Playing Safe in Online Games: Determinants of Player Acceptance of Account Security Technology

A paper presented to the

School of Information Management

Victoria University of Wellington

by

Xiaomei Yang

in partial fulfilment of the requirements for the course MMIM592

Research Project in Information Management

15 February 2013

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this *Research Project* entitled *Playing Safe in Online Games: Determinants of Player Acceptance of Account Security Technology* from the work(s) of other people has been attributed, and has been cited and referenced.

3. This paper is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work

5. I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Signature(s) …Xiaomei Yang….. Date …14/Feb/2013…

Full name(s) of student(s): Xiaomei Yang Student ID: 300073761

PREFACE

This report is not confidential.

This research project represents the culmination of four years of study, and I would like to thank all those who have helped and supported me over that time.

To all those who participated in my online survey, I am most grateful for the valuable data provided. For me personally their participation was very rewarding and inspirational.

I would like to thank my supervisor, Tony Hooper, for his advice, guidance and encouragement during my research and writing of this report.

Finally, I wish to thank my partner, Stephen Pei, and family for their support, encouragement and patience throughout my study.

Xiaomei (Susan) Yang

Table of Contents

List of Figures

List of Tables

ABSTRACT

Online security is a major problem for networked games worldwide. Specifically, account hijacking is on the rise. To fight against the security issue, game vendors are offering specific security services, such as account protection technology. The purpose of this paper is to validate an augmented Technology Acceptance Model (TAM) for the online gaming context. This research aims to investigate how players are influenced by perceived enjoyment and perceived security jointly with the traditional TAM instrument. It is hoped to explain online gamers' behaviour toward newly emerging account security technology.

The paper proposes a research model that describes the causal relationships between perceive usefulness, perceived enjoyment, perceived ease of use, perceived security, and the usage intentions for account protection technology in the most popular online game World of Warcraft. After the measurement assessment, the hypothesised model is statistically tested. The findings suggest that perceived enjoyment and perceived security jointly with two traditional TAM constructs have a positive influence on intention to use. While perceived ease of use positively affects perceived usefulness and perceived enjoyment, perceived security does not seem to affect both of them. This study contributes to the ongoing literature by formulating and validating a proposed research model to explore determinants of player adoption of security technology in the virtual gaming environment. It also provides useful information for both academia and industry.

Keywords: Online games; Account protection; Perceived enjoyment; Perceived security; Technology Acceptance Model (TAM)

1. INTRODUCTION

Online games or networked games are being rapidly developed with the phenomenal growth of the Internet (Ki, Cheon, Kang, & Kim, 2004). Due to deep penetration into the consumer market, gaming is considered a prime driver of PC technology (McGraw & Hoglund, 2007) and currently is one of the few profitable e-commerce applications (Yan, 2003). With online gaming being a billion dollar industry and game companies making revenue from subscription charges (Byrne, 2004), the presence of security issues is becoming more evident.

Online security is a problematic and pervasive issue for networked games, especially massively multiplayer online role-playing games (MMORPGs). The most popular MMORPG is the Blizzard Entertainment's World of Warcraft (WoW) (Linderoth & Bennerstedt, 2007), which has been threatened by security problems such as attacks and cheating. Among these risks, account hijacking is a critical security concern in WoW. The game company provides a variety of security services to players to help protect their game accounts, including authentication tokens, software patch, and SMS protect. Despite various security mechanisms available, little is known what factors positively influence individual player acceptance of the technology.

This research is concerned with security risks gamers encounter during online games playing. More precisely, it concerns behavioural intention of players toward adopting account security technology, attempting to explain the relation between user perception, satisfaction and intention to use the technology. Davis (1993) claims that user acceptance is the pivotal factor determining the success or failure of an information system project. The technology acceptance model (TAM) proposed by Davis (1986) has been widely used in explaining the adoption of information technologies. The model predicts two factors determining whether a user accepts any technology, which are perceived usefulness and perceived ease of use (Roca, García, & Vega, 2009).

The primary objective of the current research project is to explore the influence of perceived enjoyment and perceived security along with the TAM constructs in the online gaming context. The secondary objective is to test an extended TAM that can be used to explain the usage intention for security technology that protects online accounts. This research addes to the existing body of knowledge within technlogy acceptance studies, particularly within the rapidly evolving field of social media and online gaming studies.

In this study, an in-depth review of the relevant literature is carried out, concerning the variables affecting online players' behaviours toward account security technology and the TAM instrument. Drawing upon the literature review and theoretical framework, the hypotheses are formalised and an online survey is conducted to gather data in relation to factors determining the adoption of account protection technology. Analysis of the collected data supports the hypotheses and validates the extended TAM. Finally, this paper will present some discussion and conclusion, along with implications for future research.

2. BACKGROUND

In this section, three gaming-related concepts - MMORPG, World of Warcraft and Battle.net - are examined to outline a particular networked game environment.

2.1 MMORPG

Massively Multiplayer Online Role-Playing Games (abbreviated as MMORPGs) are a new type of computer games, which have achieved success in the gaming field, such as Second Life, EverQuest and Star Wars Galaxy (McGraw & Hoglund, 2007; Linderoth & Bennerstedt, 2007).

Massively Multiplayer

Massively multiplayer games allow thousands of players to take part simultaneously in the same game world, and to interact with each other (Beginner's guide, 2012).

Online

Unlike most computerised games, MMORPGs do not have an offline mode. Players need to be connected to the Internet while playing. Much of the game's advanced content is geared towards groups of players working together to explore dangerous "dungeons" and defeat powerful "monsters" (Beginner's guide, 2012).

Role-Playing

In the game world, each player appears in the form of personalised avatars that have a specific set of skills and abilities (Kaplan & Haenlein, 2010). Role-play also means that gamers play the role of a character living in the game's fantasy world (Beginner's guide, 2012).

In an MMORPG, the virtual world is a platform that replicates a three-dimensional environment, and also becomes social communities where players carry out different tasks together (Linderoth & Bennerstedt, 2007). Gamers play the role of a unique character (Beginner's guide, 2012), and interact with one another as they would in real life, which is probably the ultimate manifestation of social media (Kaplan & Haenlein, 2010).

2.2 World of Warcraft

The most popular MMORPG is World of Warcraft (often shortened to WoW) by the video game developer and publisher Blizzard Entertainment. The game was released on November 23, 2004, followed by four expansion sets - (1) *The Burning Crusade* released on January 16, 2007; (2) *Wrath of the Lich King* on November 13, 2008; (3) *Cataclysm* on December 7, 2010; (4) *Mists of Pandaria* on September 25, 2012 ("World of Warcraft," n.d.). WoW was honoured at the 2005 Spike TV Video Game Awards where it won Best PC Game, Best Multiplayer Game, Best RPG, and Most Addictive Game (Sinclair, 2005). It was ranked 11th on the Game Informer's list of *The Top 200 Video Games of All Time* (The Game Informer staff, 2009).

WoW requires a subscription to be paid, either by buying prepaid game cards for a selected amount of playing time or by using a credit or debit card to pay on a regular basis. With 9.1 million subscribers as of August 2012, WoW is claimed to be the world's largest subscription-based MMORPG (Activision Blizzard, 2011). The game also holds the Guinness World Record for the most popular MMORPG by subscribers (Ziebart, 2012).

WoW takes place within the planet of Azeroth, which is home to a vast number of races and cultures. There are thirteen playable races in WoW (Figure 1), divided between the two factions that form the two major power blocs of Alliance and Horde. Only members of the same faction can speak, mail, group, and join guilds. When selecting races, players also are selecting potential classes with unique abilities and play-styles (Blizzard Entertainment, 2004). Eleven classes are available to choose including warrior, paladin, hunter, rogue, priest, dark knight, shaman, mage, warlock, monk and druid. In the high-fantasy universe of Warcraft, a player controls a character avatar in third- or first-person view, exploring the landscape, fighting various monsters, completing quests, and interacting with non-player characters (NPCs) or other players ("World of Warcraft," n.d.). WoW thrusts players into a central role of an ever-changing story, fighting for either of the two factions of Horde and Alliance, and experiencing a fully-realised fantasy world (Beginner's guide, 2012).

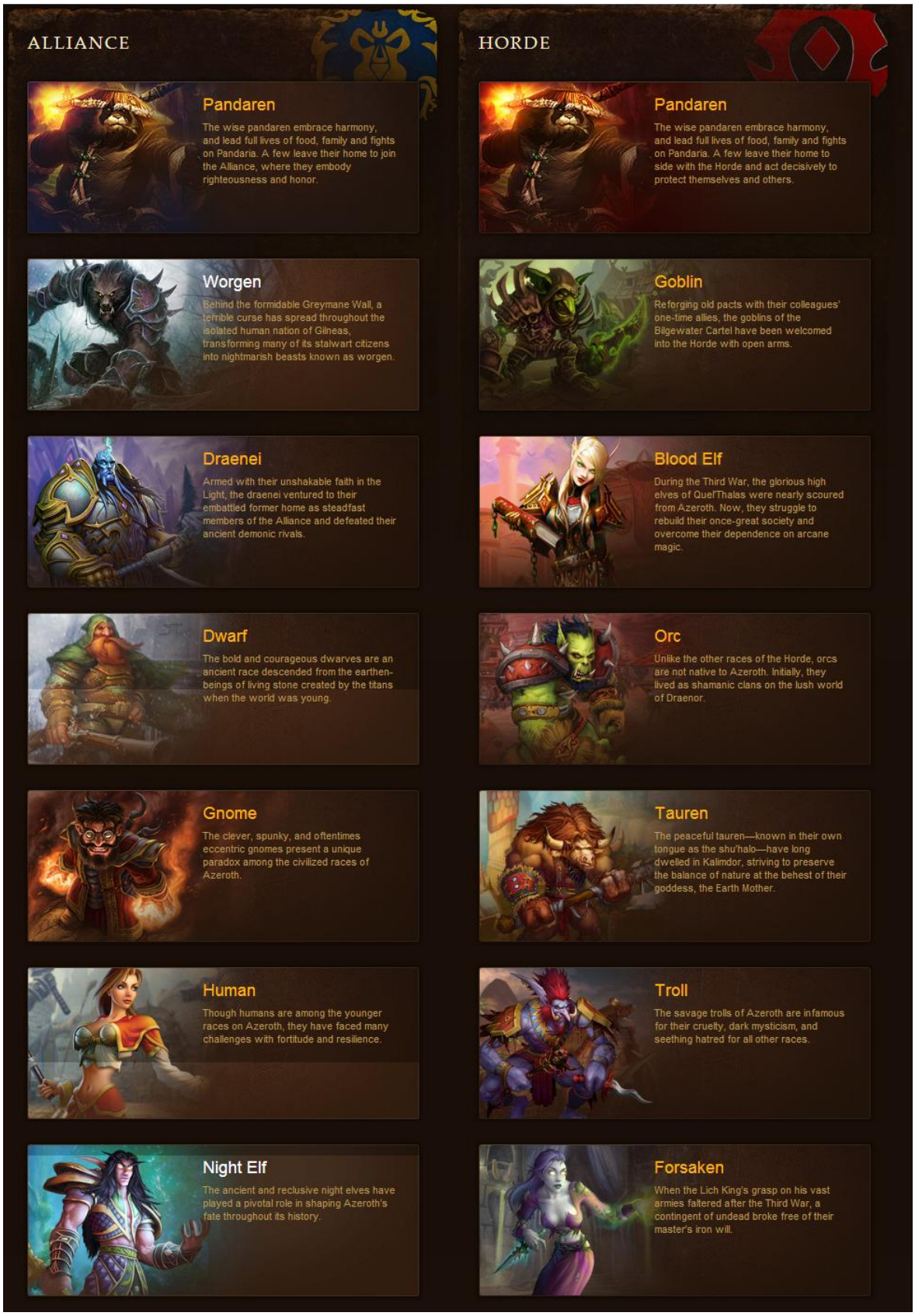

Figure 1: Image of World of Warcraft Races (Blizzard Entertainment, 2012c)

2.3 Battle.net

Battle.net is an online platform offered by Blizzard Entertainment. Its purpose is to bring all gamers together in a connected gaming community, and provide them with a user-friendly, consistent and fun online experience. Battle.net also gives the company a way to interact and support its players through direct digital sales, free trials, and value-added services. The current Battle.net supports StarCraft II, Diablo III and World of Warcraft (Activision Blizzard, 2011; Blizzard Entertainment, 2012b; "Battle.net," n.d.).

A Battle.net account is an email address and password registered to Battle.net, a centralised account system that enables gamers to organise their Blizzard games, transactions, and friend lists in one place. There is no fee or subscription for creating the Battle.net account (Blizzard Entertainment, 2012a). Battle.net contains three unique sections (Blizzard Entertainment, 2012b; "Battle.net," n.d.), including:

- The first section enables players to connect all Battle.net accounts, WoW characters and friends list together and integrated them into a unified single Battle.net account.
- The second section involves transforming Battle.net into a competitive platform for gamers, which involves a smart and accurate matchmaking system, simplifying the process of players managing games.
- The final section consists of the new chat system that is similar to Instant Messaging across all the Blizzard Entertainment's games. Players can communicate with friends across games, servers, and characters.

3. LITERATURE REVIEW

This section aims to conduct a literature review, understanding what has already been studied in the field and forming the foundation for the research (Hart, 1998).

3.1 Perceived Enjoyment

Perceived enjoyment has received considerable research attention for several years. The role of enjoyment has been studied in various e-commerce applications, such as instant messaging (Li, Chua, & Lou, 2005), blogging (Wang, Lin, & Liao, 2005), and online gaming (Wu & Liu, 2007). Online games are a genre of entertainment technology (Hsu & Lu, 2004), and the individuals' primary use of games is for entertaining and generating enjoyable experiences.

Prior research has given a working definition of perceived enjoyment. Davis, Bagozzi and Warshaw (1992, p.1113) refer to enjoyment as "the extent to which the activity of using the computer is perceived to be enjoyable in its own right, apart from any performance consequences that may be anticipated". This definition specifies the extent to which fun can be derived from using the system (Van der Heijden, 2004).

Perceived enjoyment is a strong determinant of adopting hedonic systems. Consumer behaviour researchers have studied the nature of product and consumption activities, and classify utilitarian and hedonic goods (Babin, Darden, & Griffin, 1994; Hirschman & Holbrook, 1982; Holbrook & Hirschman, 1982; Holt, 1995). In line with the consumer behaviour literature, Van der Heijden (2004) distinguishes between hedonic (or pleasured-oriented) and utilitarian (or productivity-oriented) information systems (IS). While hedonic systems are intended to offer self-fulfilling value and enable the user to have pleasurable experience, utilitarian systems are intended to offer instrumental value and help the user increase task performance and efficiency. Online games are a type of hedonic information systems, offering entertaining and playful services (Shin & Shin, 2011). Since hedonic systems focus on the fun experienced by users and encourage prolonged use, perceived enjoyment is an essential construct to be included in any model explaining the use of these information systems (Rosen & Sherman, 2006).

Perceived enjoyment is one of intrinsic motivation sources. Deci (1975), one of motivation theorists, distinguishes between the effects of extrinsic and intrinsic motivation on individual behaviours. The theory has also been utilised to explain individuals' technology acceptance behaviours (Davis, et al., 1992; Moon & Kim, 2001; Venkatesh, 2000). An extrinsically motivated user is driven by the anticipation of rewards external to the system-user interaction. An intrinsically motivated user is driven by benefits derived from the interaction with the system per se (Brief & Aldag, 1977; Van der Heijden, 2004). According to Davis et al. (1992, p.1113), perceived enjoyment is one of intrinsic motivators and "enjoyment will explain significant variance in usage intentions beyond that accounted for by usefulness alone". In the online gaming settings, most players tend to be motivated by intrinsic interests (Huang & Cappel, 2005; Kim, Park, Kim, Moon, & Chun, 2002). Players are involved in the activity for pleasure and enjoyment rather than extrinsic rewards.

3.2 Perceived Security

Although online games offer a new range of opportunities for player entertainment and experience, the lack of security has emerged as a critical issue in the virtual gaming environment. The idea has been criticised that security is not a major concern for gaming industry and there is no profit to gain (Schober, 2009). In fact, the virtual economies in gaming world are creating a new and real business, which generates significant revenue in terms of real money. Virtual characters and items have become virtual assets. Players can gain real money from trading their digital assets (Yan & Choi, 2002). Meanwhile, an attacker can have quick gains from stealing virtual assets from legitimate player, selling assets produced through exploits, leveraging the player's account as well as obtaining available payment information (Schober, 2009).

A number of security threats with online games are shared with other network applications (McGraw & Hoglund, 2007). Some security problems are generic to e-commerce applications but others are specific to online games (Yan & Choi, 2002). Byrne (2004) classifies eleven different types of online gaming security, consisting of copy protection, hacking the client, packet sniffing, social abuse, hacking accounts, denial of service, internal misuse, backup, cheat detection, disconnecting, and disciplinary measures. Ki et al. (2004) also create a classification of security problems based on attacks, objectives and methods. More importantly, they identify security

tools for virtual games, such as encryption, message authentication codes (MAC), and digital signature.

Security is viewed as a combination of objective and subjective concept. On the one hand, perceived security is defined as "a threat that creates a circumstance, condition, or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosures, and modification of data, denial of service, and/or fraud, waste and abuse" (Kalakota & Whinston, 1997, p.853). The security engineering approach, together with technical advancements, is capable of protecting users from security risks. The technical aspects of security issue ensure the integrity, confidentiality, authentication and non-recognition of relationships in the virtual world (Flavián & Guinaliu, 2006). On the other hand, Roca et al. (2009) point out that security in interactive spaces is not only dependent on technical security mechanisms. The perception of security is largely determined by users' feelings of control in a system (Kim, 2008). Subjective security can be interpreted as the mirror image of risk affinity (Dewan & Chen, 2005).

Three main reasons surface for studying enjoyment and security in this research. First, the impact of perceived enjoyment on individual's behavioural intention to play online games has been examined in a number of studies, but it has yet to be explored in the context of gaming security services, such as account protection technology. Players experience with service mechanisms offered after they have played an online game including fairness, security, and incentives (Wu, Wang, & Tsai, 2010), which could also affect their enjoyment perceived and continued motivation to play. Second, the role of enjoyment has a stronger effect on the use of hedonic systems, but not that of utilitarian systems (Van der Heijden, 2004). With the newly emerging IT, the boundary between hedonic and utilitarian systems is blurring, such as the Internet (Moon & Kim, 2001; Van der Heijden, 2004). Additional research is needed to examine enjoyment in information systems mixed of utilitarian and hedonic nature. Third, the account protection technology is one of those security services offered by online publishers, which technically make players' accounts safer. However, individuals' perceptions of security can differ from real security levels (Shin & Shin, 2011), In other words, the level of perceived security could rely on how strongly a player believe in the security of a specific online game.

4. THEORETICAL FRAMEWORK

Since IT grows rapidly, user acceptance of technology has become a significant field of study. Lack of users' willingness to accept and use new systems is often impeding performance gains and implementation success (Bowen, 1986; Davis, 1993; Young, 1984). Among a number of models proposing to explain and predict system use, the Technology Acceptance Model (TAM) is in fact a highly cited model, capturing the most attention of the IS community (Chuttur, 2009).

4.1 Technology Acceptance Model

TAM, proposed by Davis (1986) in his doctoral thesis, is an IS theory that models how individuals come to accept and use a technology ("Technology acceptance model," n.d.). TAM studies the determinants of IS and IT acceptance to predict behavioural intention of users (Chen, Li, & Li, 2011), explaining why users accept or reject a new technology and how user acceptance is affected by system design features (Davis, 1993).

Derived from the theory of reasoned action (TRA) by Fishbein and Ajzen (1975), TAM (Figure 2) is specifically meant to explain computer usage behaviour (Davis, Bagozzi, & Warshaw, 1989). The model posits that user perception of usefulness and ease of use determines behavioural intention toward using the system. Perceived usefulness was defined as "the degree to which a person believes that using a particular system would enhance his/her job performance", and perceived ease of use is defined as "the degree to which a person believes that using a particular system would be free of physical and mental effort" (Davis, 1989, p. 320).

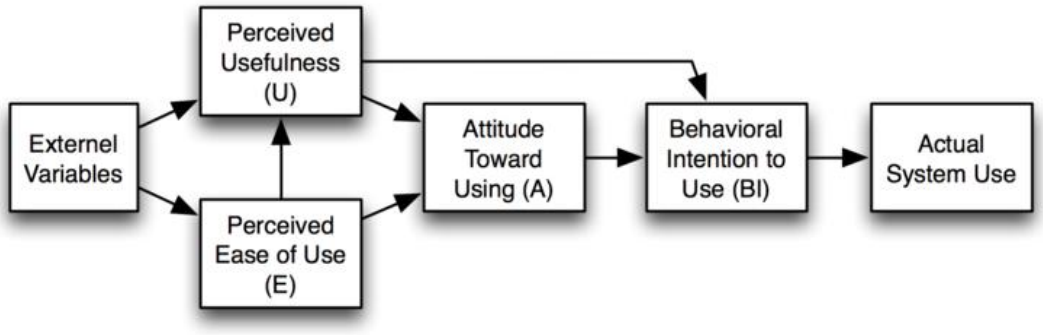

Figure 2: Technology Acceptance Model (Davis et al., 1989)

According to TAM, both perceived usefulness and ease of use positively influence the attitude towards a particular technology usage while attitude and perceived usefulness predict the individuals' behavioural intention to use IT. Also, perceived ease of use positively affects the usefulness whereas both perceived ease of use and usefulness are affected by external variables. Finally, behavioural intention to use IT is expected to lead to actual usage (Davis, 1989; Davis, et al., 1989; Roca, et al., 2009).

Compared to TRA (Fishbein & Ajzen, 1975), TAM provides a much simpler and less expensive method to implement (Chuttur, 2009). TAM replaces many of TRA's attitude measures with the two technology acceptance measures – perceived ease of use and perceived usefulness. It does not include TRA's subjective norm as a determinant because Davis et al. (1989) discover that there is very little correlation between the subjective norm and the behavioural intention variables. While TRA is a general model used across a variety of subject areas, TAM is more appropriately applied in the context of IS and IT (Chen et al., 2011).

4.2 Evolving Technology Acceptance Model

Many studies of user IT acceptance have validated the model empirically (Mathieson, 1991; Venkatesh & Davis, 2000; Venkatesh, Morris), and the original TAM has been continuously modified and expanded. There are two major upgrades, which are TAM 2 (Venkatesh 2000; Venkatesh & Davis 2000) and UTAUT (Unified Theory of Acceptance and Use of Technology) (Venkatesh et al., 2003). One of modified models by Venkatesh and Davis (1996) suggests that both perceived usefulness and perceived ease of use are found to directly influence behavioural intention to use IT, which leads to eliminate the need for the attitude construct from the model. Thus, as shown in Figure 3, the evolving TAM drops the attitude construct.

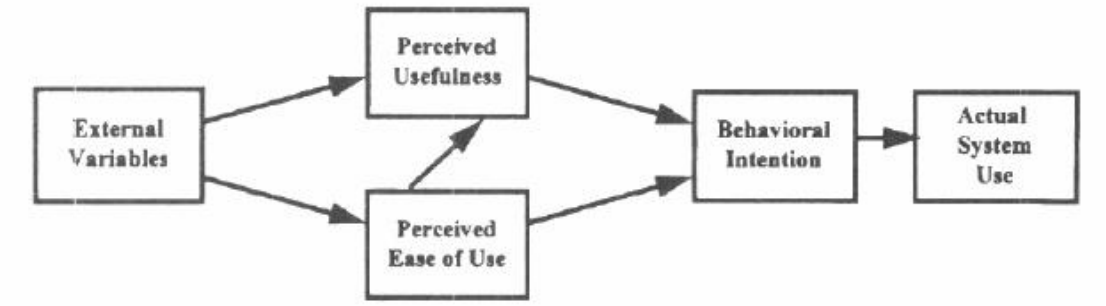

Figure 3: Evolving Technology Acceptance Model (Venkatesh & Davis, 1996)

5. RESEARCH MODEL AND HYPOTHESES

Drawing upon the prior empirical findings and theoretical framework, Figure 4 graphically represents the initial research model underpinning this study. The model is an extension of Davis' TAM, which includes perceived enjoyment and perceived security as constructs influencing player acceptance of account security technology while playing online games. The following section elaborates on the constructs that make up the model and the proposed relationships among them.

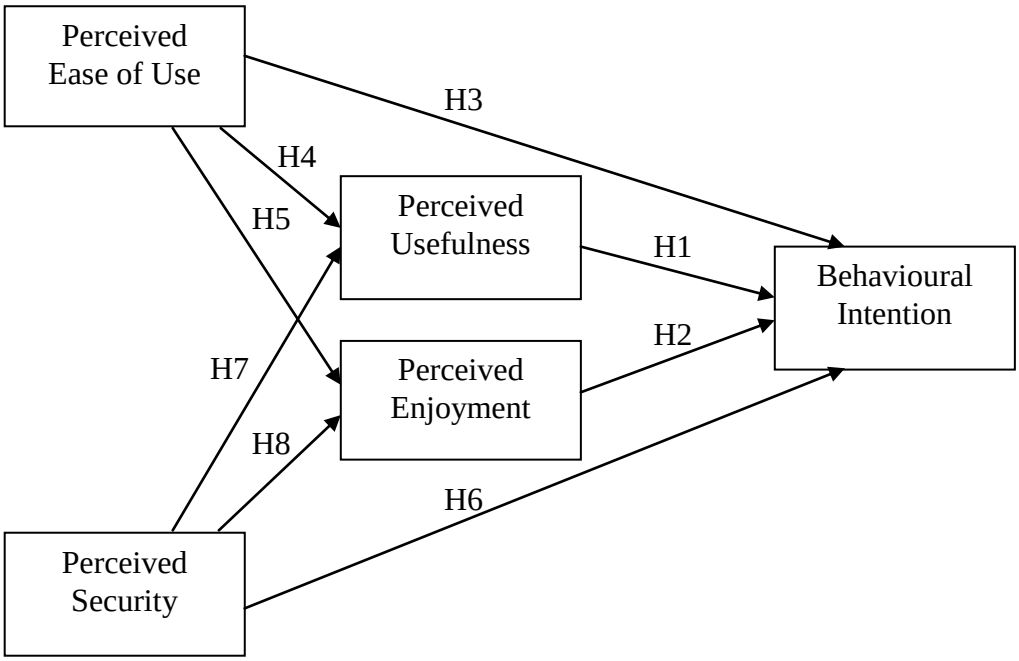

Figure 4: Research Model

TAM researchers have validated that the construct of perceived usefulness is the basis for predicting end-user acceptance of computer technology (Davis, 1989; Davis et al., 1989). Of the two TAM variables, perceived usefulness has been found to have the strongest influence (Davis, 1989). TAM originates from the study of IS that increase productivity in the workplace environment (Van der Heijden, 2004). The current study explores perceived usefulness in the home or entertainment environment, highlighting the aspect described as capable of being used advantageously (Shin & Shin, 2011). Thus, the following hypothesis is proposed:

Hypothesis 1: *There is a positive influence of perceived usefulness on the intention to use account protection technology in the online gaming context.*

The household environment is the natural habitat of hedonic information systems. Since the value of hedonic systems is the fun experienced by users, perceived enjoyment is believed to play a more dominant role (Rosen & Sherman, 2006; Van der Heijden, 2004). Enjoyment can be derived from using the system, and is perceived to be personally enjoyable in its own right aside from the instrumental value of the technology (Shin & Shin, 2011). In the context of networked games, perceived enjoyment has been extensively proven as a major intrinsic motivation factor (Huang & Cappel, 2005; Kim et al., 2002; Wu & Liu, 2007). In addition, service mechanisms are claimed to significantly affect players' continued motivation to play, which is crucial to their proactive stickiness to an online game (Wu et al., 2010). Hence, the hypothesis is proposed as following:

Hypothesis 2: *There is a positive influence of perceived enjoyment on the intention to use account protection technology in the online gaming context.*

Perceived ease of use is another main construct in TAM by Davis (1989). It is an assessment of the mental effort involved in the use of IS or IT. Extensive empirical literature has demonstrated that perceived ease of use is important in determining the individuals' behavioural intention to use a system (Davis et al, 1989; Keil, Beranek, & Konsynski, 1995; Venkatesh, 2000), and positively influence intention indirectly through perceived usefulness (Roca et al., 2009; Rosen & Sherman, 2006). According to Van der Heijden (2004), the role of perceived ease of use is more central to the prediction of intention to use hedonic systems than perceived usefulness. Perceived ease of use is related to the enjoyment of interacting with computer systems (Moon & Kim, 2001). Therefore, this leads to the following hypotheses:

Hypothesis 3: *There is a positive influence of perceived ease of use on the intention to use account protection technology in the online gaming context.*
Hypothesis 4: *Perceived ease of use has a positive effect on perceived usefulness of account protection technology in the online gaming context.*
Hypothesis 5: *Perceived ease of use has a positive effect on perceived enjoyment of account protection technology in the online gaming context.*

Security problems are a major obstacle to e-commerce development, preventing the adoption of online trading practices (Roca et al., 2009). Critical security flaws and mass-cheating can ruin a good online game, resulting in players giving up (Byrne, 2004; Yan & Choi, 2002). Security service mechanisms provided by online game publishers have a positive influence on players' continuance motivation to play online games (Wu et al., 2010). From a broad perspective, perceived security involves both technical mechanisms and users' comprehensive sense of security and well-being (Shin & Shin, 2011). The online games that have the ability to perform expected activities, such as security services, will make players feel and believe the safety of their account when interacting with online games (Wu & Liu, 2007). On the one hand, security threats could reduce the playability of online games (Wu et al., 2010). On the other hand, players' enjoyment of games could also dwindle when security services restrict player access to certain data to protect information confidentiality, integrity system availability and application from manipulation or contamination (Chang & Chen, 2009). So the following hypotheses are proposed:

Hypothesis 6: *There is a positive influence of perceived security on the intention to use account protection technology in the online gaming context.*
Hypothesis 7: *Perceived security has a positive effect on perceived usefulness of account protection technology in the online gaming context.*
Hypothesis 8: *Perceived security has a negative effect on perceived enjoyment of account protection technology in the online gaming context.*

6. RESEARCH METHODOLOGY

To validate the proposed model and hypotheses discussed above, this research study employed a survey method. In this section, the research methodology is presented including a discussion of epistemology guiding the study, survey design, and data collection method applied.

6.1 Epistemology

When discussing methodology, it is often significant to look at another intimately related notion: epistemology. According to Trochim (2006), epistemology is the philosophy of knowledge or of how people come to know the world. Methodology is focused on the specific ways or the methods that people can use to try to understand the world better. All research is based on assumptions about how the world is perceived and how people can best come to understand it. Easterby-Smith, Thorpe and Lowe (1997) claim that the exploration of research philosophy can assist researchers to understand the interrelationship of key elements of study, and clarify the overall research strategy applied.

In the broader context of research philosophy, positivism and post-positivism are two core philosophical traditions. As one of positivists Comte (1853) puts it, all authentic knowledge should be obtained from human observation of external world. The positivist philosophy claims that truth depends on the belief which can be verified through examination and observation of objective reality (Crossan, 2003). Positivism is traditionally regarded as one of scientific approaches to research. Positivism focuses on measurement and objectivity, leading to the quantitative design (Williamson, 2006). This research study maintained a positivist position, and was aiming at validating the constructs of perceived enjoyment and security jointed with traditional technology acceptable model. A quantitative research was selected as it was considered to be most suitable for collecting objective and measurable data.

6.2 Instrument Development

This survey was developed base upon the proposed research model (Figure 4). It adapted the questions for the context of online game WoW and account security technology, and added a series of baseline questions to establish demographic covariates for each respondent. Demographic questions utilised the appropriate

response categories for questions about gender, age, ethnography, and gaming experiences, etc. The core segment of the questionnaire consisted of 3 questions about individual perception of usefulness, 3 questions about individual perception of enjoyment, 2 questions regarding individual perception of ease of use, and 5 questions regarding individual perception of security. These questions were then followed by an open-ended question about players' experience with the account security technology.

The measures used in this study were mainly adapted from relevant prior research studies. Respondents were asked to rate each item on a five-point Likert-type scale, where one meant "completely disagree" and five meant "completely agree". Items measuring for perceived usefulness and ease of use were adapted from prior work by Davis (1993). Items for perceived enjoyment were derived from prior research by Van der Heijden (2004). Scales of perceived security was measured by items adapted from prior studies by Shin and Shin (2011) as well as Roca et al. (2008). A full version of the survey can be found in the Appendix A.

6.3 Data Collection

For the purpose of this research study, the population of interest was individuals who played the online game WoW across the world. A web-based survey questionnaire was built using Google Forms, an online free and collaborative survey tool. The online survey was employed for this research based on the nature of both the online players and the Internet. Bhattacherjee (2001) claims that the advantages of online surveys outweigh traditional paper-based mail-in surveys, because (1) participants are not restricted by geographic location, (2) lower costs, and (3) faster response.

Subjects were self-selected via messages with research purpose, the Participator Information Sheet (Appendix B) and a hyperlink to the survey form, placed on numerous game-related online forums. Each participant was required to answer each question in the online survey system. The data were gathered from the survey engine in the form of individual survey responses, formatted in Excel Spreadsheets, and subjected to statistical analysis. The anonymous online survey ran between 23th December 2012 and 11th January 2013, and a total of 99 questionnaires were received and used for analysis.

7. DATA ANALYSIS AND RESULTS

This section provides an analysis of data gathered by means of a questionnaire, and is divided into the following areas: analysis of demographics, validation of measurement model, as well as test of proposed model and hypotheses.

7.1 Demographic Analysis

Among the 99 responses recorded by the online survey tool, two of them were discarded due to invalid data. This left 97 usable questionnaires for analysis, giving a response rate of 97.98%. Detailed statistics relating to the characteristics of the respondents are shown in Table 1.

Of the respondents, 59.79% were male and 40.21% were female. The figure for male players is slightly higher than that for females, as presented in Figure 5. Ages of the respondents ranged between 15 and 67, with the average age of the respondents being 25.41. Figure 6 illustrates that majority of the respondents were from the 20-29 years age group, followed by the age groups of 15-19 and 30-39 years old. The data shows that the respondents were from thirteen different countries or regions. Over half of them stated their country of origin was USA. Figure 7 presents the number of the respondents clustered by continents, and ranking from the highest to lowest is North America, Asia, Australasia, Europe and Africa.

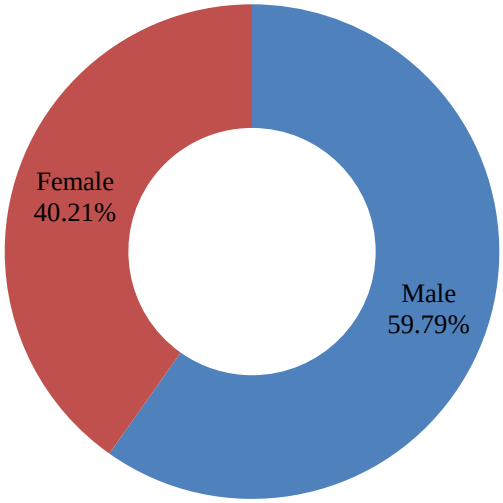

Figure 5: Gender Division of Respondents

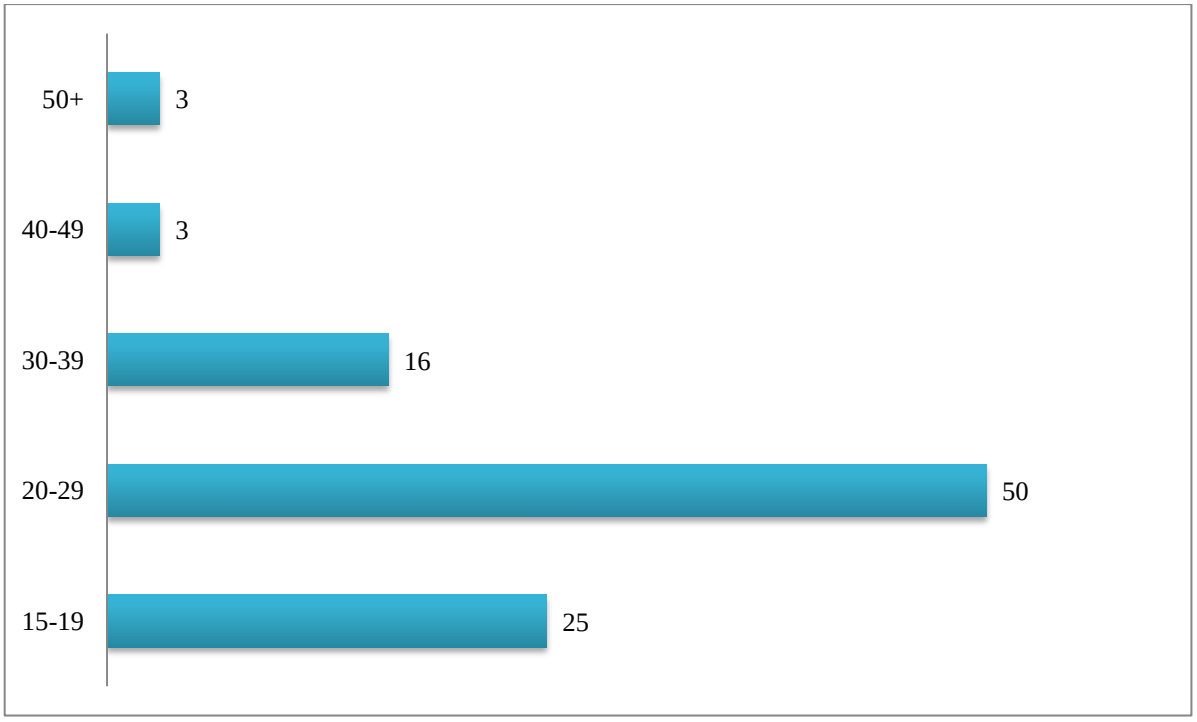

Figure 6: Age Bands of Respondents

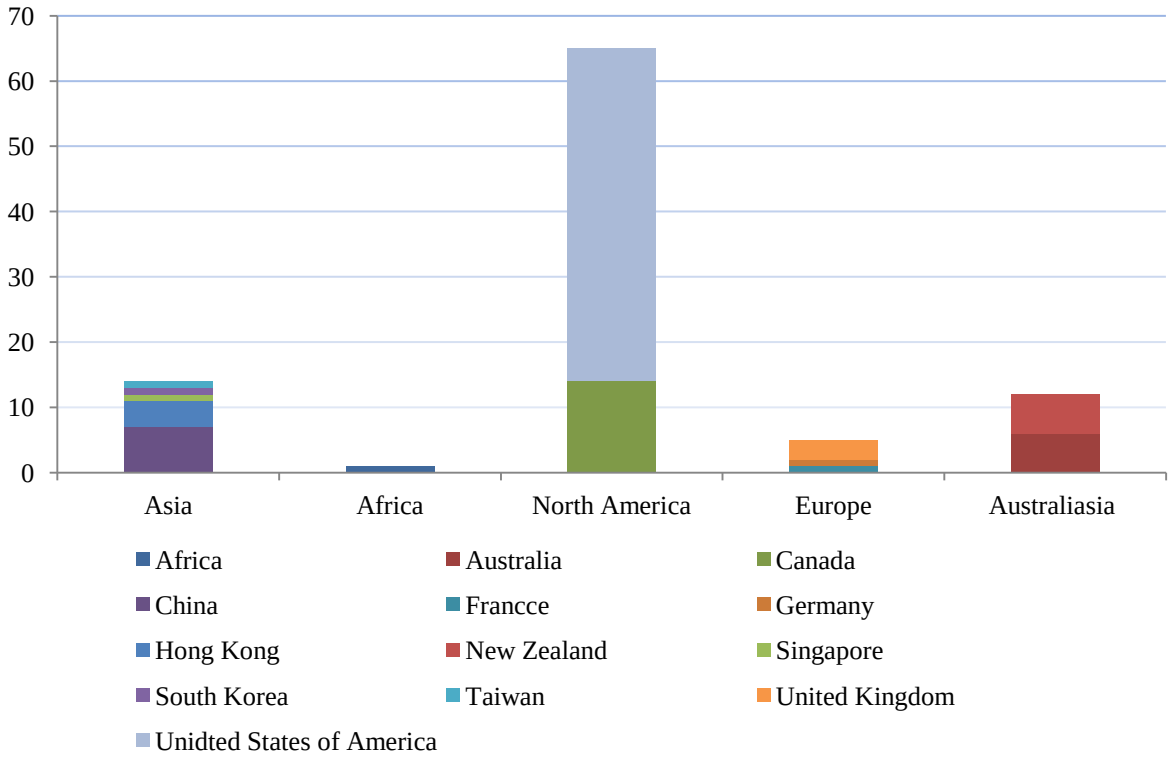

Figure 7: Respondents' Country of Origin by Continents

Table 1: Demographic Profile

Measure	Items	Frequency	Percent
Gender	Male	58	59.79%
	Female	39	40.21%
Age	15-19	25	25.77%
	20-29	50	51.55%
	30-39	16	16.49%
	40-49	3	3.09%
	50+	3	3.09%
Country of origin	Africa	1	1.03%
	Australia	6	6.19%
	Canada	14	14.43%
	China	7	7.22%
	France	1	1.03%
	Germany	1	1.03%
	Hong Kong	4	4.12%
	New Zealand	6	6.19%
	Singapore	1	1.03%
	South Korea	1	1.03%
	Taiwan	1	1.03%
	United Kingdom	3	3.09%
	United States of America	51	52.58%
Seniority of playing World of Warcraft	0-6 months	14	14.43%
	6-12 months	12	12.37%
	1-3 years	18	18.56%
	3-5 years	16	16.49%
	5-8 years	37	38.14%

Measure	Items	Frequency	Percent
Times of WoW account accessed by an unauthorised third party	Never	55	56.70%
	Once	22	22.68%
	Twice	14	14.43%
	Three Times	4	4.12%
	Four times or more	2	2.06%
Types of Battle.net security technology*	Battle.net SMS Protect	42	28.57%
	Keychain Authenticator sold in Blizzard Store	43	29.25%
	Mobile Authenticator on Google Play	7	4.76%
	Mobile Authenticator on iTune App Store	32	22.22%
	Mobile Authenticator on BlackBerry AppWorld	1	0.65%
	Mobile Authenticator on Zune	0	0
	None of them	22	14.97%

***** Note that the total of Battle.net security technologies adopted is larger than the overall number of respondents, because one player can choose multiple tools.

As to the degree of WoW gaming experience, 38.54% respondents had been playing between 5 and 8 years, who could be seen as devoted players considering the game WoW being online for over eight years. From Figure 8 it can be seen the rest of respondents playing from a few days to six months, half to a year, one to three years, as well as three to five years were relatively even. Moreover, 56.71% of the respondents stated that their accounts had never been accessed by an unauthorized third party whereas remaining 43.29% had their accounts hacked for a different number of times (Figure 9). Finally, while 77.32% of the respondents used Blizzard Entertainment's account security technology, 22.68% of them had not adopted any of the listed Battle.net security technology. In addition, the respondents were able to select more than one account protection mechanisms. As illustrated in Figure 10, 10.31% of the respondents used three different tools to protect WoW accounts and 31.96% of them adopted two approaches.

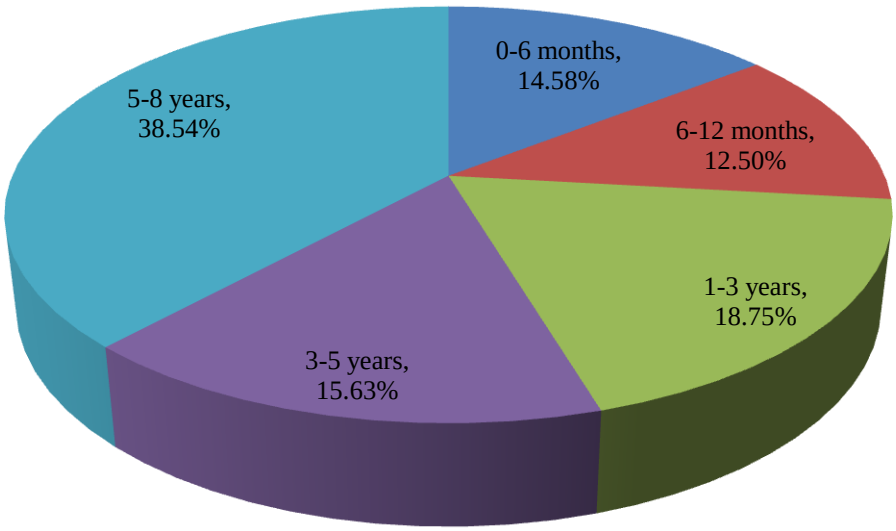

Figure 8: Seniority of WoW Playing Division of Respondents

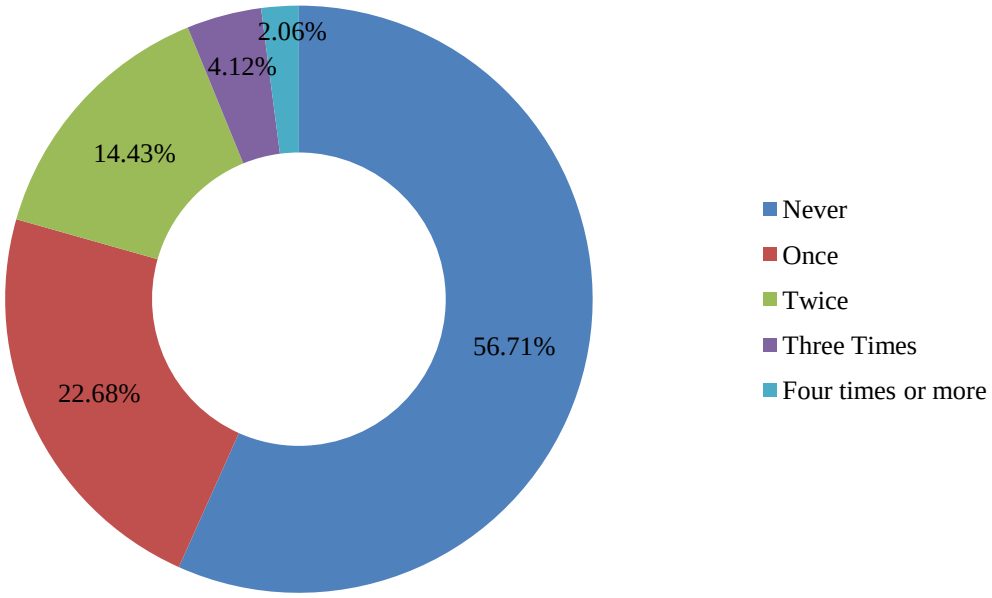

Figure 9: Account Hacked Frequency Division of Respondents

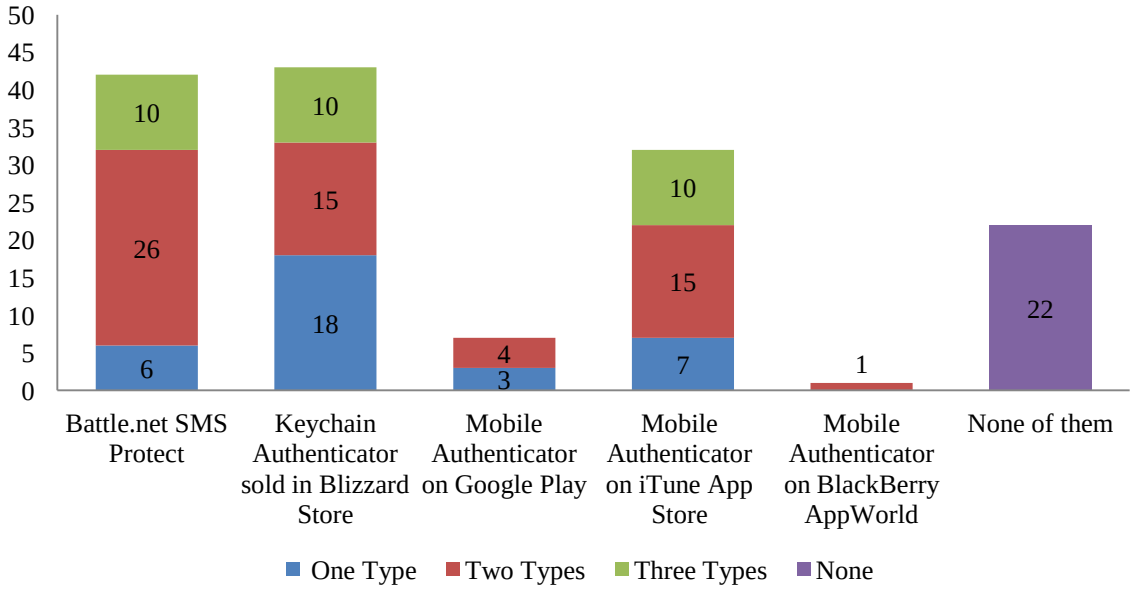

Figure 10: Types of Battle.net Security Technology Adopted by Respondents

7.2 Measurement Model Assessment

All of the measures in this study are based upon the constructs that were previously validated and were considered reliable. Furthermore, the acceptability of the measurement model was examined in terms of reliability and validity.

Reliability refers to the extent a measuring procedure yields consistent results on repeated trials (Miller, 2003). The purpose for testing the reliability of a construct is to ensure that part containing no purely random error (Carmines & Zeller, 1979). In the present study, Cronbach's alpha was selected to evaluate the degree of consistency among the items in each measure. Hair, Anderson, Tatham and Black (1998) have indicated 0.7 to be an acceptable reliability coefficient. As summarised in Table 2, all the measures had a value above the suggested threshold value, which demonstrated adequate construct reliability.

Validity refers to the extent a measuring procedure accurately assesses or captures the specific concept that it purports to measure (Miller, 2003). Convergent validity can be employed to evaluate that each construct correlates positively with its own measures than to those of other constructs (Wu et al., 2010). As presented in Table 2, convergent validity was demonstrated as the average variance extracted (AVE) for all constructs exceeded the suggested threshold value of 0.50 (Fornell & Larcker, 1981). Also, discriminant validity can be used to assess how much a concept and its indicator variables do not correlate with other conceptually distinct construct (Shin & Shin, 2011). Discriminant validity was checked that the square root of the AVE was higher than the correlation shared between the construct and any other construct in the model. The low correlations are evidence for validity (Fornell & Larcker, 1981).

Table 2: Summary Statistics for Cronbach's Alpha and AVE

	Cronbach's α	***AVE***
Perceived Usefulness	0.95	0.89
Perceived Enjoyment	0.83	0.81
Perceived Ease of Use	0.89	0.67
Perceived Security	0.70	0.68
Behavioural Intention	0.85	0.82

7.3 Hypothesis Testing

In order to test the proposed model, a quantitative analysis technique was applied to examine the six hypothesised causal relationships. Table 3 shows the results for the questionnaires from question number seven to nineteen, which were measured by means of a 5 point Likert Scale.

Table 3: Summary of Survey Question 7-19 Results

	1- Completed Disagree		2- Mostly Disagree		3- Neither Agree nor Disagree		4- Mostly Agree		5- Completely Agree	
	#	%	#	%	#	%	#	%	#	%
Q7	5	5.15%	2	2.06%	18	18.56%	41	42.27%	31	31.96%
Q8	4	4.12%	1	1.03%	26	26.80%	44	45.36%	22	22.68%
Q9	4	4.12%	3	3.09%	18	18.56%	36	37.11%	36	37.11%
Q10	15	15.46%	6	6.19%	52	53.61%	20	20.62%	4	4.12%
Q11	3	3.09%	1	1.03%	38	39.18%	40	41.24%	15	15.46%
Q12	5	5.15%	2	2.06%	32	32.99%	40	41.24%	18	18.56%
Q13	1	1.03%	1	1.03%	22	22.68%	46	47.42%	27	27.84%
Q14	2	2.06%	3	3.09%	20	20.62%	42	43.30%	30	30.93%
Q15	4	4.12%	1	1.03%	14	14.43%	61	62.89%	17	17.53%
Q16	4	4.12%	18	18.56%	19	19.59%	40	41.24%	16	16.49%
Q17	5	5.15%	3	3.09%	21	21.65%	56	57.73%	12	12.37%
Q18	6	6.19%	7	7.22%	14	14.43%	25	25.77%	45	46.39%
Q19	2	5.15%	4	3.09%	15	21.65%	48	57.73%	28	12.37%

H1: *There is a positive influence of perceived usefulness on the intention to use account protection technology in the online gaming context.*

Q7. I feel using Battle.net Authenticator and/or SMS Protect gives me greater control over my World of Warcraft account security management.

Q8. I feel using Battle.net Authenticator and/or SMS Protect makes it easier to do the World of Warcraft account security management.

Q9. Overall, I think the Battle.net Authenticator and/or SMS Protect are useful to me.

Question 7, 8 and 9 were designed to measure how useful the account security technology was from the view of WoW players. Figure 11 shows that 74.23% of the respondents rated 4 or 5 (mostly or completely agree) for Q7, 68.04% for Q8, and 74.22% for Q9. On the other side of Likert Scale, 7.21% respondents selected 1 or 2 (completely or mostly disagree) for Q7, 5.15% for Q8, and 7.21% for Q9. This indicates majority of the respondents believed using the tools would enhance account security management. Moreover, 63.92% respondents agreed with question 7, 8 and 9, and they all used security mechanisms. For those 10 respondents who used three different kinds of protection technology, they also agreed with all three questions. The results stress the vital role of usefulness in determining players' intention to use account protection technology in online gaming context, supporting H1.

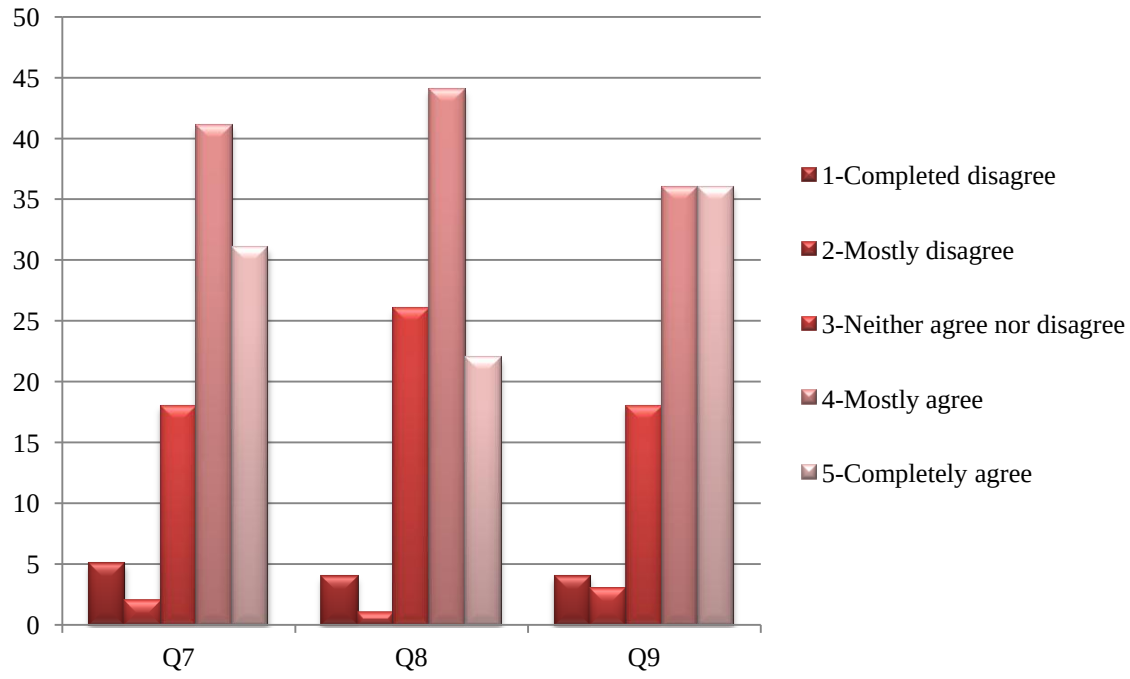

Figure 11: Results of Five Point Likert Scale Question 7, 8 and 9

H2: *There is a positive influence of perceived enjoyment on the intention to use account protection technology in the online gaming context.*

Q10. I feel using Battle.net Authenticator and/or SMS Protect is enjoyable and fascinating.

Q11. I had a pleasant experience from the Battle.net Authenticator and/or SMS Protect.

Q12. Overall, I enjoy using Battle.net Authenticator and/or SMS Protect.

Question 10, 11 and 12 attempted to assess the extent of pleasure and enjoyment players perceived with the account security mechanism. From Figure 12, no distinct difference was observed among respondents who agreed or disagreed with Q10, with 24.74% rating 4 or 5, and 21.65% rating 1 or 2. Over half respondents chose not to agree or disagree with Q10. Apparently, they did not consider Battle.net Authenticator and/or SMS Protect as enjoyable. Nevertheless, 56.70% and 59.79% of the respondents agreed with Q11 and Q12 whereas 4.12 % and 7.22% expressed disagreement with two questions. This reflected that more than half of them enjoyed using the tools and had pleasurable experiences. In addition, 50.52% respondents mostly or completely agreed with both Q11 and Q12. All of them used at least one type of the security tool. For those 22 respondents who did not use any tools, their rating was either 1 or 3 for Q10, Q11 and Q12. This is consistent with Hypothesis 2.

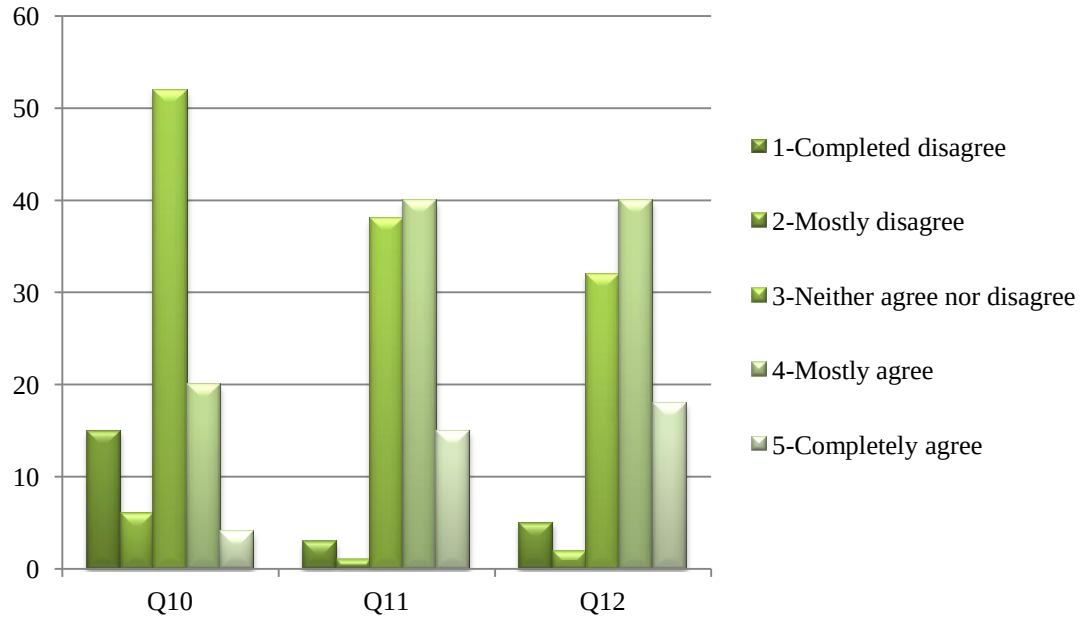

Figure 12: Results of Five Point Likert Scale Question 10, 11 and 12

H3: *There is a positive influence of perceived ease of use on the intention to use account protection technology in the online gaming context.*

Q13. My interaction with the Battle.net Authenticator and/or SMS is clear and understandable.

Q14. Overall, I find the Battle.net Authenticator and/or SMS Protect easy to use.

Question 13 and 14 were designed to evaluate the Battle.net Authenticator and SMS Protect in terms of ease of use. As Figure 13 presented, 75.26% and 74.23% of the respondents mostly or completely agreed with Q13 and Q14, whereas only 2.06% and 5.15% mostly or completely disagreed with them. Among the respondents who mostly or completely agreed with both Q13 and Q14, 70.10% adopted the account security tools. Consistent with Hypothesis 3, perceived ease of use has a positive impact on intention to use account protection technology while playing online game.

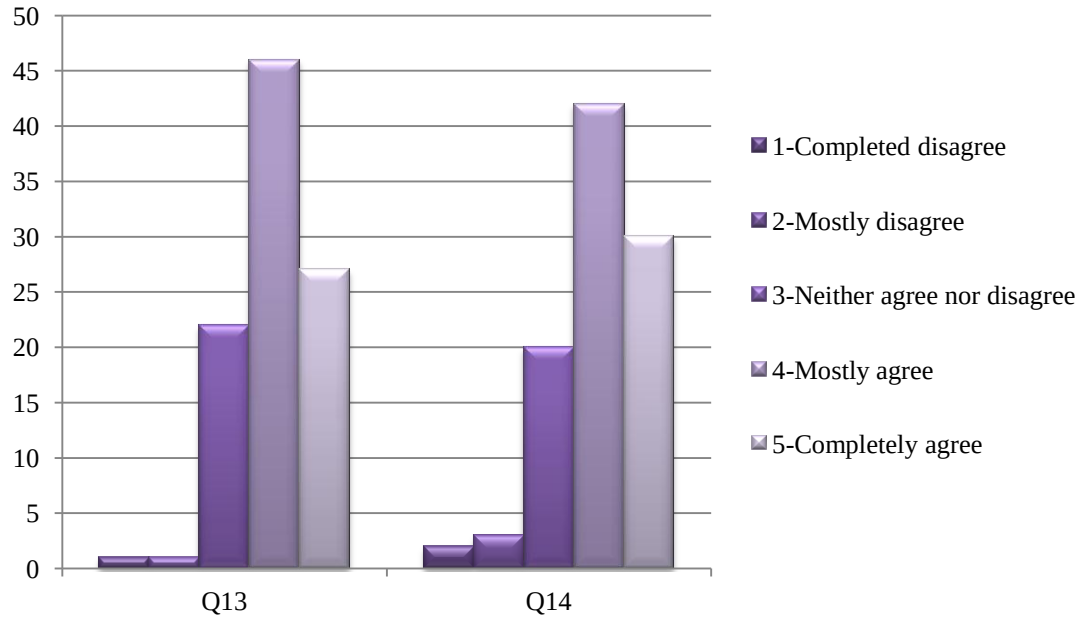

Figure 13: Results of Five Point Likert Scale Question 13 and 14

H4*:* *Perceived ease of use has a positive effect on perceived usefulness of account protection technology in the online gaming context.*

To test this hypothesis, the results of Q9, Q13 and Q14 were combined together and examined. Of the respondents who considered the account protection tools as clear, understandable and easy to use, 95.59% also thought the tools were useful. All the respondents, who mostly or completely disagreed with Q13 and Q14, also disagreed with Q9 that the account protection technologies were useful to them. Thus, there is a positive influence of perceived ease of use on perceived usefulness of account security technology in the context of online gaming, as Hypothesis 4 stated.

H5*:* *Perceived ease of use has a positive effect on perceived enjoyment of account protection technology in the online gaming context.*

Firstly, the results of Q13 and Q14 were studied along with that of Q11. Of the respondents who rated 4 or 5 for both Q13 and Q14, 70.59% mostly or completely agreed they had a pleasant experience with security protection technology while none of them disagreed with it. Secondly, by considering the results of question 12, 13 and 14, 76.47% of the respondents rating 4 or 5 for both Q13 and Q14, mostly or completely agreed they enjoyed using the tools. Those disagreeing with both Q13 and Q14, also completely disagreed with Q12. The results support Hypothesis 5 that perceived ease of use has a positive impact on perceived enjoyment of account security technology while playing online games.

H6*: There is a positive influence of perceived security on the intention to use account protection technology in the online gaming context.*

Q15. I am confident that my World of Warcraft account information with the game company Blizzard Entertainment is secured.

Q17. The Battle.net Authenticator and/or SMS Protect offered by the game company Blizzard Entertainment has enough security measures to protect my World of Warcraft account information.

Q19. Overall, using Battle.net Authenticator and/or SMS Protect reduces the security risks of my World of Warcraft account.

Question 15, 17 and 19 were designed to measure the safety level WoW players perceived by using the security services. Figure 14 shows 80.14% of the respondents mostly or completely agreed with Q15 that their accounts with the game company were safe. For Q17, 70.10% respondents agreed (rated 4 or 5) that the game company offered sufficient security measures while only 8.25% disagreed (rated 1 or 2). For Q19, 78.35% of them agreed that Battle.net Authenticator and SMS Protect reduced security threats while just 6.19% disagreed. The results suggested that most respondents felt safe with security mechanisms offered by the online game publisher. Of those who selected 4 or 5 for all the three questions, 94.64% respondents used the account protection mechanism. This supports Hypothesis 6.

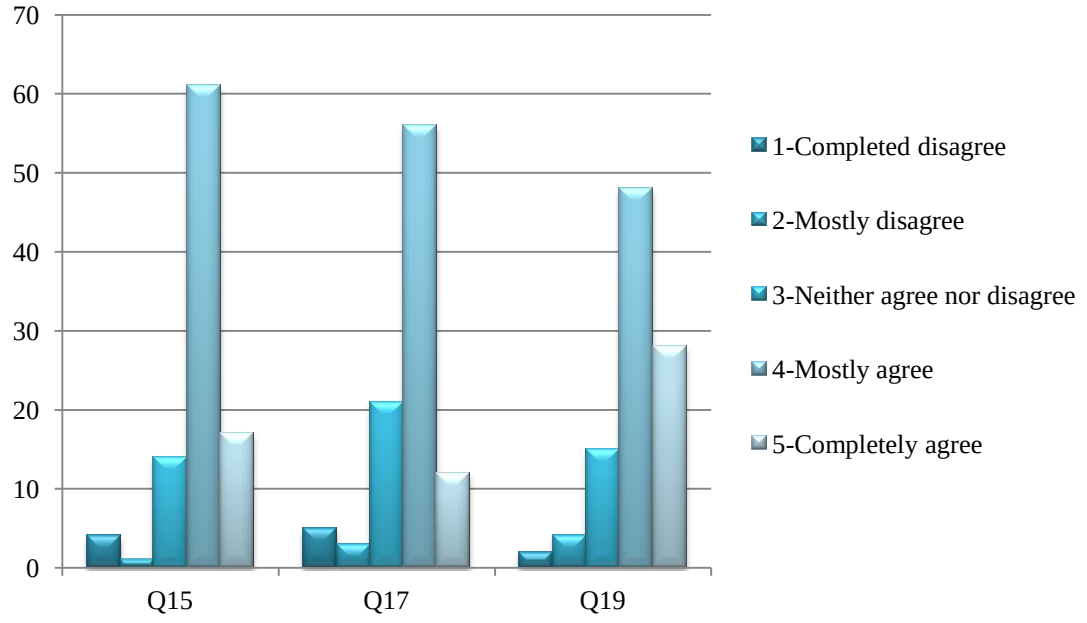

Figure 14: Results of Five Point Likert Scale Question 15, 17 and 19

H7*:* *Perceived security has a positive effect on perceived usefulness of account protection technology in the online gaming context.*

Q16. I feel that unauthorised third parties may still deliberately access my World of Warcraft, whether I am using the Battle.net Authenticator and/or SMS Protect or not.

To test this hypothesis, the results of question 15, 16, 17 and 19 were investigated. Question 16 attempted to assess whether respondents felt the increased account security level with the use of security technology (Figure 15). Among the respondents who perceived high level of security (rated 4 or 5 for Q15, Q17 and Q19), 26.70% agreed that unauthorised third parties might not access their accounts after applying the security technology whereas 57.14% thought their accounts could still be hacked. Inconsistent with Hypothesis 7, players' perceived usefulness of account security mechanisms is apparently not affected by perceived security.

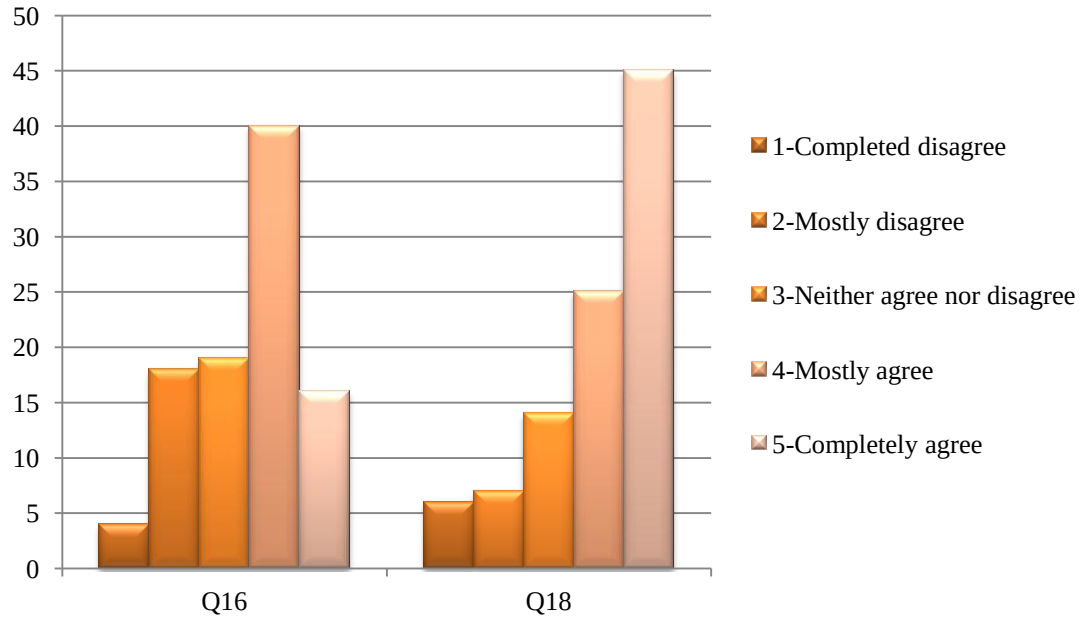

Figure 15: Results of Five Point Likert Scale Question 16 and 18

H8*:* *Perceived security has a negative effect on perceived enjoyment of account protection technology in the online gaming context.*

Q18. Using the Battle.net Authenticator and/or SMS Protect to keep my World of Warcraft account safe is more important than having fun.

Question 18 was intended to measure how WoW players weighed between account security and playing enjoyment. While 72.16% of the respondents believed using protection technologies to keep their accounts safe was more significant than having fun (rated 4 or 5 for Q18), only 13.40% thought enjoyment was more important (rated 1 or 2 for Q18), as shown in Figure 15. Additionally, Figure 16 illustrates the trend between the number of times account being illegally accessed (Q3) and the extent of enjoyment by using security tools (Q12). It seems that the ratio of respondents whose accounts had been accessed by unauthorised third parties for over three times enjoyed using security technologies more than the others, which rejects Hypothesis 8.

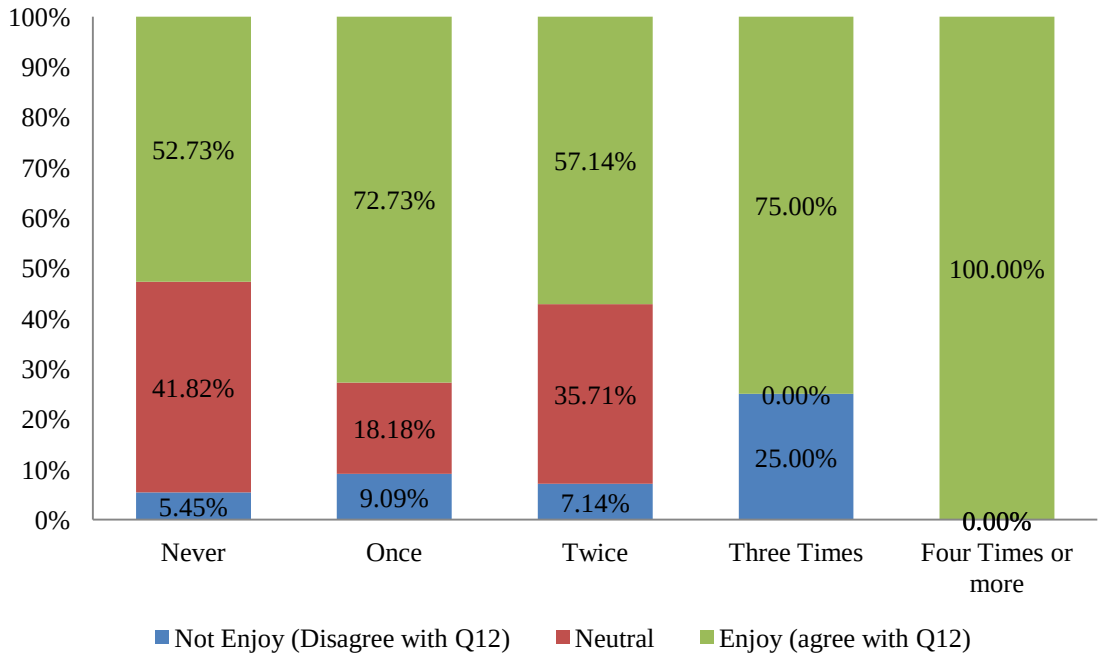

Figure 16: Account Hacked Frequency and Enjoyment of Tool Usage

To summarise, six of the eight hypotheses are supported as shown in the Table 4, and the proposed research model has been modified and presented in Figure 17.

Table 4: Summary of Hypothesis Test Results

Hypothesis	Causal Path	Expected Sign	Support
H1	Usefulness → Intention to Use	+	Yes
H2	Enjoyment → Intention to Use	+	Yes
H3	Ease to Use → Intention to Use	+	Yes
H4	Ease to Use → Usefulness	+	Yes
H5	Ease to Use → Enjoyment	+	Yes
H6	Security → Intention to Use	+	Yes
H7	Security → Usefulness	+	No
H8	Security → Enjoyment	-	No

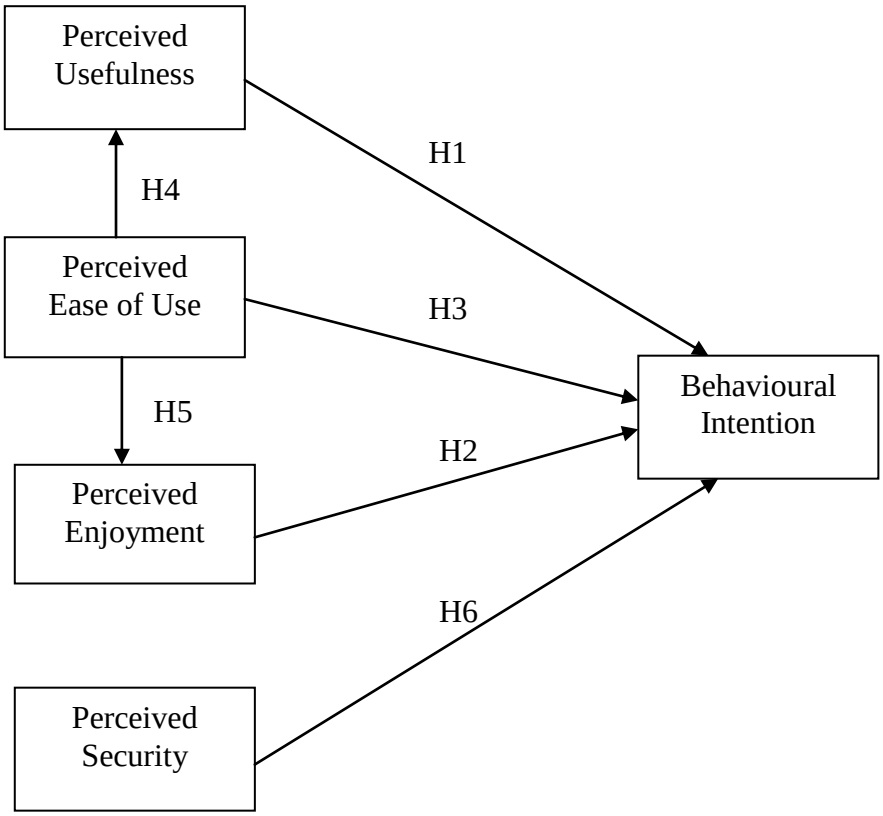

Figure 17: Modified Research Model

8. DISCUSSION

The intent of the present study is to test an augmented TAM in the online gaming context, and to investigate players' acceptance of account protection technology. In particular, the model postulated the influence of perceived enjoyment and perceived security on the intention to use and the relationships with the traditional TAM constructs. According to the analytical results in the previous section, all the four constructs of perceived usefulness, perceived enjoyment, perceived ease of use and perceived security reveal a positive impact on behavioural intention. Also, the hypothesised relationships between perceived ease of use and perceived usefulness, and perceived ease of use and perceived enjoyment, have been proved. However, there are a number of specific results that warrant discussion.

The intrinsic motivation factor, perceived enjoyment, has the same explanation power as perceived usefulness in predicting intention to use account security technology in the online gaming context. The empirical results suggest that WoW players' acceptance of security technology is significantly affected by any satisfactory experiences gained using Battle.net Authenticator and SMS Protect. While perceived usefulness is normally seen as a dominant factor in adopting utilitarian systems, perceived enjoyment is a strong determinants of hedonic systems usage (Van der Heijden, 2004). In a virtual entertainment environment, however, the nature of an information system can have a mixture of utilitarian and hedonic value. Both perceived usefulness and perceived enjoyment play a significant role in determining this kind of technology adoption.

The current investigation shows a positive relationship between perceived ease of use and the other three constructs: perceived usefulness, perceived enjoyment and intention to use. That is, if players consider that using account security technology is easy to understand and free of effort, they will tend to perceive it as more useful and enjoyable. Often, the first impression of how easy the technology is to use is important, as players make their decisions based on it. Moreover, once they choose to use the security technology, players have to use it every time they access their game accounts. As one respondent put it, *"Easy to use, however gets frustrating when logging into website as it requires code every time as opposed to single use codes for*

IP address when logging into the game." Another respondent commented, *"Easy to use, only issue I had was when I was transitioning cell phones."* When it comes to perceived ease of use, players are concerned not only about difficulties in learning how to use the technology, but also about regular usage across the different platforms or devices.

The findings of this research advance previous studies by clarifying the relationship between perceived security, perceived enjoyment and perceived usefulness in online games. The effects of perceived security on perceived enjoyment or perceived usefulness turn out to be insignificant. This can be explained by the fact that security is always an issue in online games. One respondent commented, *"…I think it's important to remember thought that hackers will always remain a step ahead of even the most sophisticated security systems. Online security is something that regrettably only works well as a reactive system for the most part. While it is possible to theorize how a hacker might try to penetrate your system and provide a security measure to deter them, it is unreasonable to expect even an army of security professionals to imagine and plan for any and all possible means of access that hackers might employ to gain access to a computer system…."* Besides, more and more players have realised that a single security tool will not address all the security threats. Another respondent said *"I use the key chain purchased from the store. Have never been hacked or had any security issues. While I realize the point of the authenticator is simply a layer of protection, I also make sure to scan my pc on a regular basis as anyone can get hacked/key-logged if their pc is not clean."* Therefore, there is no strong correlation existing between perceived security, perceived enjoyment and perceived usefulness by game players.

While the research findings provide meaningful insights for TAM in the virtual game environment, a number of common limitations persist in the study.

Firstly, testing the model fit is measured by the researcher's interpretation of survey results. This implies the possibility of methodological bias, as it is subject to personal experience and beliefs. It would be appropriate to develop a more direct and objective method, such as structural equation modelling (SEM) and Partial Least Square (PLS)

calculations. These advanced techniques are not used mainly because they are standard beyond the requirement of this Masters level project.

Second, the reliability and validity of the construct of perceived security, with Cronbach's alpha = 0.7 and AVE = 0.68, meets the acceptable level but is apparently lower than that of the other constructs. There is a possibility that the relevant survey questions are ambiguous. A pilot test and modification of the survey instrument should be considered.

Finally, the number of the research subjects is lower than a hundred, which is a very small portion of online game players. The majority were young North American WoW players. This may potentially limit the applicability of the research findings in other settings or populations. It would be appropriate to conduct additional research to examine the generalisability of the model and its findings to a wide array of settings and populations.

9. CONCLUSION

To conclude, this study is conducted to examine determinants of player acceptance of account security technology in the online gaming context. The proposed research model and hypotheses are based on TAM and prior literature on enjoyment and security. The research subjects are online gamers who play the most popular MMORPG – World of Warcraft. The results of this study validate an augmented TAM, confirming the important roles of perceived enjoyment and perceived security in predicting behavioural intention. Moreover, perceived ease of use is proved to have a positive impact on perceived usefulness, perceived enjoyment and intention to use. The lack of significant link between perceived security, perceived usefulness and perceived enjoyment indicates the need for further research on security in the virtual gaming environment.

The results also highlight theoretical and practical implications for further research. From the standpoint of individual-level technology acceptance research, this study extends TAM with enjoyment and security concepts. A primary contribution may lie in clarifying the link between the factors influencing the usage intention for account security technology in the context of online gaming. Future studies should develop more sophisticated instruments based on further clarification of conceptual differences and using a wider sample of online players. From a practical perspective, players' intention to use account protection technology while playing is of considerable interest because creators, publishers, and operators of online games can benefit greatly from improved understandings of the driving factors behind players' intention. As online games grow rapidly, the creation of a safe virtual environment can enhance players' gaming experience and may also be useful to improve the levels of reputation by game vendors.

10. REFERENCES

Activision Blizzard. (2011). *Annual Report 2011.* Retrieved October 26, 2012, from http://files.shareholder.com/downloads/ACTI/2065287894x0x564196/DAD3CBE4-2B7B-4DBF-B5FF-328F598E2E63/Activision_Blizzard_2011AR_FINAL.pdf

Babin, B. J., Darden, W. R., & Griffin, M. (1994). Work and/or fund: Measuring hedonic and utilitarian shopping value. *Journal of Consumer Research, 20*(4), 664-656.

Battle.net. (n.d.). In *Wikipedia.* Retrieved October 12, 2012, from http://en.wikipedia.org/wiki/Battle.net#cite_note-New_B.net-7

Beginner's guide. (2012). Retrieved October 6, 2012, from http://us.battle.net/wow/en/game/guide/

Bhattacherjee, A. (2001). An empirical analysis of the antecedents of electronic commerce service continuance. *Decision Support System, 32*(2), 201-214.

Blizzard Entertainment. (2004). *World of Warcraft.* Retrieved October 6, 2012, from http://willishome.com/Manual.pdf

Blizzard Entertainment. (2012a). *Battle.net account FAQ.* Retrieved October 12, 2012, from https://us.battle.net/support/en/article/battle-net-account-faq

Blizzard Entertainment. (2012b). *What is Battle.net?* Retrieved October 12, 2012, from http://sea.battle.net/en/what-is/

Blizzard Entertainment. (2012c). *World of Warcraft Races* [Image]. Retrieved October 11, 2012, from http://us.battle.net/wow/en/game/race/

Bowen, W. (1986). The puny payoff from office computers. *Fortune, 26,* 20-24.

Brief, A. P., & Aldag, R. J. (1977). The intrinsic-extrinsic dichotomy: Toward conceptual clarity. *Academy of management Review, 2*(3), 496-500.

Byrne, G. (2004). *Security issues of online gaming.* Retrieved September 25, 2012, from http://www.gamedev.net/page/resources/_/technical/multiplayer-and-network-programming/security-issues-of-online-gaming-r2062

Carmines, E. G., & Zeller, R. A. (1979). *Reliability and validity assessment: Quantitative applications in the social sciences.* Beverly Hills: Sage.

Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information and Management, 46*(7), 411-417.

Chen, S. C., Li, S. H., & Li, C. Y. (2011). Recent related research in technology acceptance model: A literature review. *Australian Journal of Business and Management Research, 1*(9), 124-127.

Chuttur, M. (2009). Overview of the Technology Acceptance Model: Origins, developments and future directions. *Sprouts: Working Papers on Information Systems, 9*(37). Retrieved October 15, 2012, from http://sprouts.aisnet.org/9-37/

Comte, A. (1853). The positive philosophy. In Thompson K. & Tunstall J. (Eds) *Sociological Perspectives.* Harmondwoth: Penguin.

Crossan, F. (2003). Research philosophy: Towards an understanding. *Nurse Researcher, 11*(1), 46-55.

Davis, F. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* PhD Thesis. MIT Sloan School of Management, Cambridge, MA. Retrieved October 18, 2012, from http://hdl.handle.net/1721.1/15192

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioural impacts. *International Journal of Man-Machine Studies, 38,* 475-487.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1992). Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology, 22*(14), 1111-1132.

Deci, E. L. (1975). *Intrinsic Motivation*. New York: PlenumPress.

Dewan, S., & Chen, L. (2005). Mobile payment adoption in the US. *Journal of Information Privacy and Security, 1*(2), 4-28.

Easterby-Smith, M., Thorpe, R., & Lowe, A. (1997). *Management research: An introduction.* London: Sage.

Fishbein, M., & Ajzen, I. (1975). *Belief, attitude, intention, and behaviour: An introduction to theory and research.* MA: Addison-Wesley.

Flavián, C., & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy – The basic elements of loyalty to a web site. *Industrial Management & Data Systems, 106*(5), 601-620.

Fornell, C., & Larcker, V. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18,* 39-50.

Hair, J. F., Anderson, R. E., Tatham, R. L., & Black, W. C. (1998). *Multivariate data analysis.* Ney Jersey: Prentice Hall.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination.* London: Sage Publications.

Hirschman, E. C., & Holbrook, M. B. (1982). Hedonic consumption: Emerging concepts, methods and propositions. *Journal of Marketing, 46*(3). 92-101.

Holbrook, M. B., & Hirschman, E. C. (1982). The experiential aspects of consumption: Consumer fantasies, feelings, and fun. *Journal of Consumer Research, 9*(2). 132-140.

Holt, D. B. (1995). How consumers consume: A typology of consumption practices. *Journal of Consumer Research, 22*(1), 1-16.

Hsu, C., & Lu, H. (2004). Why do people play on-line games? An extended TAM with social influences and flow experience. *Information and Management, 41*(7), 853-868.

Huang, Z., & Cappel, J. J. (2005). Assessment of a web-based learning game in an information systems course. *Journal of Computer Information Systems, 45*(4), 42-50.

Kalakota, R., & Whinston, A. B. (1997). *Electronic commerce: A manager's guide.* Massachusetts: Addison Wesley.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons, 53,* 59-68.

Keil, M., Beranek, P. M., & Konsynski, B. R. (1995). Usefulness and ease of use: Field study evidence regarding task consideration. *Decision Support Systems, 13*(1), 75-91.

Ki, J., Cheon, J. H., Kang, J., & Kim, D. (2004). Taxonomy of online game security. *The Electronic Library, 22*(1), 65-73.

Kim, K. H., Park, J. Y., Kim, D. Y., Moon, H. I., & Chun, H. C. (2002). E-lifestyle and motives to use online games. *Irish Marketing Review, 15*(2), 71-77.

Kim, W. (2008). Applying the technology acceptance model and flow theory to Cyworld user behaviour: Implication of Web2.0 user acceptance. *Cyberpsychology & Behaviour, 11*(3), 378-382.

Li, D., Chau, P. Y. K., & Lou, H. (2005). Understanding individual adoption of instant messaging: An empirical investigation. *Journal of the Association for Information Systems, 6*(4), 102-129.

Linderoth, J., & Bennerstedt, U. (2007). *Living in World of Warcraft – The thoughts and experiences of ten young people.* Retrieved September 25, 2012, from http://www.highlandbusinessresearch.com/downloads/introtoonlinesocialnetworks.pdf

Mathieson, K. (1991). Predicting user intentions: Comparing the TAM with the theory of planned behaviour. *Information System Research, 2*(3), 173-191.

McGraw, G., & Hoglund, G. (2007). Online games and security. *IEEE Security & Privacy, 5*(5), 76-79.

Miller, M. J. (2003). *Reliability and Validity.* Retrieved January 17, 2013, from http://michaeljmillerphd.com/res500_lecturenotes/Reliability_and_Validity.pdf

Moon, J. W., & Kim, Y. G. (2001). Extending the TAM for a World-Wide-Web context. *Information & Management, 38*(4), 217–230.

Roca, J. C., García, J. J., & Vega, J. J. (2009). The importance of perceived trust, security and privacy in online trading systems. *Information Management & Computer Security, 17*(2), 96-113.

Rosen, P., & Sherman, P. (2006). Hedonic information systems: Acceptance of social networking websites. *Americas conference on information systems, AMCIS 2006 Proceedings*, 1218-1223.

Schober, F. (2009). *Gaming – The next overlooked security hole.* Retrieved October 29, 2012, from http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-schober.pdf

Shin, D. H., & Shin, Y. J. (2011). Why do people play social network games? *Computers in Human Behaviour, 27,* 852-861.

Sinclair, B. (2005). *RE4 named Game of Year at Spike Awards.* Retrieved October 10, 2012, from http://www.gamespot.com/news/re4-named-game-of-year-at-spike-awards-6140144

Technology acceptance model. (n.d.). In *Wikipedia.* Retrieved October 16, 2012, from http://en.wikipedia.org/wiki/Technology_acceptance_model

The Game Informer staff. (2009). The top 200 games of all time. *Game Informer, 200,* 44-79.

Trochim, W. M. K. (2006). *Research methods knowledge base.* Retrieved December 19, 2012, from http://www.socialresearchmethods.net/kb/index.php

Van der Heijden, H. (2004). User acceptance of hedonic information systems. *MIS Quarterly, 28*(4), 695-704.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research, 11*(4), 342-364.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Towards a unified view. *MIS Quarterly, 27*(3), 479-501.

Wang, Y. S., Lin, H. H., & Liao, Y. W. (2010). Investigating the individual difference antecedents of perceived enjoyment in the acceptance of blogging. *World of Academy of Science, Engineering, and Technology, 43,* 1014-1023.

Williamson, K. (2006). Research in constructivist frameworks using ethnographic techniques. *Library Trends, 55*(1), 83-101.

World of Warcraft. (n.d.). In *Wikipedia.* Retrieved October 10, 2012, from http://en.wikipedia.org/wiki/World_of_warcraft

Wu, J., & Liu, D. (2007). The effects of trust and enjoyment on intention to play online games. *Journal of Electronic Commerce Research, 8*(2), 128-140.

Wu, J. H., Wang, S. C., & Tsai, H. H. (2010). Falling in love with online games: The uses and gratifications perspective. *Computers in Human Behaviour, 26,* 1862-1871.

Yan, J. (2003). *Security design in online games.* Retrieved September 25, 2012, from http://homepages.cs.ncl.ac.uk/jeff.yan/yan_acsac03.pdf

Yan, J. J., & Choi, H. (2002). Security issues in online games. *The Electronic Library, 20*(2), 125-177.

Young, T. R. (1984). The lonely micro. *Datamation, 30*(4), 100-114.

Ziebart, A. (2012). *World of Warcraft currently down to 9.1 subscribers.* Retrieved October 11, 2012, from http://wow.joystiq.com/2012/08/02/world-of-warcraft-currently-down-to-9-1-million-subscribers/

Appendix A: Survey Questions

Questionnaire

The goal of this research is to examine online players' adoption of account security technology. The survey should take approximately 10 minutes to complete. By completing and submitting the survey, you are implying that you consent to participate and that you understand the following:

Your participation in this study is completely voluntary and your responses will remain anonymous. You answer cannot be matched to your identify [or location] and will be released only as summaries grouped with other people's responses. Information about the computer and Internet service provider you are using will not be collected. Your survey responses will be entered into a non-identifiable data file with other people's response.

The results of the study will be deposited in the Victoria University library, and presented at conferences and/or journals. If you choose to enter your contact information to receive a summary of the findings, this information will not be linked to your survey responses, will be kept in a password protected file on a secure server, and will be deleted once the findings have been communicated.

You may withdraw prior to submitting your survey, without consequences of any kind. To leave the study, simply close the web browser window. Once you have submitted your survey, it is no longer possible to withdraw your data because your responses are entered into a non-identifiable data file.

A. General Information

Q1. How long have you been playing World of Warcraft?

□ 1 - 0-6 months

□ 2 - 6-12 months

□ 3 - 1-3 years

□ 4 - 3-5 years

□ 5 - 5-8 years

Q2. Which following Battle.net security technology have you used for your World of Warcraft account?

□ 1 - Keychain Authenticator sold in Blizzard Store

□ 2 - Mobile Authenticator on iTune App Store

□ 3 - Mobile Authenticator on Google Play

□ 4 - Mobile Authenticator on BlackBerry AppWorld

□ 5 - Mobile Authenticator on Zune

□ 6 - Battle.net SMS Protect

□ 7 – None of them

Other (please specify)

Q3. How often has your World of Warcraft account been accessed by an unauthorised third party?

□ 1 - Never

□ 2 - Once

□ 3 - Twice

□ 4 - Three times

□ 5 - Four times or more

Q4. My age is ……

Q5. My gender is:

□ 1 - Male

□ 2 - Female

Q6. My country of origin is: ……

B. Perceived Usefulness

Q7. I feel using Battle.net Authenticator and/or SMS Protect gives me greater control over my World of Warcraft account security management.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q8. I feel using Battle.net Authenticator and/or SMS Protect makes it easier to do the World of Warcraft account security management.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q9. Overall, I think the Battle.net Authenticator and/or SMS Protect are useful to me.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

C. Perceived Enjoyment

Q10. I feel using Battle.net Authenticator and/or SMS Protect is enjoyable and fascinating.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q11. I had a pleasant experience from the Battle.net Authenticator and/or SMS Protect.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q12. Overall, I enjoy using Battle.net Authenticator and/or SMS Protect.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

D. Perceived Ease of Use

Q13. My interaction with the Battle.net Authenticator and/or SMS is clear and understandable.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q14. Overall, I find the Battle.net Authenticator and/or SMS Protect easy to use.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

E. Perceived Security

Q15. I am confident that my World of Warcraft account information with the game company Blizzard Entertainment is secured.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q16. I feel that unauthorised third parties may still deliberately access my World of Warcraft, whether I am using the Battle.net Authenticator and/or SMS Protect or not.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q17. The Battle.net Authenticator and/or SMS Protect offered by the game company Blizzard Entertainment has enough security measures to protect my World of Warcraft account information.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q18. Using the Battle.net Authenticator and/or SMS Protect to keep my World of Warcraft account safe is more important than having fun.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q19. Overall, using Battle.net Authenticator and/or SMS Protect reduces the security risks of my World of Warcraft account.

□ 1 - Completely disagree

□ 2 - Mostly disagree

□ 3 - Neither agree nor disagree

□ 4 - Mostly agree

□ 5 - Completely agree

Q20. Please describe your experience with the Battle.net Authenticator and/or SMS Protect

Please indicate whether you want a copy of the results

□ 1 – Yes, I would like to receive a copy, and my email address is .....

□ 2 – No, thanks.

If you choose to enter your email address to receive a summary of the findings, this information will not be linked to your survey responses, will be kept in a password protected file on a secure server, and will be deleted once the findings have been communicated.

Appendix B: Participant Information Sheet

Participant Information Sheet

For a Study of World of Warcraft Players

Researcher: Susan Yang, School of Information Management, Victoria University of Wellington

I am a Master student in Information Management at Victoria University of Wellington. As part of this degree I am undertaking a research project to examine the factors determining the acceptance of account security technology by online gamers. The University requires that ethics approval be obtained for research projects involving human participants.

I am inviting World of Warcraft players to participate in this study. Participants will be asked to complete a questionnaire via an online survey web-link. The questionnaire will take no more than 10 minutes to fill out.

Your participation is voluntary and anonymous. While I would be pleased to have you participate, I respect your right to withdraw from the study prior to submitting your survey, without consequences of any kind. To leave the study, simply close the web browser window. Once you have submitted your survey, it is no longer possible to withdraw your data because your responses are entered into a non-identifiable data file.

All research findings reported will be on an anonymous basis. It will thus not be possible for you to be identified personally. All material collected will be kept confidential. No other person besides me and my supervisor will see the questionnaires. The results of this study will be submitted for marking to the School of Information Management and deposited in the University Library.

If you have any questions, please contact me at yangxiao10@myvuw.ac.nz or my supervisor, Tony Hooper, at the School of Information Management, Victoria University, tony.hooper@vuw.ac.nz.

Susan Yang

Appendix C: Acronyms and Abbreviations

AVE	Average Variance Extracted
IS	Information System
IT	Information Technology
MAC	Message Authentication Codes
MMORPG	Massively Multiplayer Online Role-Playing Game
NPC	Non-player character
PLS	Partial Least Square
SEM	Structural Equation Model
TAM	Technology Acceptance Model
TRA	Theory of Reasoned Action
UTAUT	Unified Theory of Acceptance and Use of Technology
WoW	World of Warcraft