Security on Video Games

Author: Rebeca Trigo Prado
Tutor: Jordi Duch Gavaldà
Professor: Joan Arnedo Moreno

Video Game Design and Programming
Research and New Technologies

Copyright

FINAL PROJECT SHEET

Title:	*Security on Video Games*
Author's Name:	*Rebeca Trigo Prado*
Associate Teacher's Name :	*Jordi Duch Gavaldà*
PRA's Name:	*Joan Arnedo Moreno*
Due date:	*06/2024*
Degree or program:	*Video Game Design and Programming*
Final Project Field:	*Research and New Technologies*
Language:	*English*
Keywords:	*Security, Bad Actors, Prevention*

Abstract (in English, 250 words or less):

Video Game security affects developers, publishers, and gamers in multiple ways.
To safeguard the gaming experience and the economic success of video games, developers need to create games that are protected from bad actors.
From lack of monetization to lack of engagement, there are many ways that bad actors can affect your game and impede its success.
This investigation recollects risks, prevention methods, and possible solutions.
It also analyses the opinions of both players and developers on the matter, which are actually very similar.
About half of the surveyed players and professionals said they would stop playing a game if there were security issues.
Half of the surveyed professionals have formal education in the field, but most did not learn about cybersecurity in their courses or get training from their companies.

To those who did not believe in me,
as proving you wrong was an inspiration.
I'd like to thank the EAjits (Tomtom, Will, and Misha) and all those who supported me and believed I could do it!

INDEX

Tables and Graphs

Tables Index

Image Index

Graphs Index

Abstract

Video Game security affects developers, publishers, and gamers in multiple ways.
To safeguard the gaming experience and the economic success of video games, developers need to create games that are protected from bad actors.
From lack of monetization to lack of engagement, there are many ways that bad actors can affect your game and impede its success.
This investigation recollects risks, prevention methods, and possible solutions.
It also analyses the opinions of both players and developers on the matter, which are actually very similar.
About half of the surveyed players and professionals said they would stop playing a game if there were security issues.
Half of the surveyed professionals have formal education in the field, but most did not learn about cybersecurity in their courses or get training from their companies.

Keywords

Video Game Security, Bad Actors, Prevention, Attacks, Safety Measures, Anti-cheat, Players, Developers.

1. Introduction

1.1. Introduction

Security is an essential part of any digital product; this investigation focuses on the impact of safety on the Video Game industry.
Developers and publishers must be protected from bad actors to safeguard the gaming experience and video game economic success. Protection starts with awareness of the possible threats that your game will face.

The idea behind this project is to study:

- Aspects that could become a liability.
- Possible threats.
- The motivation behind them.
- Identify prevention systems.
- Lay down the best approaches used for those threats.
- When security measures should be implemented.
- Gather which aspects of security worry most players and developers.

Bad actors can seriously negatively impact a game's success; from lack of monetization to lack of engagement, there are many ways that can affect your game and impede its success.
This report analyzes causes, consequences, and possible solutions. It is accompanied by an investigation of the risks that developers worry about most and an investigation of players' perceptions.

1.2. Description

This project tries to gauge the risks that trouble developers and gamers the most and gather resources and information about video game security centered explicitly around online games.

Most recently released games have an online component, even if they are not entirely based on an online experience.

This topic is paramount as it can make or break a game or cause financial trouble to a whole studio.

Issues like DDoS attacks on Diablo 4 [16] have been making the news and have been reported to increase over the last few years [1].

The obscurity surrounding security measures to increase effectiveness makes it difficult to find literature on this topic. Also, most of the articles written are after security has been compromised in a way that a company is forced to acknowledge it publicly.

Currently, some companies provide their services, helping game teams cover some of their needs with tailored solutions. However, when solutions are implemented after a game is created and already in production, there may be oversights.

This investigation aims to get the most holistic comprehension of the security issues that impact video games.

This project aspires to provide some clarity on the general perception of video game security both at a professional and user level.

As a final product, we will have a report on the main threats, approaches to avoid them, an analysis of solutions that have been implemented before, and best practices and data on the perception players and industry workers have of them.

This project will offer key benefits:

- Make knowledge about how to develop safe games readily available.
- Gauge the primary worries of players and developers about game safety.
- Analyze if there are differences between player's and developer's concerns at a user level.

1.3. General Objectives

Project objectives:

1. Unify information about safety in video games.
2. Collect data about user's and developer's perceptions of security.

Developer objectives:

1. Developers can use the data to prioritize protection methods.

2. Understanding of safety concerns from players (priorities and perception of the issue).

Personal objectives for the author:

1. Acquire knowledge about security technologies for video games.
2. Developer objectives also apply to the author.

1.4. Methodology and work process

The project will use a combined approach, using narrative review (NR) and descriptive research. NR is conducted by describing previously published literature regarding the topic of study, and descriptive research will be performed through sample surveys.

Two sets of close-ended questionnaires were developed for this project, distinguishing worries about security as a player and as a developer, to learn if players who professionally have worked in games, players with development knowledge, and players with no development knowledge.

Questionnaires will be distributed online through forums, social media, and other gaming discussion platforms such as LinkedIn, Reddit, and Discord.

1.5. Planning

PEC 1: Project plan (From 28/02 To 24/03)

16/03: Video Conference about the project with the associate teacher to discuss the idea of the project.

During the first PEC, an idea originated, was discussed, and research was initiated on the topic.

PEC 2: Investigation and first version of questionnaires. (From 25/03 To 21/04)

Where sources are read and put together, questionnaires are crafted, and feedback is received from the teachers.

A scheme with information starts to be developed.

PEC 3: Final version of questionnaires and survey of subjects. (From 22/04 To 19/05)

Meeting with the associate professor to obtain feedback on survey questionnaires and approval.

Once questionnaires are approved and ready, they will be distributed to study subjects.

PEC 4: Memory and Final Project. (From 20/05 To 16/06)

The data collected is analyzed and presented with conclusions.

The final memory is written, and formatting and language are corrected.

PEC 5: Virtual defense (From 17/06 To 08/07)

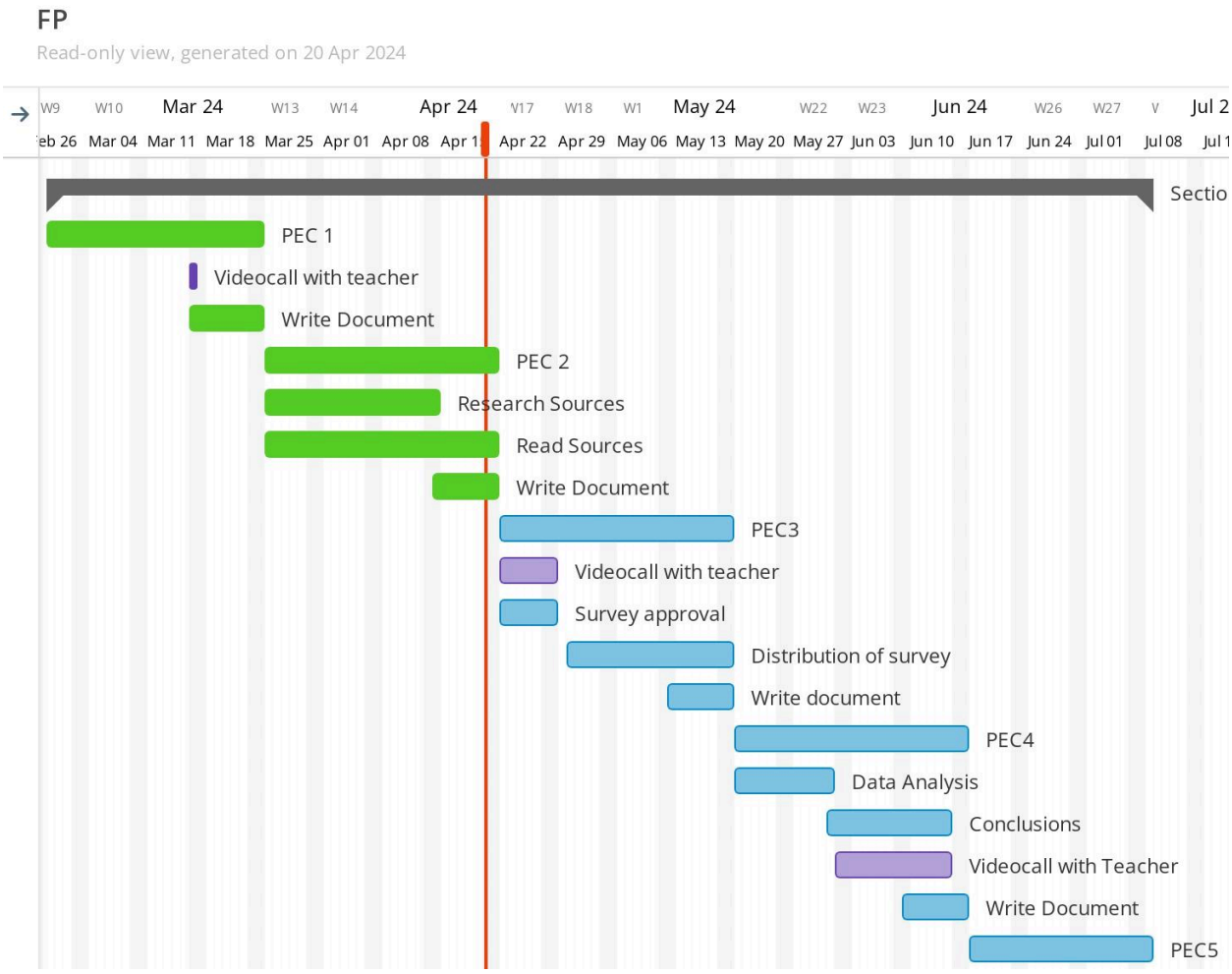


Chart 1: Gantt's Planning Chart

1.6. Budget

Books and other articles used for research were found online and in the Wiley digital library associated with the university, which is available for free.

2. Market Analysis

2.1. Target Audience

This is a project that is directed toward video game developers and publishers. Currently, security issues affect the video game industry and could potentially ruin an otherwise successful title.
There are multiple claims online of a continuous rise in different security attacks and the cost that they have on the industry; however, most of these numbers are unreliable as most of them are released by cybersecurity companies.
Since giving official numbers of how much monetary harm bad actors cause the industry could be perceived as advertising its profitability, companies do not share numbers.

This data can be used by independent developers who don't have the shared knowledge of a big company, the budget to hire external experts or the experience of having encountered some of these issues before.

When we aim this article to developers and publishers, we aim it to both whole organizations and individuals; security is more effective when all levels of development play their part in it. This project is aimed particularly, yet not exclusively, at:
Design: Safety should be by design, considering any threats that the product or a feature can face independently of the development stage of the product.
Engineering: The implementation of protection measures needs the support of the engineering team.
Quality Assurance: From penetration testing to exploits testing, testers, analysts, and the whole quality team should be deeply involved in ensuring the game is safe.
Live Operations: Once the game is live, new challenges will arise regarding how to defend the game from bad actors and how to respond to any threats to the game.
Security team: Experts on the matter can also benefit from updated information and more literature on the subject.

2.2. Precedents

There is a scarcity of formal literature about video game security based on obscurity. This seems to be based on the belief that providing information about how to keep games safe will also make the bad actors know how to skip the measures or convert players into bad actors. Articles about highly visible attacks, leaks, or failures are readily available, but that is just a small percentage compared with the reality of security. After all, companies would not like to encourage bad actors by giving them credit.

There is also the issue that video games are an industry that evolves fast, and articles and research need to be updated quickly to stay relevant.

Regardless of the small amount of literature on how to defend games, there is a lot of information readily available on how to penetrate security at different levels.
A big source of information about security is unofficially written by those who try to circumvent it, and even though it is not academic and can't be cited, it is not possible to dismiss its importance for security teams.

There is a great book[1] that is very relevant to the topic. Although it is from 2009 and partially dated, it studies deeply different security threats that affect developers and publishers and countermeasures.
In contrast, there is a lot of useful and readily available information on how to skip security for anyone interested (though it is not being published as papers or by reputable sources).

There are studies and books that focus on aspects related to bad actors, like cheaters' relationship with video games [30] or psychological studies about cheaters' motivations, but we are not going to go in-depth more than knowing what they seek in order to stop them.

The most significant gap in information is academic research regarding player worries about video game safety. We are asking some of the questions we could not find many reputable sources answered.

3. Proposal

3.1. Objectives

To provide up-to-date information that can help educate developers about security, study their perception about the current issues that the industry faces about security, and recollect data from a player's perspective.

The information about game security is going to be focused on perpetrators, threats, and solutions.

Developers' perceptions will be measured through the surveys, and it is expected to shed light on what threats they tend to prioritize to see if their worries align with specific threats in general or by the development department.

Player perception will also be measured through surveys, and we want to know if they will align with developers' priorities, what developers usually prioritize in general, and which threat types can or have made players stop playing.

3.2. Execution

Recollecting information from credible sources, examining and studying it, and then relying on it in an easy way to be understood.

The survey will be anonymous, online, and passed through Google Forms. Before they are passed on to other subjects, the professors will review them.

Surveys will be written in English. The questionnaire will have multiple-choice questions. There will be at least one open-ended question at the end of the survey.

The analysis will be presented as a summary; however, depending on the results, visual aids will be provided in the form of charts.

3.3. General structure of the project

Firstly, the project will present information gathered from other publications aimed to provide general knowledge on the matter, divided into the perpetrator types, threat types, prevention, and solutions.

Then, the results and analysis of two survey sets were passed around, one on platforms aimed at players and the other at video game professionals.

Lastly, the project will have conclusions based on the results of the surveys completed by players and industry professionals.

4. Threats

This information is categorized by the order that was considered most easy to digest and understand. However, for an updated listing of cheating methods and cheating prevention, Haapaniemi's *Bachelor's thesis Cheat Detection & Prevention Methods in video games* [19] offers an updated listing of cheating methods and cheating preventions recollected from other publications and contains summarised and comparative tables of them.

4.1. Perpetrator types

Internal: Workers of the game may be the ones creating a security threat. This can be with or without malicious intent. Sometimes, due to human error, lack of knowledge, or awareness, the ones that generate risk in the game are their developers. Sometimes, a worker is a bad actor who tries to gain money, boycott a project, or obtain an unfair advantage for themselves or others.

External: These are people unrelated to the game, and there are subdivisions, even though bad actors are often under more than one category.

Hackers: These bad actors use tools and knowledge for different purposes such as financial gain, cheating, testing their abilities, revenge, or as a power demonstration.

Cheaters: These bad actors want to gain an unfair advantage in the game.

Exploiters: These are actors who use an issue on the system to obtain a benefit; sometimes, exploiters are unaware that what they are doing is wrong because of a lack of clarity or how extended the use of the exploit is or rules are not clear. However, for this text, we will associate them and treat them as cheaters.

Fraudsters: They often communicate with players through forums, in-game chat, other messaging apps, etc. To sell players currency from the game, steal accounts or personal information.

Stalkers, pedophiles, terrorists, and other bad actors may use our game to perpetrate an illegal activity as one platform that is easy to use. This is often the case with online games that have live chat.

4.2. Threat Types Definition

We classify threats by type; however, one issue can be caused by a combination of threats. This classification is only meant to make the matter more easy to understand, study, and approach.

4.2.1. ***Intellectual property theft:*** Anything in a video game can be stolen or copied. Often, some bad actors target art, music, game mechanics, source code, and anything else in the game. The uses they make of it are wide, from knock-off imitations to counterfeit merchandise.

- **Piracy:** Interpol defines it as *the illegal copying or distribution of copyrighted material via the Internet. It negatively affects the creative industries, including film, TV, publishing, music, and gaming* [13].

  Piracy used to be limited to copies of the games being illicitly distributed, but since online games, the rise of pirate servers has also become an issue.

  We can distinguish the following forms of piracy:

  - *Hardware:* Originally, games were distributed through physical support. That was cassettes, CDs, DVDs, cartridges, etc. Bad actors learned how to circumvent these distribution systems to obtain copies of games without purchasing them from the publisher.
  - *Server:* When the first online games became popular, bad actors adapted and learned how to copy servers where they host games without paying a subscription fee.
  - *Emulators:* Since sometimes copying certain hardware is expensive, some bad actors obtain the main code of a game and use it in other systems (most commonly a PC).

- **Modding:** This is an unofficial modification of the source code; even though illicit, a lot of times, it is not prosecuted, and developers and publishers allow it when this modification is not made with the intent of obtaining revenue.

  It is a difficult thing to prevent, and sometimes, the only action that can be taken is to request the elimination of content from platforms. However, it becomes a game of whack-a-mole as more content can be created.

  Some risks of this practice are bad actors posting videos of modded content and advertising it as authentic when that modded content can damage a game's image or bad actors selling modded content, which would fall into IP theft.

Some games even support it, making competitions and then using the content generated by players as part of the game. Instead of an "if you can defeat them, join them!" it becomes an "if you can't avoid it, obtain revenue from it."

A game known to allow this is *Human: Fall Flat.* They do not only allow but encourage it, and instead of fighting it, they have welcomed it through competitions of fan-made levels posted on their Steam Workshop that have become officially released to players. They also offer support for fans who want to make their levels, with tutorials on how to do it and a Discord channel dedicated especially to helping people create levels. [41]

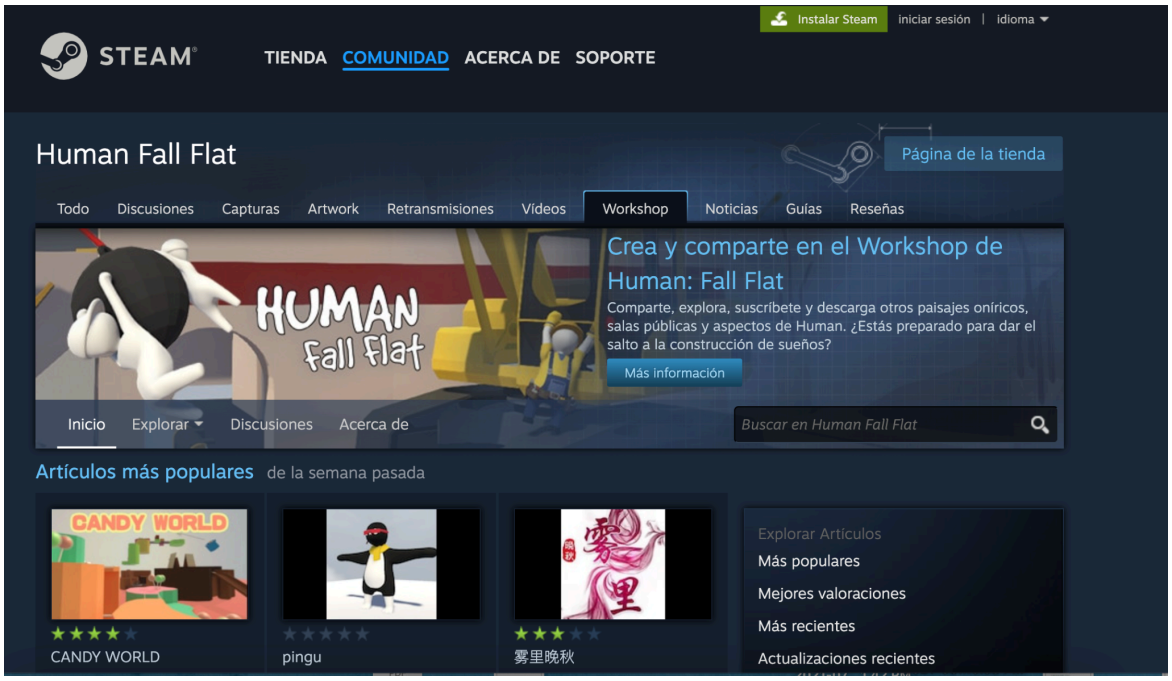


Image 1: Human Fall Flat's Workshop (Steam, 2024)

Threat type	Subtype	Variations	Example/Summary
IP Theft	**Piracy**	*Hardware*	Copying blue rays
		Server	Copying servers
		Emulators	Use source code in a different system.
	Modding	–	Unofficial modification of the source code

Table 1: IP Theft schema

4.2.2. ***Unfair advantage:*** There are unique ways that a bad actor or a group of them can find themselves depending on the game. Usually, these methods are shared online unless the game is competitive, and then bad actors may keep them secret to maintain their advantage over the opponents.

- **Cheating:** when a player does not follow the rules established in the game to win. There are many ways of cheating, but some of the most common ones are:
    - *Collusion:* when more than one player works together towards a result in a game. This is common in ranked or competitive games to allow an account to win. Win trading is a big issue in games that have rewards at the end of a determined period. When matchmaking is not randomized or can be manipulated, especially when the games consist of only two players, an example of a game that could be affected is competitive games.

    - *Account Sharing:* To get more experience points or rank up higher, sometimes multiple people would take over an account. Sometimes, players do it with no cheating intention but with the intention of saving money on the purchase of an extra license or account.

    - *Account Theft/Hijacking:* Sometimes bad actors steal someone's accounts through social engineering. They can do it in order to obtain objects or merits in a faster or easier way than to work their way to reach the results using other honest or dishonest methods or to extort some money from players who already have invested many hours into the game and are so committed that would be willing to pay to regain control over their accounts. Many examples of this can be found on forums narrated by the victims; for example, some Dota 2 players got their accounts stolen whilst they were playing [28].

    - *Botting or automated play:* A hacker can create a bot or automate an action that will grant them an advantage. For example, in some games, there is grinding and making a tool that is capable of collecting the items the player needs without the player needing to physically do the action that is required to achieve the resources. This type of cheating can use machine learning or AI.

- *Hardware hacks:* This is something that has evolved and only affects a few of the current games as we have moved into online gameplay. Through them, bad actors could unlock advantages in single-player games, and they were also a part of piracy. Examples of this have moved from the infamous R4 card for Nintendo DS to the EPO AIM, which is apparently not detected by anti-cheat systems [38].

- *Memory editors:* People will identify which part of the code pertains to whatever they want to modify, and then they will change it, granting themselves currency, objects, experience, or anything else that is stored in the client. It can also be used to get information that will grant the user some advantage.

- *Fake videos:* Sometimes, people do not cheat on the video game; they just cheat on their online viewers. They do this through video editing content they later post or reproduce online. It is a common practice for people who want to gain viewers but are not indeed as skilled as they want to portray themselves. Sometimes, they also fake cheats, damaging a video game's reputation.

- **Exploiting:** deficiencies in design or implementation are not detected by the development team. However, there are numerous players, and they will eventually find any error. When an error is profitable to players, they will adopt it as a strategy or abuse it to gain an advantage. Some people do not consider this cheating as the vulnerability is inside the game, and the rules for what is considered cheating are blurry. Here are some common ways a player can exploit a game through:
  - *Cheat codes:* combinations that make something happen, used to facilitate testing. Cheat codes left behind were the most common exploits. This became part of the gaming culture, where you could purchase guides with cheats and exploits. Nowadays, this tradition has been continued online and at no cost to the user through online publications. A well-known cheat code exploit is how to get more currency in *The Sims* franchise; this game has sustained the cheat codes as an essential part of the game, as stated on their web [42].

  - *Duplication:* Sometimes, through a disconnection, players can duplicate an item or currency (even though they risk losing the original item completely

sometimes). An example of this was how players would disconnect the game link cable on the *Gameboy* when exchanging *Pokemon* so it would duplicate them. In online games, this can seriously affect the economy.

- *Geometry:* Players may find ways to access areas they should not, creating shortcuts, finding safe zones where the player can shoot and not be shot, or other advantages.

- *Twinking/Smurfing:* Low-level players may get high-level equipment gifted to them, or highly skilled players will create a newer low-level account that enables them to compete against new players who often also carry high-level equipment. This can cause a game imbalance and a very negative player experience for new players. This is a common practice in some MMORPGs.

- *Connectivity:* Players can sometimes disconnect themselves from the game to avoid storing a negative score on the server. Disconnection can also be used for duplication. Lag can grant extra time to react in some games. Also, it is possible to DDoS an opponent.
  I.E., League of Legends has had some attacks during tournaments, and it is causing a lack of trust among the eSports fans [24]; this has been so much of a worry that there is an article on Riot's page about it [33].

- *Movement speed bugs/Straffing:* In some games, a player can increase the speed of running or jumping depending on the direction they are running or jumping to. Quake is known to have accepted what initially was considered a bug as a feature with the strafe-jumping.

Threat type	Subtype	Variations	Example/Summary
Unfair advantage	**Cheating**	*Collusion*	More than one player fixing a result
		Account Sharing	Multiple people take over an account.
		Account Theft/Hijacking	Bad actors steal players' accounts.
		Botting or automated play	Create a bot or automate an action that will grant them an advantage.
		Hardware hacks	Modifying hardware to make it work different
		Memory editors	Get information or grant something.
		Fake videos	Video edited content
	Exploiting	*Cheat codes*	A combination to facilitate testing that makes something happen.
		Duplication	Through a disconnection, players can duplicate an item or currency.
		Geometry	To find ways to access inaccessible areas
		Twinking/ Smurfing	Low-level characters using high-level equipment.
		Connectivity	Manipulate internet connection to get advantages.
		Movement speed bugs/Straffing	Increase the speed of running or jumping depending on the direction

Table 2: Unfair Advantage Schema

4.2.3. ***Fraud*****:** an attack where the players or studio could be the victim. There is fraud where a bad actor steals from users, but sometimes fraud is committed against the video game distributor.

4.2.4. ***Distributed Denial of Service (DDoS)*****:** is the flow interruption on a server through excess of activity. These attacks can be against the server or a player. Sometimes hackers want to hurt a game service and it attacks their servers, costing those games an important sum of money. However, the attacks can also be a form of cheating, and the target is a single player who plays competitively to force a forfeit or a loss (see connectivity exploit). [29]

4.2.5. ***Ransomware*****:** a series of attacks that try to extort individuals or companies, holding hostage their accounts or the whole game. During an attack, the malicious attacker in

Insomniac Games was a victim of an attack that leaked an upcoming game and a lot of employee information [17] [35].

4.2.6. ***Terrorism*:** Video games are currently being used as a recruiting tool by some extremely violent groups. The legal and moral repercussions of a game becoming a recruitment point for this purpose are deeply troubling. This is something that is not usually admitted by video game companies in public articles for two main reasons: firstly, it will create a bad image of the video game and tarnish the reputation of the players, developers, publishers, and the whole video game industry; secondly, it can act as a call to action for other terrorists to join in. There is an apology letter published by Discord as an extremist person detailing his intentions on his private server before an attack in May of 2022 in Buffalo, US [32].

4.2.7. ***Other attacks*:** This encompasses stalkers, pedophiles, bullies, and a whole lot of undesirable users of our services. This issue can carry a lot of damage to not only a game but a whole studio or publisher and have legal consequences, apart from making our game a dangerous place instead of a place of enjoyment. It is a known fact that sexual predators may use online chats in video games to try and find possible victims [6]; there is also a lot of documented harassment in online games

Threat type	Subtype	Variations	Example/Summary
IP theft	**Piracy**	*Hardware*	Copying blue rays
		Server	Copying servers
		Emulators	Use source code in a different system
	Modding	-	Unofficial modification of the source code
Unfair advantage	**Cheating**	*Collusion*	More than one player fixing a result
		Account Sharing	Multiple people take over an account
		Account Theft/Hijacking	Bad actors steal player's accounts
		Botting or automated play	create a bot or automate an action that will grant them an advantage
		Hardware hacks	Modifying hardware to make it work different
		Memory editors	get information or grant something
		Fake videos	video editing content

	Exploiting	*Cheat codes*	A combination to facilitate testing that makes something happen
		Duplication	Through a disconnection, players can duplicate an item or currency
		Geometry	To find ways to access inaccessible areas
		Twinking/ Smurfing	Low-level characters using high-level equipment.
		Connectivity	Manipulate connection to get advantages.
		Movement speed bugs/Straffing	increase the speed of running or jumping depending on the direction
Fraud	-	-	Towards players or distributor
DDoS	-	-	Flow interruption on a server
Ransomware	-	-	Attacks that try to extort individuals or companies
Terrorism	-	-	Use of games by some extremely violent groups
Other attacks	-	-	Stalkers, pedophiles, bullies

Table 3: Complete Threats Schema

5. Prevention and Solutions

In this section, the aim is to expose a series of solutions or approaches to security that developers and publishers use to avoid the consequences that attacks can carry.
Prevention is costly. However, the ability to foresee issues before they occur can be invaluable.
The price of prevention may not be worth it for the possible actual economic impact on a game.
Detection is never infallible; therefore, it is preferable to error in favor of the player than against it and monitor suspicious activity before taking an unfair action.
Sometimes, letting the breaches go unpunished can offer a layer of protection for security detection as bad actors may have more difficulty distinguishing between what makes them get punished.

5.1. Prevention methods:

Ideally, with good prevention, we would not need to have solutions for when a security issue occurs. However, it is not always possible to prevent or anticipate attacks, as many risks factor into this.

- **Vulnerability management:** It is a constant cycle where developers can identify, prioritize, mitigate, or resolve vulnerabilities in the system that bad actors may take advantage of. This is a security strategy as much as a prevention method in itself and would need to be combined with other methods.

- **Server authentication:** It is more difficult to modify information through a protected server than through the client; however, verifying all information a server receives could severely impact the speed of the game, and it can be very expensive to maintain. Thus, it is fundamental to choose which information must be verified on the server.

- **Kernel security:** These are measurements that require access to the core level of the Operating System of the console or computer used to play. These are controversial measures, as giving access to a third-party program to such sensitive parts can actually compromise the user's equipment. There are precedents of vulnerabilities and attacks

on users. This is a win/lose situation where developers get a better sense of security, and players lose control of their own devices.
As a bad actor used Genshin Impact Anti-cheat to turn off antivirus [39], these worries are being validated.

- **Encryption:** Changing data into a more complex code makes it a bit more difficult to steal, change, or compromise. This method is very weak by itself; however, combined with other methods, it may help deter the least determined bad actors.

- **Security communications:** to send players information about rule changes, frauds, or any other safety-related information from inside the game. Usually, the same system delivers other information to players.

- **Player education:** To avoid players giving their account information online, we need to educate them on what information they can't share with anyone online. Teach them the practices to avoid putting their game accounts or their personal data at risk.

- **Good password practices:** enforcing strong passwords, using password managers, and expiration passwords from both players and everyone inside the organization can protect both players' accounts, player information, servers, intellectual property, and other issues.

- **Authentication measures:** Services like multi-factor authentication can be used to avoid account theft or hijacking. This is true for players as much as for developers. This also helps protect against ransomware, IP theft, and leaks. This should be accompanied by the good password practices mentioned above.

- **Obscurity:** In itself, hiding information from bad actors is not effective; there is, of course, some obscurity to be always observed. A mantra in cybersecurity is "Obscurity is not security," and even though it is true, making it easy for attackers to understand our systems is just going to leave our systems more vulnerable.

- **Terms of Service:** Even though this is not something a developer usually thinks of as a prevention method, it covers what is allowed and is not in our game. This also protects

the videogame from legal repercussions in case of misuse of the service by bad actors, avoiding possible legal consequences.

- **Limitations of use:** Some video games have some limitations depending on the subscription method or the age of the user. In some video games, players younger than a determined age do not have access to chat (to avoid practices like grooming), or they do not get ads on their games (this limits the possible influence that ads can have on a minor but also they can't get access to rewards that are linked to viewing ads) between many other measures.

- **Data investigation:** This should accompany any automatic detection; before taking action against a player, there should be an investigation that validates whether the detected infraction is a real one or if the automatic detection system has any validity or may be a false positive.

- **Third-party payment methods:** The use of platforms such as Google Play Store, Steam, Apple Pay, PlayStation Store, or others to process in-game payments has a cost. However, it reduces the cost of investigating chargebacks, fraud, and verifying cards. This does not eliminate the need for it, and some bigger companies have their purchase platforms like the EA app [14]. However, this is a solution for smaller companies or studios. This won't eliminate the need to investigate payment issues, but it will alleviate some of the work weight.

- **Legal assessment:** In order to implement any prevention or solution plan, in-game promotion, or contest, have some lawyers proofread and verify that the actions comply with the laws of the countries in which the game is operating and can protect the game from fraudsters or from being sued for profit.

- **Malware protection:** To protect from malicious software, this is a basic of security on any digital product; if hiring professional companies to supply this service, it is often recommended to combine multiple providers; in case one provider has a vulnerability, it is most probable that a second layer of security by another provider won't have the same crack.

- **Commercial anti-cheat systems:** Sometimes, a studio or company will have their own systems developed and adapted to different games; however, smaller studios can't afford to develop a whole system and decide to lease or purchase the license of a system developed by a third party.
  This is something that needs to be analyzed in a case-by-case scenario, and each game team needs to evaluate how to proceed depending on the resources they have available.

- **Knowledge sharing:** Knowing about exploits and cheats can help a development team decide if they would like to avoid them or accept them as part of the game. Sometimes, the knowledge of security issues in a particular genre of games is just a Google search away. Sometimes, in bigger companies, documentation and post-mortems are shared internally to help avoid specific issues, and sometimes, in professional conferences, there are sessions about security that can benefit smaller teams greatly.

- **Penetration testing/security testing:** an attack or series of attacks that are prepared internally to find weaknesses and possible security issues. The better prepared and equipped the security testers are, the better. However, there is a limit on the scenarios and areas to test.

- **Content Delivery Networks (CDN):** This is the distribution of servers, so it is more difficult for bad actors to make a global DDoS attack. Also, critical information can be spliced, spread and encrypted to make more difficult access to it, however this also will affect other users access to it, delaying response time. Nintendo shares which third party providers they use on their web [43].

- **Honeypot traps:** To set up traps that would entice attackers to engage in foul behaviors in order to catch them. This could work for a variety of issues, such as preventing leaks or investigating breaches.

Prevention	Example/Summary
Vulnerability management	Constant cycle where developers can identify, prioritize, mitigate, or resolve vulnerabilities. Security strategy.
Server authentication	To avoid information modification.
Kernel security	Installed on the core level of the Operating System of the equipment
Encryption	Changing data into a more complex code
Security comms	To send players information about rule changes, frauds, or any other safety-related information from inside the game
Player education	Teach them the practices to avoid putting their game accounts or their personal data at risk
Good password practices	Enforcing strong passwords, using password managers, and expiration passwords
Authentication	Services like multi-factor authentication
Obscurity	Hiding information from bad actors
Terms of Service	Protects the videogame from legal repercussions in case of misuse
Limitations of use	Limitations based on the subscription method or the age of the user
Data investigation	An investigation that validates whether the detected infraction is real
Third-party payment methods	Google Play Store, Steam, Apple Pay, PlayStation Store
Legal assessment	Verify that the actions comply with the laws where the game operates
Malware protection	To protect from malicious software, this is a basic of security on any digital product
Commercial anti-cheat	The license of a system developed by a third-party
Knowledge sharing	Knowing about exploits and cheats can help a development team decide if they would like to avoid them or accept them
Penetration/security testing	An attack or series of attacks that are prepared internally to find weaknesses and possible security issues
Content Delivery Networks (CDN)	Distribution of servers so it is more difficult for bad actors to make a global DDoS attack
Honeypot traps	Setting up traps to catch bad actors

Table 4: Prevention schema

5.2. Solutions

When everything else fails, these are some possible methods to minimize the impact of some of the security breaches.

- **Account Recovery:** This is a complicated process because personal information from the player is needed to verify an account. However, if we already minimized the amount of information collected and stored and the amount of people who treat the data, an account recovery system should be put in place. If a person has been heavily hacked or their identity stolen, there is the risk that a hacker will steal the account.

- **Patching:** This is a common practice in any online video game; once an exploit is discovered and abused, the development team should work on a fix for the issue; this is usually implemented through an update.

- **Clarifying or adding rules:** Sometimes correcting or specifying what is and is not considered cheating is needed. It is better if the rules are specified from the launch of the game or game mode; however, clarifying rules when there is possible misunderstanding or exploitation is necessary at a later stage.
  For example, Fortnite had to clarify its collusion rules two and a half years after launch because signaling between players was commonplace[36].

- **Rollback:** a solution for when a player has been granted or acquired currency, rank, or items that players may have acquired unfairly, through a bug or exploit, or by any error on the system. Setting the account back into an earlier stage. It also works when players get scammed and lose progress.

- **Banning:** This is a practice of removing access for someone temporarily or definitely to access an online video game server. It can also affect accounts, IP addresses, or devices. The most common type of banning affects accounts only, as there may be legal actions when banning devices or IP addresses. When implementing a ban system, you must be able to implement a way to reverse that ban.
  - *Temporary bans:* The player is denied acces temporarily. There is the possibility of some players redeeming themselves and not losing a possible source of

revenue in a videogame, and applying temporary bans allows for the correcting of some bad actors and the transformation of them into regular players.

- *Permanent bans:* Player is denied acces permanently. There are cases where the infractions cannot be overlooked, or the bad actor is not considered redeemable. Sometimes, the best thing to do is to remove the person from the server.

- *Combined strategy:* with a limit of temporary bans that increase in length and end up in a permanent ban in case bad actors do not redeem themselves. Valorant from Riot Games has published an article about how they ban players who display any "unsportsmanlike conduct" [44] that can serve as an example. Other games prefer not to share how they determine bans, sometimes not even banning all confirmed bad actors to add a layer of obscurity to their detection system.

- **Cheater Island:** this is a measurement taken against cheaters that consists on making them to compete against each other. A lot of times they get derived to a different server.
  Cheater Island has risks:
  - Bad actors can improve on their cheating techniques and come back with a legitimate account; they will be sent to Cheater Island if etected,until they discover their existence.
  - Cheaters can refine their cheating until they do not get into Cheater Island once they discover they have been sent to one.
  - Cheaters can use Cheater Island as a learning sandbox of cheats and tricks against other cheaters.

  The above-mentioned risks of Cheater Island are why many games choose not to have one. However, it has also some positives:
  - Avoids the backlash of banning players with false positives for cheating.
  - Learning from cheaters through analyzing the cheating methods.
  - Some cheaters actually purchase items even though Cheater Island is often not considered profitable per se.
  - It costs less than banning, and even though it should require a previous investigation, there is less volume of support contacts.

- **Anti-terrorism advisors:** On top of educating the players, having reporting tools where players can report any suspicious activity and monitoring tools. Some organizations try to combat terrorism in video games, like the EGRN, which defines itself on its website: "The EGRN leads evidence-based research at the nexus between gaming and extremism while providing effective solutions for various public and private stakeholders. Our members work to evidence the ways in which gaming is used by malign actors for harm, as well as the opportunities to use gaming for good to counter harm. Core to this is our collaborative work with gaming platforms to create resilience-building solutions for gamers."[15]

- **Managed Detection & Response**
    - *Automatic detection:* By using a flagging system with parameters that are considered normal within a game, there is the possibility of finding possible cheaters or exploiters. Of course, any positives should be double-checked by a security analyst before taking action, just to avoid taking action against legitimate players through false positives. Also, in order to avoid false positives, a process for updating parameters and updating the system should be put in place. For example, Electronic Arts has created a patent for collusion detection [40].

    - *Player reports:* Through different methods, players can submit reports with what they believe proves that they found bad actors in the game. However, this can produce a lot of false reports and create a bottleneck of reports that will need to be investigated. Players will often think that someone has cheated when they get bested in competition games. It is a handy tool. However, a process to handle this should be put in place before implementing any such measure. Sometimes, there is the possibility of creating in-game reports.
      This is a tool that could also be used to report bullying or any other threats like the ones mentioned in 5.2.7.
      An example of the use is Fortnite from Epic Games [21].

    - *Client-side detection:* a method to avoid overloading servers by verifying all the data received by clients; storing data parameters in more than one part of the client and comparing them before sending the info to the server can help avoid

slowing down the game. This can still be circumvented by more advanced cheaters. However, it can flag a large amount of less careful ones.

- *Data investigation:* the ability to verify events, currency, items, movements, etc. It can help uncover foul play from bad actors; this data can be pulled by security analysts and studied carefully before sanctioning a player who is suspected of not following the rules.
  Sanctioning legitimate players will create distrust among the players in the game.

Solution	Subtype	Example/Summary
Account Recovery	-	To recover an account that may have been lost, erased, or stolen.
Patching	-	The development team should work on fixing exploits.
Clarifying or adding rules	-	Correcting or specifying what is and is not considered cheating
Rollback	-	Setting the account back into an earlier stage
Banning	*Temporary Bans*	The player is denied access temporarily
	Permanent Bans	The player is denied access permanently
	Combined Strategy	With a limit of temporary bans that increase in length and end up in a permanent ban in case bad actors do not redeem themselves
Cheater Island	-	Placing cheaters in a different server or competition to play against each other
Anti-terrorism advisors	-	Some organizations try to combat terrorism in video games
Managed Detection & Response	*Automatic detection*	A flagging system with parameters that are considered normal within a game
	Player reports	Players can submit reports with what they believe proves that they found bad actors in the game
	Client-side detection	Storing data parameters in more than one part of the client and comparing it
	Data investigation	The ability to verify events, currency, items, movements, etc.

Table 5: Solutions Schema

5.3. Considerations

The more successful a game is, the more attacks it will suffer (the IP is more interesting to steal, getting to a high level appeals more for cheaters, and the fraudsters have a bigger pool of targets..).
So, if your game or company is targeted, it means it has gained some relevance, the bigger the relevance the bigger of a target you are.

Security is costly, especially in any online game, as the game operates as a service. Security becomes one of the basic features of that service.
It is impossible to make a game that is impenetrable. Said that there are parts of security that you have to get as close as possible to it.
Personal data must be protected according to the legislation of the countries in which your game operates, which are usually European laws that are the harshest.

For almost every type of security, a multiple approach is required.

The most common types of bad actors are the less specialized; as the level of knowledge and dedication required increases, the number of threats decreases. As explained above, popular games are more threatened, and the reputation of a game may influence the amount and types of attacks.
Trying to remove bad actors often becomes similar to a game of whack-a-mole, where offenders are punished, and they re-offend and reappear.
One of the most important methods to avoid this feeling is through rule enforcement from the beginning. A reputation that harassment and bullying lead to a quick ban alone may deter some.

Depending on what motivates a cheater, the deterrent facts will change, for example if the incentive is just obtaining results, high difficulty may dissuade some bad actors but if they are doing it in order to gloat online, it won't.

6. Analysis of Survey Results

6.1. Survey Considerations

Before the reader inspects the data, it is important to explain that some questions were answered on a scale from 1 to 5. Being 1 "None" or "Not at all" and 5 "Complete" or "Absolutely".

What is understood as a professional is someone who is a student, graduate, or worker in the industry.

Four developers, one blogger, and one student participated in the player survey.

In the professional survey, even though eight people identified themselves as players by the rest of the answers, one or maybe two have no further relation with gaming.

Currently, the player survey shows 102 responses. However, the survey numbers 49 and 64 are empty. Therefore, only 100 eligible responses were recorded.

The professional survey shows 55 responses; however, surveys 16,24,32 and 35 are empty. Therefore, only 51 eligible responses were recorded.

6.2. Survey Structure

Surveys had some segmentation questions (Sex, Age group, Relationship with video games) to know a little of the profile of the people answering them.

Then, in the case of professionals, we enquired about their knowledge and experience with security.

Also, asked players and video game professionals' opinions on security matters.

6.3. Survey distribution

The surveys were created on Google Forms, without any personal data being collected, not even emails.

They have been distributed through the following methods:

- Social media (Facebook and LinkedIn).
- Messaging apps (Telegram, Discord, and WhatsApp).

6.4. Player Demographics

The distribution regarding the sex of players who answered is close to the natural distribution of the population. A majority of them identify as men, closely followed by women.

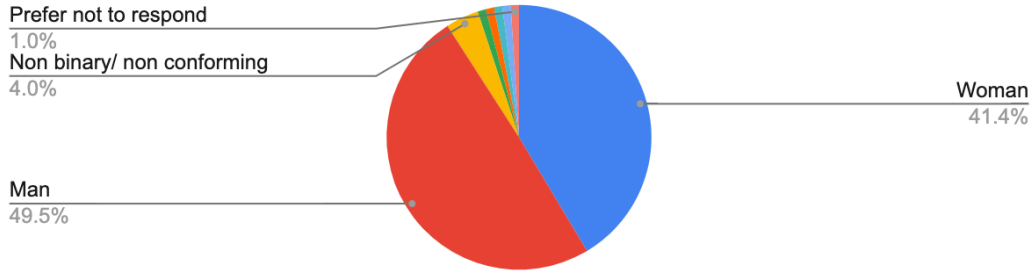


Chart 2: Players sex distribution chart

The age of the players who answered the survey is primarily under thirty-five.

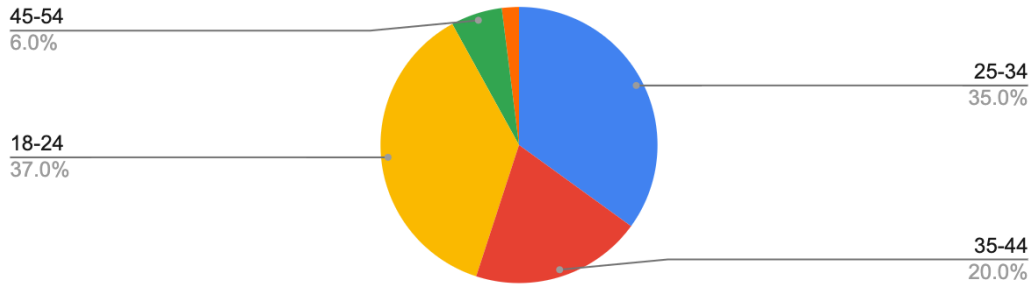


Chart 3: Players age group distribution chart

6.5. Professional Demographics

The representation of sex in the professional survey is male-dominated.

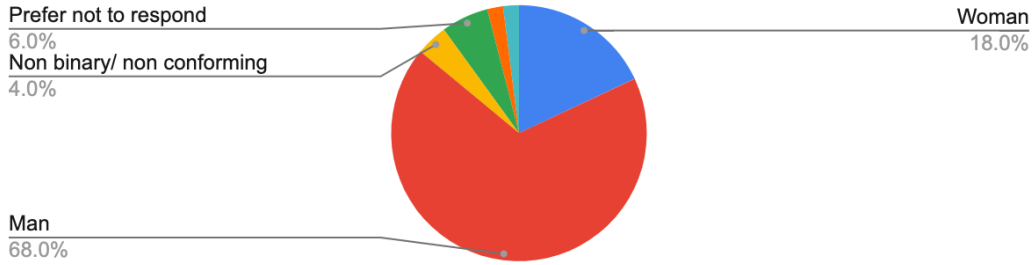


Chart 4: Professionals sex distribution chart

The age of the professionals who answered is between 25 to 44 years old.

There is a mix of types of games, developed experience, and position types.

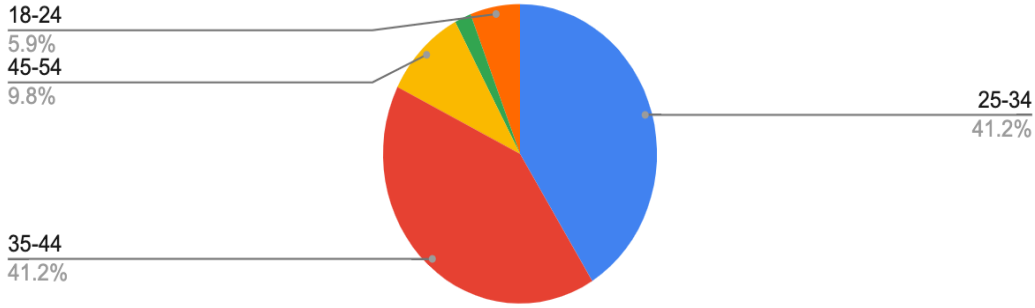


Chart 5: Professionals sex distribution chart

6.6. Common Questions Overview

Over 77% of surveyed players say that they encountered security issues in video games, whereas only 55% of surveyed video game workers have encountered issues in their games. Cheating is the most commonly reported security issue in both cases.

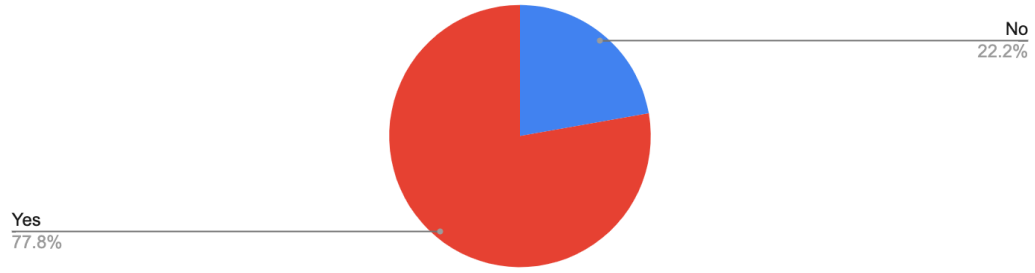


Chart 6: Players perspective on experience security breaches

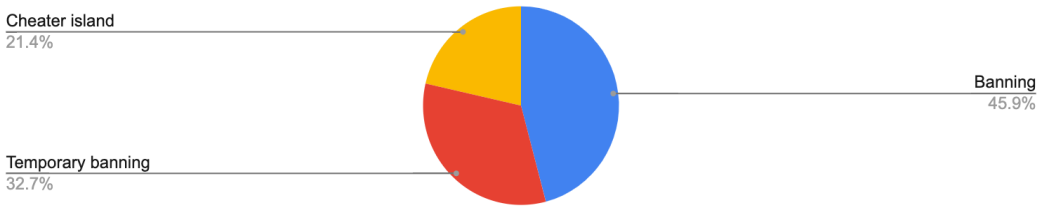


Chart 7: Professionals' perspective on Security breaches experience

51.5% of surveyed players would stop playing a game for security issues, and 44.4% would consider it.

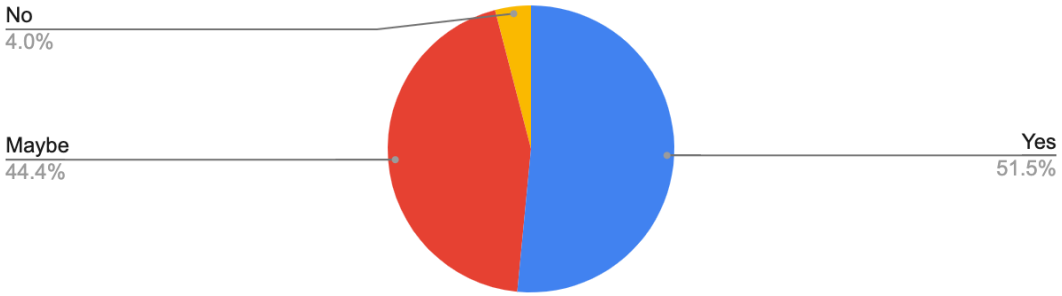


Chart 8: Players answers on if they would leave a game because of security issues

A very similar result was obtained from professionals.

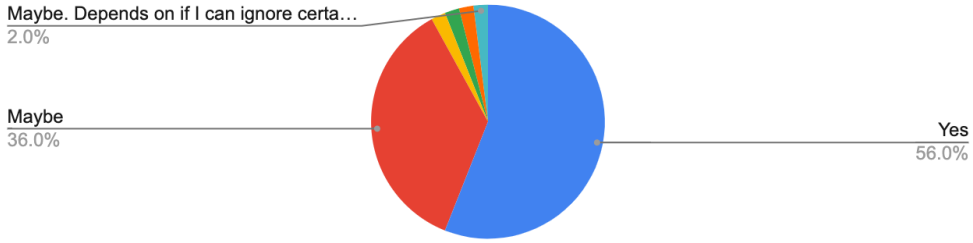


Chart 9: Professionals answers on if they would leave a game because of security issues

Players prefer banning over temporary banning or cheater island as a measure against cheating, and the same proves to be true for developers. However, developers prefer Cheater Island over temporary banning as the second best, contrary to players.

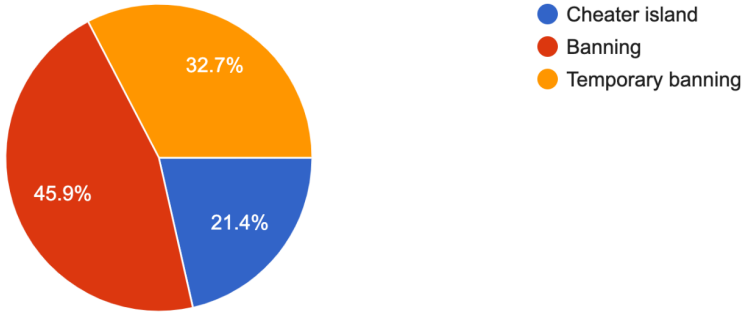


Chart 10: Preferred measures against cheating by players

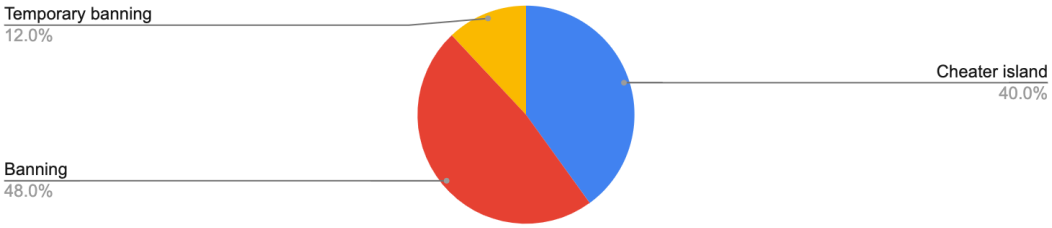


Chart 11: Preferred measures against cheating by professionals

The biggest concern for players is their data being compromised, as 67% of players revealed, the same as for developers when playing, with almost 88% choosing that same option.

6.7. Specific questions for professionals

About half of the developers have formal education in video games; however, most of the professionals who got formal education say that they did not receive proper security training in the courses they studied. With a range from 1 to 5, where 1 is none at all, 5 is absolute, 100% of the ones with formal education rated 3 and below, 60% of which rated 1.

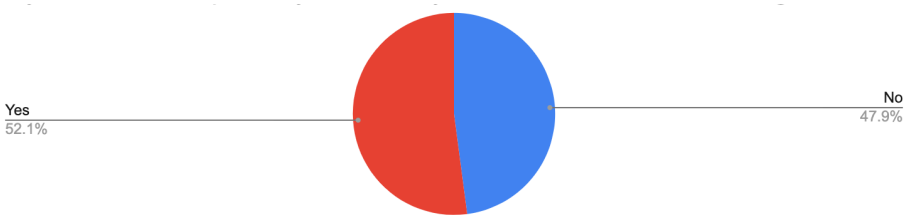


Chart 12: Professionals formal education percentages

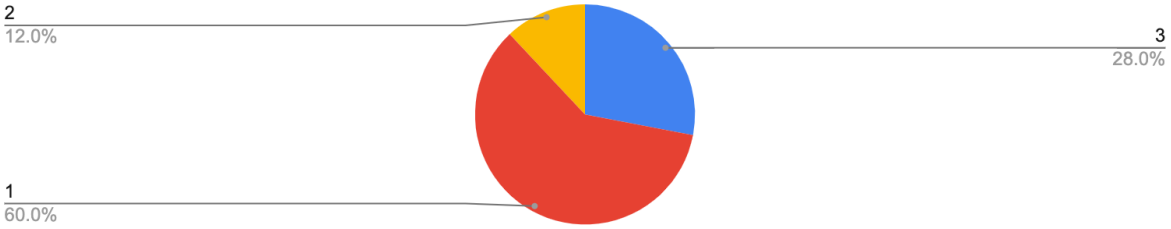


Chart 13: Formally educated professionals perception about security education

71% of developers have yet to receive video game security training from their employer.

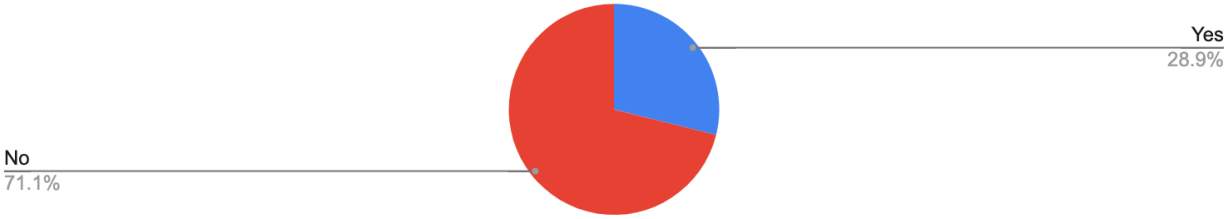


Chart 14: Professionals video game security training provided by the employer

62% of the interviewed professionals have no involvement in security, ranking it from 1 being none to 5 being complete.

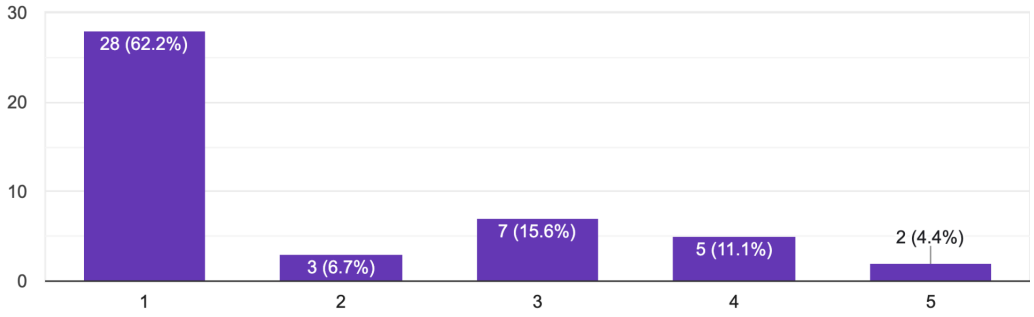


Chart 15: Professionals involvement in security

However, 73.3% of the interviewed people who answered how much involvement their role type should have answered from 3 to 5. The scales go from 1 being None and 5 being Complete.

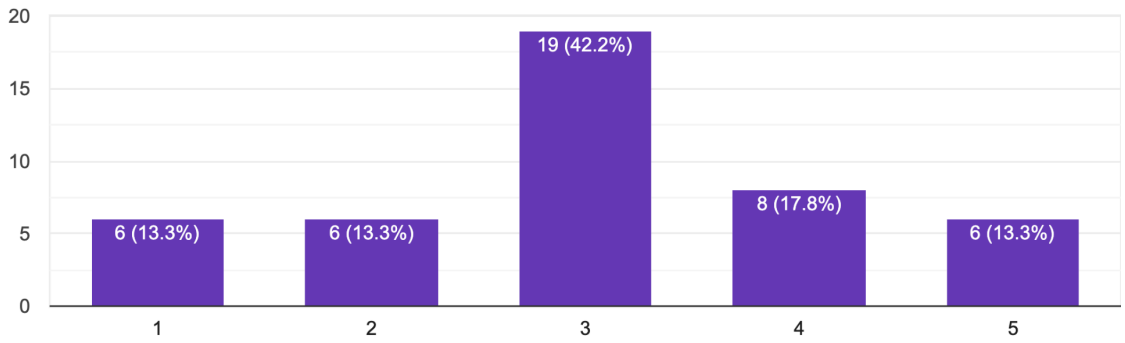


Chart 16: Professionals perception of the involvement their role type should have in security

52.1% think that security should start to be implemented during design and planning, followed by 25% saying that it is early in programming and 14.6% after there is a playable alpha.

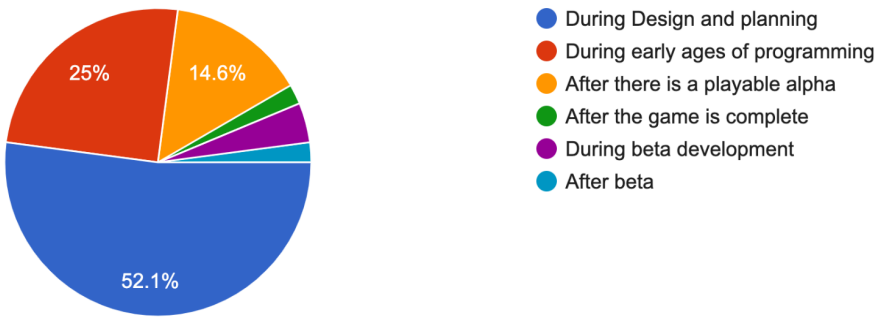


Chart 17: Professionals' opinion on when security should be implemented in video games

About the outsourcing of security, 34% think it is okay to partially outsource work, but some of it needs to be in-house, 23.4% think it is good, cost-efficient, and a specialized company has all the knowledge available, and 19.1% think it is not good, neither cost-efficient to outsource security.

Regarding how much security should be outsourced, the scale goes from 1 being None to five being All; 42.9% answered a 3.

Chart 18: Professionals opinion on security outsourcing

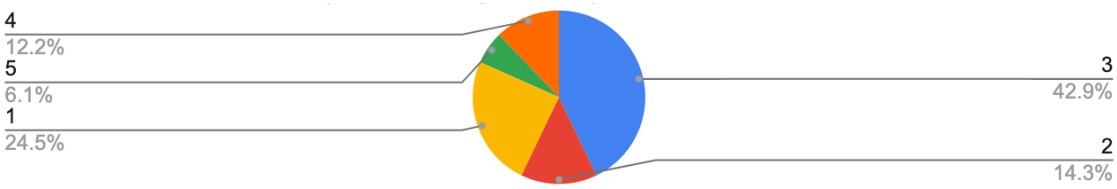


Chart 19: Professionals' opinion on how much security should be outsourced

The security breaches considered most dangerous are:

1. User privacy compromised (81.6%)
2. Ransomware (67.3%)
3. Terrorism (57.1%)
4. Other attacks on users (55.1%)

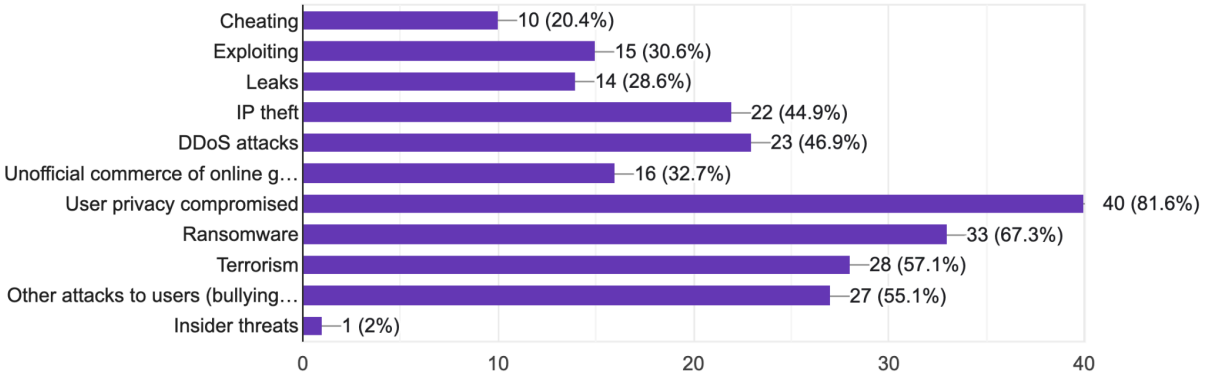


Chart 20: Most dangerous threats according to professionals

The security breaches considered most expensive by professionals to companies are:

1. User privacy compromised or Leaks(46% each)

2. Ransomware (44%)
3. DDoS attacks (42%)
4. IP theft (40%)

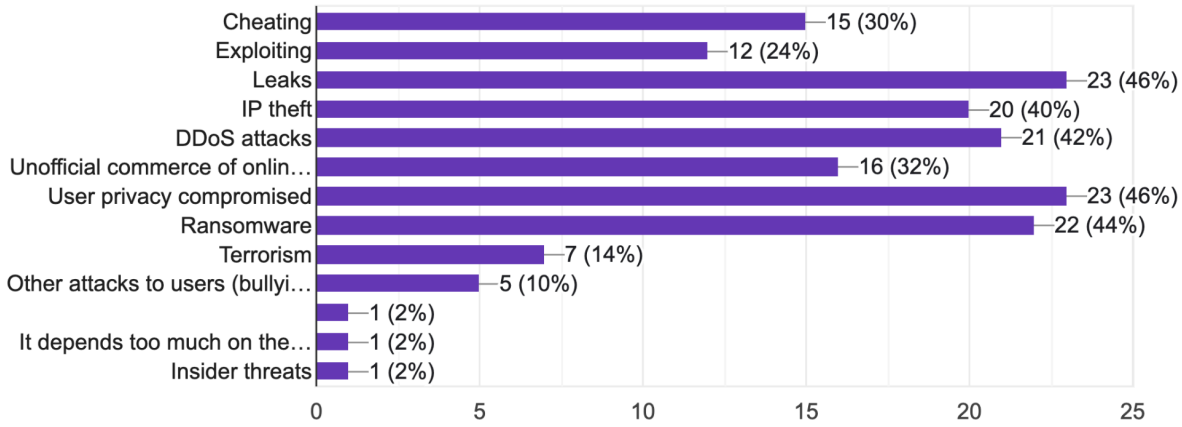


Chart 21: Most dangerous threats according to professionals

6.8. Comparative Results

There is almost no difference between the groups in many of the 15 questions that were asked to both groups:

- 61.2% of players and 66% of professionals said they never cheated.
- 51.5% of players and 56% of professionals said they would stop playing a game if there were security issues.
- The opinions about whether games are secure are almost equally divided into yes, no, and maybe.
- They think games are unsafe for minors, followed by the answer that only some are.
- Neither group has a strong positive or negative opinion about kernel security.
- Neither group has been reading the terms of service of video games.
- They share almost the same level of confidence in video game safety, with less trust from industry professionals than players.
- Both groups' preferred anti-cheating measure is banning.

7. Conclusions & Recommendations

7.1. Survey Reactions

Players received very positively being surveyed, as they liked the idea of feeling heard or given a voice, this was reflected in some of the comments of the survey and also commented when asked if they would be willing to participate in the studio.

They also understood that they could skip any question they did not want to answer or did not apply to their circumstances.

With the developers, the surveys were received in a more polarised manner. Some of them were very negative, thinking it was an attempt to sell some sort of service, and some of them were very excited about it. A lot of them worried about the gathering of personal data, even though no emails or identifiable data were collected. Another group was actually interested in seeing this project's results.

During the survey, some notes were added so some professionals knew that they were not expected to answer all questions and to skip the ones not pertinent to them (this was not an issue with players).

7.2. Conclusions & Recommendations

To cover all the vulnerabilities, the best strategy is to plan security from the earlier stages on. As the survey shows, over half of the interviewed developers agree that it should be done during design and planning. Security can be quite expensive, and it is also necessary to budget for it.
Developers are not opposed to hiring help even though they believe that some security should be kept in-house. However, most of the interviewed professionals have not had video

game security formation in a formal setting or their companies, which only would lead to unofficial research, figuring things out by trial and error, and learning on the go.

Most professionals did not have involvement in security in the games they worked, even though most of them believe people on their role type should have some involvement.
Therefore, education on security could be proven useful for those in the future, taking into account the current job crisis in the industry [9], and could represent an advantage.
It can also be an opportunity for educational institutions to put themselves ahead of the trend and respond to what it can perceived as a need.

Interviewed players and professionals are mostly aligned in their opinions of security; even so, professionals failed to predict what would worry players the most—thinking about what they care about as players would be a better way of actually knowing what is on players' minds. However, surveying players and communicating with them is the method that will prove more reliable and appreciated by players.

Player data is the number one priority to protect, having possible legal repercussions aside from economic or reputational.
A better approach would be to use a combination of methods explained above, such as encryption, keeping player data to a minimum, player education, developer education, enforcement of safe passwords, and double authentication.

Currently, the opinion about how safe online gaming is is very divided. However, it is mostly not considered a safe place for minors (by both groups), as some games may be. If a developer wishes to keep minors safe in a game, there is a lot to do. Compare which games are safe vs not safe, study characteristics, and implement all the possible characteristics and measures of the safe ones. There should be more account restrictions than regular players, like no private messaging or restrictions on purchases. However, minors can avoid being truthful to avoid restrictions, even though that should go against the terms of service.

7.3. Future Paths

There are multiple ways this project can be a starting point for others:

- Investigate where and how professionals get their security information, as it is not through formal education, and how much knowledge they have. This can be done through a smaller survey.
- Seeing that players are not sure about how safe video games are, it could be investigated what makes them feel they may be unsafe. It has the potential to improve player's perceptions about games who implement those learnings.
- Investigate how to make games safer for minors.

Sources

[1] ***Akamai Research Shows Attacks on Gaming Companies Have More than Doubled Over Past Year.*** **(2022, August 4).Akamai. https://www.akamai.com/newsroom/press-release/akamai-research-shows-attacks-on-gaming-companies-more-than-doubled-over-past-year**

[2] Antipov O. (2023, June 13). ***3 Entry Points for DDoS Attacks in Gaming Services*** **DDoS-GUARD. https://ddos-guard.net/en/blog/ddos-attacks-in-gaming-services**

[3] Asma, A. (2022, September 23). ***HOW TO AVOID RANSOMWARE ATTACKS (PREVENTION STEPS TO KNOW & FAQS)*** **https://playnoevil.com/avoid-ransomware-attacks/**

[4] Behnke, R. (2023, September 25). ***Top 5 types of cybersecurity attacks in gaming.*** **https://www.halborn.com/blog/post/top-5-types-of-cybersecurity-attacks-in-gaming**

[5] Borisovas, P., & Borisovas, P. (2023, August 29). ***8 biggest video game leaks caused by hackers*****. NordVPN. https://nordvpn.com/es/blog/video-game-leaks/**

[6] Bowles, N., & Keller, M. H. (2020, February 3). ***Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators*****. The New York Times. https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html#:~:text=Sexual%20predators%20and%20other%20bad,conversation%20and%20gradually%20build%20trust.**

[7] Cardoso, R. (2022). ***Security issues in massively multiplayer online games.*** **www.academia.edu. https://www.academia.edu/74798044/Security_Issues_in_Massively_Multiplayer_Online_Games?email_work_card=title**

[8] Carpenter, N. (2023, December 20). ***The Insomniac Games hack is unprecedented.*** **Polygon. https://www.polygon.com/24009631/insomniac-games-leak-hack-rhysida-files-breach**

[9] Carroll M. (2024, April 17). ***Why are thousands of video game workers losing their jobs?*** **Sky News. https://news.sky.com/story/record-job-losses-despite-an-industry-on-the-rise-whats-going-on-in-uk-gaming-13113559**

[10] Consalvo, M. (2007). ***Cheating*****. https://doi.org/10.7551/mitpress/1802.001.0001**

[11] ***Cybersecurity in the Game Industry Statistics*****. (2024, April 16). GitNux https://gitnux.org/cybersecurity-in-the-game-industry/**

[12] Davis, S. B. (2009). ***Protecting Games: A security handbook for game developers and publishers*****. http://dl.acm.org/citation.cfm?id=1538724**

[13] ***Digital piracy*****. (n.d.) Interpol https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Digital-piracy**

[14] ***Download the EA app – Powering next generation of PC gaming*** **(2024, April 25). Electronic Arts Inc. https://www.ea.com/ea-app**

[15] ***Extremism and Gaming Research Network (EGRN) - Home.*** **(2024, June 5). EGRN https://extremismandgaming.org/**

[16] Gach, E. (2023, June 25). ***Diablo IV suffers extended DDOS attack [Update]*****. Kotaku. https://kotaku.com/diablo-4-ddos-attack-server-status-what-is-blizzard-rpg-1850574778**

[17] Gatlan, S. (2024, February 23). ***Insomniac Games alerts employees hit by ransomware data breach*****. BleepingComputer. https://www.bleepingcomputer.com/news/security/insomniac-games-alerts-employees-hit-by-ransomware-data-breach/**

[18] Godsey, B. (2017, March 6). ***Video game security: The future belongs to machines*****. Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/video-game-security-future-machines/**

[19] Haapaniemi, H. (2024). ***Cheat detection & prevention methods in video games*** **(Bachelor's thesis, H. Haapaniemi).**

[20] ***Hate is No Game: Hate and Harassment in Online Games 2023*** **(2024, February 6). ADL. https://www.adl.org/resources/report/hate-no-game-hate-and-harassment-online-games-2023#:~:text=76%20percent%20of%20adults%20experience,adult%20gamers%20overall%20(76%25).**

[21] ***How to report bad player behavior in Fortnite*** **(n.d.). Epic Games. https://www.epicgames.com/help/en-US/c-Category_Fortnite/c-Fortnite_PlayerBehavior/how-to-report-bad-player-behavior-in-fortnite-a000086135**

[22] Kirmse, C.(1997, July 7).Security in online games. https://www.gamedeveloper.com/game-platforms/security-in-online-games#close-modal

[23] Lakhani, S. (2021). VIDEO GAMING AND (VIOLENT) EXTREMISM: An exploration of the current landscape, trends, and threats. https://home-affairs.ec.europa.eu/system/files/2022-02/EUIF%20Technical%20Meeting%20on%20Video%20Gaming%20October%202021%20RAN%20Policy%20Support%20paper_en.pdf

[24] LCK Hit by Severe DDoS. (2024, March 3). GGBoost https://ggboost.com/blog/post/lol-lck-hit-by-ddos

[25] Leder, M. (2023, May 30). Gaming Cyber Threats: Risks & Impacts. Imperva Blog. https://www.imperva.com/blog/cyber-attacks-gaming-industry/

[26] Lee, S. J., Jeong, E. J., Lee, D. Y., & Kim, G. M. (2021, November 29). Why Do Some Users Become Enticed to Cheating in Competitive Online Games? An Empirical Study of Cheating Focused on Competitive Motivation, Self-Esteem, and Aggression. Frontiers In Psychology, 12. https://doi.org/10.3389/fpsyg.2021.768825

[27] Lehtonen,S (2020, March 7). Comparative Study of Anti-cheat Methods in Video Games (Master's thesis, Lehtonen,S). https://helda.helsinki.fi/server/api/core/bitstreams/89d7c14b-58e0-441f-a0de-862254f95551/content

[28] Massive Account Hijack/Hacking . (2023, August 7). Steam Community https://steamcommunity.com/discussions/forum/7/3802779235953508377/

[29] ***Network Technical Difficulties Caused by DDoS Attacks (May. 6) FINAL FANTASY XIV, The Lodestone. (*****2024, May 6). SQUARE ENIX Ltd. https://eu.finalfantasyxiv.com/lodestone/news/detail/ce7c49af75f176a98b831e506fa3ebfcad59d31c

[30] Orland, K. (2022, March 24). Stop treating cheaters in online games as "the enemy." Ars Technica. https://arstechnica.com/gaming/2022/03/why-do-people-cheat-in-online-games-and-what-can-we-do-about-it/

[31] Orland, K. (2022, September 14). EA's new anti-cheat tools dip into the dreaded "kernel mode." Ars Technica. https://arstechnica.com/gaming/2022/09/eas-new-anti-cheat-tools-dip-into-the-dreaded-kernel-mode/

[32] Our Response to the Tragedy in Buffalo. (2023, May 20). Discord https://discord.com/safety/our-response-to-the-tragedy-in-buffalo

[33] Picture of Horse (2019, July 17) ***DDoS Prevention Guide*** **https://support-leagueoflegends.riotgames.com/hc/en-us/articles/201751764-DDoS-Prevention-Guide**

[34] Pritchard, M.(2000, July 24). How to Hurt the Hackers: The scoop on internet cheating and how you can combat it. https://www.gamedeveloper.com/design/how-to-hurt-the-hackers-the-scoop-on-internet-cheating-and-how-you-can-combat-it

[35] Richardson, B. T. (2023, December 22). Insomniac: PlayStation studio «angered» by ransomware hack. https://www.bbc.com/news/newsbeat-67805736

[36] Sheehan, G. (2020, January 20). «Fortnite» adds new competitive rules focused on collusion. Bleeding Cool News And Rumors. https://bleedingcool.com/games/fortnite-adds-new-competitive-rules-focused-on-collusion/

[37] SIGNALING UPDATE - COMPETITIVE FORTNITE 2020. (2020, January 20). The Competitive Fortnite Team https://www.fortnite.com/competitive/news/signaling-update-competitive-fortnite-2020?lang=en-US

[38] Singh Rawat A. (2020, October 8). New CS:GO Cheat Exposed That is Nearly Impossible to Detect by Anti-Cheats. AFK Gaming. https://afkgaming.com/csgo/news/5157-new-csgo-cheat-exposed-that-is-nearly-impossible-to-detect-by-anti-cheats

[39] Soliven,R & Kimura, H(2022, August 24). Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus. Trend Micro. https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html?cjdata=MXxZfDB8WXww&PID=7706533&SID=pcg-es-4429984077259979084&cjevent=0e5d4a8424c811ef82d6004a0a18b8f

[40] Staff, V. (2024, March 19). Electronic Arts files patent for collusion detection system for online gaming. Verdict. https://www.verdict.co.uk/electronic-arts-files-patent-for-collusion-detection-system-for-online-gaming/

[41] Steam Community: Human fall flat. (n.d.)Steam https://steamcommunity.com/app/477160/workshop/

[42] The Sims cheats. (2022, October 12). Electronic Arts https://www.ea.com/games/the-sims/cheats?setLocale=en-us

[43] What is a content delivery network (CDN) and which CDN providers is Nintendo working with? Nintendo Of Europe AG. (n.d.) Nintendo https://www.nintendo.com/en-za/Legal-information/What-is-a-content-delivery-network-CDN-and-which-CDN-providers-is-Nintendo-working-with-/What-is-a-content-delivery-network-CDN-and-which-CDN-providers-is-Nintendo-working-with-1378848.html

[44] whatacoolwitch (2023, November 01). Be on Your Best Behavior https://support-valorant.riotgames.com/hc/en-us/articles/360044270174-Be-on-Your-Best-Behavior#:~:text=If%20you%20take%20part%20in,%2C%20harassing%2C%20or%20offensive%20language.

[45] Yan, Jeff (n.d.) Security Design in Online Games https://prof-jeffyan.github.io/yan_acsac03.pdf

[46] Yan, Jeff & Randell, Brian. (2005). A systematic classification of cheating in online games. 1-9. 10.1145/1103599.1103606.

[47] Yan, Jeff & Randell, Brian. (2009). An Investigation of Cheating in Online Games. IEEE Security & Privacy. 7. 37-44. 10.1109/MSP.2009.60.

[48] Zinszer, D. (2022, May 24). The history of cybersecurity in video games. PlexTrac. PlexTrac. https://plextrac.com/the-history-of-cybersecurity-in-video-games/

Appendix

Appendix A: Players Survey Questionnaire

Appendix B: Professional Survey Questionnaire

Appendix C: Charts of player survey results

Appendix D: Charts of professional survey results

Security Survey for Players

This security survey is part of a final project from a student of a masters in Videogame design and Programming from the UOC. **The use of the data is academical.**
No personal data will be recorded or saved or is requested at any point.

P.S: This survey contains credits to get free survey responses at SurveySwap.io

1. **1) What is your sex?**

   Mark only one oval.

   - ◯ Man
   - ◯ Woman
   - ◯ Transgender Man
   - ◯ Transgender Woman
   - ◯ Non binary/ non conforming
   - ◯ Prefer not to respond
   - ◯ Other: _____

2. **2)What is your age group?**

   Mark only one oval.

   - ◯ 18-24
   - ◯ 25-34
   - ◯ 35-44
   - ◯ 45-54
   - ◯ 55-64
   - ◯ 65 and over

3. **3)What is your relation with Gaming?**

Mark only one oval.

- ◯ Player
- ◯ Developer
- ◯ Blogger
- ◯ Customer service
- ◯ Student

4. **4) To your knowledge , has any of the games you worked or played suffered from any security breach? (Cheating is included).**

Mark only one oval.

- ◯ Yes
- ◯ No

5. **5) If so, do you know the type of attack?**

Tick all that apply.

- ☐ Cheating
- ☐ Exploiting
- ☐ Leaks
- ☐ IP Theft (i.e. games that look exactly like the original, games using the same sound...)
- ☐ DDos attacks
- ☐ Unofficial commerce of online goods
- ☐ User privacy compromised
- ☐ Ransomware
- ☐ Terrorism
- ☐ Other attacks to users (bullying, grooming of minors, stalking...)

6. **6)In your opinion, have these issues been resolved successfully?**

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Completely

7. **7) As a player which attacks worry you the most? (Multiple answers are accepted)**

Tick all that apply.

- [ ] Cheating or any form of people gaining unfair advantage
- [ ] DDoS attacks that will stop you from playing
- [ ] User privacy compromised
- [ ] Other attacks to users (bullying, grooming of minors, stalking...)
- [ ] Other: _____

8. **8)As a player, Would you leave a game if there were security issues?**

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

9. **9)Of the following measures against cheating, which one do you agree the most?**

Mark only one oval.

- ◯ Cheater island
- ◯ Banning
- ◯ Temporary banning

10. **10) Do you think your personal data is safe in the games you play?**

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Completely

11. **11)Have you ever read the Terms of Service of a Videogame?**

Mark only one oval.

	1	2	3	4	5	
Nev	◯	◯	◯	◯	◯	Always

12. **12) What is your opinion in regards of kernel based security measures?**

Mark only one oval.

	1	2	3	4	5	
I am	◯	◯	◯	◯	◯	I am in favor

13. **13) Have you ever cheated in a videogame?**

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

14. **14) Do you think online videogames are safe in general?**

Mark only one oval.

- Yes
- No
- Maybe

15. **15) Do you feel that online videogames are a safe place for minors?**

Mark only one oval.

- Yes
- No
- Only some

16. **16) Would you like to add any comment?**

Professional Security Survey

This security survey is part of a final project from a student of a masters in Videogame design and Programming from the UOC. **The use of the data is academical.**
No personal data will be recorded or saved or is requested at any point.

ANY questions can be left unanswered.

P.S: This survey contains credits to get free survey responses at SurveySwap.io

1. **1) What is your sex?**

   Mark only one oval.

   - ◯ Man
   - ◯ Woman
   - ◯ Transgender Man
   - ◯ Transgender Woman
   - ◯ Non binary/ non conforming
   - ◯ Prefer not to respond
   - ◯ Other: _____

2. **2) What is your age group?**

   Mark only one oval.

   - ◯ 18-24
   - ◯ 25-34
   - ◯ 35-44
   - ◯ 45-54
   - ◯ 55-64
   - ◯ 65 and over

3. **3) What is your relation with Gaming?**

Mark only one oval.

- ◯ Player
- ◯ Developer
- ◯ Blogger
- ◯ Customer service
- ◯ Student

4. **4) If you are a developer, what is your type of role? (More than one answer is possible)**

Tick all that apply.

- ☐ Designer
- ☐ Programmer
- ☐ Live OPS
- ☐ Security
- ☐ Quality
- ☐ Artist
- ☐ Animator
- ☐ Writer
- ☐ Producer
- ☐ Other: _____

5. **5) What type of games have you developed?**

Tick all that apply.

- ☐ Mobile
- ☐ HD (console/computer)
- ☐ Indie
- ☐ AAA
- ☐ AA
- ☐ Other: _____

6. **6) If you are a developer, do you have any formal education about videogames?**

   Mark only one oval.

   - ◯ Yes
   - ◯ No

7. **7)[Answer ONLY if you selected yes in 6] In the course or courses you took about video games development did you learn about videogame security?**

   Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Absolutely

8. **8) Have you gotten any security training related to videogames by your employer?**

   Mark only one oval.

   - ◯ Yes
   - ◯ No

9. **9) [Answer ONLY if you selected yes in 8] How often is this training reinforced?**

Mark only one oval.

- ◯ Monthly
- ◯ Quarterly
- ◯ Twice a year
- ◯ Once a year
- ◯ Less than once a year
- ◯ I do not know

10. **10) To your knowledge , has any of the games you worked or played suffered from any security breach? (Cheating is included).**

Mark only one oval.

- ◯ Yes
- ◯ No

11. **11) [Answer ONLY if you selected yes in 10] If so, do you know the type of attack?**

Tick all that apply.

- ☐ Cheating
- ☐ Exploiting
- ☐ Leaks
- ☐ IP Theft (i.e. games that look exactly like the original, games using the same sound...)
- ☐ DDos attacks
- ☐ Unofficial commerce of online goods
- ☐ User privacy compromised
- ☐ Ransomware
- ☐ Terrorism
- ☐ Other attacks to users (bullying, grooming of minors, stalking...)

12. **12) [Answer ONLY if you selected yes in 10] In your opinion, have these issues been resolved successfully?**

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Completely

13. **13) What involvement have you had on security of games you worked at?**

Mark only one oval.

	1	2	3	4	5	
Non	◯	◯	◯	◯	◯	Complete

14. **14) What involvement you think people in your role type should have?**

Mark only one oval.

	1	2	3	4	5	
Non	◯	◯	◯	◯	◯	Complete

15. **15) When do you think security should be started to be implemented on a videogame?**

Mark only one oval.

- ◯ During Design and planning
- ◯ During early ages of programming
- ◯ After there is a playable alpha
- ◯ After the game is complete
- ◯ During beta development
- ◯ After beta

16. **16) What is your opinion on outsourcing security in videogames? Select the estatement you agree with the most**

Mark only one oval.

- ◯ I don't think is good, but it ends up being cost efficient
- ◯ I do not think is a good option and is not cost efficient
- ◯ I think is okay to partially outsource work, but some of it needs to be in house.
- ◯ I think it is good, cost efficient and a specialised company has all the knowledge available.
- ◯ I think is a good option but more expensive than doing it in-house

17. **17) How much of security in videogames you think should be outsorced?**

Mark only one oval.

	1	2	3	4	5	
Non	◯	◯	◯	◯	◯	All aspects

18. **18) What types of security breaches do you think are the most dangerous in a game?**

Tick all that apply.

- [ ] Cheating
- [ ] Exploiting
- [ ] Leaks
- [ ] IP theft
- [ ] DDoS attacks
- [ ] Unofficial commerce of online goods
- [ ] User privacy compromised
- [ ] Ransomware
- [ ] Terrorism
- [ ] Other attacks to users (bullying, grooming of minors, stalking...)
- [ ] Other: _____

19. **19) Which types of attacks do you think cost more money to videogame companies?(Multiple answers are accepted)**

Tick all that apply.

- [ ] Cheating
- [ ] Exploiting
- [ ] Leaks
- [ ] IP theft
- [ ] DDoS attacks
- [ ] Unofficial commerce of online goods
- [ ] User privacy compromised
- [ ] Ransomware
- [ ] Terrorism
- [ ] Other attacks to users (bullying, grooming of minors, stalking...)
- [ ] Other: _____

20. **20) Which security breaches do you worry most about as a developer? (Multiple answers are accepted)**

Tick all that apply.

- [ ] Cheating
- [ ] Exploiting
- [ ] Leaks
- [ ] IP theft
- [ ] DDoS attacks
- [ ] Unofficial commerce of online goods
- [ ] User privacy compromised
- [ ] Ransomware
- [ ] Terrorism
- [ ] Other attacks to users (bullying, grooming of minors, stalking...)
- [ ] Other: _____

21. **21) As a player which attacks worry you the most? (Multiple answers are accepted)**

Tick all that apply.

- [ ] Cheating or any form of people gaining unfair advantage
- [ ] DDoS attacks that will stop you from playing
- [ ] User privacy compromised
- [ ] Other attacks to users (bullying, grooming of minors, stalking...)
- [ ] Other: _____

22. **22) Which attacks do you think worries players the most? (Multiple answers are accepted)**

Tick all that apply.

- [ ] Cheating or any form of people gaining unfair advantage
- [ ] DDoS attacks that will stop you from playing
- [ ] User privacy compromised
- [ ] Other attacks to users (bullying, grooming of minors, stalking...)
- [ ] Other: _____

23. **23) As a player, Would you leave a game if there were security issues?**

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe
- ◯ Other: _____

24. **24) Of the following measures against cheating, which one do you agree the most?**

Mark only one oval.

- ◯ Cheater island
- ◯ Banning
- ◯ Temporary banning

25. **25) Do you think your personal data is safe in the games you play?**

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Completely

26. **26) Have you ever read the Terms of Service of a Videogame?**

Mark only one oval.

	1	2	3	4	5	
Nev	◯	◯	◯	◯	◯	Always

27. **27) What is your opinion in regards of kernel based security measures?**

Mark only one oval.

	1	2	3	4	5	
I am	◯	◯	◯	◯	◯	I am in favor

28. **28) Have you ever cheated in a videogame?**

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

29. **29) Do you think online videogames are safe in general?**

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

30. **30) Do you feel that online videogames are a safe place for minors?**

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Only some

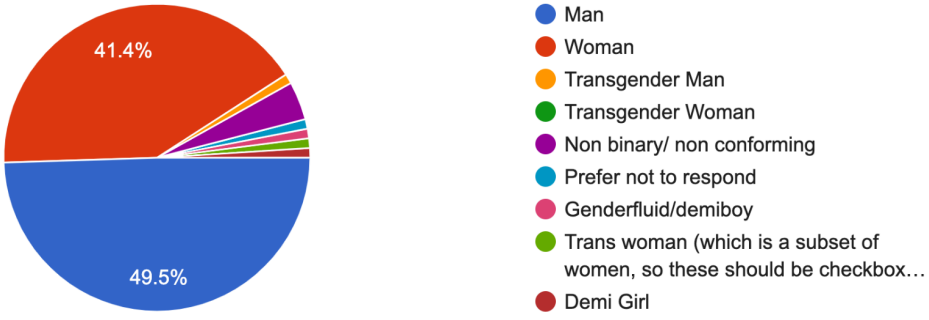
31. **31) Would you like to add any comment?**

Appendix C

Security Survey for Players

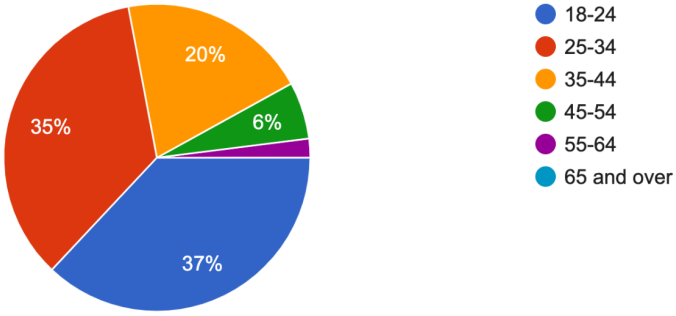
1) What is your sex?

99 responses



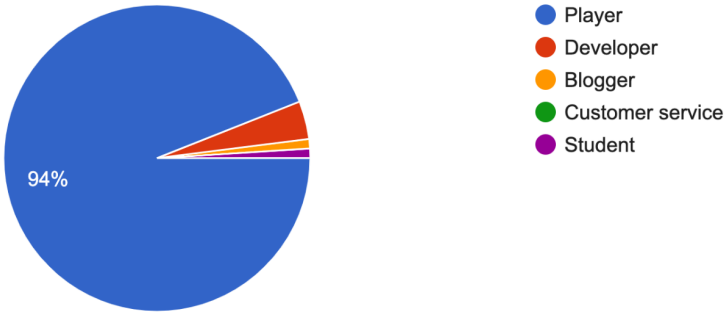
2)What is your age group?

100 responses



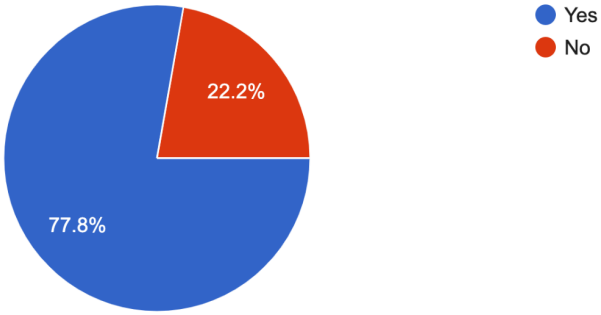
3)What is your relation with Gaming?

100 responses



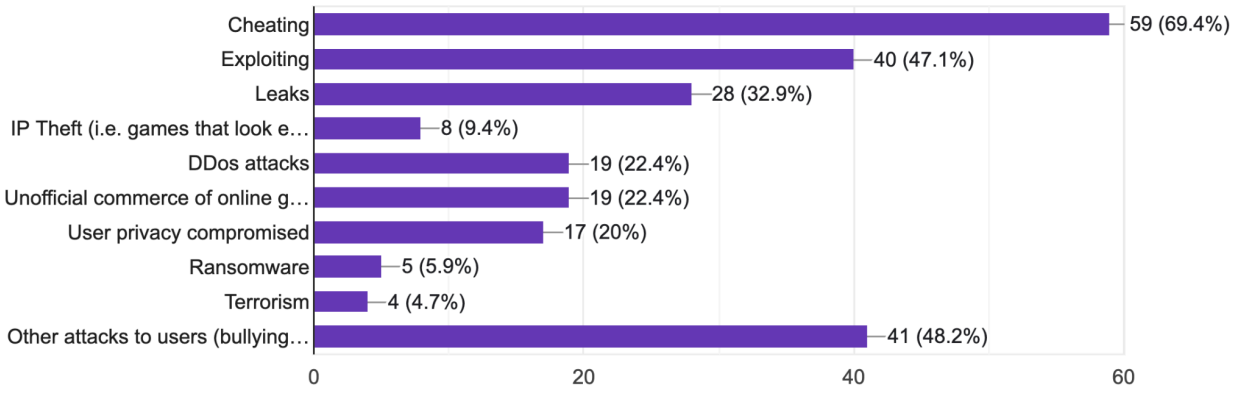
4) To your knowledge , has any of the games you worked or played suffered from any security breach? (Cheating is included).

99 responses



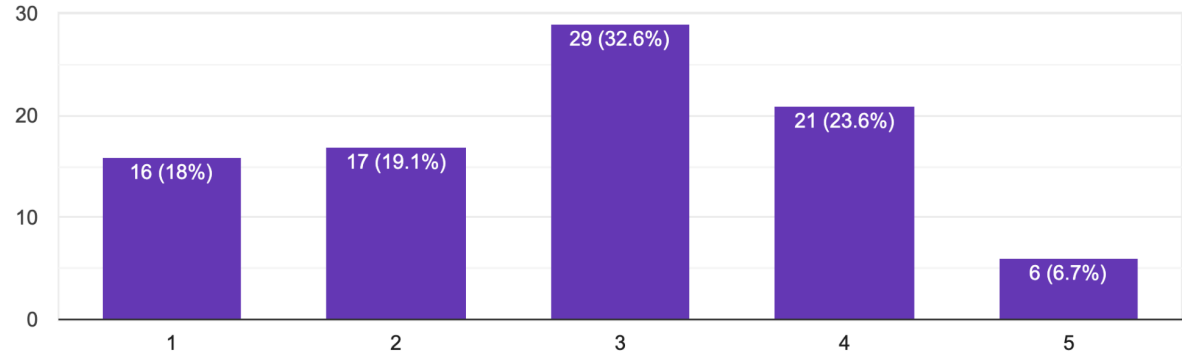
5) If so, do you know the type of attack?

85 responses



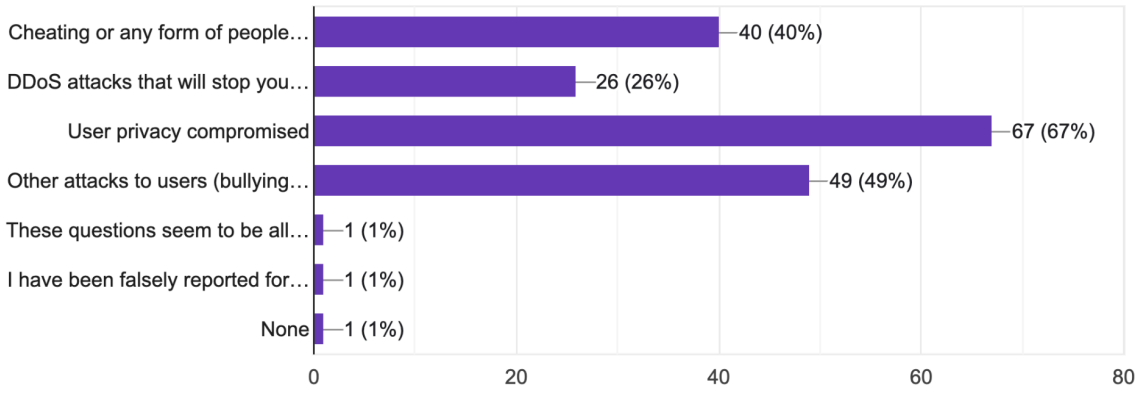
6)In your opinion, have these issues been resolved successfully?

89 responses



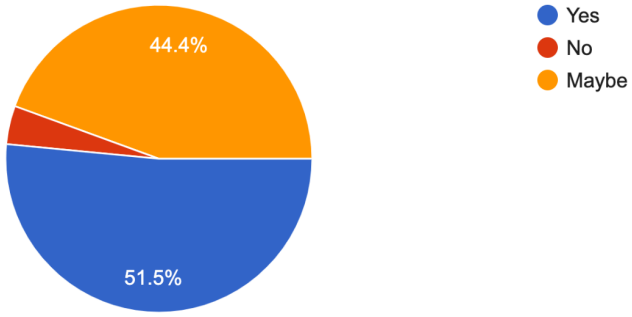
7) As a player which attacks worry you the most? (Multiple answers are accepted)

100 responses



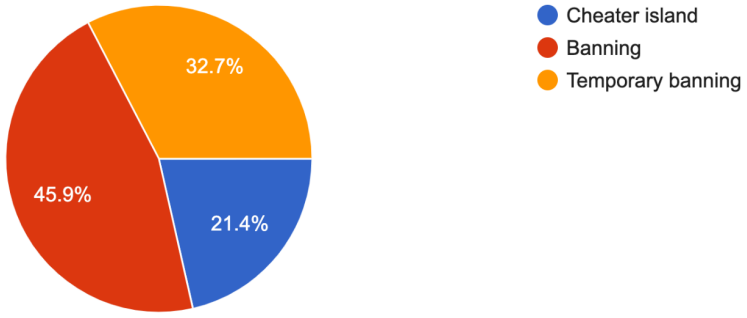
8)As a player, Would you leave a game if there were security issues?

99 responses



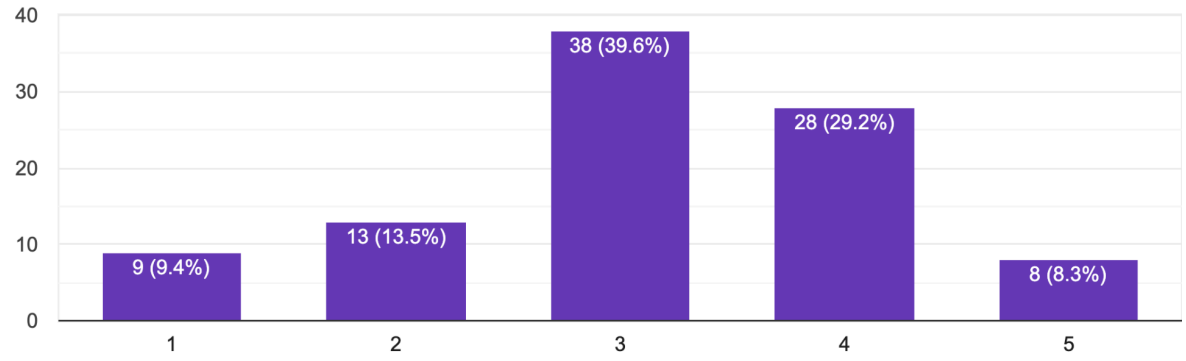
9)Of the following measures against cheating, which one do you agree the most?

98 responses



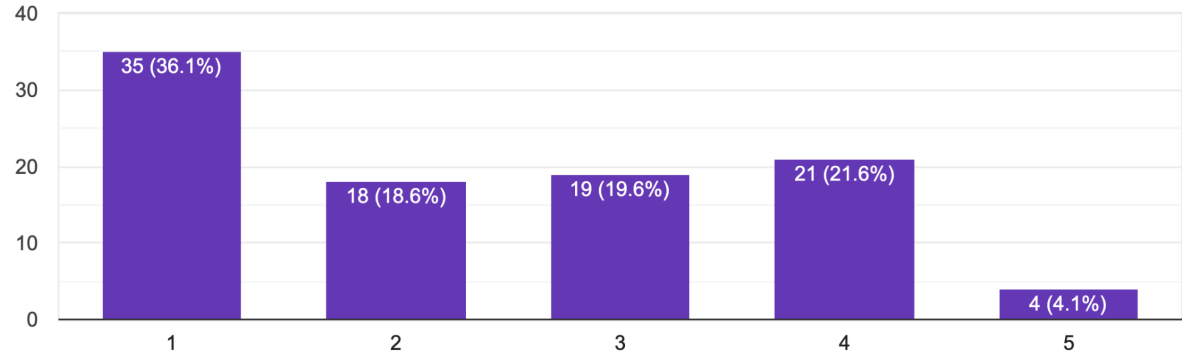
10) Do you think your personal data is safe in the games you play?

96 responses



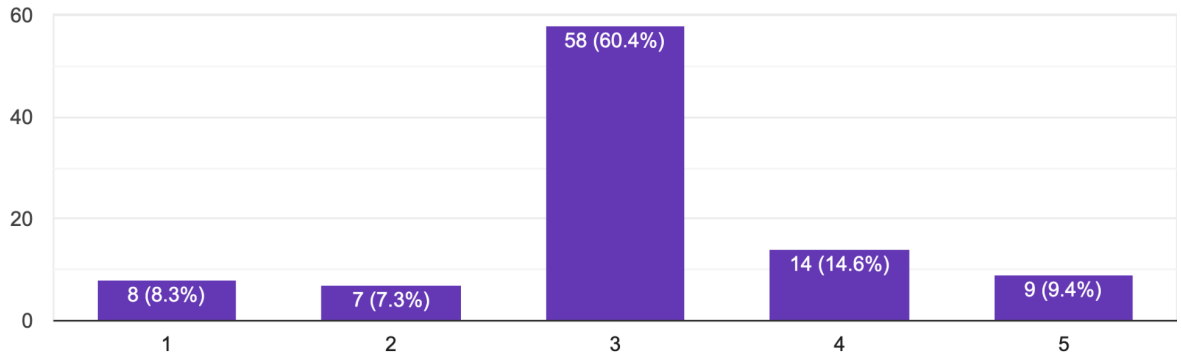
11)Have you ever read the Terms of Service of a Videogame?

97 responses



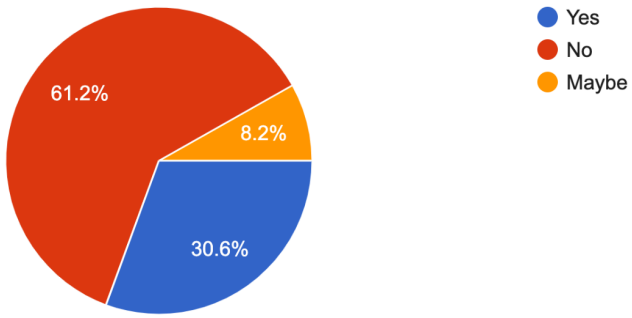
12) What is your opinion in regards of kernel based security measures?

96 responses



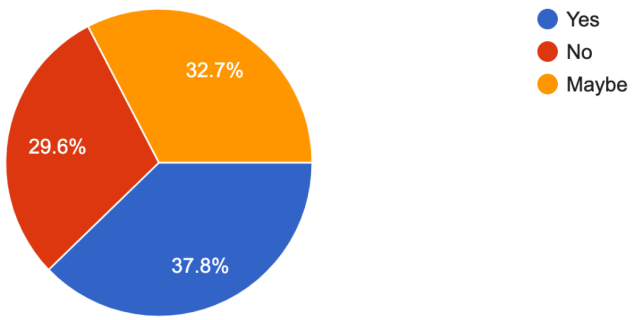
13) Have you ever cheated in a videogame?

98 responses



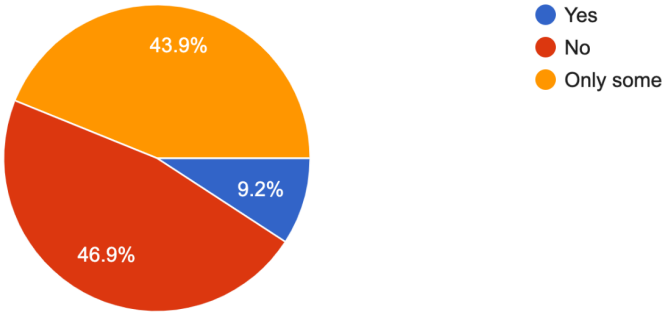
14) Do you think online videogames are safe in general?

98 responses



15) Do you feel that online videogames are a safe place for minors?

98 responses



16) Would you like to add any comment? 22 responses

No

If a video game company can be open and honest about the issues they are facing and make the effort to fix said issues then the player base will remain stable through those issues.

Sometimes a great cheat, while unfair, will go down in gaming history, and that's so fun to watch.

cheats an anticheats suck

Your question 3 should be to select multiple answers because some people might be a player and a student and some could be a player and developer. But your questionnaire was really good. Good luck with your project.

My case of cheating was wallhacking in a PVP shooter when I was 11. Even though the game was terrible, I still regret doing that.

-

No

.

Kids younger than 13 must refrain from online games and 13-15 should play online games under parental guidance

Un saludo

We must develop a data privacy culture to make people aware of their rights as a user and as a player.

You should have given your name and the name of your uni to make it more legit.

N/A

Creo que en general son sitios seguros, pero pienso que para menores de edad no lo son puesto que es muy difícil saber quien esta detrás de un perfil de Internet, no me preocupa que alguien haga trampas en un videojuego (me parece mal pero el sabrá lo que hace), si me preocupa, robo de identidades, que roben cuentas y puedan acceder a datos sensibles

Some games are more safe then others, as a game with a lower age player range is more targeted to pedophiles then others, like Minecraft would have more Catfishers then a game like GTA

No.

I received more attacks like bullying once my gender was revealed.

I have worked in the gaming industry in the past, so I know a bit more about the security measures than a 'regular' player.

Players purchase services from the facilitators of cheating in games which perpetuate Is it. Players need to be educated against this to help improve the online experience for all

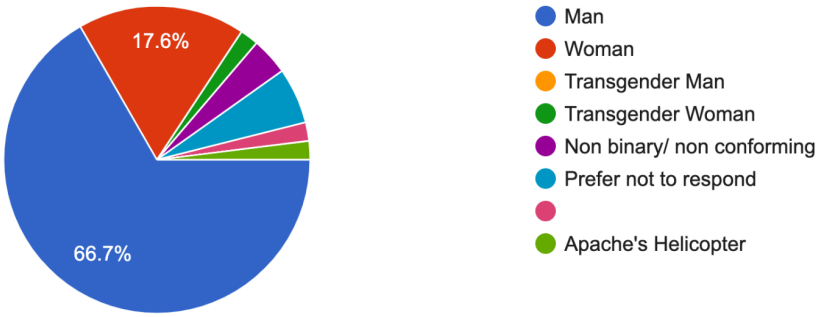
Especially games aimed at teens are very unsafe and very prone to sexual predators. A lot of competitive games for higher ages have very toxic comments but are not neccessarily unsafe

Appendix D

Pro Security Survey Charts

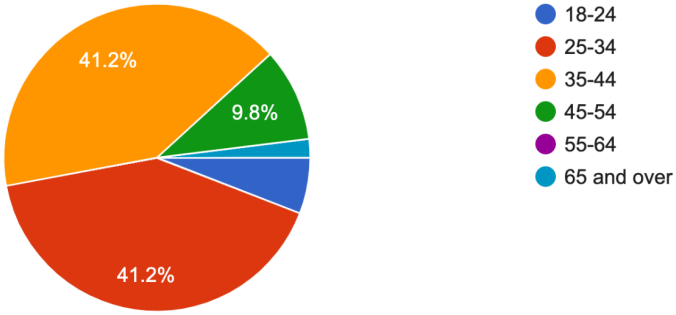
1) What is your sex?

51 responses



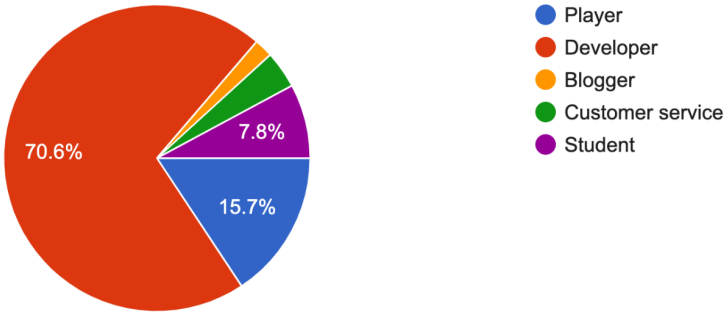
2) What is your age group?

51 responses



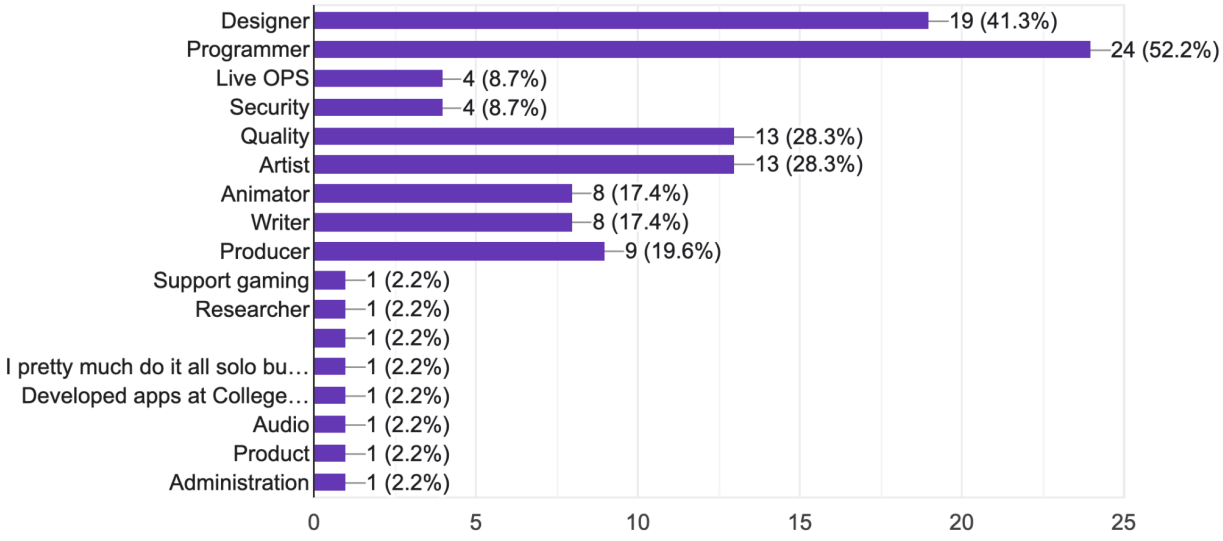
3) What is your relation with Gaming?

51 responses



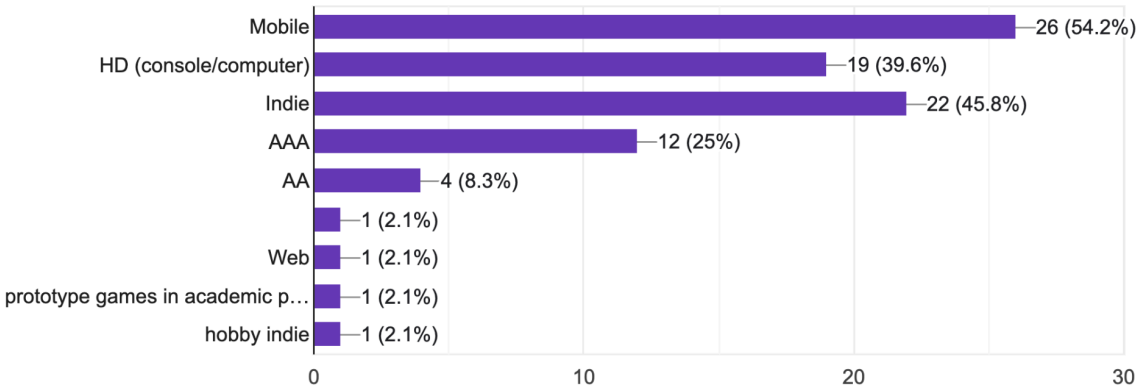
4) If you are a developer, what is your type of role? (More than one answer is possible)

46 responses



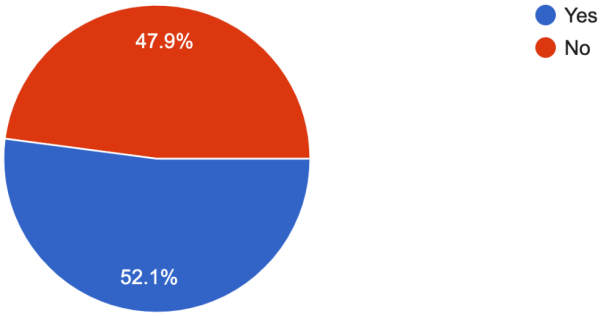
5) What type of games have you developed?

48 responses



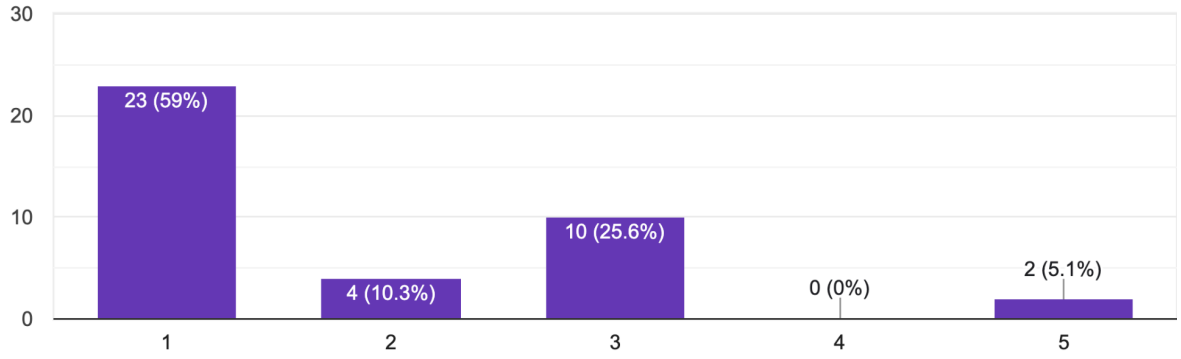
6) If you are a developer, do you have any formal education about videogames?

48 responses



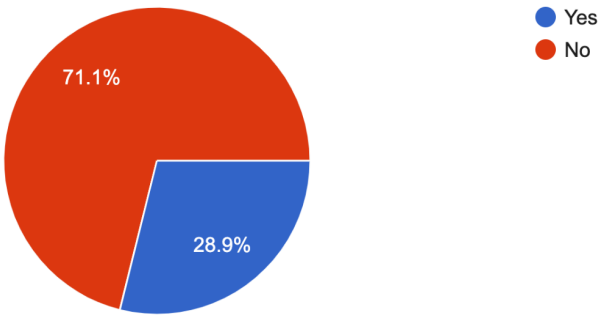
7)[Answer ONLY if you selected yes in 6] In the course or courses you took about video games development did you learn about videogame security?

39 responses



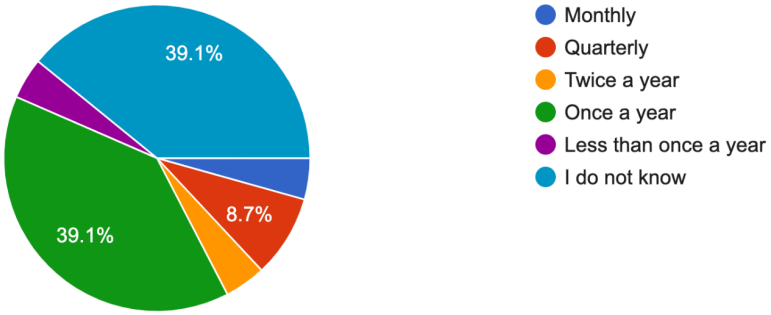
8) Have you gotten any security training related to videogames by your employer?

45 responses



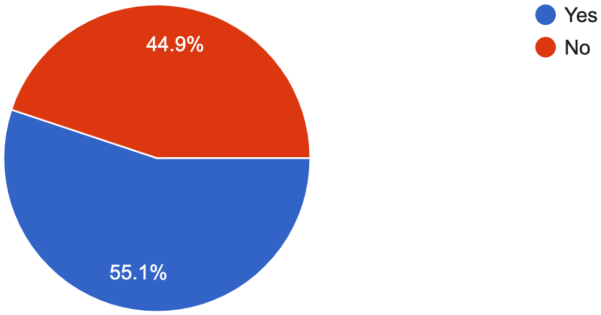
9) [Answer ONLY if you selected yes in 8] How often is this training reinforced?

23 responses



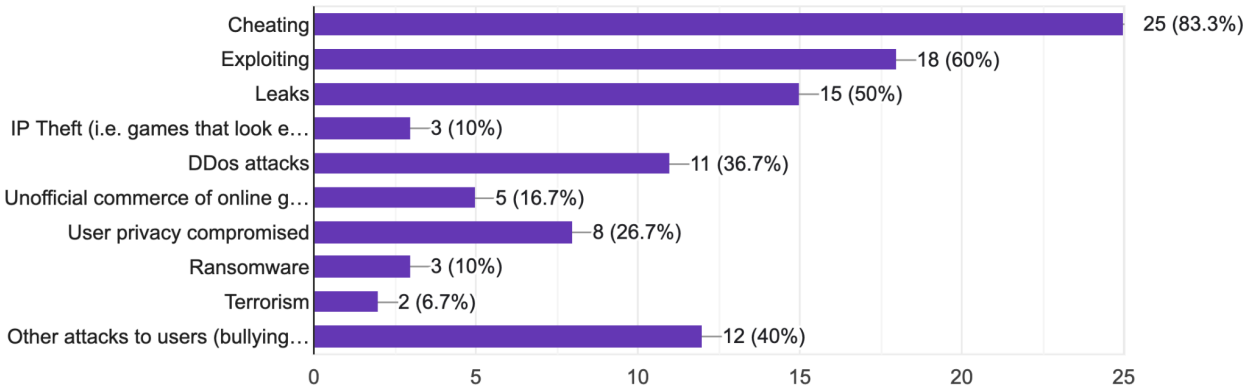
10) To your knowledge , has any of the games you worked or played suffered from any security breach? (Cheating is included).

49 responses



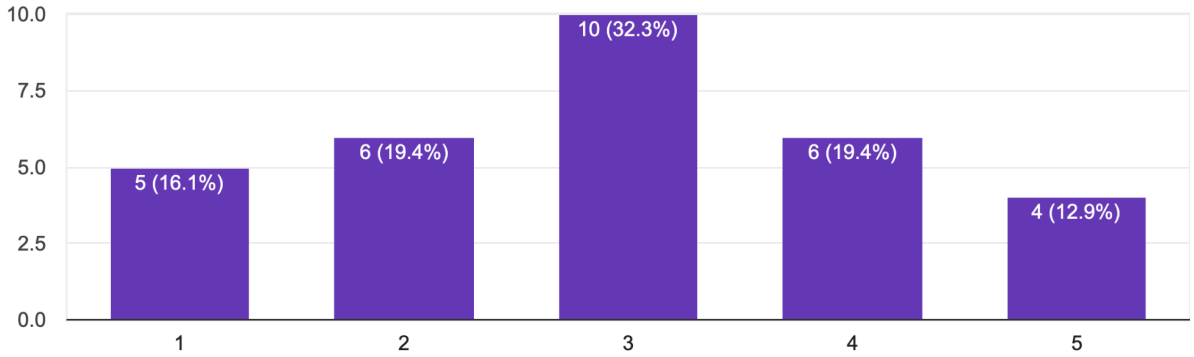
11) [Answer ONLY if you selected yes in 10] If so, do you know the type of attack?

30 responses



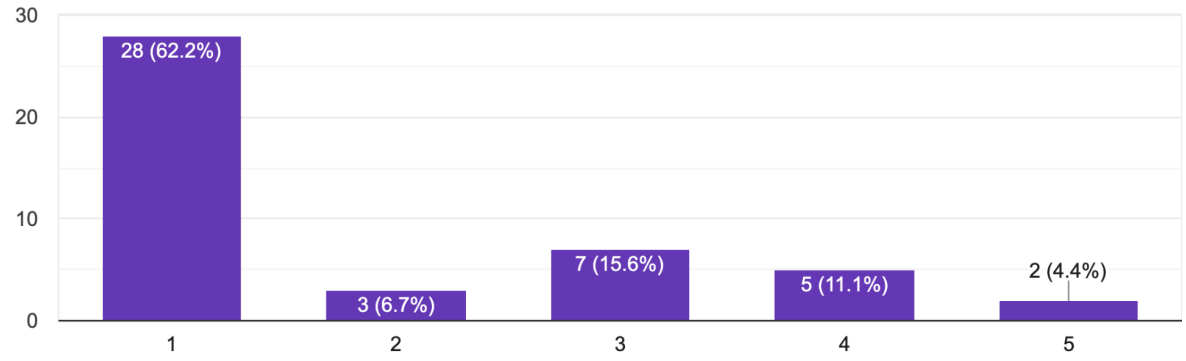
12) [Answer ONLY if you selected yes in 10] In your opinion, have these issues been resolved successfully?

31 responses



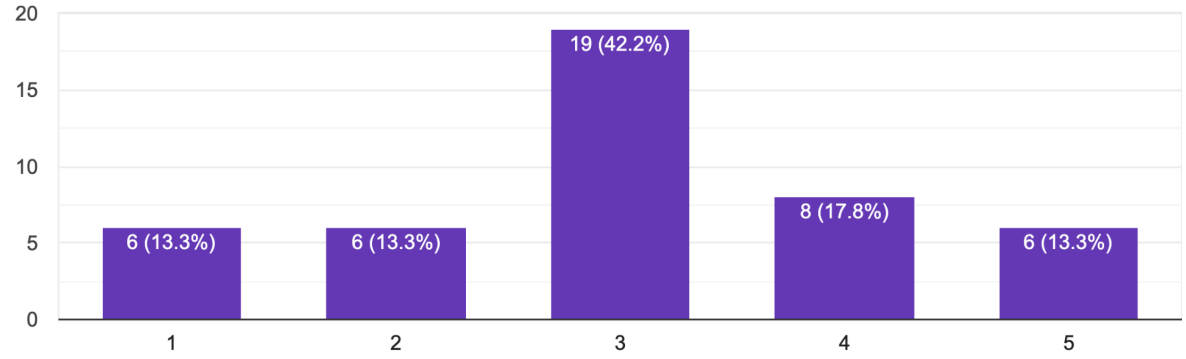
13) What involvement have you had on security of games you worked at?

45 responses



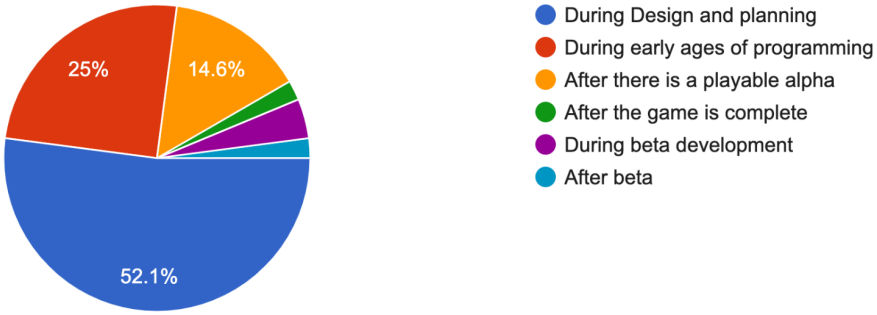
14) What involvement you think people in your role type should have?

45 responses



15) When do you think security should be started to be implemented on a videogame?

48 responses

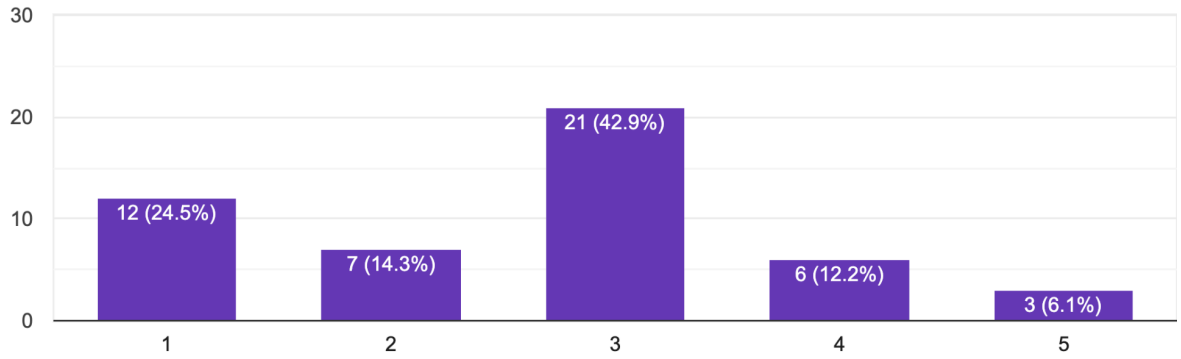


16) What is your opinion on outsourcing security in videogames? Select the estatement you agree with the most

47 responses

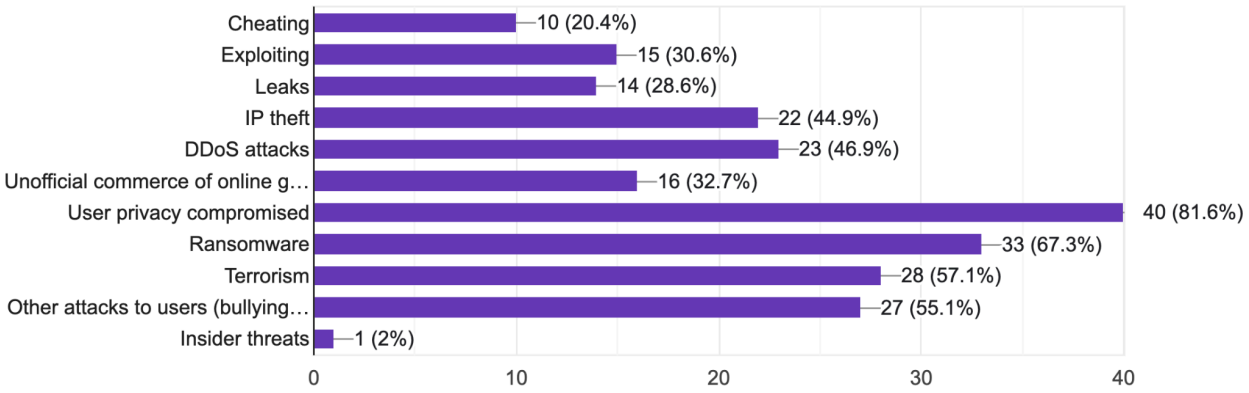
17) How much of security in videogames you think should be outsorced?

49 responses



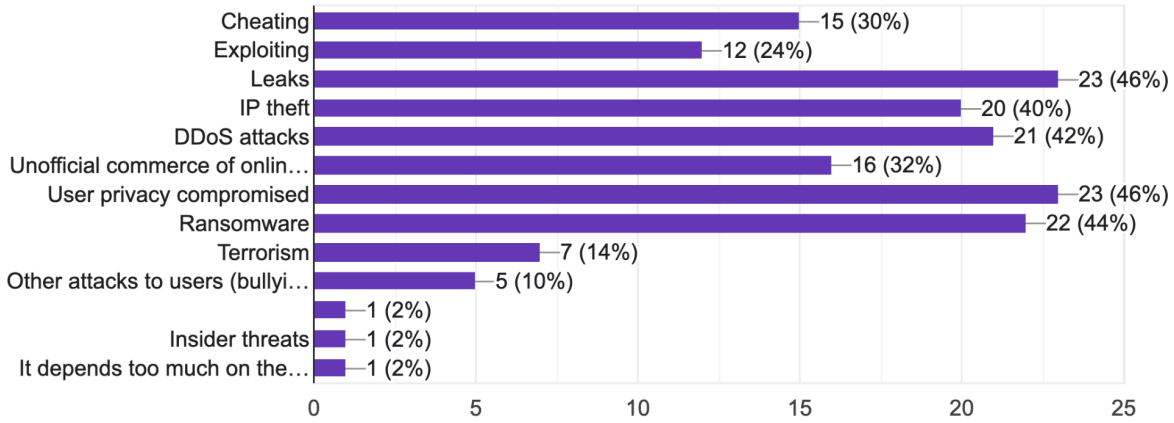
18) What types of security breaches do you think are the most dangerous in a game?

49 responses



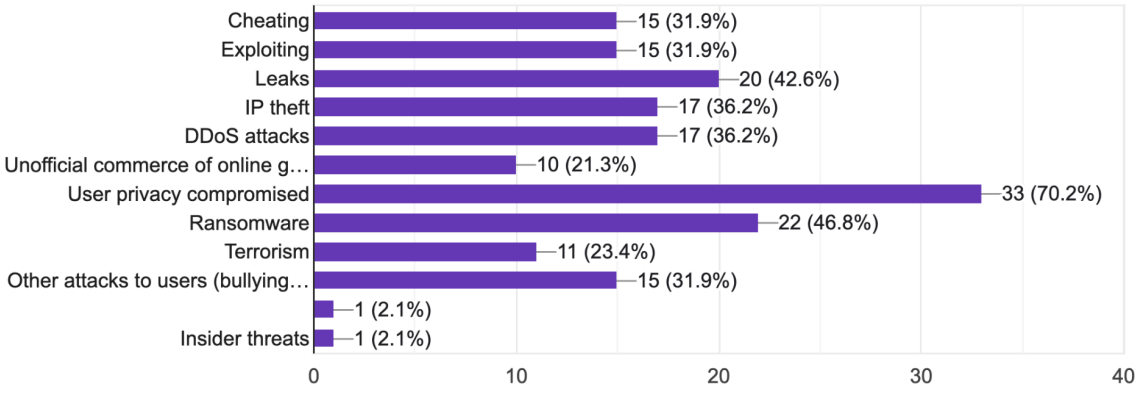
19) Which types of attacks do you think cost more money to videogame companies?(Multiple answers are accepted)

50 responses



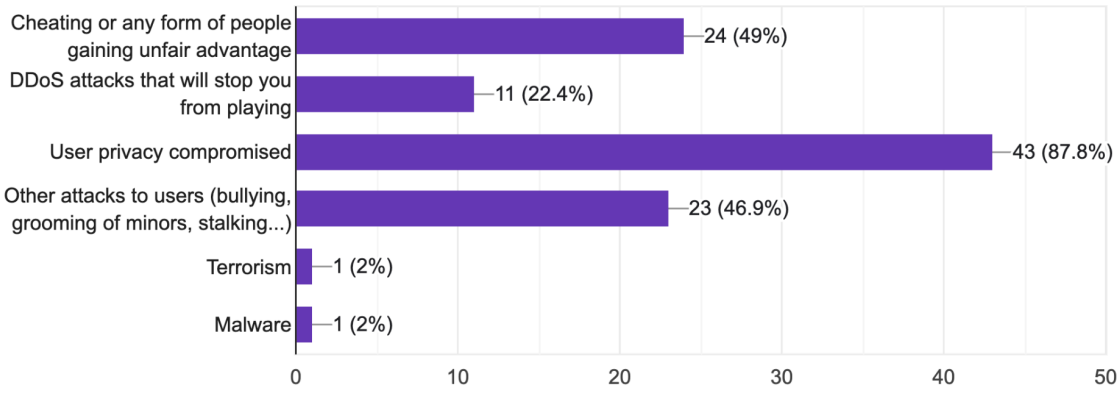
20) Which security breaches do you worry most about as a developer? (Multiple answers are accepted)

47 responses



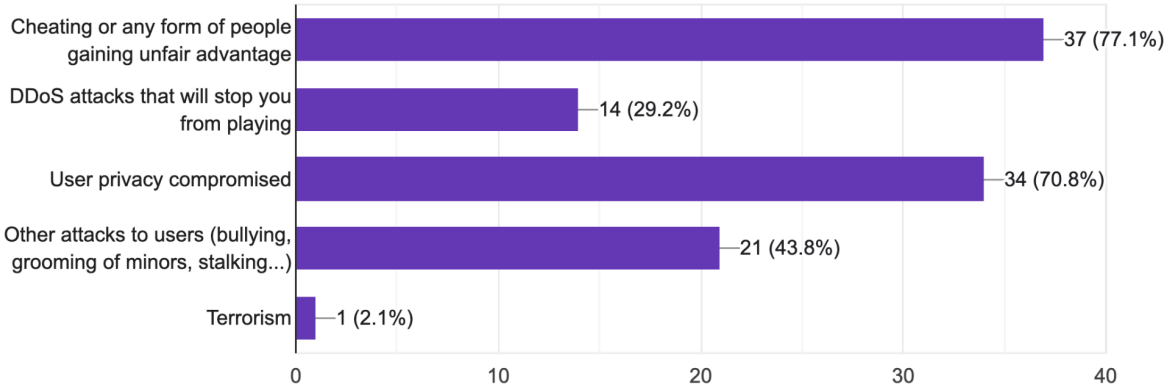
21) As a player which attacks worry you the most? (Multiple answers are accepted)

49 responses



22) Which attacks do you think worries players the most? (Multiple answers are accepted)

48 responses

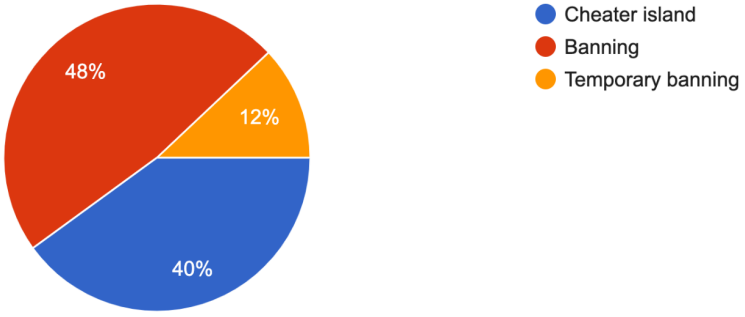


23) As a player, Would you leave a game if there were security issues?

50 responses

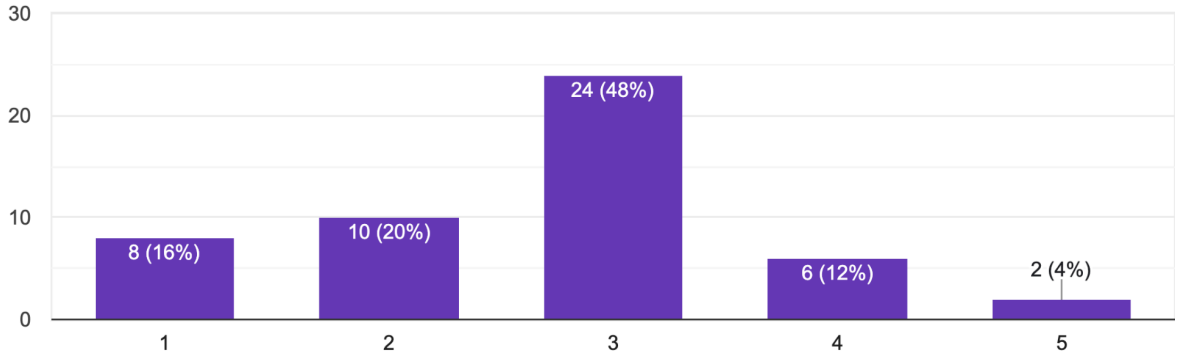
24) Of the following measures against cheating, which one do you agree the most?

50 responses



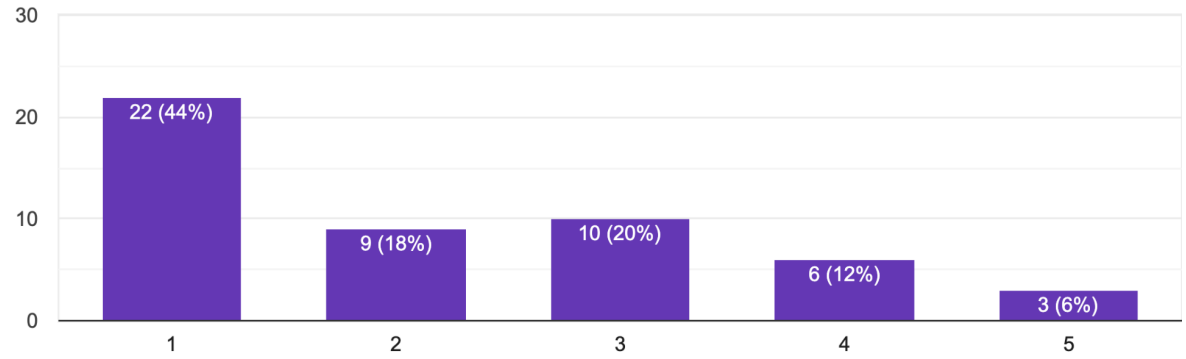
25) Do you think your personal data is safe in the games you play?

50 responses



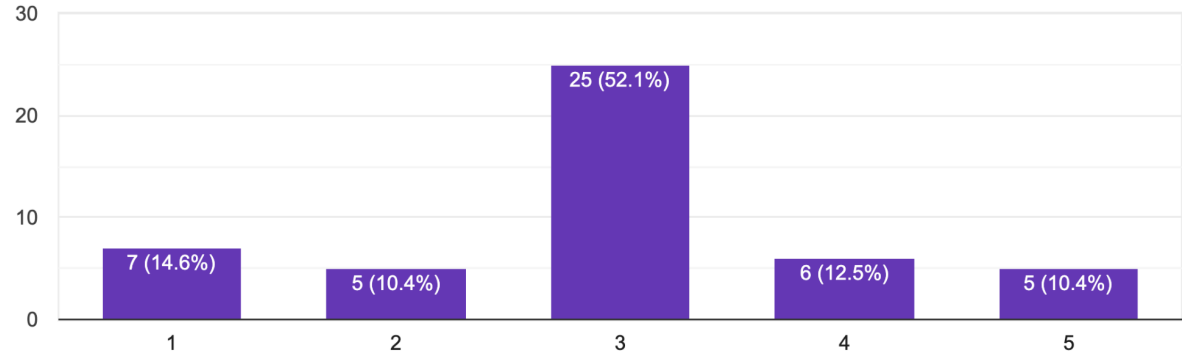
26) Have you ever read the Terms of Service of a Videogame?

50 responses



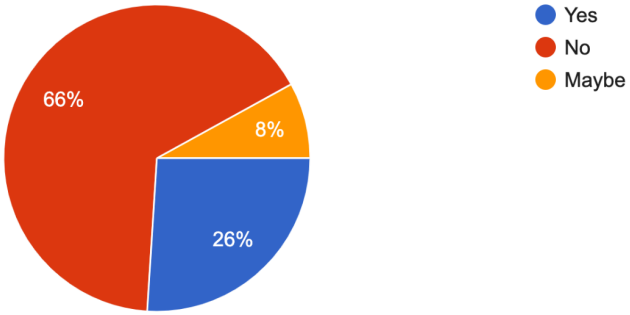
27) What is your opinion in regards of kernel based security measures?

48 responses



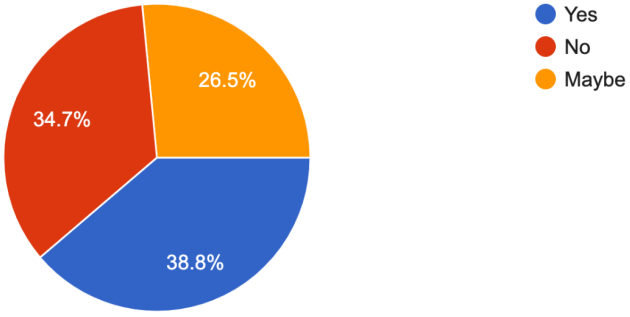
28) Have you ever cheated in a videogame?

50 responses



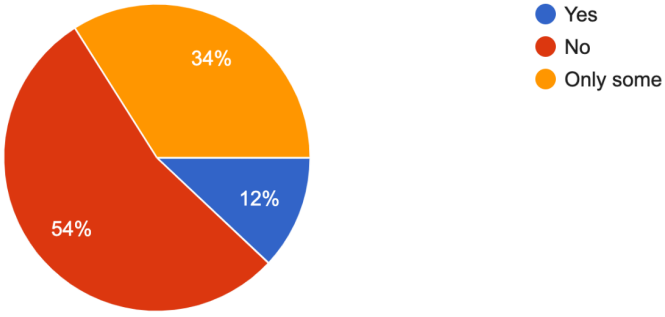
29) Do you think online videogames are safe in general?

49 responses



30) Do you feel that online videogames are a safe place for minors?

50 responses



31) Would you like to add any comment? 5 responses

I make video games as a hobby, But professionally as a career I am a web developer for a small partner relationship management company based in incentive programs and elearning

Having security thought of during the design and planning phase of a game is highly recommended as without it, it can lead to vulnerabilities being exposed and exploited, which can prove quite costly to mitigate in the future.

Too many leading questions, too many assumptions, the data will be of questionable accuracy. If we select no to an answer, it still acts as if we selected yes and asks leading questions. Also almost all of this depends on the game and isn't valid generalized.

Anti cheat systems like Vanguard is a prime example on how despite a great system can block a lot of cheating and exploits can also prevent users to play even of they aren't cheating. So quality of such softwares is important.

I have cheated, but single-player games only, back in the late 90's and early 2000's mostly.

I'll still use mods for some single-player titles, mostly to add content/features/quests.

I'll also say that I think a lot of players don't really think about security in their games, as for developers, I do think security is part of the dev-cycle early on, but much further than anti-cheat and other tools such as store/platform apps with an account system that can be secured and then the usual DRM stuff that goes into games, I don't think there's much else they can do.

It's the inherent nature of things, any system, any where, whatever its purpose, will always be tested for its weaknesses, at best, that leads to some cheating or exploiting the system, at worst, it leads to others getting compromised (by which I mean both the company and players alike, in the broadest sense of the word).