Protecting Unreleased Music: Usability and Security Challenges in Creative Collaboration

Problem Statement and Goals

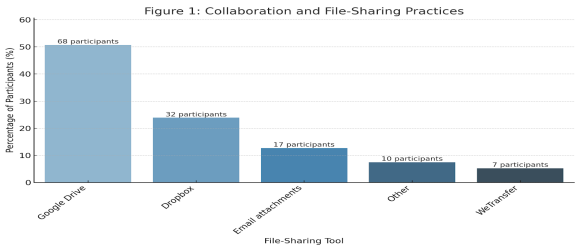
Unreleased music is high-value intellectual property, yet leaks remain common despite the availability of secure file-sharing tools. Music professionals collaborate quickly, share large files, and work across distributed teams. When security tools disrupt creative workflows, they are often bypassed in favor of convenient but risky alternatives.

This study aims to:

- Identify how unreleased music is shared in real-world creative workflows
- Understand why secure file-sharing tools are avoided or bypassed
- Examine how usability challenges lead to risky sharing behavior
- Inform the design requirements for secure, workflow-compatible creative tools

Approach

This study used an anonymous online survey of musicians, producers, and sound engineers recruited through Prolific who actively collaborate on music creation. A total of 255 valid responses were collected. The survey captured both quantitative and qualitative data on file-sharing tools, security practices, perceptions of leak risk, and experiences with unauthorized distribution. Responses were analyzed to identify patterns linking usability challenges to risky sharing behavior.



Results

Key Findings

Finding 1: Convenience Drives Tool Choice
Most participants used general-purpose cloud platforms over industry-specific secure tools.

- Google Drive: **51%**
- Dropbox: **25.5%**
  Ease of use outweighed security features.

Finding 2: Risky Workarounds Are Common

- Over **50%** shared unreleased music via email or text messages.
- **72.4%** avoided security tools due to inconvenience or workflow disruption.

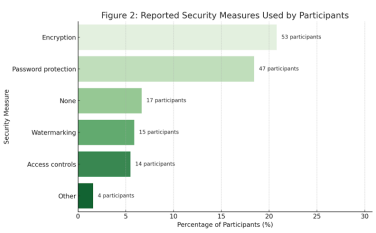
Finding 3: Leak Experience Does Not Reduce Risk

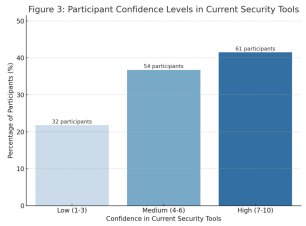
- Prior leak exposure did not lead to safer behavior.
  76% of affected participants continued risky sharing practices.

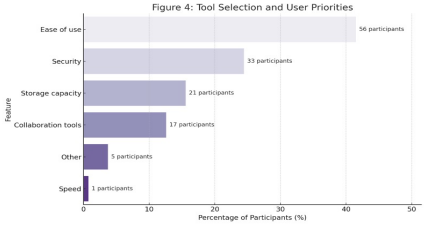
Overall Insight: Security awareness alone does not prevent leaks and usability friction pushes creative professionals toward insecure workarounds.

Future Work

- Observational studies in real studio environments
- Interviews across industry roles and label sizes
- Usability testing of secure, creative-workflow-friendly tools







Works Cited
Horowitz, S. J. (2023). Protecting the "throne": How jay-Z & kanye beat the leaks. Retrieved from https://www.billboard.com/music/music-news/protecting-the-throne-how-jay-z-kanye-beat-the-leaks-4879204/
Karaganis, Joe, Media Piracy in Emerging Economies (Social Science Research Council, March 2011), https://www.ssrc.org/publications/media-piracy-in-emerging-economies/
Stolen hard drives with unreleased Beyoncé Music: A major security breach on the "cowboy carter" tour (n.d.). Retrieved from https://www.vinylmeplease.com/blogs/music-industry-news/stolen-hard-drives-with-unreleased-beyonce-music-a-major-security-breach-on-the-cowboy-carter-tour?srsltid=AfmBOoqYJXEgJlFEP

Rutika Kushe
University of California, Berkeley

Berkeley UNIVERSITY OF CALIFORNIA

Protecting Unreleased Music: Usability and Security Challenges in Creative Collaboration

Abstract

The leaking of unreleased music has become an increasingly serious cybersecurity and intellectual property issue. Artists, producers, and sound engineers regularly exchange unfinished tracks through cloud services, messaging apps, and shared studio systems, often with minimal security controls. When these files are compromised, the losses extend beyond reputation and revenue because they undermine trust within creative communities and expose broader weaknesses in digital collaboration security. This research examines how these leaks occur and why existing protection measures such as encryption, watermarking, and access control often fail in practice.

Through surveys and interviews with music professionals, I found that many breaches stem from usability barriers rather than purely technical flaws. Security tools that are too rigid, disruptive, or poorly integrated into creative workflows tend to be ignored or bypassed altogether.

Using a human-centered cybersecurity approach, this study analyzes the trade-offs between security strength and creative usability. It highlights recurring usability pain points and proposes solutions such as embedded access controls, transparent encryption, and invisible watermarking that preserve both protection and ease of collaboration.

By focusing on the human factors behind digital asset protection, this work contributes to the growing field of usable security and privacy. It also raises broader questions about how cybersecurity design can adapt to specialized domains like the arts, where creativity and speed often outweigh strict policy enforcement. The goal is to build systems that make secure sharing effortless while maintaining the flexibility that artists and producers need.

Rutika Kushe
University of California, Berkeley