NUDGING CYBERSECURITY MEASURES THROUGH A CHECKLIST

Master Thesis Behavioural Economics | Marketing track

January 2020

Annemijn de Kleijn | 409588

Supervisor: Prof. Dr. Aurélien Baillon

First reader: Dr. M. Hainguerlot

Abstract:
This thesis investigates the effectiveness of a checklist nudge to increase the use of cybersecurity measures for Dutch employees working from home during the COVID-19 regulations. Data were collected through an experiment consisting of two surveys and analyzed with an independent and paired samples t-test. The results show that the checklist was not effective in increasing of the number of cybersecurity measures taken when working from home.

Key words: cybersecurity, nudge, checklist, independent samples t-test, paired samples t-test

Erasmus Universiteit Rotterdam
Erasmus School of Economics

The views stated in this thesis are those of the author and not necessarily those of the supervisor, second assessor, Erasmus School of Economics or Erasmus University Rotterdam

Preface

Laying before you, is my master thesis on the effectiveness of a checklist on cybersecurity measures to take. Due to the COVID-19 pandemic the path of conducting an experiment, writing this thesis and thus finishing my educational career took a different turn than expected. In the amidst of the first pandemic wave, I had to start over with a different research plan than initially decided. Making use of the changing situation to work from home instead of at an office, impacting many employees, I became interested in ways to improve the cybersecurity of those forced to work remotely. With help from my first supervisor, Sophie van der Zee, I conceptualized this new topic into an experiment using two surveys to test the effectiveness of a nudge, a checklist. Personally, being forced to change the topic, the research design and being confronted with changing expectations of finishing my master thesis was not always easy. Luckily Sophie van der Zee helped me with adapting to the situation and making the best out of it. I would therefore like to thank Sophie van der Zee for her enthusiasm on cybersecurity and combining this with a nudge, her critical yet very helpful feedback, and quick responses when I had questions. I would also like to thank my second supervisor Aurélien Baillon for taking over after Sophie found a new job. You helped me get motivated again and finish my thesis with enthusiasm.

I would also like to thank my family and friends for supporting me throughout this process. From helping me reach as many respondents to giving me the mental support and pep talks when I was in doubt or lost motivation. You pushed me to give my best and push my limits in this hard process in the middle of a pandemic.

At last I can happily say that I am proud of the thesis laying before you and thereby ending my educational career. Although it might be in a different way than expected and hoped for, it was very valuable nonetheless.

"It always seems impossible until it's done"
- Nelson Mandela -

Contents

1. Introduction

Since the beginning of the Internet in 1983, online security has been important for users, such as governments and organisations (The Washington Post, 2015). Three years later, in 1986, the United States Congress published the first law regarding computer crimes. This 'Computer Fraud and Abuse Act' made data theft and unauthorized access to networks, among other crimes, punishable by law (US Congress, 1986). Other countries and unions followed as well. For example, the European Union adopted the 'European Data Protection Directive' in 1995 to protect online personal data (European Union, 1995). Over time, this directive has been updated. In 2016 the European Union developed the new and broader 'General Data Protection Regulation' (GDPR), which was enforced in 2018, as a substitute for the old directive (Euopean Union, 2016). The aim of such legislation is to protect both individuals in their private online activities and organizations against cybercrimes. According to the United Nations, there are currently 107 countries worldwide (64%) that have developed legislations to protect online data (United Nations Conference on Trade and Development, 2020).

Just like regular crimes, cybercrimes are evolving over time. Europol (2019) states that cybercrime is becoming more 'bold' nowadays. They observe cybercrime to be maturing and becoming more focussed on new ways to target more profitable institutions. Their 'Internet Organised Crime Threat Assessment' (IOCTA), lists ten main trends of 2019 regarding cybercrime. This list is created annually to report authorities on cybercrime trends and online developments based on impact (Europol, 2017). The ten trends are (1) ransomware, (2) DDos (distributed denial of service) attacks[1], (3) data overload linked to child sexual exploitation material, (4) self-generated explicit material, (5) 'smart cities', (6) attacks on critical infrastructure, (7) fragmentation of the 'Darknet', (8) blockchain marketplaces, (9) business email compromise[2] (BEC), and (10) the EU emergency response protocol.

[1] DDos attacks occur when the 'host' or network of a site or system is overstretched with traffic requests by hackers (Department of Homeland Security, 2019). This can result in the network or 'host' not being able to comply with the requests and therefore shutting itself down, crashing or preventing any access, including access for legitimate users.

[2] 'Business email compromise' (BEC) can take multiple forms but it is mostly aimed at employees. BEC starts with choosing and (usually) 'grooming' a target (FBI, 2017). The next phase is the exchange of information, which could be a requested wire transfer. The final phase is the actual transfer of cash.

Five of these ten cybercrimes are crimes that could be targeted at organisations. These are ransomware, DDos attacks, attacks on critical infrastructure, fragmentation of the 'Darknet', and BEC. These five trends in crimes listed on the IOCTA can have a large impact on organisations and individuals. Cyber viruses used to access the needed information in a hack has grown from 50,000 viruses on average ten years ago to 40 million nowadays. Being used to face-to-face interaction instead of interaction through cyberspace makes us unaware of, and more vulnerable to cybercrimes, due to our perceived anonymity online (Aiken, 2016). The Internet however, enables an "online syndication" in which criminals can easily find like-minded people, thus increasing impact and possible targets. When LinkedIn fell victim to hackers in 2012, more than 6 million credentials of LinkedIn users were stolen (Genova, 2014). When this breach got public, the same hackers emailed users to change their passwords, gaining even more credentials. This is just one example of large impact. During the Ebola outbreak in 2014, thousands of people gave control over their computer after receiving an email, supposedly send by the World Health Organisation (WHO). However, these emails were sent by scammers posing as the WHO (Aiken, 2016).

1.1 COVID-19 pandemic

Cybercrime and therefore also cybersecurity has been an issue since the beginning of the Internet. It does not only affect private individuals but also large corporations and public institutions through their employees. This is even more relevant regarding the current development of the COVID-19 pandemic. In December 2019, this virus was first found in China, causing severe pneumonia (RIVM, 2020). The COVID-19 virus is spread by small particles in air, causing the fast spread around the globe. According to the WHO (2020), there were more than 5,5 million confirmed contaminations worldwide at the end of May (May, 28th) resulting in 5,595,550 confirmed deaths in 216 countries. The pandemic has also reached the Netherlands. At the end of May (May, 28th) there are almost 46,000 cases of confirmed contaminations and 5,903 deaths (RIVM, 2020).

The COVID-19 pandemic has not only affected our health, it also affected cybercrimes. The WHO has stated that attempts of cybercrimes against their data have more than doubled during the pandemic crisis (Reuters, 2020). A large group of hospitals in Paris were hit by a DDoS attack while being busy treating COVID-19 patients (VPNoverview, 2020) and another DDoS attack was targeted at a large food delivery service in the Netherlands (NLTimes, 2020). In the Netherlands, the number of cybercrimes occurring in April 2020 increased with 174% in comparison to the previous year (De Volkskrant, 2020). The Dutch audit office even stated that the Dutch Ministry of Foreign Affairs doesn't have enough security measures in place to protect their online data (De Volkskrant, 2020).

This globally spread virus has caused many governments to put regulation into place to get control over the contamination rate, including the Dutch government (Rijksoverheid, 2020). On the 12th of March, Dutch citizens were first told to work from home instead of going to their office, unless they work in a vital sector (NRC, 2020). These regulations are temporary and change regularly. By working from home people are able to socially distance themselves from others outside their household, slowing down the fast spread of contaminations. Only employees in vital sectors are allowed to go to work outside of their homes. It is estimated that one in three employees is not working in a vital sector and therefore should be able to work from home (De Volkskrant, 2020). An analysis from Google (2020) into movements in the Netherlands, shows that there is a 78% decline in mobility linked to work places compared to their baseline. This is in line with a decline of 85% in the number of people using public transport (Metro, 2020).

Although there are also positive effects of decline in mobility, such as fighting climate change (The New York Times, 2020) or new innovations needed to adapt to the regulations (FYA, 2020), many news channels are reporting higher online risk due to working from home during regulations and hackers being aware of the vulnerability of employees working from home (CNBC, 2020; Reuters, 2020; EenVandaag, 2020; FYA, 2020). First of all, when working from home, more (private) devices are used by employees to do their job (Business Insider, 2020). When multiple devices are connected through a WIFI-network at the same time there is an increase in possible entry points for hackers. Second, the online activity of employees is growing. Instead of meeting in the office, online conference tools like Zoom and Skype are used. More online activity makes it easier for hackers to find a target. Working remotely due to the COVD-19 regulations therefore increases the opportunities for cybercrimes to occur. Though some experts expected regulations to be temporary and to have a vaccine by fall, it soon became clear that a vaccine would at best become available at the end of 2020 (Medical News Today, 2020; Het Parool, 2020). Regulations to work from home keep being extended and are becoming 'the new normal' (Rijksoverheid, 2020). Thus, it is of high priority for organisations and their employees to minimize the chances of cybercrimes.

1.2 Relevance of this thesis

What can be done to minimize being exposed to cybercrimes and thus increase the use of cybersecurity measures? Though some research has shown that awareness for cybercrimes can be increased by training (Whalen, 2001) other research has stated that there are conditions for trainings to be effective (Wilson & Hash, 2003). Other methods that are previously studied are the use of video games to experience possible online situations (Cone, Irvine, Thompson, & Nguyen, 2007) or the use of an awareness campaign (Higgins, 1998), just to name a few. Another tool to increase the use of cybersecurity measures is the use of behavioural insights.

Behavioural insights from psychology are used in economic models to influence behaviour using our automatic thinking (Kahneman & Tversky, 1979; Thaler, 1980). In practice, people do not always behave in a rational way, but use heuristics. This creates biases. Knowing these heuristics and biases gives an opportunity to steer people’s behaviour. Such insights could provide a stimulus for employees to become aware of cybersecurity measures when working online from home and to take action to apply such measures. However, no research has been conducted on the use of behavioural insights in increasing the use of cybersecurity measures. A behavioural stimulus to increase the use of cybersecurity measures must be easy to understand, easy to apply and low in development costs. More importantly, this stimulus, or nudge, must not be forced on to individuals but must be easy to deviate from (Thaler & Sunstein, 2009).

There are many different nudges which can be applied in many everyday situations. One example of a nudge is a checklist. Research on the use of checklists is mostly done on applying checklists in a medical context. For example, de Korne et al. (2010) examined the application of checklists in an intensive care unit in the Netherlands. They concluded that the use of a checklist in the work process of health care professionals leads to better standardization of the process and thus improved patient safety. Haynes et al. (2009) looked into the effectiveness of checklists in operating rooms instead of intensive care units. They tested whether a checklist for communication among teams and standardization would improve the safety of surgeries. This checklist resulted in a decline in the death rate during surgeries. Thus, in the context of health care a checklist improves the safety of patients. This thesis will investigate whether the use of a checklist can also be applied to the context of cybersecurity to improve the online safety of employees working from home. A checklists as a nudge can be used to provide not only a clear list with cybersecurity measures to take but also nudge employees into actually taking more cybersecurity measures.

The aim of this thesis is to examine the effect of a checklist nudge to promote cybersecurity measures used by employees working from home. Therefore, the main research question of this thesis is as follows:

‘What is the effect of a checklist on the use of cybersecurity measures by Dutch employees working from home?’

2. Literature review

2.1 Cybersecurity

Several articles have contributed to defining the term 'cybersecurity' (Kemmerer, 2003; Lewis, 2006; Amoroso, 2006). A study by Craigen, Diakun-Thibault and Purse (2014) was conducted to define cybersecurity in the most broad and clear definition. They combined several definitions from previous literature with different perspectives on cybersecurity into one definition. They define the term 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". Thus, it can be concluded that cybersecurity ranges from policies by government to measures taken by individuals. The purpose is not only to detect cybercrimes but also to minimize the opportunities of possible cybercrimes. This definition of cybersecurity will provide context for the term cybersecurity as used in this thesis.

2.1.1 Improving the use of cybersecurity measures

Our sense of anonymity online and cyberspace being a virtual space instead of physical, causes a perceived sense of safety (Aiken, 2016). Aiken claims that this perceived safety could lead to online behaviour in which we are unaware of online risks and therefore not protected against it. She states that cybersecurity is complex for non-experts due to the constantly changing technology and is mostly associated only with the measure of changing passwords regularly. The complexity of cybersecurity is caused by the fast development of new online possibilities and information overload. For hackers on the other hand, who are online experts, there is no authority with online jurisdiction, making the chances of being caught minimal. Aiken claims that most hacks are possible because of not taking cybersecurity measures such as strong password use.

A vast amount of research has been conducted on improving the use of cybersecurity measures. The effect of a classic awareness training is disputable. Whalen (2001) studied the human factors in computer security for coast guard members. Both their current awareness of computer security and possible ways to increase awareness were tested. Current awareness was measured using a survey, resulting in recommendations on ways to increase awareness. The study concluded an awareness training to be the most effective for coast guard members to increase awareness on online risks. Likewise, Aiken (2016) claims that being informed and getting to know a new (online) environment by doing research about it and knowing the risks is the best approach to adapt. However, other researchers have concluded that there are conditions to a training to be effective (Wilson & Hash, 2003). Wilson and Hash created a guideline identifying four conditions in the 'life cycle' of an awareness training. In the first phase internal research must be done within the firm to assess the needs for a training. Then the means of the firm, the audience, and material content needs to be discussed. The third phase focusses on the communication of the training and materials. The life cycle ends with evaluation of the training and using feedback methods to measure the effectiveness.

Likewise, a study by Beuran, Chinen, Tan and Shinoda (2016) was conducted to identify requirements for cybersecurity trainings to be effective. Five Japanese trainings were analysed based on ten features, including participants, level of current knowledge, training content and needed skills. They concluded that a training should (1) fit the knowledge and skills level of participants, (2) be in line with the needed skills of the program, (3) use practical assignments based on real-life situations, (4) have as many participants as possible to improve impact, and (5) should be sustainable in terms of costs and performances. Complementary to this, according to Bada, Sasse and Nurse (2019), changing online behaviour is not achieved by only providing information through training or an awareness campaign. They state, based on literature research, that individuals need to understand and be able to apply the information learned, and be willing to do so.

Being aware of online risks doesn't mean cybersecurity knowledge is applied in real life. An overload of complex information can lead to 'security fatigue' causing avoidance of cybersecurity measures. They conclude that (1) only organised and professional awareness campaigns are effective, (2) using fear can cause avoidance of measures, (3) a training needs to be "targeted, actionable, doable and provide (continuous) feedback", and (4) awareness campaigns need to be adapted to different cultures.

Several studies have looked into applying information regarding cybersecurity measures. Aldawood and Skinner (2019) have created a literature overview of 30 of these recent studies. Their analysis is aimed at defining needs for a cybersecurity training and how to implement the received knowledge. One way to apply the information regarding cybersecurity measures is through interactive videos (Alkhamis & Renaud, 2016). This tool allows information to be easily provided to many participants at low costs. Receiving information in an interactive way increases the effectiveness. In the experiment, Alkhamis and Renaud developed an interactive video which was tested within a company with 24 employees. They concluded the tool to be effective. Moreover, an interactive video is easy to adjust for different cultures of knowledge levels, as suggested by Bada, Sasse and Nurse (2019). Instead of an interactive video, a video game could have the same results according to Cone, Irvine, Thompson and Nguyen (2007). The use of a video game to train employees enables them to experience online risks in the save environment of a game. This helps them understand the risks and measures that can be taken. A video game was developed for the federal government of the United States and was later adapted to be used by educational institutions, with a total of 130 organisations and was showed to stimulate cybersecurity awareness. Educational video games are furthermore "lowering the barrier between education and real entertainment", and encouraging individuals to learn about various topics in an exciting way (Bellotti, Berta, Gloria, & Primavera, 2009).

To conclude, there are several tools to increase awareness online and to implement knowledge to stimulate the use of cybersecurity measures. However, these tools, such as an awareness training, take time to be developed. Tools furthermore need to be adapted to the user(s), adding time to the development process. Therefore, creating a specific tool can be costly and depends on an employer to be willing to make the effort and investment. Since employees are asked to work from home during the current COVID-19 regulations and not gather with colleagues, these tools might not be compatible with improving the use of cybersecurity measures on an individual level.

2.1.2 Cybersecurity measures lists

Multiple organisations have developed lists to provide recommendations to improve cybersecurity for employees when working from home due to the COVID-19 outbreak. One of them is the Cyber Readiness Institute. Their goal is "to provide free tools and recourses that your business can use to reduce risks" (The Cyber Readniess Institute, 2019). According to their guideline "Data Protection Basics for Remote Workers" the first step is to be aware of the used device and connection to the internet. The basic tips to work remote securely include not sharing passwords, know what type of data is stored on the device, and using passwords for confidential files (Cyber Readiness Institute, 2020). Their guideline on securing a home office includes taking measures such as using multi-factor authentication, updating regularly and sharing online data through secured software (Cyber Readiness Institute, 2020). However, these lists are incomplete or focussed on preventing a specific cybercrime. The Dutch National Cyber Security Centre (NCSC), part of the Dutch Ministry of Justice and Security, has also provided recommendations for cybersecurity measures when working remotely (Nationaal Cyber Security Centrum, 2020). This list contains more complete and specific measures, such as using a secured connection and using multi-factor authentication.

2.2 Nudging

In their book *Nudge*, Richard Thaler and Cass Sunstein (2009) define a nudge as a gentle push in the right direction without the obligation to follow that direction. In the context of 'nudging a person' this means steering someone in the right direction by a subtle nudge. A nudge makes use of our automatic thinking. Kahneman (2011) states that there are two types of thinking; system 1 and system 2 thinking. These systems refer to two 'states of mind'. System 1 refers to our automatic, unconscious and fast thinking which is used to make everyday decisions and to survive, like recognizing people. Nudges can influence our automatic thinking due to the unconscious use of the system. Hence, without consciously knowing it, individuals are pushed towards a desired choice which is made easier by providing a nudge. System 2 on the other hand, refers to our slower and more conscious thinking which costs more energy to use. When making complex puzzles, system 2 becomes active.

Sunstein (2020) explains the concept of nudging by using the metaphorical example of an GPS device. When using a GPS a person is in control of choosing the destination and to deviate from the recommended route. A nudge is used to influence behaviour without limiting the person on which the nudge is implemented, in his or her freedom. Ly, Mazar, Zhao and Soman (2013) define a nudge as a "deliberate change in choice architecture with the goal of engineering a particular outcome". Nudges change behaviour without the need for restricted choices or monetary incentives. They further state that a nudge can be used in several dimensions. For example it can be used to boost self-control like saving money or to activate a desired behaviour of the individual like sustainable behaviour. Thus, the aim of a nudge is to be beneficial for the individual being nudged. As Sunstein (2015) mentions in his research "much nudging promises to increase social welfare". However, he also acknowledges that it is important to be aware of the ethics when using a nudge. A government using a nudge for its citizens might have a different opinion on what's best for an individual than an employer using a nudge for his or her employees. To summarize, a nudge is a gentle push towards a desired decision which ought to be beneficial for the individual being nudged or to increase social welfare. This could be in the context of better wellbeing or more wealth, for example. The aim of a nudge is chosen by the individual or institution implementing the nudge.

Using nudges is part of a 'movement' called "libertarian paternalism". The idea behind this movement and thus the use of a nudge is that on one hand individuals are at all-times at liberty to avoid a nudge and make a decision themselves. This is the libertarian aspect. On the other hand the paternalistic aspect means that by nudging people, the decision towards which the individuals are nudged should be in the best interest for that individual (Thaler & Sunstein, 2003).

2.2.1 Choice architecture

Choice architecture is used to nudge people towards choosing for the desired option of that choice. Choice architecture can be defined as shaping the context and design of a choice (Thaler, Sunstein, & Balz, 2013). Changing the context and design could therefore change the decision that is being made. Every decision that needs to be made, needs to be framed in some way and therefore every individual that has (indirect) influence on the choice of others is a choice architect (Thaler & Sunstein, 2009). In their book, Thaler and Sunstein use an example of a school canteen. When choosing the positions for the unhealthy snacks, the designer can choose a random spot. However, this random spot could be near the entrance. This spot leads to a higher number of students buying the unhealthy snacks, as it is one of the first things they see. The designer could also choose to put the snacks in the end, leading to lower sales of the snacks but healthier students since they have mostly likely picked other foods before seeing snacks. This example shows that every choice needs architecture. According to Thaler and Sunstein the "golden rule" for this architecture is to provide a nudge towards the decision with the highest probable positive outcome and the least probable negative outcome. Camerer et al (2003) use as the golden rule to help the least developed individuals at minimal costs for others.

2.2.2 Nudges in practice

The application of nudges in practice is diverse and used in several contexts. Dolan et al (2012) created the 'Mindspace' framework to explain nine types of nudges that have the most behavioural influence. These nine types are messenger, incentive, norms, defaults, salience, priming, affect, commitment, and ego. The messenger effect refers to the influence a messenger can have and the weight given to the message from this messenger. The second effect of the 'Mindspace' framework is incentives. Individuals are sensitive to prices and can therefore be nudged by using a monetary reward or cost (Dolan, et al., 2012). The third effect is norms, which refers to "social or cultural norms (…) or rules, within a society or group". A media campaign showing the norm that a lot of people use a seatbelt when driving a car led to an increase of people stating to follow that behaviour (Linkenbach & Perkins, 2003). Default refers to the standard option of a decision (Dolan, et al., 2012). Many individuals tend to not deviate from that default option. Therefore, changing the standard option can affect people's behaviour. Salience refers to the fact that our attention is drawn to things that seem salient. Information is taken into account more easily when the message is spread in a new way or when it stands out compared to others.

The use of a checklists uses the same intuition. Providing a list with measures as a checklists makes it more salient to people than a regular list of measures. The priming effect makes use of our associative thinking (Thaler & Sunstein, 2009). Priming cinema visitors with a larger popcorn bucket made visitors eat 45% more popcorn (Wansink & Kim, 2006). The affect nudge leads to behavioural change due to experienced emotions which affect our decisions (Dolan, et al., 2012). Repeated use of words for a brand, positive or negative, can change the brand choice that consumers make when buying a product (Gibson, 2008). Using the nudge (pre-)commitment can help individuals to stop procrastinating and instead think about long-term goals (Dolan, et al., 2012). A bank that provided a savings account in which individuals commit to not access their savings led to higher savings by users of the product (Ashraf, D, & Yin, 2006). "We tend to behave in a way that supports the impression of a positive and consistent self-image" refers to the ego effect (Dolan, et al., 2012). When American students were asked if they drive better than the average person, 93% claimed to drive better, which is statistically impossible (Suis, Lemos, & Stewart, 2002).

To conclude, nudges can be used in many ways and in many fields. The cues can be very small and still have a large effect on the behaviour of individuals. This change can be achieved without forcing individuals to change their behaviour. A nudge provides the subtle push in the right direction. The 'Mindspace' framework conceptualizes the nine main themes to change behaviour. This context of nudging and the 'Mindspace' framework provide context for the research conducted in this thesis.

2.3 Checklists as a nudge

The use of a checklist to frame a choice has been researched mostly in the field of medical research. De Korne et al (2010) did research in a Dutch intensive care unit (ICU) to test if several aviation innovations, including checklists, improved patient safety. The study found evidence that using a checklist helped to standardize the work of medical employees during surgeries. Compared to data multiple years before implementation, using the checklist led to less wrong-site surgeries, thus improving patient safety. Research by Pronovost et al (2006) found that a checklist used in an ICU could also lead to a decline in infections. Based on measurement of catheter-related bloodstream infections before implementations and 18 months after, with three-monthly interval, they concluded a checklist to result in a decline of 66% of infections, after the last measurement 18 months after implementation. Pronovost (2010) later stated that this reduction in infections and thus healthcare costs, could save a hospital $2 million each year.

Haynes et al (2009) concluded similar results regarding reduction in surgical complications and deaths. They researched eight hospitals worldwide for a year to test the effectiveness of a checklist. The percentage of surgeries resulting in death decreased from 1.5% to 0.8% whereas percentage of complications during surgery decreased from 11% to 7%. Beneficial effects of a checklist were also concluded in research on pre-post intervention in Dutch hospitals (de Vries, et al., 2010). This study analysed whether a checklist is also effective for complications outside operational rooms. After measuring the rate of complications three months prior intervention and three months after, it was concluded a checklist reduces the rate of complications from 27.3% to 16.7%. Research on 167 hospitals in England and Wales using WHO checklists concluded that, next to improved safety in 68% of the hospitals, there was also an increase in teamwork in 77% of the hospitals and near misses that were prevented in 41% of the hospitals (National Patient Safety Agency, 2012).

To explain why the use of check(list)s can help prevent errors during surgery, Reason (2000) has created a 'Swiss cheese model'. The cheese metaphor is meant to show that there are several layers (slices) of checks needed to prevent errors from moving through the holes in the system (cheese). The more layers the better. This system of multiple checks is helpful in the complex context of healthcare to decrease the risk of errors and reduce the impact caused by errors that might get through the system. This context of complex layers and technology is similar to the complexity of cybercrime. According to Aiken (2019), cyberspace consists of many layers. She claims that cyberspace is not comparable to an infrastructure, as often used as comparison, but "is an entity that can have an almost overwhelming impact on individuals and society." The effectiveness of a checklist to improve patient safety in healthcare with similar complexity as cyberspace could suggest positive impact from using a checklist on using cybersecurity measures.

2.3.1 Nudging the use of cybersecurity measures

Cybercrimes and therefore cybersecurity is always evolving, with crimes becoming more bold and cybersecurity more complex (The Washington Post, 2015; Europol, 2019). Although providing information through a training or an awareness campaign is effective in raising awareness and understanding, it might not be effective in actually changing the behaviour of individuals into taking more cybersecurity measures (Whalen, 2001; Wilson & Hash, 2003; Bada, Sasse, & Nurse, 2019). Received information and new knowledge from trainings need to be applied to become more effective in actually changing behaviour into taking more measures (Aldawood & Skinner, 2019; Alkhamis & Renaud, 2016; Cone, Irvine, Thompson, & Nguyen, 2007).

Taking cybersecurity measures became even more relevant since the outbreak of the COVID-19 pandemic. This led to employees being forces to work from home and therefore being more vulnerable to cybercrime, and increased attempts of cybercrimes (NRC, 2020; Reuters, 2020; De Volkskrant, 2020).

Nudges can help to push individuals in a desired direction (Ly, Mazar, Zhao, & Soman, 2013; Sunstein, 2015; Thaler & Sunstein, 2009). Even a small nudge can have a large effect on behaviour (Ashraf, D, & Yin, 2006; Dolan, et al., 2012; Gibson, 2008; Linkenbach & Perkins, 2003; Suis, Lemos, & Stewart, 2002; Wansink & Kim, 2006). Choice architecture can help to frame everyday decisions and use nudging to steer individuals towards a decision. This is done without forcing people to make a choice.

However, the ethics when using a nudge must be considered by the individual or institution using a nudge. This should be in the best interest of the individual that is being nudged.

Applying salience to nudge people into taking more measures by providing them with a checklist would be less costly and more time-efficient than following an awareness training. Adapting it for different users is not as time consuming and costly as adapting escape rooms and video games. A checklist has already been proven to be beneficial in the health care sector, leading to improved patient safety. In the context of cybersecurity this could imply that the use of a checklist can improve the online safety of employees working remotely from home due to the COVID-19 pandemic. Therefore the main hypothesis that will be tested is as follows:

H1: Using a checklist as a nudge to inform employees working from home about cybersecurity measures will lead to an increase in the number of measures taken by this employee.

However, the effects of the checklist used in this thesis needs to be tested after a period of seeing this checklist. This means that the change in taken measures can be caused by not just the checklist but due to the difference in time. Time can cause changes in taken measures because of two reason; the Hawthorne effect and the effect of learning in between measurements. The Hawthorne effect was first used to describe increased productivity of workers in an experiment due to a response on the research itself instead of actually increased productivity (McCarney, et al., 2007). In between the two moments of measuring respondents were possibly made aware of increased cybercrime caused by the COVID-19 pandemic by media or their employer. Several news articles described the effect of the COVID-19 pandemic on cybercrime attacks (RTL Nieuws, 2020; Business Insider, 2020; De Volkskrant, 2020; EenVandaag, 2020; CNBC, 2020; Reuters, 2020; NOS, 2020). Reading such articles can make respondents more aware of cybercrime between the start of the experiment containing the first measurement and last measurement. Therefore, the second hypothesis that will be tested is as follows:

H2: There is an increase over time in the use of cybersecurity measures that are taken by employees working from home.

3. Research methodology

An experimental research design was chosen to answer the research question, with treatment as the between-subjects variable. An independent samples t-test and paired samples t-test was used for data analysis. Ethical approval was requested to conduct this research. This has resulted in the ERIM Internal Review Board, Section Experiments granting approval to conduct this experiment. The approval has been registered under the code 2020/04/04-66842svz.

3.1 Research design

I conducted an online experiment, consisting of two surveys. Both were available in Dutch and English. Survey 1 was conducted first to establish a baseline and to introduce the checklist based on the measures recommended by NCSC (Nationaal Cyber Security Centrum, 2020). Survey 2 was used to establish the number of cybersecurity measures taken three weeks after the distribution of Survey 1. This allows for comparison of cybersecurity measures taken over time. Therefore, this experiment has a between-subject design.

Existing research has used a time span between three to 18 months to measure the effect of a checklist (Haynes, et al., 2009; Pronovost, et al., 2006). However, due to the exogenous factor of temporary regulations to work from home, changing every couple of weeks, the time span between the two surveys was three weeks. Otherwise the change in regulations between these two times of measurement might have affected the results. Survey 1 was spread during the second week of April. During this week, regulations to work from home were in place until at least the 28th of April (NU.nl, 2020). On the 21th of April the regulations regarding working from home were extended until the 19th of May (Rijksoverheid, 2020). Survey 2 was spread during the last week of April. Several reminders were sent in the first two weeks of May.

During Survey 1 both the control and treatment group were informed about measures that might be taken to improve online security. However, to the control group, these measures were shown as a list of statements whereas the treatment group was presented with the measures in the form of a checklist. The control group was then asked for each statement whether it applied to them or not. The treatment group was asked to check the boxes of measures that are taken. For the quantitative analyses, the mean number of measures taken after the nudge (checklist) in the control group was compared with the mean number of measures taken after the nudge (checklist) in the treatment group.

3.2 Sample selection & participants

Both surveys were aimed at employees that would normally work from an office but were forced to work from home due to the regulations. Following an expected effect size of 0.5, alpha (α) of 0.05 and power of 0.80, the required total sample size is equal to 128 (List, Sadoff, & Wagner, 2011). These respondents were reached by spreading the survey through social media channels such as Instagram, LinkedIn and Facebook groups. A message containing the research topic and the request to participate was spread through the social media channels. Every person above the age of 18 was allowed to participate in the experiment and fill in the survey. Participation took 4-6 minutes and participants were not compensated in any way. To reach the same respondents again for Survey 2, they are asked to fill in their email address. These email addresses are linked to a respondent id number in a separate file than the data file. After the research this file linking email addresses to ID numbers was deleted in order for respondents to answer anonymously.

Survey 1 initially led to a sample size of 207 respondents. However, if respondents reported that their working conditions were not affected by the Dutch regulations they were removed from the sample, which was reported by 5 respondents. Therefore, the sample size for the first survey after removing these respondents from the data consists of 202 respondents. Survey 2 was filled in by 185 respondents. Therefore, the 17 respondents that did not complete the second survey were removed from the sample (Wood, White, & Thompson, 2004; Powney, Williamson, Kirkham, & Kolamunnage-Dona, 2014). Of these 185 respondents, 6 respondents reported their working conditions were not affected anymore by the Dutch regulations at the time of Survey 2. Thus, the final sample consists of 179 respondents (108 female, 1 not specified, 70 males; age 20-64, M=41, SD=12.85). The control group consists of 87 respondents (49%) and the treatment group of 92 respondents (51%).

3.3 Research materials

The checklists used in this experiment can be divided into three categories; networks, passwords and materials. The measures concerning networks includes the use of a Wi-Fi network (with password or not) or the use of a Virtual Private Network (VPN) connection, which enables the user to browse on a secured network. The second category contains the use of strong passwords, two-factor authentication or password manager software. Two-factor authentication means that the user has to go through an extra layer of security when entering passwords. Password manager software generates strong passwords for the user which are accessible through one master password. The last category of the checklist, materials, contains measures like the use of a work device and recently updated software. The complete checklist can be seen in Appendix 2.

Both Survey 1 and Survey 2 started with a message to inform participants about the research topic in general and the two surveys that were used in this study. This message also contains an informed consent stating that the participants are 18 years or older, that they agree to the use of their data anonymously and that they are able to stop participation in the research at any moment. See figure 1 for a flowchart of the rest of Survey 1 and 2.

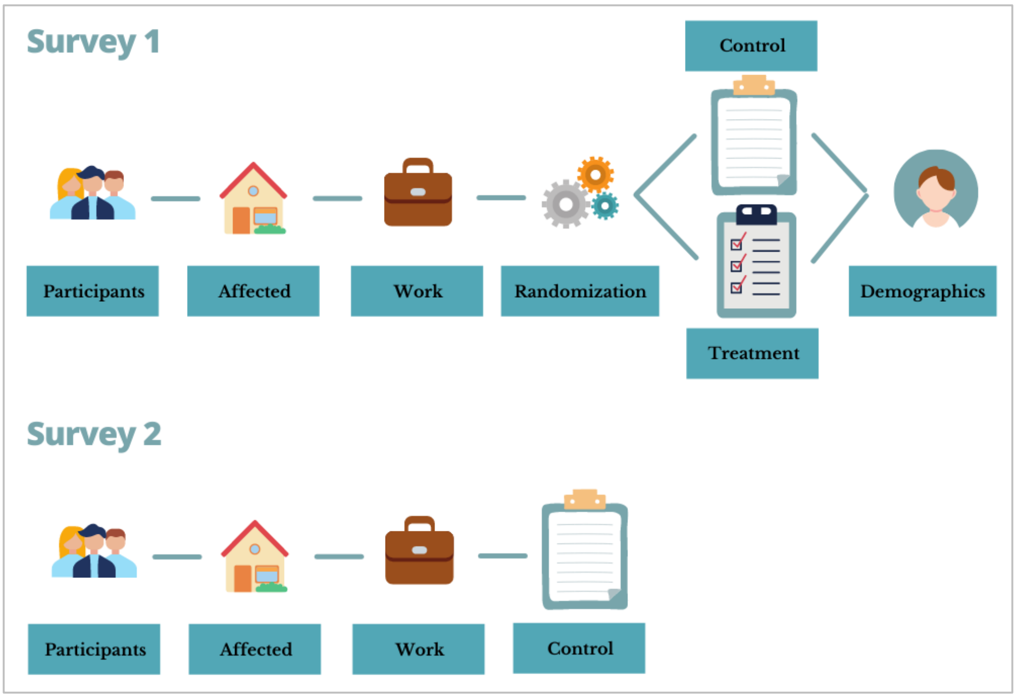


Figure 1: Flowchart of Survey 1 and Survey 2 after informed consent.

After giving consent the participants were first asked whether their working conditions were affected by the Dutch regulations at that time ('Affected' in figure 1). This was used to remove respondents from the sample if not affected.

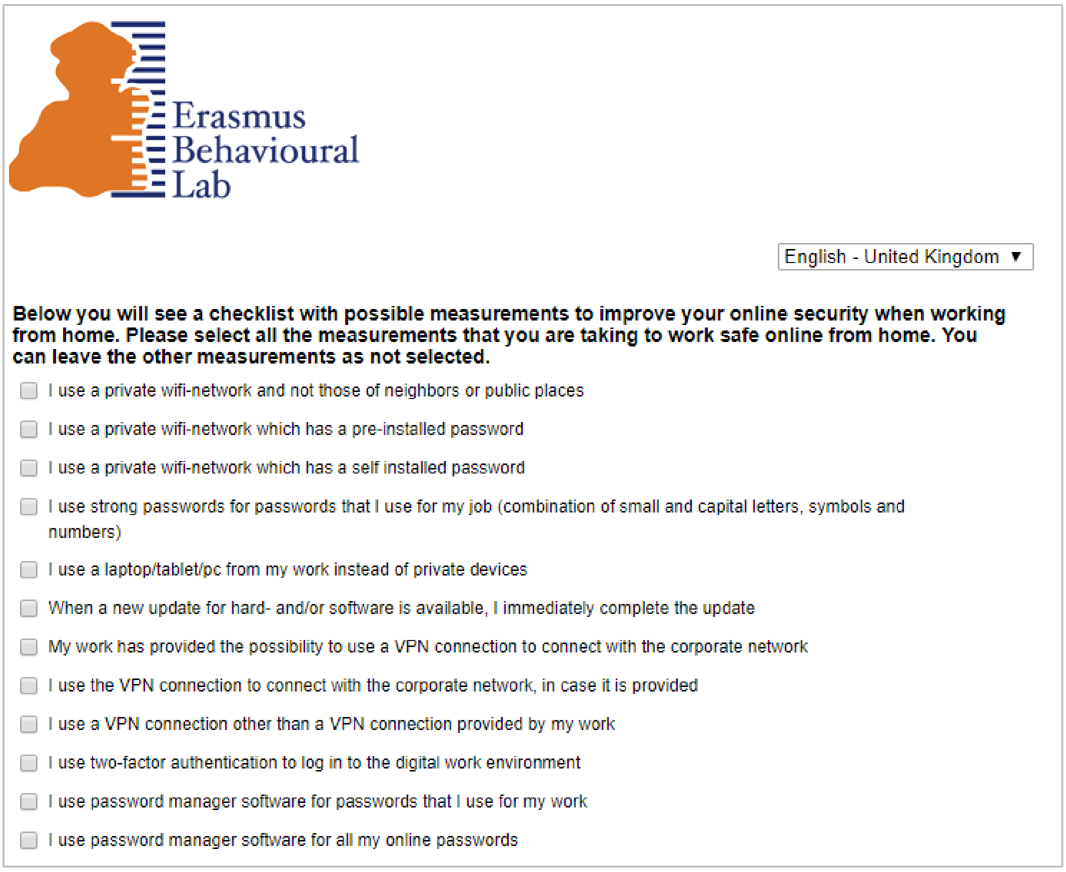
Respondents then answered several work-related questions ('Work' in figure 1). First, they reported whether they worked from home before full-time, regularly, rarely or didn't work from home prior to the regulations. The same question is asked in the second survey to check whether the working conditions are still affected by the regulations. Respondents were also asked about the effect of the Dutch regulations on the time worked from home, their mental health when working from home, and their productivity when working from home, ranging from 'severe decline' to 'severe increase'. This allows analysing whether the Dutch regulations affected working conditions other than online safety when working from home. Respondents were then asked if they are responsible for the care of others (e.g. children or elderly) when working from home. These questions were also asked in the second survey to be able to look at differences in effects over time (see figure 1). To understand the environment in which the respondents are working from home they were shown a list with possible situations. Such as 'I work in a separate room' or 'I work on a laptop'. The respondents were asked to tick the boxes that applied to them. Multiple answers were possible. This question was repeated in the second survey to check whether respondents made any changes in their work environment. Respondents were then asked about the working sector. This was chosen from a list containing all sectors.

When respondents moved to the next page, they were randomly assigned to either the control group or treatment group ('Randomization' in figure 1). This was not known by, or visible to the respondents. Respondents were then shown a list of statements or a checklist of cyber security measures depending on being in the control group (statements) or treatment group (checklist). This list and checklist contains the set of measures that are based on the list by NCSC (Nationaal Cyber Security Centrum, 2020). These measures were translated into statements. For example, the advice to use a trusted (Wi-Fi) network was translated into the statement 'I use a private Wi-Fi-network and not those of neighbours or public places'. See the complete list and checklist in figure 2 and 3. Respondents assigned to the control group were asked to state for each measure if they are currently taking it or not, to work securely from home, or don't know ('Control' in figure 1). Respondents assigned to the treatment group were asked to tick the boxes in the checklist for the measures they are taking ('Treatment' in figure 1). In Survey 2 all respondents were shown the same list with measures as seen by the control group in Survey 1 (see figure 1). Again, they were asked to state for each measurement if they are currently taking it or not when working from home, or whether they don't know ('Control', Survey 2 in figure 1).

Next, respondents were asked about their demographics, including age and gender ('Demographics' in figure 1). The demographic questions were not repeated in Survey 2. The respondents are requested to fill in their email addresses at the end of Survey 1. See Appendix 5 for the complete Survey 1.Respondents were again informed about the use of their email address to be able to send Survey 2. After these questions the respondents were shown a debriefing and were given the possibility to request the results of the research when available.

Three weeks after filling in Survey 1, participants were asked to fill in Survey 2. This was requested by email, which was gathered in Survey 1. Survey 2 started with general information about the research. This message also contains an informed consent stating that the respondents are 18 years or older, that they agree to the use of their data anonymously and that they are able to stop participation in the research at any moment. First, participants were asked whether the Dutch regulations were still affecting working conditions at the time of filling in Survey 2 ('Affected' in figure 1). Again, participants were asked work-related questions ('Work' in figure 1). First, they reported again on what level the Dutch regulations affected the time working from home, mental health, and productivity when working from home. Taking care of others (elderly or children etc.) was asked again. Respondents were asked about working environment by ticking boxes such as 'I work in a separate room' or 'I work on a laptop'.

Respondents were then again asked about the cybersecurity measures they are taking when working from home ('Control' in figure 1). This was presented as a list of statements. This list is equal to the list of statements for the control group in Survey 1. At the end of the survey the respondents were again informed on the anonymous use of data. See Appendix 6 for the complete Survey 2.



English - United Kingdom ▼

Below you will see a checklist with possible measurements to improve your online security when working from home. Please select all the measurements that you are taking to work safe online from home. You can leave the other measurements as not selected.

□ I use a private wifi-network and not those of neighbors or public places

□ I use a private wifi-network which has a pre-installed password

□ I use a private wifi-network which has a self installed password

□ I use strong passwords for passwords that I use for my job (combination of small and capital letters, symbols and numbers)

□ I use a laptop/tablet/pc from my work instead of private devices

□ When a new update for hard- and/or software is available, I immediately complete the update

□ My work has provided the possibility to use a VPN connection to connect with the corporate network

□ I use the VPN connection to connect with the corporate network, in case it is provided

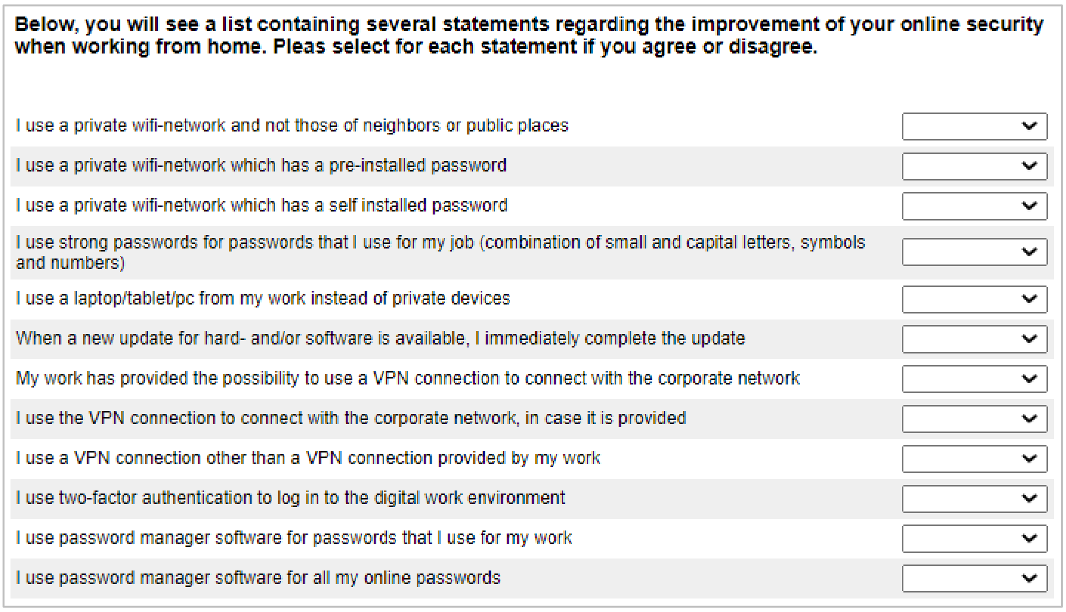
□ I use a VPN connection other than a VPN connection provided by my work

□ I use two-factor authentication to log in to the digital work environment

□ I use password manager software for passwords that I use for my work

□ I use password manager software for all my online passwords

Figure 2: Checklist used in experiment during Survey 1, as seen by treatment group.



Below, you will see a list containing several statements regarding the improvement of your online security when working from home. Pleas select for each statement if you agree or disagree.

I use a private wifi-network and not those of neighbors or public places

I use a private wifi-network which has a pre-installed password

I use a private wifi-network which has a self installed password

I use strong passwords for passwords that I use for my job (combination of small and capital letters, symbols and numbers)

I use a laptop/tablet/pc from my work instead of private devices

When a new update for hard- and/or software is available, I immediately complete the update

My work has provided the possibility to use a VPN connection to connect with the corporate network

I use the VPN connection to connect with the corporate network, in case it is provided

I use a VPN connection other than a VPN connection provided by my work

I use two-factor authentication to log in to the digital work environment

I use password manager software for passwords that I use for my work

I use password manager software for all my online passwords

Figure 3: Measures list used in experiment during Survey 1, as seen by control group.

3.4 Research procedure

3.4.1 Recruitment

The respondents were gathered through social media. Accompanied by a message containing the research topic of working safe from home during the COVID-19 regulations, was a request to use the link in the message to fill in Survey 1. This message was spread through LinkedIn, Facebook and Instagram. On LinkedIn and Facebook the message was shared by several connections. Hence, all respondents came across the study through one of these social media channels being either a connection in the first degree or through mutual connections sharing the message. Survey 2 was sent through email containing a reminder to agreeing to participate in the second survey and a personal link. This personal link is generated by linking email address to a respondent ID number. This allows the data of Survey 2 to be matched with Survey 1 based on respondent ID number instead of email address and therefore using the data anonymously. Several reminders were sent to gather as much respondents as in the first survey. After the research, all email addresses will be removed for ethical and anonymity purposes.

3.4.2 Information sheet & informed consent

Before participating in the survey the respondents were able to read information about the research in general before giving consent to use the data and start the survey. They were informed about the time needed to participate and a short explanation of the purpose of the experiment was given. It was made clear to the respondents that the experiment consists of two surveys and therefore their email address was needed, clearly stating that their email address would only be used for the purpose of spreading the second survey. Respondents were asked to be as honest as possible and were reminded that the data would be used anonymously. Participation was voluntary and respondents were able to email comments or questions about the research. Respondents were informed that, by starting the survey, they state to be 18 years or older, to understand the given information and to participate voluntarily. The complete information sheet including the informed consent for Survey 1 is enclosed in Appendix 3. The email for Survey 2, containing a message and personal link was sent to each respondent independently. The message contained the respondent ID and email address for reference and the request to fill in the second survey. The complete message of the email is enclosed in Appendix 4.

3.4.3 Debriefing

The debriefing of Survey 1 contains a message of gratitude for filling in the survey and a reminder that all data would be used anonymously. It was stated that their email address would only be used to contact them for the second survey. They were again informed to email in case of comments, further questions or complaints. The complete debriefing for Survey 1 is enclosed in Appendix 7. Survey 2 contained a shorter debriefing. The debriefing consists of a message of gratitude for filling in the survey. Respondents are reminded of the anonymous use of data and the possibility to email in case of comments, further questions or complaints. The complete debriefing for Survey 2 is enclosed in Appendix 8.

3.5 Data analysis

3.5.1 Hypothesis 1

Both the treatment group and control group filled in Survey 1 and 2. In Survey 1, the control group was shown a list of statements regarding the cybersecurity measures to take. For each statement they reported to take the measure, to not take the measure or 'I don't know'. The treatment group was shown a checklist regarding the cybersecurity measures to take. They were then asked to check the boxes of the cybersecurity measures they are taking. Thus, both groups reported on number of cybersecurity measures taken. However, they were not reported in the same manner (either a statement list or checklist). This difference in manner of answering can affect the answers itself. Hence, the difference in number of cybersecurity measures taken between the control and treatment group in Survey 1 cannot be compared. Therefore, the effectiveness of the checklist as a nudge is analysed by a comparison of number of cybersecurity measures taken between control and treatment group in Survey 2. For this type of between-subject comparison, an independent samples t-test is used (InfoNu, 2013).

Cybersecurity measures will be coded as numeric value on a ratio scale. The treatment variable will be coded as dummy variable (0=no treatment, 1= treatment). Other variables are age, gender, and whether respondents were working from home before regulations. Age will be coded as a numeric value, gender as categorical variable (0=male, 1=female, 2=other). The variable working from home prior to the regulations is coded as a categorical variable.

The independent samples t-test has three assumptions that must be met. The dependent variable must be continuous, should follow normal distribution the observations must be independent.

If the null hypothesis holds for the independent samples t-test, this indicates that there are no differences in average number of cybersecurity measures taken between control and treatment group. Thus, the checklist would not be effective. The alternative hypothesis states that there is a difference, thus implying the effectiveness of a nudge.

3.5.2 Hypothesis 2

The control group in the experiment received no nudge to stimulate the use of cybersecurity measures. Therefore, the effect over time will be tested by comparing the number of measures taken in Survey 1 with Survey 2 for the control group. A paired samples t-test will be used to compare the two times of measurements with time as independent variable and number of measures taken as a dependent variable (InfoNu, 2013). The paired samples t-test has four assumptions that must be met. The dependent variable must be continuous, should follow normal distribution, and the observations must be independent. Furthermore, the data should not have outliers.

If the null hypothesis for the paired samples t-test holds this indicates no differences over time. In this case this means no difference in the average number of cybersecurity measures taken over time by the control group. The alternative hypothesis indicates that there is a difference over time in the averages of the control group.

4. Results

4.1 Descriptive statistics

The number of cybersecurity measures taken by the sample ranges between 2 and 11 measures taken for both Survey 1 and 2 (out of 12 possible measures). However, the mean number of measures taken in Survey 2 is higher than in Survey 1 (M^1=6.12, SD^1=1.72, M^2=6.44, SD^2=1.58).

Age ranges from 20 to 64 years (M=41.39, SD=12.88). See figure 4 for the complete age distribution of the sample. One respondent preferred not to disclose gender whereas 108 are female and 70 male (see figure 5).

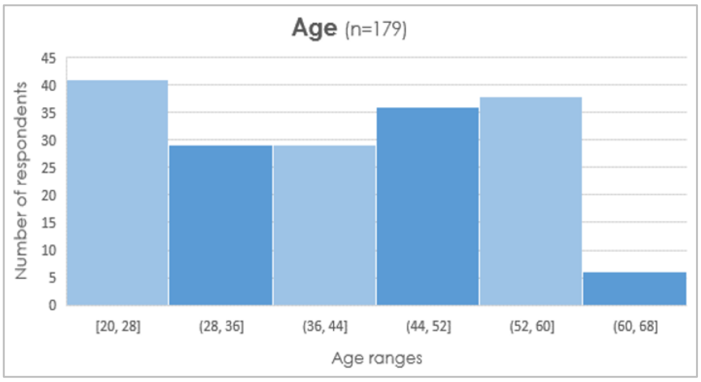


Figure 4: Age distribution of sample.

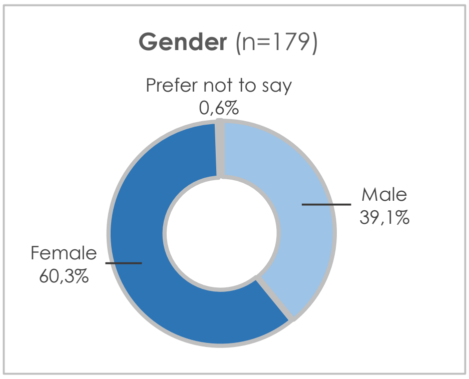


Figure 5: Gender distribution of sample.

As regards to working sector, only the sector of *agriculture, nature and environment* is not represented in the sample. The sector *education, culture and science* is overrepresented with 47% of the respondents (85 respondents) as can be seen in figure 6. This is probably caused by the distribution of the survey trough social media. The second largest group, 10% of the respondents (18 respondents) work in *automation and ICT*. Third in line is *personnel, organisation and strategy* with 9% (17 respondents). Other working sectors are *healthcare* (9%, 16 respondents); *trade and administration* (7%, 12 respondents); *public administration, security and justice* (7%, 12 respondents); *technique and production* (4%, 8 respondents); *language, media and communication* (3%, 5 respondents); *catering and housekeeping* (2%, 3 respondents); *tourism and recreation* (1%, 2 respondents); and *logistics* (1%, 1 respondent).

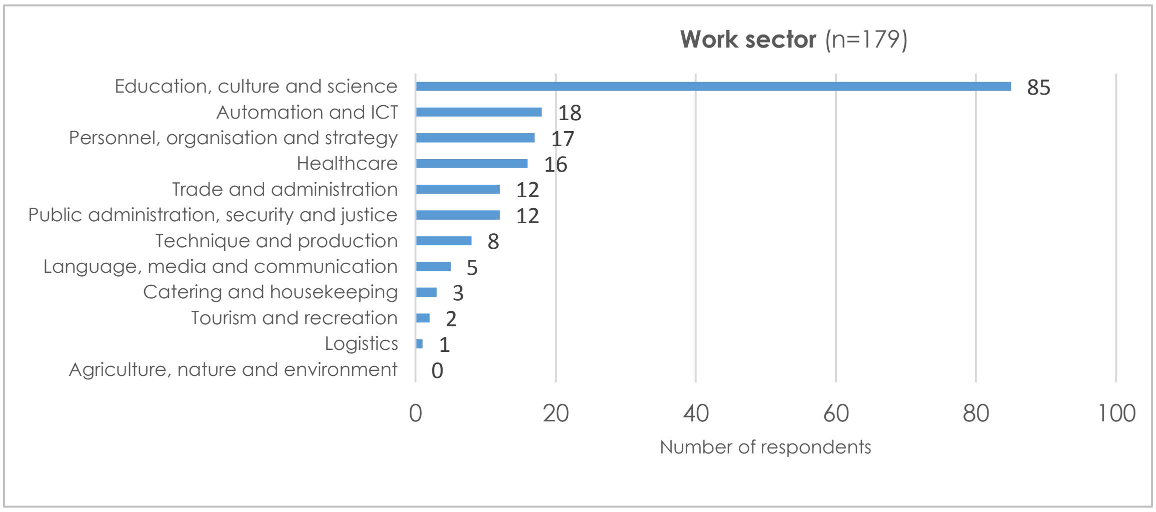


Figure 6: Work sector distribution of sample.

The majority of the respondents have worked from home prior to the regulations due to COVID-19. Only 31% of the respondents (56) have stated to never worked from home prior. The other 69% (123) has worked from home before but differs in the frequency of working from home. Out of these 123 respondents, 42 respondents (34%) have worked from home before but only rarely; 47 respondents (38%) have worked from home before regularly; and 34 respondents (28%) have worked from home before full-time. The figure with the distribution of respondents working from home before is enclosed in figure 7.

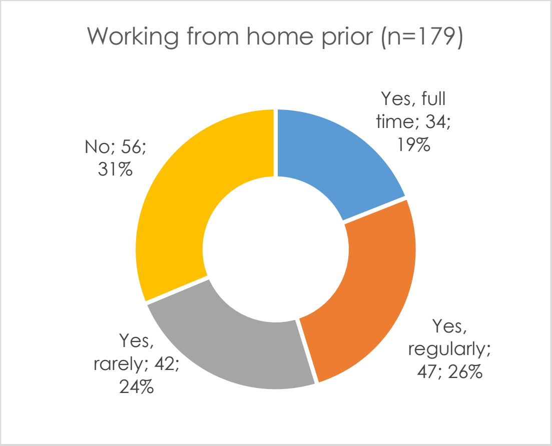


Figure 7: Distribution of time worked from home.

As can be seen in figure 8, regarding impact of the regulations on time spent working from home, respondents reported mostly a moderate decline at Survey 1 but mostly no change at Survey 2. Regarding mental health, respondents reported a moderate decline at both Survey 1 and 2. Productivity was mostly reported to decline moderately at Survey 1 and no change at Survey 2. Overall, the regulations mostly impacted respondents in a negative way, decreasing their time spent working from home, their mental health and productivity.

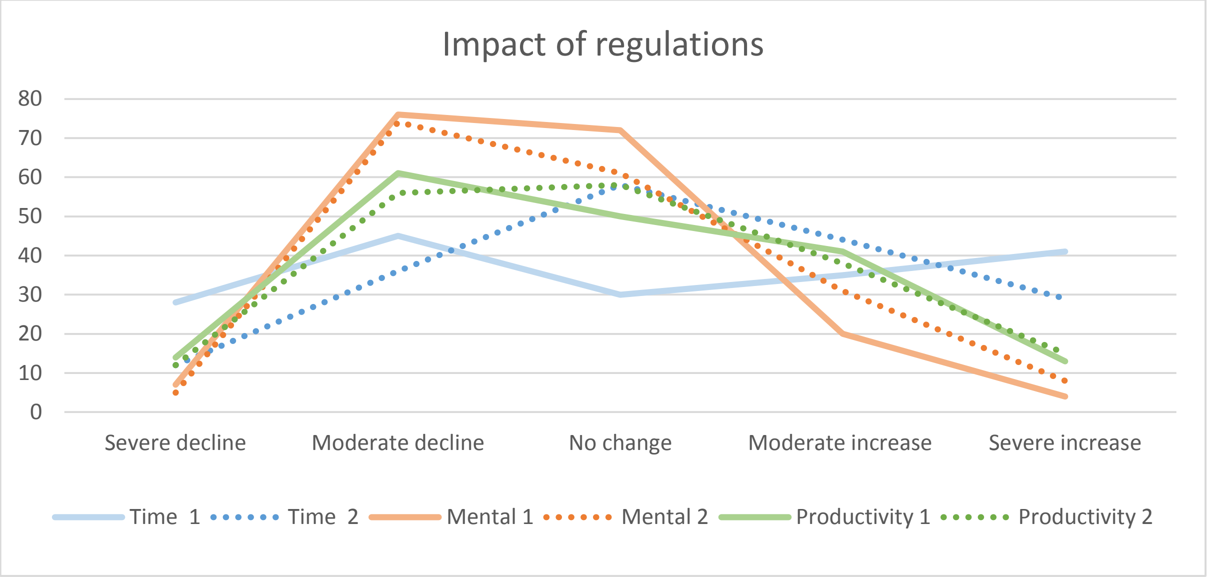


Figure 8: Impact of regulations on (1) time spent working from home, (2) mental health, and (3) productivity .

4.2 Hypothesis 1

To test if using a checklist as a nudge to inform employees working from home about cybersecurity measures will lead to an increase in the number of measures taken by this employee, an independent samples t-test was conducted with treatment as between-subject variable. All assumptions for the independent samples t-test are met. The dependent variable, number of cybersecurity measures taken, are continuous. To test for normal distribution of the dependent variable, the Shapiro-Wilk test is used (see Appendix 9). The number of cybersecurity measures taken are normally distributed with a p-value of 0.843. Furthermore the observations are independent.

Table 1 shows the results of the independent samples t-test. The results show a difference in number of cybersecurity measures taken between control an treatment group equal to -0.132 with an effect size of -0.083. This implies that the control group used 0.083 less cybersecurity measures at the time of Survey 2 compared to the treatment group. However, this difference is not significant (t(177)=-0.555; p-value>0.05). The null hypothesis is therefore not rejected, meaning there is no difference in cybersecurity measures taken between control and treatment group.

Table 1 – Results of independent samples t-test

	Mean	Std.error	Std.dev	95% Confidence interval		Sign.
				Upper	Lower	
Control group*	6.379	0.176	1.644	6.029	6.730	
Treatment group*	6.511	0.160	1.530	6.194	6.828	
Difference	-0.132	0.237		-0.600	0.337	0.580

*Note: Table 1 shows the results of the independent samples t-test with N=197. *Number of cybersecurity measures taken by control and treatment group is denoted by 'Control group' and 'Treatment group'.*

4.3 Hypothesis 2

To test if there is an increase over time in the use of cybersecurity measures that are taken by employees, a paired samples t-test was conducted for the control group. If the null hypothesis in this test holds, this implies no difference in average number of cybersecurity measures taken over time, by the control group. The alternative hypothesis states that there is a difference, thus implying there is an effect over time on cybersecurity measures taken. First, the assumptions for the paired samples t-test are tested. The dependent variable, number of cybersecurity measures taken, is continuous. To test for normal distribution of number of cybersecurity measures taken in both Survey 1 and Survey 2 the Shapiro-Wilk test is used (see Appendix 10). The number of cybersecurity measures taken are normally distributed with a p-value of respectively 0.995 and 0.991. Furthermore there are no outliers and the observations are independent. Thus, all assumptions for the paired samples t-test are met.

Table 2 shows the results of the paired samples t-test. The results show a difference in number of cybersecurity measures taken between Survey 1 and Survey 2 equal to -0.195 with an effect size of -0.1603. This implies that the control group used 0.1603 less cybersecurity measures at the time of Survey 2 compared to Survey 1. However, this difference is not significant (t(86)=-1.496; p-value>0.05). The null hypothesis is therefore not rejected, meaning there is no effect over time in the use of cybersecurity measures taken by the control group.

Table 2 – Results of paired samples t-test

	Mean	Std.error	Std.dev	95% Confidence interval		Sign.
				Upper	Lower	
Survey 2*	6.380	0.176	1.644	6.029	6.730	
Survey 1*	6.575	0.170	1.589	6.236	6.913	
Difference	-0.195	0.131	1.218	-0.455	0.064	0.138

*Note: Table 2 shows the results of the paired samples t-test with N=87. *Number of cybersecurity measures taken in Survey 1 and 2 is denoted by 'Survey 1' and 'Survey 2'.*

5. Discussion

Since the Internet was invented, there have been concerns about the online safety of users. Minimizing cybercrime, and thus maximizing cybersecurity has been of high priority for Internet developers and governments, among others. This became even more relevant when the COVID-19 pandemic started at the end of 2019. Governments were forced to put regulations into place to reduce the contamination rate, including the regulation to work from home. This opened new doors of possibilities for hackers with more (vulnerable) Internet users to target. There are multiple ways to increase the use of cybersecurity measures to increase online safety. In this research it was tested whether the use of a checklist with cybersecurity measures has a positive effect on taking these measures.

A randomized control experiment was conducted to collect data on the use of cybersecurity measures taken before and after the treatment using two surveys. To test the effectiveness of the checklist an independent samples t-test was used. Results of this tests show no significant difference in cybersecurity measures taken between control and treatment group. These results are not in line with previous research on the effectiveness of a checklist in healthcare (de Korne, et al., 2010; Pronovost, et al., 2006; Haynes, et al., 2009; de Vries, et al., 2010). A possible explanation for this is that the treatment group only saw the checklist once, whereas in previous literature regarding the effectiveness of a checklist in healthcare, the checklist was used before each surgery.

To test the effect over time between Survey 1 and 2, a paired samples t-test was conducted for the respondents in the control group of the sample. Results of this test show a negative effect over time. However, this difference is not significant. This is contrary to previous research (McCarney, et al., 2007). A possible reason for this contradiction is the short amount of time in between Survey 1 and 2. In contrast to other experiments, using a time span between three to 18 months (Haynes, et al., 2009; Pronovost, et al., 2006), due to temporary COVID-19 regulations, this experiment has used a shorter time span of three weeks. Another possible reason is that, although respondents might be confronted with the impact of the pandemic on cybersecurity, they underestimated their online risks (Aiken, 2016) or hold employers accountable for organizing secured remote working.

5.1 Limitations and further research

This research has several limitations. Regarding data collection, the sample of respondents were reached through personal social networks. With 47% respondents working in the educational sector, this group is overrepresented in the sample. This might have affected the results due to educational background. Another possible limitation is the changes in regulations in between Survey 1 and 2. Although no change occurred regarding working from home, it is not known how other changes might have affected employees working from home. The last limitation regarding data collection is late responses for Survey 2. Although respondents were informed about the time span of three weeks in Survey 1 and were asked to fill in Survey 2 three weeks after Survey 1, some respondents filled in Survey 2 later than three weeks. For future research it would be beneficial to test if there are not only effects on short term, but also on a long term after seeing the checklist.

Another limitation of the data collection is the manner of measuring cybersecurity measures taken and the introduction of the checklist. First of all, respondents were asked to report the cybersecurity measures they already take. However, reported measures can be different from actual measures taken. A field experiment can solve this limitation by actually observing which measures are taken by participants in the experiment. Second, the introduction of the checklist is a limitation of this research. In Survey 1, the control group reported on cybersecurity measures taken through a list of statements. The treatment group reported on cybersecurity measures taken through a checklist. This difference has several implications. Due to the different manner of measuring the number of cybersecurity measures taken, the dependent variable in Survey 1 cannot be directly compared with the dependent variable in Survey 2. This comparison can only be made within the control group (as was done for hypothesis 2). Another implication of the difference in manner of measuring is the fact that the control group had to report their answers for each statement whereas the treatment group was only asked to tick the relevant boxes. This could have impacted reporting behaviour of the treatment group.

A recommendation for further research would therefore be to conduct a field experiment within a company with two times of data collection (time=0 and time=1). All data on the use of cybersecurity measures should be automatically collected in a database. At time=0 data should be collected on the actual use of cybersecurity measures taken by employees. After data collection, employees would be split into either control or treatment group. The treatment group would then be introduced with a checklist on cybersecurity measures to take. This checklist would be provided to employees to keep on their desks (for example), being made aware of the checklist multiple times a day. Another treatment could be to provide the checklist and give a reminder (on screen) when going online. At time=1 data can be automatically collected again. Then, comparison between measures taken at time=0 and time=1 is possible without the impact of the manner of asking and impact of reported answers instead of observed answers.

Furthermore, there are some limitations regarding the checklist itself. Some measures refer to using facilities organised by the employer, such as an VPN connection or a corporate network. However, taking these measures might not be applicable for self-employed respondents, therefore impacting the results of the effectiveness of a checklist on taken cybersecurity measures. The last limitation regarding the checklist is the difference in application in comparison to previous literature. Where medical checklists are used before every surgery, the checklist in this experiment was only showed ones to the respondents. Therefore, respondents were not repeatedly made aware of possible measures to take when working remotely. Future research is needed to further test the effectiveness of a checklist when used repeatedly for multiple working conditions.

This research was done to test the effectiveness of a checklist to increase the use of cybersecurity measures by employees working from home. This specific context of testing has consequences for the ability to generalise the results for another populations. A non-effective checklist on the use of cybersecurity measures taken by employees working from home due to COVID-19 regulations, does not mean that the same effect is found for employees not working from home or not affected by COVID-19 regulations.

At last, it is recommended for future research to investigate the effectiveness of checklists in multiple contexts. Previous research on checklists have only been done in the context of medical health with positive effects as a result. Future research in other contexts, such as cybersecurity, could contribute to a more complete overview on the effectiveness and application of a checklist.

6. Conclusion

This thesis was done to answer the research question on what the effect is of a checklist on the use of cybersecurity measures by Dutch employees working from home. A sample was collected to take part in an experiment consisting of two surveys. Respondents were split into control and treatment group to analyse differences in measures taken over time due to receiving the treatment (seeing the checklist). The results of the independent samples t-test show no significant difference over time between the control and treatment group regarding cybersecurity measures taken by the respondents. Therefore, it can be concluded that a checklist is not effective in improving the use of cybersecurity measures taken by Dutch employees working from home. This is contrary to the hypothesis and previous research.

It was then tested whether there is an effect over time within the control group between taking the two surveys. A paired sample t-test was used for this analysis. The results show no significant difference over time in cybersecurity measures taken by the control group. Therefore, it can be concluded that there is no effect over time between the two surveys. This is contrary to the hypothesis and previous research.

6.1 Implications

There are several implications of this conclusion. The results of this research might be of interest for companies that are active in the field of cybersecurity and/or improving cybersecurity for employees. Although the results show no significant increase in the use of cybersecurity measures by providing employees with a checklist, it can be interesting for companies to seek better implementation of a checklist. In this research, employees working from home due to the COVID-19 regulations only reported to take six cybersecurity measures on average. This is not much, and can therefore be of concern for organizations. The results can also be of interest for governments. As the descriptive statistics show, the regulations to work from home mostly impacted respondents in a negative way. Governments should be aware of such 'side effects' of the pandemic and governmental regulations.

Bibliography

Aiken, M. (2016). *The Cyber Effect: A pioneering cyber-psychologist explains how human behavior changes online*. Spiegel & Grau.

Aiken, M. (2019). *Life in cyberspace*. European Investment Bank.

Aldawood, H., & Skinner, G. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. *International Journal of Security, 10*(1), 1.

Alkhamis, E., & Renaud, K. (2016). The Design and Evaluation of an Interactive Social Engineering Training Programme., (pp. 125-134).

Amoroso, E. (2006). *Cyber security* . New Jersey: Silicon Press.

Ashraf, N., D, K., & Yin, W. (2006). Tying Odysseus to the mast: Evidence from a commitment savings product in the Philippines. *Quarterly Journal of Economics, 121*, 635-671.

Bada, M., Sasse, A., & Nurse, J. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672.*

Bellotti, F., Berta, R., Gloria, A., & Primavera, L. (2009). Enhancing the educational value of video games. *Computers in Entertainment (CIE), 7*(2), 1-18.

Beuran, R., Chinen, K. I., Tan, Y., & Shinoda, Y. (2016). *Towards effective cybersecurity education and training.* Japan: JAIST.

Business Insider. (2020, March 16). *Working from home? Here are the steps all workers and companies should take to avoid cyberattacks, according to experts*. Retrieved April 1, 2020, from Business Insider: https://www.businessinsider.com/how-to-avoid-cyberattacks-working-from-home-covid-19-2020-3?international=true&r=US&IR=T

Camerer, C., Issacharoff, S., Loewenstein, G., O'donoghue, T., & Rabin, M. (2003). Regulation for Conservatives: Behavioral Economics and the Case for "Asymmetric Paternalism". *University of Pennsylvania law review, 151*(3), 1211-1254.

CNBC. (2020, March 20). *Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems*. Retrieved March 23, 2020, from

CNBC: https://www.cnbc.com/2020/03/20/phishing-spam-spike-as-hackers-use-coronavirus-to-hit-remote-work.html

Cone, B., Irvine, C., Thompson, M., & Nguyen, T. (2007). A video game for cyber security training and awareness. *Computer & Security , 26*(1), 63-72.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Deifning cybersecurity. *Technology Innovation Management Review, 4*(10).

Cyber Readiness Institute. (2020, June 30). *Data Protection Basics for Remote Workers*. Retrieved November 7, 2020, from Cyber Readiness Institute: https://cyberreadinessinstitute.org/resource/in-response-to-covid-19-there-was-a-rapid-shift-to-remote-work-now-as-the-pandemic-enters-a-new-phase-we-are-seeing-another-shift-to-a-hybrid-work-environment-in-which-some-employees-will-be-work/

Cyber Readiness Institute. (2020, June 30). *Securing a Remote Workforce*. Retrieved July 3, 2020, from Cyber Readiness Institute: https://cyberreadinessinstitute.org/resource/securing-a-remote-workforce/

de Korne, D. F., van Wijngaarden, J., Hiddema, U., Bleeker, F., Pronovost, P., & Klazinga, N. (2010). Diffusing Aviation Innovations in a Hospital in the Netherlands. *The Joint Commission Journal on Quality and Patient Safety, 36*(8), 339-347.

De Volkskrant. (2020, May 22). Buitenlandse Zaken beveiligt informatie slecht. *De Volkskrant*, p. 6. Retrieved May 22, 2020

De Volkskrant. (2020, May 23). Dringt corona misdaad terug? *De Volkskrant*, p. 17.

De Volkskrant. (2020, March 15). *Thuiswerken? Niet voor de arts, schoonmaker en buschauffeur*. Retrieved April 1, 2020, from De Volkskrant: https://www.volkskrant.nl/nieuws-achtergrond/thuiswerken-niet-voor-de-arts-schoonmaker-en-buschauffeur~b182dbae/

de Vries, E., Prins, H., Crolla, R., den Outer, A., van Andel, G., van Helden, S., . . . Boermeester, M. (2010). Effect of a Comprehensive Surgical Safety System on Patient Outcomes. *The New England Journal of Medicine, 363*(20), 1928-1937.

Department of Homeland Security. (2019, November 20). *Understanding Denial-of-Service Attacks*. Retrieved March 18, 2020, from Cybersecurity and Infrastructure Security Agency: https://www.us-cert.gov/ncas/tips/ST04-015

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology, 33*(1), 264-277.

EenVandaag. (2020, March 22). *Internetcriminals seize their opportunity in coronavirus; 3 tips to work safe from home*. Retrieved March 25, 2020, from EenVandaag: https://eenvandaag.avrotros.nl/item/internetcriminelen-grijpen-hun-kans-in-coronacrisis-3-tips-om-veilig-thuis-te-werken/

Euopean Union. (2016, April 26). Regulation (EU) 2016/679 of the European Parliament and of the council. *Official Journal of the European Union*. Retrieved March 18, 2020

European Union. (1995, October 24). Directive 95/46/EC of the European Parliament and of the Council. *Official Journal of the European Communities*. Retrieved March 18, 2020, from European Data Protection Supervisor: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

Europol. (2017, October 3). *INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA)*. Retrieved May 29, 2020, from Europol: https://www.europol.europa.eu/iocta-report

Europol. (2019, October 9). *Cybercrime is becoming more bolder with data at the centre of the crime scene*. Retrieved March 18, 2020, from Europol: https://www.europol.europa.eu/newsroom/news/cybercrime-becoming-bolder-data-centre-of-crime-scene

FBI. (2017, February 27). *Business E-Mail Compromise*. Retrieved March 18, 2020, from FBI: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

FYA. (2020, April 2020). *The Pros and Cons Of Working From Home During A Pandemic*. Retrieved October 3, 2020, from The Foundation for Young Australians: https://www.fya.org.au/2020/04/27/the-pros-and-cons-of-working-from-home-during-a-pandemic/

Genova, M. (2014). *Komt een vrouw bij de hacker.* Veltman Distributie inzake Just Publishers.

Gibson, B. (2008). Can evaluative conditioning change attitudes toward mature brands? New evidence from the implicit association test. *Journal of Conusmer Research, 35*, 1788-188.

Google. (2020, May 21). *Mobility Changes Netherlands.* Retrieved May 29, 2020, from COVID-19 Community Mobility Report: https://www.gstatic.com/covid19/mobility/2020-05-21_NL_Mobility_Report_en.pdf

Haynes, A., Weiser, T., Berry, W., Lipsitz, S., Lipsitz, A., Dellinger, E., . . . Gawande, A. (2009). A Surgical Safety Checklist to Reduce Morbidity and Mortality in a Global Population. *The New England Journal of Medicine, 360*, 491-499.

Het Parool. (2020, September 12). *Volgend jaar een vaccin, misschien in 2022 of toch pas na 2030?* Retrieved October 10, 2020, from Het Parool: https://www.parool.nl/nederland/volgend-jaar-een-vaccin-misschien-in-2022-of-toch-pas-na-2030~b4f8a73c2/

Higgins, E. (1998). Promotion and prevention: Regulatory focus as a motivational principle. *Advances in Experimental Social Psychology , 30*, 1-46.

InfoNu. (2013, February 26). *Verschillen tussen twee datasets: de t-test*. Retrieved 12 4, 2020, from InfoNu: https://wetenschap.infonu.nl/diversen/110297-verschillen-tussen-twee-datasets-de-t-test.html

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

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*, 263-291.

Kemmerer, R. (2003). Cybersecurity. *Proceedings of the 25th IEEE International Conference on Software Engineering* , (pp. 705-715).

Lewis, J. (2006). *Cybersecurity and Critical Infrastructure Protection.* Washington DC: Center for Strategic and International Studies.

Linkenbach, J., & Perkins, H. (2003). Most of us wear seatbelts: The process and outcomes of a 3-year statewide adult seatbelt campaign in Montana. *Conference presentation: The national conference on the social norms model*.

List, J., Sadoff, S., & Wagner, M. (2011). So you want to run an experiment, now what? Some simple rules of thumb for optimal experimental design. *Experimental Economics, 14*(4), 439.

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

McCarney, R., Warner, J., Iliffe, S., Van Haselen, R., Griffin, M., & Fisher, P. (2007). The Hawthorne Effect: a randomised, controlled trial. *BMC medical research methodology, 7*(1), 30.

Medical News Today. (2020, April 16). *COVID-19: How long is this likely to last?* Retrieved October 10, 2020, from Medical News Today: https://www.medicalnewstoday.com/articles/covid-19-how-long-is-this-likely-to-last

Metro. (2020, March 16). *Reizigers in OV maandag flink gedaald*. Retrieved April 1, 2020, from Metro Nieuws: https://www.metronieuws.nl/in-het-nieuws/2020/03/reizigers-in-ov-maandag-flink-gedaald

Nationaal Cyber Security Centrum. (2020, March 26). *Veilig thuiswerken*. Retrieved April 4, 2020, from Nationaal Cyber Security Centrum: https://www.ncsc.nl/onderwerpen/veilig-thuiswerken

National Patient Safety Agency. (2012). Five steps to safer surgery. *Implementing the Surgical Safety Checklist: The Journey so Far, 2*.

NLTimes. (2020, March 19). *DDoS attack hinders popular food delivery service*. Retrieved April 1, 2020, from NL Times: https://nltimes.nl/2020/03/19/ddos-attack-hinders-popular-food-delivery-service

NOS. (2020, March 2). *Minder inbraak of geweld, meer cybercrime in Veiligheidsmonitor*. Retrieved December 3, 2020, from NOS: https://nos.nl/artikel/2325461-minder-inbraak-of-geweld-meer-cybercrime-in-veiligheidsmonitor.html

NRC. (2020, April 20). *Drie maanden corona in Nederland, een overzicht van de maatregelen*. Retrieved May 29, 2020, from NRC.nl: https://www.nrc.nl/nieuws/2020/04/20/twee-maanden-corona-in-nederland-een-overzicht-van-de-maatregelen-a3995447

NU.nl. (2020, March 27). *https://www.nu.nl/coronavirus/6040831/tijdlijn-het-coronavirus-in-nederland.html*. Retrieved May 30, 2020, from NU.nl: https://www.nu.nl/coronavirus/6040831/tijdlijn-het-coronavirus-in-nederland.html

Powney, M., Williamson, P., Kirkham, J., & Kolamunnage-Dona, R. (2014). A review of the handling of missing longitudinal outcome data in clinical trials. *Trials, 15*(1), 237.

Pronovost, P. (2010). *Safe patients, smart hospitals: How one doctor's checklist can help us change health care from the inside out.* New York: Hudson Street Press.

Pronovost, P., Needham, D., Berenholtz, S., D, S., Chu, H., Cosgrove, S., . . . Goeschel, C. (2006). An Intervention to Decrease Catheter-Related Bloodstream Infections in the ICU. *New England Journal of Medicine, 355*(26), 2725-2732.

Reason, J. (2000). Human error: models and management. *BMJ, 320*(7237), 768-770.

Reuters. (2020, March 23). *Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike*. Retrieved April 1, 2020, from Reuters: https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

Reuters. (2020, March 18). *Mass move to work from home in coronavirus crisis creates opening for hackers: cyber experts*. Retrieved March 25, 2020, from Reuters: https://www.reuters.com/article/us-health-coronavirus-cyber/mass-move-to-work-from-home-in-coronavirus-crisis-creates-opening-for-hackers-cyber-experts-idUSKBN2153YC

Rijksoverheid. (2020, September 28). *Aangescherpte maatregelen om de verspreiding van het virus terug te dringen*. Retrieved October 10, 2020, from Rijksoverheid: https://www.rijksoverheid.nl/actueel/nieuws/2020/09/28/aangescherpte-maatregelen-om-de-verspreiding-van-het-virus-terug-te-dringen

Rijksoverheid. (2020, April 21). *Maatregelen corona verlengd*. Retrieved May 30, 2020, from Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/nieuws/2020/04/21/maatregelen-corona-verlengd

Rijksoverheid. (2020, March 12). *New regulations against the spread of coronavirus in the Netherlands*. Retrieved March 25, 2020, from Rijksoverheid: https://www.rijksoverheid.nl/onderwerpen/coronavirus-covid-19/nieuws/2020/03/12/nieuwe-maatregelen-tegen-verspreiding-coronavirus-in-nederland

RIVM. (2020, May 28). *Actuele informatie over het nieuwe coronavirus (COVID-19)*. Retrieved May 29, 2020, from Rijksinstituut voor Volksgezondheid en Milieu: https://www.rivm.nl/coronavirus-covid-19/actueel

RIVM. (2020, May 27). *De ziekte COVID-19*. Retrieved May 29, 2020, from Rijksinstituut voor Volksgezonheid en Milieu: https://www.rivm.nl/coronavirus-covid-19/ziekte

RTL Nieuws. (2020, April 30). *Europol: grote toename cybercrime door coronavirus*. Retrieved December 3, 2020, from RTL Nieuws: https://www.rtlnieuws.nl/tech/artikel/5107766/grote-toename-cybercrime-door-coronavirus

Suis, J., Lemos, K., & Stewart, L. (2002). Self-esteem, construal, and comparisons with the self, friends and peers. *Journal of Personality and Social Psychology , 82*, 252-261.

Sunstein, C. (2015). The ethics of nudging. *Yale J. on Reg, 32*, 413-450.

Sunstein, C. (2020). *Behavioural Science and Public Policy.* Cambridge: Cambridge University Press.

Thaler, R. (1980). Toward a Positive Theory of Consumer Choice. *Journal of Economic Behaviour and Organisation, 1*, pp. 39-60.

Thaler, R., & Sunstein, C. (2003). Libertarian paternalism. *American Economic Review, 93*(2), 175-179.

Thaler, R., & Sunstein, C. (2009). *Nudge: Improving decisions about health, wealth, and happiness.* Penguin.

Thaler, R., Sunstein, C., & Balz, J. (2013). Choice architecture. *The behavioral foundations of public policy*, 428-439.

The Cyber Readniess Institute. (2019, October 5). *Our History*. Retrieved April 1, 2020, from The Cyber Readiness Institute: https://www.cyberreadinessinstitute.org/our-history

The New York Times. (2020, March 13). *Social Distancing? You Might Be Fighting Climate Change, Too*. Retrieved April 1, 2020, from The New York Times: https://www.nytimes.com/2020/03/13/climate/coronavirus-habits-carbon-footprint.html

The Washington Post. (2015). *A History of Internet security*. Retrieved March 17, 2020, from https://www.washingtonpost.com/graphics/national/security-of-the-internet/history/

United Nations Conference on Trade and Development. (2020, February 18). *Data Protection and Privacy Legislation Worldwide*. Retrieved March 18, 2020, from United Nations Conference on Trade and Development: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

US Congress. (1986). Computer Fraud and Abuse Act of 1986. *Publication No. 99-432*. Retrieved March 18, 2020, from https://www.cia.gov/library/readingroom/docs/CIA-RDP87B00858R000400480020-8.pdf

VPNoverview. (2020, March 24). *Parisian Hospitals hit by DDoS attack*. Retrieved April 1, 2020, from VPNoverview: https://vpnoverview.com/news/parisian-hospitals-hit-by-ddos-attack/

Wansink, B., & Kim, J. (2006). Bad popcorn in big buckets: Proportion size can influence intake as much as taste . *Journal of Nutrition and Behavior, 37*, 242-245.

Whalen, T. (2001). *Human factors in Coast Guard Computer Security-an analysis of current awareness and potential techniques to improve security program viability.* Monterey CA: Naval Postgraduate School.

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and training program. *NIST Special publication, 800*(50), 1-39.

Wood, A., White, I., & Thompson, S. (2004). Are missing outcome data adequately handled? A review of published randomized controlled trials in major medical journals. *Clinical Trials, 1*(4), 368-376.

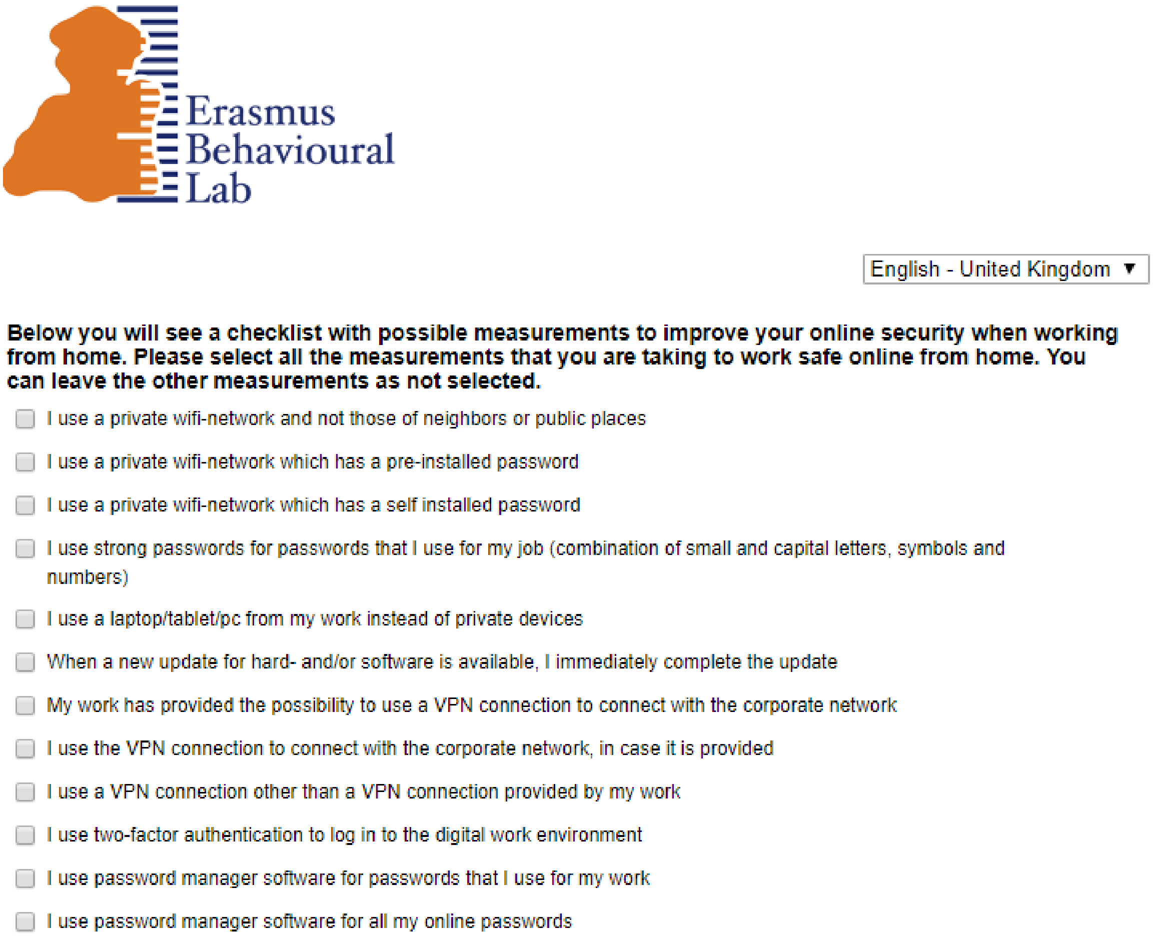
World Health Organisation. (2020, May 28). *Coronavirus disease (COVID-19) pandemic*. Retrieved May 29, 2020, from World Health Organisation: https://www.who.int/emergencies/diseases/novel-coronavirus-2019

Appendix

Appendix 1: List of measures to take by NCSC

- Make use of a VPN connection to connect to the office network
- Use multi-factor authentication to log in to the office network
- Use strong passwords
- Install the most recent updates on hard- and software
- Use a secured and trusted (Wi-Fi)network
- Be aware of using private devices for work

Appendix 2: Checklist cybersecurity measures from survey



Below you will see a checklist with possible measurements to improve your online security when working from home. Please select all the measurements that you are taking to work safe online from home. You can leave the other measurements as not selected.

☐ I use a private wifi-network and not those of neighbors or public places

☐ I use a private wifi-network which has a pre-installed password

☐ I use a private wifi-network which has a self installed password

☐ I use strong passwords for passwords that I use for my job (combination of small and capital letters, symbols and numbers)

☐ I use a laptop/tablet/pc from my work instead of private devices

☐ When a new update for hard- and/or software is available, I immediately complete the update

☐ My work has provided the possibility to use a VPN connection to connect with the corporate network

☐ I use the VPN connection to connect with the corporate network, in case it is provided

☐ I use a VPN connection other than a VPN connection provided by my work

☐ I use two-factor authentication to log in to the digital work environment

☐ I use password manager software for passwords that I use for my work

☐ I use password manager software for all my online passwords

Appendix 3: Information and informed consent provided before participating in Survey 1

“Welcome to this research about working safe from home. Participation in this research will take about 5 to 6 minutes. Your participation will help me graduate for my master Behavioural Economics at the Erasmus Universiteit Rotterdam.

This research looks into the online security of employees who normally work from an office, but are now forced to work from home due to the COVID-19 rules in the Netherlands. Thanks you for your interest in helping with the research. Please read the information underneath carefully.

This research consists of two surveys. Therefore, the effect of the regulations due to the COVID-19 outbreak can be measured at multiples times. This means that, if you choose to participate in this research, you will be contacted again in three weeks to fill in a short survey about this subject. To be able to contact you for further research, we will ask for your email address during this survey. Your email address will not be linked to the answers provided, will not be used for other purposes, and will not be passed on to others.

Your data will be used anonymously. This research contains several about u personally and about your online safety when working from home. Please try to answer the questions as honest as possible. All answer will be treated confidentially. Answers of individual participants will never be identified or published. The collected data of all participants will be bundled and only be published in merged form using group averages.

Participation is voluntarily and you can stop the survey at any time. If you have questions regarding this information or research, please contact Annemijn de Kleijn by mailing to 409588ak@student.eur.nl

If you are 18 years old or older, understand the information above and are willing to voluntarily participate in this research, then please select the "next" button to start the survey.”

Appendix 4: Information provided before participating in Survey 2

Subject of mail: Second survey research online safety when working from home

Dear respondent [RespondentID] with email address [email address],

Three weeks ago you filled in a survey for my research into online safety when working from home. Thank you for participating in that survey! You have indicated that you were willing to also fill in the second survey. Through this mail I would like to ask you to fill in this follow-up survey. The second survey is shorter than the first survey and can be started by clicking on the personal link below:

[personal link]

Again, thank you for filling in the survey. This is highly appreciated and is of high value for my research!

Kind regards,

Annemijn de Kleijn

Appendix 5: Survey 1

Introduction (see Appendix X)

1. **Have the Dutch regulations regarding the COVID-19 outbreak affected your work situation?**
    a. Yes
    b. No
2. **Did you already work from home before the Dutch COVID-19 regulations?**
    a. Yes, full time
    b. Yes, regularly
    c. Yes, rarely
    d. No
3. **On what scale have the COVID-19 regulations affected your:**

(Choice between: severe decline, moderate decline, no change, moderate increase, severe increase)

a. Time spent working from home
b. Your mental health when working from home

    c. Your productivity when working from home?

4. **Are you responsible for the care of others when working from home like children and elderly etc.?**
    a. Yes
    b. No
5. **What statements regarding working from home apply to you?**

- I work from home in a separate room
- I work from home in a shared room (kitchen/dinner room)
- I work at home behind a desk
- I work at home with a laptop/tablet
- I work at home with a laptop with separated mouse or keyboard
- I work at home on a connected computer

6. **In what sector are you working?**
    a. Agriculture, nature and environment
    b. Logistics
    c. Tourism and recreation
    d. Catering and housekeeping
    e. Language, media and communication
    f. Technique and production
    g. Public administration, security and justice
    h. Trade and administration
    i. Healthcare
    j. Personnel, organisation and strategy
    k. Automation and ICT
    l. Education, culture and science
7. **Below, you will see a list containing several statements regarding the improvement of your online security when working from home. Pleas select for each statement if you agree, disagree or don't know.**

- I use a private wifi-network and not those of neighbours or public places
- I use a private wifi-network which has a pre-installed password
- I use a private wifi-network which has a self-installed password
- I use strong passwords for passwords that I use for my job (combination of small and capital letters, symbols and numbers)
- I use a laptop/tablet/pc from my work instead of private devices

- When a new update for hard- and/or software is available, I immediately complete the update
- My work has provided the possibility to use a VPN connection to connect with the corporate network
- I use the VPN connection to connect with the corporate network, in case it is provided
- I use a VPN connection other than a VPN connection provided by my work
- I use two-factor authentication to log in to the digital work environment
- I use password manager software for passwords that I use for my work
- I use password manager software for all my online passwords

8. **What is your age?**
9. **What is your gender?**
    a. Male
    b. Female
    c. Other
    d. I prefer not saying
10. **As you have seen in the introduction a new survey will be send in three weeks. To be able to contact you for this survey, we need your email address. Your email address will not be linked to answers, will not be used for other purposes and will never be passed on to others. What is your email address?**

Debriefing (see Appendix X)

Appendix 6: Survey 2

Introduction (see Appendix X)

1. **Do the Dutch regulations regarding the COVID-19 outbreak still affect your work situation?**
    a. Yes
    b. No
2. **On what scale have the COVID-19 regulations affected your:**

(Choice between: severe decline, moderate decline, no change, moderate increase, severe increase)

    a. Time spent working from home

b. Your mental health when working from home

c. Your productivity when working from home?

3. Are you responsible for the care of others when working from home like children and elderly etc.?

a. Yes

b. No

4. What statements regarding working from home apply to you?

- I work from home in a separate room
- I work from home in a shared room (kitchen/dinner room)
- I work at home behind a desk
- I work at home with a laptop/tablet
- I work at home with a laptop with separated mouse or keyboard
- I work at home on a connected computer

5. Below, you will see a list containing several statements regarding the improvement of your online security when working from home. Pleas select for each statement if you agree, disagree or don't know.

- I use a private wifi-network and not those of neighbours or public places
- I use a private wifi-network which has a pre-installed password
- I use a private wifi-network which has a self-installed password
- I use strong passwords for passwords that I use for my job (combination of small and capital letters, symbols and numbers)
- I use a laptop/tablet/pc from my work instead of private devices
- When a new update for hard- and/or software is available, I immediately complete the update
- My work has provided the possibility to use a VPN connection to connect with the corporate network
- I use the VPN connection to connect with the corporate network, in case it is provided
- I use a VPN connection other than a VPN connection provided by my work
- I use two-factor authentication to log in to the digital work environment
- I use password manager software for passwords that I use for my work
- I use password manager software for all my online passwords

Debriefing (see Appendix X)

Appendix 7: Debriefing Survey 1

"Thank you for filling in this survey. Your participation is highly valued!

All collected answer will be used anonymously and confidentially. Your email address will be linked to a respondent ID number and will only be used to contact you for the second survey. You will receive an email with this survey in three weeks. Your email address will not be passed on to others or used for other purposes. For questions, comments or possible complaints, please contact Annemijn de Kleijn by mailing to 409588ak@student.eur.nl.

If you would like to receive the combined results of this research, please indicate below. Your email address will be used to send the results."

Appendix 8: Debriefing Survey 2

"Thank you for filling in this survey. Your participation is highly valued!

All collected answer will be used anonymously and confidentially. Your email address is linked to a respondent ID number and will only be used to link the data from the two surveys. Your email address or data will not be passed on to others or used for other purposes. For questions, comments or possible complaints, please contact Annemijn de Kleijn by mailing to 409588ak@student.eur.nl.

In case you have indicated during the first survey that you would like to receive the combined results of this test, the previously filled in email will be used for this purpose only."

Appendix 9: Testing the assumption of normal distribution for the independent samples t-test

Table 9.1 – Shapiro-Wilk test for normal distribution test

	N	W	V	z	Significance
Survey 2*	179	0.995	0.643	-1.009	0.844

*Note:. *Number of cybersecurity measures taken in Survey 2 is denoted by 'Survey 2'.*

Appendix 10: Testing the assumption of normal distribution for the paired samples t-test

Table 10.1 – Shapiro-Wilk test for normal distribution test

	N	W	V	z	Significance
Survey 1*	87	0.996	0.311	-2.571	0.995
Survey 2*	87	0.995	0.342	-2.364	0.991

*Note:. *Number of cybersecurity measures taken in Survey 1 and 2 is denoted by 'Survey 1' and 'Survey 2'.*