# Serious games for cybersecurity

## Investigating the effectiveness of using a persuasive game to influence cybersecurity attitude and behavior

Joël Grevelink
ANR 584356

THESIS SUBMITTED IN PARTIAL FULFILMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN COMMUNICATION AND INFORMATION SCIENCES,
MASTER TRACK BUSINESS COMMUNICATION AND DIGITAL MEDIA,
AT THE FACULTY OF HUMANITIES
OF TILBURG UNIVERSITY

**SUPERVISOR**: Dr. Ir. P.H.M. Spronck
**SECOND READER**: Prof. Dr. E.J. Krahmer

**Tilburg University**
**Faculty of Humanities**
**Department of Communication and Information Sciences**
**Tilburg, the Netherlands**

**January 2015**

# Abstract

Empirical research on the use of serious games to influence cybersecurity attitude and behavior is scarce. The aim of this study is to find an answer to the question to what extent playing a persuasive game can influence attitude and behavior. It uses the game *ThreatBattle*, which employs a concept called "transreality" to incorporate actual real-world data in the virtual world of the game, in order to engage players.

A user study was performed in which two versions of *ThreatBattle* were used, one version with transreality elements and one version without. User attitudes were measured with scales from the Protection Motivation Theory (PMT), user behavior was measured by the STOP-index, and user engagement was measured with the Game Engagement Questionnaire (GEQ).

Analysis showed that participants rated the game below average on engagement. There were no main effects on engagement, but male participants considered the non-transreality version more engaging than the transreality version of the game. A trend was discovered which indicated an increase in self-efficacy after playing *ThreatBattle*. Several small significant effects were found, though none were significant for the participant group as a whole.

From the analysis we may draw the tentative conclusion that persuasive games can positively influence attitude and behavior, in particular as far as self-efficacy is concerned. Results vary based on gender and the results did not show a definite effect of the transreality element that is unique for *ThreatBattle*.

# Contents

# 1. Introduction

This thesis concerns research into the effectiveness of serious games for cybersecurity, and in particular, a serious game which encompasses the concept of "transreality". In this introduction, an attempt is made to define video games and the different types of videogames are explained (1.1). The distinction between games for entertainment and serious games is made clear and serious games are explained in more detail (1.2). After that, games for cybersecurity are introduced (1.3). The chapter then presents a problem statement and research questions (1.4). It concludes with an overview of the research methodology (1.5).

## 1.1 Defining videogames

Videogames are a popular pastime, and comparable to the movie industry in terms of revenues. An example of the success of video games is the success of Take Two's Grand Theft Auto 5, which has sold more than 34 million copies (Pereira, 2014). According to the NPD Group, a retail tracking service, in the year 2013 computer and video game sales in the United States amounted to a total of 15.4 billion dollars. This figure amounts to almost 160 million units of computer games sold (Siwek, 2014). There are many different genres of games that contribute to this figure. Of all these genres, action games such as shooters and sports games, and roleplaying games are the most popular.

As familiar as most people are with the term game, no comprehensive definition of the concept seems to exist. Furthermore, the definition of game is continually changing. For example, Sid Meier states that a game is a series of interesting decisions (Rollings & Morris, 2003). Bernard Suits defines games as "the voluntary attempt to overcome unnecessary obstacles" (Suits, Hurka, & Newfeld, 2014). A more complex definition of game is given by anthropologist Johan Huizinga in *Homo Ludens*, where Huizinga defines games as "…a free activity standing quite consciously outside ordinary life as being not serious, but at the same time absorbing the player intensely and utterly … according to fixed rules and in an orderly manner" (Huizinga, 1955). Although this definitional diversity is not necessarily a bad thing, many popular definitions can be considered too simple or too complex to describe videogames (Arjoranta, 2014). For the purpose of this thesis, we will use an extended version of the definition of game by Katie Salen and Eric Zimmerman, which strikes a balance between the simpler and more complex definitions mentioned above: "A game is a system in which players engage in artificial conflict, defined by rules, that results in a quantifiable outcome." (Salen & Zimmerman, 2004).

A videogame, then, is:

*"A system in which players engage in artificial conflict, defined by rules, that results in a quantifiable outcome and is played on a digital platform."*

Videogames can be divided into two groups, which are games for entertainment and serious games. Games for entertainment constitute the largest group and include those games that are developed

primarily for recreational use. The second category of games is serious games, and they will be described in the next section.

## 1.2 Serious games

Serious games are part of a long history of using games and play for teaching skills and abilities. According to Huizinga, play has a social and cultural function in society and is used to teach about serious subjects (Huizinga, 1955). Nevertheless, the notion of serious games is sometimes considered a paradox. On the one hand, this type of game is concerned with serious topics such as health issues, environmental issues and politics. On the other hand, we associate games and play with entertainment and leisure activities. Seriousness is not the direct opposite of play, however, and the two terms are not mutually exclusive.

One of the first definitions of serious games was proposed by Clark Abt in his book *Serious Games* (Abt, 1970). Abt states that serious games "have an explicit and carefully thought-out educational purpose and are not intended to be played primarily for amusement". This means that although serious games are designed for a specific goal that concerns the makers of the game, it does not exclude entertainment as outcome (Abt, 1970; Bogost, 2010).

Although nowadays many definitions of serious games exist, it was not until the Serious Games Initiative was founded in 2002, that the term "serious game" became widespread. The goals of this initiative were to utilize computer game designs and technologies for policy education, exploration and management tools. Since then, serious games have seen an increase in attention, and consequently, an increase in number of definitions as many scholars have tried to combine seriousness and game playing. David Michael and Sande Chen (2006) define serious games as "games that do not have entertainment, enjoyment, or fun as their primary purpose". Kevin Corti states that serious games are "all about leveraging the power of computer games to captivate and engage end-users for a specific purpose, such as to develop new knowledge and skills" (Corti, 2006). The definition of serious games that will be used in this thesis is one by Ian Bogost, who defines serious games as:

*"Games which have the intention of teaching the user something by immersing them in a constructed model"* (Murr, 2012).

Although serious games have seen an increase in popularity, there has not been an abundance of high quality empirical evidence on their effectiveness (Connolly, Boyle, MacArthur, Hainey, & Boyle, 2012). This research aims to contribute to the body of empirical research that is available on that very topic, by doing research into the effectiveness of a serious game for cybersecurity.

## 1.3 Games for cybersecurity

Cybersecurity is concerned with applying security measures to ensure confidentiality, integrity and availability of digital data that is either stored, sent or received. Security measures can range from

protection software to risk assessment or even awareness training, all of which aim to prevent security violations such as loss or theft of data, or damage to a system. According to research by the Dutch national cybersecurity center (NCSC), in 2013, the amount of security violations has increased exponentially compared to the year before. Almost 75% of these violations are trojans, which are harmful programs that disguise themselves as useful to trick users into installing them. They are often updated to circumvent modern protection software and contracted without the user's consent or active participation. As such, they are increasingly difficult to protect against. Most of these programs are aimed at desktop computers, but mobile platforms such as Android are increasingly the target of security violations (Nationaal Cyber Security Centrum, 2014).

Serious games are being used as a new type of prevention mechanism to combat these new and existing threats. They aim to achieve this by expanding cybersecurity awareness and increasing people's cybersecurity knowledge. Recent examples of serious cybersecurity games include *Agent Surefire* (MAVI Interactive LLC, 2014) and *CyberCIEGE* (The Center for Information Systems Security Studies and Research, 2014). These games have targeted business users, but there is an increasing need for creating cybersecurity awareness within the group of home users as well (Choo, 2011).

In order to increase cybersecurity awareness amongst home users, the Dutch government commissioned the development of a serious game. The result is *ThreatBattle*, a game that aims to increase cybersecurity awareness in order to prevent potential damage done by cybersecurity threats. The game is developed and built by a consortium of companies, including Sightes, Ranj Games and ThinkSharp. It uses a concept that the designers call "transreality", by which they mean that the game takes security elements from the player's real-life situation and incorporates them in the game. In the case of *ThreatBattle*, this means that the difficulty is based on the cybersecurity measures that the player has taken, and that the game searches for real-time attacks in the player's neighborhood to incorporate in the game.

Several forms of transreality gaming exist, including location based games, mixed reality games, augmented reality games and pervasive games. What these types of games have in common is that the virtual environments in these games are combined with game-related real-world experiences or information. The purpose of this combination is to make videogames more engaging. In order to achieve this, the combination of real and virtual environments and elements needs to be as seamless as possible.

As transreality is a fairly new concept, there are no comprehensive definitions readily available. For the purpose of this thesis, transreality in videogames is defined as:

*Actual real-world data, incorporated into virtual environments to make videogames more engaging.*

While the concept of transreality seems appealing, in actuality it has never been evaluated whether it makes a serious game more effective. What the influence of the transreality elements in *ThreatBattle* is on perceived engagement, and whether they make the game more effective in changing attitudes and behavior is the main research question of this thesis.

## 1.4 Problem statement and research questions

As stated in the previous section, this thesis is concerned with the effectiveness of serious games. It will do this by researching if and how serious games can influence attitudes and related behavior. Concretely, it does this by investigating the effect of playing the game *ThreatBattle* on attitudes towards cybersecurity and cybersecurity related behavior. Therefore, the following problem statement will be addressed:

*To what extent can playing a persuasive game influence attitude and behavior?*

To address this problem statement an experiment has been conducted in which the effect of playing *ThreatBattle* on cybersecurity awareness and behavior was measured. In particular, it explores whether the addition of transreality elements is of influence on the perceived engagement and the persuasiveness of the game. The three following research questions will be answered in this thesis:

1) *How do serious games persuade?*
2) *How can engagement, attitude towards cybersecurity and cybersecurity related behavior be measured?*
3) *What is the influence of ThreatBattle's transreality elements on engagement, attitude towards cybersecurity and cybersecurity related behavior?*

## 1.5 Research methodology

This thesis is made up of six parts. This first chapter featured an introduction to the research. It briefly explained what videogames are, continued with a definition of serious games and it introduced the game and the specific features that provided the motivation for this topic. In order to find answers to the research questions, we also need to establish what persuasive games are.

In chapter 2, the theoretical framework, we will elaborate on this topic with a literature review in which we determine how games can be used for persuasion, and what the different properties are that make persuasive games effective. Current literature on what makes games persuasive is reviewed, and we define and determine how to measure engagement. This section then provides an in-depth analysis of the components that contribute to the engagement factor of a (serious) game, and a description of the Game Engagement Questionnaire (GEQ) which will be used to measure engagement in our experiment. In addition, we research how to measure cybersecurity attitudes and behavior and the factors that determine one's attitude towards cybersecurity and cybersecurity related behavior are identified. These are then related to the Protection Motivation Theory (PMT), from which the different components will be used as a measurement of attitude in the survey.

After this literature review follows the experimental part of the thesis. In chapter 3 the research methodology is explained. The chapter begins with a description of the game *ThreatBattle*. Then the experimental design is explained and the materials used in the experiment are described. The overall experimental procedure is elaborated on and the different scales that are used to measure the constructs that were identified in chapter two are presented. Finally, the participant base and their demographic characteristics are described.

Chapter 4 contains the results obtained in the experiment in which data, collected by the game and by surveys, is tested for statistically significant effects. It compares the average scores on the PMT-components before and after playing the game between game versions. The influence of the results obtained by the components of the GEQ is presented, in addition to comparisons based on gender.

Chapter 5 features a discussion of the results. The actual implications of the results are discussed, including consideration of the limitations of this experiment. Recommendations, suggestions and improvements for future research are presented.

Finally, in chapter 6 we will provide answers to the research questions and problem statement. In this chapter the hypotheses that followed the theoretical framework are accepted or rejected.

# 2. Theoretical Framework

This section is centered on understanding the factors that determine serious games' effectiveness. We start with a background on serious games (2.1) and then continue by defining rhetoric, which is the framework of persuasion (2.2). After establishing this framework, previous research on how games persuade is analyzed and reviewed (2.3). From the theory of procedural rhetoric we propose that this principle is complemented by engagement as another requirement for successful persuasion and propose the Game Engagement Questionnaire as a measuring tool (2.4). In addition, we introduce the Protection Motivation Theory, which will be used to measure the underlying factors that determine protective cybersecurity behavior (2.5). We conclude with a presentation of our hypotheses based on this literature review (2.6).

## 2.1 Serious game background

Videogames have been around since the 1950's. At that time, videogames were only available for people and organizations with the technical knowledge required and access to expensive machines. For example, the game that is widely considered as the first videogame, "Tennis for Two" by William Higginbotham, was only playable in the laboratory that housed the computer the game was developed on. The same goes for the famous game "Spacewar!" that was developed in 1962 on the PDP-1 computer of the Massachusetts Institute of Technology, and only playable on that specific type of computer (Mäyrä, 2008).

In the following decades videogames became more and more accessible to the general public. Arcade halls emerged where people played games, and affordable consoles provided people the opportunity to play games in their own homes. Nowadays, almost every western household owns at least one computer or console that is used to play videogames. This widespread access and availability has resulted in a proliferation of games and game types (Mäyrä, 2008).

Until recently, video games were seen mainly as leisure activities. Within video game research the focus of attention seemed to be mostly on the relationship between games and negative qualities, such as aggressive behavior, violence and addiction (Connolly et al., 2012). As the medium matured more positive sides of video games were shown as well. Nowadays, researchers and teachers are starting to see the potential of serious games for training and for the acquisition of knowledge and skills, in addition to providing entertainment. Although the amount and diversity of games in this category is smaller than the former, serious games are receiving an increasing amount of attention.

Serious games have been applied in various areas, such as governance, politics, the military, healthcare and education. Although all serious games have a purpose, they can be designed with very different underlying goals. For example, serious games are often considered similar to games for learning, but the two terms are not interchangeable. All games for learning are serious games, but not all serious games are games for learning. Games for learning are games that are developed primarily for

learning goals, where entertainment value comes in second place. Most of these games are used to teach or train a highly specific skill. Many of these games are designed for children, but learning games for adults exist as well. Examples are games that are used to teach a language or mathematics, for increasing typing skill or for students of medicine to learn how to dissect a human body.

In addition to games for learning, serious games include advergames, simulation games, persuasive games, productivity games and games for health, among others. Advergames are games used for advertising, for example by product placement, in-game banners or traffic triggers. Simulation games are games that are used to simulate conditions or situations, such as in a driving simulator. Games for health are games that are used for therapy, rehabilitation or cognitive and emotional training and productivity games are used to increase productivity by rewarding real-world tasks. Finally, persuasive games, such as *ThreatBattle*, are used to teach a way of thinking. In the next sections we will define persuasive games and determine what elements make such a game persuasive.

## 2.2 Rhetoric

Persuasive communication envelops any message, of which the purpose is to change, shape or strengthen emotions, beliefs, perceptions, intentions and behavior (Miller, 2012). Building on this statement, persuasive games can be considered as conveyors of persuasive messages, for the purpose of affecting other people's responses. For this thesis, we will define persuasive games as digital games that *"aim to shape, reinforce or change the perceptions, emotions, beliefs, behavioral intentions and behaviors of players"* (De la Hera Conde-Pumpido, 2014)

Persuasive communication as a concept has been analyzed for over two millennia, dating back to ancient Greece (Bogost, 2010). The term used by scholars such as Aristotle and Plato was rhetoric, which consisted of the three complementing parts ethos, pathos and logos and focused on oral persuasion. Ethos is concerned with a person's morals, resulting in the trust of the person to be persuaded. Pathos uses emotional appeals to gain sympathy, and logos uses the spoken word to appeal on rationality. Rhetoric as a persuasion technique was later defined as "speech designed to persuade" by the Roman scholar Cicero (Burke, 1969). More recently, the introduction of mass media such as film and television led to redefinitions of the term rhetoric which included the possibility of techniques other than oratory, keeping it relevant for analysis of persuasion (Bogost, 2010).

For example, the definition of rhetoric has been elaborated on by rhetorician Kenneth Burke, who was one of the earliest to attribute persuasive properties to non-verbal messages. Although he defined rhetoric as "the use of words by human agents to form attitudes or induce actions in other human agents" (Burke, 1969), he argues that rhetoric facilitates human action in general. This is underlined by his statement that wherever persuasion is, there is rhetoric and vice versa (Burke, 1969).

The attribution of persuasive properties to non-verbal messages in turn led to increased interest in persuasion from other disciplines, which applied rhetoric to the visual image. For example, it provided

insight in how visual advertisements convey messages. Attention from other branches of science such as psychology led to a proliferation of persuasion theories, including elaboration likelihood (Petty & Cacioppo, 1986), cognitive dissonance (Miller, 2012), and transportation (Green & Brock, 2000). In the specific case of games, several factors have been identified that warranted further investigation of how they affected persuasion and a number of frameworks has been developed to explain how games convey meaning, and to analyze game rhetoric (Bogost, 2010; Ruggiero, 2012).

Still, after several decades of research on rhetoric, advertising and marketing, persuasion has proven to be a difficult-to-grasp and elaborate concept. It is dependent on many different factors that relate to each other, leading to cross-effects that are challenging to separate (O'Keefe, 2003). Some of the factors that are of influence are the medium used to convey the message, how much the message's topic interests the receiver, their gender, educational and cultural backgrounds, how much they know about the issue and whether they like the sender of the message or not. Each of these factors can determine the success or failure of a persuasion attempt (Lavender, 2011; Petty & Cacioppo, 1986)

## 2.3 Rhetoric in video games

When Ian Bogost published the first edition of his book *Persuasive Games* (2007), it contributed to the interest in academics as well as the game industry to investigate the way video games convey persuasive messages. In this book Bogost states that it is not their capacity to produce and show images, but the ability to operationalize rules that sets video games apart from other media as a persuasive medium. He sees video games as environments that open up new possibilities for persuasion by using procedures and rules to convey messages and persuade players (Bogost, 2010).

The term Bogost uses for the way games persuade is procedural rhetoric. It is a unique feature of video games, and stems from combining two concepts: procedurality and rhetoric. Procedurality is the way processes are created, explained and understood and rhetoric concerns the "methods, techniques and logics that drive the operation of systems" (Bogost, 2010). Procedural rhetoric, then, is "the art of persuasion through rule-based representations and interactions, rather than the spoken word, writing, images or moving pictures" (Bogost, 2010).

Procedural rhetoric as the primary persuasive property of video games is not without criticism, however. There has been some debate about its validity. Instead of claiming that a game's rules construct meaning, scholars such as Miguel Sicart argue that there are other processes at work, such as interactivity and balance. They complement procedural rhetoric by appropriating rules and creating a dialogue between a player and the game (Sicart, 2011). Instead of forcing players to exhibit certain behavior by limiting interactivity, Sicart argues that interactivity is of great importance because it improves the fun factor of video games.

In addition, a factor that a focus on procedurality alone tends to overlook is balance. Instead of a closed system approach resulting in predictable play, as would be preferred by proceduralism, a more

balanced approach keeps players interested in playing the game. The skill level of a player should be the main influence on success in a balanced game, and players who are more skilled should be more accomplished than less skilled players. However, both skilled and unskilled players should experience the right amount of challenge, which can be achieved by incorporating difficulty settings. When a game is predictable and unbalanced it lacks challenge and is therefore unable to make people want to play them (Sicart, 2011).

In conclusion, when games are not attractive for players, they are unable to convey persuasive arguments. In addition to procedural rhetoric, factors such as interactivity and balance are essential in increasing the persuasiveness of serious games. These factors should complement the procedural element of games to try and provide pleasurable experiences, in order to make the best use of the persuasive properties of games. By using rules embedded in a digital game, procedural rhetoric can certainly be a useful mechanism for persuasion. In video games, however, it is not the only mechanism that is of influence in attempts to convey persuasive messages. The next paragraph elaborates further on this topic, and introduces engagement as another important factor that is of influence in persuasive games.

## 2.4 Engagement

As described in the previous section, it is not their capacity to produce and show images, but the ability to operationalize rules that sets video games apart from other media. Prensky states that one of the reasons that serious games are effective is because in addition to learning something, they are engaging (Prensky, 2001). According to Janet Murray, we store events that happen in video games as personal experiences because of a game's transformative nature, by which she means their ability to create environments to role-play in (Murray, 1997). The tendency to store in-game events as personal experienes is especially present in young players, for whom the boundary between real and simulated experiences may become blurred over time (Blackmon & Terrell, 2007).

These effects of engagement are related to what Green & Brock (2000) call transportation. According to the theory of transportation, when players are absorbed in a game world, experiences in this game world can influence the player's beliefs in the real world (Green & Brock, 2000). When players are engaged in playing a game, they may be less aware of what happens in the real world, making it easier to assimilate values implied in the game's narrative. Taken together, these theories show that the more engaged players are in a game, the more likely they are to take the perspective that is represented by the game.

Empirical research on the relationship between game engagement and attitude is scarce, but there is some research available. One experiment let students control avatars based on themselves, but with the aesthetics of elderly people (Yee & Bailenson, 2006). In a digital classroom they tested the students' attitudes towards elderly people, and saw a decrease in stereotyping and increases in empathy

towards elderly people with similar traits to those of the avatars. In another experiment, students who played a computer math game developed more positive attitudes towards math learning (Ke, 2008).

Combining these theories and empirical results, the present study will measure engagement in our experiment for possible mediating effects on the effectiveness of the serious game. To be able to measure the level of engagement, we propose to use the Game Engagement Questionnaire (GEQ), developed by Brockmyer et al. (2009). Its original purpose was to develop a measurement instrument for typical psychological engagement levels for players of violent video games, based on the assumption that deeper levels of engagement can lead to larger impact of game playing. The authors analyzed the responses on the questionnaire in an experiment, in addition to the relationship to other questionnaires. These analyses provided preliminary indications that their questionnaire is both reliable and valid as a measurement tool of engagement. In addition, they found preliminary evidence for a hierarchy in the different measures of engagement in game-playing, which breaks down engagement into four components: Immersion, presence, flow and absorption (Brockmyer et al., 2009).

Immersion is the first and hierarchically lowest level of engagement. The term immersion describes what people experience when they become engaged in the gameplay of a game, while a sense of awareness of the player's real-world environment remains (Baños et al., 2004). Part of the concept of immersion is the feeling that a player is present in the world of the game (Wirth et al., 2007). According to Murray (1997), immersion transports the player to a simulated environment. Through immersion the game world becomes enveloping, and takes over the player's perception (Murray, 1997). Part of the concept of immersion is that the player is actively contributing to making the game world appear more realistic.

The immersive quality of games also appears in non-digital versions. According to Abt (1970), the representation of the real world in a game is capable of conveying knowledge of the real world. He illustrates this by stating that acting in a Shakespeare play results in a deeper impression than a teacher's reading would. Coleman (1971) states that "persons do not learn by being taught; they learn by experiencing the consequences of their actions". Games are an improvement to traditional methods of teaching, because they actively involve students in the experience of learning by presenting real-world information in more engaging ways.

The second level of engagement is presence. Brockmyer et al. (2009) have found that presence entails being in one's normal state of consciousness, but feeling as if present in the world of the game. In this it builds on immersion, the difference being that players are less aware of their environments. According to Wirth (2007), presence involves the experience of being integrated in the world of the game. Presence has the potential to be of influence on a player's attitude because scripts or mental models that a player develops in-game may be referred to in similar situations in real-life (Tamborini & Skalski, 2006).

The third level of engagement is flow. Players experience flow when they are compelled by the game and find themselves in an energized state of focus and concentration, through which they

subconsciously assimilate values and facts (Quinn, 2005). The term flow is used to refer to pleasurable feelings from being in control and one with an activity that is the result of achieving a balance between skill and challenge while performing a rewarding task (Csikszentmihalyi, 1999). To achieve this, it is important that the difficulty of the game increases with the skill of a player, finding a balance between boredom and frustration.

Flow often leads to the distortion of time, but it also seems to enhance learning. Amory, for example, states that knowledge is assimilated through processes emerging from flow (Amory, 2007). On simulations, Herz notes that convincing people that certain behavior is appropriate is possible because once players enter a virtual environment, they automatically accept that someone other than themselves has set the parameters (Herz, 1997).

The last level of engagement discerned in the Game Engagement Questionnaire is absorption. This is considered the deepest form of engagement. Absorption is used to describe total engagement in the present experience (Irwin, 1999). When one experiences absorption, there is "a separation of thoughts, feelings, and experiences and affect is less accessible to consciousness" (Brockmyer et al., 2009). The difference between flow and absorption can be explained by type of affect and motivation. Absorption is more concerned with negative affect, and instead of intrinsic motivation, peer competition is often the most prominent motivational factor.

These four levels of engagement, in addition to procedural rhetoric, all contribute to the persuasiveness of video games. They shape, reinforce or change the perceptions, emotions, beliefs, behavioral intentions and behaviors of players (De la Hera Conde-Pumpido, 2014) by blurring the boundary between what is virtual and real so that players appropriate the values and logic of the game as their own. For this to happen, games need to be balanced, interesting and realistic (Lavender, 2008).

## 2.5 Cybersecurity and the Protection Motivation Theory (PMT)

This study aims to determine the effectiveness of serious games in influencing cybersecurity attitude and behavior. Most previous work on behavior change and serious games has been conducted in the field of healthcare, with several studies showing the positive effects of playing serious games on exhibiting healthy behavior (Baranowski, Buday, Thompson, & Baranowski, 2008). Consequently, a large amount of the models used to measure attitude and behavior in these studies is healthcare based as well. Although originally developed from a healthcare point of view, they are increasingly being used in other domains. Cybersecurity is one of these domains (Ng, Kankanhalli, & Xu, 2009), and in line with this development we propose to use the Protection Motivation Theory (PMT) as a measurement for cybersecurity attitude. This particular model has been validated for use in cybersecurity research in a previous study on the effectiveness of serious games for cybersecurity awareness (Van der Linden, 2014).

The Protection Motivation Theory was developed by Rogers (1975). Its original purpose was to provide an understanding of the workings of fear appeals. Later on this theory has been completely reworked (Maddux & Rogers, 1983) into a theory of persuasive communication. It describes adaptive and maladaptive techniques of coping with threats to one's health.

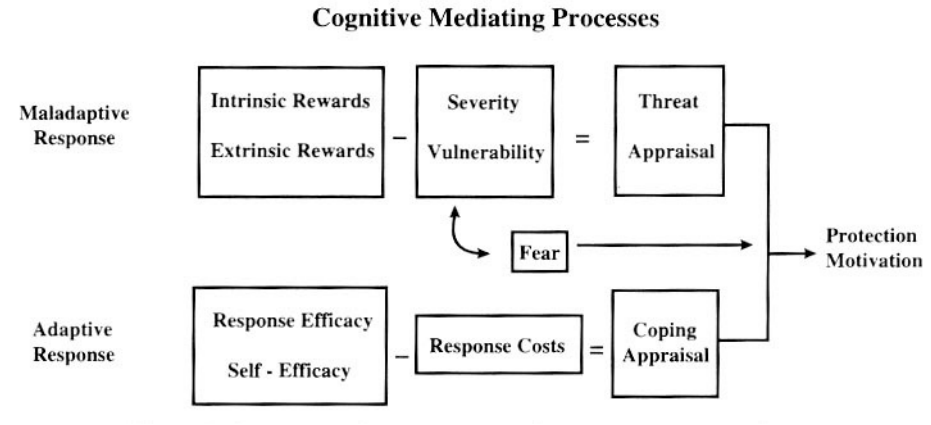


*Figure 1: PMT Framework. Reprinted from Floyd et al. (2000)*

As shown in Figure 1, the determination to demonstrate protective behavior is the result of a combination of four factors, combined with response costs or rewards from performing unhealthy behavior. The four factors are (1) the perceived severity of a threat, (2) the perceived vulnerability to a threat, (3) the efficacy of the recommended protective response and (4) a person's perceived self-efficacy. These four factors are part of two coping appraisal processes, which are (1) threat appraisal and (2) coping appraisal. They evaluate behavioral responses to deal with the perceived threat and these appraisal processes in turn lead to protection motivation, which is the mediating variable that should lead to protective behavior. A person can also perform a maladaptive response when response costs or rewards from performing bad behavior are too high. Maladaptive responses can lead to negative behavior or absence of positive behavior, which can have potentially negative consequences and place an individual at risk (Van der Linden, 2014).

The four factors described above can also be interpreted from a cybersecurity point of view. The first factor, perceived vulnerability, has originally been defined as an estimation of the possibility of contracting a disease (Boer & Seydel, 1996). When applied to cybersecurity, it is a person's estimation of the possibility of a security violation to occur. A security violation in this context can be, for example, a virus, spyware or malware infection, firewall breach, hacking attempt or privacy violation (Van der Linden, 2014).

The original definition of perceived severity is an estimation of the severity of consequences of a particular health threat (Boer & Seydel, 1996). When applied to cybersecurity, this component can be described as a person's estimation of the severity of consequences of a security violation. A person can,

for example, believe that a malware infection is relatively harmless, while a hacking attempt is a big problem or vice versa (Van der Linden, 2014).

The third factor influencing protection motivation is response efficacy. In the original use of the model it is described as one's perception of how effective a recommended response to a perceived health threat is (Boer & Seydel, 1996). From a cybersecurity perspective, it is one's perception of how effective a recommended security measure is in preventing a security violation. In this context a security measure can be, for instance, installing and updating anti-virus software, scanning a system for malware, installing a firewall or checking sources for downloads (Van der Linden, 2014).

The fourth factor, self-efficacy, was originally defined as to what extent one believes to be able to successfully perform the recommended response measure to a perceived health threat (Boer & Seydel, 1996). To apply self-efficacy in a cybersecurity model, it needs to be defined as the belief in one's ability to successfully apply recommended security measures to prevent a security violation (Van der Linden, 2014).

Based on these four factors, Van der Linden (2014) developed a questionnaire to measure one's cybersecurity awareness. This questionnaire was then used in a study into the effectiveness of the serious game *Agent Surefire*. It found multiple significant effects in the different components, and was therefore considered a suitable measuring instrument for cybersecurity awareness (Van der Linden, 2014). In the current thesis, the same questionnaire was used to measure the effectiveness of the game *ThreatBattle*.

## 2.6 Hypotheses

With regards to the overall effectiveness of *ThreatBattle*, we expect that because of the procedural rhetoric in the game, participants score higher on measures of the PMT-components and behavior after playing *ThreatBattle*, regardless of the condition the participant is in.

*H1: All participants that played ThreatBattle score higher on the PMT-components, intention and behavior measures on the post-test than on the pre-test.*

With regards to the difference between the versions of *ThreatBattle* with and without transreality, we expect that the version with transreality will show higher increases on measures of the PMT-components, intention and behavior than the version without transreality elements.

*H2a: Participants that played the transreality version of ThreatBattle show higher increases than the non-transreality version between the pre-test and post-test on the PMT-components, intention and behavior.*

In addition, we expect that participants in the transreality condition will score higher on measures of engagement.

*H2b: Participants that played the transreality version of ThreatBattle show higher scores on engagement measures than those who played the non-transreality version.*

In the original research by Van der Linden (2014) a significant effect of gender on the protection motivation measures was found. For the present research, we expect this effect of gender to be present as well:

*H3: Male and female participants differ in changes in scores on the PMT-components, intention, behavior and overall engagement.*

# 3. Method

This chapter describes the experimental design that was used to set up and execute this research. First the serious game is described (3.1). After this the design of the experiment and the independent and dependent variables are explained (3.2). In the following sections, the details of the experimental procedure (3.3) and the materials (3.4) will be elaborated on. Finally, the composition of the participant group is described (3.5).

## 3.1 ThreatBattle

The game that was used in this experiment is *ThreatBattle*. It is a serious game commissioned by the Dutch government and developed and built by a consortium consisting of Sightes, Ranj Games and ThinkSharp. The goal of the game is to change people's cybersecurity attitudes and behavior. It aims to achieve this through increasing engagement by taking elements from the player's real-world situation and incorporating them in the reality constructed by the game. *ThreatBattle* is a tower defense game built in *Unity Web Player*, available for PC, iOS and Android.

Upon loading the game, players are asked to register an account with a username and password. They can then log in with this account. Once they are logged in, the game explains that you have to answer some questions to establish the cybersecurity status of your device. The better you are protected against cybersecurity threats, the easier it is to win the game. In the next screen are six questions about how secure your device is. The game will then determine if you have one, two or three paths to defend. In the next screen the game asks you if your operating system is up to date. If it is, this results in a small boost to how many hits you can withstand.

*Figure 2: Screenshots of security questions in ThreatBattle*

The game then searches for recent attacks on your system, in your neighborhood and in your city. It will give an overview of the threats that have been found, which you can click on for additional information.


*Figure 3: Screenshots of ThreatBattle searching and displaying recent attacks*

Pressing the start button will open the main game screen, showing your base and one to three lanes of attack with different spots where you can place defense mechanisms. Every threat that reaches your base takes some of its hit points off. Once your hit points reach zero, the game is over. The goal is to survive as long as possible, by buying scanners, vaults and firewalls with the money you get from destroying threats, and positioning them between the threats and your base. When the game is over, the player is presented a screen with their score and level of protection as compared to other players.


*Figure 4: Screenshots of ThreatBattle showing the main level, defense mechanisms and post-game screen*

## 3.2 Experimental design

The experiment is of a mixed design. The between subjects factors are game version (transreality versus no transreality) and gender (male versus female). The dependent variables are protection motivation (perceived severity, perceived vulnerability, response efficacy and self-efficacy), intention and behavior with respect to cybersecurity. The within-subjects factor is time, as the dependent variables were measured during a pre-test and post-test. In addition, engagement was measured as a dependent variable during the post-test only.

## 3.3 Procedure

Before the start of the experiment, participants were informed that they had to fill out an online survey, play the game *ThreatBattle* for a week and then fill out another survey. It was explained that the surveys are anonymous and permission was asked to use the data in an analysis. Participants were told that they were free to refrain from answering or terminate their participation at any time. It was explained that the

research involved a serious game for cybersecurity. No additional information about the experiment was given, as this might possibly influence the participants and the outcome of the experiment.

The first part of the experiment was conducted in one of the computer rooms in Tilburg University's Dante building. The computer room had space for a maximum of 18 participants at a time, and 4 total sessions were held over the course of 2 days. This first part, in which participants received instructions, filled in the first questionnaire and played the game for the first time, lasted an average of 30 minutes. In these 30 minutes all groups received instructions first, and then started by answering the pre-questionnaire that had been made available through a web link in Qualtrics. Participants then clicked a link to play one of the two versions (with or without transreality elements) of the game *ThreatBattle*, depending on their group number.

After the first play session, participants were asked to play the game a minimum of two times over the course of one week. After the week of gameplay, participants filled in the online post-questionnaire. This second part of the research took another average of 30 minutes.

For participants recruited via e-mail and social networking sites, the overall procedure was nearly the same. The difference is that these participants received the instructions by e-mail, played each game session from home and filled in both surveys from home as well.

## 3.4 Materials

Two versions of the game *ThreatBattle* were used. The first version was the original game as described previously. The second version was one without the transreality elements, meaning there was a fixed difficulty setting, no questions about the protection of the player's devices and no overview of the player's results. Originally, the idea was to collect data from every *ThreatBattle* play session. These data would be sent to a database automatically using an API, and would include username, platform, info clicks, number of play sessions and total time played. However, due to technical problems outside the experimenter's control, the data were incomplete and could not be used.

In addition to the game, two online surveys were used. The first survey contained questions about demographics, including username, gender, age and education. In addition, direct and indirect self-assessment were used to ascertain cybersecurity knowledge, computer game appreciation and the level of protection of participant's devices. Afterwards, cybersecurity attitude was measured. The first questionnaire can be found in Appendix I.

The second survey omitted demographic questions and questions about the appreciation of computer games, but the level of protection, cybersecurity knowledge and attitude were measured again. In addition, the second survey measured perceived engagement. The post-questionnaire can be found in Appendix II.

**Cybersecurity attitude.** To measure cybersecurity attitude, the questionnaire developed by Van der Linden (2014) which is based on the Protection Motivation Theory (PMT) (Maddux & Rogers,

1983) was used. Participants were asked to rate on a 5-point Likert scale (1 = “Strongly disagree”, 5 = “Strongly agree”) to what extent they agreed with statements concerning cybersecurity. Cronbach’s alpha was used to compute the internal consistencies of the subscales. To increase the internal consistency of the scales to acceptable levels, questions with low item-scale correlations were excluded from the created scales. This resulted in a scale which included all four items for perceived severity (pre $\alpha = .691$, post $\alpha = .715$) and after deletion, a scale of two items for perceived vulnerability (pre $\alpha = .594$, post $\alpha = .831$). Although this first value is below the value of .7 that is generally considered acceptable, when dealing with psychological constructs this can be expected and in preliminary research values above .6 or even .5 may suffice (Field, 2013). After excluding one item, three items were used to create a scale for response efficacy (pre $\alpha = .338$, post $\alpha = .688$). This pre-test $\alpha$ is, on its own, unacceptable. However, due to the post-test $\alpha$ close to .7 it was decided to group the three items into one scale. After this, all four items were used to create a scale for self-efficacy (pre $\alpha = .803$, post $\alpha = .794$). Lastly, one item was used to measure intention for future behavior. The original questionnaire had four items measuring intention, but as they were overall quite similar wordings of one statement, the additional were deemed redundant and not present in this research.

**Engagement.** Questions from the Game Engagement Questionnaire (GEQ) (Brockmyer et al., 2009) were used to measure the amount of engagement the participants experienced when playing the game *ThreatBattle*. Although in the original version these questions were yes or no questions, participants were asked to rate their experience on a 5-point Likert scale (1 = “Strongly disagree”, 5 = “Strongly agree”) to be able to compare between different gradations among the subscales of engagement. As the original authors stated, the groupings of the GEQ were preliminary, and required confirmation to be used as such (Brockmyer et al., 2009). Therefore Cronbach’s alpha was computed to determine the internal consistencies of the subscales. To increase internal consistencies of the scales to acceptable levels, questions with low item-scale correlations were excluded from the created scales. As in the original questionnaire, one item measured immersion. After excluding two items, the remaining two were used to create a scale for presence ($\alpha = .648$). Out of the original nine items, eight were used to create a scale for flow ($\alpha = .767$) and three out of the original five items were used to create a scale for absorption ($\alpha = .806$). An overall scale for engagement which included 17 out of 19 items ($\alpha = .891$) was created as well.

**Cybersecurity behavior.** To measure behavior, the State of Preparedness (STOP) index which was developed by the makers of *ThreatBattle* and deployed in the game to determine good cybersecurity behavior and the level of protection of a player’s devices, was incorporated in the surveys. These questions could be answered with either yes (1) or no (0). A scale for behavior was created by adding the values of the components for each participant. The result was an index ranging from 0 (low) to 7 (high).

## 3.5 Participants

A total of 61 people participated. Of these, 46 completed the experiment. The mean age of the participants was 22.5 years (*SD* = 6.45). Of these participants 52 percent was male and 48 percent female. The average age of the male participants was 24.2 years and the average age of the female participants 21.1 years. A large part of these participants consisted of students recruited from the test subject pool at Tilburg University, where students can participate in experiments in exchange for research participation credit. Other participants were recruited via social media and personal contacts of the researcher. The participants were randomly assigned to one of two experimental conditions. Condition one was manipulated by the presence of transreality elements in the game, and was completed by 26 participants (13 male and 13 female) with a mean age of 23.9 (*SD* = 8.14). Condition two was manipulated by the absence of transreality elements and was completed by 20 participants (11 male and 9 female), with a mean age of 21.2 (*SD* = 2.65).

# 4. Results

To compare each of the engagement scales between conditions, two-way analysis of variance (ANOVA) was employed. In addition, two-way mixed ANOVA was used to check for differences in the PMT-components, intention and behavior between pre-test and post-test and between game versions and genders. In case a difference between tests, game version, gender, or a combination thereof was classified as statistically significant, post hoc analysis consisting of pairwise comparisons was utilized to examine these differences. Bonferroni-adjustments were used to make the tests more robust and to control for familywise error rate. The following section presents an overview of significant effects. For an overview of all results and tables of means, refer to appendix IV.

## 4.1 Engagement

Table 1 shows the means and standard deviations of the ratings on the different scales of engagement, organized by game version and gender. Overall, participants rated the game below average on engagement ($M = 2.10$, $SD = 0.60$). Two-way ANOVA was used with engagement as dependent variable (DV) and transreality and gender as independent variables (IV) to examine the influence of transreality elements and gender on engagement. No significant main effects were found for transreality ($F(1, 42) = 0.58$, $p = .45$, $\eta^2 = .012$) or gender ($F(1, 42) = 1.61$, $p = .211$, $\eta^2 = .033$) on the combined engagement scale. However, a small significant interaction effect was found between game version and gender ($F(1, 42) = 1.45$, $p = .043$, $\eta^2 = .089$), for which Bonferroni-adjusted pairwise comparisons indicated that male participants rated the non-transreality version significantly higher on engagement than the transreality version ($t(42) = 2.07$, $p = .045$).

Next, two-way ANOVAs were conducted for the individual subscales of the engagement measure. None of these showed significant main effects, but there was a medium significant interaction effect found between game version and gender for immersion ($F(1, 42) = 8.28$, $p = 0.06$, $\eta^2 = .16$). Bonferroni-adjusted pairwise comparisons indicated that male participants rated the non-transreality version significantly higher on immersion than the transreality version ($t(42) = 2.60$, $p = .013$).

Table 1.

*Comparison of engagement measures between groups based on game version and gender (min = 1, max = 5).*

| Transreality | Gender | *N* | Engagement | | Immersion | | Presence | | Flow | | Absorption | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | *M* | *SD* | *M* | *SD* | *M* | *SD* | *M* | *SD* | *M* | *SD* |
| **No** | Male | 11 | 2.45 | 0.65 | 2.82 | 1.17 | 2.68 | 1.01 | 2.39 | 0.62 | 2.09 | 0.88 |
| | Female | 9 | 1.88 | 0.49 | 0.87 | 1.67 | 1.89 | 0.86 | 1.81 | 0.48 | 1.52 | 0.53 |
| | Total | 20 | 2.19 | 0.64 | 2.30 | 1.17 | 2.33 | 1.00 | 2.13 | 0.62 | 1.83 | 0.78 |
| **Yes** | Male | 13 | 1.96 | 0.63 | 1.77 | 0.93 | 1.92 | 1.00 | 1.96 | 0.64 | 1.72 | 0.81 |
| | Female | 13 | 2.10 | 0.52 | 2.31 | 0.95 | 2.04 | 0.69 | 1.97 | 0.51 | 1.79 | 0.75 |
| | Total | 26 | 2.03 | 0.57 | 2.04 | 0.96 | 1.98 | 0.84 | 1.97 | 0.57 | 1.76 | 0.77 |
| **Total** | Male | 24 | 2.19 | 0.67 | 2.25 | 1.15 | 2.27 | 1.05 | 2.16 | 0.65 | 1.89 | 0.85 |
| | Female | 22 | 2.01 | 0.51 | 2.05 | 0.95 | 1.98 | 0.75 | 1.90 | 0.49 | 1.68 | 0.67 |
| | Total | 46 | 2.10 | 0.60 | 2.15 | 1.05 | 2.13 | 0.92 | 2.04 | 0.59 | 1.79 | 0.77 |

*Note: *M*=Mean, *SD*=Standard Deviation.

## 4.2 Differences on PMT-components and behavior between pre-test and post-test

Two-way mixed ANOVAs were conducted to examine the associations between the 5 variables from the PMT-framework, intention and behavior (DVs), and transreality and gender (IVs) within subjects. No significant main effects were found when comparing overall pre-test and post-test results. However, a trend was found which indicated a weak effect of playing either version of the game *ThreatBattle* on self-efficacy ($F(1, 42) = 3.56$, $p = .066$, $\eta^2 = .072$). Bonferonni-adjusted pairwise comparisons indicated a trend towards an increase in self-efficacy ($t(44) = 1.89$, $p = .066$).

Furthermore, a small significant main effect was found for transreality on behavior ($F(1, 42) = 5.21$, $p = .028$, $\eta^2 = .11$). Bonferroni-adjusted pairwise comparisons did not find any significant differences, although a trend was found which indicated an increase in cybersecurity-related behavior between pre-test and post-test in the transreality condition ($t(42) = 1.83$, $p = .074$), but not in the non-transreality condition ($t(42) = 1.43$, $p = .16$). A small significant main effect was found for gender on response efficacy ($F(1, 42) = 5.11$, $p = .029$, $\eta^2 = .099$). Specifically, Bonferroni-adjusted pairwise comparisons showed a significant decrease in response efficacy between pre-test and post-test for male participants ($t(42) = -2.39$, $p = .021$), but not for female participants ($t(42) = 0.85$, $p = .40$).

A nearly significant trend was found for the interaction between transreality and gender on intention ($F(1, 42) = 3.91$, $p = .054$, $\eta^2 = .079$). Bonferroni-adjusted pairwise comparisons indicated a nearly significant decrease in intention for female participants in the non-transreality version ($t(40) = -1.98$, $p = .054$) but not in the transreality version ($t(40) = -0.41$, $p = .68$). No further significant effects were found.

## 4.3 Differences on PMT-components and behavior between groups

Two-way mixed ANOVAs also examined the associations between the PMT-components and behavior (DVs) and transreality and gender (IVs) between subjects (i.e. the difference in scores between groups). The ANOVA revealed a medium-sized significant main effect of gender on self-efficacy ($F(1, 42) = 6.43$, $p = .015$, $\eta^2 = .13$). Bonferonni-adjusted pairwise comparisons indicated that self-efficacy increased more for male participants than for female participants ($t(44) = 2.54$, $p = .015$)

In addition, a significant interaction effect between gender and transreality on behavior was found ($F(1, 42) = 4.44$, $p = .041$, $\eta^2 = .086$). Bonferroni-adjusted pairwise comparisons indicated that behavior increased more for female participants in the transreality condition than for female participants in the non-transreality condition ($t(42) = 2.42$, $p = .020$). No further significant effects were found.

## 4.4 Summary of the results

Overall, participants rated the game below average on engagement. There was no main effect of engagement, but male participants considered the non-transreality version as more engaging than the transreality version of the game. The responsible underlying concept of engagement in this case was immersion.

No significant main effects of playing *ThreatBattle* were found, although a trend indicated an overall increase in self-efficacy between pre-test and post-test. Game version seemed to be of significant influence on behavior with respect to taking cybersecurity measures, while follow-up analysis found a trend that indicated an increase in cybersecurity-related behavior in the transreality condition.

Response efficacy significantly decreased for male participants. In addition, a nearly significant decrease in intention was found for female participants in the non-transreality version. Finally, self-efficacy increased more for male participants than female participants, and behavior with respect to cybersecurity increased more for female participants in the transreality condition than for female participants in the non-transreality condition.

# 5. Discussion

This chapter will discuss the findings of the experiment. First, a more detailed interpretation of the results is provided (Section 5.1). Second, limitations of the study are addressed and recommendations are given for how future work investigating the relationship between persuasive games and engagement, attitude and behavior can be improved (Section 5.2). Finally, potential applications of the results are discussed (Section 5.3).

## 5.1 Interpretation of results

This research examined whether playing a serious game designed to create cybersecurity awareness could lead to changes in attitude towards cybersecurity and cybersecurity related behavior. Attitude was measured with scales from the Protection Motivation theory, which were perceived severity, perceived vulnerability, response efficacy, self-efficacy and intention. Behavior was measured by the STOP-index developed by the makers of the game *ThreatBattle*, which measures good cybersecurity practice and the level of protection of a player's devices. To look at what elements make a game persuasive, a version of *ThreatBattle* with transreality elements, which incorporates actual real-world data in the virtual world of the game, and a version without transreality elements were compared. In addition, engagement was measured in the form of immersion, presence, flow and absorption. Finally, the influence of gender was examined. The results obtained from the analysis of the *ThreatBattle* experiment indicate that transreality and gender appear to be at least partially of influence on the effectiveness of *ThreatBattle*, although most of the observed effect sizes are small.

Participants rated the game below average on engagement measures, but for male participants there was a difference observed between versions, as they thought the non-transreality version was more engaging and more immersive than the transreality version. This effect was the opposite of what we expected. A possible explanation for this effect is that the addition of questions on the level of protection of the player's devices, and pop-ups with information on attackers, were too distracting, and limited the experience of immersion.

No significant difference was found in participant's estimation of the severity of consequences. In addition, playing *ThreatBattle* had no effect on participant's estimation of the possibility that a security violation will occur. A possible explanation for these results is that as the game uses real-world cyber-attack data to generate attackers, the player has to defend mostly against common threats for which they may already be aware of the possibility of occurrence and of the severity of consequences. In addition, participants expressed that it was quite easy to defend against attackers in the game, which may have resulted in a failure to convey vulnerability and severity.

A trend was found which indicated an overall increase in self-efficacy between pre-test and post-test, as we expected. In addition, male participants scored higher on self-efficacy than female

participants. As described in the theoretical framework, an influence of gender was found in the original research of the PMT-questionnaire and the present research seems to re-confirm this.

Response efficacy significantly decreased for male participants. A possible explanation is that these participants realized two of the defense mechanisms in the game were inferior to the other defense mechanisms. It was reported that only placing scanners made it impossible for attackers to get through and resulted in a guaranteed win, which required almost no interaction from the player. If this is indeed part of the reason, participants may have seen the vault and firewall as ineffective, which may in turn have translated into lower response efficacy. However, qualitative data would have to be collected to support this statement.

A nearly significant decrease in intention was found for female participants in the non-transreality version. Although we expected differences based on gender and game version, we did not expect this indication of a decrease. A significant difference in behavior with respect to taking cybersecurity measures between game versions was found, while follow-up analysis only found a trend that indicated an increase in cybersecurity-related behavior in the transreality condition. In addition, female participants in the transreality condition scored higher on behavior measures than female participants in the non-transreality condition. What we expected was an increase in both conditions, although these results do seem to agree with our hypothesis that behavior would increase more in the transreality condition and with the hypothesis on gender differences.

All in all the results obtained from the analysis of the *ThreatBattle* experiment give a preliminary indication that serious games may be used to influence cybersecurity attitude and behavior. Although a trend was found which indicated an increase in cybersecurity-related behavior in the transreality version, transreality elements did not have the definite effect we expected. Overall engagement was low, which could be responsible for the lack of significant main effects and for the low effect sizes. Finally, gender appeared to have substantial influence. Most of the effects that were found were only applicable to either male or female participants.

## 5.2 Limitations and suggestions for future research

Almost all participants in this study were university students, which means that most participants were in the same age group and at comparable levels of education. Because this makes it difficult to generalize beyond this scope, future research could compare effects among a more diverse sample of participants. In addition, due to the high drop-out ratio in this experiment, which may have been caused by a combination of conducting the experiment during exam weeks and the multiple steps involved in completing the experiment, 46 instead of the intended 60 participants finished the experiment. Conclusions drawn for sub-groups that include a small number of participants become increasingly difficult to generalize.

In the theoretical framework the influence of engagement with concern to the effectiveness of persuasive games was elaborated on. Engaging players seems to be a challenge for serious games. As De Castell and Jenson (2003) stated: “What neither researchers nor educational game-developers developers have so far been able to do is to create an ‘educational game’ that offers its players the kind of engaging, immersive play-space in which users want to stay, explore, and learn, as they do consistently in commercial games.” (De Castell & Jenson, 2003). Since then, there have been examples of serious games that managed to do this, although as the result of small budgets and less available talent the quality of serious games is still often considered unsatisfactory when compared to commercial games (Ochalla, 2007). Even though 91% of the participants reported below average scores of engagement, no causal connection can be drawn between this figure and the low amount of significant positive results in the current study. Future research on the relationship between engagement and the effectiveness of serious games would benefit from having a clear distinction between high and low engagement game versions, which may be achieved by developing a game from scratch or selecting a game based on extensive engagement testing in pilot studies.

There is a certain amount of complexity involved in assessing intangible measures such as engagement and attitude. Results may vary depending on chosen measurement instruments and operationalization. In addition, the present study used protection motivation purely as a measurement of attitude. Used in this way, little can be said about the nature of the relationship between attitude and behavior. Future research could therefore examine causal relations between protection motivation and cybersecurity behavior, to shed light on questions of how the concepts relate.

Furthermore, in the current study, participants played a single game. Future research may benefit from a comparison between multiple games of the same genre. Finally, participants were instructed to play *ThreatBattle* for a minimum of 3 times during the period of 1 week. However, due to technical problems outside the experimenter’s control, the number of play sessions and total amount of time played were not registered for most of the participants. This means that there is no way to discern effects of playing more than the minimum amount of sessions or between total time played. In future research, it may be of interest to analyze the possible influence of these factors on the results.

## 5.3 Applications

There is little empirical research available on the use of serious games to influence cybersecurity attitude and behavior. Moreover, transreality as it is used in the game *ThreatBattle* does not appear to have been related to effectiveness before. Although the results of this study should be interpreted with the previously mentioned limitations in mind, they do have some implications and provide directions for future work.

The idea behind transreality, that the link between the game and the real world may make the game more effective, is appealing. However, in the present research no definite evidence was found for this effect. Instead, a link was found between transreality and engagement, which turned out to be that the transreality version of the game led to lower engagement for some subgroups. It might be worthwhile to perform future research into this relation between transreality and engagement, for example by eliminating the need for user input in determining the level of protection of a device. Because if this negative effect of transreality on engagement can be avoided, transreality might lead to more effective persuasive games.

Finally, this study provides an insight into the relationship between gender and the effectiveness of persuasive serious games. Acknowledging this influence may lead to more effective design of persuasive games.

# 6. Conclusion

In this chapter the hypotheses presented in the theoretical framework will be confirmed or rejected and the problem statement which was formulated in the introduction will be answered.

The first hypothesis assumed that based on the procedural rhetoric embedded in persuasive games, playing *ThreatBattle* would have a positive effect on attitude and behavior, regardless of the condition the participant was in:

*H1: All participants that played ThreatBattle score higher on the PMT-components, intention and behavior measures on the post-test than on the pre-test.*

Based on the results of this study, the hypothesis is rejected. No main effect was found on these measures, although there was a trend found which indicated an overall increase in self-efficacy.

With regards to the difference between the versions of *ThreatBattle* with and without transreality, we expected that the version with transreality would show higher increases for attitude and behavior than the version without transreality elements:

*H2a: Participants that played the transreality version of ThreatBattle show higher increases than the non-transreality version between the pre-test and post-test on the PMT-components, intention and behavior.*

Based on the results of the study, this hypothesis is rejected, although there was preliminary evidence found for an effect on behavior. A trend was found indicating an increase in behavior in the transreality group. Female participants in the transreality condition scored higher on behavior measures than female participants in the non-transreality condition as well.

Hypothesis 2b assumed that participants in the transreality condition would score higher on measures of engagement:

*H2b: Participants that played the transreality version of ThreatBattle show higher scores on engagement measures than those who played the non-transreality version.*

This hypothesis is rejected as there was partial confirmation found for the opposite effect. Male participants thought the non-transreality version was more engaging than the transreality version of the game. The responsible underlying concept of engagement in this case was immersion.

The last hypothesis assumed there would be a significant effect of gender on the protection motivation measures, as was found in the original research by Van der Linden (2014):

*H3: Male and female participants differ in changes in scores on the PMT-components, intention, behavior and overall engagement.*

The results of the study confirm this hypothesis. Gender, alone or combined with other factors, was of influence on response efficacy, self-efficacy, intention and behavior. Most of the effects that were found were only applicable to either males or females.

The aim of this study was to find an answer to the question to what extent playing a persuasive game can influence attitude and behavior. The gathered data lead to the tentative conclusion that persuasive games can influence attitude and behavior, but results vary for gender and, in the case of *ThreatBattle*, the incorporation of transreality, which did not result in the definite positive effect that was expected.

References

Abt, C. C. (1970). *Serious games*. New York, NY: Viking.

Amory, A. (2007). Game object model version II: A theoretical framework for educational game development. *Educational Technology Research and Development, 55*(1), 51-77. doi:10.1007/s11423-006-9001-x

Arjoranta, J. (2014). Game definitions: A wittgensteinian approach. *Game Studies: The International Journal of Computer Game Research, 14*(1) Retrieved from http://gamestudies.org/1401/articles/arjoranta

Baños, R. M., Botella, C., Alcañiz, M., Liaño, V., Guerrero, B., & Rey, B. (2004). Immersion and emotion: Their impact on the sense of presence. *CyberPsychology & Behavior, 7*(6), 734-741. doi:10.1089/cpb.2004.7.734.

Baranowski, T., Buday, R., Thompson, D. I., & Baranowski, J. (2008). Playing for real: Video games and stories for health-related behavior change. *American Journal of Preventive Medicine, 34*(1), 74-82. doi:10.1016/j.amepre.2007.09.027

Blackmon, S., & Terrell, D. J. (2007). Racing toward representation: An understanding of racial representation in video games. In C. L. Selfe, & G. E. Hawisher (Eds.), *Gaming lives in the twenty-first century: Literate connections* (pp. 203-215). New York, NY: Palgrave Macmillan.

Boer, H., & Seydel, E. R. (1996). Protection motivation theory. In M. Conner, & P. Norman (Eds.), (pp. 120). Buckingham, England: Open University Press. Retrieved from http://doc.utwente.nl/34896/

Bogost, I. (2010). *Persuasive games: The expressive power of videogames*. Cambridge, MA: MIT Press.

Brockmyer, J. H., Fox, C. M., Curtiss, K. A., McBroom, E., Burkhart, K. M., & Pidruzny, J. N. (2009). The development of the game engagement questionnaire: A measure of engagement in video game-playing. *Journal of Experimental Social Psychology, 45*(4), 624-634. doi:10.1016/j.jesp.2009.02.016

Burke, K. (1969). *A rhetoric of motives*. Berkeley: University of California Press.

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, 30*(8), 719-731. doi:10.1016/j.cose.2011.08.004

Coleman, J. (1971). Learning through games. In E. M. Avedon, & B. Sutton-Smith (Eds.), *The study of games* (pp. 322-325). New York, NY: John Wiley & Sons.

Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & Education, 59*(2), 661-686. doi:10.1016/j.compedu.2012.03.004

Corti, K. (2006). *Games-based learning; a serious business application.* PIXELearning Limited. Retrieved from https://www.cs.auckland.ac.nz/courses/compsci777s2c/lectures/Ian/serious%20games%20business%20applications.pdf

Csikszentmihalyi, M. (1999). If we are so rich, why aren't we happy? *American Psychologist, 54*(10), 821-827. doi:10.1037/0003-066X.54.10.821

De Castell, S., & Jenson, J. (2003). OP-ED serious play. *Journal of Curriculum Studies, 35*(6), 649-665. doi:10.1080/0022027032000145552

De la Hera Conde-Pumpido, T. (2014). *Persuasive Structures in Advergames: Conveying Advertising Messages through Digital Games* (Doctoral Dissertation). Retrieved from http://dspace.library.uu.nl/handle/1874/291047

Field, A. (2013). *Discovering statistics using IBM SPSS statistics* (4th ed.). London, England: SAGE.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Green, M. C., & Brock, T. C. (2000). The role of transportation in the persuasiveness of public narratives. *Journal of Personality and Social Psychology, 79*(5), 701-721. doi:10.1037/0022-3514.79.5.701

Herz, J. C. (1997). *Joystick nation: How videogames ate our quarters, won our hearts, and rewired our minds* (1st ed.). Boston, MA: Little, Brown & Co. Inc.

Huizinga, J. (1955). *Homo ludens: A study of the play-element in culture.* Boston, MA: Beacon Press.

Irwin, H. J. (1999). Pathological and nonpathological dissociation: The relevance of childhood trauma. *The Journal of Psychology, 133*(2), 157-164. doi:10.1080/00223989909599730

Ke, F. (2008). A case study of computer gaming for math: Engaged learning from gameplay? *Computers & Education, 51*(4), 1609-1620. doi:10.1016/j.compedu.2008.03.003

Lavender, T. J. (2011). Video games as change agents – the case of homeless: It's no game. *The McMaster Journal of Communication, 7*(1), 299. Retrieved from https://journals.mcmaster.ca/mjc/article/download/253/220

Lavender, T. J. (2008). *Homeless: It's no game - measuring the effectiveness of a persuasive videogame* (Master's thesis). Retrieved from http://summit.sfu.ca/system/files/iritems1/9314/etd4267.pdf

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi:10.1016/0022-1031(83)90023-9

MAVI Interactive LLC. (2014). Agent surefire: Insider threat. Retrieved from https://agentsurefire.com/insiderthreat/

Mäyrä, F. (2008). *An introduction to game studies*. London, England: SAGE Publications.

Michael, D. R., & Chen, S. (2006). *Serious games: Games that educate, train and inform*. Boston, MA: Thomson Course Technology.

Miller, G. R. (2012). On being persuaded: Some basic distinctions. In J. P. Dillard, & L. Shen (Eds.), *The persuasion handbook: Developments in theory and practice* (2nd ed., pp. 70-83). Thousand Oaks, CA: SAGE Publications. doi:10.4135/9781452218410

Murr, J. (2012). Ian bogost — on serious games. Retrieved from https://joshmurr.wordpress.com/2012/04/03/ian-bogost-on-serious-games/

Murray, J. H. (1997). *Hamlet on the holodeck: The future of narrative in cyberspace*. New York, NY: The Free Press.

Nationaal Cyber Security Centrum (2014). *Jaarraportage Cybersecuritybeeld Nederland.* Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/07/10/cybersecuritybeeld-nederland.html

Ng, B., Kankanhalli, A., & Xu, Y. (. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi:10.1016/j.dss.2008.11.010

Ochalla, B. (2007). *Who Says Video Games Have to be Fun? The Rise of Serious Games.* Retrieved from http://www.gamasutra.com/view/feature/129891/who_says_video_games_have_to_be_.php

O'Keefe, D. J. (2003). Message properties, mediating states, and manipulation checks: Claims, evidence, and data analysis in experimental persuasive message effects research. *Communication Theory, 13*(3), 251-274. doi:10.1111/j.1468-2885.2003.tb00292.x

Pereira, C. (2014). GTA 5 ships 34 million units -- more than borderlands 2, BioShock infinite, and NBA 2K14 combined. Retrieved from http://www.gamespot.com/articles/gta-5-ships-34-million-units-more-than-borderlands/1100-6421531/

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. *Advances in Experimental Social Psychology, 19*, 205. doi:10.1016/S0065-2601(08)60214-2

Prensky, M. (2001). *Digital game-based learning*. New York, NY: McGraw-Hill.

Quinn, C. N. (2005). *Engaging learning: Designing e-learning simulation games*. San Francisco, CA: John Wiley & Sons.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93-114. doi:10.1080/00223980.1975.9915803

Rollings, A., & Morris, D. (2003). *Game architecture and design: A new edition*. San Francisco, CA: New Riders Games.

Ruggiero, D. (2012). In Amiel T., Wilson B. (Eds.), *Conceptualizing a persuasive game framework.* Chesapeake, VA: Association for the Advancement of Computing in Education (AACE). Retrieved from http://www.editlib.org/p/40902

Salen, K., & Zimmerman, E. (2004). *Rules of play: Game design fundamentals*. Cambridge, MA: MIT Press.

Sicart, M. (2011). Against Procedurality. *Game Studies: The International Journal of Computer Game Research, 11*(3) Retrieved from http://gamestudies.org/1103/articles/sicart_ap

Siwek, S. E. (2014). *Video games in the 21st century: The 2014 report.* Entertainment Software Association. Retrieved from http://www.theesa.com/wp-content/uploads/2014/11/VideoGames21stCentury_2014.pdf

Suits, B., Hurka, T., & Newfeld, F. (2014). *The grasshopper, third edition: Games, life and utopia*. Toronto, Canada: Broadview Press.

Tamborini, R., & Skalski, P. (2006). The role of presence in the experience of electronic games. In P. Vorderer J. Bryant (Ed.), (pp. 225-240). Mahwah, NJ: Lawrence Erlbaum Associates Publishers.

The Center for Information Systems Security Studies and Research. (2014). CyberCIEGE. Retrieved from http://cisr.nps.edu/cyberciege/

Van der Linden, J. (2014). *Protection motivation theory and cybersecurity awareness: The effect of serious games* (Unpublished bachelor thesis). Tilburg University, Tilburg.

Wirth, W., Hartmann, T., Böcking, S., Vorderer, P., Klimmt, C., Schramm, H., . . . Gouveia, F. R. (2007). A process model of the formation of spatial presence experiences. *Media Psychology, 9*(3), 493-525.

Yee, N., & Bailenson, J. N. (2006). *Walk a mile in digital shoes: The impact of embodied perspective-taking on the reduction of negative stereotyping in immersive virtual environments*. Paper presented at the PRESENCE 2006: The 9th Annual International Workshop on Presence, Cleveland, OH.

# Appendix I: Pre-test survey

**Demographics**

1. Anonymous Username. The code consists of the prefix TIU, the first 2 letters of your first name, the first 2 letters of your mother's name, the first 2 letters of your birth place, and your house number.
2. What is your gender? (Male/Female)
3. What is your age?
4. What is your highest level of education?

- WO-doctoral or master
- HBO or WO bachelor
- HBO or WO propedeuse
- MBO
- HAVO / VWO
- MAVO / VMBO
- Primary school / No education
- Other / Do not know

5. How often do you play videogames? (Incl. Facebook games, mobile games etc.) (1 never – 5 often)
6. How would you rate your cybersecurity knowledge? (1 no knowledge – 5 expert)

**Behavior** (1 Yes 2 No / Do not know)

7. My operating system is the newest version
8. I have a virus scanner installed
9. My virus scanner is up to date
10. I always check the sources of files I download
11. I never consider links in e-mails safe, even when I know the sender
12. I never share files on my computer with others on unprotected networks
13. I never use my portable storage devices (e.g. USB-sticks) on multiple computers

**PMT-components**

*For the following questions, security violations include threats such as virus attacks and unauthorized access to data by hackers. Indicate the degree to which you agree or disagree with the following statements: (1 Strongly Disagree – 5 Strongly Agree)*

1. I believe that a security violation on my computer is a serious matter.
2. I believe that information stored on my computer is vulnerable to security violations.
3. A security violation could seriously affect the information on my computer.
4. A security violation could seriously harm my computer.
5. The risk that a security violation on my computer will occur is significant.
6. The chances of getting, or already having, some forms of security violation on my computer are significant.
7. Someone I know was exposed to some form of security violations to his computer.
8. Whether my computer is vulnerable to security violations is important to me.

*For the following questions, security measures are individual actions such as running and updating antivirus software, keeping passwords secure, running a firewall when necessary, and exercising care when opening e-mail attachments.Indicate the degree to which you agree or disagree with the following statements: (1 Strongly Disagree – 5 Strongly Agree)*

1. A security violation on my computer is inevitable.
2. There is not much that any one individual can do to help secure their computer.

3. Taking security measures to protect my computer could counteract security violations.
4. If I take security measures to protect my computer, I can prevent security violations.
5. I feel comfortable taking security measures to protect my computer.
6. Taking the necessary security measures is entirely under my control.
7. I have the resources and the knowledge to take the necessary security measures.
8. Taking the necessary security measures is easy.
9. I would be able to take the security measures even if there was nobody to show me how.

*Thinking of your future actions, indicate the degree to which you agree or disagree with the following statement regarding your likelihood of implementing security measures to protect your computer: (1 Strongly Disagree – 5 Strongly Agree)*
1. I am likely to take security measures to protect my computer.

# Appendix II: Post-test survey

**Demographics**

1. Anonymous Username. The code consists of the prefix TIU, the first 2 letters of your first name, the first 2 letters of your mother's name, the first 2 letters of your birth place, and your house number.

**Behavior** (1 Yes 2 No / Do not know)

7. My operating system is the newest version
8. I have a virus scanner installed
9. My virus scanner is up to date
10. I always check the sources of files I download
11. I never consider links in e-mails safe, even when I know the sender
12. I never share files on my computer with others on unprotected networks
13. I never use my portable storage devices (e.g. USB-sticks) on multiple computers

**Engagement**

*The following statements are related to playing the game ThreatBattle. Indicate the degree to which you agree or disagree with the following statements: (1 Strongly Disagree – 5 Strongly Agree)*

1. I lose track of time
2. Things seem to happen automatically
3. I feel different
4. I feel scared
5. The game feels real
6. If someone talks to me, I don’t hear them
7. I get wound up
8. Time seems to kind of stand still or stop
9. I feel spaced out
10. I don’t answer when someone talks to me
11. I can’t tell that I’m getting tired
12. Playing seems automatic
13. My thoughts go fast
14. I lose track of where I am
15. I play without thinking about how to play
16. Playing makes me feel calm
17. I play longer than I meant to
18. I really get into the game
19. I feel like I just can’t stop playing

**PMT-components**

*For the following questions, security violations include threats such as virus attacks and unauthorized access to data by hackers. Indicate the degree to which you agree or disagree with the following statements: (1 Strongly Disagree – 5 Strongly Agree)*

1. I believe that a security violation on my computer is a serious matter.
2. I believe that information stored on my computer is vulnerable to security violations.
3. A security violation could seriously affect the information on my computer.
4. A security violation could seriously harm my computer.
5. The risk that a security violation on my computer will occur is significant.
6. The chances of getting, or already having, some forms of security violation on my computer are significant.
7. Someone I know was exposed to some form of security violations to his computer.
8. Whether my computer is vulnerable to security violations is important to me.

*For the following questions, security measures are individual actions such as running and updating antivirus software, keeping passwords secure, running a firewall when necessary, and exercising care when opening e-mail attachments.Indicate the degree to which you agree or disagree with the following statements: (1 Strongly Disagree – 5 Strongly Agree)*

1. A security violation on my computer is inevitable.
2. There is not much that any one individual can do to help secure their computer.
3. Taking security measures to protect my computer could counteract security violations.
4. If I take security measures to protect my computer, I can prevent security violations.
5. I feel comfortable taking security measures to protect my computer.
6. Taking the necessary security measures is entirely under my control.
7. I have the resources and the knowledge to take the necessary security measures.
8. Taking the necessary security measures is easy.
9. I would be able to take the security measures even if there was nobody to show me how.

*Thinking of your future actions, indicate the degree to which you agree or disagree with the following statement regarding your likelihood of implementing security measures to protect your computer: (1 Strongly Disagree – 5 Strongly Agree)*

1. I am likely to take security measures to protect my computer.

# Appendix III: Consent form and instruction

**Code:** 60-24-2014

**Title:** Serious games for cybersecurity

Purpose of the experiment:

In this experiment we want to research the effectiveness of serious games for cybersecurity. Serious games are games that do not have entertainment as their primary goal. You will be asked to play a serious game and fill in online pre- and post-game surveys.

Duration of the experiment:

The experiment will take approximately 1 hour and you will receive 1 research subject hour for participation.

Confidentiality:

All collected data, including the answers on survey questions, will be treated confidentially. Your name will in no circumstance be connected to the results. Only members of the research team or researchers who want to re-analyse the data have access to the data. The research data will be saved for a minimum of five years.

Voluntary Participation:

You are in no way obligated to participate in this experiment. You may choose to withdraw from the experiment at any time. You do not have to answer questions you do not want to answer.

Contact:

If you have any questions after this experiment, you can contact Joël Grevelink (j.grevelink@uvt.nl). For more information on the guidelines and regulations for research, see *The Netherlands Code of Conduct for Scientific Practice* under course information for Blackboard course Proefpersonenpool.

---

**Permission**

I have had the opportunity to read this consent form and have the experiment explained. I have had the opportunity to ask questions about the research and my questions have been answered. I am prepared to participate in the research described above. I will receive a copy of this consent form after I sign it.

_____

Participant signature

_____

Participant name

_____ _____

Researcher signature Date

This experiment consists of 2 parts.

---

Part 1 (now)

1) After reading the remainder of this document, please open the Google Chrome browser and go to http://threatbattlel.tk/

2) Click the first link to fill in survey 1. You will have to answer some demographic questions and statements on cybersecurity.
   *Note: You will be asked to create an anonymous identification code. Write it down below; you will need it to register and log in to the game.*

   ……

3) After finishing the survey, click the second link to go to the game. Click on "Ik heb geen account" to register an account. In the "Gebruikersnaam" box, fill in the code you have just written down. In the 'Wachtwoord" box fill in a password of your own liking.

4) Play the game and defend your base. Click on the tiles along the paths to place firewalls, vaults and scanners to destroy incoming threats. The game is over when all threats have been destroyed, or your hit points reach 0.

Part 2 (at home)

1) You will be asked to play the game during a period of 1 week. You are free to play as many times as you like, with a minimum of 2 times.

2) After 1 week (18-12-14, 00:00) the link to survey 2 will be activated. Please fill in this survey as soon as possible, before 21-12-14.

If you have any questions during the experiment, do not hesitate to ask.

**Note: The instruction was the same for both conditions, except for the link in part 1. The transreality group contained a link to threatbattle1.tk, the non-transreality group a link to threatbattle2.tk. Both pages were used to display links to the pre- and posttest surveys and the game ThreatBattle.*

# Appendix IV: Tables of results

Table 2.

*Effects of gender and transreality on engagement (between subjects)*

| IV (Between subjects) | DV | *F* | *df* | Error *df* | *p* | $\eta^2$ |
|---|---|---|---|---|---|---|
| Gender | Engagement | 1.61 | 1 | 42 | .21 | .033 |
| | Immersion | 1.09 | 1 | 42 | .30 | .021 |
| | Presence | 1.61 | 1 | 42 | .21 | .034 |
| | Flow | 2.81 | 1 | 42 | .10 | .058 |
| | Absorption | 1.17 | 1 | 42 | .29 | .026 |
| Transreality | Engagement | 0.58 | 1 | 42 | .45 | .012 |
| | Immersion | 0.48 | 1 | 42 | .49 | .009 |
| | Presence | 1.30 | 1 | 42 | .26 | .027 |
| | Flow | 0.58 | 1 | 42 | .45 | .012 |
| | Absorption | 0.044 | 1 | 42 | .83 | .001 |
| Gender * Transreality | Engagement | 4.33 | 1 | 42 | .043* | .089 |
| | Immersion | 8.28 | 1 | 42 | .006* | .16 |
| | Presence | 2.89 | 1 | 42 | .096 | .060 |
| | Flow | 3.01 | 1 | 42 | .090 | .062 |
| | Absorption | 2.01 | 1 | 42 | .16 | .044 |

Note: *Significant at $p < .05$ level.

Table 3.

*Univariate effects for PMT-components, intention and behavior (between subjects)*

| DV (Between subjects) | IV: G=Gender T=Transreality | *F* | *df* | Error *df* | *p* | $\eta^2$ |
|---|---|---|---|---|---|---|
| Perceived Severity | G | 2.35 | 1 | 42 | .13 | .052 |
| | T | 0.12 | 1 | 42 | .73 | .0027 |
| | G*T | 0.69 | 1 | 42 | .41 | .015 |
| Perceived Vulnerability | G | 1.76 | 1 | 42 | .19 | .040 |
| | T | 0.41 | 1 | 42 | .53 | .0093 |
| | G*T | 0.49 | 1 | 42 | .83 | .0011 |
| Response Efficacy | G | 1.50 | 1 | 42 | .23 | .034 |
| | T | 0.59 | 1 | 42 | .45 | .013 |
| | G*T | 0.07 | 1 | 42 | .93 | .00016 |
| Self-Efficacy | G | 6.43 | 1 | 42 | .015* | .13 |
| | T | 0.31 | 1 | 42 | .58 | .0064 |
| | G*T | 0.15 | 1 | 42 | .70 | .0031 |
| Intention | G | 0.19 | 1 | 42 | .67 | .0042 |
| | T | 0.15 | 1 | 42 | .70 | .0034 |
| | G*T | 1.78 | 1 | 42 | .19 | .040 |
| Behavior | G | 3.29 | 1 | 42 | .077 | .064 |
| | T | 2.01 | 1 | 42 | .16 | .039 |
| | G*T | 4.44 | 1 | 42 | .041* | .086 |

Note: *Significant at $p < .05$ level.

Table 4.

*Univariate effects for PMT-components, intention and behavior (within subjects)*

| DV (Within subjects) | IV: t = time, G=Gender, T=Transreality | *F* | *df* | Error *df* | *p* | $\eta^2$ |
|---|---|---|---|---|---|---|
| Perceived | t | 1.35 | 1 | 42 | .25 | .028 |
| Severity | G*t | 2.53 | 1 | 42 | .12 | .053 |
| | T*t | 0.29 | 1 | 42 | .59 | .0062 |
| | G*T*t | 1.43 | 1 | 42 | .24 | .030 |
| Perceived | t | 1.34 | 1 | 42 | .25 | .031 |
| Vulnerability | G*t | 0.024 | 1 | 42 | .88 | .00056 |
| | T*t | 0.019 | 1 | 42 | .89 | .00043 |
| | G*T*t | 0.024 | 1 | 42 | .88 | .00056 |
| Response | t | 1.05 | 1 | 42 | .31 | .020 |
| Efficacy | G*t | 5.11 | 1 | 42 | .029* | .099 |
| | T*t | 3.08 | 1 | 42 | .087 | .060 |
| | G*T*t | 0.27 | 1 | 42 | .60 | .0053 |
| Self-Efficacy | t | 3.56 | 1 | 42 | .066 | .072 |
| | G*t | 0.92 | 1 | 42 | .34 | .019 |
| | T*t | 0.77 | 1 | 42 | .39 | .016 |
| | G*T*t | 1.94 | 1 | 42 | .17 | .039 |
| Intention | t | 1.01 | 1 | 42 | .32 | .020 |
| | G*t | 2.54 | 1 | 42 | .12 | .051 |
| | T*t | 0.022 | 1 | 42 | .88 | .00044 |
| | G*T*t | 3.91 | 1 | 42 | .054 | .079 |
| Behavior | t | 0.016 | 1 | 42 | .90 | .00032 |
| | G*t | 0.074 | 1 | 42 | .79 | .00015 |
| | T*t | 5.21 | 1 | 42 | .028* | .11 |
| | G*T*t | 1.87 | 1 | 42 | .18 | .038 |

Note: *Significant at $p < .05$ level.

Table 5.

*Means and standard deviations for perceived severity (minimum = 1, maximum = 5)*

| Gender | Transreality | *N* | *M* (pre) | *SD* (pre) | *M* (post) | *SD* (post) |
|---|---|---|---|---|---|---|
| Male | No | 11 | 4.11 | 0.55 | 4.27 | 0.49 |
| | Yes | 13 | 4.10 | 0.46 | 4.00 | 0.34 |
| | Total | 24 | 4.10 | 0.49 | 4.13 | 0.43 |
| Female | No | 9 | 4.03 | 0.54 | 3.78 | 0.44 |
| | Yes | 13 | 4.04 | 0.55 | 3.88 | 0.45 |
| | Total | 22 | 4.03 | 0.53 | 3.84 | 0.44 |
| Total | No | 20 | 4.08 | 0.53 | 4.05 | 0.52 |
| | Yes | 26 | 4.07 | 0.50 | 3.94 | 0.40 |
| | Total | 46 | 4.07 | 0.51 | 3.99 | 0.45 |

Note: *N* = Participants, *M* = mean, *SD* = Standard Deviation.

Table 6.

*Means and standard deviations for perceived vulnerability (minimum = 1, maximum = 5)*

| Gender | Transreality | *N* | *M* (pre) | *SD* (pre) | *M* (post) | *SD* (post) |
|---|---|---|---|---|---|---|
| Male | No | 11 | 3.64 | 0.55 | 3.45 | 0.65 |
| | Yes | 13 | 3.42 | 0.89 | 3.31 | 0.80 |
| | Total | 24 | 3.52 | 0.74 | 3.38 | 0.73 |
| Female | No | 9 | 3.28 | 0.51 | 3.17 | 0.87 |
| | Yes | 13 | 3.19 | 0.99 | 3.08 | 0.86 |
| | Total | 22 | 3.23 | 0.81 | 3.11 | 0.84 |
| Total | No | 20 | 3.48 | 0.55 | 3.33 | 0.75 |
| | Yes | 26 | 3.31 | 0.93 | 3.19 | 0.83 |
| | Total | 46 | 3.38 | 0.78 | 3.25 | 0.79 |

Note: *N* = Participants, *M* = mean, *SD* = Standard Deviation.

Table 7.

*Means and standard deviations for response efficacy (minimum = 1, maximum = 5)*

| Gender | Transreality | *N* | *M* (pre) | *SD* (pre) | *M* (post) | *SD* (post) |
|---|---|---|---|---|---|---|
| Male | No | 11 | 3.55 | 0.60 | 3.39 | 0.66 |
| | Yes | 13 | 3.74 | 0.71 | 3.41 | 0.72 |
| | Total | 24 | 3.65 | 0.66 | 3.40 | 0.68 |
| Female | No | 9 | 3.52 | 0.47 | 3.78 | 0.41 |
| | Yes | 13 | 3.82 | 0.44 | 3.74 | 0.45 |
| | Total | 22 | 3.70 | 0.47 | 3.76 | 0.43 |
| Total | No | 20 | 3.53 | 0.53 | 3.57 | 0.58 |
| | Yes | 26 | 3.78 | 0.58 | 3.58 | 0.62 |
| | Total | 46 | 3.67 | 0.57 | 3.57 | 0.59 |

Note: *N* = Participants, *M* = mean, *SD* = Standard Deviation.

Table 8.

*Means and standard deviations for self-efficacy (minimum = 1, maximum = 5)*

| Gender | Transreality | *N* | *M* (pre) | *SD* (pre) | *M* (post) | *SD* (post) |
|---|---|---|---|---|---|---|
| Male | No | 11 | 3.30 | 0.71 | 3.64 | 0.58 |
| | Yes | 13 | 3.48 | 0.86 | 3.52 | 0.83 |
| | Total | 24 | 3.40 | 0.78 | 3.57 | 0.72 |
| Female | No | 9 | 2.86 | 0.65 | 2.89 | 0.56 |
| | Yes | 13 | 3.02 | 0.68 | 3.12 | 0.69 |
| | Total | 22 | 2.95 | 0.66 | 3.02 | 0.64 |
| Total | No | 20 | 3.10 | 0.70 | 3.30 | 0.68 |
| | Yes | 26 | 3.25 | 0.79 | 3.32 | 0.78 |
| | Total | 46 | 3.18 | 0.75 | 3.31 | 0.73 |

Note: *N* = Participants, *M* = mean, *SD* = Standard Deviation.

Table 9.

*Means and standard deviations for intention (minimum = 1, maximum = 5)*

| Gender | Transreality | *N* | *M* (pre) | *SD* (pre) | *M* (post) | *SD* (post) |
|---|---|---|---|---|---|---|
| Male | No | 11 | 3.82 | 0.40 | 4.09 | 0.30 |
| | Yes | 13 | 3.85 | 1.14 | 3.69 | 0.95 |
| | Total | 24 | 3.83 | 0.87 | 3.88 | 0.74 |
| Female | No | 9 | 4.00 | 0.50 | 3.56 | 1.01 |
| | Yes | 13 | 4.15 | 0.55 | 4.08 | 0.49 |
| | Total | 22 | 4.09 | 0.53 | 3.86 | 0.77 |
| Total | No | 20 | 3.90 | 0.45 | 3.85 | 0.75 |
| | Yes | 26 | 4.00 | 0.89 | 3.88 | 0.77 |
| | Total | 46 | 3.96 | 0.73 | 3.87 | 0.75 |

Note: *N* = Participants, *M* = mean, *SD* = Standard Deviation.

Table 10.

*Means and standard deviations for behavior (minimum = 1, maximum = 7)*

| Gender | Transreality | *N* | *M* (pre) | *SD* (pre) | *M* (post) | *SD* (post) |
|---|---|---|---|---|---|---|
| Male | No | 11 | 3.82 | 1.40 | 3.73 | 1.68 |
| | Yes | 13 | 3.38 | 1.56 | 3.62 | 1.26 |
| | Total | 24 | 3.58 | 1.47 | 3.67 | 1.43 |
| Female | No | 9 | 2.56 | 1.33 | 1.89 | 1.05 |
| | Yes | 13 | 3.31 | 1.55 | 3.92 | 1.55 |
| | Total | 22 | 3.00 | 1.48 | 3.09 | 1.69 |
| Total | No | 20 | 3.25 | 1.48 | 2.90 | 1.68 |
| | Yes | 26 | 3.35 | 1.52 | 3.77 | 1.39 |
| | Total | 46 | 3.30 | 1.49 | 3.39 | 1.57 |

Note: *N* = Participants, *M* = mean, *SD* = Standard Deviation.