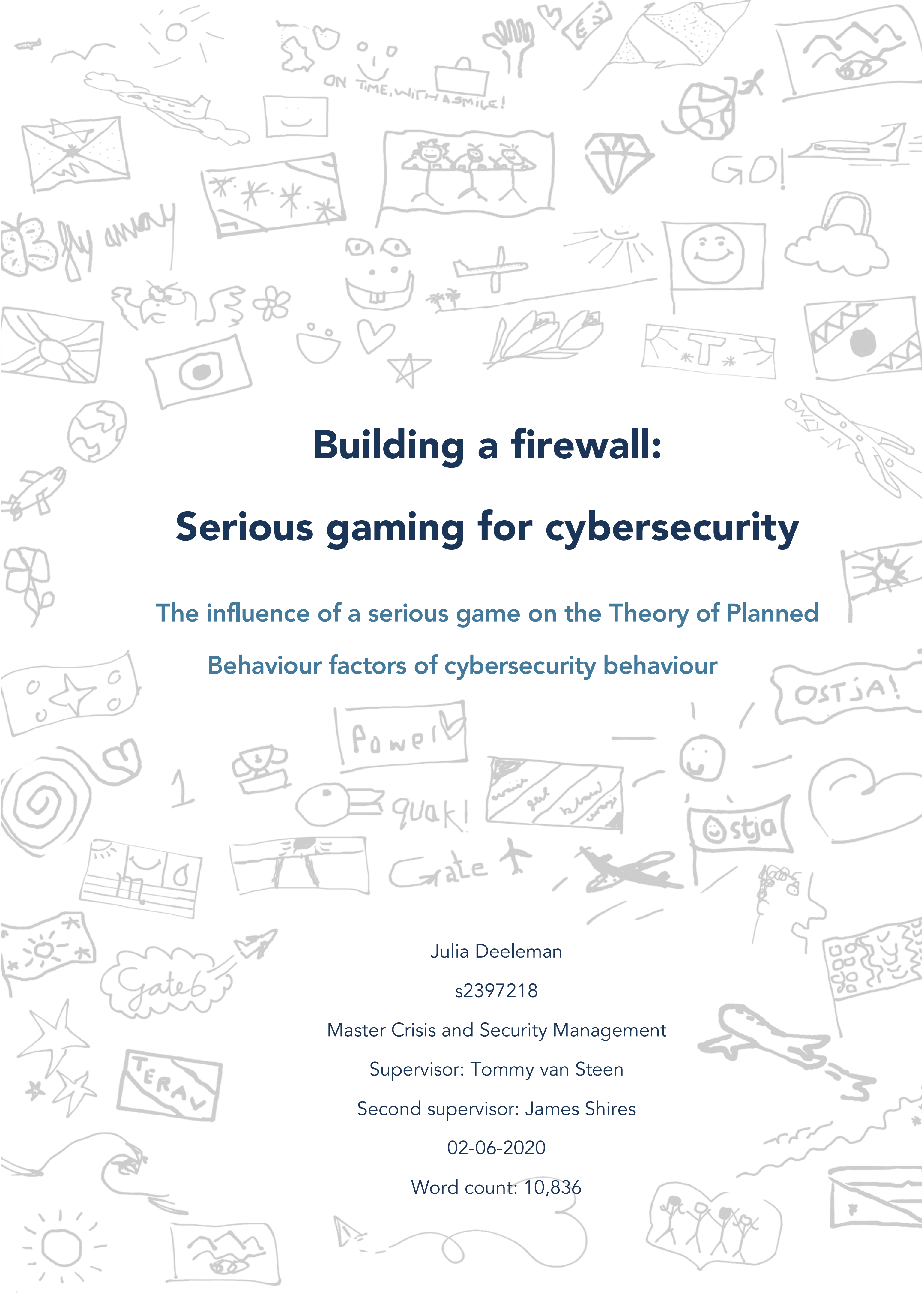


Building a firewall:

Serious gaming for cybersecurity

The influence of a serious game on the Theory of Planned Behaviour factors of cybersecurity behaviour

Julia Deeleman

s2397218

Master Crisis and Security Management

Supervisor: Tommy van Steen

Second supervisor: James Shires

02-06-2020

Word count: 10,836

Abstract

Humans are often said to be the weakest link in cybersecurity, allowing for most breaches. Although often without any bad intentions, this way human behaviour forms a key cyber risk. This thesis aims to explore the method of serious gaming as a way to influence such human behaviour. In doing so, the thesis assesses the influence of a cybersecurity serious game on the Theory of Planned Behaviour (TPB) factors of cybersecurity behaviour. Therefore, two different serious games were designed; one on the topic of cybersecurity and one on teamwork. An experiment measured whether participants of the cybersecurity game scored higher on TPB factors in a survey, which was conducted after playing one of the games. Results showed that participants of the cybersecurity game indeed scored higher on all TPB factors than participants of the teamwork game. Therefore, a cybersecurity game showed to have been effective in positively influencing all TPB factors of cybersecurity behaviour. Future research is encouraged to conduct a similar experiment on different topics, or by including an objective behavioural measurement instead.

Foreword

The basis of this research comes from the fun I often experience while facilitating live interactive serious games for LIB Businessgames as my side job. Participants who are fully engaged in a game and thus into a certain topic, and learn something about this topic while gaming, is super exciting to watch. I wanted to integrate this fun experience into my coursework, and combine it with a topic I find highly interesting. This marked the beginning of this thesis, a thesis on serious gaming for cybersecurity. A thesis which combines my side job with my masters' programme. In doing so, it has been written to fulfil the graduation requirements for the master Crisis and Security Management at Leiden University.

I highly wish that this research could be inspiring people or organisations to look more closely into the method of serious gaming for training purposes. It is not only fun, but also very educating. Due to COVID-19, a change to this thesis had to be made, which resulted in an online game instead of a live interactive game to be conducted. Even though participants could not physically build a firewall anymore, the fun elements are displayed on every page of this thesis. At the bottom of each page, a logo or flag can be found which participants of this study created during the game. Make sure to have a look at them.

First of all, a big thank you to the participants of this study, who took quite some time to do the game in the end. Secondly, I would like to thank both supervisors for their great guidance and support. Thank you, Tommy van Steen, for your positivity, enthusiasm, and for always helping me out when needed. Thirdly, thanks a lot to LIB Businessgames for the trust, the support and the games I could create or amend for this research. And finally, thanks to all my dear friends and family who have helped me out with finding respondents, and continued to distract me from my thesis work. The second point was needed too I guess.

I hope you will have a wonderful time reading this thesis,

Julia Deeleman

Rotterdam, 02-06-2020

Table of contents

Introduction

As known to many, the consequences of cyber-attacks are often severe. This is the case both in business environments and in the personal sphere. Data breaches or hacks potentially lead to major economic or reputational damage. Such damage can result in less trust in the company (IBM, 2018, p. 23-24). These financial and reputational consequences may, therefore, eventually pose a more significant problem than the actual attack experienced (Pearson, 2014, p. 11). Furthermore, even the data of individual users gets stolen for malicious purposes. The consequences of cyber-attacks are thus very widespread and can cause a potential threat to national security (Saini, Rao, & Panda, 2012, p. 206). It is therefore essential to educate users and achieve behavioural change with regards to cybersecurity practices.

When participating in the Dutch National Cyber Security Summer School, an employee of the Dutch intelligence service provided a guest lecture. For having her presentation on screen, she brought personal HDMI cables, therefore preventing having to use the one of the organisation. She was well aware of the consequences of a malicious cable plugged into a port. She did not take any risks. Many people do not have such consciousness, even though this knowledge is often essential. This lack of awareness results in users seen as the weakest link in cybersecurity, allowing for most breaches (Yan et al., 2018, p. 376). Being with criminal intentions or not, in this way human behaviour continues to be the primary source of cyber risk (Eling & Wirfs, 2019, p. 1110).

Human cybersecurity behaviour, therefore, needs to change. Taking part in a serious game could be one of the possible ways to bring about this behavioural change. Serious games strive towards facilitating learning amongst the participants in addition to their entertaining function (Charsky, 2010, p. 179). In doing so, they can be more successful in facilitating knowledge and cognitive skills than regular instructional approaches (Sitzmann, 2011, p. 489). Much literature limits serious gaming to computer- or video gaming. However, this research also takes board games, live serious games, or other forms into account. It, therefore, joins the approach taken by Le Compte, Watson and Elizondo (2015, p. 205).

Research objective. Through an explorative approach, this research investigates whether participation in serious games could lead to a change in different behavioural factors. In doing so, it uses the Theory of Planned Behaviour (TPB) by Ajzen (1991) as a framework for behavioural change and the development of the games. This research will assess all factors of the Theory of Planned Behaviour in doing so. The research is explorative as no previous quantitative research conducted an experiment combining cybersecurity training with this type of serious gaming.

Research question. For this purpose, the research will answer the following research question: *What are the effects of a cybersecurity serious game on the Theory of Planned Behaviour factors of cybersecurity behaviour?*

Relevance. This research is academically relevant as no experimental studies researched the connection between all of these TPB factors and cybersecurity serious games before. Nevertheless, serious games have shown to be effective in different domains, like sustainable behaviour (Courbet, Bernanrd, Joule, Hallimi-Falkowiczm & Gueguen, 2016, p. 949). However, given the prediction that a cybersecurity game will be a useful tool for behavioural change in this specific domain too, this is interesting to explore (Hendrix, Al-Sherbaz & Bloom, 2016, p. 53). Even though a qualitative experiment described a change in awareness of cybersecurity with a type of serious games called wargames, no quantitative experiment into all TPB factors with online serious games on cybersecurity took place (Haggman, 2019). This study aims to fill this gap in the literature.

The research is societally relevant as the consequences of cyberattacks are very widespread and can cause serious harm to society, its organisations, structure and economy (IBM, 2018, p. 23-24). Additionally, knowledge of secure cyber behaviour often lacks amongst employees and individual users, being identified as the weakest link (Yan et al., 2018, p. 376). Many different companies receive phishing emails or become victims of other cybercrimes (NOS, 2019). For this purpose, the games used in the research are both targeted at individual users and users in business environments. The expectation is that users with little IT knowledge are most likely to benefit from this experience, given that it can serve as a good base of information. The main aim is to achieve a positive change on the TPB factors of cybersecurity behaviour so that future attacks may be limited.

COVID-19. Before proceeding to the structure of this thesis, it is valuable to know that this study was set up somewhat different in the first place. The initial research design created contained two live interactive serious games, one of which was specially designed for this study. The set-up was to play these serious games with 150 employees from different companies. However, given the COVID-19 outbreak in the Netherlands, no events could be organised until at least the 1st of June 2020. This situation made it impossible to carry out the live serious games since they characterise as business events. Therefore, online versions of the live interactive serious games were created. With these games, the experiment thus slightly changed but continued.

Structure. This thesis covers different elements which will collaboratively answer the research question. First of all, the literature review explores the extant literature on the topics of serious gaming and cybersecurity behavioural change approaches. Following this, a methodology section describes the experimental approach taken in this research. It elaborates upon the experimental procedure, and the serious games played in this experiment. Thirdly, the results section presents the findings of the study. Finally, the discussion elaborates extensively upon these findings and provides the main answer to the research question posed.

Theoretical framework

Academic field. This research uses the method of serious gaming to bring about a positive change in the TPB factors of cybersecurity behaviour. In doing so, the topic fits within the security management academic field. More specifically, it fits into literature investigating ways to improve cybersecurity behaviour. While research has been done into interventions improving this behaviour, the academic field is a rather young and developing one. Furthermore, a clear gap in knowledge exists in the connection between serious gaming and cybersecurity. Except for qualitative or literature research, no quantitative experiments have been conducted in this domain yet.

The Theory of Planned Behaviour

As mentioned before, this research aims to find out whether serious games can cause a positive change in the TPB factors of cybersecurity behaviour. Therefore, it is essential to elaborate on the Theory of Planned Behaviour by Ajzen (1991), as this provides a good base for what is to come.

The TPB is a theory which aims to explain human behaviour (Ajzen, 1991, p. 189). In doing so, it argues that intention is the most important predictor of planned behaviour. Intentions follow from three other factors; attitude, perceived behavioural control, and subjective norms. It defines the concept of attitude as an attitude towards the behaviour, which can both be a negative or positive evaluation of the specific behaviour (Ajzen, 1991, p. 188). Perceived behavioural control is defined as the confidence one has in performing the behaviour, or how easy or difficult it is perceived to be (Ajzen, 1991, p. 184; p. 188). Thirdly, subjective norms refer to any perceived social pressure experienced to perform this behaviour, or not (Ajzen, 1991, p. 188). Intentions are assumed to be motivational factors influencing behaviour. They express the effort of people to perform this behaviour. The strength of intentions should influence the performance of the behaviour (Ajzen, 1991, p. 181). Finally, it defines behaviour as an action performed (Ajzen, 1991, p. 182).

Ajzen (1991, p. 189) argues that the three predictors of intentions are based upon beliefs. Behavioural beliefs influence the attitude towards certain behaviour; normative beliefs determine the subjective norms; and control beliefs form the perceptions of behavioural control.

Combining these three factors, leads to the development of a behavioural intention. A more positive attitude and subjective norm towards the behaviour, and a greater perceived behavioural control is argued to lead to a stronger intention. A strong actual control over the behaviour facilitates people to carry out these behavioural intentions when possible (Ajzen, 1991, p. 182). Furthermore, Ajzen (1991, p. 184) expects that perceived behavioural control can also influence behaviour directly, as it often acts as a substitute for actual control.

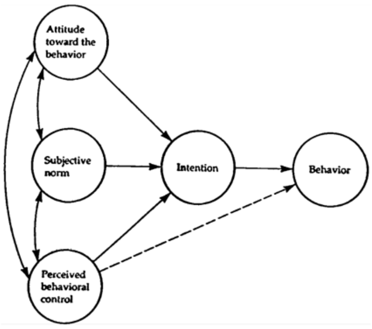


Figure 1: The Theory of Planned Behaviour (Ajzen, 1991, p. 182)

Cybersecurity education

As cyber threats continue to emerge and worsen, cybersecurity education becomes more critical. Multiple scholars studied the various types of cybersecurity education. An example is Challenge Based Learning, in which participants receive multiple challenges on specific domains. This type of education has proven to be successful in improving the student their study skills and knowledge on cybersecurity (Cheung, Cohen, Lo & Elia, 2011, p. 1). Furthermore, there are Capture the Flag events, in which participants are to secure their flag or file and capture those of others. These are often effective for introducing learners to the topic of cybersecurity (McDaniel, Talvi, & Hay, 2016, p. 5479). Different educational forms can range from presentations to tabletop games (Gondree, Peterson, & Denning, 2013, p. 64). Another form is that of serious games. Research has already pointed out that cybersecurity can be a very suitable topic for serious games (Hendrix, Al-Sherbaz, & Victoria, 2016, p. 53). This study will, therefore, continue to explore the educational method of serious gaming.

Serious gaming

Le Compte, Watson and Elizondo define serious games not only as computer games but instead also include live interactive games in their definition. This paper argues in line with these scholars and sees serious games as more than just computer games (2015, p. 205). According to Michael and Chen (2006, p. 17), the most accepted definition of serious games is that a serious game is a game in which, instead of entertainment, education is a primary goal. Michael and Chen furthermore describe these as voluntary activities, played at a specific time and place, which have certain rules attached to them. The term edutainment has often been used before for such games which have education as a purpose. Edutainment became a more prominent concept from the start of personal computers onwards. However, edutainment, or serious gaming, is not only limited to video games but instead can include any form of education which seeks to entertain (Michael & Chen, 2006, p. 24).

Contrasting to others, Charsky (2010, p. 178-179) describes that serious games aim to simultaneously educate as well as entertain. Serious games use game characteristics such as challenging activities, fantasy elements, goals and choices in order to provide a learning experience in which learning and entertainment are both incorporated.

Applications. Applying serious games takes place in different ways. This section will explore the application of serious games through wargames and safety and security games. First of all, while there is not an academic consensus on whether wargames are an individual type of game design, or would fall under serious gaming, much inspiration can be sought from wargames. Wargames are often game simulations of military operations, which provide military leaders with the opportunity to gain experience in a simulated environment. The games use data and procedures to mimic the real environment as best as possible (McHugh, 2013, p. 1-2). Nevertheless, the usage of such games is not only limited to military organisations but is instead expanded to other institutions. They can, for example, be used to simulate experiences as a cybersecurity defender, or an attacker (Casey & Willis, 2008, p. 2). War games should be as realistic as possible, including realistic events. This way, vulnerabilities in systems, or gaps in security controls will best come to light (Sullivan, Colbert, Hoffman & Kott, 2018, p. 103).

An interesting scholar in the field of wargames with regards to cybersecurity is Haggman. Haggman interpreted wargames somewhat broader and saw the primary purpose of the wargame he has developed as an educational tool rather than to form a simulation (2019, p. 141). Haggman based his tabletop wargame on the cybersecurity strategy of the UK. While he recognises that previous games are often focussed on a single organisation or of a technical nature, the game he developed took on a broader focus of strategic topics. The players should engage with both attacking or defending mechanisms, and are operating on the different domains of cyberspace; including business, government and critical infrastructure (2019, p. 114). The game mainly focused on enabling the participants to ask the right questions (2019, p. 142). Although not being the focus of the research, and evaluated qualitatively, this tabletop game was said to lead to an improvement in awareness amongst the participants (2019, p. 274).

While wargames aim to be as realistic as possible, for other types of serious games, there is less urge to achieve this. Serious games may take realistic scenarios into account, but use metaphors around it and aim at a fun experience next to learning (Charsky, 2010, p. 178-179).

Furthermore, different types of serious games, as understood in this thesis, are to be applied universally instead of company-specific. Although the approach by Haggman has proven that this is not necessary for wargames, the emphasis is often still put on it.

Furthermore, wargames on cybersecurity often revolve around the players their roles to defend against a cybersecurity attack, or being the attacker. In serious games, the metaphor can rather be different so that it incorporates cybersecurity practices without too much emphasis on it.

Instead, the type of serious game explored in this thesis is more in line with safety and security games. Martínez-Durá et al. (2011, p. 107) have laid a clear focus on these safety and security games. They found that serious games can form a good alternative for regular safety training and provide the right way of allowing learners to consider specific scenarios. Such safety games exist in the domains of health and safety in construction, public safety and pedestrian safety, food safety and cybersecurity. This type of serious gaming is often used amongst police and fire departments or by decision-makers (2011, p. 107).

Safety serious games prepare people for handling potential risky situations, or even preventing them. They are proven to be successful, for example, in the domain of aviation safety (Chittaro, 2016, p. 1527). Safety games can include several scenarios, events or conditions which may also happen in the real world. Furthermore, they can simulate events which cannot be trained, like a major fire or the hack of a vital system (Dawood et al., 2014, p. 328). Safety serious games are not known to have multiple rules or features like wargames may have. Instead, they can take up a variety of forms and different topics.

Serious gaming and the Theory of Planned Behaviour

In order to find out whether such safety serious games can potentially be useful for leading to behavioural change, the following section explores the effects of serious gaming on the different factors of the TPB by Ajzen (1991) in order to provide a background and evidence for the hypotheses presented at the end.

Subjective norms. Although different studies have investigated the effect of serious games on subjective norms, no positive results were found. In a study by DeSmet et al. (2014, p. 99), there was no significant change in subjective norms measured after playing a serious game on healthy lifestyle promotion. A study by Berger et al. (2018, p. 272), also shows no difference in subjective norms after a serious game with pharmacy students.

Attitude. More research has been conducted into attitude change through serious games; although not specifically for cybersecurity serious games (Jin, Tu, Kim, Heffron, & White, 2018, p. 68; Hendrix, Al-Sherbaz, & Victoria, 2016, p. 58). Nevertheless, in other domains, positive results were measured. For example, Thomas, Cahill, and Santilli (1997, p. 84) were successful in achieving a positive attitude change regarding safe sex negotiation through an adventure game. Additionally, a study by Rossano, Roselli and Calvano (2018, p. 53) regarding improving environmental attitudes, has given positive preliminary results.

Perceived behavioural control. No studies were found which have explored the effects of serious gaming on perceived behavioural control.

Intentions. Scholars conducted different studies into a change in intentions through serious games. A study by Schakel et al. (2019, p. 11) regarding healthy food preferences and physical activity change through serious gaming, found no significant effect on the intention to engage in such activity. On the other hand, a study by Fellnhofer (2018, p. 205) did give positive results with regards to the influence of a game-based entrepreneurship education on intentions.

Behavioural change. Nevertheless, serious games have shown to be effective in causing behavioural change in different domains. They have, for example, led to improved health behaviour (Baranowski, Buday, Thompson, & Baranowski, 2008, p. 74). In terms of sustainable behaviour, serious games were also successful in changing behaviour towards less energy consumption (Courbet, Bernanrd, Joule, Hallimi-Falkowiczm & Gueguen, 2016, p. 949; Fijnheer, van Oostendorp, & Veltkamp, 2019, p. 257). However, such elaborate research has not yet been conducted in the cybersecurity domain.

Still, Arachchilage and Love argue that a serious game of any form can be effective for preventing malicious IT attacks like viruses, malware or phishing attacks. They, however, did not test this argument in their research (2013, p. 706). Hendrix, Al-Sherbaz and Bloom argued in the same line, by arguing that cybersecurity seems a specifically well-suited topic for serious games (2016, p. 53). Furthermore, Charsky (2010, p. 182) notes that as serious games are generally more enjoyable than conventional methods used, participants are more motivated to take part in the learning activity, which may lead to positive results.

Concepts

For studying this, first of all, the concept of cybersecurity is used. Cybersecurity refers to the measures taken for the protection of an individual or entity and their computer information, against potential attacks or criminal acts carried out through the internet (Cambridge Dictionary, n.d.). The second concept used is that of serious gaming. Serious games can be played both on or without a computer, and generally entail competition, challenging activities, and a level of fun. Furthermore, they aim at a learning experience for the participants (Charsky, 2010, p. 178-179).

Theory of Planned Behaviour. The theory of Ajzen defines the concepts of attitude, perceived behavioural control, subjective norms, intentions and behaviour (1991). This theory argues that intention is the most important predictor of planned behaviour. Intentions follow from three other factors; attitude, perceived behavioural control, and subjective norms.

Mechanisms. These concepts relate to one another as cybersecurity is the topic of the serious game conducted, intending to improve cybersecurity behaviour. According to the TPB, a change in attitude, subjective norms or perceived behavioural control can also indirectly lead to a behavioural change, through a strengthened intention (Ajzen, 1991, p. 182). A survey, based upon the TPB, will eventually measure all of these factors.

Hypotheses

Building upon previous research, it is hypothesised that a cybersecurity serious game causes a positive change in: H1) cybersecurity attitude; H2) cybersecurity perceived behavioural control; H3) cybersecurity subjective norms; H4) cybersecurity intentions; H5) cybersecurity behaviour.

Methodology

Game design

For this experiment, two different online games were developed. There are, however, three conditions part of the experiment. Therefore, it valuable to know that the third condition is the control game with the same cybersecurity information as provided in the experimental game.

In order to develop an appropriate cybersecurity game which would be as effective as possible, literature has been consulted on serious gaming design in order to encourage learning and lead to a change in TPB factors. Furthermore, also literature on cybersecurity serious games has explicitly been consulted. Even though there exists a lack of experiments on this topic, different frameworks for successful cybersecurity serious games do exist.

Theory of Planned Behaviour. Given that no framework exists consisting of links between the TPB and serious games, the theory will be applied to this game manually. The description of the games below will highlight these different aspects. Furthermore, in Appendix A, an overview can be found.

Strategic game. Both of the online games developed are strategy games. In strategy games, players can adopt different strategies in order to win the game (Nagarajan, Allbeck Sood, & Janssen, 2012, p. 260). At the beginning of both developed games, players can choose their strategy and select a category of assets upon which they will focus most. Eventually, the players will notice that the strategy they chose and whether or not they have successfully completed challenges on cyber threats or working together will have a significant influence upon winning the game. Not paying attention to the cybersecurity element, or collaborating, will for example, in the long run, cost them smileys.

Metaphor. The Terminal, which constitutes the experimental condition, represents an airport terminal, which consists of six different gates. Players will get to choose their preferred gate at the beginning of the game. In this game, players will face cyber security challenges. The United Nations, constituting the control condition, represents one country, consisting of 6 different states. In this game, players will face teamwork challenges. Players can, in this game, choose their state at the beginning of the game. To do so, players of both games select an area on the graphic of the playing field. They will have to manage this gate or state as good as possible during the game. Appendix E displays these playing fields.

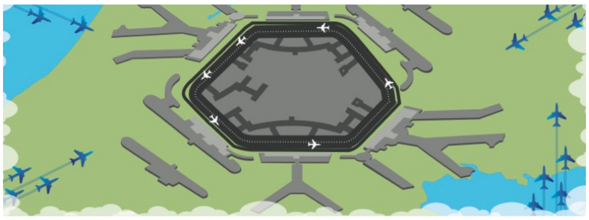


Figure 2: Playing field the Terminal

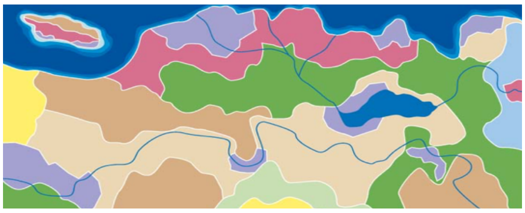
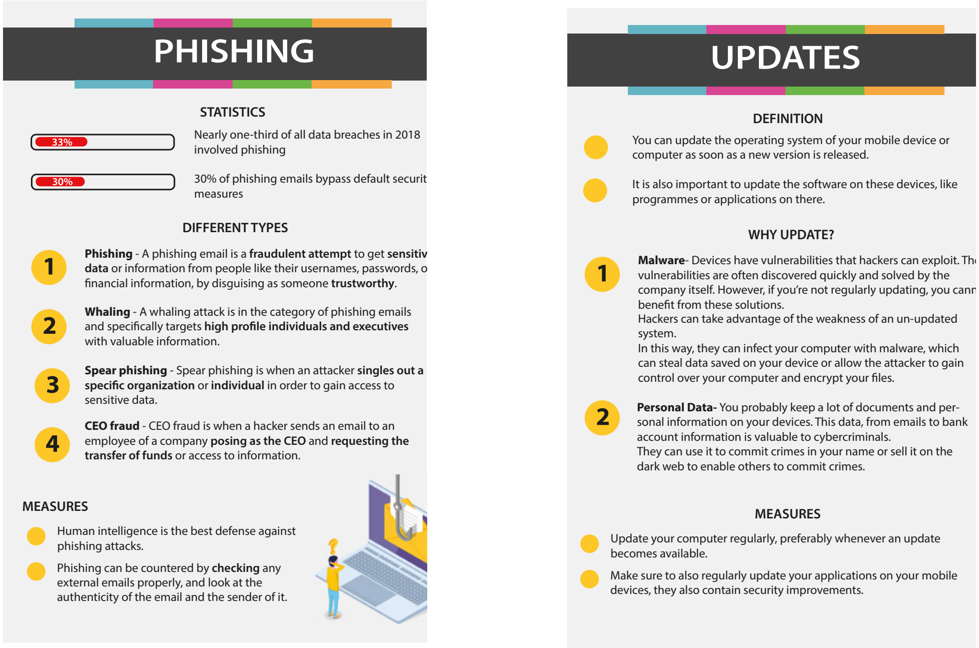


Figure 3: Playing field the United Nations

Structure of the game. First of all, before the games start, the third condition of this experiment will be shown information on cyber threats integrated into the Terminal. Four different posters summarise this information (Appendix C). Only the participants of the third condition see these posters. They are encouraged to read this information, as they are told that a memory task will be done on them later, and will afterwards proceed onto playing the United Nations game.



PHISHING

STATISTICS

33% Nearly one-third of all data breaches in 2018 involved phishing

30% 30% of phishing emails bypass default securit measures

DIFFERENT TYPES

1 **Phishing** - A phishing email is a **fraudulent attempt** to get **sensitiv data** or information from people like their usernames, passwords, o financial information, by disguising as someone **trustworthy**.

2 **Whaling** - A whaling attack is in the category of phishing emails and specifically targets **high profile individuals and executives** with valuable information.

3 **Spear phishing** - Spear phishing is when an attacker **singles out a specific organization** or **individual** in order to gain access to sensitive data.

4 **CEO fraud** - CEO fraud is when a hacker sends an email to an employee of a company **posing as the CEO** and **requesting the transfer of funds** or access to information.

MEASURES

- Human intelligence is the best defense against phishing attacks.
- Phishing can be countered by **checking** any external emails properly, and look at the authenticity of the email and the sender of it.

UPDATES

DEFINITION

- You can update the operating system of your mobile device or computer as soon as a new version is released.
- It is also important to update the software on these devices, like programmes or applications on there.

WHY UPDATE?

1 **Malware**- Devices have vulnerabilities that hackers can exploit. Th vulnerabilities are often discovered quickly and solved by the company itself. However, if you're not regularly updating, you cann benefit from these solutions.
Hackers can take advantage of the weakness of an un-updated system.
In this way, they can infect your computer with malware, which can steal data saved on your device or allow the attacker to gain control over your computer and encrypt your files.

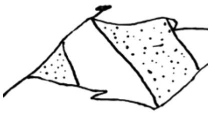
2 **Personal Data-** You probably keep a lot of documents and personal information on your devices. This data, from emails to bank account information is valuable to cybercriminals.
They can use it to commit crimes in your name or sell it on the dark web to enable others to commit crimes.

MEASURES

- Update your computer regularly, preferably whenever an update becomes available.
- Make sure to also regularly update your applications on your mobile devices, they also contain security improvements.

Figure 4: Information posters United Nations game

Both games consist of three different rounds. In round 1, the players should create their identity. They do this creating a logo or flag in the drawing field (Appendix F). Furthermore, they should come up with a motto. A selection of these logo's or flags can be found at the bottom of each page. Furthermore, a selection of motto's is presented below. The reason why each team should create a logo or flag, and motto, is that a fun element in the game is essential. Marne, Wisdom, Huynh-Kim-Bang, and Labat (2012, p. 210) have come up with a framework of facets for serious games. Their framework emphasises the fun elements of the game. They translate this into their fifth facet, called decorum. Decorum includes fun elements, which

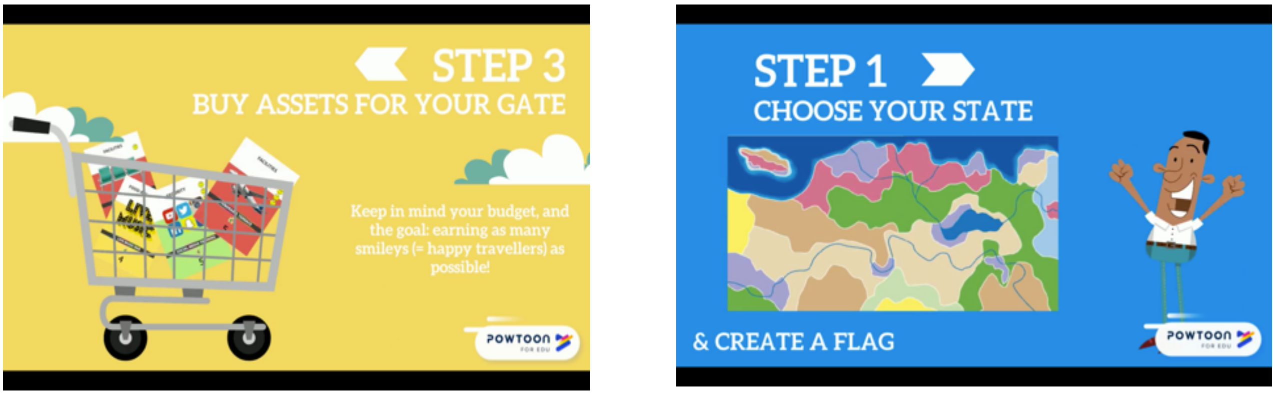


improve the motivation of the players and does not necessarily have to be related to the game content itself. In the games developed, this thus represents the logo or flags to be made.

Furthermore, such fun aspects in the game also aim at leading to a more positive attitude towards cybersecurity behaviour or collaboration. The participants should experience a fun game on these topics, leading to a more positive association with cybersecurity or teamwork. Such a positive association can potentially cause a more positive attitude towards cybersecurity behaviour, which will be measured.

Selection of motto's	
Happiness is our way of living	Gate 1, at which customer's come first!
Bread, Equality and Freedom!	Just Fly where ever YOU want 2 go
Where mountains meets the sea	A gate to come to home to!

Additionally, in round one, the players will also receive more information on the game itself through a fun video made (Appendix D). Besides this, they should develop a strategy for the assets they plan to buy in the next two rounds. They should determine which assets to buy, and on which category of assets they focus by making use of a shifting bar. By creating this strategy in the Terminal, the players will express their intentions for buying cybersecurity assets and performing cyber secure behaviour. This process aims to develop more cyber secure intentions in the daily work of participants too. In the United Nations, one of the goals is to stick to a strategy, for which they express their intention. When focusing, for example, mainly on tourism assets, they can present themselves as a holiday destination, or any other type of state.



STEP 3
BUY ASSETS FOR YOUR GATE

Keep in mind your budget, and the goal: earning as many smileys (= happy travellers) as possible!

STEP 1
CHOOSE YOUR STATE

& CREATE A FLAG

Figure 5: Introduction video's the Terminal and United Nations

GO!

In the second and third round, the players can buy any assets they want to have, or think they need to win with, during the buying rounds. In these rounds, also cybersecurity incidents in the Terminal, or collaboration incidents in the United Nations, will be presented.

Goal. The goal of the games is to earn as many smileys as possible. The players can earn these smileys by buying asset playing cards during the four buying rounds. The player with the most smileys wins a gold medal if they wish to participate in the competition. They can earn smileys in all three rounds of the game. The smileys represent happy travellers in the Terminal or happy inhabitants in the United Nations.

Smileys and assets. The playing cards represent assets that gates or states need to function correctly. Examples of these are VIP lounges, antivirus software, or toilets in the Terminal; or hotels, train stations, or cow farms in the United Nations. The assets are worth a certain number of smileys. A VIP lounge is, for example, more expensive to buy than a toilet, but also provides the participant with more smileys. Appendix G displays a selection of these assets. In order to keep the players motivated during the game, this type of scoring system shows the players their progress, motivates improvement, and encourages the players (Martínez-Durá et al., 2011, p. 121). Furthermore, a scoring system with smileys aims at leading to a more positive attitude towards cybersecurity behaviour in the Terminal or collaborative behaviour in the United Nations. Bonus smileys which players can earn by performing cyber-secure or collaborative behaviour in the game will create a positive atmosphere surrounding this behaviour. Such a positive association could potentially lead to a more positive attitude towards cybersecurity behaviour, which will be measured.

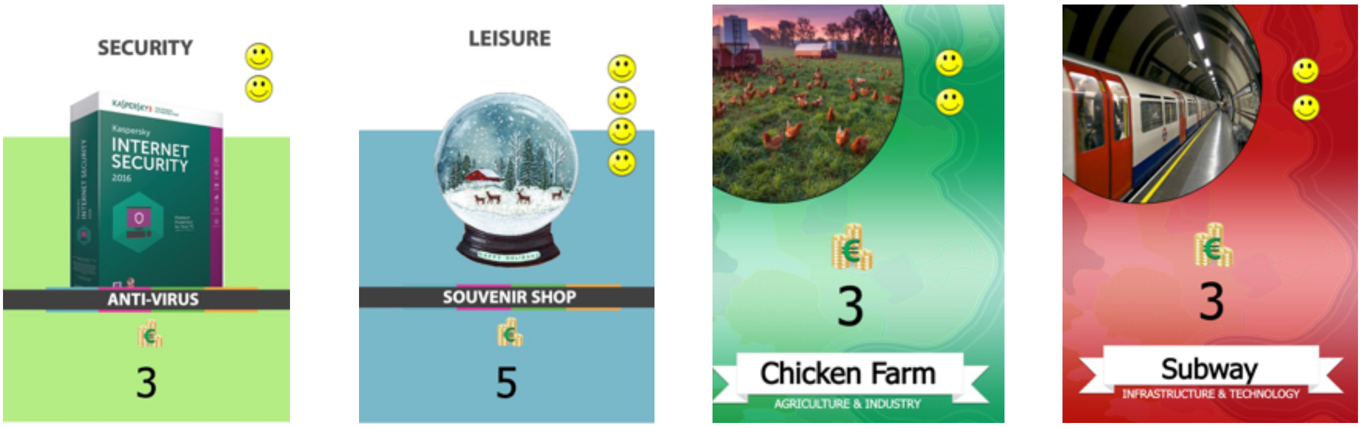
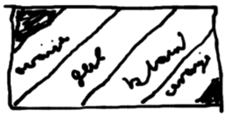
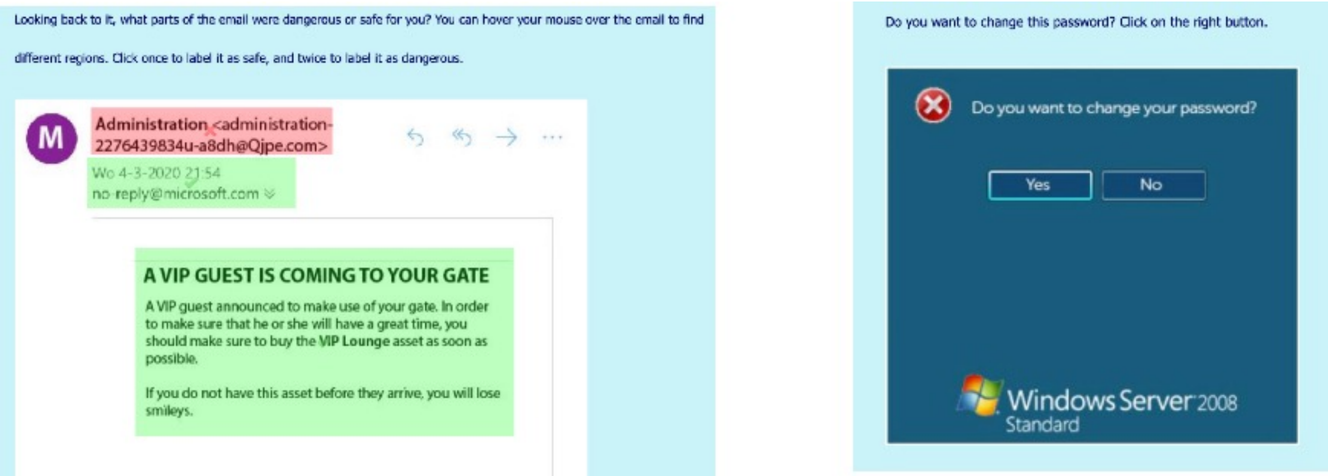


Figure 6: Examples of asset playing cards



Currency. The participants can purchase these assets with money. At the beginning of the game, they will receive their budget of 30 million euros. The idea of having a limited budget lies in prioritising which assets players prefer to buy, and especially also under which category they fall.

Cases. The games present four different cybersecurity or teamwork cases. Appendix H portrays a selection of these. These cases are implemented for making the game as realistic as possible, which is mainly in security and safety training necessary (Martínez-Durá et al., 2011, p. 108).



Looking back to it, what parts of the email were dangerous or safe for you? You can hover your mouse over the email to find different regions. Click once to label it as safe, and twice to label it as dangerous.

Administration <administration-2276439834u-a8dh@Qjpe.com>

Wo 4-3-2020 21:54
no-reply@microsoft.com

A VIP GUEST IS COMING TO YOUR GATE

A VIP guest announced to make use of your gate. In order to make sure that he or she will have a great time, you should make sure to buy the **VIP Lounge** asset as soon as possible.

If you do not have this asset before they arrive, you will lose smileys.

Do you want to change this password? Click on the right button.

Do you want to change your password?

Figure 7: Selection of, partially answered, cases in the Terminal

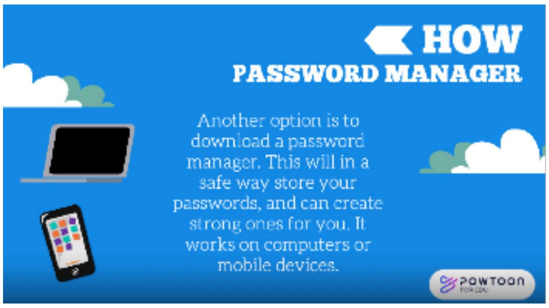
Le Compte, Watson and Elizondo point that serious games for cybersecurity need to start with implementing more basic concepts of cybersecurity, and gradually implement more complex ones (2015, p. 212). In the Terminal, this is done by starting with slightly easier cases in round two and continuing with more complicated cases in round three. In round two, the cases will thus focus on more well-known cyber threats as phishing emails and password strength. In this case, the players are, for example, challenged to recognise a phishing email. This email looks like an email from the administration department which can potentially include a tip for during the game. If the players have learned from the video they have watched before, they will recognise that this is a phishing email and thus not valid. In the third round, the cases will become more complicated, and will, for example, focus on updating a computer, or the threat of malicious USB devices. The threat of not updating a device can be due to the presence of a zero-day. Players will learn more about this type of threat in the third round, but will in this round only learn about this after the incident has taken place. In this way, the game presents the more complex concepts which are still relevant to the players at a later stage.

The decision to include these specific cyber-threats was made since these threats are the most common or applicable to the respondents. These are threats which many computer users will experience or come across often, and which are not only applicable to companies specifically (HP, 2019; ZDNet, 2020). Furthermore, information on these topics is not too complicated and can potentially make a difference in TPB factors.

Furthermore, according to Bateson, in his first level of learning, players receive information, need to memorise it and consequently need to react to it, without explicitly needing to know the reason for it (1972, p. 284 in Mitgutsch, 2011, p. 48). Therefore, in the second round, players receive information on the cases before seeing them. They can watch a video on countering the cyber threats they are about to experience. Appendix I displays screenshots of these videos. However, during the incidents in round three, they will not have access to this information anymore. In this case, they will only be presented with these informational videos after the incident has taken place. This practice is in line with the second level of learning when players find out responses to repeatable contexts.

In the United Nations, cooperation and sticking to strategies are the most important themes. As the United Nations is played individually by the players, the incidents which take place during the game instead emphasise cooperation. Examples of incidents can be neighbouring states asking for support during a military conflict, neighbouring states wanting to borrow money, or neighbouring states who want to cooperate in building assets collaboratively in order to stimulate growth in both countries. An example can be found in Appendix H. Whenever players are open to such cooperation, they will notice to gain more profit out of it than when choosing for an individual strategy instead.

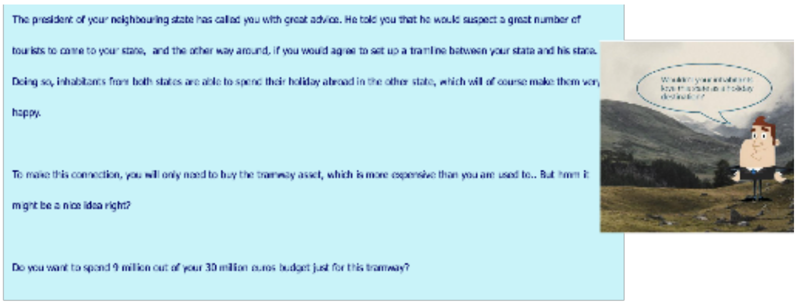
The games implement these cases and the corresponding information, in order to stimulate the perceived behavioural control of the participants. While practising with realistic cyber threat or cooperation scenario's, the participants might feel more in control of the situation if it would take place in their daily life or work.



HOW PASSWORD MANAGER

Another option is to download a password manager. This will in a safe way store your passwords, and can create strong ones for you. It works on computers or mobile devices.

Figure 8: Screenshot of information video



The president of your neighbouring state has called you with great advice. He told you that he would suspect a great number of tourists to come to your state, and the other way around, if you would agree to set up a tramline between your state and his state. Doing so, inhabitants from both states are able to spend their holiday abroad in the other state, which will of course make them very happy.

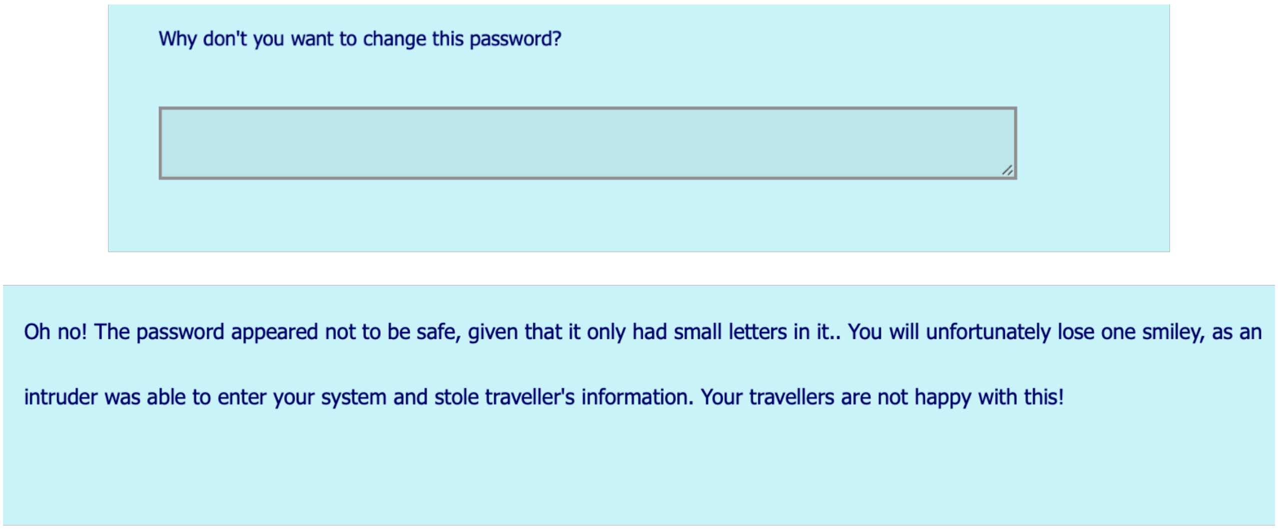
To make this connection, you will only need to buy the tramway asset, which is more expensive than you are used to.. But hmm it might be a nice idea right?

Do you want to spend 9 million out of your 30 million euros budget just for this tramway?

Wouldn't your inhabitants love this state as a holiday destination?

Figure 9: Example of case United Nations

Evaluation. The third level of learning by Bateson asks the question: ‘What does this mean to me?’. On this level, the player his conception of himself and the work he may be doing is transforming (Mitgutsch, 2011, p. 51). This learning most prominently takes place during the second and third round of the games, during which an evaluation rounds will take place. For example, after an incident, the players are asked for why they have made the decision they did (Appendix H). Furthermore, also after the game, they are asked what they would have done differently and what they have learned from the game. All of these open-questions stimulate thinking and reflection upon decisions made.



Why don't you want to change this password?

Oh no! The password appeared not to be safe, given that it only had small letters in it.. You will unfortunately lose one smiley, as an intruder was able to enter your system and stole traveller's information. Your travellers are not happy with this!

Figure 10: Evaluation round in the Terminal

Based on the third facet by Marne et al., also debriefing or quick feedback rounds are complimenting for the interactions with the simulation (Marne et al., 2012, p. 210). The third facet thus represents both the feedback received through the smiley system and the evaluation at the end of the game.

Summary. Appendix A provides a summary of the differences between these two games included in the experiment.

The experiment

Conceptual model. This research holds one independent and multiple dependent variables. The independent variable is the participation in the serious game condition; being the Terminal, the United Nations game, or the United Nations game with the cybersecurity information (Appendix B). The dependent variables are all elements of the TPB, including perceived behavioural control, attitude, subjective norms, intentions and behaviour. A post-test measured the effect of this independent variable.

This experiment exposes the possible influence of the independent variable on the dependent variables. An experiment provides the best tools for eventually measuring such a change on dependent variables, as it can best control conditions.

Research design. The experiment makes use of a post-test control group design. In this case, this design entails that there are three conditions, being one experimental condition and two control conditions. The experimental condition undergoes the online cybersecurity serious game, the Terminal, and post-test. The control condition undergoes the same post-test but participates in an online teambuilding serious game instead, the United Nations, or in the United Nations with the cybersecurity information of the Terminal (Gravetter & Forzano, 2018, p. 249). This last condition was added so that the effect of the game itself can be measured best, instead of only the information provided in the game. The difference in the results of the post-tests of these conditions provided insights into the effectiveness of the experimental condition.

The randomisation of participants to either the control or experimental groups took place at the start of the game experience. Participants who clicked on the game link got assigned to one of these conditions through means of randomisation.

Serious game. The serious game used as an experimental condition is an online cybersecurity serious game developed in assignment for the company LIB Businessgames. The online cybersecurity serious game, the Terminal, was designed from scratch through making use of best practices found in the academic literature on both regular serious games and cybersecurity serious games. With permission of LIB Businessgames, the live team building game, the United Nations, which constitutes the control condition was re-developed into an online game. The reason for this change from live interactive serious games into online games has been for practical measures taken in response to the COVID-19 virus, which prohibits more than three people gathering.

Data collection. The sampling for this experiment happened through the non-probability sampling technique of convenience sampling. Through this sampling technique, individuals who were readily available for the researcher were selected (Gravetter & Forzano, 2018, p. 122). Convenience sampling means that the participants come from contacts close to the experimenter, and people reached through personal networks. To be precise, the recruitment of respondents happened through social media, email, and a company networking service. The sample eventually included 425 participants, with 258 participants finishing the game and completing the survey at the end of it. The additional 167 participants did not finish the game nor took part in the survey at the end of it.

The experiment has produced primary source data to be used in the analysis, as no data was available before. However, background literature upon which the study and game design builds used secondary source data instead.

Measurement: Theory of Planned Behaviour. This research adopted a post-test experimental design for measuring the difference in the TPB components between the groups before and after the serious game. This measurement happened through a questionnaire. The post-test questionnaire, conducted right after the serious games asks questions towards the TPB factors of cybersecurity behaviour through a 7-point Likert scale. In doing so, it includes amended questions of the questionnaires by Poulter, Chapman, Bibby, Clarke, and Crundall (2008, p. 2061); and Mcmillan and Conner (2003, p. 320-321). Appendix J includes this questionnaire. The questionnaire uses concepts of the TPB. Because of privacy concerns, the experiment did not include a post-test conducting an objective behavioural measurement. Therefore, this study will only measure self-reported behaviour. This type of measurement also comprises one of the limitations of this study, given that conducting an objective behavioural measurement is more accurate and less prone to biases.

When participants have taken part in a Terminal, one can expect them to experience a social desirability to answer survey questions on cybersecurity in the post-test positively. For making the effect of this social desirability from the Terminal game unlikely, the third game condition was created. As mentioned before, in this condition, the participants also received cybersecurity information. These participants were, therefore, expected to display similar social desirability.

Data analysis. For answering the research question, ANOVA tests analysed the difference in the post-tests between the groups. This statistical analysis was conducted in SPSS. It applied an adjustment through the posthoc tests in order to increase the robustness and validity of the results. This way, the aggregate scores of the TPB survey after the games are compared between the three conditions. Further tests were conducted with regards to other game elements, such as the duration of the games or the quitting rate.

Results

Participants

In order to learn more about the participants who were part of this experiment, the descriptive statistics of the demographic variables “age”, “gender”, “occupation”, “workplace”, and “computer usage” will be explored. These are valuable to include, as they give more information towards the composition of the sample at hand.

Both employees, students, and persons with another occupation participated in the survey which provides this data. A total of 258 respondents completed both the game and the survey. Furthermore, exactly half of the respondents were male, with the average age of the respondents being 30.54 (*SD* = 12.32). Participants were either employed at an organisation, as 53.1 percent was; enrolled in a study programme, as 40.7 percent was; or had another occupation, as 6.2 percent did.

The participants had different workplaces, with the majority working primarily from an office, which constituted 41.5 percent of the sample. Other participants worked primarily from home, constituting 35.5 percent; from a public space or library, which 10.9 percent did; or from another place which they manually filled in manually like 6.2 percent did. To another 6.2 percent of the respondents, this was not applicable, given that they did not report studying or working to be their occupation.

In terms of computer usage, the respondents mainly clustered around always using a computer, with 86.4 percent of the participants. 7.0 percent of the participants used the computer only sometimes, while 0.4 percent never used the computer while working or studying. Again, to 6.2 percent of the respondents, this was not applicable, given that they did not report studying or working to be their occupation.

Finally, the scale variables of the baseline group are explored. The baseline group comprises of the participants of the regular United Nations game condition (*N* = 89). This group is seen as the baseline, as they did not receive any cybersecurity content or information during their game experience.

With regards to the scale variables, the average attitude score of this group is 16.61 (*SD* = 2.84). The lowest possible score on all scales was 3, while the highest possible score was 21. Therefore, the mean lies much above the middle score of 12.00. The average of the respondents of this group thus had a positive attitude towards cybersecurity practices. Furthermore, results show that the average score on subjective norms is 12.25 (*SD* = 3.14). The average score on subjective norms is this time slightly above the middle point of 12.00, showing that the average of the respondents of this group experienced rather neutral subjective norms.

Thirdly, results show that the average perceived behavioural control is 13.80 ($SD = 3.59$). Given that the average score on perceived behavioural control is thus somewhat higher than the middle point of 12.00, this shows that the average of the respondents of this baseline group had a slightly strong perceived behavioural control. Fourthly, the average score on intentions is 14.55 ($SD = 3.84$). Given that the average score on intentions is thus higher than the middle point of 12.00, this shows that the average of the respondents of this group had a relatively strong intention to perform cybersecurity behaviour.

Finally, the average score on behaviour of this group is 14.75 ($SD = 3.74$). Given that the average score on behaviour is thus again higher than the middle point of 12.00, this shows that the average of the respondents reveals relatively strong self-reported cybersecurity behaviour.

ANOVA

This section aims to find out more about the difference between participants of the Terminal, the regular United Nations game, and the United Nations game with cybersecurity information on all elements of the TPB. To do so, through a one-way ANOVA, the means of these elements based on the game condition were compared. Whenever according to Levene's homogeneity of variance test equal variances could be assumed, then a Bonferroni test was chosen as a posthoc test. Whenever equal variances could not be assumed based upon Levene's homogeneity of variances test, then a Games-Howell test was chosen for the posthoc analysis instead.

Attitude

The ANOVA results for attitude as presented in table 1 show that a statistically significant difference, $F(2, 255) = 6.196$, $p = .002$, is present in the attitude value between the three game conditions. Consequently, the posthoc Games-Howell test showed that there is a significant mean difference ($p = .001$) between the Terminal game condition ($M = 18.01$, $SD = 2.31$) and the regular United Nations condition ($M = 16.61$, $SD = 2.84$), with the Terminal scoring higher. Furthermore, there is also a significant mean difference ($p = .034$) between the Terminal game condition ($M = 18.01$, $SD = 2.31$) and the United Nations condition with cybersecurity information ($M = 16.93$, $SD = 3.17$), with again the Terminal scoring higher. As all scores lie much above than the middle score of 12, all groups show a positive attitude towards cybersecurity behaviour. Especially the score of the Terminal is in the high end of the possible scores, with 21 being the maximum. Based upon the posthoc test, there is no significant difference (*p* = .773) between the attitude on cybersecurity behaviour of the United Nations condition (*M* = 16.61 *SD* = 2.84) and the United Nations condition with cybersecurity information (*M* = 16.93, *SD* = 3.17).

Subjective norms

Secondly, the ANOVA results for subjective norms as presented in table 1 show that a statistically significant difference, *F*(2, 255) = 4.038, *p* = .019, is present in the subjective norms value between the game conditions. Consequently, the posthoc Bonferroni test showed that there is a significant mean difference (*p* = .028) between the Terminal game condition (*M* = 13.53, *SD* = 3.28) and the regular United Nations condition (*M* = 12.25, *SD* = 3.14), with the Terminal scoring higher. As the Terminal score lies somewhat above the middle score of 12, the subjective norms are rather positive. The average score of the United Nations condition is instead rather neutral, lying close to the middle score.

Based upon the posthoc test, there is no significant difference (*p* = .077) between the subjective norms on cybersecurity behaviour of the Terminal game condition (*M* = 13.53, *SD* = 3.28), and the United Nations condition with cybersecurity information (*M* = 12.40, *SD* = 3.30). The difference in subjective norms may, therefore, be accounted to the cybersecurity information provided instead of the presentation method. Finally, there is also no significant mean difference (*p* = 1.000) between the regular United Nations (*M* = 12.25, *SD* = 3.14) and the United Nations condition with cybersecurity information (*M* = 12.40, *SD* = 3.30).

Perceived behavioural control

Thirdly, the ANOVA results for perceived behavioural control as presented in table 1 show that a statistically significant difference, *F*(2, 255) = 5.024, *p* = .007, is present in the perceived behavioural control value between the game conditions. Consequently, the posthoc Bonferroni test showed that there is a significant mean difference (*p* = .011) between the Terminal condition (*M* = 15.31, *SD* = 2.95) and the regular United Nations condition (*M* = 13.80, *SD* = 3.59), with the Terminal scoring higher. Furthermore, there is also a significant mean difference (*p* = .042) between the Terminal (*M* = 15.31, *SD* = 2.95) and the United Nations condition with cybersecurity information (*M* = 14.00, *SD* = 3.79), with the Terminal again scoring higher. As all scores lie somewhat above than the middle score of 12, all groups show a rather positive perceived behaviour control. Based upon the posthoc test, there is no significant difference (*p* = 1.000) between the perceived behavioural control on cybersecurity behaviour of the regular United Nations condition (*M* = 13.80, *SD* = 3.59) and the United Nations condition with cybersecurity information (*M* = 14.00, *SD* = 3.79).

Intentions

Fourthly, the ANOVA results for intentions as presented in table 1 show that a statistically significant difference, *F*(2, 255) = 12.561, *p* = .000, is present in the intentions value between the game conditions. Consequently, the posthoc Games-Howell test showed that there is a significant mean difference (*p* = .000) between the Terminal game condition (*M* = 17.08, *SD* = 3.10), and the regular United Nations condition (*M* = 14.55, *SD* = 3.84), with the Terminal scoring higher. Furthermore, there is also a significant difference (*p* = .000) between the means of the Terminal game condition (*M* = 17.08, *SD* = 3.10) and those of the United Nations condition with cybersecurity information (*M* = 14.65, *SD* = 4.36), with again the Terminal scoring higher. As all scores, and especially that of the Terminal, lie above than the middle score of 12, all groups show positive intentions towards cybersecurity behaviour. Based upon the posthoc test, there is no significant difference (*p* = .987) between the intentions on cybersecurity behaviour of the regular United Nations condition (*M* = 14.55, *SD* = 3.84) and the United Nations condition with cybersecurity information (*M* = 14.65, *SD* = 4.36).

Behaviour

Finally, the ANOVA results for behaviour as presented in table 1 show that a statistically significant difference, *F*(2, 255) = 5.761, *p* = .004, is present in the behaviour value between the game conditions. Consequently, the posthoc Bonferroni test showed that there is a significant mean difference (*p* = .010) between the Terminal game condition (*M* = 16.37, *SD* = 3.53) and the regular United Nations condition (*M* = 14.75, *SD* = 3.74), with the Terminal scoring higher. Furthermore, there is also a significant mean difference (*p* = .010) between the Terminal game condition (*M* = 16.37, *SD* = 3.53) and the United Nations condition with cybersecurity information (*M* = 14.28, *SD* = 4.63), with the Terminal again scoring higher. As all scores lie much above than the middle score of 12, all participants show rather positive self-reported cybersecurity behaviour. Based upon the posthoc test, there is no significant difference (*p* = .906) between the cybersecurity behaviour of the regular United Nations condition (*M* = 14.75, *SD* = 3.74) and of the United Nations condition with cybersecurity information (*M* = 14.28, *SD* = 14.63).

Condition	**N**	**Attitude** M (SD)	**Subjective Norms** M (SD)	**Perceived Behavioural Control** M (SD)	**Intentions** M (SD)	**Behaviour** M (SD)
The Terminal	89	18.01 (2.31)	13.53 (3.28)	15.31 (2.95)	17.08 (3.10)	16.37 (3.53)
The United Nations A	89	16.61 (2.84)	12.25 (3.14)	13.80 (3.59)	14.55 (3.84)	14.75 (3.74)
The United Nations B (cyber)	80	16.93 (3.17)	12.40 (3.30)	14.00 (3.79)	14.65 (4.36)	14.28 (4.63)

Table 1: Descriptives

Measuring other game elements

In order to gain more insights into the effectiveness of the game designs of the different conditions, several other tests were conducted. These tests will assess whether the conditions influenced quitting or finishing the game, whether the duration did, and finally in which stage of the game most participants quit. The topic of quitting is put much emphasis on, as 181 of the 439 participants quit the game early. Insights into this process can be valuable for future experiments into serious gaming on cybersecurity.

From the 181 unfinished or uncompleted recorded responses, 14 respondents quit the survey on the first briefing screen. Therefore, they were not assigned a condition yet, and are not taken into account when evaluating the conditions of the game.

Finished or not

This section will assess whether there is a significant difference between the respondents quitting in the various game conditions. Therefore, it is good to know that a total of 54 respondents of the Terminal game condition did not finish the game. The same went for a total of 50 respondents of the regular United Nations condition, and 63 respondents of the United Nations condition with cybersecurity information. The game was considered as finished, whenever the progress value was at least 97 percent. This percentage was chosen as at 97 percent; all necessary questions were answered. These participants have only missed the last debriefing screen. A Pearson Chi-square test showed whether there is a significant difference between the respondents quitting in the various conditions.

	Finished	**Did not finish**	
The Terminal	89 (62.2%)	54 (37.8%)	143 (100%)
United Nations A	89 (64.0%)	50 (36.0%)	139 (100%)
United Nations B (cyber)	80 (55.9%)	63 (44.1%)	143 (100%)
	258	167	425

Table 2: Bivariate Relationship between Finished or not and the Game Condition (N = 425).

This test showed that finishing the game or not, and the condition participated in are not related amongst the respondents. Consequently, there is no statistically significant relationship between finishing the game and the game condition, χ^2 (2, N = 425) = 2.143, p = .342. This finding provides evidence that the game designs of the various game conditions did not lead to significant differences in the finishing/quitting rate.

Duration

In order to find out whether participants might have quit the game as they have already spent a very long time on playing it, the average duration of the finished games and unfinished games was compared. Again, the game was considered to be finished, whenever the progress value was at least 97 percent.

Before conducting this comparison, several outliers were removed in order to guarantee more representative results. This process entailed the removing of all responses, which took longer than a total of 70 minutes. Given that the data set contained several outliers with durations of more than 40 hours, different data points were removed.

As seen in Table 3, the average of the duration of the finished games is 25.75 minutes (*SD* = 14.89). The average of the duration of the unfinished games is 4.33 minutes (*SD* = 7.67). These results thus show that participants finishing the game spent more time playing it, and thus had a significantly higher duration. This finding does not give any evidence for the statement that players might have quit the game early because of the long time they had already spent on playing it. On the other hand, they can still have quit because of the expected long duration of the game. Nevertheless, players who quit the game early only engaged in it rather shortly.

Condition (minutes)	**N**	**Mean**	**S. Deviation**
Finished	239	25.75	14.89
Unfinished	159	4.33	7.67

Table 3: Duration vs. Finished/unfinished

Progress

Finally, the progress variable shows at what percentage of the games the participants quit. For most of the participants, this value is 100, as they have completed the game. However, given that also 167 participants quit during the game, it is interesting to look more elaborately at the data surrounding this progress variable.

Conducting a descriptive analysis shows that the average of the progress variable is 69.78 (*SD* = 41.21). Therefore, the average progress thus lays around 70%. In order to gain more insights into the progress distribution of the unfinished games, three different progress categories were created. The beginning category represents those that quit the game at the beginning of it, comprising the progress percentages of 0-33 percent. The middle category represents those that quit the game in the middle of it, comprising the progress percentages of 34-66 percent. Lastly, the final category represents those that quit the game towards the end of it, comprising of 67-96 percent. From 97 percent onwards, the response qualified as finished. Table 4 shows more insights into the distribution.

Variable	**Frequency**	**Percentage**
Progress		
Beginning	130	77.8%
Middle	18	10.7%
End	19	11.4%

Table 4: Frequency Table Progress Variable

This table shows that most participants, 77.8%, quit at the beginning of the game. Therefore, a high number of people have only been checking what the game was and how it worked but did not complete a significant part of the game.

A much lower number of people quit in the middle of the game, probably because they wanted to finish what they have started. Furthermore, also a smaller percentage quit the game towards the end of it. While investigating the data, the vast majority of this group appeared to quit the game upon seeing the survey questions towards the end of it.

Discussion

This section will provide more substance to eventually answer the research question of *'What are the effects of a cybersecurity serious game on the Theory of Planned Behaviour factors of cybersecurity behaviour?'*. In doing so, it builds upon extant literature and the results of this study. This section will provide new insights into the topics of cybersecurity education and serious gaming.

Interpretation

The results of this experiment showed a significant difference in all elements of the TPB. This difference means that the Terminal game scored significantly higher than the regular United Nations game on all elements of the TPB. Furthermore, the Terminal scored significantly higher on all but one element of the TPB, that of subjective norms, than the United Nations game with same cybersecurity information. For this particular factor, the improvement in subjective norms cannot accurately be accounted to the serious game, but may instead be caused by the cybersecurity information provided.

In terms of alternative explanations, one can expect participants who played the Terminal game to experience social desirability to answer the survey questions on cybersecurity in a positive direction. Nevertheless, this expectation is unlikely, given that also a control condition with cybersecurity information was included in the experiment. This same social desirability can thus apply to participants of the United Nations game condition with cybersecurity information. Therefore, as in all but one element of the TPB, a significant difference was observed between these conditions, the role social desirability is unlikely.

Another alternative explanation which may influence the answers on self-reported behaviour, is that of consistency. As it was beyond the scope of this research to conduct an objective behavioural measurement, self-reported behaviour was measured instead. Given that the participants have, however, only just completed the game before this measurement, they did not have the chance to change their behaviour in this short time. Therefore, one can assume that their answers are mainly based upon consistency instead. In the case that the participants have for example already given positive answers towards their intentions to perform specific cyber-secure behaviour, and when being asked whether they also perform such behaviour, they are likely to answer those in a positive direction too.

To sum up, these findings provide good evidence for all five hypotheses as proposed in the theoretical framework. This conclusion means that there is evidence that a cybersecurity

game has indeed caused a positive change in cybersecurity attitude; perceived behavioural control; subjective norms; intentions; and self-reported behaviour.

The findings on the TPB factors also show that providing participants with sole information did not have significant influence on the these factors. This is the case as there were no significant differences observed between the regular United Nations game and the United Nations game with cybersecurity information on any element of the TPB. While one may expect that, for example, attitudes being on the lowest level of the TPB can be influenced by solely providing information, this experiment finds evidence for the contrary.

With regards to other game elements, the results show no significant difference between the various game designs and their quitting rates. Therefore, there is no need for future amendments in order to counter such behaviour. Furthermore, as expected, participants who finished the game and survey spent considerably more time on the experience than participants who quit during the game did. This result provides evidence for the finding that participants did not quit the game because of the long time they had already spent on it. Finally, again as expected, participants who quit the game, mainly did so at the beginning of the game experience. This finding can most likely be accounted to participants wanting to have a look out of interest but did not want to invest time into participating in the end.

Implications

In terms of implications, first of all, this research has shown that the method of serious gaming can be added to the different existing types of cybersecurity education. Besides the successful methods of Challenge Based Learning or Capture the Flag events, serious gaming has shown to be successful in influencing the TPB factors of cybersecurity behaviour (Cheung, Cohen, Lo and Elia, 2011, p. 1; McDaniel, Talvi, & Hay, 2016, p. 5479).

In addition, this research can also contribute to the literature on serious gaming and the TPB. Given that the Terminal serious game has shown to be effective on all elements of the TPB, the main implication here is that serious games can also be efficient in leading to a change in perceived behavioural control and subjective norms. This change was not found before. Therefore, a new theme in research could be to further study this relationship (Berger et al., 2018, p. 272; DeSmet et al., 2014, p. 99). This suggestion will be elaborated upon further below.

Subjective Norms. Previous research did not find any significant changes in subjective norms amongst participants after participating in a serious game (Berger et al., 2018, p. 272; DeSmet et al., 2014, p. 99). Contrary to these previous findings, this study did measure a significant change in subjective norms amongst the participants, as the Terminal game condition had a significant mean difference in subjective norms with the regular United Nations game condition. This difference may be due to the higher N in this study, the experimental design rather than meta-study as DeSmet et al. (2014) conducted, or as this design compared findings to other conditions rather than to a post-test (Berger et al., 2018).

Attitude. In the domain of attitude, previous research has proven that serious games on variables topics are capable of leading to an attitude change (Thomas, Cahill, and Santilli, 1997, p. 84; Rossano, Roselli and Calvano, 2018, p. 53). The topic of cybersecurity can be added to this, as the experimental condition has led to a positive attitude change on cybersecurity behaviour in comparison to the control conditions.

Perceived behavioural control. While no previous literature found explored the effects of serious games on perceived behavioural control, this study did take the element of perceived behavioural control into account. In doing so, it showed that this serious game on cybersecurity led to a significantly more positive perceived behavioural control in comparison to the control conditions. Therefore, serious games can be effective in leading to a change in perceived behavioural control.

Intentions. While positive changes were measured in intentions through serious gaming in previous research, no consensus was achieved (Fellnhofer, 2018, p. 205; Schakel et al., 2019, p. 11). This research has, however, shown that also a positive and significant change in intentions can be caused by serious gaming. In doing so, it is in line with the findings of Fellnhofer (2018). As this finding is about cybersecurity serious games, specifically, more research into serious games on other topics with relation to behavioural intentions is needed.

Behavioural change. Various previous research has shown that serious gaming can be effective in leading to behavioural change on the topic of the game (Courbet, Bernanrd, Joule, Hallimi-Falkowiczm & Gueguen, 2016, p. 949; Fijnheer, van Oostendorp, & Veltkamp, 2019, p. 257). This study adds to these researches and concludes that also games on the topic of cybersecurity can be effective in leading to a self-reported behavioural change. This study did not conduct an objective behavioural measurement.

The main practical implication of this study is that as serious games have shown to be effective in leading to a positive change on all elements of the TPB, they can be used more frequently for training or educational purposes. The advice to businesses or even educational programs is thus to look more extensively into the method of serious gaming for training purposes. This finding is line with the predictions of Hendrix, Al-Sherbaz, and Victoria (2016, p. 53) noting that cybersecurity can be a very suitable topic for serious games.

Limitations

The first limitation of this study lies in the fact that this study only measured self-reported behaviour. Due to privacy concerns, no objective behavioural measurement was conducted. Instead, through a questionnaire, the participants were asked for their behaviour. This self-reported behaviour is, however, prone to more bias and can be less accurate than conducting an objective behavioural measurement. Participants could, in this case, for example, want to be consistent and therefore answer more positively towards their behaviour than the behaviour they experience.

A second limitation lies in the fact that this research could not get to know more about how the participants have experienced the game because of the quantitative approach it has taken. Measuring this could however give useful insights into the quality of the game itself, which is interesting for further implementation of the game. Taking on such a broad approach was, however, beyond the scope of this research.

A final limitation is that the online games were developed to be live interactive serious games at the start. Given the COVID-19 virus, there was no possibility of conducting these live serious games with large groups anymore. For that purpose, the games were redesigned into online variants. Whenever the games were, however, designed for online purposes from the start, the design could have been better adjusted.

Recommendations

Future research is encouraged to further look into the method of serious gaming on the topic of cybersecurity. First of all, building upon this study, future research should extend this type of online serious game, to include more and a wider variety of cases. This way, the participants will familiarise themselves with more cybersecurity topics, which will give them better hands-on information for their daily work. Also, having a more elaborate game and a wide variety of topics may provide for an even more substantial effect for leading to a change in TPB factors.

Secondly, also building upon this study, future research is instead encouraged to conduct an objective behavioural measurement, rather than using self-reported behaviour. This way, a proper measurement can be done on the effectiveness of serious games like these. Such a behavioural measurement can, for example, be conducted a week after the game has taken place so that the experience of the game itself will be influencing the behaviour less than it would right after the game has taken place.

From a theoretical lens, future research is encouraged to look more into the angle of live interactive serious games. Given that these games provide for teamwork and more interaction between the participants and the game facilitators, that they can even be more efficient than online games played individually can be. The working together in teams, and having to trade with other teams can foster learning, through the communication of learnings (Camilleri, Busuttil, & Montebello, 2011, p. 482). In a live interactive version of the games, participants are to be grouped in six different teams representing different states or gates with five players each. This division implements the process of teamwork in order to stimulate the development of positive subjective norms. In order to win, participants should work together and stimulate each other to also think of the cybersecurity or cooperative dimension in everything they do. In this way, participants will experience social pressure from one another to perform this type of behaviour.

In terms of the application of serious games, future research is encouraged to perform more experiments with serious games on different topics than cybersecurity. The literature on serious gaming continues to be rather thin and limited, especially on their efficiency with the TPB. Therefore, scholars are encouraged to perform more experiments with both new as well as existing serious games.

Conclusion

To conclude, this research has used an experimental approach in order to test the effectiveness of a serious game on cybersecurity in leading to a change in TPB factors of cybersecurity behaviour. This research adopted a quantitative experiment, as no previous study conducted this type of research on the connection between all of the TPB factors and cybersecurity serious games before. Serious games were however already effective in other domains, like sustainable behaviour (Courbet, Bernanrd, Joule, Hallimi-Falkowiczm & Gueguen, 2016, p. 949).

For studying this, the research asked the following research question: *What are the effects of a cybersecurity serious game on the Theory of Planned Behaviour factors of cybersecurity behaviour?*

After participating in an online serious game, 267 participants filled in a survey including TPB factors. The results of the questionnaire showed that on every factor of the TPB, participants of the Terminal game condition scored the highest and the most positive with regards to the TPB factors of cybersecurity behaviour. Participants of this cybersecurity game thus show a significant mean difference, on every aspect of the TPB, compared to the participants of the regular serious game, which acted as the control condition.

Putting this in context with the literature used, the results of this study showed that also in the cases of perceived behavioural control and subjective norms, a serious game on cybersecurity scored better than a regular serious game. Furthermore, this research showed that the topic of cybersecurity can indeed be suitable for online serious games. For these reasons, cybersecurity serious games can be used more often and more extensively as cybersecurity training. Businesses or even educational programs are therefore recommended to look more extensively into the method of serious gaming for training purposes.

Given that humans are seen as the weakest link in the chain of cybersecurity, any methods which prove to be efficient in cybersecurity training, which could improve this situation are useful to assess. Doing so could at best even lead to a lower number of data breaches, malware incidents, reputational damage and possible damage to national security.

References

Ajzen, I. (1991). The Theory of Planned Behavior. Organizational behaviour and human decision processes, 50, 179-211.

Arachchilage, N. A. G., & Love, S. (2013). A game design framework for avoiding phising attacks. Computers in Human Behaviour, 29, 706-714.

Baranowski, T., Buday, R., Thompson, D. I., & Baranowski, J. (2008). Playing for Real: Video Games and Stories for Health-Related Behaviour Change. American Journal of Preventive Medicine, 34, 74-82.

Bateson, G. (1972). Steps to An Ecology of Mind. Chicago, IL: The University of Chicago Press.

Berger, J., Bawab, N., De Mooij, J., Widmer, D. S., Szilas, N., De Vriese, C., & Bugnon, O. (2018). An open randomized controlled study comparing an online textbased scenario and a serious game by Belgian and Swiss pharmacy students. Currents in Pharmacy Teaching and Learning, 10, 267-276.

Cambridge Dictionary. (n.d.). Meaning of Cybersecurity in English. Retrieved on 5 December, 2019 from https://dictionary.cambridge.org/dictionary/english/cybersecurity.

Camilleri, V., Busuttil, L., & Montebllo, M. (2011). Social Interactive Learning in Multiplayer Games. In M. Ma, A. Oikonomou, & L. C. Lain (Eds.), Serious Games and Edutainment Applications. London: Springer.

Casey, T., & Willis, B. (2008). Wargames: Serious play that tests enterprise security assumptions. Retrieved on 20 April, 2020 from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Intel%20-%20Wargames-%20Serious%20Play%20that%20Tests%20Enterprise%20Security%20Assumptions.pdf.

Charsky, D. (2010). From edutainment to serious games: A change in the use of game characteristics. Games and Culture, 5(2), 177-198.

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge Based Learning in Cybersecurity Education. Paper presented at WorldComp '11: The World Congress in Computer Science, Computer Engineering and Applied Computing, Las Vegas.

Chittaro, L. (2016). Designing Serious Games for Safety Education: "Learn to Brace" versus Traditional Pictorials for Aircraft Passengers. IEEE Transactions on Visualization and Computer Graphics, 22(5), 1527-1539.

Courbet, D., Bernard, F., Joule, R., Hallimi-Falkowicz, S., & Gueguen, N. (2016). Small clicks, great effects: the immediate and delayed influence of websites containing serious games on behavior and attitude. International Journal of Advertising, 35(6), 949-969.

Dawood, N., Miller, G., Patacas, J., & Kassem, M. (2014). Construction Health and Safety Training: The Utilisation of 4D Enabled Serious Games. Journal of Information Technology in Construction, 19, 326-335.

DeSmet, A., Van Ryckeghem, D., Compernolle, S., Baranowski, T., Thompson, D., Crombez, G., Poels, K., Van Lippevelde, W., Bastiaensens, S., Van Cleemput, K., Vandebosch, H., & De Bourdeaudhuij, I. (2014). Preventive Medicine, 69, 95-107.

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272, 1109-1119.

Fellnhofer, K. (2018). Game-based Entrepreneurship Education: Impact on Attitudes, Behaviours and Intentions. World Review of Entrepreneurship, Management and Sustainable Development, 14, 205 – 228.

Fijnheer, J. D. L., van Oostendorp, H., & Veltkamp, R. C. (2019). Enhancing Energy Conservation by a Household Energy Game. In M. Gentile, M. Allegra, & H., Söbke (Eds.), Games and Learning Alliance. New York, NY: Springer.

Gondree, M., Peterson, Z. N. J., & Denning, T. (2013). Security through play. IEEE Security & Privacy, 11(3), 64-67.

Gravetter, F. J., & Forzano, L., B. (2018). Research Methods for the Behavioral Sciences. Boston, MA: Cengage.

Haggman, A. (2019). Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education (Doctoral dissertation). Retrieved from https://core.ac.uk/reader/219839790.

Hendrix, M., AlSherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games, 3(1), 5361.

HP. (2019). What Are the Most Common Types of Cyber Attacks? Retrieved on 22 April, 2020 from https://store.hp.com/us/en/tech-takes/most-common-types-of-cyber-attacks.

IBM. (2018). 2018 Cost of Data Breach Study: Impact of Business Continuity Management. Retrieved November 24, 2019, from https://www.ibm.com/downloads/cas/AEJYBPWA.

Jin, G., Tu, M., Kim, T., Heffron, J., & White, J. (2018, February 21-24). Game based Cybersecurity Training for High School Students. Paper presented at SIGCSE '18: 49th

ACM Technical Symposium on Computer Science Education, Baltimore. doi: 10.1145/3159450.3159591

Le Compte, A., Watson, T., & Elizondo, D. (2015, May 26-29). A renewed approach to serious games for cyber security. Paper presented at 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallinn. doi: 10.1109/CYCON.2015.7158478

Marne, B., Wisdom, J., Huynh-Kim-Bang, B., & Labat, J-M. (2012). The Six Facets of Serious Game Design: A Methodology Enhanced by Our Design Pattern Library. In A. Ravenscroft, S. Lindstaedt, C. Delgado Kloos, & D. Hernández-Leo (Eds.), 21st Century Learning for 21st Century Skills. Berlin: Springer.

Martínez-Durá, R. J., Arevalillo-Herráez, M, García-Fernández, I., Gamón-Giménez, M. A., & Rodríguez-Cerro, A. (2011). Serious Games for Health and Safety Traning. In M. Ma, A. Oikonomou, & L. C. Lain (Eds.), Serious Games and Edutainment Applications. London: Springer.

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. Paper presented at 2016 49th Hawaii International Conference on System Sciences (HICSS), Manoa.

McHugh, F. (2013). U.S. Navy fundamentals of war gaming. New York, NY: Skyhorse Publishing.

Mcmillan, B., & Conner, M. (2003). Using the theory of planned behaviour to understand alcohol and tobacco use in students. Psychology, Health & Medicine, 8(3), 317-328.

Michael, D., & Chen, S. (2006). Serious Games: Games that Educate, Train and Inform. Boston, MA: Thompson Course Technology PTR.

Mitgutsch, K. (2011). Serious Learning in Serious Games: Learning In, Through, and Beyond Serious Games. In M. Ma, A. Oikonomou, & L. C. Lain (Eds.), Serious Games and Edutainment Applications. London: Springer.

Nagarajan, A., Allbeck, J. M., Sood, A, & Janssen, T. L. (2012). Exploring Game Design for Cybersecurity Training. Paper presented at 2012 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, Bangkok. Doi: 10.1109/CYBER.2012.6392562

NOS. (2019). Vaker gijzelsoftware, 'betalen is goedkoper dan bedrijf stil laten liggen'. Retrieved on 2 March, 2020 from https://nos.nl/artikel/2307980-vaker-gijzelsoftware-betalen-is-goedkoper-dan-bedrijf-stil-laten-liggen.html.

Pearson, N. (2014). A larger problem: financial and reputational risks. Computer Fraud & Security, 4, 11-13.

Poulter, D. R., Chapman, P., Bibby, P. A., Clarke, D. D., & Crundall, D. (2008). An application of the theory of planned behaviour to truck driving behaviour and compliance with regulations. Accident Analysis and Prevention, 40, 2058-2064.

Rossano, V., Roselli, T., & Calvano, G. (2018). A Serious Game to Promote Environmental Attitude. In V. L. Uskov, R. J. Howlett, & L. C. Jain (Eds.), Smart Education and e-Learning 2017. New York, NY: Springer.

Saini, H., Rao, Y. S., & Panda, T. S. (2012). Cyber-Crimes and their Impacts: A Review. International Journal of Engineering Research and Applications, 2, p. 202-209.

Schakel, L., Veldhuijzen, D. S., Manai, M., van Beugen, S., van der Vaart, R., van Middendorp, H., & Evers, A. W. M. (2019). Optimizing healthy food preferences by serious gaming. Psychology & Health, p. 1-20.

Sitzmann, T. (2011). Meta-analytic examination of the instructional. Personnel Psychology, 64, 489–528.

Sullivan, D. T., Colbert E. J. M., Hoffman, B. E., & Kott, A. (2018). Best Practices for Designing and Conducting Cyber-Physical-System War Games. Journal of Information Warfar, 17(3), 92-105.

Thomas, R., Cahill, J., & Santilli, L. (1997). Using an Interactive Computer Game to Increase Skills and Self-Efficacy Regarding Safer Sex Negotiation: Field Test Results. Health Education & Behavior, 24(1), 71-86.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? Computers in Human Behaviour, 84, 375-382.

ZDNet. (2020). Most common cyber attacks we'll see in 2020, and how to defend against them. Retrieved on 22 April, 2020 from https://www.zdnet.com/article/most-common-cyberattacks-well-see-in-2020-and-how-to-defend-against-them/

Appendix A: Differences between the games

Game elements	**The Terminal**	**The United Nations**
Conditions	Experimental condition	Comprises two control conditions. The first one is the regular United Nations game. The second one is the United Nations game with information on cyber security from the Terminal presented to the participants at the beginning of the game.
Strategic game	The terminal is a strategic game.	The United Nations is a strategic game.
Metaphor	One airport, of which the teams all represent one of the six gates.	One country, of which the states all represent one of the six states.
Structure	The game consists of three rounds: In round 1, teams will create a logo and motto for their gate. They will also develop a strategy. In rounds 2 and 3, they will buy assets for their gates, and solve cyber security incidents.	The game consists of three rounds: In round 1, teams will create a flag and motto for their state. They will also develop a strategy. In rounds 2 and 3, they will buy assets for their states, and solve cooperative incidents.
Goal	Collecting as many smileys as possible, representing happy travellers.	Collecting as many smileys as possible, representing happy inhabitants.
Smileys and assets	Smileys are portrayed on the assets in the game. They can	Smileys are portrayed on the assets in the game. They can

	also be earned by successfully completing cyber security incidents.	also be earned by successfully completing cooperative incidents.
Currency	The players will receive a budget of 30 million euros.	The players will receive a budget of 30 million euros.
Cases	A total of four cases are integrated in the game. These cases are on the topics of phishing, password strength, computer updates, and malicious USB devices.	A total of four cases are integrated in the game. These cases are on the topics of neighbouring states who ask for support during a military conflict, neighbouring states wanting to borrow money, or neighbouring states who want to cooperate in building assets collaboratively. One case is not related to the topic of cooperation.
Evaluation	After some of the incidents, participants are asked why they have made a certain decision, to reflect back on their choices.	After some of the incidents, participants are asked why they have made a certain decision, to reflect back on their choices.

Table 5: Differences between the games

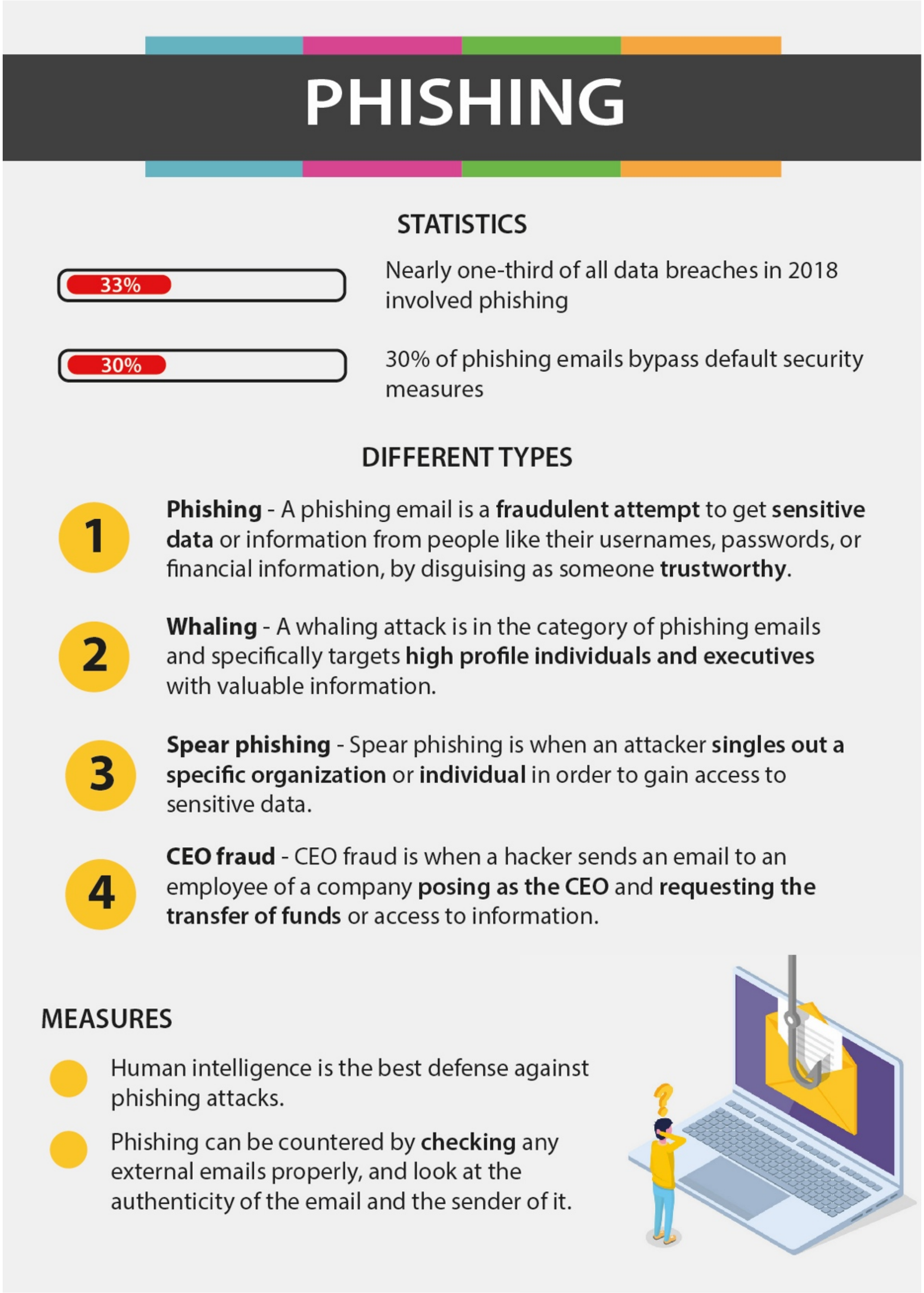
Appendix B: Implementation of the TPB

Theory of Planned Behaviour Element	**Implementation Terminal**	**Implementation United Nations**
Attitude	• Fun aspects in the game are expected to lead to a more positive attitude towards cyber security, given the fun experience surrounding it. • The smiley system implemented provides a positive experience surrounding rewards on cyber security behaviour.	• Fun aspects in the game are expected to lead to a more positive attitude towards cooperation behaviour, given the fun experience surrounding it. • The smiley system implemented provides a positive experience surrounding rewards on cooperation behaviour.
Perceived behavioural control	• The cases implemented in the game provide realistic cyber security scenarios through which the players will enhance their perceived behavioural control, by practicing with realistic events. • Through the information provided in the informational videos, they will get hands-on knowledge on how to recognise cyber threats and what to do against them.	• The cases implemented in the game provide metaphoric cooperative scenarios through which the players will enhance their perceived behavioural control, by practicing with realistic events. • Through the information provided in the information videos, they will receive some information on the benefits of cooperation.
Subjective norms	• By participating in a competition and upon finding out that more cyber secure behaviour will make them more likely to win the game, the players will experience social pressure to perform cyber secure behaviour.	• By participating in a competition and upon finding out that cooperative behaviour will make them more likely to win the game, the players will experience social pressure to perform cooperative behaviour.
Intentions	• The players have to come up with a strategy for playing this game.	• The players have to come up with a strategy for playing this game.

	They can e.g. decide to focus most on security, and later on divide their budget. This way, they will have to express their intentions to focusing on cyber security throughout the game.	They can e.g. decide to focus most on tourism, and later on divide their budget. This way, they will have to express their intentions on categories of assets throughout the game. This does not provide for intentions on cooperation.
Behaviour	• By buying cyber security assets, the players can perform cyber secure behaviour. • By solving the cases, the players are stimulated to perform cyber security behaviour.	• By helping other states, the players can perform cooperative behaviour and find out about the benefits.

Table 6: Implementation of TPB

Appendix C: Information posters United Nations Game



PHISHING

STATISTICS

33% — Nearly one-third of all data breaches in 2018 involved phishing

30% — 30% of phishing emails bypass default security measures

DIFFERENT TYPES

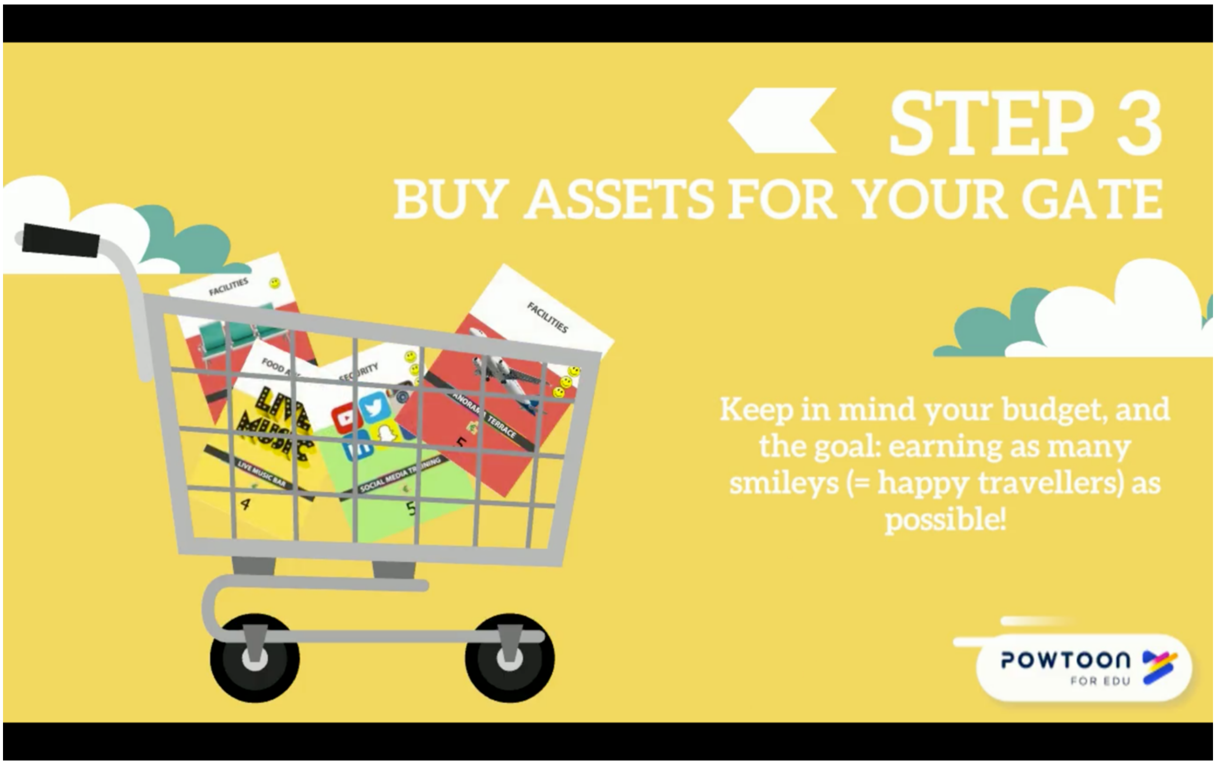
1. **Phishing** - A phishing email is a **fraudulent attempt** to get **sensitive data** or information from people like their usernames, passwords, or financial information, by disguising as someone **trustworthy**.
2. **Whaling** - A whaling attack is in the category of phishing emails and specifically targets **high profile individuals and executives** with valuable information.
3. **Spear phishing** - Spear phishing is when an attacker **singles out a specific organization** or **individual** in order to gain access to sensitive data.
4. **CEO fraud** - CEO fraud is when a hacker sends an email to an employee of a company **posing as the CEO** and **requesting the transfer of funds** or access to information.

MEASURES

- Human intelligence is the best defense against phishing attacks.
- Phishing can be countered by **checking** any external emails properly, and look at the authenticity of the email and the sender of it.

Figure 11: Information poster phishing

Appendix D: Introduction videos

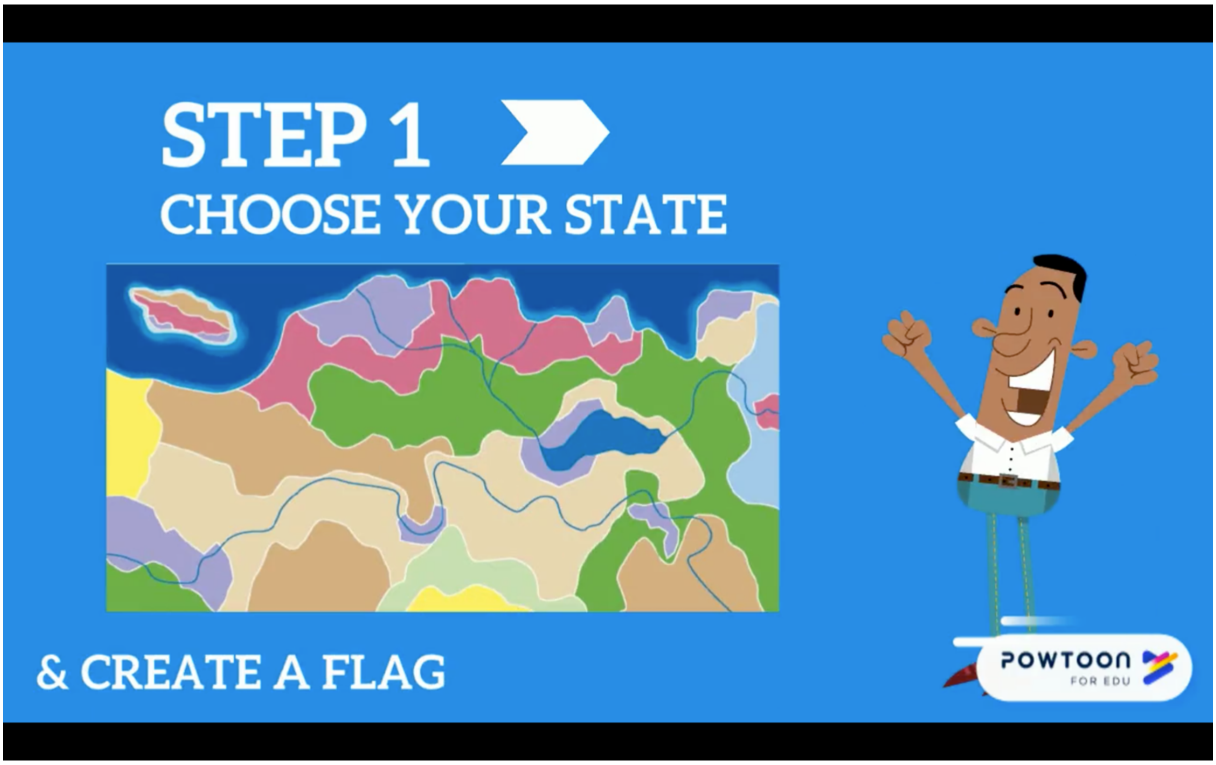


STEP 3

BUY ASSETS FOR YOUR GATE

Keep in mind your budget, and the goal: earning as many smileys (= happy travellers) as possible!

Figure 12: Screenshot from introduction video the Terminal



STEP 1

CHOOSE YOUR STATE

& CREATE A FLAG

Figure 13: Screenshot from introduction video the United Nations game

Appendix E: Playing fields

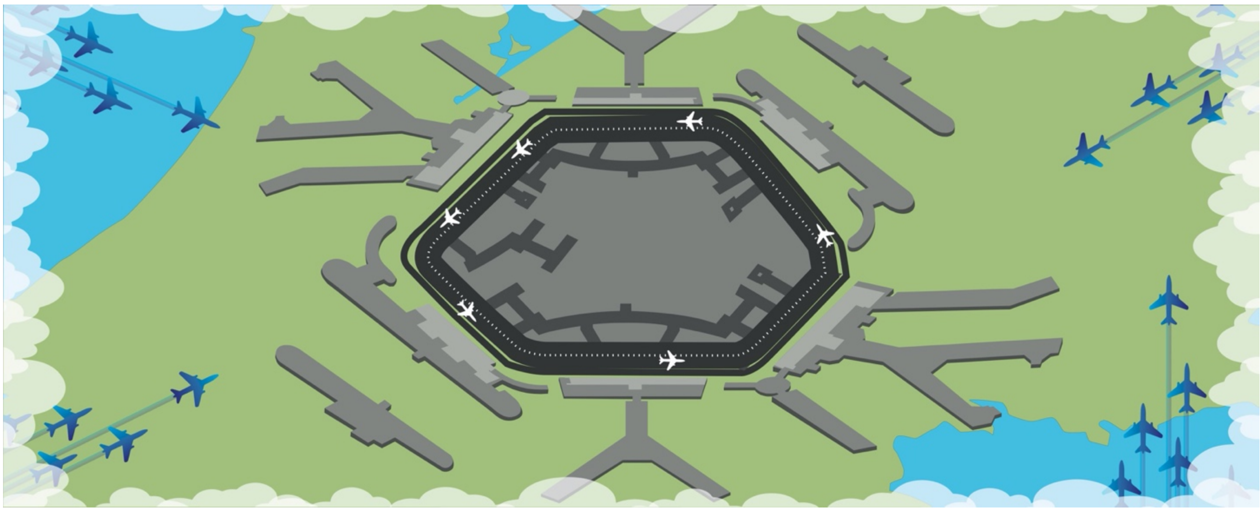


Figure 14: Playing field The Terminal

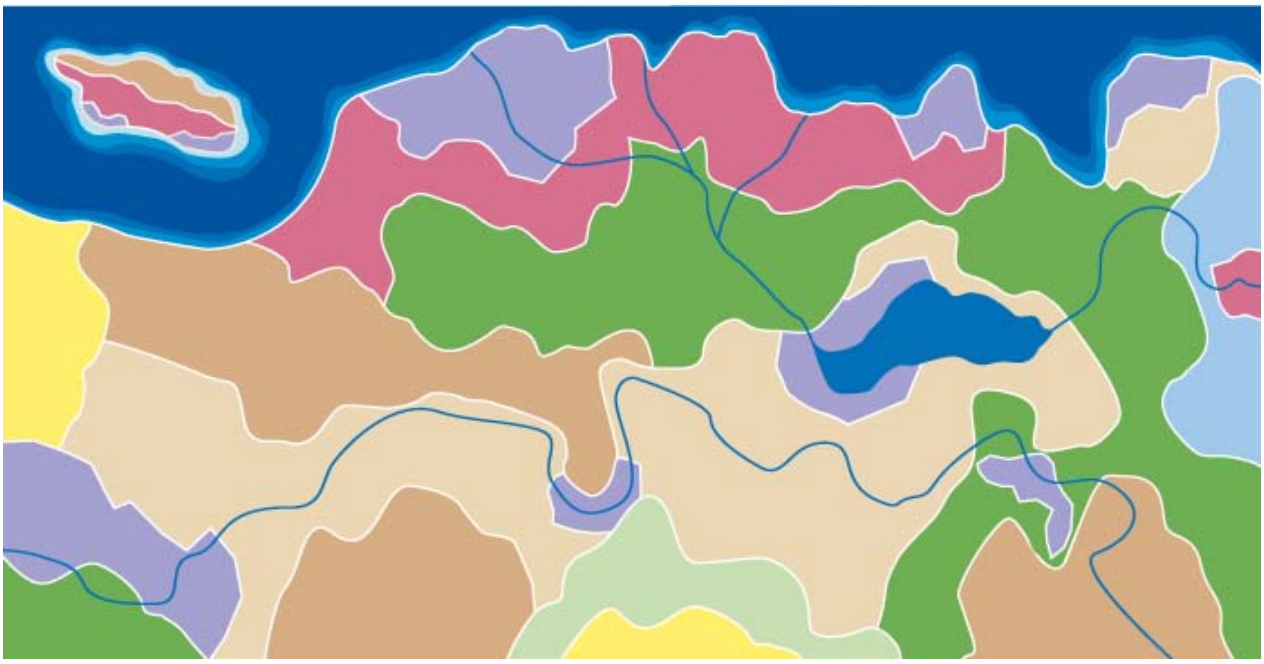
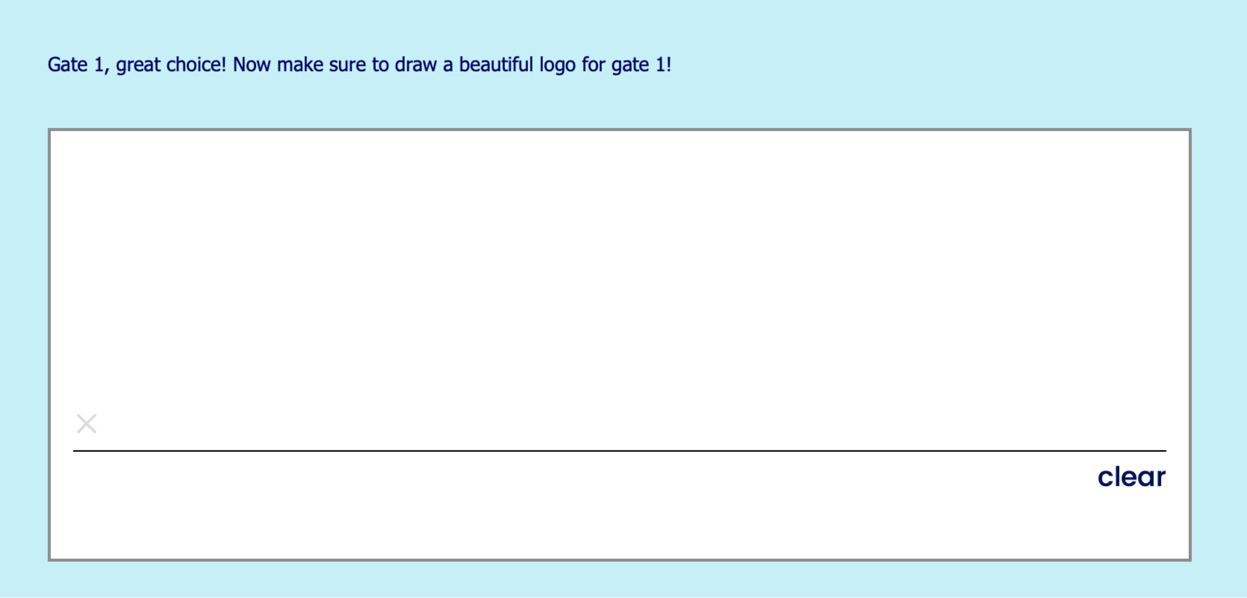


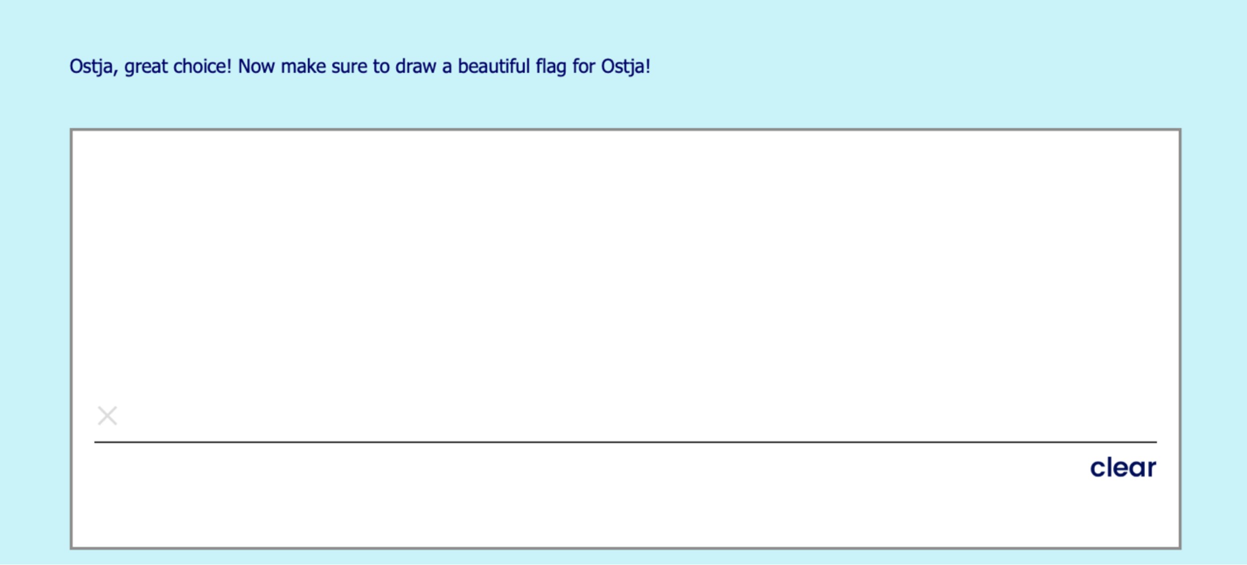
Figure 15: Playing field The United Nations.

Appendix F: Creating a logo or flag



Gate 1, great choice! Now make sure to draw a beautiful logo for gate 1!

Figure 16: Drawing box for a logo the Terminal



Ostja, great choice! Now make sure to draw a beautiful flag for Ostja!

Figure 17: Drawing box for a flag the United Nations

Appendix G: Assets playing cards

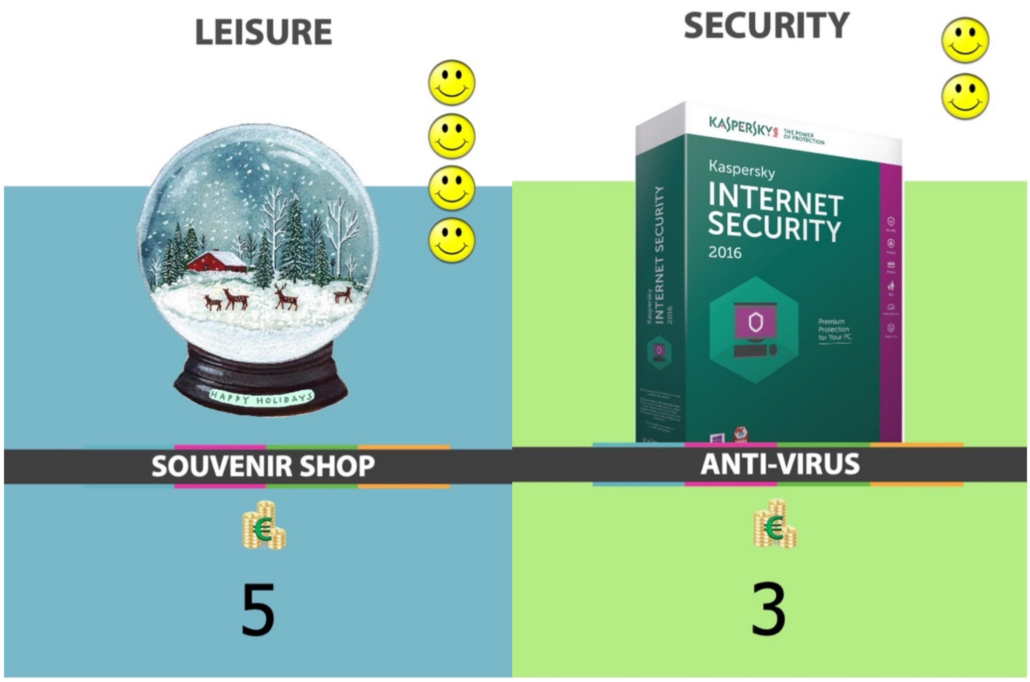


Figure 18: Selection of assets from The Terminal

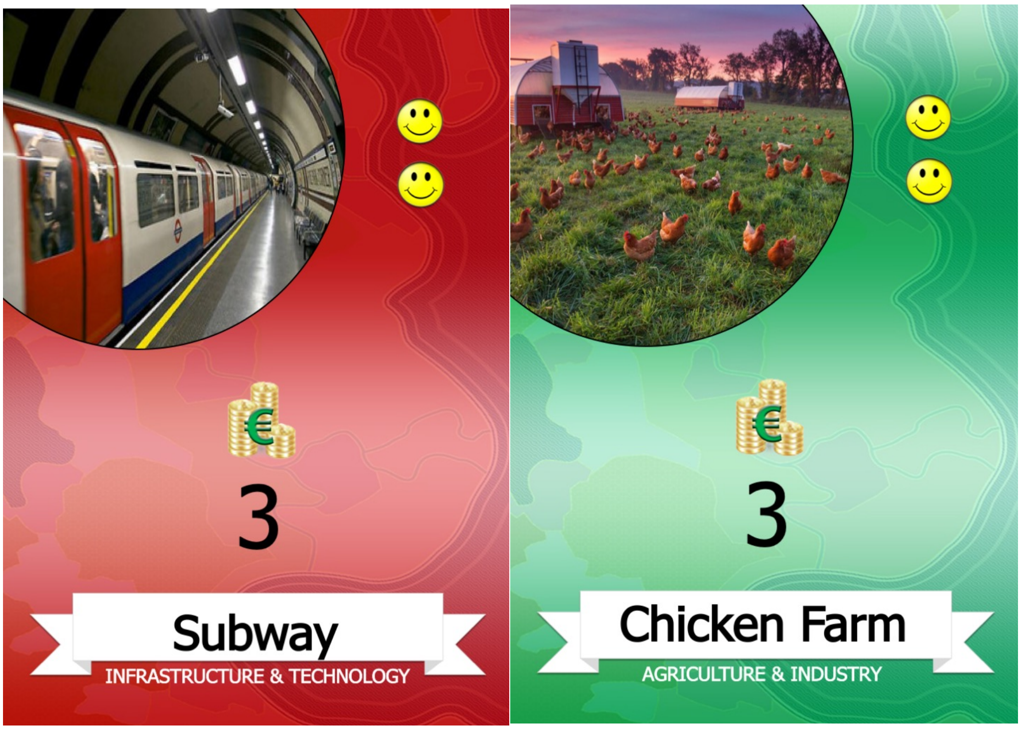
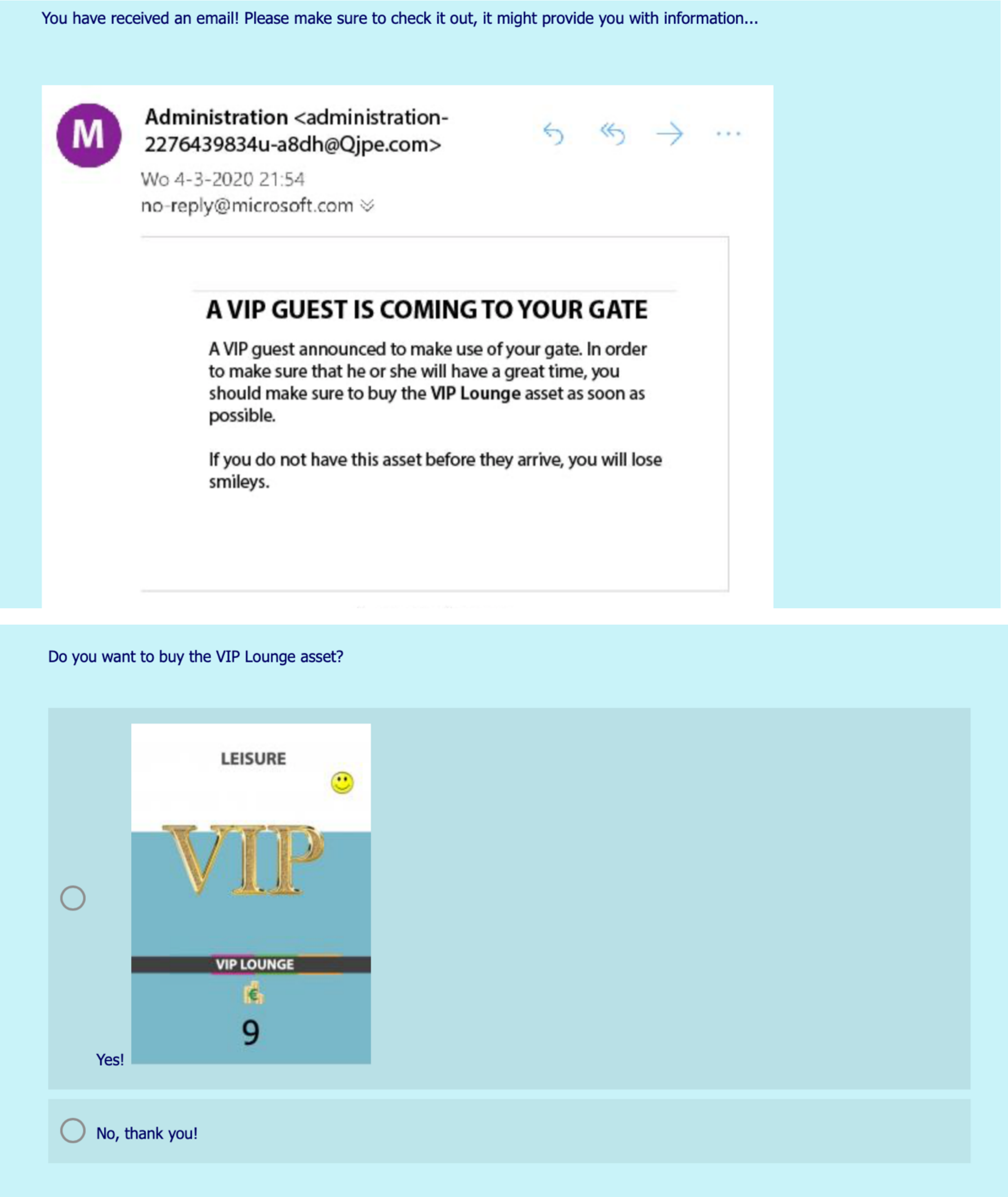


Figure 19: Selection of assets from The United Nations

Appendix H: Incidents



You have received an email! Please make sure to check it out, it might provide you with information...

Administration <administration-2276439834u-a8dh@Qjpe.com>
Wo 4-3-2020 21:54
no-reply@microsoft.com

A VIP GUEST IS COMING TO YOUR GATE

A VIP guest announced to make use of your gate. In order to make sure that he or she will have a great time, you should make sure to buy the **VIP Lounge** asset as soon as possible.

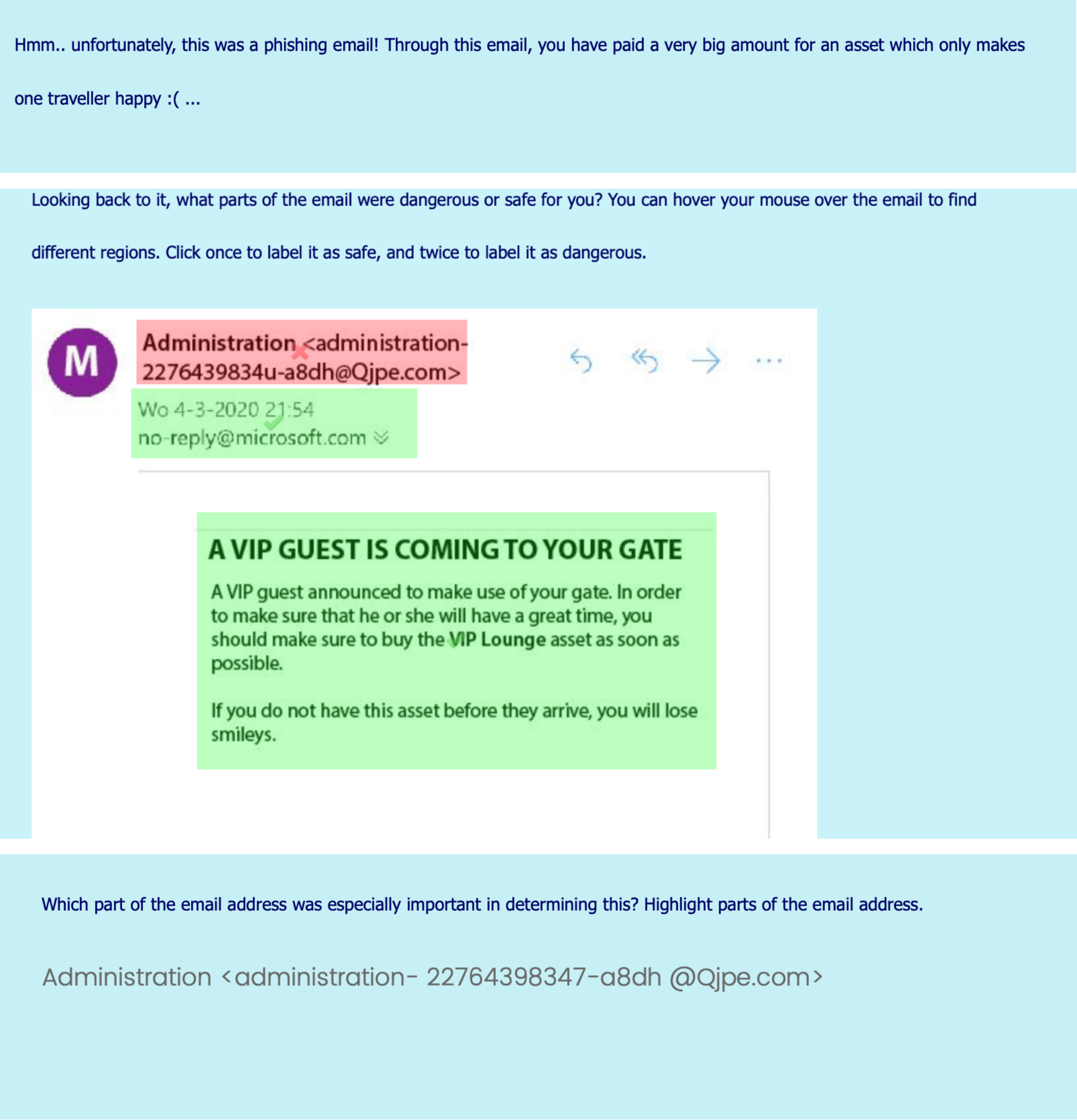
If you do not have this asset before they arrive, you will lose smileys.

Do you want to buy the VIP Lounge asset?

○ Yes!

○ No, thank you!

Figure 20: Example of an incident the Terminal



Hmm.. unfortunately, this was a phishing email! Through this email, you have paid a very big amount for an asset which only makes one traveller happy :(...

Looking back to it, what parts of the email were dangerous or safe for you? You can hover your mouse over the email to find different regions. Click once to label it as safe, and twice to label it as dangerous.

Administration <administration-2276439834u-a8dh@Qjpe.com>

Wo 4-3-2020 21:54
no-reply@microsoft.com

A VIP GUEST IS COMING TO YOUR GATE

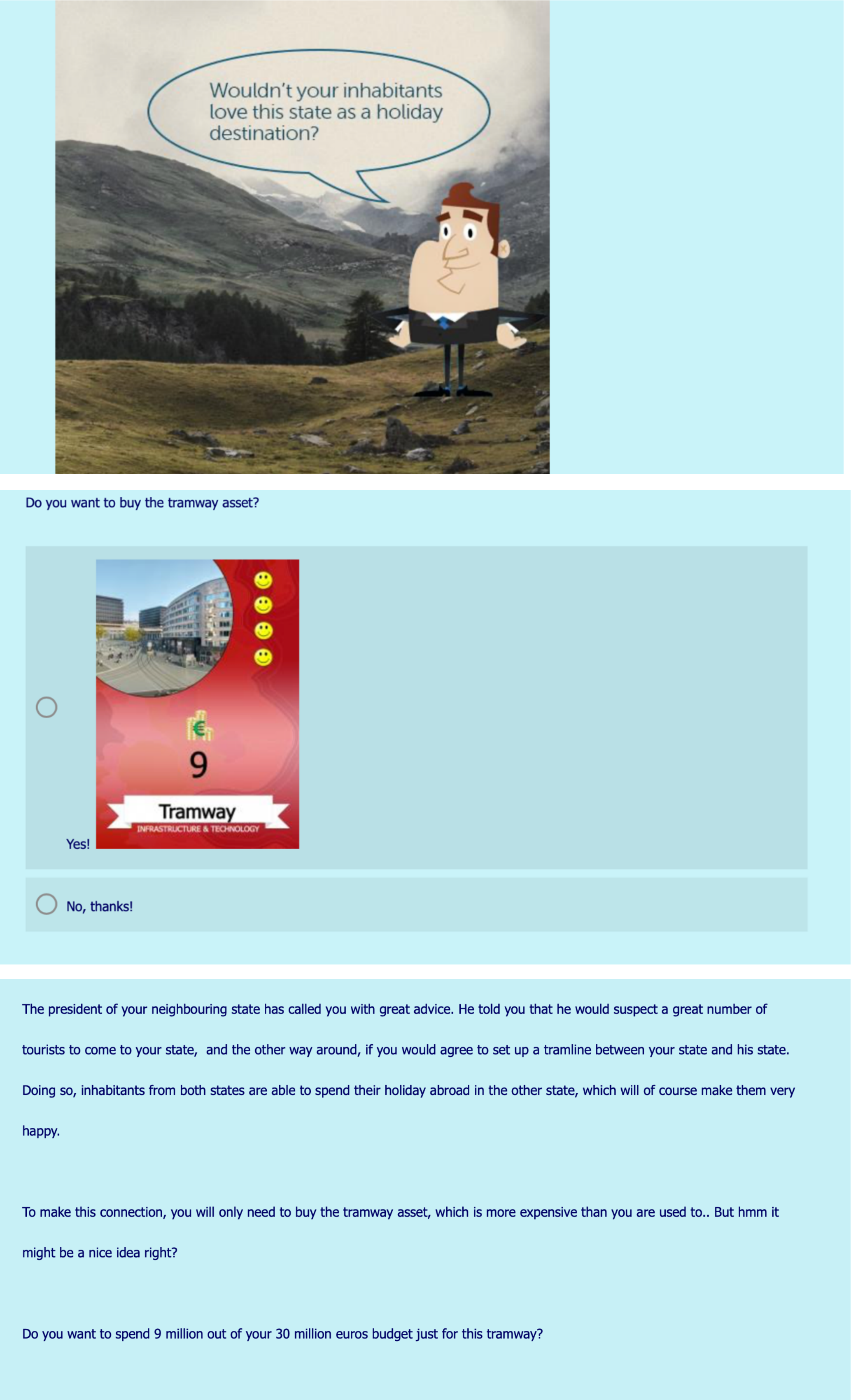
A VIP guest announced to make use of your gate. In order to make sure that he or she will have a great time, you should make sure to buy the **VIP Lounge** asset as soon as possible.

If you do not have this asset before they arrive, you will lose smileys.

Which part of the email address was especially important in determining this? Highlight parts of the email address.

Administration <administration- 22764398347-a8dh @Qjpe.com>

Figure 21: Example of a partly filled in reflection after an incident in the Terminal.



Wouldn't your inhabitants love this state as a holiday destination?
9
Tramway
INFRASTRUCTURE & TECHNOLOGY

Do you want to buy the tramway asset?

○ Yes!

○ No, thanks!

The president of your neighbouring state has called you with great advice. He told you that he would suspect a great number of tourists to come to your state, and the other way around, if you would agree to set up a tramline between your state and his state. Doing so, inhabitants from both states are able to spend their holiday abroad in the other state, which will of course make them very happy.

To make this connection, you will only need to buy the tramway asset, which is more expensive than you are used to.. But hmm it might be a nice idea right?

Do you want to spend 9 million out of your 30 million euros budget just for this tramway?

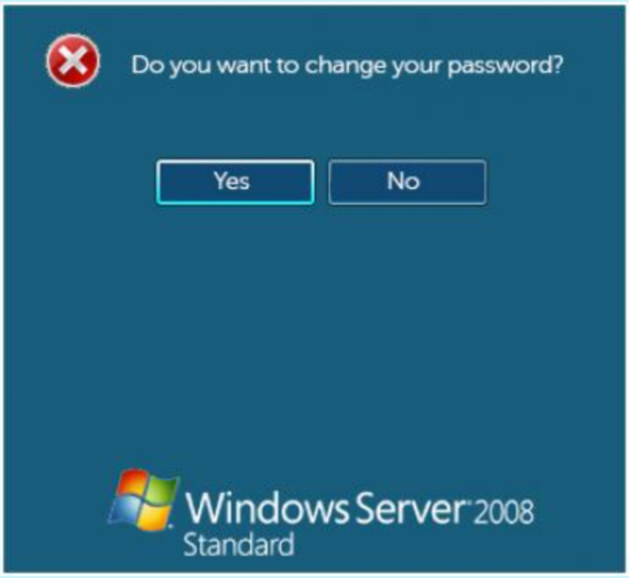
Figure 22: Example of an incident the United Nations game

You are given the option to change the password of the computer system of your gate! However, you can also always keep it this way.. It is up to you to assess whether it is needed.

The current password is the following:

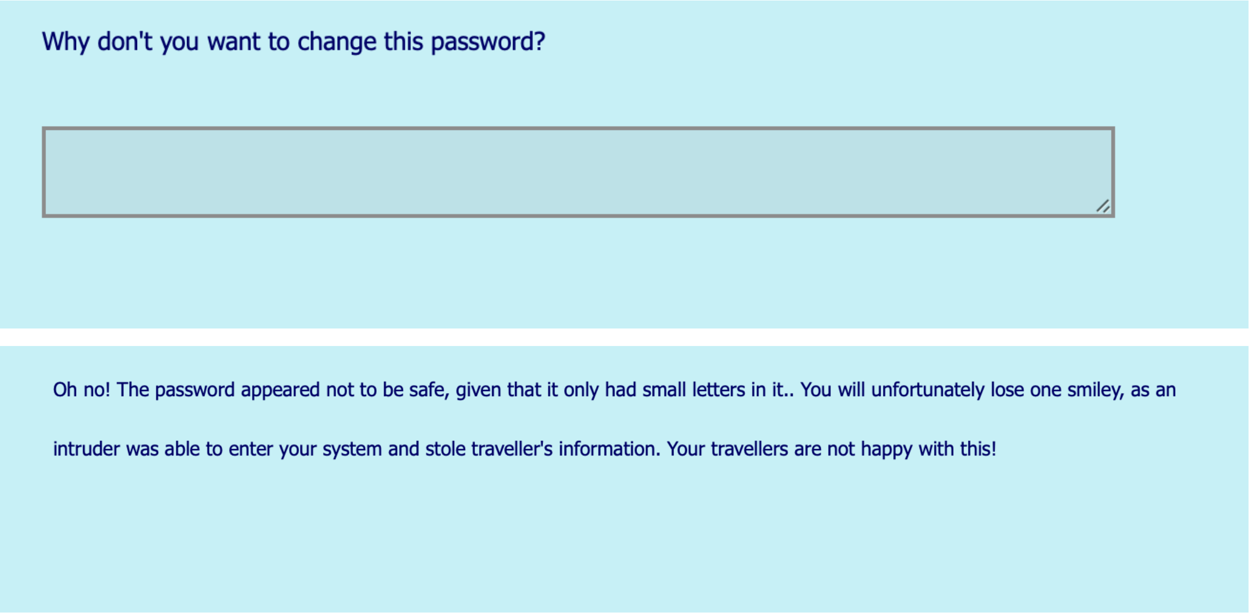
mygateisthebest

Do you want to change this password? Click on the right button.



Do you want to change your password?

Figure 23: Example of an incident the Terminal

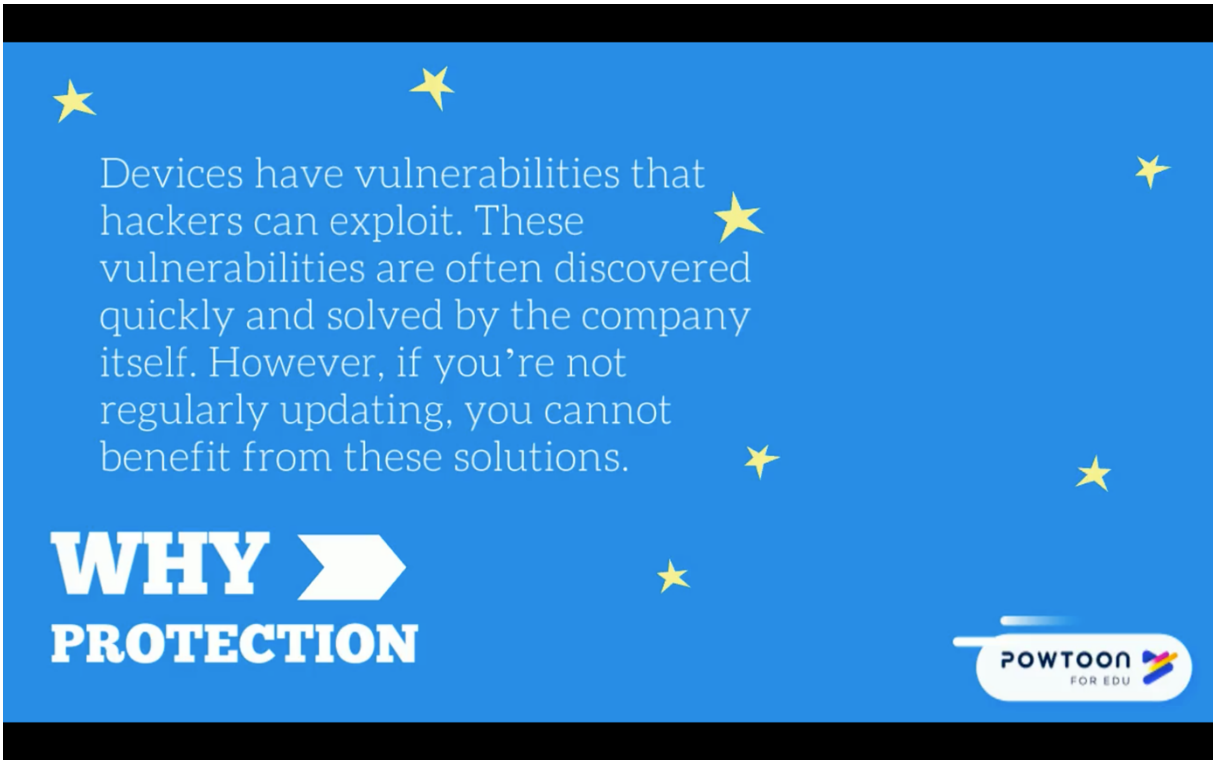


Why don't you want to change this password?

Oh no! The password appeared not to be safe, given that it only had small letters in it.. You will unfortunately lose one smiley, as an intruder was able to enter your system and stole traveller's information. Your travellers are not happy with this!

Figure 24: Example of a reflection after incident the Terminal

Appendix I: Information videos the Terminal

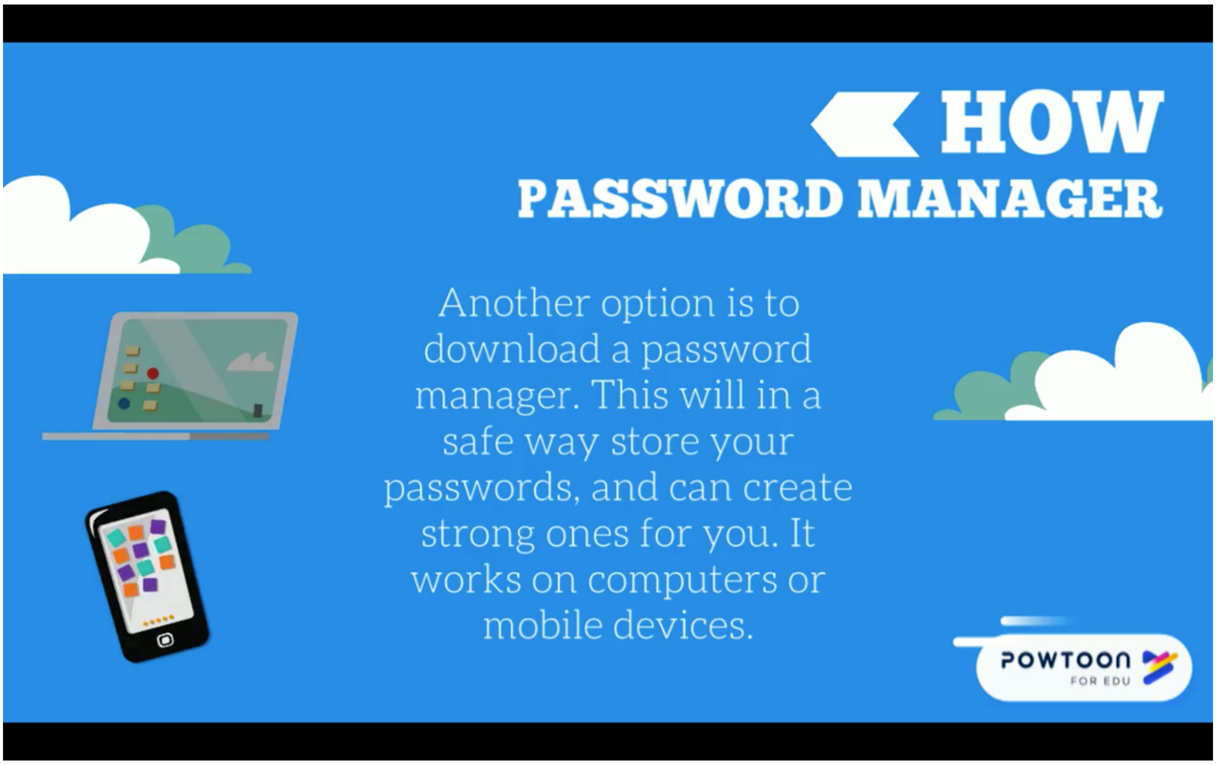


Devices have vulnerabilities that hackers can exploit. These vulnerabilities are often discovered quickly and solved by the company itself. However, if you're not regularly updating, you cannot benefit from these solutions.

WHY

PROTECTION

Figure 25: Information video screenshot



HOW

PASSWORD MANAGER

Another option is to download a password manager. This will in a safe way store your passwords, and can create strong ones for you. It works on computers or mobile devices.

Figure 26: Information video screenshot

Appendix J: TPB Questionnaire

This TPB questionnaire consists of 35 statements, to which participants can respond to according to a 7-Likert scale. 15 of these statements are concerned with cyber security behaviour. The other 20 statements are about work/study place behaviour, and are in place in order to not put too much emphasis on the cyber security statements. This will make the questionnaire more general, and may lead to less biases of participants feeling they need to focus on cyber security behaviour elaborately.

STATEMENT	Strongly Agree	Agree	Somewhat Agree	Neither Agree nor Disagree	Somewhat Disagree	Disagree	Strongly Disagree
My work/study environment allows me to work distraction-free when I need to.							
My work/study environment allows me to work distraction-free when I need to.							
I plan to always check received emails for potential phishing emails.							
It is important to be satisfied with the level of comfort at my physical work/study place.							
I find it easy to access the material resources I need to do my work properly (equipment, supplies, etc.).							
I do my best to perform cyber secure behaviour at all times.							
I intend to get most of my work done at the office/the university.							
Most people around me feel like my work/study							

environment reflects the organizational culture.							
Most people around me obey to the cyber security policy of my company/study programme at all times.							
I intend to lock my screen every time I leave my computer.							
I do my best to perform effective working behaviour at all times.							
I find it easy to ensure that I always comply with the cyber security policy.							
I intend to always develop strong passwords.							
I plan to always check my materials before starting working/studying.							
People around me feel comfortable in their work/study environments.							
I intend to always work distraction-free.							
Most people around me lock their screen at all times when leaving their computer.							
I always check an email for being a potential phishing email.							
It is important to at all times adhere to cyber security policies.							

I always help other people at my work/study place when they ask me to.							
People around me work together at their study/work place often.							
It is important to work together with colleagues/study peers.							
I find it easy to ensure that I never open any phishing emails.							
It is important to always update computers and software.							
I find it easy to ensure working together with other people when I want to.							
I always lock my screen when I leave my computer.							
My work/study environment allows me to work together with other people.							
I find it easy to perform effective behaviour at my study/workplace.							
Most people around me update their computers at all times.							
I plan to always be effective at my work/study place.							

I find it easy to ensure that I always scan my computer.							
I am satisfied with the level of comfort in my physical work/study place.							
My work/study environment allows me to help other people.							
I intend to always help colleagues/study peers with their work whenever they are in need of help.							
It is important to always use antivirus to scan computers.							
People around me always help colleagues/study peers with their work whenever they are in need of help.							

Table 7: TPB Questionnaire

Attitudes

Perceived behavioural control

Subjective norms

Intentions

Behaviour

Please note that before this questionnaire, some demographic questions are posed to the participants. These are the following:

1. What is your primary occupation at the moment?

a. I am employed

b. I am enrolled in a study programme

c. None of the above are applicable to me.

2. Where are you primarily working/studying?

a. At an office

b. At home

c. At a public space/library

d. Somewhere else: ….

4. Do you make use of a computer while working or studying?

a. Yes, always

b. Sometimes

c. No, never