Department of Computer
and Systems Sciences

Computer and Systems Sciences

Stockholm University

Gamers' Information Security Risks Awareness and their Actual Online Behavior

An exploratory study of the relationship between gamers' understanding of information security risks (phishing, account theft etc) and their actual online behavior within gaming communities

Akuen Akoi Deng

akuiendng@gmail.com

Eimantas Butkus

butkus505@gmail.com

Abstract

During the societal shutdown due to Covid-19, the gaming industry emerged as the biggest entertainment industry soaring in popularity among all age groups. Despite the growing popularity of online gaming, little research has examined how gamers perceive information security risks in these communities. This study explores the relationship between gamers' awareness of information security risks and their online behavior within gaming communities. Applying surveys as the main research strategy, the data was collected through an online questionnaire form and semi-structured interviews with 3 online gamers analyzed using thematic analysis. The findings show that the more an individual(gamer) is knowledgeable about information security the more they are concerned and cautious about it and their actions. Similarly, the less knowledge they possess, the less they are concerned or cautious. Lastly, we can see that those with previous experience of an attack or risk were successfully able to identify the threat when faced with. These findings suggest that the level of concern and caution is directly proportional to the level of information security risks awareness and previous experience helps gamers identify threats and act more appropriately. This study highlights the need for more indepth research into understanding gamers perception of information risks and information security awareness programs tailored to gaming communities.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

Distributed Denial-of-Service (DDoS)

Two Factor Authentication (2FA)

Personal computer (PC)

1 Introduction

1.1 Background

The use of computers and other digital devices has become an integral part of our society today. Despite all the different applications and uses of computers and the internet, the gaming industry has emerged as the biggest entertainment industry today (Dahabiyeh et al., 2021) and (Kröger et al., 2023). This was in some form contributed by the recent societal shutdown due to covid 19 (Zolkiffli et al., 2023). Today we see an increased number of people of all age groups; children, young adults and others, highly active and taking part in online gaming, both single and multiplayer(Zolkiffli et al., 2023).

Due to constant and rapid technological advancements, the gaming industry is getting more advanced and sophisticated with real time interactive games, multiplayer online games and virtual reality gaming experience. With these advancements, we see an increased number of players all over the world participating and interacting. However, this surge in the number of gamers along with the intricate and interconnected nature of modern games has made the gaming industry a prime target and victim of information and cyber security threats.

In the digital space, all devices and users are increasingly exposed to the ever increasing risks of information and cybersecurity attacks. According to Szatmáry (2024), information security concerns such as Distributed Denial-of-Service (DDoS) attacks, ransomware, and data breaches are a few examples facing the gaming industry today. At the company level, information security breaches can lead to financial losses and operational disruptions hence eroding gamers' trust and loyalty, causing reputational damage and negatively impacting gamers experiences (Szatmáry, 2024). At the user level, with increased online interactions, gamers are at risk of phishing, social engineering, account and identity theft (Zhuang, 2023).

As cyber attack techniques get more sophisticated and creative, they usually exploit the user behaviour, information security awareness and hygiene practices. Frequently, some of these attacks both at company and user level may be due to user behaviour and information security ignorance while using the gaming platform or interacting with other gamers (Zolkiffli et al., 2023). Information security awareness can be defined as fundamental knowledge of the basic information security risks, threats and practices while user behaviour for gamers in our case, can be defined as the decisions and actions taken by a gamer when interacting or sharing personal information with other individuals on the gaming platform or communities.

Based on the theory of planned behaviour, we understand that an individuals' behaviour and action are mostly influenced by three factors;

(1) attitude towards the behaviour - this refers to an individual's positive or negative evaluation of performing a behavior i.e If a gamer believes that using two-factor authentication (2FA) is beneficial and easy to use, they are more likely to adopt it.

(2) subjective norms - this refers to social pressure or the influence of others (friends, family, community) on whether a person engages in a behavior i.e if most gamers in a community emphasize the importance of cybersecurity (e.g., avoiding phishing scams), an individual is more likely to follow safe practices.

(3) perceived behaviour control - this refers to a person's perception of how easy or difficult it is to perform the behavior, considering external and internal factors i.e if a gamer believes they lack the technical skills to enable security settings, they might not take protective actions, even if they recognize the risks. (Sommestad, T. et al, 2017) and (van Steen, T and Deeleman, J.R.A., 2021).

1.2 Research problem

As mentioned above, several important things for research problems have been discussed. In the video game industry, there is a threat to the players' information security. There are regular attempts of account theft, phishing and other security breaches on gamers (Zhuang, 2023). These threats usually exploit the user's ignorance of information security, hygiene and online behaviour to be successful (Zolkiffli et al., 2023). Therefore, as more devices and users connect to the internet and the population of gamers constantly increases, these risks increase as well.

In an attempt to help reduce the risk of these information security threats in the gaming community and industry, several studies of user behaviour (gamers) have been conducted to uncover and understand their online behaviour, especially gamers' information security behaviour. In a study, Zolkiffli et al., (2023) state that "casual gamers, especially those without knowledge and unskilled with security, cause most online game cybersecurity issues" due to their online behaviour. In another study, in an attempt to examine factors that motivate gamers' information security behaviours, Zhuang (2023) suggests that raising one's awareness of security threats should increase their adoption of security behaviours.

Despite this suggestion, according to the best of our knowledge at the time of this study, there is no empirical proof or study conducted to prove this to be always true. Evidence contradicting Zhuang's (2023) suggestion can be seen in a study to "examine users' awareness of and perception of information security issues" by Hamid et al., (2014) where they found that the users possessed a high level of information security awareness, however, they still fell victim to information security threats.

What remains missing is an investigation of how gamers' knowledge of information security correlates to specific and practical security actions and decisions in their real-life gaming context. This study explicitly identified a need for future research to examine "greater variety of survey questions pertaining to security behavior by asking about: two-factor authentication, password strength, manual privacy settings, and more" (Zhuang, 2023). Also, while previous studies have acknowledged risks and awareness generally, they do not go deeply into how gamers' awareness of information security correlates to their decisions which this study aims to look into. This is why it is important to understand the true relationship between knowledge and actions as it could help to prevent further information security threats.

Therefore, this study aims to address this gap of research by looking into the relationship between gamers' information security knowledge, their self-reported security actions and their decision-making in real-life situations. Because of the study scope, this study will not go into reasons for why decisions are made, it will only look into what they are.

1.3 Aim and research question

As outlined in the problem section above, the aim of this research is attempt to investigate how knowledge of information security and actual video gamers' behaviour correlate. It will look into how gamers try to avoid their information from being leaked or stolen by evaluating whether;

- They experience phishing and other kinds of social engineering?
- How often does it occur and what precautions are taken to not fall for it?
- Even if gamers have acquired knowledge on how to protect themselves, do they use that knowledge daily in their behaviour while playing video games?

To achieve the aim of this study, we will address the following research question;

1. *How does gamers' knowledge of information security correlate to decision making and action in real life?*

1.4 Delimitations of the study

Delimitations of this study include that it only aims to look at the relationship between knowledge of gamers' regarding information security and how they act in real life situations. But it does not try to classify them in any way because of the scope of the study. Also, it is limited to participants being from a couple countries in Europe so it cannot be generalized for the whole world population. The limitation for specific countries to use for participation is because of the connection as to who can participate in surveys and interviews. Because of those restrictions, the delimitation of this study goes down to a couple countries. The study is also limited to gamers aged 18 and above. That is because of needing consent from parents if aged below 18 and because study has to be conducted faster it was decided to keep it at 18 and above.

1.5 Use of ChatGPT

No prompts from chatgpt/gemini were used because there was no reason at this point of research. All the necessary information has been provided and research questions came up from previous experience. As chatgpt is mostly used to generate ideas for research it was not needed. If there would be a need for explanation of concepts or ideas how to summarize results then chatgpt would be helpful. These tools were also used to refine the interview transcripts generated from the audio transcription tools.

2 Method

2.1 Research strategy

According to Denscombe (2014), one of the most important aspects of a study is choosing a research study appropriate to the research problem and aim. He points out that there is no single pathway to the choice since there are always alternatives (Denscombe, 2014, p.51).

For this study, to explore and understand the relationship between gamers' knowledge of information security and their actual online behavior by answering the research question. We found using the survey strategy as the best fit. This is because this strategy type gives us the ability to reach the relevant people but in a generalised way. By conducting a survey, we can potentially reach all sub-groups of gamers; the casual gamers, hobbyist and addicted gamers group. Along with this, knowledge of information security is subjective to individual gamers, meaning some are ignorant, some have intermediate knowledge while others advanced. Applying a survey gives a wide and inclusive coverage hence advantageous for our research aim and problem (Denscombe, 2014, p.54).

Our research question has two different variables; knowledge of information security risks and threats and actual online behaviour. In order to draw any significant relationship between these two, we need to capture them well simultaneously, in a generalised way and without introducing any bias. Applying a survey with methods such as interviews and questionnaires and all the possible techniques of distribution can help achieve this aim better than other possible strategies without introducing creation of any controlled settings or environment.

Other possible research strategies such as sampling, case study and mixed methods were considered. However, due to the limited time scope of the study and the need of a controlled environment for some, these alternative strategies were found to be not suitable. For example, if the time scope was not limited, an alternate strategy would have been sampling. This would involve gathering two different sample groups of gamers; one composed of those knowledgeable in information security risks and practices and another with those without. These two sample groups would then be presented with a similar security threat while placed in a gaming setting then observed. This approach would yield a more indepth observation and understanding into their behaviour and choices. However, it would be highly time and resource consuming.

Therefore, due to the nature of the research problem, the need to reach a wide, inclusive and generalised gamers' and the limited time scope, using a survey was found to be the best fitting. This decision was drawn and concluded after a wide exploration of all the potential strategies as shown by the example above.

2.2 Data Collection Method

As previously discussed in the strategy section, we choose the survey as the most appropriate strategy for this study. According to Denscombe (2014), surveys differ in terms of techniques they use to communicate with respondents. He continues to outline these as; postal, face-to-face, phone, email, web and social media based surveys (Denscombe, 2014, p.55). Due to the nature of the research aim and problem, to answer the research question adequately, we need to collect both qualitative and quantitative data through interviews and questionnaires. To collect these data, we believe that using web-based, social media and email survey methods would be the most appropriate choices. We considered other alternatives such as, postal, face-to-face and phone based surveys, however, due to factors such as cost and time delay as discussed by Denscombe (2014), these options were deemed as not appropriate for this research at this particular time.

As briefly mentioned above, we choose both the questionnaire and interview data collection methods for this research. These two will give us wide and inclusive coverage via the questionnaire and an in

depth view via the interviews. The initial plan is to capture a minimum of 15 full respondes on the questionnaires and at least 3 interviews. Other methods such as observation and documents and images would be viable options, however, we saw no appropriate suitability of these methods when dealing with survey research strategy.

In a similar study conducted by Zhuang (2023) to explore the information security behavior of gamers, he similarly applied the survey research strategy along with web-based survey questionnaires to capture quantitative data to examine factors that motivate gamers' information security behaviors.

To help collect the most suitable data from the respondents, the questions in both the interviews and questionnaires will be carefully desired to reflect example scenarios of security risk in a gaming environment along with using the domain knowledge of both gaming and information security. The respondents will be expected to answer as they would react, respond and act given the scenario. The questions will be constructed in a simplified manner to eliminate any bias since different gamings have different levels of understanding of the information security risks and threats.

2.3 Data Collection Strategy

The ideal participant pool consists of active video game players between 18 and 35 years old who play video games weekly and are located in Europe. Because of the study's scope limitation, the participant pool is limited, and diversity is a struggle in this case. This age range was selected because it is most likely for people who are participating in video games and are susceptible to cyber-attacks.

Ideal participant selection would use a random sample to ensure that as many different video game genre players could participate in the survey. This could help comprehend how different genre gamers respond to cyber security as well as keeping selection bias to a minimum and maximizing the generalization of the results to the target population. An ideal recruitment process would be to directly collaborate with game publishers within Europe. They would send surveys to players of their platforms, to the age range of 18 and 35 as well as meeting requirements of weekly play time and having locations within Europe. This way it would provide a representative sample, having a great response rate and minimizing self-selection bias.

Because of the research scope being small and short time selection of participants will not go through ideal choosing. Participants will be chosen from contacts of researchers as well as additional forums for whoever can do the survey. It will not be asked what genre of games they play so the survey will not be able to give results based on the genre of games participants play and how to respond to cyber security. That is unfortunate, but again because of the scope of the study, it is most appropriate to have as many participants as possible without giving too much time to select perfect candidates. This way is chosen because of feasibility and accessibility, because of lack of time and resources it would be the best approach to collecting data. While this way will not allow to generalize to a bigger population it would potentially give insight on cybersecurity and video game players' perception of it.

Biases of chosen sample would include sampling bias, self-selection bias, snowball bias as well as limited generalizability. Sampling bias because the selection of friends and participants from forums would not represent the general European gaming population. Some genres and demographic groups could be more often present than others. An example could be a specific video game genre that could have players with better knowledge about computers including cybersecurity than other groups. Self-selection bias if people from forums and similar choose to respond to surveys themselves they could be different from others. Perhaps more technologically advanced, and more aware of cybersecurity and its threats. Snowball bias is that participants recruited through referrals could have the same opinions and knowledge as the previous participants and would limit diversity in answers. Limited generalizability is basically that people aged from 18 to 35 and from Europe cannot be generalized to the whole video game player population of the world. It could provide insight and some trends but never can be used to generalize to the whole population.

Data will be collected using online surveys with questions regarding video games as well as participant knowledge of cybersecurity and its risk including real-life situations and their responses to

them. The link to the survey will be posted in an online forum for gamers to access as well as through private messages within the gaming community. Also, initial participants will be encouraged to share with others to get as many results as possible.

2.4 Data Analysis Method

As discussed in the data collection and collection strategy in the previous sections, using interviews and questionnaires, we will collect qualitative data from random subjects from different geographical areas, age, gender and nationalities. The resulting data from these two activities will be carefully analysed using different methods and techniques.

The data collected from the survey questionnaire will be carefully analysed and used to get a general understanding of the different sub-groups of gamers as mentioned in other sections previously. Gamers will be grouped based on their gender, age, nationality and others in an attempt to understand whether such factors play any significant role in their behaviour and actions. This is because for example, a good percentage of gamers today is composed of children barely above 15 years old and the general assumption would be that, this age group can be totally oblivious about information security and their own behaviour most of the time. These sub-groups will help bring more understanding into what other key factors play a role.

The interviews will be recorded and transcribed for careful analysis which will provide a more in-depth insight. Following the six steps of Braun and Clarke's approach, the following steps will be used in analysing both data from the questionnaire and interview:

1. ***Familiarisation with the data***

   This step will involve the transcription and documentation of both the interview audio and questionnaire responses. We will read and familiarise ourselves with the content of data and information briefly before drawing any relationships or significant observation towards a conclusive point.

2. ***Generating initial codes***

   After carefully familiarising ourselves with the data, in this step, we will generate the initial codes to be applied for thematic coding and analysis.

3. ***generating themes***

   Based on the previously generated codes, we will respectively generate the themes for the data encoding. The themes will generally be based on both knowledge of information security and the behaviour or action choices of a gamer. This will facilitate the actualization of any correlation that might exist between the two variables.

4. ***reviewing potential themes***

   This step will involve reviewing and revision of the previously generated themes. As stated by Braun & Clarke (2022), it involves "a recursive review of the candidate themes in relation to the coded data items and the entire dataset".

5. ***defining and naming theme***

   This step will involve renaming and defining of the themes to ensure consistency and coherency across the thematic encoding of the dataset.

6. ***producing the report***

   This last step is basically the finalisation and reporting of the conclusions drawn from the encoding process that can be used to draw conclusive results for the study and answer the research question.

Below is a brief illustration of an example of the thematic encoding and the result from the process defined above. The statements, code and themes and just examples and not the final.

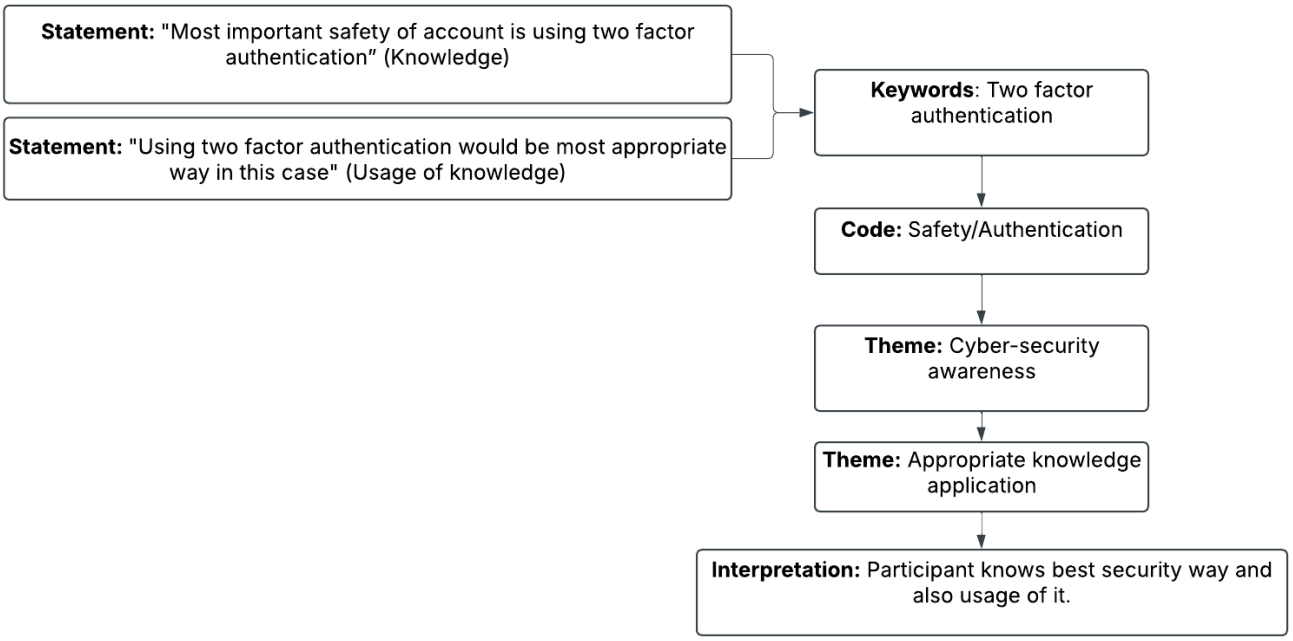

Figure 1 thematic encoding method with example

2.5 Research Ethics

As this study is doing both surveys as well as interviews there will be two different consent forms. One will be presented in the online survey first page so that participants can read through it and agree or disagree to participate in the survey. For the interview a separate consent form will be presented. Ethical consideration that has to be taken account for is anonymity, security of data provided and right to withdraw from study if participant wants to. Surveys as well as interviews will be conducted anonymously to keep the integrity of the participants. Data will be saved for 6 months and deleted afterwards. There is no risk for participants, as they are not exposed to any physical test or mental ones.

Debriefing will be done both after surveys and interviews. Participants will be thanked for participating as well as debrief on what this study is aimed for as well as their right to withdraw their results.

3 Results

3.1 Data Collection and Analysis

Survey questionnaire

As described in the previous section, we collected data via both survey questionnaires and interviews. The Questionnaire was composed of sixteen questions divided into several sections; personal profile, gaming profile, information awareness, and information security experience and practices. The design of these questions was inspired by a similar study conducted by Zhuang (2023). However, some questions were modified and others were totally created based on our specific research question and aim. The consensual form for the survey was shared along with the questionnaire and respondents were prompted to read and consent before taking the questionnaire questions as shown in (appendix B). The questionnaire was open for a total of 9 days between March 2nd and 10th 2025. Considering that the targeted subjects were only gamers, the survey link was shared with people we know within our circle that are gamers. These individuals were also asked to share the link to other gamers' friends within their friends groups and gaming forums. The link was shared via email, discord, WhatsApp and other gaming community forums we had access to. The survey was also targeted for individuals above eighteen years old hence during the review process, one response was discarded since the respondent was seventeen years old. The survey responses were kept completely anonymous and no email or personal data was collected. It was also designed in a way that the respondent could only answer once to prevent redundancy and duplication in the data.

Before analysing the questionnaire responses, we firstly reviewed the data in an Excel sheet to ensure there were no faults or invalid responses in the data. We received a total of thirty valid responses which were individually reviewed to ensure all the questions had been correctly answered. We proceeded by generating charts and graphs to compare and see the relationship between the results from various questions. Examples of these charts can be seen below in figure 2. Further reviewing and analysis of the data were conducted in Microsoft Excel sheet and Google questionnaire tools.

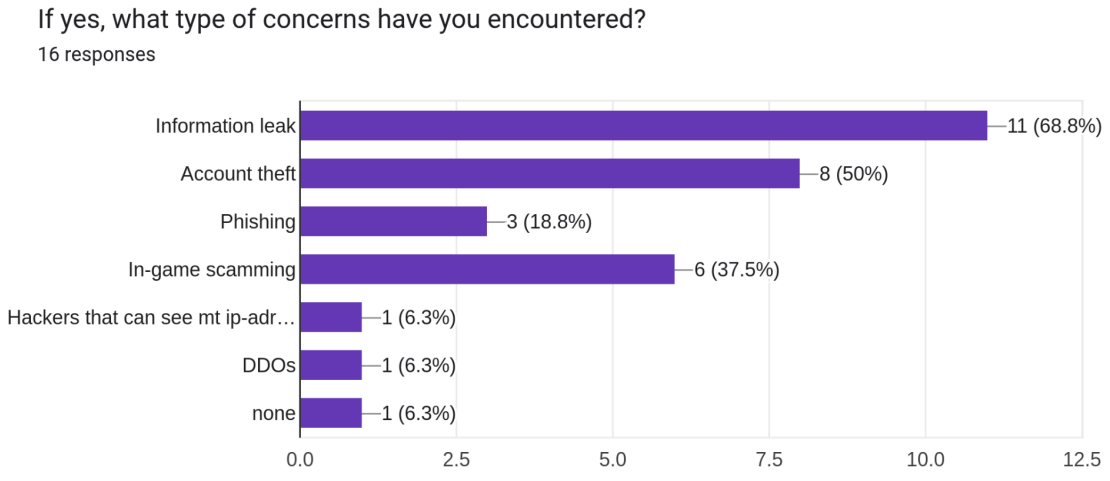

Figure 2 Bar graph of concerns encountered

Interview

The interview participants were selected based on availability and also randomly to prevent expert bias. After getting five people willing to participate in the interviews, we selected three people at random. Since the interviews were meant to give complementary in depth data to the survey, we ensured that the participants had also taken the survey. The interviewees were of different ages above eighteen years old and different nationalities. The interview questions followed the same format as the questionnaire questions (as shown in appendix D). However, they were designed to give a more in depth view. They were divided into five sections; gamers profile and experience, awareness of information security risks, personal security practices, experience with security incidents and lastly community and social influence. The questions were inspired by our own experience in both gaming, information security knowledge and experience and based on the theory of planned behaviour. For example, asking questions about community and social influence to determine how the aspect of subjective norms (peer pressure) influences individual gamer's actions.

The interviews were conducted online via zoom or discord calls where the audio was recorded in a4m format. A day or hours before the interview, the consent form (shown in appendix B) was shared with the participants which outline research aim and summary, researchers contact details and data handling policies throughout the study. Also 30 minutes before the interview started, the interview questions were sent out to the participants to help them familiarise themselves with them and help the interview process move smoothly and fast. We believed that in doing so, the participants would have time to think about the questions hence give a more in depth explanation whenever necessary. The interview audio was recorded by recording the zoom or discord call screen, by using a mobile audio recorder and using tools such as Audacity. The recorded audios in a4m format were transcribed using tools such as Seshat Audio Transcriber provided by the university. These transcribed interviews in text format were then converted to microsoft word version, refined using tools such as ChatGPT and Gemini. Lastly, the final version of the transcription was verified by listening to the audio while reading the text line by line. This ensured no data was added, lost or modified in any form throughout the process of transcription and refinement.

To analyse the interview data, we applied thematic encoding as proposed in the previous section. We followed the six steps of Braun and Clarke's approach.

step 1: Familiarisation with the data

This step was implemented through the process of transcribing the audio data of the interviews. We converted the a4m audio recording to text via Seshat Audio transcriber. We read through these transcriptions to ensure consistency with the original audio, followed by refining the text with tools such as ChatGPT and Gemini. This consistent reading of the interview material overtime, made us much familiar with the content of each individual interview.

step 2: Generating initial codes

In this step, we looked at each individual question in the interview and how it was answered by the interviewees. By comparing the responses for the same question, we derived patterns using keywords and phrases. These keywords were used to generate the first initial codes. For example, when we looked at the question,

"How often do you interact with other players online for example chat voice forums or discord?"

The respondents used keywords such as "chat", "voice chat", "discord", and "in-game chat" to refer to their interactions and platforms they use to communicate with other gamers.

"Yeah, if I play online games then I interact with my friends via Discord or other call methods and often I chat in-game also."

"...I read or write messages in chat and then sometimes use voice chat…"

based on the consistency of these keywords in reference to their interactions, we generated the initial code “chat”. This can be seen more elaborately in table 1.

step 3: generating themes

In this step, based on the codes generated in step 2 previously, we developed initial codes to group similar codes together. We took codes that were referring to the same ideology or concept and generated a theme to cover them. For example, in the previous step, we generated the initial code “chat” and after exploring and comparing it with other codes we had, finding no similar code related to it, we generated the theme “interaction” to cover the idea of interaction, or communication among gamers. This theme and how it was developed can also be seen in table 1 below.

How often do you interact with other players online for example chat voice forums or discord?	Phrase	Code/Keyword	Theme
Participant 1	“Let's say like three four times a week”	Chat	Interaction
Participant 2	“Yeah, if I play online games then I interact with my friends via Discord or other call methods and often I chat in-game also.”	Chat	
Participant 3	“Yeah, I do that.” Every day in some form. I read or write messages in chat and then sometimes use voice chat.	Chat	

Table 1: Generation of theme interaction

example 2:

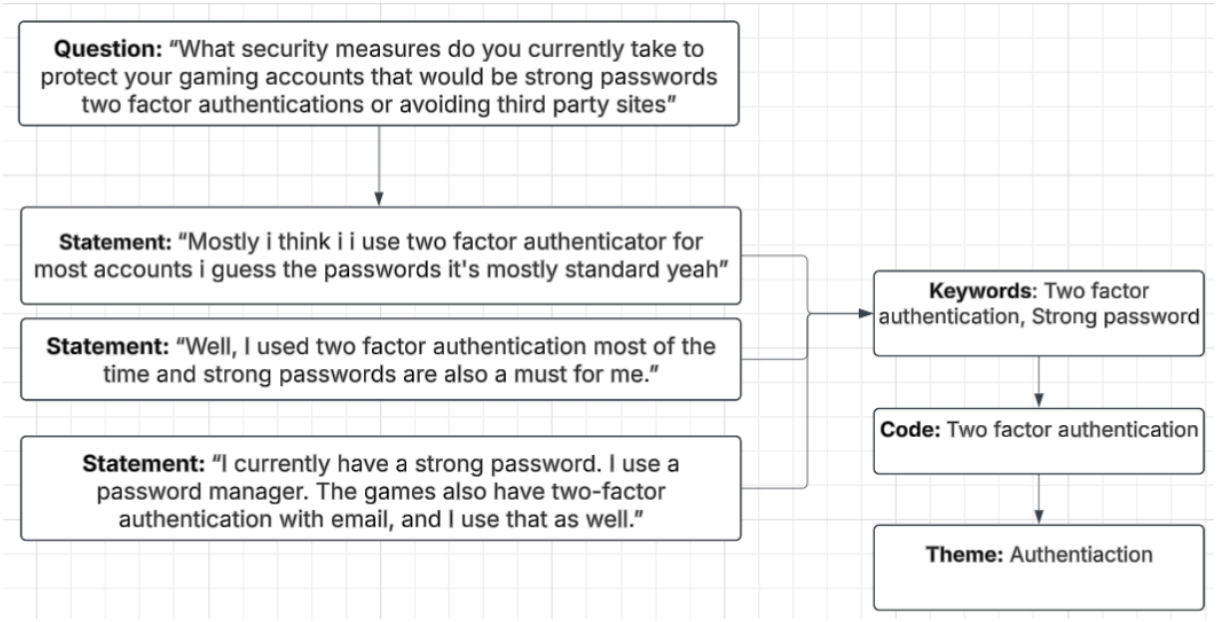

Figure 3: example of thematic encoding implementation

step 4: reviewing potential themes

After familiarizing ourselves with the data through the process of transcription and reading through the transcripts several times in step 1, we developed initial codes such as *scammed, two factor authentication, trust, family and friends, chat rooms* in step 2 just to mention a few. From these codes we developed themes such as interactions, cyber attacks, authentication, and vulnerability in the previous step, step 3. In this step, we reviewed all the potential themes we had developed in the previous section by looking for similarities and differences. Themes that seemed too closely related were to be merged into a single new theme while those that seemed to broaden were to be broken down into different independent themes. However, due to the small size of our interviews, there were no themes found to be too similar or broad worth merging or breaking down hence, we ended up with 4 key themes; interaction , cyber attack, authentication and vulnerability. These themes can be seen in table 1 above and through table 2 - 4 shown below.

How familiar are you with online security threats such as phishing, account theft or scams in gaming?	Phrase	Code/Keyword	Theme
Participant 1	"yes i was scammed when i was little i think"	Scammed	

Participant 2	“Well, I have heard about it quite often because in the games I play the gambling community is quite big and the phishing community also the account thefts are quite notorious. So, I have known about it for quite some time now.”	Phishing, Account theft	Cyber attacks
Participant 3	“I know that they can happen, that people could steal information, try to steal accounts, and things like that. I know it's very common if you have bad passwords.”	Steal information, bad passwords	

Table 2: Generation of theme cyber attacks

“What security measures do you currently take to protect your gaming accounts that would be strong passwords two factor authentications or avoiding third party sites”	Phrase	Code/Keyword	Theme
Participant 1	“Mostly i think i i use two factor authenticator for most accounts i guess the passwords it's mostly standard yeah”	Two factor authenticator, Strong Password	Authentication
Participant 2	“Well, I used two factor authentication most of the time and strong passwords are also a must for me.”	Two factor authenticator, Strong Password	
Participant 3	“I currently have a strong password. I use a password manager. The games also have two-factor authentication with email, and I use that as well.”	Two factor authenticator, Strong Password	

Table 3: Generation of theme authentication

“Have you ever shared your gaming account credentials with anyone? If so, why?”	Phrase	Code	Theme
Participant 1	“yes with my close friends because i trust them”	Sharing account	Vulnerability
Participant 2	“I've shared it with my friends because they wanted to play some games and they did not have an account. But those friends I know in real life so I'm not worried about them stealing my account. That's no problem for me I think.”	Sharing account	
Participant 3	“Yeah, with my family, I have. It's mostly to let them play on the same account, so they don't have to buy the game or content separately.”	Sharing account	

Table 4: Generation of theme vulnerability

step 5: defining and naming theme

In this step we defined and named all the previously mentioned 4 themes.

The 'Interaction' theme relates to player communication and categorizes the various ways they engage socially within the gaming communities and while playing.
The ‘cyber attack’ theme related to gamers' understanding of possible attacks and risks within information security. It was renamed from attack to the current name to reflect a more general idea.
The 'Authentication' theme relates to security measures gamers used to protect gaming accounts. It also demonstrates participants' proactive use of security measures to protect their accounts.
The 'Vulnerability' theme relates to any risking behaviour or actions gamers take despite their level of information security awareness.

3.2 Findings

This section presents findings aimed at answering the research question "*How does gamers' knowledge of information security correlate to decision making and action in real life?"*. The number of responses from surveys received was 30 and interviews done on 3 separate participants. The majority of participants were male at 90% and the age of participants were between 18 years old and oldest being 30. At which majority of participants were aged 19 at 23.3% as well as 25 years old at 20%. Nationality of participants were a bit more diverse than expected, but the majority was Lithuanian at 50% and second most common being Swedish at 36.6%. That was it for the personal profile of participants in surveys.
Gaming profile of participants included what platforms they use while gaming, how many hours they spend while gaming in a week and what types of video games they play. For what platforms do participants use while gaming majority was pc at 86.7% and equally for console and mobile phones with 26.7% each. How many hours played per week were diverse and can be seen in a figure 4. Were the most percentage being 0-5 hours per week at 40% and least amount of participants playing 20+ hours per week at 10%.

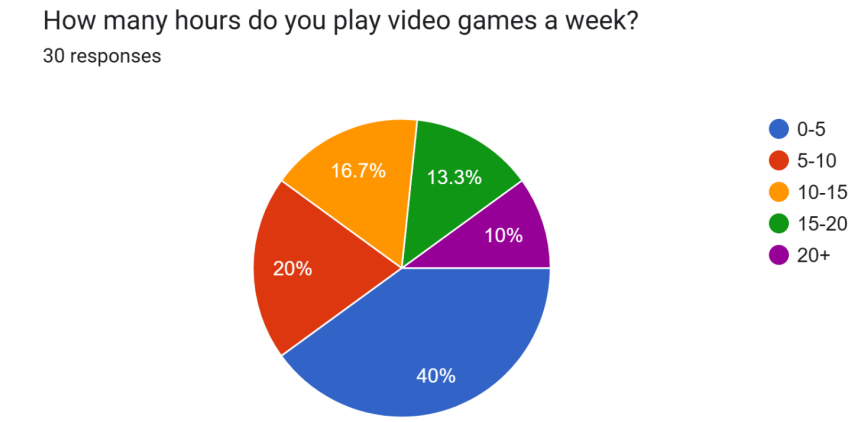

Figure 4 pie chart of how many hours do gamers play per week

The types of games played by participants were dominated by shooter type of games at 70% and action second at 43.3%. Casual and MMORPG have the same amount at 40% and can be seen in figure 5.

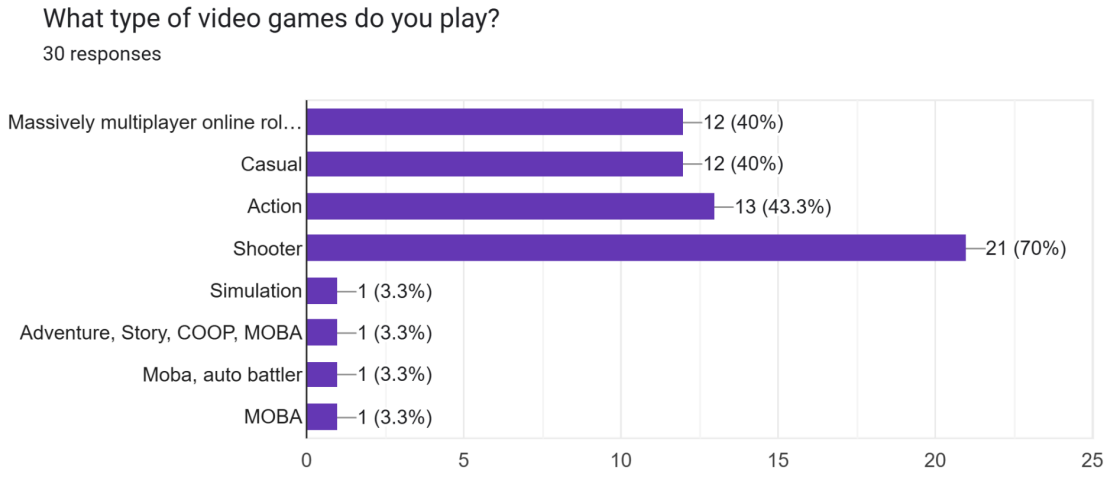

Figure 5 Bar graph of survey response to what type of video games do you play

And that would be it for the part of personal and gaming profiles from surveys.

Following questions were regarding information security and awareness. The survey started with asking participants if they had concerns regarding information security while playing video games. From which 56.7% participants answered “No” and the remaining answered “Yes”. Then the following question was if the participants have had concerns then what kind of concerns they were. And the primary answer for this was “Information Leak” at 68.8%. Remaining answers can be seen in the figure 2. Which then follows with how would each participant rank their awareness of information security. Where the majority of participants have identified their awareness at 5 out of 10. But as can be seen in the graph more people have ranked their awareness on a higher side with only 3 participants ranking them at 10 out of 10 and can be seen in figure 6. This is how gamers perceive their awareness of information security.

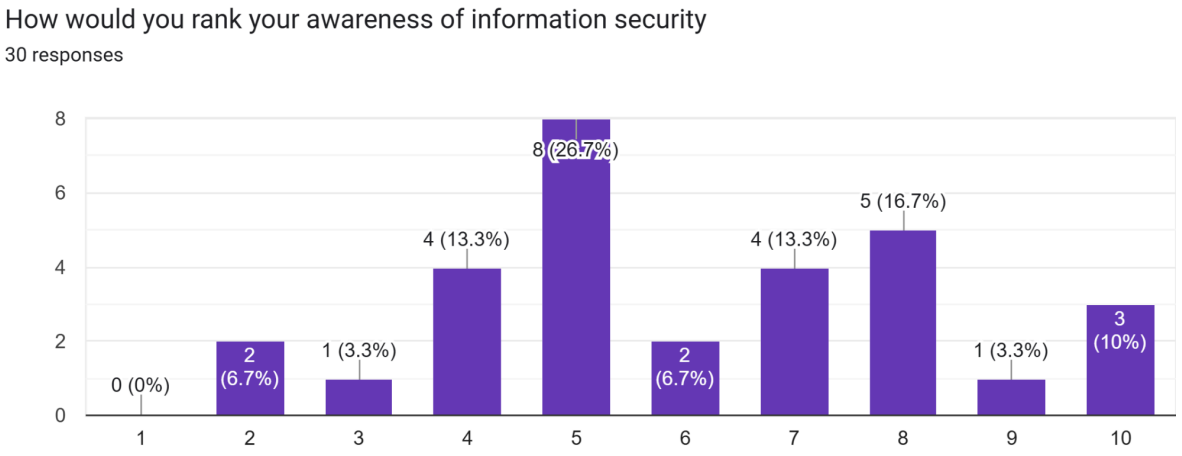

Figure 6 information security awareness ranking

Following questions included experience while gaming as well as practices they use to secure their safety while playing video games. Only 5 participants have identified that they have experienced phishing while playing video games. Following question asked people that have experienced it what it was about and what measures they take. Most common answer was that “Received a link to do X and enter credentials”. And measures they took was either to ignore it or block the sender immediately. Which shows understanding of how to protect themselves from these kinds of attacks. For the people who answered that they did not experience phishing, the following question was do they know what it means. While most of them answered they do and couple including definitions such as “ When a scammer pretends to be someone else and tries to get information from you”, some of participants did not know what it meant or did not know the definition of it. Following question was regarding have they ever reported incidents of online security to a respective game company. Because not many people have experienced the incidents, only 3 people have said that they have reported it. And the experience was either the company saying it is your own responsibility to make sure your account is secure or helping them with getting back their accounts.
And finally questions regarding practices included do people have antivirus software on their machines and how regularly do they change their passwords.

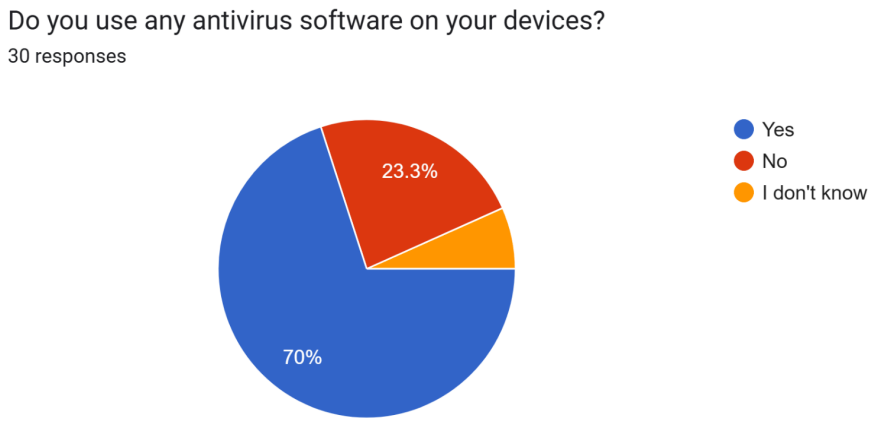

Figure 7 antivirus software results

As can be seen in the chart around 70% of people do have antivirus software on their machines, 23.3% don't have it and 2 participants don't know if they do see figure 7. This is quite a high number of participants that do have software that protects their machines. Following and last question included how often do they change their passwords. And 70% of participants answered that they never change their passwords. There was one person who responded that they do not change their passwords but identified that a 2 factor authentication is more important which does show some understanding of information security. Rest of participants answered that they do change their passwords rarely or they rotate them. We also can see a chart that showcases how many participants have answered that they do not have concerns regarding information security and how often they change their password can be seen in figure 8. It shows that only 11.1% of participants change their passwords once in a while.

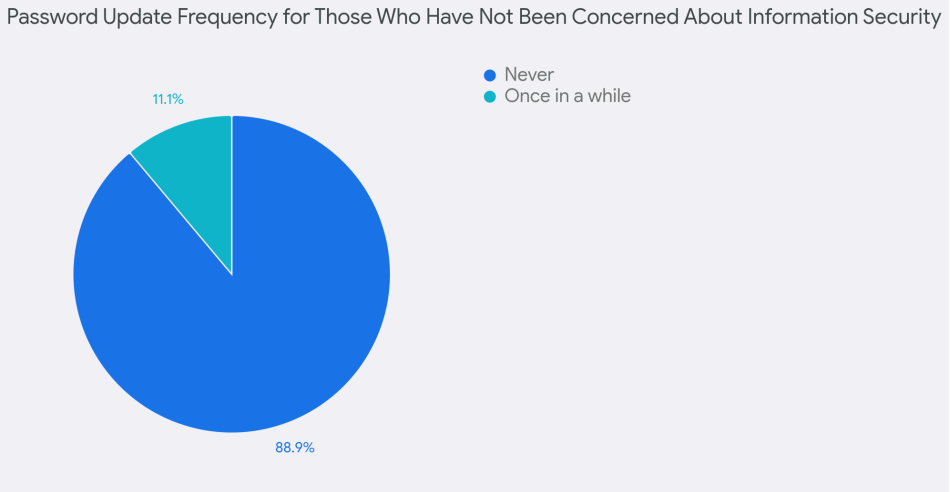

Figure 8 password update frequency for those who are not concerned about information security

Moving on to another chart that showcases how many console users are concerned about information security figure 9. Only 11.1% have concerns. This could lead to some speculation that console users are not that interacted in information security threats or they play single player games where there is no social interaction whatsoever. As well as the only person who answers that they do have concerns is a player who also plays on PC and mobile phone. Which further could prove that social interaction could lead to information security risks, especially phishing.

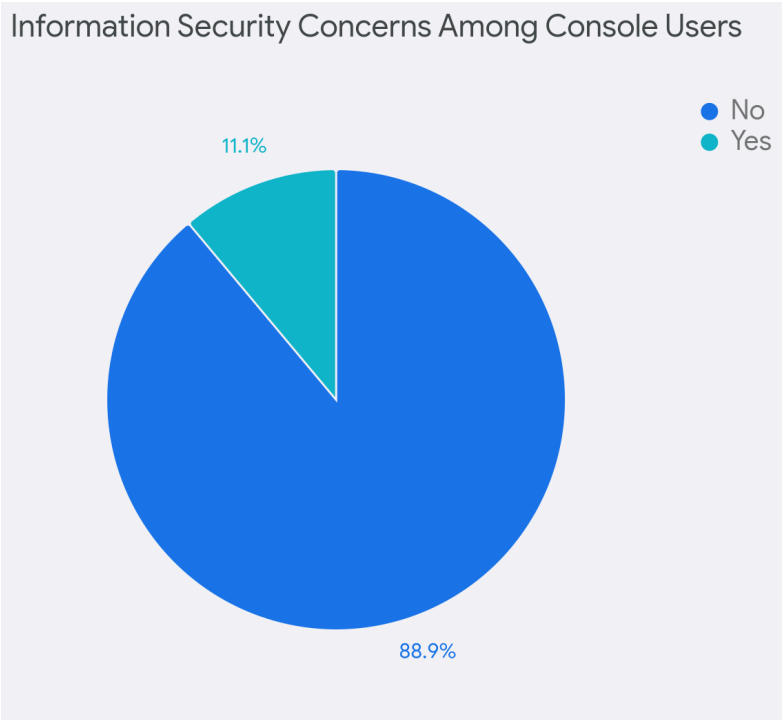

Figure 9 information security concerns among console users

Another two charts showcase how many people are concerned about information security based on how they rank their awareness of it figure 10 and figure 11. On the first chart we can see that participants who ranked their awareness 5 or below out of 10 were much less concerned regarding information security then the ones that ranked their awareness above 5. The correlation between self-reported awareness and concerns could indicate indeed that knowledge and understanding may correlate to a security behaviour of gamers while playing.

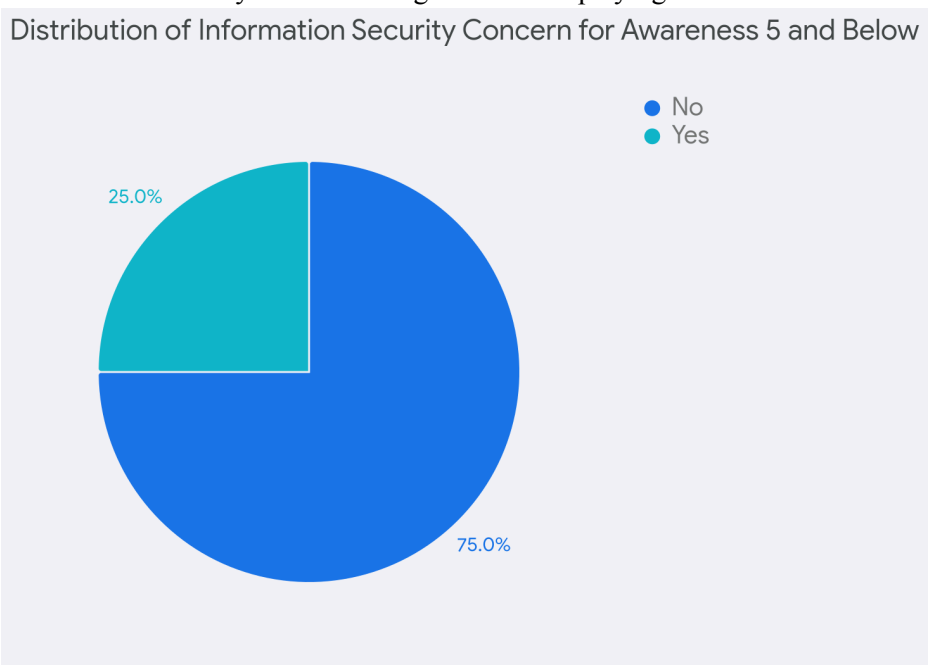

Figure 10 distribution of information security concerns for awareness 5 and below

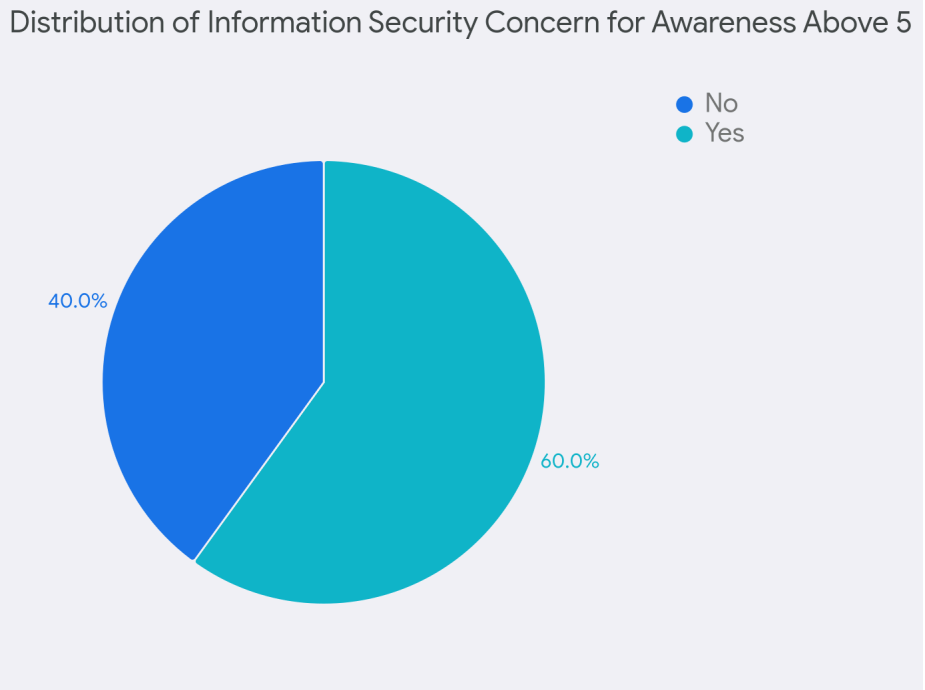

Figure 11 distribution of information security concerns for awareness above 5

Interviews themes and key findings :

Themes:

1. **Interaction:** This theme was developed after identifying the interaction patterns of gamers on the gaming platforms and other community forums. Most responses indicated that gamers at least interact with other gamers on a daily basis mostly via chat.
2. **Cyber attacks:** This theme was developed after identifying the most frequent form of attack that gamers experience. Most respondents identified “scamming” as a reference to phishing and other forms of social engineering attack methods.
3. **Authentication:** This theme was developed after identifying what respondents view as the most basic and efficient way of protecting their accounts and data. Most elaborated their understanding of two factor authentication methods as their most frequent choice.
4. **Vulnerability:** This theme was developed by identifying potential weaknesses that appeared most among the interviewee. Despite individual levels of information security awareness, all respondents showed that they trust and share their gaming credentials with close friends and family which could be identified as a potential vulnerability.

The 'Interaction' theme emerged from coding key phrases related to player communication. The process began by identifying important phrases from interview responses to the question: "How often do you interact with other players... by chat, voice, forums, or Discord?" Participants consistently indicated frequent interaction, with phrases like "I chat in-game" and using external platforms like "Discord". These phrases were initially coded with a focus on the method of interaction, such as "chat". Because the core of all these responses related to the act of players connecting and communicating, the overarching theme of 'Interaction' was developed. This theme categorizes the various ways players engage socially, which is relevant for understanding potential information security risks that may arise from these interactions. (See Table 1).

The 'Cyber Attacks' theme emerged in a similar manner, but focused on responses to the question about familiarity with information security risks. Key phrases were extracted from participant answers, including mentions of "scamming," "account theft," "phishing," and "steal information." These phrases, while diverse, were all coded based on the type of threat they represented. The connection

was clear and showed, all of them had an important common connection, which is harmful, malicious activity; the theme 'Cyber Attacks' was created. This theme demonstrates participants' awareness of potential online threats within the gaming context. (See Table 2).

The 'Authentication' theme emerged from coding participant responses regarding security measures used to protect gaming accounts. The interview question directly asked about practices like "strong passwords, two-factor authentication, or avoiding third-party sites."
First, 'open codes' – direct quotes from participants – were identified. Examples include: "Mostly I think I use a two-factor authenticator for most accounts," and "I currently have a strong password. I use a password manager." These were then grouped into 'axial codes' based on the type of security measure. The primary axial codes were 'Two-Factor Authentication' and 'Strong Passwords'. Because all of the participants use ways to protect their accounts, which all do provide some way of authentication, the 'selective code'(theme) of 'Authentication' was chosen. This demonstrates participants' proactive use of security measures to protect their accounts. (See Table 3).

The 'Vulnerability' theme emerged from analyzing responses to the question: "Have you ever shared your gaming account credentials with anyone? If so, why?" This question directly explored a potential security risk. Key phrases were extracted from the participant answers, all of which confirmed sharing credentials. Examples include: "yes with my close friends because i trust them," and "Yeah, with my family, I have." The initial coding focused on the act of sharing, resulting in the code 'Sharing account'. Because all participants engaged in this behavior, which inherently creates a security vulnerability, despite the stated reasons (trust, convenience), the theme 'Vulnerability' was chosen. This theme highlights a common practice that could expose accounts to risk. (See Table 4).

4 Discussion

4.1 Analysis of the results

As described previously, this study aims to see how gamers' knowledge of information security correlates to decision-making and action in real life.

To answer our main research question; *How does gamers' knowledge of information security correlate to decision making and action in real life?*

We had to identify different aspects of how "knowledge" of information security can be categorised; we identified that information security knowledge can be;

i) general learned knowledge - something they learnt by reading, or were taught.

ii) experience based knowledge - something they experienced or fell victim to and learnt

From surveys it was deduced that the less knowledge regarding information security the person has the less concerns for it they have. And another aspect is that having previous experience directly correlates to avoiding making the same mistakes as done before.

knowledge confidence vs degree of concern

From surveys, we found that participants who self-reported awareness of information security higher than 5 out of 10 have had more concerns regarding the topic. In contrast, participants with self-reported awareness 5 and below have had fewer concerns regarding information security. This shows that knowledge of the topic could lead to more concerns and perhaps a better understanding of actions needed to protect themselves. This is further proven by participants who have reported that they do not have concerns regarding information security and also don't use known practices of updating their passwords regularly. This shows that, the more confident a gamer is in his/her knowledge and ability concerning information security, the higher their level of concern and hence are more inclined to take the appropriate actions and practices of information security. Additionally, this finding shows that the gamers decision making and action in real life is influenced by the level of confidence he/she has in their own knowledge. This can closely be related to the factor of perceived behaviour control from the theory of planned behaviour, that is, if the gamer perceives that they possess the knowledge and capability, they will have the confidence needed hence might be more inclined to make good decisions and take good action.

gaming platform vs degree of risk exposure

On another note, 70% of participants who play video games mainly on PC have identified that they have antivirus software installed on their machines, which showcases at least some understanding of security practices. On another hand, console users are mostly not concerned regarding information security. This could be from a lack of social interactions or their trust in the console ecosystem. These two findings show different groups of gamers on different platforms having different attitudes and perceptions towards their security practices and risk exposure. This shows that the type of gaming platform a gamer uses, influences their attitude towards their security risks hence he/she might behave more cautious or reckless based on this formed attitude.

Mimetic behavior (Authentication theme)

Moving onto interviews, participants have identified a great understanding of information security practices. Mentioning that they use strong passwords and almost always use two-factor authentication. This shows that they value their information and understand how to protect themselves. From this finding, we realised that, since the use of 2FA has become a very widely followed practice, most gamers in most cases are forced to mimic and adopt the behavior. This can closely be related to the factor of subjective norms from the theory of planned behaviour which suggests that social pressure or the influence of the majority, forces one to engage in a behaviour or practice. This suggests that, if more of the good information security practices are promoted and pushed by the gaming platforms, companies or communities, a great number of gamers would be influenced to make a similar decision or action (behaviour). This shows that mass knowledge (knowledge possessed by many people) can directly influence individual decision making and actions in real life.

Risk type frequency (Cyber attack theme)

When asked about real-life examples of information security risk, all the 3 participants identified the attempted scamming scheme straight away and said that they would either ignore it or also report it. In this finding, we saw that a great percentage of gamers can successfully identify phishing types. We also learnt that phishing is the most frequent type of attack that gamers encounter on different gaming platforms. This shows that, the frequency at which a particular risk occurs, contributes to a great percentage of gamers being knowledgeable about it hence can easily identify and avoid it.

Trust and human factor in information security

Vulnerability theme

Despite showing adequate knowledge of information security, on the downside, all of the participants have identified that they share their credentials with their family members who they trust. This could potentially lead to information security problems, as not all users of the account could be well versed in how to protect themselves from threats while playing games. A main owner of an account, even knowing how to protect information could potentially be a victim of information leakage and similar due to their sharing of credentials. This shows that personal values such as trust and generosity can influence the users decisions and actions despite their level of awareness.

Interaction theme

All of the participants of the interview have said that they actively participate in social interactions. Which could lead to some security concerns, mainly phishing and social engineering. But as they have identified what it is and how they can protect themselves it seems that it should not pose any danger. However, 2 of the participants have mentioned that they have fallen victim to phishing while being young. And that they have learned how to protect themselves in a hard way. This point shows that more caution and adherence to good security practices might be influenced by previous negative experiences such as falling victim to account theft or phishing.

Literature connection

Our findings show different relationships between knowledge and actions taken by gamers regarding information security. Higher awareness showed more concern and some good practices which would partially support what was said by Zhuang(2023). As well as on risks of low knowledge that was mentioned by (Zolkiffli et al., 2023). Also, showing there are still security risks for knowledgeable gamers who are sharing their credentials not always awareness and knowledge lead to better decisions which supports what was proposed by Hamid et al., (2014). Past experiences strongly affect how people act in decision-making which showcases that not only knowledge is a factor and points out that specific security behaviours still need more research as was suggested by Zhuang(2023).

4.2 Limitations and future research

As we know with all studies, there always exists limitations. For this study, some of the key limitations were that, despite the fact that a great percentage of active gamers today are children below 18 years old, the study was only limited to individuals between 18 to 30 years old which limited the scope. This led to the exclusion of a huge percentage of the age group that makes up today's gaming community. To mitigate this limitation and as part of future research, a more in depth feedback and insights into the topic could be done by involving subjects below 18 years old considering they happen to compose the majority of information security risk victims on gaming platforms. This would ensure that the study obtains fruitful and enormous data compared to this study.

Another limitation to this study was that the population that was available for both the survey and questionnaire was predominantly composed of males. The survey results included 90% males which would be hard to generalize to the whole gaming community. This could introduce some unpredicted biases to the final findings of the study. To mitigate this limitation, future research could target a broad and more gender diverse sample group.

Lastly, another limitation was the limited short time frame for the study. The whole study was conducted within 10 weeks which limited the scope and depth of analysis and investigation that we could have performed. Due to this factor some potential gaps and concerns were left unexplored. For future research, other studies could investigate the effect and potential vulnerability gaps introduced by gamers' culture such as account sharing among close friends and family. And how such cultural practices increase information security risk for the gamers and companies.

In future hope of expansion of this study, with ample time to broaden the scope and perform wider subject sampling and analysis, and help answer the research question in depth we propose grouping gamers within the following groupings for better understanding.

Knowledgeable type Those who have information security awareness and respond to threats appropriately.	***Reckless type*** Those who have information security awareness but do not respond to threats appropriately.
Ignorant type Those who do not have information security awareness and do not respond to threats appropriately.	***Cautious-intuitive type*** Those who do not have information security awareness but respond to threats appropriately.

Table 5: Gamers categorisation

4.3 Conclusion

To conclude, this study has many limitations and potential for future research. From the received data, it was deduced that knowledge of information security does correlate to decision-making as well as actions in real life. It was shown that there are two types of knowledge, one is where a person has experienced vulnerability before and has learnt from it. Those with this knowledge showed caution and acted carefully when encountering a similar risk as they had experience or encountered before. This showed how their knowledge influenced their behavior and actions hence showing the correlations clearly. The second one was the knowledge that was learnt and proved that being more knowledgeable increased concerns regarding security which further helped decision-making. Those with this knowledge were more cautious as the previous group. However as there is not enough generalization due to the lack of participants and diverse pool, it cannot be concluded fully on it. Further studies with a more diverse participant pool and more time to prepare for data collection could improve the answer to the research question even further.

References

- Byrne, D. (2022) ‘A worked example of Braun and Clarke’s approach to reflexive thematic analysis’, Qual Quant, 56, pp. 1391–1412.
- Dahabiyeh, L., Najjar, M.S. and Agrawal, D. (2021) ‘When ignorance is bliss: The role of curiosity in online games adoption’, Entertainment Computing, 37, 100398..
- Hamid, H. and Zeki, A.M. (2014) ‘Users' Awareness of and Perception on Information Security Issues: A Case Study of Kulliyyah of ICT Postgraduate Students’, 2014 3rd International Conference on Advanced Computer Science Applications and Technologies, Amman, Jordan, pp. 139-144.
- Kröger, J.L., Raschke, P., Campbell, J.P. and Ullrich, S. (2023) ‘Surveilling the gamers: Privacy impacts of the video game industry’, Entertainment Computing, 44, 100537.
- Lee, N. (2024) ‘Encyclopedia of Computer Graphics and Games’. Springer Nature.
- Szatmáry, K.S. (2024) ‘Cybersecurity of the Gaming Industry’, 2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY), Pula, Croatia, pp. 000441-000446.
- Zhuang, J. (2023) ‘An exploratory study of the information security behavior of gamers. ‘ Master's thesis.
- Zolkiffli, J., Bakar, N.A.A., Ya’acob, S., Salehuddin, H. and Hussien, S.S. (2023) ‘The Assessment of Online Games’ Cyber Security Awareness Level Based on Knowledge, Attitudes, and Behaviour Model’, in Uden, L. and Ting, I.H. (eds) Knowledge Management in Organisations. KMO 2023. Communications in Computer and Information Science, vol 1825. Springer, Cham.
- Sommestad, T., Karlzén, H. and Hallberg, J. (2017) ‘The theory of planned behavior and information security policy compliance’, Journal of Computer Information[1] Systems, 59, pp. 344–353.
- van Steen, T. and Deeleman, J.R.A. (2021) ‘Successful gamification of cybersecurity training’, Cyberpsychology, Behavior, and Social Networking, 24, pp. 593–598.

Appendix A - Glossary of terms

No special (technical) terms need to be explained

Appendix B - Informed Consent Form

Survey on Gamers' Information Security Risks Awareness and their Actual Online Behavior

This survey is conducted to get information on how gamers understand information security risks and their online behaviour. Your participation is voluntary and anonymous. Your answers will be used for research purposes only and will help to understand and improve gamers' online safety.

Please read the consent form below carefully before proceeding.

Consent form:

Topic: Gamers' Information Security Risks Awareness and Their Actual Online Behavior

Introduction:

Contact information: Eimantas Butkus butkus505@gmail.com, Akuen Akoi Deng akuiendng@gmail.com

Organization: Stockholm University

By taking part in this survey, you are agreeing to the following:

- I voluntarily agree to participate in this survey.
- I am over 18 years old.
- I can withdraw my participation from this study at any time.
- The purpose of the study is explained and I understand
- I understand that I can fill out this survey only once
- All responses will be kept confidential and anonymous. No personally identifiable information will be collected. The data will be used for research purposes only.

* Indicates required question

Consent Statement *

I have read and understood the information above. I voluntarily agree to participate in this study. I understand that I can withdraw at any time without consequences.

☐ Yes, I consent

Interview Consent from

Participant Consent Form
Study Title: Gamers' Information Security Risks Awareness and their Actual Online Behavior

"An exploratory study of the relationship between gamers' understanding of information security risks (phishing, account theft etc) and their actual online behavior within gaming communities"

Researchers: Akuen Akoi Deng and Eimantas Butkus
Institution/Affiliation: Stockholm University, department of Computer Science & Engineering (DSV)
Contact Information: akuiendng@gmail.com , butkus505@gmail.com
Introduction

You are invited to participate in a research study exploring how gamers perceive and respond to information security risks, such as phishing and account theft, within online gaming communities. This study aims to understand gamers' security awareness and behaviors to improve online safety measures.
Purpose of the Study

The purpose of this study is to examine the relationship between gamers' understanding of information security risks and their actual online behavior. Data collected will contribute to research on improving information security within gaming communities.
Procedures

If you agree to participate in this study, you will be asked to take part in an interview, which will last approximately [duration, e.g., 30–45 minutes]. The interview will include questions about your gaming habits, awareness of security risks, and personal experiences related to online security. The session may be recorded for accuracy in data collection, but all recordings will remain confidential and secure.
Voluntary Participation

Your participation in this study is completely voluntary. You may choose not to answer any question and may withdraw from the study at any time without any consequences.
Confidentiality

Your responses will be kept confidential. No personally identifiable information will be included in any reports or publications. Data will be stored securely and only accessible to the research team. Interview audio recordings are used and will be deleted after transcription and analysis.
Risks and Benefits

There are minimal risks associated with this study. However, discussing security incidents may cause slight discomfort. You may benefit from increased awareness of online security best practices. Findings from this study may also contribute to better security measures for the gaming community.
Compensation

Participation is free with no compensation.
Questions and Contact Information

If you have any questions about this study, you may contact the researcher via the emails provided above.

Appendix C - Data Collection Protocols Used

Survey questions

1. How old are you?
2. What is your gender?
3. Nationality?
4. What platform do you play video games on?
5. How many hours do you play video games a week?
6. What type of video games do you play?
7. Have you been concerned about information security while playing video games?
8. If yes, what type of concerns have you encountered?
9. How would you rank your awareness of information security
10. Have you experienced phishing while playing video games?
11. If yes, could you describe what happened and what measures did you take?
12. If no, do you know what phishing is?
13. Have you ever reported about online security to the game company?
14. If yes, how was experience in doing so?
15. Do you use any antivirus software on your devices?
16. How often do you update your passwords for gaming accounts?

Appendix D - Parts of the data collected/Details about statistical tests (One of the titles is used depending on whether the study is qualitative/quantitative.)

Interview questions

Section 1: Gamers profile and experience

- Which gaming platform do you often use?
- How often do you interact with other players online? (e.g., via chat, voice, forums, Discord)
- Have you ever made purchases in online games? (e.g., in-game items, skins, subscriptions)

Section 2: Awareness of information security risks

- How familiar are you with online security threats such as phishing, account theft, or scams in gaming?
- If you receive a message, email, or in-game chat urging you to click a link or enter credentials, what would you do?
- If yes, do you report it? - new

Section 3: Personal security practices

- What security measures do you currently take to protect your gaming accounts? (e.g., strong passwords, 2FA, avoiding third-party sites)
- Have you ever shared your gaming account credentials with anyone? If so, why?

Section 4: Experience with security incidents

- Have you ever fallen victim to a phishing scam, account hack, or other security breach in a game? If yes, what happened?
- How did you react after experiencing a security threat? Did you change any behaviors?
- Did you report the incident to the game's support team? Why or why not?

Section 5: Community and social influence

- Have you had any discussions or shared experiences with other players about online security risks?
- How do you perceive the general awareness of cybersecurity among other gamers you interact with?

Present the transcribed text used for the citations that support the derived themes/sub-themes/codes if your study is qualitative.

Presents the details regarding implementing the statistical tests.

Interview 1

(Interviewer) All right we can start interview then my name is a Eimantas we are together with my group member Akuen we're doing a uh interview on gamers information security risks awareness and their actual online behavior so i'll provide some questions for you to answer please answer them as best as you can as clear as possible uh can we start?

(Participant) Yes we can start

(Interviewer) So interview questions for section one it's a gamer's profile and experience, which gave gaming platforms do you often use?

(Participant) Steam and maybe riot games

(Interviewer) Platforms would be like for example pc or console or mobile phone

(Participant) I mean then just a laptop i guess

(Interviewer) All right uh how often do you interact with other players online for example chat voice forums or discord?

(Participant) Let's say like three four times a week

(Interviewer) All right have you ever made purchase in online games for example in game items skins or subscription?

(Participant) Yes, skins, subscriptions.

(Interviewer) We'll continue on to section two which is awareness of information security risks uh how familiar are you with online security threats such as phishing account theft or scams in gaming?

(Participant) I guess it's quite familiar from games like the runescape or on steam as well

(Interviewer) So you have some previous experience with them

(Participant) yes i was scammed when i was little i think

(Interviewer) all right uh if you receive a message email or in-game chat urging you to click a link to enter credentials what would you do

(Participant) i ignore it never click anything

(Interviewer) do you report it at all

(Participant) no

(Interviewer) all right we'll move on to section three which is personal security practices what

security measures do you currently take to protect your gaming accounts that would be strong passwords uh two factor authentications or avoiding third party sites

(Participant) um mostly i think i i use two factor authenticator for most accounts i guess the passwords it's mostly standard yeah

(Interviewer) okay can we want to have you ever shared your gaming account credentials with anyone if so why

(Participant) uh yes with my close friends because i trust them

(Interviewer) all right uh we can move on to section four which is experience with security incidents have you ever fallen victim to phishing scam account hack or other security breach in game if yes what happened

(Participant) um i think if i remember correctly i was scammed by social engineering and uh when i was like eight years old on groundscape they took my gold away

(Interviewer) have you reported

(Participant) no i i was little i didn't know what to do

(Interviewer) all right uh how did oh yeah so it's how did you react after experiencing such a threat did you have change any behaviors

(Participant) uh yeah i think that there was a lesson for my whole life and uh i don't think i've ever fall for something like that ever again that was a good lesson even in let's say a professional environment to not click anything

(Interviewer) yeah it's a similar question about reporting the incident to support team and you mentioned that you were little so you could not do that right

(Participant) yes

(Interviewer) all right section five would be community and social influence uh have you had any discussions or shared experience with other players about online security risks

(Participant) uh no i don't think so

(Interviewer) all right uh how do you perceive the general awareness of cyber security among other gamers you interact with

(Participant) um i'd say it's pretty similar as mine the awareness yeah i don't know what else

(Interviewer) yeah all right thank you very much for your participation uh everything else was informed to you by consent form and thank you for your time

(Participant) thank you

Interview 2

(Interviewer) Hello, my name is Eimantas. I'm doing a research on gamers' information security risk awareness and their actual online behavior. We are doing this together with my colleague Akuen. And today I'm going to ask you some questions. Please answer them as best as you can. And can you confirm if you consented to a consent form?

(Participant) Yes, I do consent.

(Interviewer) Thank you. We can start with the interview. So, section one is gamers profile and experience. So, which gaming platform do you often use?

(Participant) Well, I mostly play games on my personal computer and that's it.

(Interviewer) Alright, moving on. How often do you interact with other players online? So, that would be via chat in-game, voice, forums or Discord for example.

(Participant) Yeah, if I play online games then I interact with my friends via Discord or other call methods and often I chat in-game also.

(Interviewer) Alright, have you ever made purchases in online games for example in-game items, skins or subscriptions?

(Participant) Yes, but very rarely I would say.

(Interviewer) Alright, thank you. We'll move on to section two which is awareness of information security risks. How familiar are you with online security threats such as phishing, account theft or scams in gaming?

(Participant) Well, I have heard about it quite often because in the games I play the gambling community is quite big and the phishing community also the account thefts are quite notorious. So, I have known about it for quite some time now.

(Interviewer) Alright, thank you. If you receive a message, email or in-game chat urging you to click a link or enter credentials what would you do?

(Participant) I would just ignore it.

(Interviewer) Alright, but would you report it?

(Participant) Most of the time no because if I get that message I simply do not click on it or I don't know where is it from and most of the time the platforms on which the online games which I play do not do anything about it.

(Interviewer) Alright, thank you. We'll move on to section three which is personal security practices. What security measures do you currently take to protect your gaming accounts? For example, do you do strong passwords to factor authentications or avoiding third-party sites?

(Participant) Well, I used to factor authentication most of the time and strong passwords also is a must for me.

(Interviewer) Perfect. Have you ever shared your gaming account credentials with anyone? If so, why?

(Participant) I've shared it with my friends because they wanted to play some games and they did not have an account. But those friends I know in real life so I'm not worried about them stealing my account. That's no problem for me I think.

(Interviewer) Perfect. We can move on to section four which is experience with security incidents. Have you ever fallen victim to phishing scam, account hack or other security breach in game? If yes, what happened?

(Participant) No, I have never fallen for those kind of things.

(Interviewer) Alright, so you cannot answer second question which would be about experience regarding it and you cannot also answer third question which is reporting the game's support team because you have never fallen victim to a security incident. Then we'll move on to section five which is the last one. It's community and social influence. Have you had any discussions or shared experiences with other players about online security risks?

(Participant) Well, I've read some information about it and discussed it with other players on some forums. Also watched some videos online about phishing on other scams online and about account thefts. So yeah.

(Interviewer) Alright. And the last question would be how do you perceive the general awareness of cyber security among other gamers you interact with?

(Participant) Well, in the gaming community that I interact with I think the awareness in general is quite good because everyone values their online accounts and everyone tries to keep them to themselves, keep their information to themselves and they don't want their information be stolen. So that's it.

(Interviewer) Perfect. Thank you very much for your answers and have a nice day.

(Participant) Thank you.

Interview 3

Interviewer: [Briefing] Hello, okay, so I hope you've read the interview consent form, and I'm going to record the audio for the interview. Then we're going to transcribe the interview, but we're going to delete the audio after the transcription, and the transcribed data will not have your name or anything; it will completely stay anonymous. Okay, so this is interview number three with Simeon or Simon, as he said.

Okay, so I'm going to start with section one, and since you're more familiar with the questions right now at this point, I'm hoping you're going to answer them with some explanation if possible. If you have something you want to add, you can always add. So the first section is

going to be the gamer's profile and experience, and then the second part is awareness, followed by personal security practices, then experience with security incidents, and finally community and social influence. So we're going to start with section one.

Interviewer: So the first question is, which gaming platform do you often use? This could be a laptop, PC, console, things like that.

Respondent: I use mostly a smartphone and PC. Sometimes other consoles when I bring them to others.

Interviewer: And how often do you interact with other players online via chat, voice chat, or forums like Discord and others?

Respondent: Yeah, I do that.

Interviewer: How often?

Respondent: Every day in some form. I read or write messages in chat and then sometimes use voice chat.

Interviewer: But how often? Like, is it on a daily basis or how?

Respondent: It's on a daily basis via chat.

Interviewer: Okay, and have you ever made purchases in online games?

Respondent: Yeah, I have. Mostly in-game items like skins, in-game currency like Riot Points, and also things like Gold Pass.

Interviewer: Okay, great. Now on to section two, awareness of information security risks. So how familiar are you with online security threats such as phishing, account theft, or scams in gaming?

Respondent: I know that they can happen, that people could steal information, try to steal accounts, and things like that. I know it's very common if you have bad passwords.

Interviewer: In case one of these happens, would you be able to identify, for example, phishing?

Respondent: Yeah, if somebody tried to steal something from me by trying to get information, I would be able to recognize it.

Interviewer: Okay, so if you receive a message, an email, or an in-game chat urging you to click a link or enter credentials, what would you do?

Respondent: Well, I probably wouldn't click the link unless it's on a well-known domain, probably like YouTube or a page where you can see the stats of a player in the game. Then I would consider filling in my credentials.

Interviewer: Okay, if it looks suspicious or fishy, do you report the messages or emails, or do you just ignore them?

Respondent: Yeah, if it had a weird address or an unusual request, like asking for a username and password, I would report it. If it seemed common, maybe not.

Interviewer: Okay, amazing. Now on to section three about personal security practices. What security measures do you currently take to protect your gaming account, like strong passwords, two-factor authentication, or avoiding third-party sites? What measures do you currently take?

Respondent: I currently have a strong password. I use a password manager. The games also have two-factor authentication with email, and I use that as well.

Interviewer: Nice, okay. Have you ever shared your gaming account credentials with anyone? It could be friends or family.

Respondent: Yeah, with my family, I have.

Interviewer: Outside your family?

Respondent: No, I haven't shared my accounts.

Interviewer: Okay, and with your family, why do you share it?

Respondent: It's mostly to let them play on the same account, so they don't have to buy the game or content separately.

Interviewer: Okay, now moving to our next section, which is experience with security incidents. Have you ever fallen victim to a phishing scam, account theft, or any other security breaches in a game?

Respondent: Well, I had one incident. It was a Discord free Nitro scam. I clicked a link that claimed I could get free Nitro, and I entered my Steam account credentials. A couple of minutes after, I realized that even when I entered the correct credentials, it wasn't working. Then they asked me to enter another password, and when none of them worked, I realized my account had been compromised.

Interviewer: Okay, and how did you react after experiencing that incident? Did you change your behavior?

Respondent: Yeah, I changed my password immediately. Now I don’t input my credentials on any link I click, especially on Discord or any place where a private person can send me a link.

Interviewer: And did you report the incident?

Respondent: Yeah, I reported the person who sent me the link. I also Googled and saw that it was a known scam.

Interviewer: That's good. Now for the last section, community and social influence. Have you had any discussions or shared experiences with other players about online security risks?

Respondent: I have had some discussions on Discord. Some were about security risks, like what people should avoid, and others were about scams that people might fall for. I warned some people about those.

Interviewer: And how do you perceive the general awareness of cybersecurity among other gamers you interact with?

Respondent: They're usually quite aware that people can scam or try to dox others. Not all online communications are friendly in games. However, I think younger people tend to be a little less aware or cautious.

Interviewer: Okay, well, that was the final question. Thank you so much for your time. You provided really great insights with your answers. We hope to use this information to do something positive. Really appreciate your time.

Respondent: Thanks, it was nice to be here.

Interviewer: Okay, amazing. Thank you.

Appendix E

Timestamp	Consent Statement I have read and understood the information a	How old are you?	What is your gender?	Nationality?	What platform do you play video games on?	How many hours do you play video games a	What type of video games do you play?
02/03/2025 18:31:48	Yes, I consent	18	Male	Lithuania	Pc	5-10	Shooter
02/03/2025 18:34:34	Yes, I consent	29	Male	Lithuanian	Pc, Mobile phone	20+	Massively multiplayer online role-playing game (MM
02/03/2025 18:40:22	Yes, I consent	23	Male	Turkish	Pc	15-20	Shooter, Adventure, Story, COOP, MOBA
02/03/2025 18:53:19	Yes, I consent	29	Male	Lithuanian	Pc, Console, Mobile phone	0-5	Massively multiplayer online role-playing game (MM
02/03/2025 18:53:59	Yes, I consent	21	Male	Indian	Pc, Mobile phone	0-5	Action, Shooter
02/03/2025 18:58:27	Yes, I consent	19	Male	Latvia	Pc	15-20	Shooter
02/03/2025 18:58:32	Yes, I consent	25	Male	Lithuanian	Pc	10-15	Massively multiplayer online role-playing game (MM
02/03/2025 19:00:11	Yes, I consent	19	Male	Swedish	Pc	15-20	Massively multiplayer online role-playing game (MM
02/03/2025 19:01:39	Yes, I consent	23	Male	Lithuanian	Pc	0-5	Massively multiplayer online role-playing game (MM
02/03/2025 19:03:52	Yes, I consent	19	Male	Sweden	Pc, Console, Mobile phone	5-10	Casual, Action, Shooter
02/03/2025 19:04:59	Yes, I consent	20	Male	Swedish	Pc	5-10	Action, Shooter
02/03/2025 19:05:30	Yes, I consent	19	Male	swedish	Pc	20+	Action, Shooter
02/03/2025 19:07:04	Yes, I consent	19	Male	swedish	Pc	20+	Casual, Action, Shooter
02/03/2025 19:07:30	Yes, I consent	25	Male	Lithuanian	Mobile phone	0-5	Massively multiplayer online role-playing game (MM
02/03/2025 19:14:46	Yes, I consent	25	Male	Lithuanian	Pc, Console	5-10	Massively multiplayer online role-playing game (MM
02/03/2025 19:18:03	Yes, I consent	29	Male	Lithuania	Pc, Console, Mobile phone	15-20	Massively multiplayer online role-playing game (MM
02/03/2025 19:24:52	Yes, I consent	20	Male	Swedish	Pc, Mobile phone	0-5	Casual, Action, Shooter
02/03/2025 19:28:57	Yes, I consent	28	Male	Lithuanian	Console	0-5	Casual, Action
02/03/2025 19:33:07	Yes, I consent	23	Female	Lithuanian	Console	0-5	Casual
02/03/2025 19:36:16	Yes, I consent	25	Prefer not to say	Lithuanian	Laptop	5-10	Massively multiplayer online role-playing game (MM
02/03/2025 19:40:43	Yes, I consent	26	Male	Lithuanian	Pc	10-15	Moba, auto battler
02/03/2025 19:47:41	Yes, I consent	19	Male	Swedish	Pc	0-5	Casual, Action, Shooter
02/03/2025 19:48:37	Yes, I consent	19	Male	Swedish	Pc	0-5	Shooter
02/03/2025 19:49:01	Yes, I consent	18	Male	Swedish	Pc	10-15	Shooter, MOBA
02/03/2025 20:28:15	Yes, I consent	30	Female	Lithuanian	Pc, Mobile phone	10-15	Massively multiplayer online role-playing game (MM
02/03/2025 21:10:30	Yes, I consent	26	Male	South Sudanese-Canadi	Pc, Console	0-5	Massively multiplayer online role-playing game (MM
02/03/2025 22:23:15	Yes, I consent	25	Male	Lithuanian	Pc	0-5	Massively multiplayer online role-playing game (MM
07/03/2025 21:47:24	Yes, I consent	22	Male	Swedish	Pc, Console	10-15	Casual, Shooter
07/03/2025 21:51:01	Yes, I consent	23	Male	Swedish	Pc	5-10	Casual, Action, Shooter
08/03/2025 14:21:19	Yes, I consent	17	Male	Sweden	Pc, Console	5-10	Casual, Shooter
08/03/2025 15:20:36	Yes, I consent	25	Male	Lithuania	Pc	0-5	Action, Shooter

Have you been concerned about information	If yes, what type of concerns have you encou	How would you rank your awareness of infor	Have you experienced phishing while playing	If yes, could you describe what happened anc	If no, do you know what phishing is?	Have you ever reported about online security
No		5	No			No
Yes	Information leak	10	No		Yes i know what it is	No
Yes	Information leak, In-game scamming	5	No		No	Yes
No	Information leak, Phishing	7	Yes	Just change of inner information so it doesnt get	Yes	No
No	Account theft, In-game scamming	5	No			No
Yes	Account theft	7	No		Yes	No
Yes	Account theft, In-game scamming	5	No		Kind of	No
Yes	Information leak, Account theft	7	Yes	I got sent a link to vote for a team, i did not log in	I do know what phishing is	No
No	none	4	No		Yes	No
Yes	Information leak, Account theft, Phishing, In-game	8	Yes	Fake steam websites trying to get you to login to t Just didn't press any links to signed in or anything		No
No		8	No		kinda	No
No		5	No		yes	No
Yes	Information leak, Account theft, Phishing	2	No		yes, people acting like companies to gain	No
No		4	No		No	No
No		4	No		Yes	No
No		5	Yes	Person contacted me. Asked for my log in informa		Yes
Yes	Information leak, Hackers that can see mt ip-adre	9	No		Yes	No
No		5	No		No	No
No		5	No		No	No
Yes	In-game scamming	10	No		no	No
No		2	No		I know what it is, but I didn't know it was	No
No		8	Yes	Someone tried to scam me on skins on a video ga		No
No		8	No		Yes egen a victim acts on a fradulent Emi	No
Yes	Information leak	7	No		Yes, I think so.	No
No		6	No		When a scammer pretends to be someon	No
No		10	No		Yes	No
Yes	Information leak, Account theft	4	No		Gathering information while pretending t	Yes
No		3	No		Phishing is an attempt to steal someone	No
Yes	Information leak	8	No		Yes	No
No		4	No		Yes	No
Yes	Information leak, Account theft, In-game scammir	6	No		Yes	No

If yes, how was experience in doing so?	Do you use any antivirus software on your de	How often do you update your passwords for	Updated password
	Yes	Never	Never
	Yes	not really often, but once in a while a rotate them.	Once in a while
The support from that company helped me ç	No	Never unless forced.	Never
	No	Never	Never
	Yes	Every 1-2 months	Once in a while
	Yes	Not often	Once in a while
	Yes	Once a year	Never
	Yes	Almost never	Never
	Yes	Rarely	Never
	Yes	Once in a while	Once in a while
	Yes	once a year or when i forget	Once in a while
	Yes	rarely	Never
	I don't know	never	Never
	No	Never	Never
	Yes	Never	Never
They told me it was my responsibility to keep	Yes	One time in 10 years	Never
	Yes	Never, more importantly I use 2fa.	Never
	I don't know	Never	Never
	No	I don't do it	Never
	No	when I forget them	Never
	Yes	Never, unless i forget the password lol	Never
	Yes	Never	Never
	No	Never	Never
	No	Never	Never
	Yes	Never, unless I forget what the password was and	Never
	Yes	Barely	Never
	Yes	Almost never	Never
	Yes	Never	Never
	Yes	Never	Never
	Yes	Not often	Never
	Yes	Prefer not to say	Prefer not to say