Guidelines to Improve the Security and Privacy Consciousness among Online Gamers

Nicholas Lennox and Bertram Haskins
School of Information and Communication Technology, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
s212231081@nmmu.ac.za and bertram.haskins@nmmu.ac.za

Abstract

Online gaming has become a major pastime in recent years. Gamers who participate in these games place a lot of personal information online, some of which may be valuable in the wrong hands. This study attempts to provide a series of guidelines for participants in online gaming, to make them more security and privacy conscious in their online activities. To this end, a literature review was conducted to determine common threats in online activities and a few online gaming portals were scrutinized to determine which account settings could aid users in maintaining the privacy of their account settings. A survey was conducted to determine the general profile of online gamers. The 325 survey responses were used, along with the information gathered from the literature review and online portal scrutiny to construct a series of guidelines which serve to improve the security and privacy consciousness among online gamers.

Introduction

Online multiplayer gaming has come a long way over the last few decades. From playing with your friends in a room to engaging with millions of gamers around the world, this globalization of gaming has opened the platform up to new challenges. These challenges include trade scams, in which one user attempts to convince another to make a deal (such as a trade or a gift purchase) under false pretenses, and account theft. Chief among the vehicles used for these acts is social engineering, which is used to trick unsuspecting gamers into revealing their private information. The private information could include contact details, credit card information or even transferrable purchases. The loss of these details therefore constitute a real, financial risk to the gamers. The gamers themselves may be unaware of the risks of interacting online or are simply indifferent. This has led to many gamers being tricked into handing over their information and having their online information and purchases stolen. This could easily be avoided if the gamers themselves were aware of these risks and the actions necessary to avoid them or were instilled with the forethought to be proactive with regards to their online account privacy and security settings.

Study Objectives

In order to raise the security and privacy consciousness of online gamers while making use of online services, this paper presents a series of guidelines to make them aware of aspects to address in their online activities in an attempt to ensure that their information remains private and secure. In order to devise these guidelines, the remainder of the paper is structured as follows. In the *Online Gaming* section literature is consulted to provide an overview of the online gaming environment and the possible attacks which might affect users of these platforms. The section titled *Platform-Specific Security Settings* describes a study conducted on the privacy settings of various widely used online gaming platforms to determine which common settings may be used to increase the security and privacy of users of these platforms. The *Online Gamer Survey* section provides an overview of the results of a survey conducted among the users of these online sites. In the *Guidelines for Online Gamers* section, the information gathered in the three aforementioned sections are condensed into a series of guidelines which serve to improve security and

privacy consciousness among online gamers. The study is then concluded in the *Conclusion and Future Work* section.

Online Gaming

Overview of Online Gaming

Online gaming or online games are the games that are played online via LAN, the Internet or even Telecommunication (Chen, Y., Chen, P., Song, & Korba, 2004). Online gaming includes Massively Multiplayer Online Roleplaying Games (MMORPGs), Internet gaming, web gaming, online gambling, local LAN gaming and mobile gaming, but not non-networked video and personal computer gaming. This classification is illustrated in Figure 1.

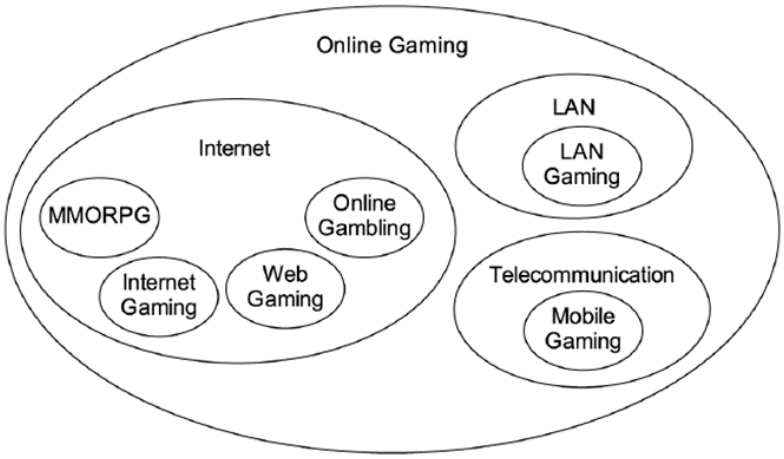

Figure 1: Classification of online games (Chen Y.C. et al., 2005).

Chen Y. et al. (2004) state that these online games have three business models associated with them, namely; charging for the software license, charging for the network connection or charging for both. In the first business model, game companies earn profits by selling their software license as boxed products. Players only need to pay once in order to use the software. Network connection functionality is often provided free of charge. In the second business model, the game companies charge gamers for using the service and the games themselves are often free or very cheap. This provides a more stable income for the providers as the gamers pay to log on to the servers hosted by the game company. In the third business model gamers must purchase the game at retail price and then also pay an amount to play online. This is the most expensive method and may act as a deterrence to modern gamers.

Traditionally gamers would have to go to the store and purchase a physical copy of a game to install on their computers. In the modern gaming environment this method of purchasing games has also been digitized and encapsulated into a digital game library. A digital game library is a collection of games stored in a digital environment. This eliminates the need to purchase physical copies of games as it can be done digitally, where the serial key is linked to the customer's account. There are three main, widely used digital game libraries that exist for PC gamers: Steam (Valve, 2016), Battle.net (Blizzard, 2016) and Origin (Electronic Arts, 2016).

When a gamer creates an account with any game company they provide personal information, which often includes banking or credit card details. Once the account is created the user is provided with a set of associated login credentials. Since the login credentials represent access to everything owned by players in the virtual world; as well as real-world information such as credit card details, this information should be treated as strictly confidential. Unfortunately, because of the sensitive and private nature of the information, these account details are a prime target for malicious activities by hackers. These activities

may include acts such as compromising the data or theft. In a study by Chen Y.C. et al. (2005) the theft of accounts was the largest contributor to online gaming crimes in Taiwan.

Privacy in Online Gaming

At the broadest level, privacy is the right to be left alone (Pearson & Benameur, 2010). Privacy in terms of information could thus be expanded to state that information privacy is the right to have your personal information kept personal. To determine whether information should be deemed personal, we may ask a simple question: Would there be any repercussions if a stranger knew this information? If the answer is yes, then that information is personal and needs to be protected to in order to ensure that it remains personal.

Due to the nature of the information provided by gamers during online gaming account creation, most of the information should be kept private. To ensure this, there are many settings in the game clients that allow the gamers to change their settings. If the private information is left unprotected, criminals could use various methods to illegally retrieve it. In this paper, these methods are referred to as attacks. There are two broad categories of attacks; direct and indirect attacks.

Direct attacks occur when the attacker targets the player directly. To facilitate the attack, the attacker employs various social and technical methods in order to gain the account information of the player. One such attack employs the use of spam emails and malicious emails to embed Trojan horse programs to gather information on the target computer (Chen et al., 2004). Another approach used by attackers is to use social engineering to gather information on the intended target. Social engineering in an online gaming context may be defined as tricking honest players into handing over their account details by making them believe they are getting a reward or that something attractive is on offer (Van Summeren, 2011).

Online gaming participants are used to being connected to each other via in-game chat or email and it is not common practice to hand over account details when asked. The attacker, therefore, needs to trick the player by providing an incentive, such as a rare in-game item or the promise of participation in an upcoming beta test for new game content. The web sites, emails or chats promising these rewards look legitimate, but are designed to record any keystrokes made by the intended victim, for later use. Another approach used by attackers is to exploit the lack of authentication to servers by setting up dummy servers for players to join. The servers simply save the account details of any player who logs on to it. Trade scams are another form of direct attack against a player. Valve (2015) defines a trade scam as a form of deception in which one system user convinces another to make a deal. These trades are centered on deals, gifts or market transactions; all of which carry a real-world monetary value or in-system credit. The deals may seem good or fair to the recipient, but in fact they are not. To avoid these kinds of trades, it is recommended that account holders on these sites ignore pressure to finalize the deal quickly, ignore pressure to trust the user initiating the deal, double-check the properties of the item involved in the deal, monitor the trade log associated with the deal, do not make trades outside of the designated trade window / area and make sure that the deal is being conducted with the correct person, as scammers often impersonate friends or trusted traders.

Indirect attacks occur when the attacker targets the platform the service is provided on. These attacks are usually not noticed by the player until their accounts have been compromised. There are various methods of performing these indirect attacks. Most client-to-client interaction in an online game is handled through a server middleman (Bono, Caselden, Landau, & Miller, 2009). An attacker can compromise game servers by emulating the game client to avoid the validation and then gain access to the server's ports where the traffic can be measured. An attacker can eavesdrop in order to insert, delete or modify game events or commands that are transmitted over the network. This exploits the lack of secrecy (Van Summeren, 2011). Another approach is to use some form of denial-of-service attack. By denying service to players, a dishonest person could take advantage of their difficulty in connecting to gather information on them or gain an advantage in an online match.

Platform-Specific Security Settings

Game companies have various methods which they make use of in order to protect gamers from the previously mentioned attacks. Most software applications include an End User License Agreement (EULA). The EULA has to be accepted when installing the software and acts as a legal contract between the software producer and the end user, stating how the software is used (TechTarget, 2005). A EULA may be accompanied by a Terms of Service (ToS) or a Terms of Conduct (ToC) document. Both the ToS and ToC dictate how the users must behave when using the software or risk having the license revoked. This protects gamers as it gives the game companies the power to punish users who are malicious.

Game companies also employ extra authentication methods which go beyond the standard user ID and password authentication. Most of these settings require that gamers go into their profile, account settings, privacy settings or communication preferences. Once accessed, the various companies offer different options to their site users. Steam (Valve, 2016) allows users to modify who is able to view their profile, make comments on their profile or view their games inventory. The individual profile settings may be set to *private*, *friends only* or *public*. Descriptions of these settings are listed in Table 1. The account holder also has the option of keeping any gifted items in their inventory private, regardless of other privacy settings. Account holders have the option of adding their real name to the account (besides their online username) and adding the details of another social media site, such as *Facebook*. Steam also provides a second level of authentication by means of its *Steam Guard* platform. *Steam Guard* requires an access code to be entered whenever a user logs in on a new device. This access code may be sent to an email address or from the *Steam Mobile App*. A further level of security may be provided by the *Steam Guard Mobile Authenticator*, which forms part of the *Steam Mobile App*. The *Authenticator* generates a code which needs to be entered any time a user logs into their Steam account. A new code is generated every 30 seconds.

Table 1: Steam privacy settings

Setting	Description
Private	Only the account holder may view the details.
Friends only	Only other Steam members already in the current user's friends list may view the details
Public	Anyone may view the details.

Battle.net (Blizzard, 2016) provides the ability to hide or show the account holder's real identity and manage permissions allocated to various third party applications. Similar to Steam, it provides secondary authentication via a mobile app, but customers may also purchase a physical authenticator device. Battle.net also provides a service called *SMS Protect*, which allows an account user to receive text messages whenever illegal login attempts have been made on their account, whenever the account password has been updated or whenever security settings have been changed.

In a similar vein to Steam and Battle.net, Origin (Electronic Arts, 2016) provides a means by which to perform *Login Verification* when logging in via an untrusted device. This occurs via a security code sent to an email address, mobile application or text message. Once logged in, a device may be added to a list of trusted devices. A user may decide who may view their profile, they can choose to allow *Everyone*, *Friends*, *Friends of Friends* or *No One* (i.e. private). From the profile settings an account holder may also decide whether their profile displays or hides their real name. Origin users also have the option to hide their in-game achievements from anyone visiting their profile. Because Origin may link to online platforms on other systems, such as *Xbox Live* or *PSN Online*, and the Origin profile may contain an email address; a user may allow or disallow other users to search for their profile via any one of these ID or address types. Finally, Origin also allows an account holder to explicitly block specific other users.

Although all of these digital game libraries do provide simple login functionality; it is apparent that there are many other common security and profile features, shared amongst the various sites. These sites may however name the same feature differently. These common features have been condensed and presented in Table 2.

Table 2: Common digital game library privacy and security features

Feature	Description
Access restriction	This feature allows an account holder to allow or disallow access to certain profile features to certain groups of system users.
Real identity concealment	This feature allows an account holder to conceal their real identity and only allow access to their profile via a system user name or ID.
External links	This feature allows an account holder to link their account to various other sites or social networks. Enabling this functionality may allow an account to be more easily found by those searching for it.
Secondary authentication	This feature allows an account holder to enable a secondary level of user verification upon login by means of email, mobile application, physical device or text message.

Online Gamer Survey

A series of questions were designed in order to gather data about the key privacy-and security-related issues gamers face while interacting online. The survey received 325 responses over a period of 2 days. The limited time the survey was available was a result of the overarching time constraints of the study. The link to the survey questions was distributed on Reddit and Facebook. These platforms were chosen because of convenience and both platforms contain threads, dedicated to various online games, on which the survey could be disseminated. Participants were required to be 18 years or older, but no older than 59. These age profiles were chosen to align with the ethics requirements of the university at which this study was conducted.

Population Demographic

To attain a complete demographic overview of the participants, the survey questions include several general and play-related demographic questions. These questions include items related to age, gender, whether they play online games, how many hours per week do they play, and what genre of games do they primarily play. Table 3 provides a listing of some of the survey findings, in order provide an overview of the population specifics of the group of respondents.

Table 1: General questionnaire findings

Descriptor	Most frequent response
Age	18 to 24 (73.77%)
Gender	Male (95.37%)
Number of hours spent playing online per week	More than 10 (72.22%)
Make use of game clients (and their associated digital libraries) to play online games	Yes (97.53%)
Game client most frequently used	Steam (65.12%)

Password Practices

Another series of questions focused on the password practices of the respondents. The results of these questions are shown in Figure 2 and Figure 3. Figure 2 indicates which percentage of the respondents

answered in the positive (yes) on each of the questions. From these indicators it would seem as if most of the respondents are aware of the necessity of creating more secure, longer passwords which consist of a combination of various character types. Almost half of the respondents (46%) use the same password for multiple accounts. This is worrying as it means that for many of the respondents there is a big risk if someone breaches their password. This single password may give the person with malicious intent access to multiple accounts of the respondent. As stated by Ives, Walsh, & Schneider (2004), users who reuse passwords fail to realize that even if they make use of very secure login platforms for some of their online activities, the security of these platforms may be compromised if an attacker gains the shared password used elsewhere, on a service which is not as well defended.

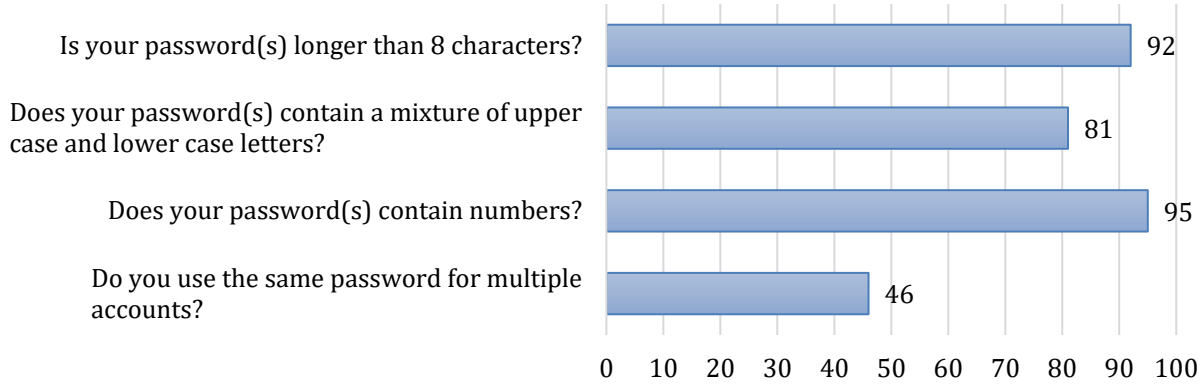

Figure 2: Percentage of respondents who answered positively on password-related questions

Figure 3 is an indicator of how often the respondents change their password. The majority of them (61%) only rarely change their passwords. When analyzed it came to light that of the 46% respondents who use the same password for multiple accounts, 68% rarely changed their password.

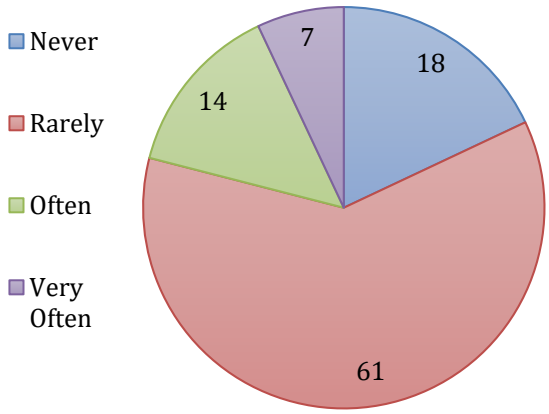

Figure 3: Distribution of the frequency of respondent password changes, expressed as percentages

EULA Completion

Although the EULA document represents the agreement between the software vendor and the client, stipulating measures to protect both parties, only 3% of respondents stipulate that they read the entire EULA when installing a new application or updating an existing application. 53% of respondents know that the EULA exists, but never bother to read it, while a further 43% only skim through it (probably because you have to scroll through it to enable the *Accept* or *Agree* button at the bottom of the EULA). 1% of respondents have stated that they are unaware of the existence of the EULA. It is unclear whether these respondents have never installed their own software or are simply unsure as to what the EULA is.

Authentication and Privacy Settings

As previously discussed, most on-line platforms provide some form of extra authentication measures. From the responses to the survey questions, it seems that most respondents do make use of these measures (77%). 19% of the respondents have indicated that they know about the extra authentication options but do not use them and the remaining 4% have indicated that they are unaware of the extra authentication options. Unfortunately, no follow-up question was asked to determine the reason why those users who are aware of the extra options do not make use of them. One possibility could be that they do not want to provide their mobile phone number to be contacted on; another could be that they do not want to install a separate application on their mobile phone to perform the authentication. It could also be that they see the extra authentication step as a waste of time.

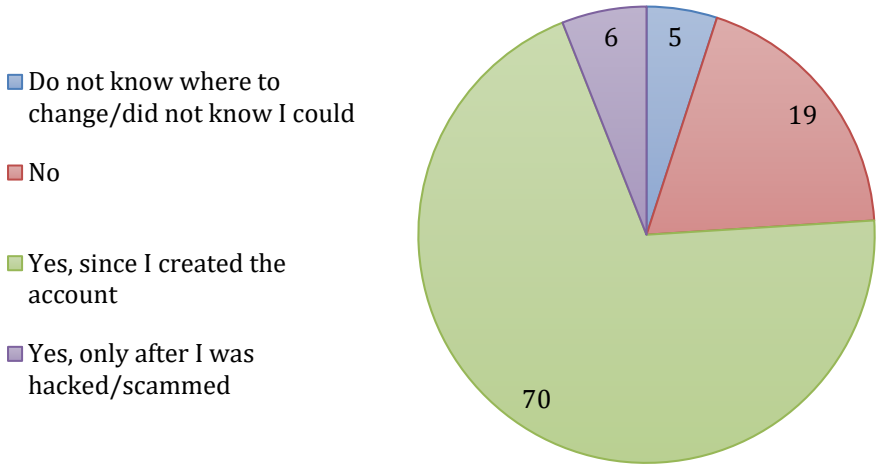

Figure 4: Percentages of respondents who change their account privacy settings

The survey asked respondents to indicate whether they change the default privacy settings on their online accounts. Figure 4 graphically illustrates the responses to this question. 76% of the respondents indicated that they do change their privacy settings. 6% of those that indicated that they made changes to their privacy settings have only done so after their accounts have been hacked or they were the victim of spam. 5% of the respondents indicated that they are unaware of any privacy settings which they can change, while 19% simply indicated that they never update their privacy settings (for whichever reason). These results are very similar to those obtained by Ntlatywa, Botha & Haskins (2012) while studying the choice of privacy settings on Facebook. In their study, they found that 12% of the Facebook profiles studied were completely open (i.e. no privacy settings modified) and that 67% had applied some form of information hiding or privacy setting to their profile. The similarity of these population numbers may possibly be ascribed to the fact that people tend to follow the same behavioral patterns regardless of which sites they frequent. This

would imply that a similar pattern should exist on other online platforms, but further study would be required to support this.

Unsolicited Messages

Unsolicited messages seem to be a fairly common occurrence amongst users of these online platforms, as 71% of respondents have indicated that they have received some form of unsolicited message while playing an online game. Unsolicited messages are messages received via email, external communication platforms or in-game chat requests which may be as simple as friend requests, but more often than not are trade requests. Figure 5 illustrates the distribution of unsolicited message platforms among those respondents who received unsolicited messages. Some respondents have indicated that they receive messages on various platforms. From the results it would seems as if most unsolicited messages are received on "*live*" platforms such as in-game chat or a personal messaging service (e.g. Facebook Messenger or Google Hangouts) and that more than half (65%) of the unsolicited messages received, do in fact contain links on which the recipient is expected to click.

With regards to the links, 51% of the respondents who have received unsolicited messages have stated that they do not click on links received in a message from a stranger. 42% have indicated that the sites which these links point to have varying levels of accuracy or correspondence with the real site, whereas 7% of the respondents have said that they struggle to tell the difference between the real site and a fake one. What is a bit worrying is that of the respondents who receive unsolicited messages only 30% say that they always check any attachments to these messages by running an anti-virus scan. The other 70% only sporadically or never scan these attachments. When asked whether they believe that clicking on links have been responsible for having their account hacked or details stolen, 24% have indicated that they have been hacked once or twice and 1% believe that they have been hacked more than twice. The rest of the respondents do not believe that they have been hacked as a result of clicking on any links.

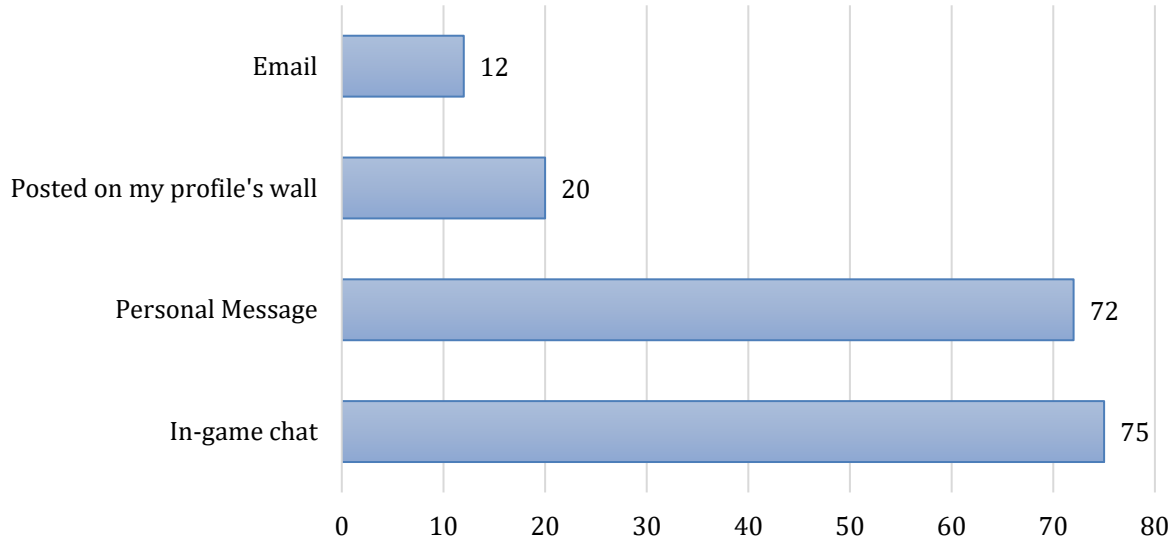

Figure 5: Percentages of respondents who have received unsolicited messages on various messaging platforms

The following section condenses the lessons learnt from the literature study, scrutiny of online gaming library security and privacy settings and the online survey to present a series of guidelines to improve security and privacy consciousness among online gamers.

Guidelines for Online Gamers

Being knowledgeable about the aspects of a domain in which you perform any action may influence the actions you take in this domain. The domain addressed in this study is that of online gaming platforms or libraries. In an attempt to improve the security consciousness of online gamers in this domain, the remainder of this section presents 6 guidelines related to profile security and privacy.

Guideline 1: Read official documentation

End User License Agreements (EULAs), privacy policies, Terms of Service and Terms of Conduct documents are there to protect both the company and the gamer, but they are often ignored by the majority of the participants of the questionnaire. In order to be sure which activities are permitted and whether any information is provided which may help retain the integrity of a gamer's account details, it is recommend that the EULA and other policies associated with a game should always be read, whenever they are presented or updated.

Guideline 2: Perform proper password maintenance

Passwords are the best, first line of defense to deter cyber criminals, thus making the correct choice in password construction essential to a secure account. The following steps, based on Gehringer's (2002) description of proper password construction and maintenance, should be applied when creating passwords:

- Ensure that all passwords are at least 8 characters in length.
- Ensure that all passwords contain a mixture of uppercase and lowercase letters, as well as digits and punctuation characters (if the account creation tool allows this).
- Change your password regularly.
- Avoid passwords which contain biographical information or information which could easily be inferred from online, in-game activities.
- Avoid reusing passwords on multiple sites.

Guideline 3: Mind your privacy

The privacy settings of your account determines who can see your profile details (such as your name and email address) and who is allowed to message you (e.g. only friends). The following steps should be taken to improve the security of your online profile:

- Privacy settings should be changed to at least restrict only friends to view profile details. These settings may usually be found under Account/Profile >Settings > Privacy/Communication preferences on most sites.
- Privacy settings should be set to only allow messages from friends.
- As far as possible, all friend requests and additions should be done using the game client and not an external website on which your login details may be insecurely (or even illegally) captured.
- Do not unnecessarily link your profile to other third-party sites or services.
- When linking to third-party sites, determine if you are able to manage the permissions associated with the site so as to allow the minimum level of access to your account information.
- Hide your real identity and only allow your profile to be accessed by means of an online user ID.
- Hide your profile from searches; this will ensure that friend requests and communication only come from those who know your user ID.

- If possible, prevent any in-game achievements from appearing as part of the account profile as this may advertise the games and activities partaken in in these games. This information may allow an attacker to perform a more directed attack.

Guideline 4: Don't be caught out by phishermen

From the data collected using the survey questions, it seems that social engineering, specifically phishing, is the most common method for attempts at account theft. Over 70% of the respondents received unsolicited messages over in-game chats and personal messaging services. Gamers should take the following steps to avoid being caught in a phishing attack:

- Ensure that all sites that require login are in the correct domain for the service. These sites may have some form of indicator, such as a green highlight in the address bar of the browser.
- Ensure that the identity of any support staff member is verified before handing over any private details.
- If random contact messages are received from another account holder, it may be wise to block this user's account from contacting you further.
- Scrutinize the authenticity of sites linked to from trade or friend requests; preferably by asking a trusted friend to investigate the site as a second opinion.
- To avoid your details appearing outside of the current online gaming environment, do not sign in to any third party website using your details. This includes tournaments where you may be required to create an account. If account creation is required, avoid linking in existing online accounts, such as Facebook as an alternate login option.

Guideline 5: Use multi-step authentication

Single-step login verification is not enough anymore, multi-stage authentication and mobile authentication are becoming the norm in other industries (such as banking) and now gaming companies are catching up. The extra steps provide the user with a security fallback to rely on to further ensure the security and privacy of their online accounts. To extend gamer authentication beyond just a simple login, it is recommended that gamers take the following steps:

- Whenever provided by the game client, make use of multi-step authentication to secure your account.
- Link your mobile phone to your account to add an extra layer of mobile authentication, whenever the game client provides this functionality.
- If available, enable notification on any account action, either by means of mobile application, mobile phone message or email. This will ensure that the account holder be notified of any changes made to the account.
- If the service provides a separate physical channel on which to perform authentication, such as an authenticator device, make use of it. This type of service will be compromised less easily than online or even mobile solutions.
- If the service maintains a list of devices and platforms from which the account has been accessed, check the list frequently and, if possible, limit the number of trusted devices from which the account may be accessed.

Guideline 6: Mind your purchases

One of the main aspects which come under attack in online, digital stores are credit card details, which are used to make new purchases, and transferable items (purchased or earned), which are linked to a user profile. These items are frequently the focus of attack as these are the items from which attackers could

most easily benefit. It is recommended that online gamers take the following steps to avoid falling prey to such an attack:

- If security and privacy settings provide the feature, hide any gifted or purchased items from appearing in your profile, both publically and privately. If these items are hidden, attackers will not have the information to target you to gain these items or have information on your purchase interests to scam you into making a false trade or purchase.
- Limit your financial liability on any of these sites by limiting your online credit card purchase limit, using prepaid credit or debit cards or by using an intermediary payment service.
- Only trade and purchase within the designated areas or channels created by the service provider.
- Do not allow anyone to rush or pressure you into a trade or sale.
- If possible, deal only with trusted traders or friends.

Conclusion and Future Work

Online gaming and the use of online digital libraries has become a widespread pastime and convenience measure for gamers around the world. The accounts associated with these services hold a variety of information related to the account holder. Some of this information may be sensitive, such as credit card information or the ownership of online content.

As discovered in the online survey, many users are either oblivious or blasé about the availability of features to aid in the protection of their accounts. Manual scrutiny of the account settings of the various services show that these settings are not hidden, nor difficult to access and as such could easily be addressed by most users who frequent these sites.

This paper has presented 6 guidelines, based on the information gathered from literature, an online gamer survey and a scrutiny of various online digital game libraries. Although, it is not possible to directly intervene in the account creation and maintenance process of all the gamers who frequent these sites; it is thought that the provision of these guidelines may increase their security consciousness when using these sites.

These guidelines have not yet been tested to determine whether they will have the desired effect of increasing the security and privacy consciousness of online gamers. A future study will be conducted in order to determine whether the security and privacy practices of gamers change if they have been given access to the set of guidelines.

References

Blizzard (2016), Battle.Net, Retrieved December 19, 2016 from http://eu.battle.net/en/

Bono, S., Caselden, D., Landau, G., & Miller, C. (2009). Reducing the Attack Surface in Massively Multiplayer Online Role-Playing Games. *Independent Security Evaluators*.

Chen, Y., Chen, P., Song , R., & Korba, L. (2004). Online Gaming Crime and Security Issue - Cases and countermeasures from Taiwan. *2nd Annual Conference on Privacy, Security and Trust*.

Chen, Y. C., Chen, P. S., Hwang, J. J., Korba, L., Song, R., & Yee, G. (2005). An analysis of online gaming crime characteristics. *Internet Research*, *15*(3), 246-261.

Electronic Arts (2016), Origin, Retrieved December 19, 2016 from https://www.origin.com/zaf/en-us/

Gehringer, E. F. (2002). Choosing passwords: security and human factors. In *Technology and Society, 2002.(ISTAS'02). 2002 International Symposium on* (pp. 369-373). IEEE.Ives, B., Walsh, K. R., & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), 75-78.

Ntlatywa, P., Botha, R. A., & Haskins, B. (2012). Factors that Influence the Choice of Privacy Settings on Facebook: Freshmen's View at a South African University. In *Privacy, Security, Risk and Trust (PASSAT),*

2012 International Conference on and 2012 International Conference on Social Computing (SocialCom) (pp. 843-850). IEEE.

Pearson, S., & Benameur, A. (2010). Privacy, security and trust issues arising form cloud computing. *Cloud Computing Technology and Science (CloudCom)*, (pp. 693-702).

TechTarget (2005), End User License Agreement (EULA), Retrieved December 20, 2016 from http://searchcio.techtarget.com/definition/End-User-License-Agreement

Valve (2015), STEAM, Retrieved December 21, 2016 from https://support.steampowered.com/kb_article.php?ref=3415-WAFH-6433#whatisascam

Valve (2016), STEAM, Retrieved December 19, 2016 from http://store.steampowered.com/

Van Summeren, R. (2011). Security in online gaming. *Bachelor Thesis, Radboud University Nijmegen*.