Digital Risks and Coping Practices among Roblox Game Creators

Qiurong Song, Rie Helene (Lindy) Hernandez, Xinning Gui, Yubo Kou
The Pennsylvania State University

Abstract

As a growing part of the creator economy, game platforms like Roblox enable millions of users to design, publish, promote, and monetize games. Alongside these opportunities, however, creators on such platforms face significant safety, privacy, and security risks. While prior work has examined online risks for content creators on social media platforms, little is known about the risk landscape of game creators. To address this gap, we interviewed 20 Roblox creators to understand how they perceive, experience, and cope with digital risks. Our analysis revealed five categories of risk—platform, production, organizational, community, and technical—that potentially compromise Roblox game creators' emotional, physical, relational, and financial safety. We also identified coping strategies such as negotiating for fairer pay and seeking community support. We conclude with recommendations for strengthening protections for game creators.

1 Introduction

Game platforms such as Roblox, Minecraft, and Fortnite Creative have increasingly become an important part of the creator economy, hosting vast numbers of games and creators [24, 43, 48]. For instance, Roblox, one of the world's most prominent game platforms, reported 111.8 million daily active users in 2025, along with 6.7 million active games and 3.1 million active game creators [13, 48]. Roblox supports creators through cycles of making, publishing, promoting, and monetizing their games via revenue-sharing business models [21, 35]. In the first half of 2025 alone, Roblox creators (RCs) collectively earned $597.94 million [48]. However, despite these opportunities, game creators also face significant safety, privacy, and security risks [9, 25, 29]. For example, media reports have documented young Roblox creators sharing experiences of exploitation, threats of dismissal and sexual harassment [9, 29]. Recent calls for action have emphasized the need to better support game creators, many of whom have been targets of harassment and doxxing [20, 27].

A growing body of research has examined the online safety of content creators, particularly on social media platforms, showing how visibility and platform dependence increase exposure to risks such as harassment, false reporting, stalking, surveillance, platform censorship, and income precarity [18, 42, 50]. These risks compromise creators' emotional, physical, relational, and financial safety [2, 42]. Game creators share these vulnerabilities, yet their work introduces additional risks. For example, game development is technically intensive and often collaborative [22, 33, 47]. Unlike social media creators, game creators must manage code, assets, and complex production pipelines, frequently in team-based environments with complex power dynamics [22, 33]. These additional complexities, coupled with the high visibility of their work, create a distinct and concerning safety landscape for game creators. Nevertheless, research on the online safety and security of game creators remains limited. While a small number of studies have touched upon some challenges for game creators, such as malicious free models, trolling, and scams [8, 22], little is known about how game creators themselves perceive a broader range of digital risks or how they cope with them.

Thus, we posed these two research questions: **(1) What digital risks do game creators perceive and experience? (2) How do game creators respond to and cope with these digital risks?** We use the term **digital risks** to refer to a broad spectrum of security, privacy, abuse, and online safety risks that game creators encounter while creating, sharing, and monetizing their work. Specifically, we examine digital risks as a two-layer phenomenon shaped by: (1) structural, platform-level conditions that create or intensify creators' exposure to harm, and (2) operational risk types—the specific digital risk events that manifest in creators' everyday practices. We include structural conditions as an integral component of the digital risk phenomenon because creators' vulnerability is not only defined by discrete incidents, but by the conditions under which these incidents become probable and consequential [31, 34]. Structural conditions like platform architectures and governance rules do not merely accompany risk; they

actively configure who is exposed, to what types of risks, and with what consequences. In this sense, structural conditions are risk-producing mechanisms, shaping the likelihood, severity, and uneven distribution of specific risks across creators. Thus, instead of treating platform structures as external background conditions, we conceptualize them as constitutive elements of the digital risk environment.

Together, these two layers of digital risks capture both the mechanisms that generate risk and the risks that creators encounter in practice. Our framing builds on Samermit et al.'s notion of **digital safety** for creators [42], which highlights digital safety as a collective outcome of risk factors and platform affordances. We extend this work by using *digital risk* to more explicitly foreground upstream structural conditions as part of the risk phenomenon itself, alongside the concrete risk events they produce within game creation. This framing helps to present a more systematic connection between structural conditions, risk events, harms, and coping strategies, which we elaborate in our findings.

To address these research questions, we used Roblox as our study site, one of the largest user-generated game (UGG) platforms [23]. Roblox is distinctive as a UGG platform as it enables players both to create and to play within the same ecosystem, lowering barriers to entry and integrating creation with monetization [21, 22]. We conducted semi-structured interviews with 20 RCs, followed by inductive thematic analysis [5]. We identified five categories of risk—platform, production, organizational, community, and technical—encompassing risks such as financial exploitation, labor scams, extortion, privacy breaches, and asset theft. Participants described coping strategies such as self-censorship, pay negotiation, community support, and privacy practices. These findings map the distinct risk landscape of UGG development, shaped by technical intensity, team precarity, and governance gaps. We conclude with recommendations for platforms, communities, policymakers, and creators to strengthen protections for creators.

This paper makes three key contributions to usable security and online safety research:

1. It offers an empirical account of how game creators on UGG platforms perceive and experience digital risks.
2. It provides conceptual insights into how risks arise from the interplay of platform infrastructures, collaborative practices, technical intensity, and creator visibility.
3. It documents game creators' coping strategies and outlines platform, community, and policy interventions to better protect and empower them.

2 Background

Roblox is a popular UGG platform with a vast global player base, particularly among young audiences [12]. 56% of users are under 16 years old, positioning Roblox as one of the leading online entertainment platforms for children [23, 48]. On average, its daily active users spent 2.4 hours per day on the platform in Q4, 2024 [51]. As of Q2 2025, Roblox reported 111.8 million daily active users, hosting 3.1 million active creators and 6.7 million active UGGs (called "experiences" by Roblox; we will use **UGG** in this paper) [1, 21, 48], created using Roblox Studio and the Lua scripting language [38]. Notably, the majority of these creators are under 24 years old($\approx$ 75%) [49], suggesting that Roblox's creator community—like its player base—skews toward a younger demographic, with teens and young adults forming the core of content creation on the platform. Importantly, UGG creation on Roblox differs from more traditional forms of user-generated content (UGC) in video games (e.g., avatars, skins). Roblox creators engage in full-cycle game development, including design, coding, testing, publishing, and ongoing maintenance, and span a wide range of professionalization, from professional developers/studios to inexperienced beginners [11, 41].

As part of the creator economy, Roblox uses a revenue-sharing model that incentivizes creators to design, publish, promote, and monetize UGGs [21, 35]. Monetization options include selling in-game products (e.g., currency, items), incorporating ad units through Roblox's immersive ads system, charging one-time fees for premium access, and more [40]. All transactions on Roblox rely on Robux, the platform's virtual currency, purchased with real money (as of the time of writing, 500 Robux costs $4.99).

Roblox employs a complex system for distributing revenue from user-created content and UGGs between game creators and the platform according to several factors, such as the revenue source (e.g., ads vs. avatar items), the type of item (e.g., 3D assets vs. classic clothing), and purchase location (e.g., in-game vs. Roblox marketplace) [37, 39]. For example, when creators sell 3D assets like avatar clothing in the Roblox Marketplace, they receive 30% of the sale while Roblox retains 70% [39]. Additionally, creators aged 13 or older who accumulate at least 30,000 Robux ($\approx$ $105 USD at the time of writing) may be eligible to convert their earned Robux into real currency through Roblox's Developer Exchange (DevEx) program [36].

3 Related Work

Digital Safety of Creators. Digital safety for creators has become an increasingly important topic within the usable security and privacy (S&P) field, with much work examining the risks faced by social media creators [18, 42, 50]. In a survey of 135 social media creators, Thomas et al. identified various online attacks, such as targeted attacks, hate speech, sexual harassment, account hacking, stalking or surveillance, and false reporting [50]. These attacks contribute to heightened digital risks for creators, which in turn undermine multiple dimensions of their safety [42] . Specifically, these risks compromise creators' emotional safety through toxic comments, bullying, trolling, and sexual harassment that fuel stress, burnout,

and mental health struggles [2, 42]. Physical safety is also at stake, with threats of surveillance, stalking, or real-world harm [42, 46, 50]. Digital risks also undermine creators' relational and community safety, damaging relationships, reputations, and the sense of security within their communities—harms that are often difficult to repair [42]. Financial safety is likewise at risk when income streams or platform access are disrupted [2, 26, 42], often compounding emotional harms as uncertainty and powerlessness intensify psychological distress [2, 42].

Researchers have identified multiple factors behind content creators' heightened digital risks. In the S&P literature, they are often conceptualized as "at-risk" users—individuals whose visibility and dependence on platforms increase their exposure to attacks and disproportionate harm [42, 53]. Key risk factors include public visibility, which exposes them to broad online audiences, shifting social norms, and platform-specific threats [42, 44]. Additional vulnerabilities are especially acute for marginalized groups, who face overlapping risks tied to gender, sexuality, disability, or content type [17, 18, 44, 52]. For instance, Uttarapong et al. noted real-time harassment of women and LGBTQ streamers on Twitch [52], while Soneji et al. showed how OnlyFans creators confront both platform precarity and the stigma of sexual content [44].

S&P scholars have also examined how content creators cope with safety risks [17, 42, 44, 50]. Strategies include using moderation and reporting tools (e.g., banning accounts, filtering harmful content, restricting interactions) [18, 42, 50], building supportive communities [42, 44], and protecting privacy to avoid potential harm [44]. Scholars further recommend measures for online creators to strengthen safety [14, 18, 42, 50] . For instance, Finska et al. propose a cybersecurity framework for influencers, advocating protective technologies and access controls to safeguard both business and personal data in the volatile social media industry [14].

Digital Risks for Game Creators. Like social media content creators, video game creators on UGG platforms such as Roblox are a growing segment of the creator economy [21, 22]. These creators not only design and build games but also publish, promote, and monetize them within complicated platform ecosystems [21, 22]. Revenue-sharing models of UGG platforms incentivize heavy labor investment, motivating creators to devote substantial time and effort [22, 45]. To succeed, creators often employ various strategies to sustain player engagement, retain users, and secure financial rewards [22, 45].

Unlike traditional social media platforms, game development require technically intensive work, including coding game logic, integrating assets, and managing server-side systems—tasks that can pose substantial challenges [33, 47]. For example, Politowski et al. identified various risks faced by game creators, including technical issues (e.g., code or asset management) and team coordination breakdown [33]. Additionally, cybersecurity threats like hacking and malware can disrupt development, damage reputations, and undermine revenue [47].

In the UGG context, these risks are embedded within a complex sociotechnical ecosystem that includes interactive real-time player engagement, intricate in-game economies, and platform-specific governance systems [8, 21, 55]. Kou et al. noted that inexperienced Roblox creators encounter malicious free models that spread viruses, steal data, or harm players, as well as risks from collaborating with bad actors [22]. Choi et al., through interviews with 18 teenage Roblox creators, touched on risks like scams and trolling, underscoring the harmful impact on child creators [8]. While these studies touch on some security concerns, we still lack a comprehensive understanding of how creators themselves perceive the breadth of digital risks they face and the strategies they develop to navigate them. This study fills this gap by examining creators' perspectives on digital risks and their coping strategies for online safety.

4 Methods

To understand how game creators perceive, experience and cope with digital risks on Roblox, we conducted a semi-structured interview study with 20 RCs from diverse backgrounds. We then performed a thematic analysis of the interview data. The study received approval from our university's Institutional Review Board (IRB) prior to data collection.

4.1 Data Collection

Participant recruitment took place between February and April 2024 using online, offline, and snowball sampling methods [28] to reach a diverse group of Roblox creators. Online outreach targeted three Reddit communities ('r/RobloxDevelopers,' 'r/RobloxScripters,' and 'r/RobloxStudio'), five Discord servers ('Learn Roblox,' 'DevForum Community Server,' 'Roblox Scripters,' 'Simply Scripting,' and 'HiddenDevs'), and six university mailing lists and organizations. All outreach was conducted with prior approval from moderators, staff, and organization officers. Offline recruitment included distributing flyers in local establishments such as school buildings. We also used personal network outreach and snowball sampling from initial participants to recruit further. Recruitment messages detailed the study's purpose, eligibility, compensation, and included a link to a screener survey. The survey both confirmed eligibility and ensured sample diversity, asking about Roblox experience (e.g., time as player/creator, creator role, development hours, earnings, and financial reliance on Roblox). Eligibility required participants to be U.S.-based, proficient in English, have created a Roblox game at any point, and be at least 13 years old. For minors (13–17), it was specified that parental permission was required; scheduling was arranged through the guardian, who remained present (i.e., in the same room) during the interview.

Consistent with Braun and Clarke [6], we view meaning as produced through interpretive engagement rather than passively "discovered" within data. Accordingly, decisions about how many data items to include—and when to stop collecting them—are inherently situated, contingent on the developing analysis rather than predetermined numerical thresholds. We adopted a judgement-based stopping rule guided by the principles of analytic sufficiency and information power [6], continuing recruitment until additional interviews offered primarily confirmatory rather than novel insights. At that point, we determined the dataset was sufficiently rich to address our analytic aims. In total, 20 RCs participated in our interview study; their demographics and creator information are provided in Appendix A. Only one participant was a minor (P11, age 17). The median age was 19, with an average of 20.1, consistent with Roblox player demographics in 2024 [10]. Participants represented diverse racial backgrounds and professional roles, such as independent developers (n=7), studio team members (n=7), and studio owners (n=5). Their engagement levels ranged from full-time game development (n=7) to part-time (n=4) or hobbyist participation (n=9). Of the participants, four identified as female and fifteen as male.

Semi-structured interviews were conducted via Zoom between February 19 and April 30, 2024, lasting 40-82 minutes (average one hour). One author conducted all interviews, which focused on participants' experiences with Roblox game developing. Questions explored how participants perceive challenges in making and publishing games as a Roblox creator (e.g., *"What was the most challenging thing when you first started game development?"*), as well as strategies for coping with these challenges (e.g., *"If you see your game becoming less popular, what can you do to increase its popularity?"*). We also used follow-up probes to surface how participants connected these experiences to digital risk. These probes encouraged elaboration on security and safety concerns, interpersonal dynamics, and platform governance issues (e.g., *"Can you tell me why some developers prefer to stay anonymous?"*; *"You mentioned there are some bad or dangerous people—what makes them bad or dangerous?"*). Such follow-ups helped illuminate how creators perceive and experience a variety of digital risks relevant to their work and well-being. All interviews were conducted in English and recorded (audio and video) with written and verbal consent. Recordings were later transcribed for analysis, and each participant received a $20 Amazon gift card as compensation.

4.2 Data Analysis

Two researchers performed an inductive, reflexive thematic analysis (RTA) [5] of the interview transcripts. As part of RTA's familiarization phase, both researchers first read all transcripts individually to develop initial analytic impressions, then met to discuss our impressions and agreed that participants provided rich reflections on digital risks faced by RCs. Two authors then independently conducted an initial round of open, inductive coding across all transcripts on Google spreadsheet—without referring to each other's codes—resulting in 243 preliminary codes after discussing and resolving disagreements.

In a second round's coding, the two authors collaboratively reviewed these codes to develop higher-level codes/categories and revisit selected excerpts to refine meaning. Through iterative discussions, the research team synthesized these categories into overarching themes while continuously referring back to the raw data to ensure analytic grounding. Because RTA emphasizes reflexive engagement rather than mechanical recoding with a finalized codebook [4, 5, 7], we did not recode all transcripts line-by-line, but instead refined codes and themes through iterative interpretation. This process resulted in five themes: platform risks, production risks, organizational risks, community risks, and technical risks, along with the coping strategies creators used to navigate each.

4.3 Positionality Statement

We recognize that our backgrounds shape how we interpret participants' experiences and the meanings we construct from the data. All team members have great familiarity with Roblox—either through prior research or personal play—but none are active Roblox creators. This positioned us with a blend of contextual knowledge and analytical distance. Our familiarity helped us understand platform norms, terminology, and creator workflows, while our lack of direct development experience required us to attend closely to participants' explanations of technical, economic, and community dynamics.

5 Findings

This section presents digital risks that creators perceived and experienced on Roblox and how they defended against those risks. As our analysis addresses both structural and platform-level conditions that shape creators' exposure to harm and the specific risk events that occur in their everyday practices, each subsection is organized accordingly. We first describe the structural conditions that create or intensify exposure to harm, then outline the specific risk events and their potential harms that occur in creators' everyday practices, and finally detail the coping strategies that creators employed in response.

5.1 Platform Risks

Roblox operates as a tightly interconnected ecosystem—with its own technical architecture, platform regulation and moderation, and monetization systems, which means that RCs are dependent on how the platform enforces policies and controls financial rewards. This dependence heightens vulnerability by exposing creators to risks shaped by platform governance. RCs emphasized two core structural conditions: (1) an opaque

and unpredictable moderation system and (2) an exploitative monetization structure. These structural conditions give rise to several specific risks related to platform governance, including moderation-related creation instability and financial exploitation.

Opaque and Unpredictable Moderation System. RCs described moderation as a powerful yet inconsistent gatekeeper of their creative work. Content is frequently flagged, removed, or penalized without clear justification, and the appeal process is slow, automated, or unresponsive. Because enforcement lacks transparency, creators cannot reliably understand what rules they must follow or how to prevent violations. As a result, decisions about what to publish, how to design assets, and whether their games and in-game elements will remain on the platform are shaped by uncertainty, creating ongoing instability in their game development practices.

Exploitative Monetization Structure. RCs also reported that Roblox tightly controls creator earnings through centralized revenue deductions and restrictions on accessing payouts. This system grants Roblox broad financial power over how creators are compensated and when they can withdraw income. Even when RCs comply with platform rules, they must navigate multiple layers of fees and withdrawal barriers that disproportionately capture value for the platform and limit their ability to convert creative labor into real-world income.

5.1.1 Moderation-Related Creation Instability

Moderation-related creation instability refers to the chronic uncertainty RCs face regarding whether their games, assets, or accounts will remain accessible or be removed without meaningful recourse. Many RCs shared that because moderation decisions are often unpredictable, overly sensitive, and difficult to appeal, creators cannot reliably anticipate what will be flagged or why. This instability exposes them to the loss of creative work, income disruptions, and ongoing emotional stress, as enforcement actions can occur suddenly and without clear justification. For example, P4 described the frustration of getting unwarranted flags, emphasizing the severity of consequences for minor infractions:

> *My account got taken down for three days because I uploaded a picture of a dollar bill. [. . .] The fact that they have a system that can just cut off my livelihood like that and there's nothing I can do is very scary. [P4]*

Similarly, P12 shared a pattern of game assets—digital resources used in game development and serving as the building blocks of a game, such as images, 3D models, or music—being flagged despite not violating any platform policies, expressing concern over the cumulative risk of account termination: *"If I got so many of those violations, it would terminate my account, I would lose everything."*

Many RCs like P4 and P12 reported that content was often flagged or removed without clear justification. This unpredictability disrupted their creative process, risked account bans, and threatened accumulated work and income. P4 described the algorithmic enforcement of content rules as inconsistent and irrational, with moderation decisions that seemed arbitrary or unjustified. As a result, RCs expressed frustration and anxiety about the opaque and unstable nature of the moderation system, underscoring its impact on their livelihoods. Over time, this anxiety became a chronic burden—an unavoidable part of sustaining work on the platform.

Furthermore, appeals often received delayed or dismissive responses, leaving creators without guidance on how to avoid future infractions. For example, P4 shared their experience appealing a three-day ban, " *Instead of addressing my concerns, [. . .] when they got back to me, it's already over. So it doesn't matter. [. . .] you can't do anything because it's all part of the automation.*" P4 described the appeal process as delayed, impersonal, and opaque. Rather than providing meaningful feedback or resolution, the moderation and appeal system reinforced a sense of powerlessness—leaving creators unsure how to contest violations, identify their causes, or avoid future penalties.

5.1.2 Financial Exploitation

Financial exploitation refers to the platform's unfair extraction of economic value from RCs' creative labor, including mandatory revenue deductions, nonrefundable removal of paid uploads, and high thresholds for converting earnings into real-world income. Financial exploitation makes it uncertain whether creators' labor will translate into meaningful financial reward. As a result, RCs experience tangible harms such as lost revenue, wasted investment in assets, and restricted access to real-world compensation—ultimately intensifying their economic precarity within the platform ecosystem.

Multi-Layered Deductions and Profit Loss. Creators expressed frustration with how their earnings are repeatedly reduced through multiple layers of fees:

> *The dev side [of Roblox] is not that great. [. . .] especially for making money, Roblox takes a 30% cut from all Robux a game makes. [. . .] And when you try to DevEx it out, which is just turning Roblox into like USD, they take another percentage out, and then you have to pay tax on that percentage. [P9]*

P9 described a multi-step loss of income: an initial platform cut followed by reductions during Robux-to-USD conversion. The payout structure demonstrated how Roblox centralizes financial control and restricts creators' autonomy over their earnings. Creators must navigate a tightly controlled economic system in which significant portions of their potential income are captured by the platform itself.

Lack of Refund or Compensation Mechanisms. Beyond cuts to revenue, some creators also noted that the platform removes paid assets (e.g., audio files) without offering refunds:

> *Every audio file that you upload costs 100 Robux [. . .] What [annoys me] is that when they take the copyright, they take down your content, but they wouldn't [reimburse] you for the Robux that you spent. So I ended up wasting about a thousand or so Robux on audio. [P17]*

When content that a creator uploads is later removed—regardless of having passed initial approval—it creates a "lose-lose" situation: creators lose both the asset itself and the money they spent to upload it. The absence of reimbursement heightens financial risk and further limits creators' autonomy over their work and earnings. This lack of control over both their content and its economic value reinforces a sense of vulnerability within the platform's ecosystem.

High Barrier to Accessing Earnings. In addition to repeated platform deductions, Roblox imposes a high threshold for creators to convert Robux into real-world money. Even as they contribute creative labor to the platform, many are effectively locked out of meaningful financial return: "*I never cashed out because [. . .] you need at least 30,000 Robux to cash out. And I never amassed that much over eight years."* In this quote, P7 highlighted how the platform's payout model structurally excludes many creators from monetizing their work. The high minimum threshold limits financial access, meaning that smaller or less-established creators can struggle to financially benefit from their contributions**.**

5.1.3 Defense

In response to unpredictable moderation, censorship, and financial exploitation, RCs develop their own protective strategies. These defenses reflect a broader awareness of structural precarity and a desire to preserve both their work and livelihood within an often unstable platform environment.

Use of Secondary Accounts to Avoid Risk Exposure. To safeguard main accounts—often tied to years of accumulated work, status, and relationships—some RCs upload assets through alternate accounts. As P14 explained: *"I created a placeholder account that would upload the shirts I made and the pants, because I felt like it wasn't worth the risk to use my main account."* This minimizes the risk of moderation penalties affecting their primary accounts and serves as a strategy to protect both their creative output and financial security.

Self-Censorship. Creators whose income relies on Roblox consciously self-regulate their behavior to avoid violations. P7 described being highly cautious:

> *I'm concerned about being banned because it's my whole livelihood. I would never do anything to violate the terms of service. I think I have very good concepts of [the] terms of service and what can bring about a ban or a strike. [P7]*

This shows how creators internalize platform rules and adjust their practices to avoid moderation and sustain livelihood.

Seeking Help From Customer Support (CS). Creators reach out Roblox's CS regarding unfair moderation. For example, P14 shared a generally positive view: *"They try to get back as soon as possible."* While support may not always reverse moderation actions, as P14 noted, *"when it comes to why you got banned, [. . .], there's not much you can do in that instance [. . .] You can't really refute it"* it still serves as a channel for communication with the platform, offering some degree of engagement and accountability.

Financial Workarounds to Avoid Fees. To avoid Roblox's steep commission, RCs sometimes rely on group payouts; as P13 noted, "*the way to get around that would be in group payouts.*" In this arrangement, clients commission RCs for work (e.g., clothing, game assets) and pay them from a group's existing Robux funds. Because *"group payouts aren't taxed [by Roblox] "* in the same way as marketplace sales, this method allows creators to retain more of their earnings. It reflects a practical adaptation to the platform's financial constraints.

5.2 Production Risks

Game production refers to how creators design, build, commercialize, and maintain games on Roblox. Game production is shaped by structural conditions that configure creators' vulnerability to production-related risks. These structural conditions include: (1) the precarity of game development and success, (2) an informal labor market, and (3) limited legal and IP protections. These conditions give rise to several specific risks related to game production, including project failure or abandonment, game clone, labor scams, and legal exposure.

Precarity of Game Development and Success. Roblox game creation and subsequent commercial success occur under unstable and fragile conditions [32, 54]. Projects are vulnerable to external disruptions—including legal shifts, market volatility, limited resources, or the demands of continuous updates—RCs cannot reliably predict whether their efforts will result in a completed or sustainable game, which might cause abandoned work, wasted resources, financial loss, and emotional strain. Even when games are completed, some RCs noted that their commercial success is equally unstable. Player attention fluctuates quickly, revenue can sharply decline, and independent RCs lack the financial safety nets available to larger studios.

Moreover, sustaining a successful game requires continuous updates and new content, introducing an additional layer of precarity. As P7 explained:

> *[I have to go to school] and I couldn't devote a lot of my time to the games. [When a game becomes popular,] I like to look at it like a fire. And once the*

fire is going, you need to keep adding stuff to it or the fire will eventually die. [P7]

Thus, even success generates risk, as maintaining popularity demands ongoing labor that some RCs—especially young or part-time developers—may struggle to sustain. Combined, the instabilities of development and success threaten RCs' ability to maintain both their creative work and their financial security.

Informal Labor Market. Many RCs in our data (e.g., P9, P15, P18) noted that game production commonly relies on informal agreements with no contracts or enforceable protections. Without standardized hiring practices, formal project ownership, or platform-supported contracting tools, most teams rely on personal trust to coordinate labor, payment, and roles. This informality shapes how work is exchanged, how collaborators are recruited, and how commitments are enforced across the development ecosystem. For example, such informal labor market can potentially leave creators—especially youth—vulnerable to deceptive collaborators who promise revenue shares or wages but never pay, potentially contributes to wasted labor, stalled projects, and loss of trust among RCs.

Limited Legal and IP Protections. Some RCs noted that Roblox lacks clear or effective procedures for handling IP and other legal dispute. Additionally, Platform policies can be difficult to interpret, and creators often lack legal knowledge or access to formal representation. As a result, decisions about ownership, originality, and infringement are shaped by inconsistent moderation and creators' own interpretations of ambiguous rules rather than by formal adjudication. These conditions leave RCs exposed to lawsuits from companies and with little recourse against others who steal or clone their work. Navigating legal conflicts can be especially difficult for young creators, who are perceived as risky or unprofessional business partners.

5.2.1 Project Failure or Abandonment

Project failure or abandonment refers to the premature discontinuation of a game's development, release, commercialization, or maintenance before reaching its intended goals. On Roblox, projects are frequently abandoned under unstable development conditions. Burnout, inadequate planning, legal or market disruptions, and lack of funding often stall game production and success, potentially exposing creators to harms such as with financial instability and emotional stress. P3 reflected on how common it is for games to be abandoned before release:

> *I've worked on [. . .] about 80 [games] that haven't [been released]. [. . .] Usually either developers get burned out because you don't have community feedback before you initially release, they run out of funding to pay staff to work, or the initial plan for the game just doesn't work. [P3]*

Similarly, P17 described a project that was more than halfway complete before their team realized they lacked the funds to finish it and had to abandon it. These accounts highlight the pressures that contribute to the fragility of Roblox game creation. Many RCs emphasized the precarity of game creation, where the absence of formal planning, reliable funding, or long-term support means that even promising projects can be abandoned. Many games are built on fragile scaffolding, easily dismantled by the weight of practical limitations.

Even when a game is completed, its success remains uncertain: market performance may be short-lived, player interest often fades quickly, and income can fluctuate drastically from month to month. For example, P4 described the volatility of game success on the platform:

> *You can make a game that does amazingly well and starts making you $500,000 a month, and then the next month it's dead. [. . .] That's part of the constant struggle to keep a full-time job is that the games die and your company isn't always going to have money. [P4]*

Creators described how games can quickly succeed and stagnate, making long-term planning difficult and threatening income sustainability. Unlike professional studios backed by investors, many RCs work independently and without financial safety nets. As a result, they are vulnerable to sudden shifts in trends, revenue declines, or broader industry challenges, such as a shrinking job market in game development.

5.2.2 Game Clone

Game cloning refers to the unauthorized replication or imitation of a game's style, mechanics, aesthetics, branding, or core design elements to capitalize on its success. On Roblox, limited IP protections and weak platform enforcement leave RCs vulnerable to such cloning. These risks can lead to harms such as loss of originality, erosion of reputation, and diversion of revenue.

P8 shared their friend's experience: *"[They] created a Star Wars [game], and some people took it and tried to make their own spin-off version of it, which happens a lot."* Despite how common these cases are, Roblox often fails to intervene, leaving creators with little recourse to protect their work. For example:

> *When people were taking my style and making a cash grab, [Roblox] shut me down really quick. I laid out a whole infographic showing that the style was copying mine, [but] their legal agent [said] they don't resemble each other at all. [. . .] It just seems like they're turning a blind eye to it because taking down games would lose them revenue. [P7]*

Despite providing detailed evidence showing the resemblance between their work and another game, Roblox denied any similarity. This left P7 feeling helpless and frustrated, especially since the platform's Terms of Service appear to prohibit such stylistic copying. P7 believed that because imitation games can still generate revenue for the platform, they are often left untouched, even if they harm original creators. P7 noted that this was not an isolated incident, but a recurring issue that undermines RCs' financial security.

5.2.3 Labor Scams

Labor scams refer to deceptive recruitment or collaboration arrangements in which creators provide work without receiving promised payment or revenue sharing. Roblox's informal labor market—where collaborations often lack contracts or enforceable agreements—makes such scams a prevalent risk. Scammers pose as employers or collaborators, soliciting labor through promises that never materialize, leaving RCs—especially those with limited experience or legal knowledge—vulnerable to unpaid work, wasted time, and stalled production. For example:

> *There are a decent number of scammers that will just get someone to do work for them, not pay, and block them. [. . .] Someone tried to [scam me] a few years ago, [. . .] they just [talk about] a bunch of stuff in a game that sounds super fun to work on, which is perfect for me. And I was almost about to accept that. [P18]*

P18 highlighted how scammers take advantage of RCs' enthusiasm and inexperience—often luring them with exciting project ideas, only to disappear after receiving free labor. These encounters create an unsafe working environment, leading to wasted time, unpaid work, and even a loss of trust in collaborative opportunities.

P9 further noted that younger RCs are particularly vulnerable to scams due to their inexperience and lack of protection:

> *[For] developers being scammed, there's no contracts. It's mostly just a word of mouth thing. Like, hey, I'll pay you 20% until the game makes a lot of money and they dip. [. . .] I think younger people just fall for scams like that or trust blindly. [P9]*

P9 emphasized that younger creators often trust too easily and lack safeguards like contracts, making them easy targets for bad actors who exploit their labor and disappear without paying. This highlighted the broader risks of unregulated, informal labor within Roblox's ecosystem.

5.2.4 Legal Exposure

Legal exposure refers to the vulnerability RCs face to legal disputes in an environment with limited formal protections or clear processes for resolving conflicts. Without accessible support or guidance, creators may become entangled in lawsuits or contractual disputes, facing potential harms like financial loss, reputational damage, and prolonged stress. One prominent issue centers on IP disputes. P4 explained how high-revenue Roblox games can attract lawsuits from large companies who feel their IP is being infringed:

> *Most big companies want money, [. . .] so they wanted to sue because they saw that they were losing six figures of revenue a year. They came to the agreement eventually, but because Roblox is very "wild west"—it's very undeveloped—there's no expected procedures. These companies tend to go to lawsuits and legal action before going 'Wait, maybe we can partner with them', especially because a lot of us [. . .] are young and they're kind of skeptical to work with young people. [P4]*

P4 perceived that Roblox lacks clear procedures around IP protection and related legal disputes. This underdeveloped legal framework leaves creators—particularly younger ones—exposed to financial loss and legal threats. In cases where large companies believe a Roblox game is infringing on their IP and costing them revenue, the absence of structured dispute-resolution options often leads them to pursue aggressive legal action rather than collaboration.

Beyond IP disputes, creators also face contractual and liability risks stemming from Roblox's largely informal labor practices. For example:

> *[Kids under 18] can't be legally bound without their guardians' permission. [. . .] Sometimes owners aren't trustworthy [. . .] owners have to establish a company, hire lawyers, and a lot of people don't want to do that. It's expensive and time-consuming, and they'd rather just take the legal risk. [P15]*

Contracts for creators under 18 typically require guardian consent, yet many project owners avoid this step to sidestep the cost and effort of establishing a legal entity. This "under-the-table" approach exposes creators' work to disputes and leaves them with little legal recourse if conflicts arise.

5.2.5 Defense

Despite the many operational risks faced by young RCs, participants described various forms of informal resilience.

Community Support. Creators emphasized the collaborative spirit within the RC community. Despite market competition, peer support is readily available for technical help and social connection. As P2 noted, *"If you have a question or a problem, you just reach out to someone and they will help you within five minutes. Everyone's super friendly, and even though our games are competing, people don't take it*

that way." They emphasized that while competition exists, the sense of community remains strong, providing valuable support that helps them overcome challenges in game development.

Player-Centered Design. Some RCs defend against financial instability by focusing on long-term player satisfaction. They emphasized balancing monetization with player experience (PX), investing heavily in playtesting and iteration. For example, P2 noted:

> *[Make] sure that the players actually get some value out of the game and not just monetization, actually enjoying the game [. . .] You don't want to overmonetize and be annoying to the player, constantly bombard them, but you don't want to undermonetize and undervalue your game. So you have to find a perfect balance between that. [P2]*

P3 echoed this emphasis on player experience and testing: *"The number one priority when developing is getting stuff playable so I'm able to test it to make sure it's fun before sinking more time into it."* These accounts show that sustainable success, in the eyes of some RCs, comes from designing with players in mind—building engaging experiences that naturally support monetization rather than relying on aggressive revenue tactics.

Signing Their Work. Some participants attempt to protect their originality and deter imitation by signing their work with distinct styles. For example, P15 noted, *"there was very little I could do [to protect my art] besides signing my artwork and using a very distinct style."*

Community Vetting System. To protect against labor scams, Some RCs described informal, community-led vetting networks, where members share information on known scammers and suspicious offers: *"There's a community of scam investigators, and a bunch of different Discord servers have a lot of ways to regulate the marketplace for that. But it's just better to be safe than sorry." [P18].* These crowdsourced systems act as grassroots safeguards in an otherwise unregulated marketplace, reflecting RCs' collective efforts to fight scams and help with platform security.

Building Trust in Collaboration. Collaboration in Roblox often lacks formal contracts, making trust a crucial defense mechanism. Some creators described investing time in personal relationships as a way to gauge reliability and reduce interpersonal risk. For example, P11 noted, *"To know that you can trust a person on Roblox, a lot of times means just getting to know them as a friend on a personal level. I've made some great online friends on Roblox [that I] might consider a real friend 'cause I've just known them for so long."*

Together, these strategies show how creators use both community-based checks and personal trust-building to create safer and more dependable collaborations in an otherwise precarious environment.

5.3 Organizational Risks

Due to the complexities of game development, which requires a variety of skill sets, RCs often collaborate in teams to build larger or more complex games, situating their work within an organizational context. This organizational mode of development is shaped by structural conditions that configure creators' vulnerability to organizational risks. RCs highlighted two main structural conditions that underpin organizational risks: (1) unstructured financial control and (2) informal labor market. These conditions give rise to several specific risks within teams, including embezzlement, labor exploitation, team instability, and interpersonal conflict.

Unstructured Financial Control. Several RCs emphasized that many Roblox development teams operate without well-structured and formal financial governance or platform-supported safeguards. For example, payment arrangements are typically based on informal, verbal agreements and distributed through platform-owned "group funds" that are fully controlled by team owners. Without contracts, shared oversight, or transparent financial mechanisms, creators depend on personal trust to receive compensation. This lack of structure leaves room for unilateral control of funds, mismanagement, and nonpayment. For example:

> *[There is a] lack of something [like] a contract where it's written out what we're going to do, how it's going to work. All of it's mostly just word of mouth. Like, hey, you can work for a game And we get like 20% but that's just words. If they take, you can't do anything about it. Roblox supports their devs very little in that aspect of it. [P9]*

P9 noted that informal payment agreements left RCs vulnerable to unstable or withheld payments. Without binding agreements, expectations are vague and disputes are difficult to resolve. This account pointed to the lack of platform-level safeguards as a source of mistrust, reduced control over earnings, and heightened financial risk.

Informal Labor Arrangement. Roblox development teams commonly operate within an informal labor arrangement that lacks legal protections, employment standards, enforceable agreements, and mechanisms for accountability. RCs—including minors—are treated as independent contractors without guarantees of fair pay, stable working conditions, or continued participation on a project. Responsibilities, expectations, and communication norms are often negotiated ad hoc and shaped by personal discretion rather than institutionalized procedures. This arrangement disproportionately affects younger creators, who often lack bargaining power or legal recourse. In the absence of organizational scaffolding such as contracts, HR processes, or formal management structures, collaboration on Roblox becomes fragile and uneven, creating vulnerabilities for RCs—particularly when projects involve multiple contributors.

5.3.1 Embezzlement Risk

Embezzlement risk refers to the possibility that project leaders can unilaterally appropriate or misuse shared group funds due to the absence of structured financial governance. Because Roblox's payout system grants group owners full control over financial distributions—with no built-in oversight, transparency mechanisms, or enforceable agreements—team funds can be altered, redirected, or withdrawn without other members' knowledge or consent. For example:

> *There's a group fund total and then a percentage that would be split up among developers. [. . .] Owners have complete access to remove funds and change percentages of developers. [The owner liked a] gambling game [. . .] [and he] took a bunch of money for himself, without any of us knowing. [P11]*

P11 described how the group payout system, which splits funds among RCs, can be easily manipulated by project leaders. Unlike larger, professionally managed companies—where financial transactions typically pass through multiple layers of oversight, formal budgeting processes, and documented approvals—many Roblox development teams operate with minimal structure or transparency. This absence of checks and balances not only fosters a sense of unfairness within teams but also threatens creators' financial security and autonomy.

5.3.2 Labor Exploitation

Labor exploitation risk refers to the vulnerabilities RCs—especially underage or informal creators—face when working in teams without legal protections, formal labor structures, or reliable financial governance. These risks include unfair treatment, unreliable or withheld pay, excessive or undefined working hours, and other poor or unstable working conditions. When such risks materialize, they result in harms such as extremely low pay, excessive hours, chronic stress, and being treated as disposable labor. For example, P4 shared:

> *[Roblox] treats us like we're our own companies. [. . .] You're a contractor, so you have no rights. You work 100 hours a week cause you're scared you're not gonna be able to pay rent. But that was your choice to work in the eyes of the law. [P4]*

P4 explained that, as a contractor, they lived in constant fear over financial security. This fear compelled them to work excessive hours under poor conditions. While technically their "choice," the work is often compelled by necessity and absence of legal protections, creating a persistent power imbalance that enables sustained labor exploitation.

The risks of labor exploitation are even more pronounced for under-18 RCs. For example:

> *These kids are treated a lot poorer than the adults because they aren't legally bound, they don't have to be kept on for a certain amount of time, and usually, they are replaceable. [. . .] Because it's under the table, they pay [kids] less. It's awful, but they get away with it. [P15]*

P15 explained that young RCs are treated as disposable—underpaid, given no guarantees, and easily replaced due to the oversupply of eager youth. Informal arrangements allow minors to be paid far below fair rates without consequences. Reflecting on their own experience, P15 recalled earning the equivalent of just one dollar a day as a kid creator, illustrating how Roblox's ecosystem can enable systematic child labor exploitation.

5.3.3 Team Instability

Team instability risk refers to the uncertainty and fragility of collaboration within Roblox development teams. Because teams are often loosely organized and operate without formal roles, contracts, or accountability mechanisms—and often rely on young or transient contributors—RCs cannot reliably predict whether collaborators will communicate effectively, remain engaged, or complete their commitments. These risks can result in harms such as wasted effort, project delays, abandoned games, financial loss, and frustration that undermines both creative and career development.

For example, P11 shared: *"I've had owners who've been completely silent. [. . .] It's terrible communication. He's the scripter of the game, we don't know what we don't know what he wants."* P11 described how game development suffers when team leadership breaks down. In this case, leaders of the project went completely silent, offering no direction or engagement. Without clear communication, RCs were left unsure what to build, leading to frustration, wasted effort, and project delays.

The transience of collaborators further contributes to instability. For example, P6 shared, *"A lot of people are inconsistent. [. . .] They'll work for a few days, and then become unresponsive. A lot of these times, they're young kids in school."* P6 noted how transient, often very young collaborators may lose interest or abandon projects entirely, making progress unpredictable and collaborations fragile. This instability within teams contributes to an unstable work environment, creating risks for both project and career success.

5.3.4 Interpersonal Conflict

Interpersonal conflict refers to the risk of disputes arising within teams when miscommunication, immaturity, or clashing expectations disrupt collaboration. In teams lacking formal labor arrangements, clear expectations, or established conflict-resolution mechanisms, misunderstandings can escalate quickly. Such conflicts can damage trust, stall coordina-

tion, and cause emotional strain, and in severe cases lead to the abandonment of partnerships or entire projects, resulting in creative and financial loss. For example:

> *You can tell when [collaborators] are young, like immature and unprofessional. [. . .] One time we were to decide on a price, but they didn't specify that they thought I was going to cover the [30% cut when using in-game items to transfer payments] and then they freaked out on me. [P7]*

P7 described how miscommunication in informal payment agreements—exacerbated by the immaturity and inexperience of younger collaborators—can cause minor disputes to escalate, disrupting coordination and jeopardizing projects. These conflicts are not isolated; they reflect a broader structural vulnerability tied to the young age and limited professional norms within many creator teams:

> *[Management] varies from game to game. [. . .] A lot of these developers are young teenagers, [. . .] and you got to make sure they do their stuff. [. . .] Working with adults is usually the easiest because we can clearly communicate [. . .] But once in a while, there's still an incident. [P15]*

P15 noted that while management quality varies, interpersonal drama—especially among younger RCs—can threaten collaboration. Immaturity and emotional volatility create unstable team dynamics, undermining discipline, morale, and productivity. Emotional struggles compound these risks, making coordination difficult. Working with adults can reduce, but not eliminate, such conflicts.

5.3.5 Defense

Informal Legal Support. Since Roblox provides little legal or financial oversight, some RCs turn to peers with more experience in contracts or revenue-sharing arrangements. P16 described a friend who had successfully negotiated contracts and profited: "*He got a percentage of a game, [. . .] made thousands off this.*" This peer expertise provided a model for navigating Roblox's largely informal labor market, helping less experienced creators understand and protect their financial interests without formal legal infrastructure.

Negotiation for Fairer Pay. Sign contracts, and negotiate compensation—providing a pathway out of exploitative informal arrangements. For example, P15 noted that *"Now that I'm 18, I can sign on contracts to work on these bigger games [. . .] You can usually negotiate pay if you think you'll pay be paid higher.*" Such self-initiated negotiations can improve job stability and lead to fairer financial rewards. However, as P15 noted, these opportunities typically arise only once creators are adults, leaving younger creators largely unprotected.

Taking on Leadership Responsibility. To prevent projects from collapsing, some step into leadership roles. P18 explained, *"If no one wants to be leader, I can just take up and take charge [. . .] [Otherwise] the project is going to fall apart."* While this initiative can stabilize projects in the short term, it also reflects a structural gap that RCs are compelled to take on extra labor due to the absence of formal team management systems.

5.4 Community Risks

RCs participate in ongoing community engagement within creator and player communities, generating a variety of peer-to-peer interactions and social dynamics. These community dynamics on Roblox are shaped by structural conditions that configure creators' vulnerability to socially driven harms. The key structural conditions include: (1) prominence and visibility within a youth-dominated audience, and (2) absence of strong community governance. Together, these conditions create opportunities for malicious actors to target RCs. The following subsections illustrate how these structural conditions give rise to specific operational risks in RCs' everyday experiences, including extortion, privacy breaches, and reputation risk.

Prominence and Visibility in a Youth-Dominated Audience. RCs often gain visibility within a large, youth-dominated audience, which can expose them to unwanted attention, harassment, and inappropriate interactions. This visibility amplifies scrutiny and invasive curiosity, making RCs more vulnerable to identity exposure and privacy violations. Some RCs shared that younger audiences may engage in boundary-crossing behavior, fueled by idolization or curiosity, increasing the likelihood of unwanted contact or exposure.

Absence of Strong Community Governance. Beyond platform-level moderation, the broader Roblox creator community lacks strong governance structures or reliable mechanisms for regulating interpersonal behavior. RCs regularly interact across loosely moderated spaces—such as Discord servers and fan communities—where norms for privacy, conduct, and accountability are inconsistently enforced. This governance gap potentially enables malicious actors to invade privacy and engage in harassment.

5.4.1 Extortion

Extortion risk refers to creators' exposure to coercion or blackmail by malicious actors in the community, particularly when leaked or exposed personal data becomes weaponized. When security breaches occur, private information can fall into the hands of exploitative groups who use it to threaten and manipulate others—risks that are amplified by RCs' high visibility within a youth-dominated community. Such risks can escalate into serious harms, including financial loss, exposure to blackmail, emotional distress, and even real-world threats to

personal safety. P7 shared:

> *There was a data breach a little bit ago, a lot of personal information came out, and a group of teenagers exploited people with a lot of Robux, such as developers. [P7]*

P7 noted group threatened and carried out severe real-world harm ("swatting") unless the creators paid them Robux. This example illustrates how security vulnerabilities in Roblox can escalate into offline harassment and coercion, with creators' financial assets and safety being leveraged against them.

5.4.2 Privacy Breach

Privacy breach risk refers to the unauthorized exposure or dissemination of personal information as RCs participate in the broader creator and player community. As RCs seek out collaboration, networking, and communication, they become exposed to risks of privacy breaches. These risks can lead to concrete harms, including unauthorized exposure of sensitive data, doxxing, invasive fan behavior, and even threats to personal safety.

For example, P17 noted that because Roblox's heavily moderated chat limits communication, many turn to third-party platforms like Discord: *"[Discord] was a big boost to be able to communicate, [. . .] [but] I know that there are some horror stories like personal details being shared."* However, while useful, this shift introduces new vulnerabilities, such as data breaches and the unintended sharing of personal details. RCs also expressed privacy concerns about invasive fan behavior:

> *Most big developers [. . .] don't want their identities out, especially when there's a younger audience, surrounding them, because they will actively seek them out and try to expose them. [P7]*

As P7 explained, popular creators—especially those with large youth audiences—often keep a low profile to protect their privacy. However, fans may still engage in invasive behavior, such as digging for real identities, driven by curiosity or idolization. Such actions can compromise creators' personal security, online wellbeing, and sense of autonomy.

Additionally, privacy breaches from technical attacks remain a concern. As P12 noted, *"some people can hack by seeing your IP address and where you live."* Such unauthorized access to IP or geolocation data creates serious risks of doxxing and real-world threats to personal safety.

5.4.3 Reputation Risk

Reputation risk refers to creators' vulnerability to reputational harm when peers, imitators, or the broader community negatively shape their public image, credibility, or creative identity. High visibility and weak community governance around protecting originality limit RCs' control over how their style, name, or work is represented. As a result, creators may experience reputational harm when others clone, distort, or misappropriate their creative identity, leading audiences to form inaccurate or unfavorable perceptions of their work:

> *Every one of those games you're seeing is a copy of mine. [. . .] If you go into [the games], you'll be met with all these in-app purchases, jump scares. [. . .] I've messaged a few of them [. . .][to] change it up a bit because you're using my style to push these cash grabs and people are starting to associate that style [. . .] with cash grabs. [P7]*

P7 described how other RCs copied their game's style, but filled these clones with aggressive in-app purchases and poor user experience. P7 emphasized that imitation can become harmful to their reputation, leading audiences to associate the original style with exploitative practices.

5.4.4 Defense

Minimizing Exposure. Anonymity is a common strategy used by RCs to protect themselves from risks such as privacy breaches and doxxing. P15 explained, "*Usually [kids] want to stay anonymous. [. . .] a lot of people are scared of being doxxed,*" noting that this approach is especially common among kid creators, who can be more socially vulnerable. Similarly, P7 noted that "*a lot of big developers try to keep a very small paper trail.*" Maintaining anonymity serves as a self-protective strategy in a community where personal information can be exploited.

5.5 Technical Risks

Due to the technical nature of game development, structural and platform-level conditions play a critical role in shaping RCs' experiences. RCs identified several such technical structural conditions, including: (1) exploitable platform security design, (2) insecure or easily manipulated asset storage systems, and (3) unstable or disruptive platform update cycles. These structural conditions give rise to technical risks, which refer to vulnerabilities and breakdowns in game architecture and platform infrastructure that can disrupt gameplay, undermine development, or create financial instability for creators. The following subsections detail how these structural conditions manifest in RCs' technical workflows, resulting in specific risks such as security breaches, asset theft, and unexpected feature breakage.

Exploitable Platform Security Design. Roblox's underlying technical architecture, such as its client–server model, contains systemic vulnerabilities that allow unauthorized manipulation of game logic or the injection of malicious code. Even as protections have improved, small gaps in server trust, script validation, or account-level deterrence continue to potentially expose RCs to security breaches.

Insecure or Easily Manipulated Asset Storage Systems. Roblox's asset storage mechanisms allow creators' digital assets to be discovered, copied, or extracted with relatively little technical effort. Predictable asset IDs, limited access controls, and exploitable interfaces enable unauthorized users or bots to replicate in-game assets such as clothing and models, posing persistent risks to RCs' ability to protect their creative work.

Unstable or Disruptive Platform Update Cycles. Platform-level updates—often altering core APIs, asset rules, or backend functionality—can break existing game features without warning or adequate backward compatibility, forcing creators to repeatedly adapt or rebuild systems, disrupting development and game functionality.

5.5.1 Security Risk

Security risk refers to the uncertainty creators face over whether technical weaknesses in their games will be exploited, such as client–server exploits, malicious script injections, and unauthorized data access. When realized, these risks can lead to harms like compromised game integrity, disruption of gameplay, erosion of player trust, and financial losses for creators.

Client–Server Exploits. Roblox's architecture has enabled unauthorized script execution, especially in its early stages when weak safeguards (e.g., filtering-disabled servers) allowed client-side users directly manipulate server behavior:

> *Because of the way Roblox operates, it's possible to force scripts into the Roblox client that then is processed by the server. And back then, there was very little protection. [. . .] People could utilize exploits to display things that probably shouldn't be shown to children. [P15]*

As P15 noted, platform updates have significantly reduced the risk of unauthorized script execution, but have not eliminated it. Roblox's underlying architecture still leaves room for exploiters to scan game scripts, spot small loopholes or weaknesses, and use them to compromise gameplay or system integrity. For example, P15 noted "*Looking at a script, scrolling through it you can see tiny vulnerabilities, exploiters would find a tiny flaw and then send whatever to mess up the entire system."* Vulnerabilities such as small coding flaws or overly trusting client messages can still create "tiny" loopholes that compromise entire systems. Countermeasures like account bans often prove ineffective: *"Because they would just terminate one account. Three more would sprout out." [P15]*. The ease of creating new accounts weakens deterrence, underscoring the persistent challenge of securing games and protecting player safety.

5.5.2 Asset Theft

Asset theft refers to unauthorized copying or appropriation of digital assets, such as audio and clothing designs, and even entire games—through technical exploits or manipulation of Roblox's asset system. These vulnerabilities undermine creative labor, cause financial loss, and reveal platform-level security gaps. For example, some participants described ID-based exploitation, where predictable numbering in asset URLs allows others to locate and copy original templates. As P14 explained: *"It's very easy to find the original template of the design. [. . .] So people would copy it, [. . .] save the image, and upload it."* A technical flaw enables others to download and re-upload items as their own. P14 recounted designing a skirt that gained significant sales and favorites—only to later find many copies appearing in the store: *"If a bot sees that this account is making a lot of sales, they're going to copy it."* Such automated and organized copying of popular items highlights a persistent technical vulnerability in Roblox's asset storage design, potentially causing revenue loss and frustration for the original creators. Although Roblox assigns ownership metadata to assets, exploits can still be used to bypass these protections:

> *Usually, Roblox has pretty good restrictions on who owns what [. . .] but there are many instances where people can steal assets from a game using some exploits. [. . .] Big games and really popular developers who have millions of Robux are big targets, [people are] trying to steal money off of them. [P11]*

Exploiters can bypass Roblox's ownership restrictions to extract assets from other creators' games. High-profile or high-revenue projects are frequent targets, leaving creators vulnerable to both financial loss and reputational harm.

5.5.3 Unexpected Feature Breakage

Unexpected feature breakage refers to the disruption caused by Roblox's platform-level updates that alter, deprecate, or remove previously available functionality. These changes can compromise the stability and usability of games:

> *Some of [Roblox's] updates interfered with a lot of the games I worked on, specifically the one where they changed music that was shared, [where originally] anyone could use [but the change meant] only the people who own them [can] use them. [. . .] They [also] have a lot of updates that do break a lot of the Roblox games. [P20]*

As P20 described, backend changes can instantly disable core features. Frequent updates thus create risks of partial or total feature failure, undermining stability and usability.

5.5.4 Defense

Hackproofing Scripts. RCs sometimes add preventative scripts to block backdoor exploits that allow attackers to manipulate gameplay or content. As P12 explained: "*There were*

certain scripts you should add to make sure someone can't create a backdoor into your game and do whatever they want."

Joining Anti-Exploiter Efforts. Some former exploiters pivot to helping secure the platform and games. P15, a former exploiter, recalled being unexpectedly recruited to improve a game's defenses rather than being banned: *"They invited me to work on the game and help patch out this stuff."* Their insider knowledge supports community-driven efforts to strengthen platform and game security.

6 Discussions

We discuss the distinct risk landscape for game creators in UGG development, highlighting the risks stemming from platform design and governance gaps. We then propose recommendations for mitigating these digital risks.

6.1 Risk Landscape of Game Development: Technical, Organizational, and Youthful Dimensions

Prior research shows that content creators—particularly those working on social media—are routinely exposed to digital threats such as harassment, doxxing, blackmail, and stalking, often linked to their public prominence [17, 42, 44, 50]. Our findings resonate with this broader landscape. For example, RCs likewise reported risks of extortion and swatting following data breaches, as well as privacy-invasive fan behaviors where audiences attempted to uncover creators' identities (e.g., P7). Yet, we extend this body of work by showing how the UGG context compounds these risks along three dimensions: the technical intensity, the organizational precarity, and the youthful demographics.

Technical Intensity of Game Creation and Security Vulnerabilities. Unlike traditional social media content, game development requires technically intensive labor to build complex, interactive systems [15, 33, 47]. This technical depth expands the attack surface, exposing creators not only to harassment- and moderation-centered risks but also to security-specific harms such as malicious scripts, asset theft, and exploit-based attacks. Echoing Kou et al.'s findings on malware introduced through free models in Roblox [22], our study extends this work by showing how platform-level architectural vulnerabilities (e.g., predictable asset IDs, client–server exploits) translate into lived security harms. For example, P11 described how asset system flaws could be exploited to "steal money off of" RCs, underscoring financial risks. **Importantly, these technical risks can also amplify and intertwine with other risks, such as harassment and abuse.** Prior work on content creators' online safety has documented various hate and harassment threats [42, 44, 50]. Our findings advance this work by showing how the technical intensity of game development compounds these dynamics, creating intersections between security vulnerabilities and social harms. For instance, P12 feared hacking could expose IP addresses and even cause physical harm to themselves and household members. Similarly, P7 recounted how a data breach enabled harassment and even extortion, demonstrating how technical vulnerabilities and social attacks can converge to threaten both digital and physical safety.

Team-Based Production Models and Associated Precarities. The development of many Roblox games mirrors small-scale studios, requiring diverse roles, collaboration, and coordination. Prior research on game development has noted challenges such as uneven skill levels and communication breakdowns [15, 33]. Our findings extend this literature by showing how such difficulties directly translate into digital risks for game creators. For example, as P9 and P11 noted, unstructured financial controls within collaborative projects are not merely inefficiencies but can enable theft, embezzlement, or withholding of payment. While prior work on social media creators has largely examined them as individual workers [17, 42, 44, 50], our study highlights the distinct risks faced by game creators who frequently operate in team-based settings. In these contexts, governance failures and the absence of formal protections can disproportionately harm the most vulnerable members. For example, contractors may be subject to exploitative arrangements, while underage creators are particularly exposed to unfair labor practices and a lack of legal protection.

Youthful Precarity on "Child-Friendly" UGG Platforms. With over half of Roblox's user base under 16 [23, 48], many RCs begin creating games while still minors [29]. This youthful demographic creates a distinctive risk landscape. While Choi et al. highlight Roblox development as play and learning for children [8], our findings extend this view by highlighting that the same environment can also be unsafe and exploitative. Minors often engage in game development without legal protection, leaving them vulnerable to unfair contracts, underpayment, or other forms of exploitation. At the same time, this youthful creator base creates risks for collaborators who depend on them. Participants (e.g., P6, P7, P15) noted that immaturity, inexperience, and limited commitment among child creators often led to abandoned projects or failed collaborations. For developers whose livelihood depends on Roblox, such disruptions create both creative setbacks and financial risks.

6.2 Risks from Platform Design and Governance Gaps

Risks Generated by Platform Moderation and Monetization. Prior work shows how platform precarity and censorship (e.g., shadowbanning, deplatforming) create risks for content creators [44]. Our findings echo this: Roblox's opaque moderation imposes financial and emotional burdens. False positives or unclear flags can remove assets, block updates, or

suspend accounts with little recourse, producing livelihood shocks and chronic stress. As P4 noted, persistent anxiety over unpredictable moderation became an unavoidable cost of sustaining creative labor. Extending previous work on platform-related risks for content creators [44], we further highlight how Roblox's monetization model compounds these risks. Stacked fees, high payout thresholds, and non-refundable upload costs heighten financial precarity and limit creators' autonomy over their creative work.

Risks Amplified by Governance Gaps and Absent Support. Internally, the lack of financial controls and oversight exposes creators to exploitation. Legal scholars note how platform design can enable systematic manipulation and exploitation [19,30]. Our findings provided empirical evidence of how platform governance—or lack thereof—can actively produce risk for game creators. As P11 noted, without structured payment systems, group owners can divert or withhold earnings, causing risks of exploitation and embezzlement, demonstrating how governance vacuum leaves creators reliant on unsafe practices and heightens their exposure to financial harm.

These governance gaps extend to external disputes, particularly around IP. Legal scholars argue platforms are the *least cost avoiders*—uniquely positioned to resolve IP disputes efficiently through mechanisms such as takedowns, licensing, or dispute-resolution channels [16]. Our findings show that Roblox provides limited support beyond content moderation and lacks a structured dispute-resolution process. As P4 noted, this often leads large companies to pursue lawsuits against individual RCs rather than engage through the platform. This reflects what legal scholars describe as a governance vacuum under *safe-harbor regimes*: because platforms are shielded from liability as long as they respond to takedown notices, they have little incentive to facilitate negotiation or assume responsibility for external disputes [3, 16]. In Roblox's case, this shifts legal and financial risks onto RCs while continuing to profit from their labor.

Coping through Individual and Collective Resilience under Platform Protection Gaps. Echoing prior work on social media content creators [42, 44, 50], our participants similarly relied on community support and knowledge-sharing and developed personal strategies to manage risks like exploitation and harassment. We extend this literature by showing these strategies function not only as coping mechanisms but also as individual and collective resilience that compensate for the platform's governance gap around labor, finance, and security. For example, P15 could only negotiate fair pay after turning 18; as a minor, they earned "a dollar a day" without contract protections. Practices such as community scammer vetting, informal contract negotiation, and self-censorship illustrate how creators build protective infrastructures where the platform does not—mitigating risk while highlighting a structural asymmetry in which creators bear disproportionate responsibility for their own safety, security, and autonomy.

6.3 Towards Solutions

Our findings highlight that addressing digital risks for game creators requires coordinated action across multiple levels: policymakers, platforms, communities, and RCs themselves.

Platform Responsibilities. Roblox's moderation, monetization, and governance structures shape creators' risk environment, underscoring the need for stronger platform interventions. These include greater moderation transparency and accountability (e.g., clear takedown rationales and timely appeals), financial safeguards (e.g., escrow payments and refundable uploads), and structured IP dispute resolution with legal support. Given the high proportion of child creators, platforms should also provide youth-appropriate labor protections, such as parental consent mechanisms, age-specific contracts, and baseline pay standards.

To address structural technical vulnerabilities, the platform should introduce complementary interventions: (1) automated bug-finding and exploit-detection tools, such as static analysis tools to identify insecure coding patterns during development, and dynamic exploit-detection systems that monitor runtime behavior for suspicious interactions (e.g., server-side anomaly detection to flag request patterns associated with known exploit strategies). (2) more secure game execution environments that reduce the attack surface (e.g., through strict server-side checks for all gameplay-critical actions and limits on client's ability to execute automated scripts or upload arbitrary, unvetted content). (3) stronger asset security, including permissions-based asset visibility, watermarking, and optional obfuscation for sensitive or high-value assets. (4) security-focused starter templates and example projects that model best practices in secure architecture (e.g., robust server-side validation and safe asset handling), providing creators with guidance for building more resilient systems.

Community Safeguards. Creators already rely heavily on community-based protections, such as scam-vetting networks and peer knowledge-sharing. Platform design could strengthen these efforts through technical scaffolds (e.g., community-driven moderation APIs, reporting tools for flagging scammers), curated resource libraries (e.g., contract templates, financial guidance, legal-literacy materials), and youth-safe learning spaces (e.g., moderated forums, platform-hosted mentorship on contracts, IP, and finances). Such supports would bolster community resilience while reducing the disproportionate burden on vulnerable creators.

Creator Resilience. Participants described a range of defensive strategies, including creating secondary accounts, self-censorship, anonymity, and informal negotiation. While these practices demonstrate resilience, they are largely reactive. Supportive interventions—such as training on safety, contracts, and financial literacy, as well as peer mentorship—could help, especially younger creators, better identify exploitation and negotiate fairer terms, shifting from survival tactics to more proactive and sustainable practices. Addition-

ally, integrating security fundamentals into Roblox's official learning pathways—such as client–server trust boundaries and creator-centered threat models—could help creators better understand and avoid common security pitfalls.

Policy Implications. Many risks for game creators stem from structural gaps beyond the control of any single actor. Policymakers could address these by adapting child labor, IP, and platform regulations to UGG ecosystems. For example, mandating independent audits of payout systems to ensure fair revenue distribution and requiring transparent IP dispute-resolution processes to support creators.

7 Limitations

This study has several limitations that shape the interpretation of our findings. First, our sample consisted exclusively of U.S.-based Roblox creators. This was due to funding and IRB constraints rather than intentional exclusion, yet it limits the transferability of our findings across cultural, infrastructural, and regulatory contexts. Given cross-national variation in platform governance, labor precarity, and access to digital resources, future work should examine creators in other regions and underrepresented groups to capture broader digital risk experiences. Relatedly, because we focused on a single UGG platform, Roblox, our findings may not fully generalize to creators working on other platforms with different technical architectures, monetization systems, or governance structures. That said, our analysis offers a transferable conceptual framework for understanding how sociotechnical systems—such as financial infrastructures and platform governance—generate and amplify creator risks. Future research can examine how digital risks manifest across diverse UGG platforms and within small-studio development in platformized economies. Second, our sample included only limited representation of minor creators, especially very young ones (e.g., under age 16), who may face distinct and heightened vulnerabilities. The presence of a parent during one interview with a minor may also have constrained the participant's willingness to discuss sensitive topics such as harassment. Future research is needed to better understand child creators' experiences. Third, as with all interview-based qualitative research, our findings are based on self-reported accounts and may be subject to recall bias. However, our goal was not statistical generalization but analytic depth: the sample provided sufficient information power for robust thematic analysis, and we therefore do not claim statistical generalizability.

8 Conclusion

We interviewed 20 RCs to examine how they perceive and cope with digital risks in game development. We found that technical intensity, organizational precarity, and youthful demographics compound known creator-economy risks, producing unique vulnerabilities for game creators. Although game creators show resilience through individual and community strategies, these underscore a structural asymmetry: creators shoulder disproportionate responsibility for protection amid weak platform safeguards. We call for coordinated action by platforms, communities, and policymakers to establish stronger protections for game creators.

Acknowledgments

We sincerely thank the anonymous reviewers for their insightful feedback and our study participants for their valuable contributions. We also extend our gratitude to Shuangpeng Bai for his helpful suggestions in refining the technical recommendations. This material is based upon work supported by the U.S. National Science Foundation under award No. 2326505 and award No. 2334934. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. National Science Foundation.

Ethical Considerations

This study was conducted with careful attention to ethical considerations to ensure **the safety, privacy, and well-being of participants**, particularly given the sensitivity of discussing online harassment, exploitation, and financial precarity. Recruitment and research procedures were approved by the our university's IRB prior to data collection. All participants provided written and verbal informed consent prior to the interview and were reminded they could skip questions or stop at any time. We took additional safeguards for under-18 participants: we obtained parental permission, scheduled interviews through guardians, and required a parent or guardian to remain present in the session to ensure oversight and comfort. Personally identifiable information (PII), such as email addresses, was collected only for scheduling and compensation and was deleted once compensation was distributed. Participants were assigned pseudonyms (e.g., P1, P2) during data analysis and reporting and identifying details in quotes were redacted or altered to prevent re-identification. Research materials and data were stored on encrypted, password-protected drives accessible only to the research team. Audio and video recordings were used solely for transcription and deleted after transcription and accuracy checks were complete. All study-related data will be permanently deleted upon project completion.

Beyond protecting individual participants, our ethical responsibility extends to the broader sociotechnical ecosystem in which these findings circulate, involving interconnected stakeholders, e.g., creators, players, and the platform. Below, we reflect on how our work may affect these three key groups.

For the creator community, our findings raise awareness of digital risks and provide actionable knowledge to sup-

port safer collaboration, clearer communication, and fairer labor practices. While we acknowledge that describing coping strategies may carry a minimal risk of malicious actors learning from these accounts, we believe the greater ethical responsibility lies in empowering creators through shared understanding and transparency. By documenting real-world mitigation practices, this work helps creators strengthen their safety strategies, foster collective learning, and advocate for better protections. These insights also benefit the privacy and security community by informing technical tools, platform design improvements, and educational interventions.

For the player audience, creator-side vulnerabilities have meaningful implications for player safety, especially given Roblox's large child and youth audience. Risks creators face, such as asset theft, client–server exploits, and financial exploitation, can cascade into harms for players through insecure games, exposure to malicious content, or exploitative in-game monetization. Prior research shows that platform monetization pressures can incentivize manipulative design practices (e.g., dark patterns in monetization) that disproportionately affect younger users [21, 22, 45]. By identifying how platform affordances and structural conditions shape creators' vulnerabilities, our research indirectly supports improved player safety and reinforces the ethical interdependence of creator and player protection.

For the platform, our findings highlight both challenges and opportunities. Revealing structural and platform-level conditions—such as weak moderation support and insecure asset exchange mechanisms—may initially draw attention to vulnerabilities within the platform's governance. However, these insights are not intended as critique alone; they point toward tangible avenues for intervention. Addressing such risks can strengthen Roblox's reputation as a secure and equitable ecosystem, build user trust, and support a more sustainable creator economy. More broadly, these findings can inform other platformized game ecosystems as they develop stronger creator protections and ethical governance practices, contributing to an industry-wide culture of responsible creation.

Open Science

We have made the following study materials available on Zenodo at https://doi.org/10.5281/zenodo.17926420: (1) Interview protocol (2) Codebook (all the codes used during data analysis), and (3) Screener survey. In compliance with IRB regulations, we cannot share interview transcripts to protect participant confidentiality and preserve the integrity of the study.

References

[1] Home - Roblox. URL: https://corp.roblox.com/.

[2] Carolina Are and Pam Briggs. The Emotional and Financial Impact of De-Platforming on Creators at the Margins. *Social Media + Society*, 9(1):20563051231155103, January 2023.

[3] Fatemeh Asadi. Digital Platforms and Intellectual Property Infringement: Exploring Legal Liability for User-Generated Content in the Context of Digital Media. *Legal Studies in Digital Age*, 2(1):39–50, 2023.

[4] Virginia Braun and Victoria Clarke. One size fits all? What counts as quality practice in (reflexive) thematic analysis? *Qualitative research in psychology*, 18(3):328–352, 2021.

[5] Virginia Braun and Victoria Clarke. *Thematic analysis: A practical guide*. SAGE Publications, 2021.

[6] Virginia Braun and Victoria Clarke. To saturate or not to saturate? questioning data saturation as a useful concept for thematic analysis and sample-size rationales. *Qualitative Research in Sport, Exercise and Health*, 13(2):201–216, 2021. doi:10.1080/2159676X.2019.1704846.

[7] Virginia Braun and Victoria Clarke. Conceptual and design thinking for thematic analysis. *Qualitative psychology*, 9(1):3, 2022.

[8] Yubin Choi, Jeanne Choi, and Joseph Seering. Leveling Up Together: Fostering Positive Growth and Safe Online Spaces for Teen Roblox Developers. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–18, 2025.

[9] Cecilia D'Anastasio. On Roblox, Kids Learn It's Hard to Earn Money Making Games. *Wired*. Section: tags. URL: https://www.wired.com/story/on-roblox-kids-learn-its-hard-to-earn-money-making-games/.

[10] Stephen Dypiangco. Understanding Roblox Player Demographics in 2025, June 2024. URL: https://www.maxpowergaming.co/post/understanding-roblox-player-demographics.

[11] Nick Tornow Engineering, Vice President of Creator. Annual Roblox Economic Impact Report, September 2025. Section: News. URL: https://corp.roblox.com//newsroom/2025/09/roblox-annual-economic-impact-report.

[12] Patricia E. Vance ESRB, President. What Parents Need To Know About Roblox, December 2024. URL: https://www.esrb.org/blog/what-parents-need-to-know-about-roblox-2/.

[13] Lauren Fichten. Roblox, one of the world's most popular gaming platforms, bans hate speech. Users have found

a way to spread it anyway. - CBS News, August 2025. URL: https://www.cbsnews.com/news/roblox-spray-paint-hate-speech/.

[14] Kia Finska, Antti Hakkala, and Anne-Maarit Majanoja. Security and privacy enhancing framework for Social Media Influencers and Content Creators. In *Proceedings of the International Conference on Computer Systems and Technologies 2024*, pages 37–42, 2024.

[15] Guo Freeman and Nathan J McNeese. Exploring indie game development: Team practices and social experiences in A creativity-centric technology community. *Computer Supported Cooperative Work (CSCW)*, 28(3):723–748, 2019.

[16] Garry A Gabison and Miriam C Buiten. Platform liability in copyright enforcement. *Colum. Sci. & Tech. L. Rev.*, 21:237.

[17] Lea Gröber, Waleed Arshad, Angelica Goetzen, Elissa M Redmiles, Maryam Mustafa, and Katharina Krombholz. " I chose to fight, be brave, and to deal with it": Threat Experiences and Security Practices of Pakistani Content Creators. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 19–36, 2024.

[18] Sharon Heung, Lucy Jiang, Shiri Azenkot, and Aditya Vashistha. "Vulnerable, Victimized, and Objectified": Understanding Ableist Hate and Harassment Experienced by Disabled Content Creators on Social Media. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2024.

[19] Xinyu Hua and Kathryn E Spier. Platform Liability Rules: Strict Liability versus Negligence. *HKUST Business School Research Paper*, (2023-105), 2023.

[20] Chris Kerr. Square Enix prepared to take legal action to protect staff from harassment. URL: https://www.gamedeveloper.com/production/square-enix-prepared-to-take-legal-action-to-protect-staff-from-harassment.

[21] Yubo Kou, Rie Helene (Lindy) Hernandez, and Xinning Gui. "The System is Made to Inherently Push Child Gambling in my Opinion": Child Safety, Monetization, and Moderation on Roblox. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, 2025.

[22] Yubo Kou, Yingfan Zhou, Zinan Zhang, and Xinning Gui. The ecology of harmful design: Risk and safety of game making on a metaverse platform. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference*, pages 1842–1856, 2024.

[23] Jamie Lang. Youtube, Roblox, Tiktok Dominate Kids' Screen Time Says New Study, February 2024. URL: https://www.cartoonbrew.com/videogames/youtube-roblox-tiktok-dominate-kids-screen-time-according-to-new-study-237841.html.

[24] Aron Garst Lee, Alexander. Fortnite Creative's creator economy represents the future of metaversal brand activations, May 2022. URL: https://digiday.com/marketing/fortnite-creatives-creator-economy-represents-the-future-of-metaversal-brand-activations/.

[25] Robin LoBuglio. Indie Bosses Are Still Bosses: Exploitation and Unionization at Small Game Studios | by Robin LoBuglio | Game Workers of Southern California | Medium. URL: https://medium.com/game-workers-of-southern-california/indie-bosses-are-still-bosses-exploitation-and-unionization-at-small-game-studios-4ade7fbe0b44.

[26] Renkai Ma and Yubo Kou. "How advertiser-friendly is my video?": YouTuber's Socioeconomic Interactions with Algorithmic Content Moderation. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW2), October 2021.

[27] Christian Nutt. IGDA issues statement condemning harassment. URL: https://www.gamedeveloper.com/business/igda-issues-statement-condemning-harassment.

[28] Charlie Parker, Sam Scott, and Alistair Geddes. Snowball sampling. *SAGE research methods foundations*, 2019.

[29] Simon Parkin. The trouble with Roblox, the video game empire built on child labour. *The Guardian*, January 2022. URL: https://www.theguardian.com/games/2022/jan/09/the-trouble-with-roblox-the-video-game-empire-built-on-child-labour.

[30] Sabriyya Pate. Platform Liability for Platform Manipulation. *Columbia Law Review*, 125(4):873–924, 2025.

[31] Charles Perrow. *Normal accidents: Living with high risk technologies-Updated edition*. Princeton university press, 2011.

[32] Amanda Peticca-Harris, Johanna Weststar, and Steve McKenna. The perils of project-based work: Attempting resistance to extreme work practices in video game development. *Organization*, 22(4):570–587, July 2015.

[33] Cristiano Politowski, Fabio Petrillo, Gabriel C Ullmann, and Yann-Gaël Guéhéneuc. Game industry problems: An extensive analysis of the gray literature. *Information and Software Technology*, 134:106538, 2021.

[34] Jens Rasmussen. Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2):183–213, 1997.

[35] Amanda Reaume. How Does Roblox Make Money? | Seeking Alpha. URL: https://seekingalpha.com/article/4486523-how-does-roblox-make-money.

[36] Roblox. Developer Exchange – Help and Information Page. URL: https://en.help.roblox.com/hc/en-us/articles/13061189551124-Developer-Exchange-Help-and-Information-Page.

[37] Roblox. Immersive ads | Roblox Creator Hub. URL: https://create.roblox.com/docs/production/monetization/immersive-ads.

[38] Roblox. Luau | Roblox Creator Hub. URL: https://create.roblox.com/docs.

[39] Roblox. Marketplace fees and commissions | Roblox Creator Hub. URL: https://create.roblox.com/docs/marketplace/marketplace-fees-and-commissions.

[40] Roblox. Monetization | Roblox Creator Hub. URL: https://create.roblox.com/docs/production/monetization.

[41] Roblox. How Roblox Is Fueling Careers Across the USA, August 2024. URL: https://corp.roblox.com//newsroom/2024/08/how-roblox-is-fueling-career-opportunities-across-the-us.

[42] Patrawat Samermit, Anna Turner, Patrick Gage Kelley, Tara Matthews, Vanessia Wu, Sunny Consolvo, and Kurt Thomas. "Millions of people are watching you": Understanding the Digital-Safety Needs and Practices of Creators. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 5629–5645, 2023.

[43] Ian Shepherd. The Unlikely Career Path That Built A Viral Creator Brand. URL: https://www.forbes.com/sites/ianshepherd/2025/04/26/from-mit-to-millions-the-rise-of-a-new-creator-economy-star/.

[44] Ananta Soneji, Vaughn Hamilton, Adam Doupé, Allison McDonald, and Elissa M Redmiles. " I feel physically safe but not politically safe": Understanding the Digital Threats and Safety Practices of {OnlyFans} Creators. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 1–18, 2024.

[45] Qiurong Song, Zinan Zhang, Rie Helene (Lindy) Hernandez, Xinning Gui, and Yubo Kou. How Predatory Monetization Designs Manifest in Child-Friendly Video Games. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 515–534, 2025.

[46] Hanne M Stegeman, Carolina Are, and Thomas Poell. Strategic invisibility: How creators manage the risks and constraints of online hyper (in) visibility. *Social Media+ Society*, 10(2):20563051241244674, 2024.

[47] Kornélia Sára Szatmáry. Cybersecurity of the Gaming Industry. In *2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY)*, pages 000441–000446. IEEE, 2024.

[48] Backlinko Team. Roblox User and Growth Stats You Need to Know in 2025, August 2025. URL: https://backlinko.com/roblox-users.

[49] Tushar Thakur. Roblox Game Creation and Monetization Statistics 2025: Goldmine • SQ Magazine, August 2025. URL: https://sqmagazine.co.uk/roblox-game-creation-and-monetization-statistics/.

[50] Kurt Thomas, Patrick Gage Kelley, Sunny Consolvo, Patrawat Samermit, and Elie Bursztein. "It's common and a part of being a content creator": Understanding How Creators Experience and Cope with Hate and Harassment Online. In *Proceedings of the 2022 CHI conference on human factors in computing systems*, pages 1–15, 2022.

[51] Nick Tornow. Unveiling the Future of Creation With Native 3D Generation, Collaborative Studio Tools, and Economy Expansion. URL: https://corp.roblox.com/newsroom/2025/03/unveiling-future-creation-native-3d-generation-collaborative-studio-tools-economy-expansion.

[52] Jirassaya Uttarapong, Jie Cai, and Donghee Yvette Wohn. Harassment experiences of women and LGBTQ live streamers and how they handled negativity. In *Proceedings of the 2021 ACM international conference on interactive media experiences*, pages 7–19, 2021.

[53] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A Framework for Unifying At-Risk User Research. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 2344–2360, May 2022.

[54] Johanna Weststar and Marie-Josée Legault. *Not all fun and games: Videogame labour, project-based workplaces, and the new citizenship at work*. Concordia University Press, 2024.

[55] Zinan Zhang, Sam Moradzadeh, Xinning Gui, and Yubo Kou. Harmful Design in User-Generated Games and its Ethical and Governance Challenges: An Investigation of Design Co-Ideation of Game Creators on Roblox. *Proceedings of the ACM on Human-Computer Interaction*, 8(CHI PLAY):1–31, 2024.

A Participant Table

Table 1: In the 'Role' column, *owner* indicates someone who leads a Roblox development team; *team member* denotes a member of such a team; *indie* refers to an independent developer; and *amateur* describes participants who primarily play Roblox but occasionally try game creation. Participants could hold multiple roles simultaneously (e.g., owning a studio while also contributing to another team).

P#	Age	Gender	Race& Ethnicity	Roblox Player Exp.	Roblox Creator Exp.	Role	Hours/Week	Robux/USD Made (6mo)	Job Type
P1	18+	M	Asian	9 years	4 years	Owner	N/A	N/A	Main job
P2	19	M	Asian	8 years	4 years	Team Member; Owner	>40 hours	>1,000,000 Robux	Main job
P3	18	F	White	5 years	4 years	Indie; Team Member	5–10 hours	>1,000,000 Robux	Main job
P4	23	M	White	11 years	4 years	Indie; Team Member; Owner	>40 hours	>1,000,000 Robux	Main job
P5	23	M	Black or African American	1 month	6 months	Amateur	11–20 hours	10,000 Robux	Side job
P6	19	M	White	11 years	9 years	Owner; Indie	11–20 hours	100,000 Robux	Side job
P7	20	M	White	8 years	8 years	Owner	21–30 hours	>1,000,000 Robux	Main job
P8	21	M	Asian	9 years	2 years	Amateur	<5 hours	0	Hobby
P9	18	M	White	8 years	1 year	Indie	<5 hours	0	Side job
P10	22	M	Hispanic/Latino/ Spanish descent	12 years	2 years	Amateur	<5 hours	0	Hobby
P11	17	M	White or Caucasian	8 years	3 years	Team Member; Indie	11–20 hours	40k–42k Robux	Hobby
P12	20	F	Middle Eastern or North African	2 years	1 year	Indie	<5 hours	100 USD	Side job
P13	20	M	Black or African American	10 years	2 years	Indie	<5 hours	10,000 Robux	Hobby
P14	20	F	White or Caucasian	10 years	Few months	Indie	<5 hours	5,000 Robux	Hobby
P15	19	F	White or Caucasian; American Indian/Native American or Alaska Native	10 years	6 years	Team Member	5–10 hours	1,000 USD	Main job
P16	18	M	Asian	10 years	5 years	Indie	<5 hours	0	Hobby
P17	19	X	White or Caucasian	12 years	11 years	Indie; Team Member	<5 hours	0	Hobby
P18	19	M	White or Caucasian; Black or African American	7 years	6 years	Team Member; Indie	5–10 hours	1,500 USD	Main job
P19	28	M	Asian	3 months	3 months	Amateur	>40 hours	200 USD	Hobby
P20	19	M	Asian	6 years	5 years	Amateur	<5 hours	15 Robux	Hobby