simple, email-based reminders to be effective when aiming to nudge with reminders. In simple words, the most effective email reminders according to literature did not contain any additional nudges, incentives or monetary inducements. As a result, all participants received the same email reminder regardless of their initial categorization to different nudges. The hypothesis was formulated to test whether there were differences across the four initial nudge groups when 7 days later all participants receive the same simple reminders. This choice constrained the overall testing of the reminder nudge. That is, the current test cannot confirm the effectiveness of the reminder nudge but rather can or cannot confirm whether there are differences between the initial treatment groups when they receive the same simple reminder email. Yet, this assortment complicates not only the formulation of hypothesis but also the understanding of the actual interpretation of the results. Optimally, a test evaluating the effectiveness of the reminder nudge on EduVPN uptake rates would be more appropriate.

Future Research

Although many initiatives have already tested the effects of nudges in the field of security, there is certainly a large area of research still to be established. This study provides a good starting point for further research and discussion concerning choice architecture and secure digital behavior as it studies the effectiveness of three nudges to the uptake of EduVPN. Future research should consider the potential effects of timing such a field experiment more carefully. For example, the experiment took place during the end of the academic year, during which the majority of students were preparing for graduation. Thus, their willingness to download and use a tool of the university may had been lower in comparison to their willingness during the start of the academic year.

Furthermore, the main finding of this study concludes that self-commitment nudges can be used to increase the uptake of EduVPN. Additional research can be conducted to unveil whether self-commitment is effective for other desired behaviors in the spectrum of secure digital behavior. For example, the Erasmus University Rotterdam plans to introduce a multi-factor authentication system for students to log-in safely to their student accounts. The transition from the current system to the MFA system could potentially cause less stress and negative responsive if perhaps this new system is introduced initially with an email containing basic information and the self-commitment nudge. Therefore, testing if the effectiveness of the self-commitment nudge on EduVPN uptake is also effective to a number of online security behaviors, could potentially assist the efforts of the security departments of numerous organizations.

In addition, testing more nudges and in different perspectives, could provide additional insights to this field of research. Particularly, priming using words did not significantly affect the behavior of the participants in the context of nudging the use of EduVPN. However, priming with different techniques may be a more suitable option in the same context. For example, priming with the use of graphical representations or grammatical tasks could potentially be more effective in the context of promoting the use of EduVPN (Wryobeck & Chen, 2003; Parish et al., 2021). Equally, even though social norms and priming nudge were not effective in increasing the uptake of EduVPN, they could be effective in increasing other online security behaviors.

Further, the actual effectiveness of reminders alone should be tested in the context of promoting tools for secure digital behavior. That is, as pointed out previously, this study does not address the effectiveness of the reminder nudge. Future studies should address this research question in the context of secure digital behavior. Lastly, the possibility of sending reminders over a period of time rather than just once warrants further investigation. Specifically, Calzolari and Nardotto (2017) sent simple weekly reminders in order to increase participants' gym attendance. Therefore, weekly reminders could be more effective in promoting the use of EduVPN.

VI. Conclusion

Cyber security remains one of the top priorities of organizations in the latest years. Tools such as Virtual Private Networks (VPNs) enable members of organizations to behave securely online and

thus increase defense against an attack. In particular, VPNs allow users connected in different networks to exchange data, as though they were connected to one private network. Although using VPNs can minimize the risk of certain types of cyber-crimes, most people do not use a VPN. This study aims utilize the insights of Nudge Theory through a field experiment, in order to promote the download and use of EduVPN among students. The most promising nudges according to literature were tested by sending emails which combined information provision with the corresponding nudges of *Social Norms*, *Priming* and *Self-commitment*. Further, in a separate analysis, this study also tests whether there are differences across the four initial nudge groups when seven days later all participants receive the same simple, email-based reminders. The results indicate that the self-commitment nudge was effective in increasing the uptake of EduVPN. The nudges of social norms and priming were not found to have a significant effect on EduVPN downloading rates. Further, the intervention of sending the same simple reminders was not found to have significantly different rates of download across the different treatments. Despite the methodological difficulties of testing the simple reminder nudge, the insights from this study, indicating the effectiveness of the self-commitment nudge, can be used to shape the future emails sent by the university but also other organisations. Future studies should be conducted to test the effectiveness of simple email reminders when combined with nudges as well as the effectiveness of social norms and priming nudge on more online security behaviors.

References

- 5 Cyber Threats That A VPN Can Handle. (2021, May). FinSMEs. https://www.finsmes.com/2021/05/5-cyber-threats-that-a-vpn-can-handle.html
- Acquisti, A. (2004, May). Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 5th ACM conference on Electronic commerce (pp. 21-29).
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), 1-41.
- Altman, M. (Ed.). (2017). Handbook of behavioural economics and smart decision-making: Rational decision-making within the bounds of reason. Edward Elgar Publishing.
- Altmann, S., & Traxler, C. (2014). Nudges at the dentist. European Economic Review, 72, 19-38.
- Baca-Motes, K., Brown, A., Gneezy, A., Keenan, E. A., & Nelson, L. D. (2013). Commitment and behavior change: Evidence from the field. Journal of Consumer Research, 39(5), 1070-1084.
- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672.
- Beasley, T. M., & Schumacker, R. E. (1995). Multiple regression approach to analyzing contingency tables: Post hoc and planned comparison procedures. The Journal of Experimental Education, 64(1), 79-93.
- Bewick, V., Cheek, L., & Ball, J. (2003). Statistics review 8: Qualitative data–tests of association. Critical care, 8(1), 1-8.
- Bicchieri, C. (2016). Norms in the wild: How to diagnose, measure, and change social norms. Oxford University Press.
- Blanco, F. (2017). Cognitive bias. Encyclopedia of animal cognition and behavior, 1(6).
- Bonferroni, C. (1936). Teoria statistica delle classi e calcolo delle probabilita. Pubblicazioni del R Istituto Superiore di Scienze Economiche e Commericiali di Firenze, 8, 3-62.
- Bonham, S. (2008). Reliability, compliance, and security in web-based course assessments. Physical Review Special Topics-Physics Education Research, 4(1), 010106.
- Brown, P. (2012). A nudge in the right direction? Towards a sociological engagement with libertarian paternalism. Social policy and society, 11(3), 305-317.
- Bryan, G., Karlan, D., & Nelson, S. (2010). Commitment devices. Annual review of Economics, 2(1), 671-698.
- Calzolari, G., & Nardotto, M. (2017). Effective reminders. Management Science, 63(9), 2915-2932.
- Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019, May). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-15).
- Chapman, J. (2019). How Safe is Your Data?: Cyber-security in Higher Education. Higher Education Policy Institute.
- Cialdini, R. B. (2003). Crafting normative messages to protect the environment. Current directions in psychological science, 12(4), 105-109.
- Cialdini, R. B., PhD. (1983). Influence: The Psychology of Persuasion (2nd ed.). The Business Library.
- Coventry, L. M., Jeske, D., Blythe, J. M., Turland, J., & Briggs, P. (2016). Personality and social framing in privacy decision-making: A study on cookie acceptance. Frontiers in psychology, 7, 1341.

Coventry, L., Briggs, P., Jeske, D., & Moorsel, A. V. (2014, June). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In International conference of design, user experience, and usability (pp. 229-239). Springer, Cham.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber-security. Technology Innovation Management Review, 4(10).

Das, S., Wang, B., Tingle, Z., & Camp, L. J. (2019). Evaluating user perception of multi-factor authentication: a systematic review. arXiv preprint arXiv:1908.05901.

Dasgupta, D., Roy, A., & Nag, A. (2017). Multi-factor authentication. In Advances in User Authentication (pp. 185-233). Springer, Cham.

Dawson, E., Hartwig, M., & Brimbal, L. (2015). Interviewing to elicit information: Using priming to promote disclosure. Law and human behavior, 39(5), 443.

de Quintana Medina, J. (2021). What is wrong with nudges? Addressing normative objections to the aims and the means of nudges. Gestión y Análisis de Políticas Públicas, (25), 23-37.

Dennis, M. Aaron (2019, September 19). cybercrime. Encyclopedia Britannica. https://www.britannica.com/topic/cybercrime

Dey, A. K., & Abowd, G. D. (2000, September). Cybreminder: A context-aware system for supporting reminders. In International Symposium on Handheld and Ubiquitous Computing (pp. 172-186). Springer, Berlin, Heidelberg.

Dias, D., Boehm, J., Lewis, C., Li, K., & Wallance, D. (2022, March 10). Cybersecurity trends: Looking over the horizon. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Dijksterhuis, A., & Van Knippenberg, A. (1998). The relation between perception and behavior, or how to win a game of trivial pursuit. Journal of personality and social psychology, 74(4), 865.

Dolan, P., Hallsworth, M., Halpern, D., King, D., & Vlaev, I. (2010). MINDSPACE: influencing behaviour for public policy.

Dur, R., Fleming, D., van Garderen, M., & van Lent, M. (2021). A social norm nudge to save more: A field experiment at a retail bank. Journal of Public Economics, 200, 104443.

Economics of Cyber Security course, lecture 10, 2021-2022

EduVPN philosophy: less code means a more secure service. (2022). EduVPN. https://www.EduVPN.org/EduVPN-philosophy-less-code-means-a-more-secure-service/

EduVPN: Index. (n.d.). EduVPN. https://www.EduVPN.org/

Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd annual ACM conference on human factors in computing systems (pp. 2873-2882).

European Commission & Kantar Belgium. (2020, January). Europeans' attitudes towards cyber security (Special Eurobarometer 499). https://europa.eu/eurobarometer/surveys/detail/2249

European Union Agency for Cybersecurity (ENISA) & e-Governance Academy (EGA). (2021, November). RAISING AWARENESS OF CYBERSECURITY, A Key Element of National Cybersecurity Strategies. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity/@@download/fullReport

Ferguson, P., & Huston, G. (1998). What is a VPN?

Fernadez Cras, P. (2022, July 6). Dutch University Recovers $550,000 in Ransom From 2019 Hack. Bloomberg. https://www.bloomberg.com/news/articles/2022-07-06/dutch-university-recovers-550-000-in-ransom-from-2019-hack

Frascella, B., Oradini-Alacreu, A., Balzarini, F., Signorelli, C., Lopalco, P. L., & Odone, A. (2020). Effectiveness of email-based reminders to increase vaccine uptake: a systematic review. Vaccine, 38(3), 433-443.

Frik, A., Egelman, S., Harbach, M., Malkin, N., & Peer, E. (2018). Better late (r) than never: increasing cyber-security compliance by reducing present bias. In Symposium on Usable Privacy and Security (pp. 12-14).

Frik, A., Malkin, N., Harbach, M., Peer, E., & Egelman, S. (2019, May). A promise is a promise: the effect of commitment devices on computer security intentions. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (pp. 1-12).

Goutam, R. K. (2015). Importance of cyber security. International Journal of Computer Applications, 111(7).

Grace-Martin, K. (n.d.). Observed Values less than 5 in a Chi Square test–No biggie. The Analysis Factor. Retrieved June 10, 2022, from https://www.theanalysisfactor.com/observed-values-less-than-5-in-a-chi-square-test-no-biggie/

Gurol-Urganci, I., de Jongh, T., Vodopivec-Jamsek, V., Atun, R., & Car, J. (2013). Mobile phone messaging reminders for attendance at healthcare appointments. Cochrane database of systematic reviews, (12).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

Hilton, D., Charalambides, L., Demarque, C., Waroquier, L., & Raux, C. (2014). A tax can nudge: The impact of an environmentally motivated bonus/malus fiscal system on transport preferences. Journal of Economic Psychology, 42, 17-27.

How to create behavior change with security awareness training. (n.d.). HOXHUNT. https://www.hoxhunt.com/ebooks/how-to-create-behavior-change-security-awareness-training

Huitink, M., Poelman, M. P., van den Eynde, E., Seidell, J. C., & Dijkstra, S. C. (2020). Social norm nudges in shopping trolleys to promote vegetable purchases: A quasi-experimental study in a supermarket in a deprived urban area in the Netherlands. Appetite, 151, 104655.

Jenkins, J. L., Durcikova, A., & Nunamaker, J. F. (2021). Mitigating the security intention-behavior gap: The moderating role of required effort on the intention-behavior relationship. Association for Information Systems.

John, P. C. H. (2018). How best to nudge taxpayers?: The impact of message simplification and descriptive social norms on payment rates in a central London local authority. Journal of Behavioral Public Administration, 1(1), 1-11.

Johnson, E. J., & Goldstein, D. (2003). Do defaults save lives?. Science, 302(5649), 1338-1339.

Johnson, E. J., Shu, S. B., Dellaert, B. G., Fox, C., Goldstein, D. G., Häubl, G., ... & Weber, E. U. (2012). Beyond nudges: Tools of a choice architecture. Marketing Letters, 23(2), 487-504.

Jung, J. Y., & Mellers, B. A. (2016). American attitudes toward nudges. Judgment & Decision Making, 11(1).

Kahneman, D. (2011). Thinking, fast and slow. Macmillan.

Kahneman, D., Slovic, S. P., Slovic, P., & Tversky, A. (Eds.). (1982). Judgment under uncertainty: Heuristics and biases. Cambridge university press.

Kankane, S., DiRusso, C., & Buckley, C. (2018, April). Can we nudge users toward better password management? an initial study. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-6).

Karlan, D., McConnell, M., Mullainathan, S., & Zinman, J. (2016). Getting to the top of mind: How reminders increase saving. Management Science, 62(12), 3393-3411.

- Kochovski, A. (n.d.). The Top 25 VPN Statistics, Facts & Trends for 2022. Cloudwards. Retrieved March 18, 2022, from https://www.cloudwards.net/vpn-statistics/
- Kroll, T., Paukstadt, U., Kreidermann, K., & Mirbabaie, M. (2019, June). Nudging People to Save Energy in Smart Homes with Social Norms and Self-Commitment. In ECIS.
- Lock, T. & Freeform Dynamics. (2022, March 2). Why training alone is not enough. ComputerWeekly.Com. https://www.computerweekly.com/opinion/Why-training-alone-is-not-enough
- Loewenstein, G., & Chater, N. (2017). Putting nudges in perspective. Behavioural Public Policy, 1(1), 26-53.
- Ly, K., Mazar, N., Zhao, M., & Soman, D. (2013). A practitioner's guide to nudging. Rotman School of Management Working Paper, (2609347).
- MacDonald, P. L., & Gardner, R. C. (2000). Type I error rate comparisons of post hoc procedures for I j Chi-Square tables. Educational and psychological measurement, 60(5), 735-754.
- Marvin, R. (2018, September 21). Breaking Down VPN Usage Around the World. PCMag. https://www.pcmag.com/news/breaking-down-vpn-usage-around-the-world
- Mol, J. M., Botzen, W. W., Blasch, J. E., Kranzler, E. C., & Kunreuther, H. C. (2021). All by myself? Testing descriptive social norm-nudges to increase flood preparedness among homeowners. Behavioural Public Policy, 1-33.
- Moore, T., Dynes, S., & Chang, F. R. (2015). Identifying how firms manage cyber-security investment. Available: Southern Methodist University. Available at: http://blog. smu. edu/research/files/2015/10/SMU-IBM. pdf (Accessed 2015-12-14), 32.
- Norman, P., Boer, H., Seydel, E. R., & Mullan, B. (2015). Protection motivation theory. Predicting and changing health behavior, 70-106.
- Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cybercrime. Computer Law & Security Review, 21(5), 408-414.
- O'Donoghue, T., & Rabin, M. (1999). Doing it now or later. American economic review, 89(1), 103-124.
- Papies, E. K. (2017). Situating interventions to bridge the intention–behaviour gap: A framework for recruiting nonconscious processes for behaviour change. Social and Personality Psychology Compass, 11(7), e12323.
- Parish, Z., Salehi-Abari, A., & Thorpe, J. (2021). A study on priming methods for graphical passwords. Journal of Information Security and Applications, 62, 102913.
- Plous, S. (1993). The psychology of judgment and decision making. Mcgraw-Hill Book Company.
- Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cyber-security issues. Internet Technology Letters, 4(2), e247.
- Rahimi, S., & Zargham, M. (2011, March). Security analysis of VPN configurations in industrial control environments. In International Conference on Critical Infrastructure Protection (pp. 73-88). Springer, Berlin, Heidelberg.
- Redmiles, E. M., Kross, S., & Mazurek, M. L. (2016, October). How i learned to be secure: a census-representative survey of security advice sources and behavior. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 666-677).
- Reisch, L. A., & Sunstein, C. R. (2016). Do Europeans like nudges? Judgment and Decision making, 11(4), 310-325.
- Reisch, L. A., Sunstein, C. R., & Gwozdz, W. (2017). Beyond carrots and sticks: Europeans support health nudges. Food Policy, 69, 1-10.
- Schenk, D. H. (2011). Exploiting the salience bias in designing taxes. Yale J. on Reg., 28, 253.

Schultz, P. W., Nolan, J. M., Cialdini, R. B., Goldstein, N. J., & Griskevicius, V. (2018). The constructive, destructive, and reconstructive power of social norms: Reprise. Perspectives on psychological science, 13(2), 249-254.

Sharma, K. (2017). Impact of framing and priming on users' behavior in cyber-security. Missouri University of Science and Technology.

Sharma, Y. K., & Kaur, C. (2020). The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World. International Journal of Recent Technology and Engineering (IJRTE) vol, 8, 2336-2339.

Sharpe, D. (2015). Chi-square test is statistically significant: Now what?. Practical Assessment, Research, and Evaluation, 20(1), 8.

Singh, K. K. V., & Gupta, H. (2016, March). A New Approach for the Security of VPN. In Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies (pp. 1-5).

Sjouwerman, S. (2022, June 8). 5 Reasons Why Compliance Alone Is Not Efficient at Reducing Cyber Risks. Corporate Compliance Insights. https://www.corporatecomplianceinsights.com/compliance-not-enough-cybersecurity-risk/

Sunstein, C. R. (2014). Nudging: a very short guide. Journal of Consumer Policy, 37(4), 583-588.

Sunstein, C. R. (2015). Nudges do not undermine human agency. Journal of consumer policy, 38(3), 207-210.

Sunstein, C. R. (2017). Nudges that fail. Behavioural public policy, 1(1), 4-25.

Sunstein, C. R., & Thaler, R. H. (2003). Libertarian paternalism is not an oxymoron. The University of Chicago Law Review, 1159-1202.

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth, and happiness. Yale University Press.

The Decision Lab. (n.d.). Defaults. https://thedecisionlab.com/reference-guide/psychology/defaults

Trope, Y., & Fishbach, A. (2000). Counteractive self-control in overcoming temptation. Journal of personality and social psychology, 79(4), 493.

Tulving, E., & Schacter, D. L. (1990). Priming and human memory systems. Science, 247(4940), 301-306.

Tversky, A., & Kahneman, D. (1985). The framing of decisions and the psychology of choice. In Behavioral decision making (pp. 25-41). Springer, Boston, MA.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. International Journal of Human-Computer Studies, 123, 29-39.

Veaudry, K. (2022). Identification of Barriers to Practicing Cybersecurity by Non-information System Trained Home Users: A Qualitative Study (Doctoral dissertation, Colorado Technical University).

Wall, D. (2007). Cyber-crime: The transformation of crime in the information age (Vol. 4). Polity.

Weijers, R. J., Ganushchak, L., Ouwehand, K., & de Koning, B. B. (2022). "I'll Be There": Improving Online Class Attendance with a Commitment Nudge during COVID-19. Basic and Applied Social Psychology, 1-13.

Weingarten, E., Chen, Q., McAdams, M., Yi, J., Hepler, J., & Albarracín, D. (2016). From primed concepts to action: A meta-analysis of the behavioral effects of incidentally presented words. Psychological bulletin, 142(5), 472.

What is a VPN? (n.d.). EduVPN. https://www.EduVPN.org/what-is-a-vpn/

White, M. (2013). The manipulation of choice: Ethics and libertarian paternalism. Springer.

- Williams, E. J., Noyes, J., & Warinschi, B. (2018, January). How Do We Ensure Users Engage In Secure Online Behavior? A Psychological Perspective. In International Conference on Cognitive and Behavioral Psychology (CBP 2018).
- Wilson, A. L., Buckley, E., Buckley, J. D., & Bogomolova, S. (2016). Nudging healthier food and beverage choices through salience and priming. Evidence from a systematic review. Food Quality and Preference, 51, 47-64.
- Wryobeck, J., & Chen, Y. (2003). Using priming techniques to facilitate health behaviours. Clinical Psychologist, 7(2), 105-108.
- Wryobeck, J., & Chen, Y. (2003). Using priming techniques to facilitate health behaviours. Clinical Psychologist, 7(2), 105-108.
- Zimmermann, V. (2021). From the Quest to Replace Passwords towards Supporting Secure and Usable Password Creation.
- Zimmermann, V., & Renaud, K. (2021). The nudge puzzle: matching nudge interventions to cyber-security decisions. ACM Transactions on Computer-Human Interaction (TOCHI), 28(1), 1-45.

Appendix I
No nudge – Control Group

Protect your accounts from cyber threats!

Dear students,

EduVPN is making it easier than ever for you to add more security for your online credentials. You can download **EduVPN** with two easy steps through the link provided in this email.

Click here to download EduVPN

What having a VPN means? Using **EduVPN** means that you can have access to resources through the internal network of the university! Additionally, you have security and privacy while browsing online from public networks. In simple words, it means that you can securely connect to the university's network from home using an encrypted connection. More information can be found on https://www.EduVPN.org/ .

PRO TIP: In order to make sure you are always protected, enable EduVPN to start on sign-on!

***EduVPN is available for Windows, macOS, Android, iOS, and Linux!**

Thank you for keeping our community safe!

EUR Security Department

Social Norm Nudge

Protect your accounts from cyber threats!

Dear students,

EduVPN is making it easier than ever for you to add more security for your online credentials. You can download **EduVPN** with two easy steps through the link provided in this email.

"88% of people find their digital security important. "

Source: *Economics of Cyber Security course, lecture 10, 2021-2022.*

Click here to download EduVPN

What having a VPN means? Using **EduVPN** means that you can have access to resources through the internal network of the university! Additionally, you have security and privacy while browsing online from public networks. In simple words, it means that you can securely connect to the university's network from home using an encrypted connection. More information can be found on https://www.EduVPN.org/ .

PRO TIP: In order to make sure you are always protected, enable EduVPN to start on sign-on!

***EduVPN is available for Windows, macOS, Android, iOS, and Linux!**

Thank you for keeping our community safe!

EUR Security Department

Priming Nudge

Protect your accounts from cyber threats!

Dear students,

Cyber security concerns us all. The **Security** Department and EduVPN are making it easier than ever for you to add more **security** for your online credentials in order to avoid being **hacked**. You can download **EduVPN** with two easy steps through the link provided in this email.

This is your chance to fight cybercrimes, increase your university's cyber security and protect your accounts!

Click here to download EduVPN

What having a VPN means? Using **EduVPN** means that you can have access to resources through the internal network of the university! Additionally, you have security and privacy while browsing online from public networks. In simple words, it means that you can securely connect to the university's network from home using an encrypted connection. More information can be found on https://www.EduVPN.org/ .

PRO TIP: In order to make sure you are always protected, enable EduVPN to start on sign-on!

***EduVPN is available for Windows, macOS, Android, iOS, and Linux!**

Thank you for keeping our community safe!

EUR Security Department

Commitment Nudge

Protect your accounts from cyber threats!

Dear students,

EduVPN is making it easier than ever for you to add more security for your online credentials. You can download **EduVPN** with two easy steps through the link provided in this email.

You are not connected from your main computer, or you don't have the time right now?

We highly recommend that you note in your calendar and set aside 5 minutes in order to download EduVPN when you do have time!

Set an appointment for yourself so you don't forget!

Click here to download EduVPN

What having a VPN means? Using **EduVPN** means that you can have access to resources through the internal network of the university! Additionally, you have security and privacy while browsing online from public networks. In simple words, it means that you can securely connect to the university's network from home using an encrypted connection. More information can be found on https://www.EduVPN.org/ .

PRO TIP: In order to make sure you are always protected, enable EduVPN to start on sign-on!

***EduVPN is available for Windows, macOS, Android, iOS, and Linux!**

Thank you for keeping our community safe!

EUR Security Department

Reminder nudge

REMINDER: Protect your accounts from cyber threats!

Dear students,

This email is a reminder to download and use EduVPN.

EduVPN is making it easier than ever for you to add more security for your online credentials. You can download **EduVPN** with two easy steps through the link provided in this email.

Click here to download EduVPN

What having a VPN means? Using **EduVPN** means that you can have access to resources through the internal network of the university! Additionally, you have security and privacy while browsing online from public networks. In simple words, it means that you can securely connect to the university's network from home using an encrypted connection. More information can be found on https://www.EduVPN.org/ .

PRO TIP: In order to make sure you are always protected, enable EduVPN to start on sign-on!

***EduVPN is available for Windows, macOS, Android, iOS, and Linux!**

Thank you for keeping our community safe!

EUR Security Department

Appendix II
Debriefing email

Nudging Secure Digital Behavior

Nudging the use of EduVPN

Dear students,

You have recently received an email informing you about EduVPN and prompting you to download and start use it. This email was part of an experiment, in which we tested the effect of three behavioral nudges on the uptake of EduVPN.

All participants either received a control email or an email containing a nudge (i.e., social proof, priming, commitment). All students who had not installed EduVPN after the first email, received a reminder email 1 week later. We only inform you now, since informing you up front could have altered your behavior.

Insights from this experiment are both theoretically interesting and practically useful, as it can help us to optimize future emails. We want to thank you for participating in this study as your contribution will help to make our university safer!

This study was a collaboration between the IT department and behavioral economics department (dr. Sophie van der Zee) and was conducted as a part of a behavioral economics MSc thesis project.

Regardless of whether you installed EduVPN, it's very important for the interpretation of our findings to learn what factors influenced your behavior. Please take 5 minutes to complete this survey _.

If you don't have time now, please set aside 5 minutes in your calendar at a future moment in time.

If you are interested in the results of the study, have any questions or comments or you wish to withdraw your data from the study you can contact us at _.

Thank you for keeping our community safe!

EUR Security Department

Appendix III
Debriefing email questionnaire

	Question	Possible Answers
1	Did you read the email the Security Department sent about downloading EduVPN?	Yes/No
2	Have you downloaded EduVPN?	Yes/No
3	Why did you download EduVPN? (Appears if you answer Yes to Question 2)	o I have used it before, and I was satisfied. o I was persuaded by the information in the email I received. o I did not know that EduVPN was available before receiving the email. o I knew it was available but never got the time to download it. o Other.
4	Why did you not download EduVPN? (Appears if you answer No to Question 2)	o I use another personal VPN. o I do not believe that using a VPN keeps me secure online. o I do not care about my security online. o I will graduate soon so i thought it was unnecessary. o Other.
5	How easy was downloading EduVPN? (Appears if you answer Yes to Question 2)	o Extremely difficult o Somewhat difficult o Neither easy nor difficult o Somewhat easy o Extremely easy
6	Have you activated the start of EduVPN on sign-in? **Starting VPN on sign-in means that each time you sign- in to your computer, EduVPN is activated automatically so you do not need to do so each time you use your device.* (Appears if you answer Yes to Question 2)	Yes/No
7	How useful do you find EduVPN after downloading and using it? (Appears if you answer Yes to Question 2)	o Extremely useful o Very useful o Moderately useful o Slightly useful o Not at all useful
8	What are VPNs for?	o VPNs provide anonymity online. o VPNs provide security online. o VPNs protect your browsing data. o VPNs provide the user with a private network connection. o **All of the above.**
9	What does the acronym VPN stand for?	o Viral Personal Notification o **Virtual Private Network** o Vivid Packaged Negligence o Virtual Parallel Neighborhood o Other

The correct answers appear in bold.