Achievement Unlocked: Let's Get Hacked!
An Empirical Study of Cybercrime in the Video Gaming Ecosystem

Anonymous submission # 1234

Additional Information

A Survey Questions

Table 1: Video game usage questions.

ID	Question	Type	Answer Options
Q1	How many hours per week do you spend playing video games approximately?	Quantitative, Single option	Free-text form (numbers only)
Q2	Do you play as a hobby or as a profession?	Quantitative, Single option	Hobby, Profession or Other
Q3	In which year did you start playing video games?	Quantitative, Single option	Free-text form (numbers only)
Q4	What is your most used video game platform in the last 12 months?	Quantitative, Single option	Nintendo console, PC, PlayStation, Smartphone/Tablet, Xbox, Other handhelds or Other
Q5a	Which operating system do you use most to play on your PC?	Quantitative, Single option	Linux, macOS, Windows, I don't know or Other
Q5b	Which operating system do you use most to play on your Smartphone/Tablet?	Quantitative, Single option	Android, iOS, I don't know or Other
Q5c	Which handheld do you use most to play?	Quantitative, Single option	Asus ROG Ally, Lenovo Legion Go, MSI Claw, Steam Deck, I don't know or Other
Q5d	Which operating system version do you use?	Quantitative, Single option	Version (free-text form) or I don't know
Q5e	Which PlayStation version do you use most to play?	Quantitative, Single option	PlayStation 5, PlayStation 4, PlayStation 3, PlayStation 2, PlayStation, I don't know or Other
Q5f	Which Xbox version do you use most to play?	Quantitative, Single option	Xbox Series, Xbox One, Xbox 360, Xbox, I don't know or Other
Q5g	Which Nintendo console do you use most to play?	Quantitative, Single option	Nintendo Switch, Nintendo 3DS, Wii U, Nintendo DS, Wii, I don't know or Other
Q6	Do you use a custom firmware that, for example, enables modding?	Quantitative, Single option	Yes or No
Q7	Please select which of the following digital game distribution platforms you use the most.	Quantitative, Single option	Apple App Store, Battle.net, Epic Games Store, GOG, Google Play Store, Microsoft Store, Nintendo eShop, Playstation Store, Steam, None or Other
Q8	Have you ever installed third-party video game modifications?	Quantitative, Single option	Yes or No
Q9	How do you ensure these modifications are safe to download and install?	Quantitative, Multi option	I use an antivirus program to check them, I upload them to VirusTotal, I search for known issues, I verify the mod author, I read reviews and comments on the modification, I do not install certain types of modifications (e.g., mods that directly change game code, like engine fixes), I do not check the security or Other
Q10	Please select which of the following game modification distribution platforms you use the most	Quantitative, Single option	Bethesda.net, CurseForge, Game Modding, MegaGames, Mod.io, ModDB, Mods Online, ModsAPK, Nexus Mods, Steam Workshop, World of Mods or Other
Q11	Which of the following gaming-related activities do you engage in?	Quantitative, Multi option	I buy in-game items from third-party websites, I take part in competitions and tournaments, I chat with other players in-game, I attend community meetings, I use community functions provided by the game distribution platforms like Steam or Other
Q12	Which of the following statements describes you best?	Quantitative, Single option	I mostly play offline with others, I mostly play offline alone, I mostly play online with others or I mostly play online alone

Table 2: Cybercrime experience questions.

ID	Question	Type	Answer Options
Q13	What measures do you take to protect yourself against cybercrime incidents in general?	Quantitative, Multi option	I use an anti-virus software, I use a firewall, I use different passwords for different accounts, I don't accept friend requests from unknown users, I don't click on unknown attachments, I don't click on unknown links, I only download files from trusted sources, I regularly update my software, I regularly update my systems, I use strong passwords, I use two-factor authentication, I don't visit websites my browser warns me to visit, I regularly change my passwords, I don't use any protection measures or Other
Q14	Have you ever been a victim in one of the following cybercrimes in the context of gaming?	Quantitative, Multi option	No, Denial of Service (Overloading a system to prevent accessibility), Fraud (Deception for financial gain), Hacking (Gaining unauthorized access), Harassment (Verbal threats or online abuse), Malware (Programs used to attack systems) , Phishing (Using fake messages to trick users), Theft (Stealing of personal belongings, including data) or Other
Q15	Please describe the cybercrime incidents you have encountered, including the context in which they occurred, as detailed as possible, including the game, platform, client, operating system, activity at the time of the incident, etc..	Qualitative	Free-text form
Q16	Please describe how you became aware of the fact that you had become a victim of cybercrime.	Qualitative	Free-text form
Q17	What impact did these incidents have on you?	Quantitative, Multi option	I lost money, I lost balance on a gaming platform, I lost virtual in-game currency, I lost skins/cases/emotes, I lost my account, I lost access to data on my system or Other
Q18	After these incidents, did you change your behavior in any way?	Qualitative	Free-text form
Q19	Have you ever been informed about security risks or a security incident related to playing video games (for example, by a digital game distribution platform or a game publisher)?	Quantitative, Single option	Yes or No
Q20	Please describe as detailed as possible how you were informed, e.g., about which incident, by whom, via which medium, the content of the notification, etc..	Qualitative	Free-text form
Q21	How often have you been a victim of video game-related cybercrimes?	Quantitative	Free-text form (numbers only)

Table 3: Demographics.

ID	Question	Type	Answer Options
Q22	What is your year of birth?	Quantitative, Single option	Select form (Prefer not to say; 1920-2010)
Q23	Please select the gender you identify with.	Quantitative, Single option	Prefer not to say, Male, Female or Non-binary/third gender
Q24	Which country do you currently live in?	Quantitative, Single option	Select form (Prefer not to say; List of countries)
Q25	What is your highest level of education?	Quantitative, Single option	Less than high school, High school or equivalent, Bachelor's degree, Master's degree, Doctoral degree (Ph.D.) or Other

B Survey Distribution

Table 4: Platforms and forums used for survey distribution.

Platform	Description	Date of Publication
GameFAQs	Website for guides and other information regarding games	23.03.25
Nexusmods	Platform for user-created modifications	23.03.25
Reddit: r/Diablo4	Subreddit for the game Diablo 4	23.03.25
Reddit: r/Dota2	Subreddit for the game DOTA 2	23.03.25
Reddit: r/Minecraft	Subreddit for the game Minecraft	23.03.25
Reddit: r/Mobilegaming	Subreddit for general topics regarding mobile gaming	23.03.25
Reddit: r/Pubg	Subreddit for the game Playerunknowns Battlegrounds	23.03.25
Reddit: r/SampleSize	Subreddit for posting surveys	23.03.25
Reddit: r/Steamscams	Subreddit help and discussion of cybercrime incidents on Steam	23.03.25
Reddit: r/Survey	Subreddit for posting and discussion of surveys	23.03.25
Steam	Biggest distribution platform for PC Games	23.03.25
The Student Room	Student community with forums for posting academic surveys	24.03.25
FAU students (Informatics department)	Mailing list of students in the IT-security department of Friedrich-Alexander University	25.03.25
GOG	Distributor of PC games	10.04.25
Discord Server: Apex Legends	Official Discord server for the game Apex Legends	16.04.25
Discord Server: Hogwarts Legacy	Official Discord server for the game Hogwarts Legacy	16.04.25
Discord Server: League of Legends	Official Discord server for the game League of Legends	16.04.25
Discord Server: PlayStation	Community Discord server for the PlayStation gaming platform by Sony	16.04.25
Discord Server: Roblox	Official Discord server for the game Roblox	16.04.25
Discord Server: Sanctuary - Diablo 4 Community	Community Discord server for the game Diablo 4	16.04.25
Discord Server: Xbox-Now	Community Discord server for the Xbox gaming platform by Microsoft	16.04.25
Discord Server: World of Warcraft	Community Discord server for the game World of Warcraft	16.04.25

Table 5: Platforms and forums which did not allow the distribution of the.

Platform	**Description**	**Reason for failed Publication**
Discord Server: Counter-Strike Discord | CSGO & CS2	Official Discord server for the games Counter-Strike: Global Offensive and Counter-Strike 2	Sharing of surveys is not allowed by the moderators on the server
Discord Server: PUBG MOBILE	Official Discord server for the game Playerunknowns Battlegrounds	Posting of links on the text channels requires a special rank on the server
Reddit: r/Apexlegends	Subreddit for the game Apex Legends	Forum moderators declined the posting of surveys that are not solely about Apex Legends
Reddit: r/Csgo	Subreddit for the game Counter-Strike: Global Offensive	Forum moderators declined the posting of surveys that are not solely about Counter Strike
Reddit: r/Gaming	Subreddit for general game topics	Forum moderators declined the posting of surveys
Reddit: r/Hogwartslegacy	Subreddit for the game Hogwartslegacy	Forum moderators declined the posting of surveys
Reddit: r/Leagueoflegends	Subreddit for the game League of Legends	Forum moderators declined the posting of surveys that are not solely about League of Legends
Reddit: r/NintendoSwitch	Subreddit for topics regarding the Switch gaming platform by Nintendo	Forum moderators declined the posting of surveys that are not solely about Nintendo Switch
Reddit: r/PCGaming	Subreddit for topics regarding PC games	Code of conduct explicitly forbids posting of surveys
Reddit: r/Playstation	Subreddit for topics regarding Playstation gaming platforms by Sony	Forum moderators declined the posting of surveys
Reddit: r/Roblox	Subreddit for the game Roblox	Forum moderators declined the posting of surveys
Reddit: r/Steam	Subreddit for topics regarding Steam	Forum moderators declined the posting of surveys
Reddit: r/Wow	Subreddit for the game World of Warcraft	Forum moderators declined the posting of surveys that are not solely about World of Warcraft
Reddit: r/Xbox	Subreddit for topics regarding Xbox gaming platforms by Microsoft	Forum moderators declined the posting of surveys

C User Report Collection Keywords

Table 6: Scraping Keywords

ID	Keywords
K1	Vulnerability
K2	Exploit
K3	Attack
K4	Steal
K5	Malicious
K6	Hacker
K7	Malware
K8	Valve
K9	Experience
K10	Security
K11	Scam
K12	Phishing
K13	Hack
K14	Account stolen
K15	Account hijacked
K16	Virus
K17	Antivirus
K18	Items stolen
K19	Steal credit card
K20	Identity theft
K21	DDoS

D User Report Collection Subforums

Table 7: URLs used for collecting user reports.

URL	# Collected Posts
https://reddit.com/r/dota2/	2261
https://reddit.com/r/leagueoflegends/	1535
https://reddit.com/r/gaming/	996
https://reddit.com/r/steam/	994
https://reddit.com/r/csgo/	792
https://reddit.com/r/minecraft/	723
https://reddit.com/r/apexlegends/	587
https://reddit.com/r/pcgaming/	576
https://reddit.com/r/diablo4/	542
https://reddit.com/r/wow/	494
https://reddit.com/r/steamscams/	419
https://reddit.com/r/roblox/	348
https://reddit.com/r/nintendoswitch/	310
https://reddit.com/r/playstation/	260
https://reddit.com/r/pubg/	86
https://reddit.com/r/xboxseriesx/	79
https://reddit.com/r/mobilegaming/	51
https://www.gog.com/forum/general_archive/	1695
https://www.gog.com/forum/general/	1541
https://www.gog.com/forum/general_de/	496
https://www.gog.com/forum/general_beta_gog_galaxy_2.0/	476
https://www.gog.com/forum/general_pl/	35
https://www.gog.com/forum/general_ru/	23
https://www.gog.com/forum/general_fr/	14
https://steamcommunity.com/discussions/forum/1	355
https://steamcommunity.com/discussions/forum/9	346
https://steamcommunity.com/discussions/forum/0	188
https://steamcommunity.com/discussions/forum/12	165
https://steamcommunity.com/discussions/forum/10	154
https://steamcommunity.com/discussions/forum/7	94
https://steamcommunity.com/discussions/forum/30	71
https://steamcommunity.com/discussions/forum/11	45
https://steamcommunity.com/discussions/forum/17	28
https://steamcommunity.com/discussions/forum/24	28
https://steamcommunity.com/discussions/forum/14	21
https://steamcommunity.com/discussions/forum/8	18
https://steamcommunity.com/discussions/forum/2	17
https://steamcommunity.com/discussions/forum/13	16
https://steamcommunity.com/discussions/forum/15	12
https://steamcommunity.com/discussions/forum/29	12
https://steamcommunity.com/discussions/forum/18	9
https://steamcommunity.com/discussions/forum/16	7
https://steamcommunity.com/discussions/forum/20	6
https://steamcommunity.com/discussions/forum/27	2
https://steamcommunity.com/discussions/forum/26	1

E User Report Filtering Prompt

LLM filtering prompt iteration 1.

You are a tool that receives an online forum post, and should decide whether it is relevant for a study on cybercrime and abuse in video games.

You will receive the data in JSON format, with attributes "id" and "text". I expect your result in the following valid JSON format without code formatting, and nothing else:
{"id": "XYZ", "result": "ABC"}
You can directly abort the rest of this prompt and return with "False" in the above format if the post has no connection to video games, video game platforms, online gaming communities, or gamer-related experiences. If not, please use the following rules to determine the significance:

Return "False" if the post is only about the following OR does not deal with video game/gaming-related content at all: - Promotional announcements, sale events, or general FAQs—even if they warn about “scams”—when no user is reporting a concrete incident of fraud or malware - Generic Q&A or tech-support threads without real evidence of cybercrime or abuse (e.g., “game won’t launch,” “driver issues,” or “antivirus flagged harmless game files” where no actual malware is demonstrated) - Game-mechanics issues: bugs, crashes, performance, balancing, matchmaking, modding questions, piracy - In-game cheating, exploits, or modding: always False unless there’s evidence of malware, phishing, or account compromise - Discussions of fictional in-game violence, sexual content, or narrative critique that do not involve cybersecurity risks - User complaints / excuses about being banned for cheating / hacking in-game without any suggestion of unauthorized hacking or phishing - Any content that is completely unrelated to cyber crime / abuse

Return "True" if the post includes at least one of the following AND is clearly within a video game/gaming-related context: - Cybercrime involving games: hacking accounts, phishing other players, exploiting game servers, in-game item scams or fraud, unauthorized third-party cheats that manipulate game code, account theft or resale, and similar malicious behavior - Malware targeting gamers: viruses, trojans, keyloggers, spyware / adware infecting gaming PCs or consoles, infected game installers, or similar - Suspicious software or security flags: questions about anticheat software being flagged as malware, DRM tools behaving like spyware, or security software mistakenly quarantining game clients—but only if there is clear suspicion of a genuine security risk rather than a routine support request - Security breaches or account compromises: data leaks of gamer credentials, credential stuffing against gaming accounts, reports of forced password resets or 2FA exploits affecting players - Unauthorized access or manipulation: unexplained in-game transactions, trades, or asset transfers that suggest someone gained illicit access to an account - Plausible evidence of security risks for games or gaming accounts (e.g., posting virus scan logs showing game files infected with malware) - Hate speech, harassment, or targeted abuse within a gaming community (e.g., slurs or threats directed at players in a gaming context)

If unclear, lean toward "True" only if there’s a real chance of security risk (from the above "true" cases). Not just cheating or security unrelated posts. Before you answer, make sure you fully understand what the author is reporting and whether it has a clear connection to cybercrime or malicious abuse in the video game context.

LLM filtering prompt iteration 2.

You are a tool to help a study about cybercrime / abuse within the gaming community. You should classify if the following text obviously deals with the gaming environment. Meaning if it is obviously about video games, the gaming scene, or gaming environment or similar. If it is, answer with YES, if not with NO.

LLM filtering prompt iteration 3.

You are a tool to help a study about cybercrime / abuse within the gaming community. You should classify if the following text obviously deals with actual performed cybercrime or abuse. Meaning, if it is obvious, that the text deals about a user report of an actual performed cybercrime / abuse. If it is, answer with YES, if not with NO.

F User Study Labeling Categories

The categories used for the user report labeling are listed as follows:

- ***Types of Cybercrime*** is used to classify the incidents described into the corresponding types of attacks.
- ***Context of Cybercrime Incidents*** is used to describe the environment in which the attacks took place. This includes the platform, the game or account, and the game mode in which the incidents occurred. If third-party modifications or websites were involved in the attacks, these are also classified.
- ***Attack Vectors*** provides information about the means used by the attackers in the incidents, including social engineering and/or technical measures. Gaming-related topics that were relevant to the attack are also listed.
- ***Incident Detection*** describes how participants became aware of the attacks, either themselves, through official notifications, or other players. If specified, the immediate response after the realization of an attack is also indicated.
- ***Effects of Cybercrime Incidents*** describes any losses incurred by participants as a result of attacks and whether these were of a monetary, emotional, digital, account-related, and/or temporary nature.
- ***Help and Support*** lists information provided by participants on whether official or community assistance was provided in resolving the incidents, or whether support was not sought or was not available.
- ***Changes in Behavior after Cybercrime Incidents*** describes any adjustments or changes in the security or gaming behavior of participants as a result of the attacks.
- ***Information about Risks*** deals with security-related communication of risks or recommendations that participants have received. These are classified according to the type of information, the source, and the medium through which the communication took place.
- ***User Awareness of Risks*** deals with the classification of cybercrime risks and protective measures and whether these are considered dangerous, acceptable, or, in the case of protective measures, effective or ineffective. Information provided by participants who demonstrate a deeper technical understanding of the attacks, as well as underestimated risk aspects, is also taken into account.

G User Report Labeling Categories

The categories used for the user study labeling are listed as follows:

- ***Type of post*** is used to differentiate between experience reports, questions, answers, recommendations and warnings.
- ***Incident type*** is used to describe the incident that the player reports on.
- ***Attack vectors/risks*** specifies the means or mechanism used to carry out the attack. These can be technical or non-technical, or relate to specific game-related elements.
- ***Impact*** describes any impact the incident had on the player, such as monetary, digital, and account-related losses, emotional damage, leaked credentials, but also boycott or reduced usage of certain games or platforms.
- ***Incident detection*** describes how players became aware of the incident, either themselves, through some kind of notifications, or other people.
- ***Emotion*** describes in what state of mind the player wrote the post or how they felt when dealing with the incident.
- ***Platform, Device, OS, Game, Game mode*** describes the context of the incident and the environment in which the incident took place.
- ***Security measures (pre-incident)*** is used to measure which security measures (traditional and gaming related) were used as protective measures before the incident happened.
- ***Security measures (post-incident)*** is used to measure which additional security measures players applied after the incident happened.
- ***Support*** describes the level of help players got from the official platform support.

H Description of User Study Categories and Codes

Table 8: Categories and codes built for qualitative analysis of survey and interview responses.

Category	**Subcategory**
Types of Cybercrime	Denial of Service Fraud Hacking Harassment Malware Phishing Theft
Context of Cybercrime Incidents	Platform Account / Game(type) Game Mode Usage of Third-party Software Usage of Third-party Websites
Attack Vectors	Social Engineering Techniques Technical Techniques Gaming-Related Features
Incident Detection	Realization by Action Realization by Official Info Realization by Notification from Other Users Immediate Reaction
Effects of Cybercrime Incidents	Financial Loss Emotional Damage Loss of Items Loss of Account No Loss
Help and Support	Official Support Community Support No Support
Changes in Behavior after Cybercrime Incidents	Changes in Security Behavior Changes in Gaming Behavior No Changes in Behavior
Information about Risks	Information Source of Information Medium of Information
User Awareness of Risks	Technical Understanding of Attacks Perception of Cybercrime as a Risk Perception of Security Measures Underestimation of Dangers

I User Reports Categories and Codes

Table 9: Type of Post

Code	Explanation
Irrelevant	The post is irrelevant for the focus of the study and was not analyzed.
Experience report	The post is a personal account of an incident involving cybercrime in the gaming environment.
Request for help	The author requests assistance and opinions regarding the incidents described and how to deal with them.
Warning / News	The post contains official news relevant to cybersecurity in the gaming environment or a specific warning about a particular type of cybercrime incident.

Table 10: Incident Type

Code	Explanation
Account Theft	Describes an unauthorized takeover of a gaming account through compromised credentials, resulting in loss of control or misuse by the legitimate user.
Cheating	Discusses the use or distribution of cheating tools or exploits that undermine fair gameplay.
DDoS	Describes a (distributed) denial-of-service attack targeting game related servers or individual players, leading to service disruption.
Fraud / Scam	Reports deceptive practices aimed at financial or digital in-game economic gain within the gaming environment.
Harassment	Describes targeted harassment of players using in-game mechanics or communication to disrupt gameplay or exploit game features, excluding general online harassment.
Infection	Reports a malware infection linked to gaming-related files, mods, cheats, or platforms.
Server crashes	Reports repeated or abnormal game server crashes suspected to be caused by malicious activity.
Theft	Describes the loss of virtual items, in-game currency, or digital assets due to unauthorized actions.
Data breach	Discusses the exposure of personal or account-related data resulting from a security breach.
Account manipulation	Reports unauthorized changes to account settings or digital items without full account control.
Bruteforce Attack	Describes repeated automated login attempts used to gain unauthorized access to gaming accounts.
Doxing	Reports the exposure or publication of a player's personal information for harassment or intimidation.
Swatting	Describes false emergency reports made to authorities targeting a player, initiated through online gaming interactions.

Table 11: Attack Vectors / Risks

Code	Explanation
CD/DVD cracks	Reports the usage of cracking software as a source of security risk.
Chat functions	Describes the usage of in-game or DDP chat functions to facilitate cybercrime.
Cheat software	Reports the use or download of cheating software that caused a security incident.
Fake friend requests	Describes deceptive friend requests used to establish trust and initiate harmful actions.
Fake game tests	Reports fake beta tests designed to lure users into downloading malicious software or revealing information.
Fake games	Describes modified games to distribute malware.
Fake giveaways	Reports fraudulent giveaways used to trick players into revealing credentials or installing malware.
Fake offers	Describes fraudulent offers related to games, digital items, accounts or services.
Fake support	Reports impersonation of trusted entities to deceive players into revealing sensitive information or performing harmful actions.
Fake tournaments	Describes fraudulent tournaments used to collect personal data, entry fees, or distribute malware.
Fake websites	Reports malicious websites imitating legitimate platforms or services.
Item trading	Reports on item trading that caused a security incident, loss of items, or other harm to the player.
Modding	Describes modding activities that introduce security risks through unverified or malicious content.
Fake group	Reports fake groups created to mislead users or facilitate cybercrime activities.
Vulnerabilities	Discusses software or system vulnerabilities that expose players to cybercrime risks.
DRM servers	Reports on incidents involving DRM servers.
Infected Download	Describes malicious software distributed through infected game files, updates, plugins, fake software or other downloads.
Leaked credentials	Reports the use or consequences of leaked credentials originating from previous breaches or leaks.
Account trading	Describes risks associated with buying or selling gaming accounts.
Fake friends	Reports impersonated or hijacked user profiles created to gain trust within gaming communities.
Betting/Gambling	Describes cybercrime incidents linked to betting or gambling activities connected to digital items.
Voting	Reports the abuse of voting to trick players into revealing account credentials.
Fake items	Describes the use of counterfeit or nonexistent virtual items to scam players into paying for worthless or fake goods.

Table 12: Impact

Code	Explanation
Account loss	Reports the permanent loss of access to a gaming account as a consequence of a cybercrime incident.
Boycott	Reports intentional avoidance or boycott of a game, platform, or service following the incident.
Financial loss	Describes monetary losses resulting from the cybercrime incident.
Game loss	Reports (supposed) loss or loss of access to purchased or owned games.
Item loss	Describes the loss of in-game items, skins, or virtual assets.
Psychological damage	Reports emotional distress, stress, or anxiety experienced by the affected player.
Reduced usage	Describes reduced engagement with games or gaming platforms after the incident.
No Impact	Explicitly states that the incident caused no noticeable harm or was stopped before it could lead to serious consequences.
Games not playable	Describes games becoming temporarily or permanently unplayable due to the incident.
Data leaked	Reports the leakage or exposure of personal or account-related data.
Game stream not watchable	Describes disruption or inaccessibility of game streams due to malicious activity.
Unauthorized usage of games	Reports unauthorized access or use of games by third parties.
System turned into bot	Describes a compromised system being used as part of a botnet or automated malicious activity.
Device locked/unusable	Reports devices being locked, disabled, or rendered unusable.
Friends targeted	Describes secondary targeting of friends or contacts following the initial incident.
Banned	Reports bans from specific platforms, games, game servers, services or communities.
Friend list removed	Describes the removal or loss of the in-game or platform-based friend list.
Steam API key loss	Describes the loss or compromise of an API key for the gaming platform Steam.
Reduced account functionality	Reports restrictions placed on an account following the incident.
Unauthorized purchases	Describes purchases made with a compromised account or service against the will of the account owner.
Account used for trading	Describes trading of (digital) items made with a compromised account or service against the will of the account owner.

Table 13: Incident Detection

Code	Explanation
Antivirus alerts	Reports that a cybercrime incident was detected through alerts generated by antivirus or security software.
Community notice	Describes detection of an incident through warnings or information shared by the gaming community.
Notification	Reports detection via automated notifications from gaming platforms or services.
Official press release	Reports that the user became aware of being affected by an incident after reading an official statement or press release.
Anomaly observed	Describes unusual behavior or irregularities noticed by the user that led to incident detection.
Analysis (by user)	Describes the user's own analysis or investigation that led to identifying the incident.

Table 14: Emotion

Code	Explanation
Threat & insecurity	Expresses feelings of fear, paranoia or helplessness related to cybercrime incidents in the gaming context, including concerns about safety, privacy, or further attacks.
Anger & irritation	Conveys anger, annoyance, frustration or disgust directed at perpetrators, platforms, or the situation resulting from the incident.
Loss & self-related distress	Expresses emotional distress related to sadness, disappointment, loss, self-blame or shame following the incident.
Positive orientation	Conveys positive emotional responses such as relief, happiness about the outcome, trust in platforms and support, or optimism, often related to coping or resolution.
Cognitive disruption	Expresses confusion, shock, or difficulty understanding the incident or its implications.

Table 15: Game Mode

Code	Explanation
Casual	Refers to games with casual or non-competitive gameplay.
Competitive	Refers to games with competitive gameplay, including ranked or performance-based modes or competition with other players.
Singleplayer	Refers to games played by a single player without interaction with others..
Multiplayer	Refers to games involving interaction with multiple players.
Offline Gaming	Refers to gaming activities conducted without a needed active Internet connection.
Online Gaming	Refers to gaming activities that requires an active Internet connection.
eSport	Refers to organized or professional competitive gaming, including e-sports tournaments or leagues.

Table 16: Security Measures (Pre-Incident)

Code	Explanation
Antivirus software	States that antivirus software was used as a preventive security measure prior to the incident.
Firewall	Reports the use of a firewall to protect the system before the incident occurred.
Notifications activated	Describes activated security or account notifications prior to the incident.
Strong / unique passwords	Describes the use of strong passwords intended to prevent unauthorized access.
Two-factor authentication	Reports that two-factor authentication was enabled prior to the incident.
VirusTotal	Reports the use of VirusTotal to check files or links as a preventive security practice.
Deauthorize Devices	Describes the prior use of device deauthorization to limit account access.
VPN	Reports the use of virtual private network (VPN) technology for gaming or gaming-related purposes.

Table 17: Security Measures (Post-Incident)

Code	Explanation
Antivirus software	Reports the use of antivirus software as a response after the cybercrime incident.
Firewall	Describes the use or adjustment of a firewall following the incident.
Notifications activated	Reports activating security or account notifications after the incident.
Strong / unique passwords	Describes adopting strong passwords following the incident.
Two-factor authentication	Reports enabling two-factor authentication after the incident.
VirusTotal	Reports using VirusTotal to analyze files or links after the incident.
Deauthorize Devices	Describes deauthorizing devices as a response to the incident.
Blocking users	Reports blocking users after the incident to prevent further contact or abuse.
Account lock (by user)	Describes the user locking their own account to prevent further unauthorized access.
Credential reset (by user)	Reports resetting login credentials, such as passwords or recovery information, after the incident.
Resetting systems (components)	Describes deleting, reinstalling, or resetting programs, games, the operating system, or other system components to resolve issues or recover from an incident.
External access disabled (by user)	Reports disabling remote access features in response to the incident.
Payment methods removed (by user)	Describes removing stored payment methods to prevent financial misuse.

Table 18: Support

Code	Explanation
Problem fully solved by support	Reports that the issue was completely resolved through support provided by the platform or service.
Problem not solved by support	Describes that support failed to resolve the reported issue.
Problem partially solved by support	Reports that support resolved the issue only partially, leaving some problems unresolved.