

Behind the Mask: Analyzing the Drivers and Impacts of Catfishing

by

Mahadi Ibne Bakar

21201301

Zareen Shyma

21201255

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering
Brac University
June 2025

© 2025. Brac University
All rights reserved.

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:



Mahadi Ibne Bakar
21201301



Zareen Shyma
21201255

Approval

The thesis/project titled “Behind the Mask: Analyzing the Drivers and Impacts of Cat-fishing” submitted by

1. Mahadi Ibne Bakar (21201301)
2. Zareen Shyma (21201255)

Of Spring, 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science and Engineering on June 18, 2025.

Examining Committee:

Supervisor:
(Member)

Dr. Farida Chowdhury

Professor
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)



Anika Priodorshinee Mrittika

Lecturer
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

Dr. Md. Golam Rabiul Alam

Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi, Ph.D

Associate Professor & Chairperson
Department of Computer Science and Engineering
Brac University

Abstract

The rapid expansion of social media has significantly altered interpersonal communication dynamics, introducing both opportunities and risks. One growing concern is ‘catfishing,’ where individuals create false online identities to deceive others emotionally or financially. Despite its severity, particularly in Bangladesh, there is limited understanding of catfishing’s demographic influences, psychological effects, and preventive measures. This research explores these dimensions through a mixed-methods approach, integrating survey data from 343 participants and qualitative interviews with 26 victims. Findings reveal that younger, digitally inexperienced users, especially women, are highly susceptible to catfishing, suffering substantial emotional distress and financial losses. The study further demonstrates gaps in digital literacy, insufficient preventive measures, and inadequate reporting mechanisms. Addressing these insights, a design proposal integrating trust scores, verification prompts, emotional manipulation warnings, and simplified reporting is presented, contributing significantly to user security and awareness. This research underscores the critical need for targeted digital education and robust platform safety measures in Bangladesh.

Keywords: Catfishing, Online Deception, Digital Trust, Human-Computer Interaction (HCI), Emotional Manipulation, Digital Literacy, Social Media Safety, Psychological Impacts, Identity Verification, Trust Score

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, to our supervisor Dr. Farida Chowdhury and our co-supervisor Anika Priodorshinee Mrittika for their kind support and advice in our work. They helped us whenever we needed help.

And finally to our parents without their throughout support it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

Declaration	i
Approval	ii
Abstract	iv
Acknowledgment	v
Table of Contents	vi
List of Figures	ix
List of Tables	x
Nomenclature	x
1 Introduction	1
1.1 Motivation	2
1.2 Research Problem	3
1.3 Problem Statement	5
1.4 Research Objectives	5
1.5 Report Structure	5
2 Literature Review	7
2.1 Background	7
2.2 Catfishing Process Overview	9
2.2.1 Overview of Catfishers	10
2.2.2 Trends and Financial Impact of Catfishing	11
2.2.3 Catfishing as a Form of Online Deception	11
2.2.4 The Phenomenon of Catfishing in Online Dating	12
2.3 Related Works	12
2.3.1 Psychological, Emotional, and Social Impacts	13
2.3.2 Motivations Behind Catfishing	14
2.3.3 Detection and Prevention Mechanisms	14
2.3.4 Implications for Digital Security and Future Research Directions . .	15
3 Work Plan	16
3.1 Research Methodology	18
3.1.1 Overview	18
3.1.2 Research Design	19
3.1.3 Data Collection Methods	19

3.1.4	Ethical Considerations	21
3.1.5	Data Analysis	21
3.1.6	Prototype Design	21
4	Understanding Catfishing through Survey Analysis	22
4.1	Survey Design and Implementation	22
4.2	Participant Demographics	23
4.3	Key Findings	25
4.3.1	Victims and Non-Victims of Catfishing	25
4.3.2	Social Media Behavior and Vulnerabilities	25
4.3.3	Awareness of Catfishing and Digital Security	26
4.3.4	Preventive Practices and Behavioral Trends	27
4.3.5	Emotional and Psychological Impacts	27
4.3.6	Reporting Behavior and Systemic Gaps	28
4.4	Data Analysis and Insights	29
4.4.1	Influence of Demographics on Catfishing Susceptibility	29
4.4.2	Emotional, Social, and Financial Consequences of Catfishing	29
4.4.3	Leveraging Findings for Prevention and Support Systems	30
5	Unmasking the Impacts Through Voices from the Deceived	32
5.1	Interview Methodology	32
5.2	Questionnaire Design	33
5.2.1	Initial Questions: Investigating the Incident	33
5.2.2	Emotional Development and Psychological Impact	34
5.2.3	Support Systems and Barriers to Reporting	34
5.2.4	Language Preference and Transcription Process	34
5.2.5	Participant-Centered Design	34
5.3	Participant Selection and Demographic	35
5.4	Thematic Analysis	36
5.5	Thematic Coding	37
5.5.1	Emotional Vulnerability and Manipulation	37
5.5.2	Romantic Deception	38
5.5.3	Financial Exploitation	40
5.5.4	Suspicion and Red Flags	41
5.5.5	Trust Issues	43
5.5.6	Psychological and Emotional Impact	44
5.5.7	Social Isolation and Family Impact	46
5.5.8	Lack of Reporting and Fear of Judgment	47
5.5.9	Identity Theft and Online Safety Concerns	48
5.5.10	Barriers to Online Interaction and Increased Caution	49
5.6	Key Narratives and Patterns: Understanding Victim Experiences	51
5.6.1	The Psychological Phases of Catfishing: How Victims Are Manipulated	51
5.6.2	The Role of Social Media and Online Dating Platforms in Facilitating Catfishing	53
5.6.3	Long-Term Impact on Victims' Digital Behavior	57

6	Design Proposal	59
6.1	Feature 1: “Pause & Verify Prompt”	59
6.1.1	Interaction Design	59
6.1.2	Link to Analysis	60
6.1.3	Grounding in Theory	61
6.2	Feature 2: Trust Score and Profile Review for New Contacts	61
6.2.1	Trust Score Heuristics	62
6.2.2	UI Design	63
6.2.3	Justification & User Research Link	63
6.2.4	Theoretical Grounding	64
6.3	Feature 3: Emotional Manipulation Warnings in Chat	64
6.3.1	Implementation & Logic	65
6.3.2	UI Feedback	66
6.3.3	Rationale & Research Basis	66
6.4	Feature 4: Easily Accessible Reporting System	67
6.4.1	Design and Integration	68
6.4.2	Encouraging Uptake	69
6.4.3	Justification & Connection to Findings	69
6.4.4	Support and Feedback Loop	70
6.5	Interaction Flow and Integration of Features	71
6.6	Design Choices in Light of Literature and Data	72
7	Discussion	74
7.1	Demographic Factors and Susceptibility to Catfishing	74
7.2	Impacts of Catfishing on Victims’ Well-being and Behavior	76
7.3	Informing Prevention Strategies and Support Systems	78
8	Limitations, Future Work and Conclusion	82
8.1	Limitations	82
8.2	Future Work	83
8.2.1	Advanced Detection Methods	83
8.2.2	Cross-Platform Fraud Prevention and Monitoring	83
8.2.3	Enhanced Digital Literacy Initiatives	84
8.2.4	Empirical Evaluation of Interventions	84
8.3	Conclusion	84
	Bibliography	92

List of Figures

2.1	Flowchart illustrating the process of catfishing	9
2.2	Red flags to identify catfishers	11
2.3	Catfishing cases reported in the United States (2019-2022) [65]	11
2.4	Quarterly losses from catfishing (2019-2022) – total reported loss (in millions of dollars) [65]	12
3.1	Overview of the work plan, detailing the phases and tasks for the thesis . .	16
3.2	Overview of the research methodology	19
6.1	Pause & verify modal dialog interface	60
6.2	Trust score banner display on friend and message request page	61
6.3	Trust score display on profile page	62
6.4	Emotional manipulation warning in chat interface	65
6.5	Easily accessible report button in home page and chat interface	67
6.6	Report page interface	68
6.7	Law enforcement contact details display after reporting	69

List of Tables

2.1	The impact of catfishing on different age groups (2019-2022) [65]	8
2.2	Common lies used by catfishers (2022) based on 8,070 reports [65]	10
2.3	Top payment methods in catfishing (2022) – reported losses and number of reports [65]	10
4.1	Demographic data for survey participants (n = 343)	24
4.2	Most frequently used social media platforms among 343 respondents. Multiple selections allowed.	26
4.3	Survey responses on familiarity with the term “Catfish” (n = 343)	27
4.4	Reported repercussions of catfishing experiences (n = 149). Multiple selections allowed.	28
4.5	Survey responses about reporting catfishing incidents (n = 149)	28

Chapter 1

Introduction

With the advancement in technology, many social networking sites have come about and completely changed the way people talk to each other, share information, and make new relationships. With the availability of social media sites like Facebook [77], Twitter [84], Instagram [79], and even dating apps like Tinder [83] and Bumble [73], people are now able to keep in contact with others miles away or even create new social groups. Social networking has also allowed people to have unprecedented access to information and entertainment.

But along with the good aspects of social networking, a more sinister side of it has also come into play. The same tools that were created to facilitate genuine connections among individuals have been exploited for deception and manipulation. Malicious practices like phishing scams, malware distribution, data breaches, cyberbullying, harassment, etc. , are very common occurrences nowadays. But one of these practices, which is less clear to people but increasing rapidly, is what is called “Catfishing”. This is the practice of creating a false persona on the internet, usually to trick others into developing some kind of emotional, romantic, or financial relationship with the persona. With the anonymity that the internet provides and the ease of creating intricate lies, malicious people are easily able to deceive their victims into believing whatever they want them to believe.

To gain the trust of the victims, catfishing is usually done by using false pictures, made-up histories, and empty promises. The catfisher allows the target to become deeply involved in the relationship and then tries to exploit the victim in some way, either emotionally, financially, or sometimes just for the thrill of deception. In order to protect the genuineness of their fictitious persona, the catfishers will often go to extreme lengths to avoid any personal meetings whatsoever. As a result, they will construct the most intricate lies as to why they cannot possibly meet or reveal their true selves. In this way, the vulnerable victims can easily get emotionally attached to someone who does not even truly exist.

Basically, catfishing is a scheme that many people fall victim to, especially when they are emotionally vulnerable, lonely, or just looking for someone to hang out with. People looking for dating, specifically on dating sites, are more susceptible to being catfished [18]. The internet offers the ideal mask for criminals to work without the fear of immediate retaliation. Also, those who are not digitally literate or those who are naive and trusting may miss warning signs in relationships developed purely online [59].

People engage in catfishing for various reasons, including deep-rooted insecurities,

the need to conceal their real identity, mental health issues, seeking revenge against others, or deliberately harassing and causing distress to their target. In some cases, a catfisher steals another individual's complete identity, including their image, date of birth, and geographical location, and pretends that it is their own. Then, the catfisher uses this identity to trick other people into associating with them or doing business online. Moreover, catfishing is no longer the act of an individual; it has become a larger phenomenon of cyber-industrialization, with large organized groups using the internet for scams and deception [58]. With governments and other organizations using digital platforms more and more for communication, catfishing is now not just an issue of personal attacks but also a social issue of trust and security on the internet. It only further showcases the immediate need for more research on this topic that will lead to preventive measures that deal not only with individual catfishers but also with the systemic causes of these kinds of deception.

1.1 Motivation

With the rise of online dating, catfishing has also taken a rise due to loneliness, depression, and boredom increasing rapidly. According to reports [48], from 2018 to 2020, catfishing has risen 33%, and 40% of those cases happened on dating apps. It is a big problem now, affecting 20,000 people a year in the US and costing 600 million dollars in damages in the year 2020. 41% of catfishers say that they do it because they are lonely, and 22% of victims have sent explicit material to catfishers [48]. Besides that, the catfishing scams, 85% of which started on Facebook, just prove that the current safety precautions that Facebook or other social networking sites have in place are not enough to protect users. Catfishing is highly unethical, but it is only illegal if it involves monetary theft [70]. While victims who lose money can seek legal recourse, those who suffer emotional and psychological damage, such as anxiety, depression, and loss of trust, are often left without any form of legal protection. There is no legal structure to cover this issue, and the psychological damage caused by catfishing goes unrecognized, and the victims are left to deal with it on their own.

The issue is even worse in places like Bangladesh, where a large percentage of the population is not as technologically literate [69] and can be easily tricked by catfishers. With all these risks involved, one would think that there would be some discussion about catfishing. However, in Bangladesh, it is pretty much a dead issue, and everyone is completely unaware of the dangers of it and how to avoid it. This makes users very vulnerable to exploitation because they just do not see the red flags. Addressing this gap in knowledge is very crucial. The goal of this research is to understand the current landscape of catfishing in Bangladesh and, based on that understanding, propose preventive measures that would create a much safer online environment where users can feel more confident and secure in their online interactions.

1.2 Research Problem

While some people might have heard of the word ‘Catfishing’, most of them do not know exactly what catfishing means. They just know that it has something to do with online deception, and many times they confuse catfishing with phishing or online impersonation [58], [66]. This misinterpretation opens up users to being emotionally and financially hurt and, therefore, less trusting of the internet overall.

Catfishing is rampant, with research [49] showing a significant percentage of users have already come across fake profiles on different platforms. The psychological impact of catfishing on its victims has been proven [53], [58] to be strong enough that people experience trauma from the incident and anxiety regarding how they’ll interact with others online moving forward. Moreover, the emotional aspect can cause low self-esteem and a sense of betrayal that would prevent victims from involving themselves in real relationships again. Thus, the emotional harm that results from these experiences can move beyond those digital borders and into the “real world” social functioning for the victim [59], [67].

Another reason catfishing has become so common nowadays is because of how easy it is to make multiple accounts on social media and dating websites. Users can put forth their “edited” versions, and it becomes hard for other users to determine what the person is truly like in real life. Online communication being asynchronous makes it even worse because it gives catfishers all this time to build up these believable stories and slowly develop these emotional attachments with the victims over weeks or even months. These factors not only facilitate deception but also amplify the urgency to understand catfishing’s evolving tactics and long-term consequences in digital interactions.

Despite the status of catfishing as a global phenomenon, academic research on the topic remains limited, particularly in the context of real-time detection. Existing studies have predominantly taken a retrospective approach, analyzing incidents after the harm has already occurred. As a result, current interventions are reactive rather than preventive, offering little protection before users become victims. This delay enables catfishers to exploit digital vulnerabilities with minimal resistance.

Moreover, existing mechanisms for verifying identity on digital platforms, such as profile verification badges and facial recognition, focus primarily on static attributes, offering limited support to assess trust in dynamic relationships [81]. While such methods may authenticate a user at the time of account creation, they do not account for how trust is developed and broken through digital interactions over time. As a result, users often rely on self-constructed trust models based on profile completeness, mutual connections, and conversational tone, which are not always reliable indicators of authenticity.

In addition, user-submitted reporting features have been introduced on many platforms to allow users to flag suspicious profiles. However, many individuals are either unaware of these tools, hesitant to use them, or unsure of what constitutes catfishing [66]. Stigma and concerns over privacy discourage reporting even more, with a portion fearing retribution at the hands of whom they report, and a portion not having confidence in reporting effectiveness [58]. This highlights a critical challenge in HCI and online safety research, where the effectiveness of platform security features is often compromised through usability barriers, user perception, and trust in platform sanc-

tioning processes.

Furthermore, an understanding of why an individual engages in catfishing activity is critical in developing effective counter-strategies for its discovery. Most studies have revealed that most catfishers indulge in such an activity in a quest to realize unfulfilled desires for praise, acknowledgment or a morale boost that cannot be achieved in reality [49]. This desire for acceptance is what causes people to fabricate personas and use them to deceive others. Through the examination of these motivations, behavioral patterns can be found and may act as signals of deception and lead to the creation of some successful interventions before the damage is already done.

The stakes are very high, as the emotional and financial repercussions of catfishing can be devastating. Reports of victims losing significant amounts of money to fraudulent schemes or experiencing severe emotional distress are not uncommon at all. This raises urgent questions about how social media platforms can better protect their users from falling prey to such deceptive practices.

Thus, the questions that this research is attempting to answer are the following:

RQ1: *How do different demographic factors (age, gender, education, digital literacy) influence susceptibility to catfishing among Bangladeshi social media users?*

RQ2: *What are the psychological, social, and financial impacts of catfishing on victims in Bangladesh, and how do these impacts shape their subsequent online behavior?*

RQ3: *How can understanding these drivers and impacts inform the development of effective prevention strategies and support systems for the Bangladeshi context?*

The goal of this research is to explore the causes and impact of catfishing on Bangladeshi social media users, focusing on victim demographics, emotional and financial effects, and recovery. In examining the intricacies of catfishing activities, the research will also examine unique deception tactics in Bangladesh and offer recommendations for prevention and support systems.

1.3 Problem Statement

The widespread problem of catfishing presents a serious threat to the emotional well-being and financial security of users who use social media and dating platforms. Despite the increasing prevalence of catfishing, public understanding of its psychological, social, and financial consequences remains limited. This underscores the serious lack of awareness and the need for a deeper understanding of how users in Bangladesh perceive, experience, and respond to catfishing in online interactions. From an HCI perspective, examining how users develop trust, interpret online identities, and navigate deception within digital environments is essential to understanding the cognitive and behavioral dimensions of this issue.

1.4 Research Objectives

Our research aims to explore how users in Bangladesh perceive, experience, and respond to catfishing within digital environments, focusing on the interactional and behavioral aspects of online deception through the lens of Human-Computer Interaction (HCI). By examining trust formation, digital identity assessment, and user adaptation to deception, this study seeks to provide a deeper understanding of the cognitive and social dimensions of catfishing in online spaces. The aim is to understand the causes and effects of catfishing in Bangladesh to determine the common tricks used in catfishing and give suggestions for preventing it and helping victims.

The objectives of the research are given below:

- Providing an introduction to catfishing and how it differs from phishing or online impersonation.
- Examining the relationship between user demographics and vulnerability to catfishing in Bangladesh.
- Documenting and analyzing the various impacts of catfishing on victims, including emotional, social, and financial consequences.
- Understanding how victims cope with and recover from catfishing experiences and what support systems are available or needed.
- Developing recommendations for prevention strategies and support systems based on the analyzed patterns and impacts.

1.5 Report Structure

This report is organized into nine chapters, each contributing to a comprehensive understanding of catfishing as a form of online deception in the Bangladeshi context. Chapter 1 introduces the research topic, outlines its relevance, and defines the problem statement, objectives, and scope. Chapter 2 reviews relevant literature, covering key concepts such as digital deception, emotional manipulation, and privacy vulnerabilities, while situating global findings within local cultural contexts. Chapter 3 explains the research methodology, detailing the mixed-methods design, data collection processes, and ethical considerations. Chapter 4 presents a quantitative analysis of

survey data, exploring patterns in user behavior, victimization, and awareness of catfishing.

Later on, Chapter 5 analyzes qualitative interviews, offering narrative-based insights into emotional and psychological impacts, trust erosion, and coping mechanisms. Chapter 6 synthesizes the findings through a discussion of research questions, emphasizing demographic influences, consequences of catfishing, and potential preventive strategies. Chapter 7 proposes a design intervention informed by research findings, introducing a prototype featuring safety tools such as trust indicators and reporting prompts. Finally, Chapter 8 discusses limitations and future research directions, highlighting areas for innovation in policy, education, and technology. Lastly, concludes the thesis by summarizing key contributions and their implications for social platforms, cybersecurity professionals, and digital users. The report ends with a References section that consolidates all scholarly and web-based sources used throughout the study.

Chapter 2

Literature Review

This chapter presents a systematic overview of the latest research into catfishing, its psychological, social, and technological dimensions. Also including the ways in which platform design, verification systems, and digital affordances facilitate or prevent online deception. It examines the how the term was originated, strategies employed by catfishers and impacts on the victims. Through a synthesis of existing literature, this section identifies common trends in online deception, examines motives for catfishing, and addresses the broader implications for digital security and trust in users. It also reviews a variety of detection and prevention strategies, setting the stage for how Human-Computer Interaction (HCI) can assist in solving the issue.

2.1 Background

The term catfish gained general use in 2010 with the documentary *Catfish* [46], [91] which deals with a real-life case of online deception. In the documentary, a man named Nev Schulman develops a virtual romantic relationship with a woman he met online. But later discovers that she had fabricated her identity using a fake profile. This case study highlighted the intricate emotional factors involved in online impersonation and brought the issue of catfishing into the public eye.

The topic gained further visibility through MTV's *Catfish: The TV Show* [26], which focused on various instances where individuals were deceived by fake online identities. The show's format involved investigating and uncovering the truth behind such deceptions [39]. It placed a strong emphasis on highlighting how easily people can fall victim to manipulated personas in digital spaces.

The term catfish originated as a metaphor in the documentary [46], referring to a practice where live catfish were placed in containers with codfish to keep the cod active during long transports, which ensured the freshness of the codfish. Analogously, in the digital realm, a catfish represents someone who disrupts and manipulates online interactions through deceptive and constantly shifting identities [48]. While initially focused on romantic deceit, the concept of catfishing has broadened to encompass a range of online impersonation behaviors, including those without romantic motives.

According to reports [65], half of the people who lost money to romance scams in the first half of 2023 said that the fraud started on social media platforms like Facebook [77], Instagram [79], or Snapchat [82]. In 2022, over 19,000 people fell victim to romance scams. Moreover, the FTC (Federal Trade Commission) received nearly 30%

more reports of these scams compared to the already high numbers from 2021 [65].

Recent research has also explored the rise of catfishing as a social phenomenon. Many studies analyzed catfishing within cultural contexts, focusing on how it enables alternative forms of intimacy in digital spaces, especially in developing countries [64]. Similarly, another study emphasized how anonymity in online platforms facilitates online deception, making it easier for perpetrators to manipulate and exploit victims [37]. As catfishing incidents continue to rise, with 33% occurring on dating apps, it is crucial to address the difficulties faced by users.

Consequently, the chances of people being susceptible to emotional distress [38] and financial exploitation continue to increase. Moreover, victims often endure severe psychological consequences, including anxiety, depression, and a reluctance to engage in future online interactions [18]. In addition to emotional harm, many victims also suffer substantial financial losses, as illustrated in Table 2.1. Since catfishing is immoral but not typically illegal, victims often cannot seek legal aid. Between 2017 and 2022, more than \$1.3 billion was reported lost due to romance scams, making it one of the most financially damaging forms of internet fraud [65]. The median loss per individual rose dramatically: from \$2,400 in 2021 to \$4,400 in 2022 [65]. Besides, older adults are particularly vulnerable, reporting greater total losses than any other age group, with approximately \$213 million lost in 2021 alone [78]. However, younger generations, including many Gen Z and millennials, have also reported both participating in and falling victim to such scams.

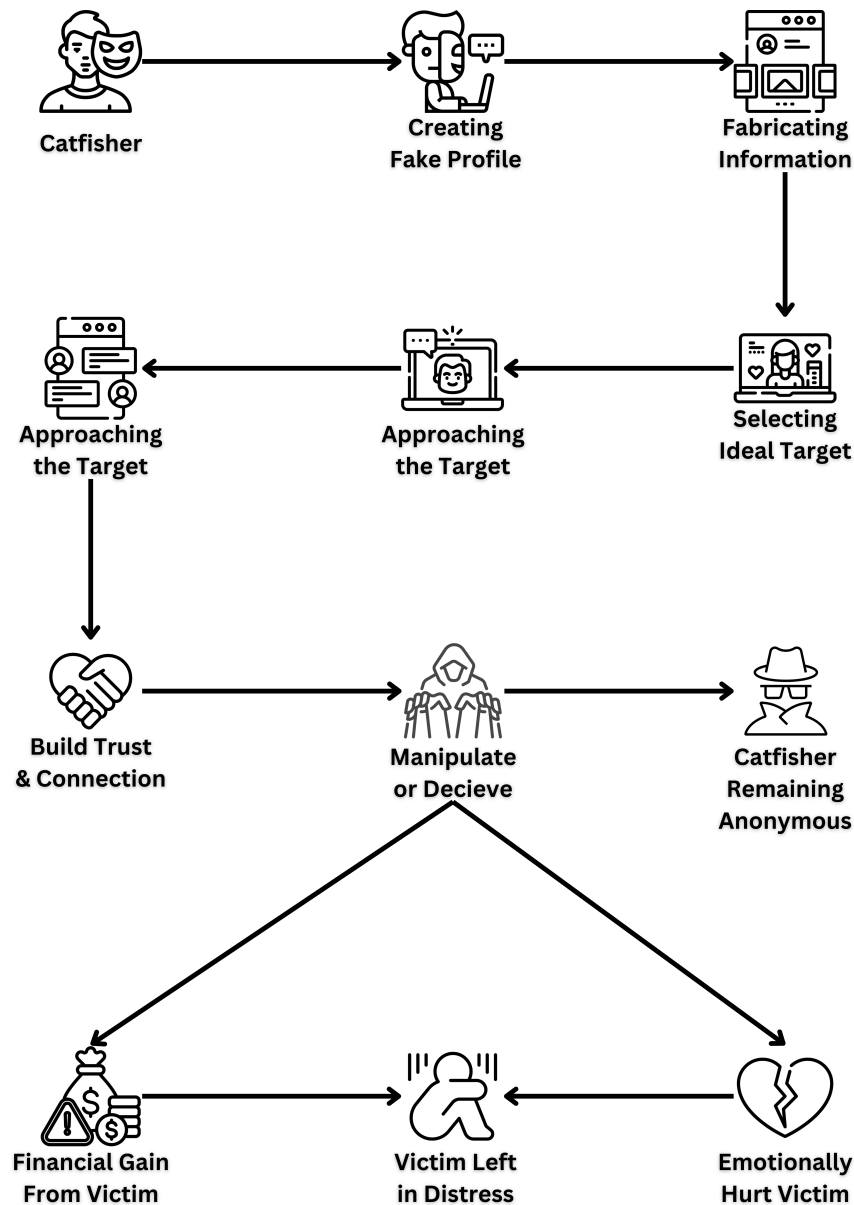
Victim Age Range	Total Cases	Total Money Lost	Average Amount Lost Per Case
20-29	17,479	\$64,297,224	\$3,679
30-39	18,598	\$156,066,108	\$8,392
40-49	17,876	\$201,007,364	\$11,245
50-59	17,331	\$277,391,594	\$16,006
60-69	15,426	\$363,463,711	\$23,562
70-79	6,898	\$211,802,085	\$30,705
80+	1,193	\$36,324,476	\$30,448

Table 2.1: The impact of catfishing on different age groups (2019-2022) [65]

Now, to combat this phenomenon, Human-Computer Interaction (HCI) solutions have emerged as a crucial tool. Addressing the complexities of catfishing with HCI strategies can be very helpful in detecting deceptive behaviors. Meanwhile, this also promotes user education and awareness. As a result, this approach ultimately contributes to a safer online environment.

2.2 Catfishing Process Overview

The following flowchart in Figure 2.1 illustrates the typical process of catfishing, starting from the creation of a fake profile to the manipulation and eventual deception of victims. It highlights some of the major steps, like the first contact, the emotional manipulation, and then the eventual exploitation. This graphic explains how catfishers leverage online platforms to deceive users, emphasizing the complexity and progression of the scam.



(Traditional Laws Don't Provide Proper Support For Catfishing Incidents If Any)

Figure 2.1: Flowchart illustrating the process of catfishing

Recently, researchers have tried to explore many different aspects of catfishing, including the motivation behind such deceptive behavior and the emotional toll on victims, and also discuss the potential strategies for detection and prevention [70] [49].

2.2.1 Overview of Catfishers

Catfishers often prey on vulnerable individuals seeking companionship by using fictional, made-up stories and fabricated identities to earn the victim's trust. They make elaborate stories to put themselves in a fictional situation of dire need and ask for the victim's help to resolve their issues, which can be observed in Table 2.2. Influenced by the sensitive messages asking for help, the innocent victims believe they are doing the right thing by helping their potential friend or partner, only to end up getting emotionally hurt or financially taken advantage of.

Claim or Statement	Reported Usage (%)
"I or someone close to me is sick, hurt, or in jail"	24%
"I can teach you how to invest"	18%
"I'm in the military far away"	18%
"I need help with an important delivery"	18%
"We've never met, but let's talk about marriage"	12%
"I've come into some money or gold"	7%
"I'm on an oil rig or ship"	6%
"You can trust me with your private pictures"	3%

Table 2.2: Common lies used by catfishers (2022) based on 8,070 reports [65]

Scammers often persuade victims to transfer money using various payment methods, such as gift cards, bank wire transfers, and cryptocurrencies. Among these, gift cards are frequently reported as there is less chance of it being tracked as seen in Table 2.3. Cryptocurrency payments are the ones that result in the highest aggregate financial losses.

Payment Method	Total Reported Loss (%)	Number of Reports (%)
Cryptocurrency	34%	19%
Bank Transfer or Payment	27%	14%
Gift Card	7%	24%
Payment App or Service	3%	15%
Other	28%	27%

Table 2.3: Top payment methods in catfishing (2022) – reported losses and number of reports [65]

Recognizing common red flags is crucial to avoid falling victim to catfishing scams. These include claims of immediate emotional attachment, requests for money due to emergencies, and avoidance of in-person meetings or video, which can be seen in Figure 2.2.



Figure 2.2: Red flags to identify catfishers

2.2.2 Trends and Financial Impact of Catfishing

Between 2019 and 2022, reports of catfishing cases and monetary loss have steadily increased as shown in Figure 2.3, Figure 2.4. Data shows that scammers have increasingly targeted victims, resulting in significant financial losses. The situation below highlights how widespread catfishing is. The data shows a strong need for better prevention efforts, awareness campaigns, and targeted actions to protect vulnerable people from online scams.

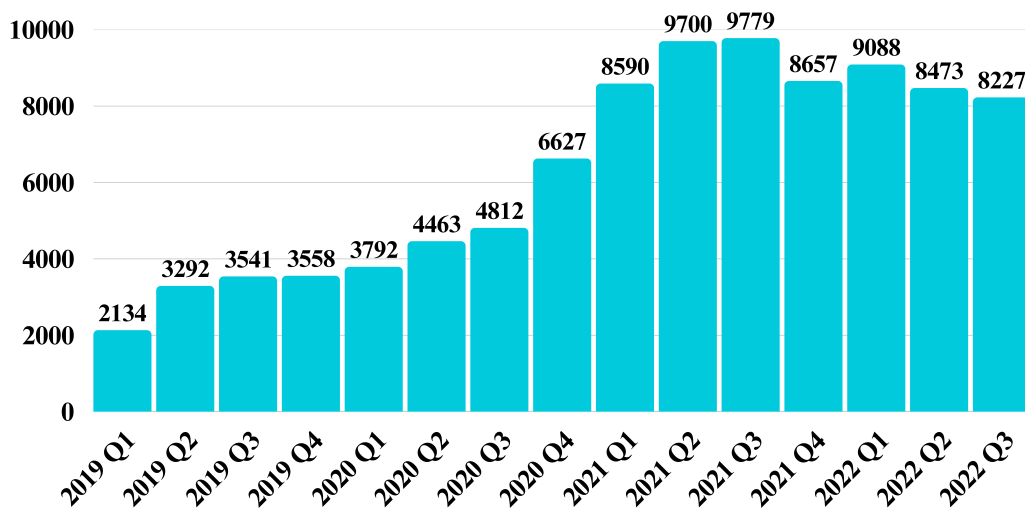


Figure 2.3: Catfishing cases reported in the United States (2019-2022) [65]

2.2.3 Catfishing as a Form of Online Deception

The article [59] delves into the broader dimensions of catfishing as a deceptive practice that is easily facilitated by social media and online dating platforms. It examines how

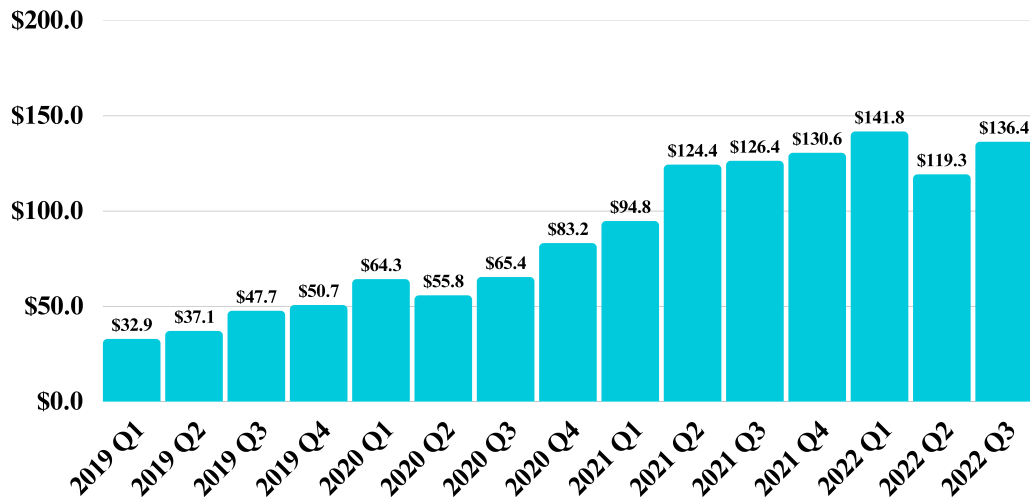


Figure 2.4: Quarterly losses from catfishing (2019-2022) – total reported loss (in millions of dollars) [65]

offenders exploit the anonymous nature of the digital world to create false identities and manipulate others. Additionally, the study highlights the significant emotional and psychological distress experienced by victims, often leaving them with feelings of betrayal and a diminished sense of trust in future online interactions. As noted in the article [55], the heightened awareness and improved digital literacy are crucial in helping users detect and protect themselves from such deceptive behaviors. Besides, it underscores the need for stronger measures and increased awareness to combat the rising prevalence of catfishing.

2.2.4 The Phenomenon of Catfishing in Online Dating

The research [66] considers the possibility of identity impersonation on online dating platforms, specifically Tinder [83]. It takes a phenomenological approach in studying the lived experiences of catfishers. Furthermore, it does so by uncovering their behavior, which in most instances is driven by the need to present a different self or seek some kind of validation that they are not able to achieve in actual life. This illustrates how computer-mediated communication (CMC) makes such an activity possible, as its asynchronous nature provides individuals enough time to creatively engineer their interaction without instant judgment. It also notes that not all instances of catfishing are driven by negative motivations. Some individuals do so as a way of seeking social acceptance or trying to satisfy unmet needs [63]. Such subtleties do nothing but make it even more challenging to determine the reason for catfishing.

2.3 Related Works

This chapter offers an overview of contemporary research on catfishing, namely its psychological impacts, why people catfish, and what it implies for internet security. The discussion considers landmark studies that lay the groundwork for more extensive discussion of online deception and its broader ramifications for online communi-

cation.

2.3.1 Psychological, Emotional, and Social Impacts

Numerous studies have established the extreme psychological and emotional harm caused by catfishing on its victims. As per attachment theory, victims have been found to develop anxiety, depression, and trust issues that are transferred to future online relationships [58].

In addition, a study [53] has also suggested the specific vulnerabilities of sexual minorities, namely in rural areas, in using online dating sites. Lauckner et al. investigated the online experiences of rural sexual minority men, and catfishing was found particularly prevalent. Their study suggests that rural isolation and absence of social support contribute to increased risk of being victimized by deception in online dating site communities. Participants reported such catfishing attempts were commonly accompanied by harassment, emotional abuse, and sexual coercion that were largely unreported out of shame due to and fear of being revictimized. This study reveals how geographic and social isolation enhance vulnerability to risk of catfishing, and rural sexual minorities are at especially high risk of deceptive perpetrators in online dating site communities.

On the other hand, Caspi et al. [16] investigated catfishing personality traits and identified impression management and narcissism as predictors of catfishing perpetration. Their study confirms that catfishers are characterized by a social manipulation tendency, which is instigated by the desire to project an idealized self and enhance perceived mate value.

Another study looked at how catfishers exploit vulnerabilities such as emotional dependence and loneliness to add to the psychological damage that is suffered by the victims [55]. Research on romance fraud on older adults identified that they subject older adults to unreasonable emotional and financial demands and also highlighted the need for more support frameworks and awareness to protect the older population from online fraud [85].

Further rigorous analysis [81] also investigated the psychological motivations of catfishers and victims, using both automated linguistic analysis (LIWC) and thematic analysis to provide an overall picture. It theorizes that catfishers are motivated by a desire for amusement, emotional intimacy, or idealized self-image through deception. For victims, emotional responses such as suspicion, love, and extreme upset highlight the emotional exploitation involved in catfishing. The study also suggests that linguistic analysis programs can be effective at detecting patterns of deception.

Based on the psychological foundation of catfishing, Mosley et al. [58] explore how insecure attachment patterns of trust and intimacy deficits can compel individuals to engage in internet deception as a way to fulfill unmet emotional needs. Older adults are particularly vulnerable due to their trusting nature and low digital literacy levels, making them the ideal target for financial exploitation. Older adults lost a minimum of \$43 million in wire transfers and related payments, according to the FTC's 2021-2022 Protecting Older Consumers Report [65]. Such findings indicate the importance of comprehending psychological vulnerabilities to create more effective prevention strategies.

2.3.2 Motivations Behind Catfishing

Motivations behind catfishing have been studied in depth. Kristy et al. [66] enumerate escapism, loneliness, and validation-seeking as prime motivations. Following on from this, there is a study that discusses how individuals construct idealized online personas while attempting to form emotional intimacy and fulfill unmet needs [81]. This research highlights how catfishers often practice deception to project an idealized self or compensate for deficits in real life. This [66] also highlights how computer-mediated communication allows individuals to manage their interaction with precision, avoiding immediate scrutiny and allowing for prolonged deception.

Along with psychological and individual reasons, sociocultural factors have also been identified as primary motivators of catfishing. Manzanilla et al. [63] examine the intersection of cancel culture and cyber deception, arguing that individuals may adopt fake online identities not only for validation or emotional nurturing but also to evade reputation loss or public judgment. The study hypothesizes that social censure anxiety, particularly in exceedingly visible online spaces, may be at once a disincentive and an incentive for such behavior. Cancel culture in this case is a double sword as in while it punishes the offender, it could also trigger some users to conceal themselves behind pseudonyms to escape retaliation.

In addition, Manzanilla et al. [63] emphasize how social media sites like Twitter [84] and Instagram [79] are public spaces of moral judgment, where viral speech can cause instantaneous and widescale social backlash. These processes demonstrate how social pressures not internal to the self blend with internal motivations, repeating catfishing as coping strategy and means of digital risk management.

2.3.3 Detection and Prevention Mechanisms

Several works have been done on preventing and detecting catfishing. Digital literacy initiatives and real-time monitoring systems are emphasized by Tsikerdekis and Zeadally as prevention mechanisms against deception risk [37]. Similarly, social media studies prove that stricter verification processes can be a prevention measure to discourage catfishing [70]. On the other hand, Hancock et al. explore the challenge surrounding deception detection in asynchronous online communication, with all its complexities of identifying fake behavior in online interactions. According to research [18], the absence of real-time oversight in online settings permits catfishers to construct detailed deceptions.

The paper [70] describes how technology has helped amplify the problem of catfishing and romance fraud. While the authors say that the internet has allowed users to take on pseudonyms easily, it has also created online impersonators who have perfected the art of using the science of user psychology to lure victims into their trap. Romance scams, which directly stem from catfishing, cost consumers over \$730 million in the year 2022 alone, and nearly 70,000 consumers filed a complaint with the FTC [65]. Furthermore, it identifies the urgent need for prevention measures, e.g., user education, improved verification methods, and feedback mechanisms in real-time.

Also, Wani et al. [49] talk of widespread use of fraudulent profiles on social network-

ing sites, which are now a common tool of fraud like catfishing schemes. They believe that existing legal frameworks are typically inadequate to address the complexities of deception online, leaving victims with little recourse to obtain relief. Nurse [55] investigates the psychological factors that drive such behavior, highlighting how perpetrators take advantage of human vulnerabilities such as trust, emotional isolation, and social manipulation. To address these risks, Nurse [55] recommends preventive measures like biometric verification and mandatory video interactions, which could increase the difficulty of creating fake identities. Furthermore, Nurse brings to light the significance of automated messages that remind individuals about suspicious behavior, such as contradictory or unclear information, as a way to reduce the possibility of falling prey to catfishing.

2.3.4 Implications for Digital Security and Future Research Directions

The described research in entirety paints the multidimensional nature of catfishing and its effects on the victims and why there is a necessity for effective detection mechanisms. This research [59] broadens the understanding of how anonymity in online spaces enables deception. These studies emphasize the importance of addressing the psychological and behavioral aspects of catfishing through enhanced real-time monitoring and user education. Developing solutions that integrate behavioral analysis and user feedback could provide a comprehensive approach to reducing the risks associated with catfishing and fostering safer online interactions.

While considerable research has explored catfishing in the contexts of online deception, identity fraud, and digital trust, much of the existing literature remains focused on the Western perspectives, online dating platforms, and the psychological motivations of perpetrators. However, there is a notable gap in understanding how catfishing manifests in developing digital societies such as Bangladesh, where rapid internet adoption intersects with deep-rooted cultural values, social norms, and varying levels of digital literacy.

This study addresses that gap by examining catfishing within the Bangladeshi context, considering both technological and socio-cultural dimensions. Unlike previous work that predominantly centers on individual psychological factors, this research integrates Human-Computer Interaction (HCI) principles to examine how platform design, user behavior, and digital literacy influence susceptibility to catfishing. It further contributes empirical insights by capturing firsthand experiences from Bangladeshi victims through both surveys and qualitative interviews. By doing so, this study not only enriches the global discourse on catfishing but also lays the foundation for region-specific prevention strategies and platform-level safety interventions tailored to emerging digital environments.

Work Plan

The overall research is divided into three major phases: Pre Thesis 1, Pre Thesis 2, and Final Defence, with each phase helping us get a deep insight into catfishing as well as testing out design prototypes for potential solutions to the problem. The breakdown of work in the three phases can be seen in Figure 3.1. This breakdown ensures a well-organized and methodical approach to studying catfishing in Bangladesh. Each phase is designed to build upon the previous one, integrating theoretical foundations, empirical data collection, analysis, and practical recommendations.

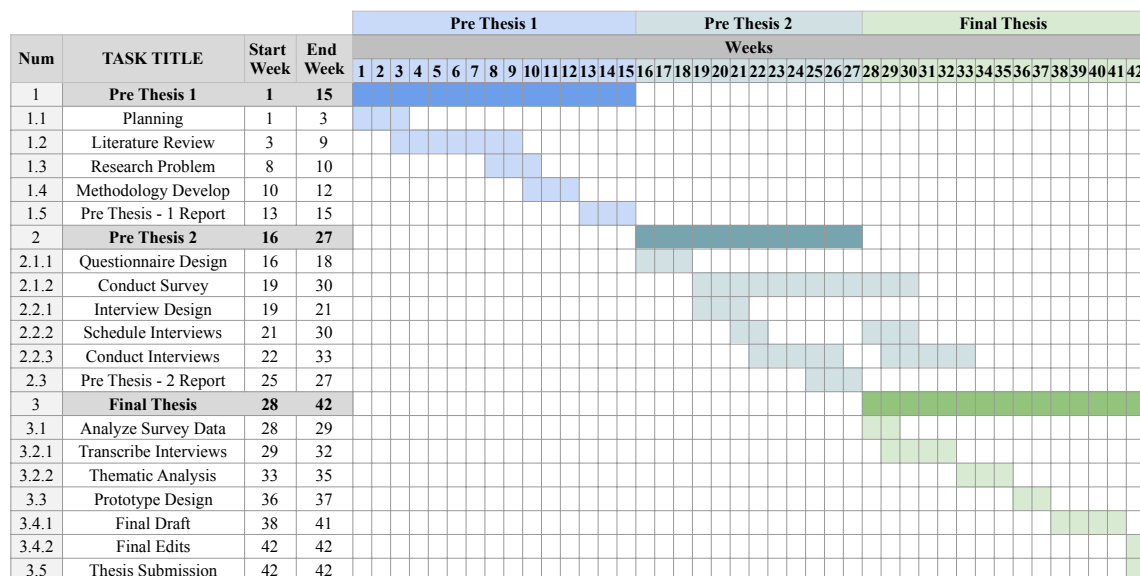


Figure 3.1: Overview of the work plan, detailing the phases and tasks for the thesis

Phase 1: Research Planning and Methodology Development

The first phase of this research focuses on establishing a strong foundation through an extensive literature review, refining the research problem, and developing an appropriate methodology. The initial step involves carefully planning the scope of research by defining the objectives and identifying key areas of focus, including demographic factors, online behaviors, and privacy awareness related to catfishing. A comprehensive literature review is conducted to explore previous studies on online deception, trust

in digital interactions, and user vulnerability, particularly in the context of Bangladesh and other developing countries. The literature review not only helps in identifying gaps in existing research but also provides insights into theoretical frameworks that can be used to structure the study.

Once the problem under study is clearly defined, then methodologies are crafted in a manner to make the collection of data relevant to the study objectives. A mixed-methods approach is adopted, integrating both quantitative and qualitative techniques to gain a holistic understanding of catfishing in Bangladesh. A structured survey is designed to capture social media behavior, awareness regarding privacy, and experiences with catfishing, while semi-structured interviews are conducted to gather deeper, individual experiences of victims. At this stage, great care is taken to ensure ethical considerations, particularly in maintaining the confidentiality of respondents, especially those who have been victims of online deception. The outcome of this phase is a comprehensive Pre-Thesis 1 Report, which includes a literature review, research problem, theoretical framework, and proposed methodologies, serving as a blueprint for the next stage.

Phase 2: Data Collection

Building upon the research design established in the previous phase, this stage focuses on empirical data collection through surveys and interviews, followed by thorough data analysis. The first step involves carefully developing the survey to ensure it effectively gathers relevant information while remaining user-friendly and accessible. To encourage broad participation across diverse demographics, the survey is created in both English and Bangla. The questions explore participants' social media usage, interactions with strangers, familiarity with privacy settings, as well as their direct and indirect experiences with catfishing. Once finalized, the survey is distributed via social media platforms, university networks, and professional communities to maximize participation. Throughout the data collection process, careful attention is given to monitoring response rates to ensure a well-balanced and representative sample across different age groups, genders, and geographical locations.

Simultaneously, in-depth interviews are carried out with a selected group of participants who have firsthand experience with catfishing. These interviews explore their emotional and psychological responses, awareness of online safety, and coping strategies. Once the interviews are completed, the qualitative data are transcribed. This phase concludes with the Pre-Thesis 2 Report, which presents a basic analysis of survey findings and insights from the interviews, further setting the foundation for the final phase of the research.

Phase 3: Analysis and Prototype Design

After collecting the survey responses, the data is cleaned and analyzed using statistical methods to identify key trends. Correlation analysis is conducted to examine relationships between social media usage frequency, demographic factors, and susceptibility to catfishing. This analysis uncovers patterns of vulnerability and associated risk factors. Later on, the interview transcripts are thematically coded to identify recurring patterns in deceptive behaviors, trust-building tactics used by catfishers, and the long-term impact on victims.

The phase shifts from data analysis to practical application, where the research findings help shape real-world solutions and recommendations to enhance online security. Based on insights from the surveys and interviews, a range of recommendations are developed. These include strategies for social media platforms to strengthen user protection, awareness programs to educate individuals about online risks, and clear guidelines for reporting catfishing incidents. Additionally, potential interventions are considered, such as an education module, an online awareness campaign, or review of existing trust and identity verification practices on social media platforms.

Recommendations are also taken from experts to determine feasibility and potential impact of our prototype. Then, a small-scale user study is conducted to generate feedback against the proposed prototype in terms of whether they are representative of actual-world digital activity and properly address security issues. Feedback from both statistical and qualitative analysis is then utilized to generate an overall final research report that provides a comprehensive assessment of user attitudes, vulnerabilities, and behavior within digital contexts.

The last actions in this phase involve composing the final thesis, such as supervisor and co-supervisor comments and revising where necessary. Upon completion, the thesis is handed in for evaluation. This phase closes the research process while offering valuable information regarding the risks of catfishing in Bangladesh through digital trust mechanisms and user experiences from an HCI perspective.

3.1 Research Methodology

The research methodology consists of several steps as shown in Figure 3.2.

3.1.1 Overview

This study adopted a mixed-methods approach, combining quantitative feedback through surveys with qualitative in-depth interviews in order to gain a composite understanding of catfishing in Bangladesh. Following the principles of Human-Computer Interaction, this study emphasized examining usability, perceived-user experience, measures of trust, and estimation of risk of communication on cyberspace. Through statistical and thematic analysis[15] of survey-based analysis of qualitative interviews, this study further explores how users interact with fraudulent profiles on cyberspace. Through these approaches, behavioral patterns, biases in trust development, and emotional effects of catfishing could be determined. The study is well planned with regard to inclusivity, accessibility, and ethics, in a manner that it was feasible for participants from diverse demographics to respond to the study in an accessible and non-intrusive way.

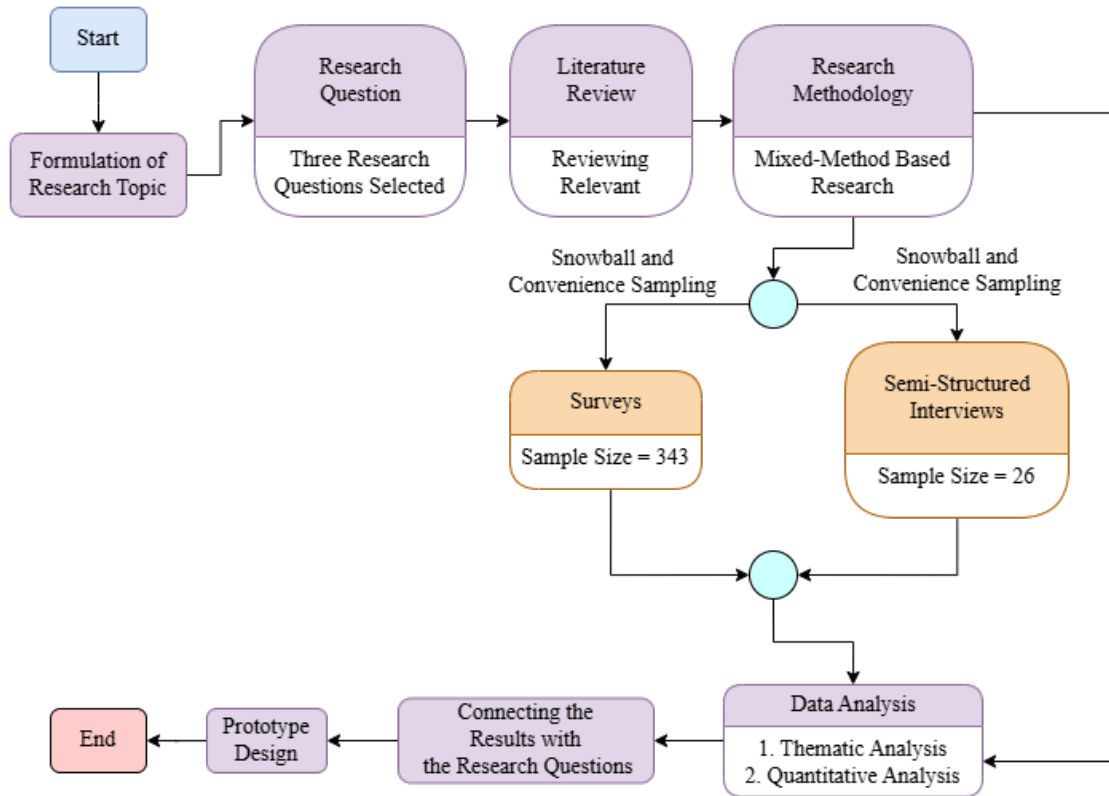


Figure 3.2: Overview of the research methodology

3.1.2 Research Design

A mixed-methods design was used to reveal both broad behavioral patterns at scale and rich experiential detail. There are two main parts to the study:

1. **Survey-based Quantitative Research:** The users' behavior, their knowledge about catfishing, online trust models, and reporting habits are outlined by means of the data obtained from the survey.
2. **Qualitative Interviews:** Thematic details about personal victim experiences, emotional responses, and coping mechanisms are understood using the gathered interviews.

This design allowed our research to combine statistical significance and qualitative richness and thus ensuring a comprehensive insight into user experiences of catfishing. The combination of the two approaches aligns with HCI-oriented methodologies, particularly in examining user attitudes, risk perception, and trust frameworks in online environments.

3.1.3 Data Collection Methods

To create a detailed understanding of how individuals in Bangladesh understand and respond to catfishing, a mixed-methods design was employed, in which quantitative surveys were supplemented by qualitative interviews. This allowed the research to capture general trends of behavior alongside detailed experiential data, offering a comprehensive investigation of the phenomenon. The survey provided statistical data on user

demographics, trust actions, and catfishing knowledge, while the interview provided insight into emotional response, coping strategies, and perceptions of online deception.

Survey Design and Distribution

The survey was made available with Google Forms [90] for easy access and mobile usability. The survey was organized in English and Bangla to suit the language requirements of Bangladeshi users, reducing the language barrier and making the interaction easy. This consideration for language aligns with usability guidelines of Human-Computer Interaction (HCI) [28] by maintaining accessibility and user convenience as the focus.

Using a combination of convenience sampling [25] and snowball [3] sampling, 343 responses were collected. Initial participants were originally recruited through social media platforms such as Facebook [77] and Discord [75], in addition to personal networks such as family and friends. The participants were then invited to forward the survey among their networks, facilitating natural expansion and diversity within the respondent group. This sampling method allowed for an assortment of digital literacy levels, social media habits, and general awareness of online threats to be captured.

In an effort to honor participant autonomy, all questions on the survey were voluntary and respondents could omit any that they felt were personal or difficult to answer. This is a user-centered design strategy typical in HCI studies, where participant comfort and control are privileged throughout the data gathering process.

Interview Procedures

Semi-structured interviews complemented the survey to collect qualitative data on user experiences with catfishing. Participants chose between WhatsApp [87] and Google Meet [88] according to their convenience and comfort. Each interview lasted approximately 15–20 minutes, and participants were free to communicate in English, Bangla, or a mixture of both, facilitating natural expression and richer data.

In line with ethical protocols in HCI research, informed consent was carefully obtained before each interview using a detailed consent form based on the World Health Organization's qualitative research template [86]. Participants were required to read and digitally sign this form. When participants expressed reluctance or preferred not to read it themselves, the researcher offered to read the consent aloud, ensuring full understanding and voluntary participation without pressure.

Only audio recordings were made during interviews to protect privacy and foster a relaxed environment conducive to honest and open responses, reflecting ethical standards in user-centered research.

Since the interviews were conducted in both English and Bangla, often mixing the two, all recordings were transcribed fully into English before analysis. The transcription was required to facilitate rigor and consistency in the process of thematic analysis, which identified emergent themes relating to emotional responses, coping mechanisms, deceptive behavior and trust online.

3.1.4 Ethical Considerations

Ethical integrity was a fundamental part of this research. It ensured privacy and confidentiality of the respondents all times. The informed consent of all respondents was requested before they were engaged in a survey and interviews. Their information was assured to be anonymous and stored in safe format in all research deliverables. As part of upholding best practices in digital research ethics, audio recordings were stored safely and programmed for destruction six months after publication.

In addition, every question was planned carefully to be non-intrusive and emotionally respectful so that no unnecessary distress was caused to participants. By giving respondents the choice to skip questions or withdraw at any point, research followed HCI guidelines that value user control and ethical usability.

3.1.5 Data Analysis

Quantitative Analysis

The survey data was analyzed using descriptive statistics [17] to identify patterns and relationships. Demographic variables such as age, gender, education level, and geographic location were examined alongside trust mechanisms, social media usage, and digital literacy to assess their influence on susceptibility to catfishing.

The responses from the Likert scale [1] analysis were processed to evaluate user perceptions of online deception, privacy, and identity verification, contributing to broader discussions on digital trust in HCI research.

Thematic Analysis

Thematic interviews were thematically coded [15], a common convention of HCI-inspired qualitative research. The interviews were translated into English, specifically since most of them were conducted in Bangla or in a mixture of both languages. The transcripts were read multiple times, and responses were coded consistently based on emerging themes around catfishing experiences. From thematic analysis, the study obtained experiential and in-depth understanding of how people perceive trust, deception, and digital vulnerability during online interaction.

3.1.6 Prototype Design

Based on the analysis findings, various initial design concepts were established. These design concepts were further iterated through expert feedback sessions, stressing usability and cultural adaptability in the context of Bangladesh. A high-fidelity interactive prototype was then made through the use of Python Flask [22]. It has features such as trust score indicators, verification requests, emotional manipulation warnings and easy reporting options.

Chapter 4

Understanding Catfishing through Survey Analysis

In this chapter, a survey-based research on catfishing in Bangladesh is presented in detail. The survey aimed to elicit empirical experiences, behavioral patterns, and attitudes towards online deception. By analyzing surveys from a heterogeneous group of participants, the study explores how different demographic factors might influence vulnerability to catfishing, emotional and monetary losses for victims, and the effectiveness of current prevention strategies. Additionally, the findings provide insights into digital trust mechanisms and reporting practices that highlight the gaps in awareness and security practice. The chapter sets the stage for further qualitative exploration by situating the prevalence and impacts of catfishing within the backdrop of the evolving digital landscape of Bangladesh.

4.1 Survey Design and Implementation

To research catfishing in Bangladesh, a user-centric survey was designed and shared through Google Forms [90]. The survey employed Human Computer Interaction principles to ensure usability and accessibility first, and on interaction dynamics as a way of inducing diverse participant inputs. The questions in the survey employed bilingual presentation by combining English and Bangla because most of the Bangladeshis involved were accustomed to conveying themselves in their own language. Such bilingual presentation of all the questions avoided confusion while allowing accurate response. This therefore allowed for cultural and language-based sensitivity. The survey collected 343 valid responses, which provided an adequate basis for researching the phenomenon. All the participants were free to leave out any of the questionnaire items, since participant autonomy received top priority. The survey instrument employed both Likert scale items [1], designed for quantitatively measuring behavior patterns and trust mechanisms, as well as open-ended questions which asked for elaboration on people's own experience of Internet deceptions. Such mixed format allowed for both quantitative measurement as well as qualitative insight through a single data collection tool.

Survey items were developed to align with the research objectives so that digital trust, user interactions, and attitudes towards deceptive online behaviors could be measured. Demographic items gathered contextual data such as age, gender, digital lit-

eracy, and social media usage patterns that enabled examination of variation in cat-fishing susceptibility among segments of users. Participants described their personal social media usage and also indicated their means of verifying others and identifying deception in online interaction. Further questions about reporting mechanisms and internet security legislation were administered in the survey in order to determine knowledge and also the obstacles that prevent individuals from reporting cases of cat-fishing. The survey maintained ethical and respectful status by avoiding excessively personal questions with the motive of protecting participant comfort as well as encourage open responses.

To maximize participation, the survey was distributed across various channels using convenience [25] and snowball sampling methods [3]. Firstly, convenience sampling was used to get participants from academic settings, social media platforms, and online communities. Later on, snowball sampling was also used to distribute the survey among other individuals through their personal networks. The survey was distributed to known contacts through Facebook groups [77] and Discord servers [75] as well as other social media platforms to obtain diverse participants and also to maximize the result. This strategy helped in capturing responses from individuals with varying levels of digital literacy, online behaviors, and social media engagement. As a result, this approach contributed to making the dataset more representative of the broader population.

The survey was optimized for mobile devices because Bangladesh shows a growing trend of smartphone usage in online communication. Participants received guaranteed protection of their privacy along with anonymity as precautions against social desirability bias. The survey examined users' online activities alongside their emotional responses and protective behaviors, aiming to understand how individuals manage trust-related challenges, identity protection, and digital threats during online interactions. Additionally, it provided valuable insights into HCI-related concerns arising from experiences of online deception.

4.2 Participant Demographics

Survey participants represented a diverse demographic profile in terms of age, gender, region, education, and employment status, as detailed in Table 4.1. The majority of respondents (46.6%) were between 18 and 24 years old, followed by 24.5% between 35 and 44, and 21.6% between 25 and 34. Additionally, 7.3% of participants were aged 45 or above. This wide age distribution enabled the study to explore catfishing experiences across multiple life stages and levels of digital exposure.

Category	Demographic	Count	Percentage
Age	18-24	160	46.6%
	25-34	74	21.6%
	35-44	84	24.5%
	45 and above	25	7.3%
Gender	Male	199	58%
	Female	130	37.9%
	Prefer not to say	14	4.1%
Location	Dhaka	149	44.2%
	Chattogram	77	22.8%
	Rangpur	25	7.4%
	Mymensingh	22	6.5%
	Rajshahi	25	7.4%
	Khulna	20	5.9%
	Barishal	11	3.3%
	Sylhet	8	2.4%
Highest Level of Education	Below High School	14	4.1%
	High School	60	17.5%
	Diploma	28	8.2%
	Bachelor's	182	53.2%
	Master's	50	14.6%
	PhD	8	2.3%
Employment Status	Student	176	51.6%
	Employed	122	35.8%
	Unemployed	34	10%
	Retired, Business, Others	9	2.6%
Relationship Status	Married	94	27.5%
	Single	146	42.7%
	In a relationship	45	13.2%
	Looking for a relationship	40	11.7%
	Prefer not to say	17	5%
Device Usage	Less than 1 year	8	2.4%
	1-5 years	65	19.2%
	5-10 years	112	33%
	10+ years	154	45.4%

Table 4.1: Demographic data for survey participants (n = 343)

Gender diversity was also reported, where 58% reported being male and 37.9% reported being female, with 4.1% not wanting to report their gender. This diversity provides a more comprehensive view of how online deception would be perceived in different gender identities.

Geographically, responses were distributed across Bangladesh's major divisions, with the highest share coming from Dhaka (44.2%) and Chattogram (22.8%). These urban centers have more internet connection and online participation, which would have impacted participation levels. Interestingly, the dataset is complemented by repre-

sentation from places like Rangpur (7.4%), Mymensingh (6.5%), and Rajshahi (7.4%), giving a glimpse of life on the internet beyond urban and megacity settings.

Educational attainment ranged from diploma and secondary school graduates to bachelor's, master's, and Ph.D. levels of education, reflecting a broad range of digital literacy skills. Likewise, there was diversity in employment status such as students (51.6%), working respondents (35.8%), and other groups such as unemployed or self-employed respondents. The diversity reflects the widespread relevance of catfishing and digital trust issues across socio-economic classes.

Overall, the demographic heterogeneity of the sample population enhances the external validity and contextual richness of the findings. It also makes it clear that digital literacy initiatives and protective actions must be fine-tuned to meet the unique requirements of different user segments, particularly in regions where internet connectivity is accelerating.

4.3 Key Findings

The survey provided rich data on the prevalence and dynamics of catfishing in Bangladesh, revealing victim experiences, behavioral patterns, and systemic dynamics. The findings address the intricate interplay between trust, identity, and emotional well-being among online relationships. They also emphasize the applicability of Human-Computer Interaction (HCI) to explore the ramifications of platform design, user conduct, and digital environments in such relationships.

4.3.1 Victims and Non-Victims of Catfishing

Participants were divided into victims or non-victims based on whether they had responded “yes” or “no” to the question, “Have you ever interacted online with someone whose identity you later found to be fake?” Victims were those participants who had confirmed experiencing fraudulent profiles, and who had suspected the truthfulness of a profile but were unable to determine if it was genuine or not. The non-victims were individuals who never asked someone's identity or had only suspicious meetings without any definite evidence of fraud.

The survey revealed that 43.2% of respondents reported being victims of catfishing, indicating a substantial prevalence within the sample. The remaining 56.8% did not consider themselves victims. Among these non-victims, 9.97% expressed no suspicion about any profiles they interacted with, while 51.17% reported having doubts or suspicions but lacked definitive confirmation. Victims were predominantly younger participants aged 18 to 24, who also reported higher levels of social media activity and more frequent interactions with strangers. In contrast, non-victims were often older individuals. Specifically, 24.5% were in the 25 to 34 age group, and 7.3% were aged 45 or above. Many of these participants attributed their safety to cautious behavior and limited online engagement.

4.3.2 Social Media Behavior and Vulnerabilities

Social media platforms emerged as the primary environments for catfishing, with 76.9% of respondents frequently using Facebook, followed by WhatsApp (63.7%) and

Instagram (54.7%), which can be seen in Table 4.2. Many respondents reported extensive daily engagement, with 15.5% spending more than six hours on social media and 30.5% spending 4-6 hours. This extended usage aligns with previous HCI research, suggesting that higher engagement levels correlate with reduced cognitive vigilance [5] and increased reliance on heuristic decision-making [8].

Moreover, younger participants, particularly those aged 18-24, were significantly more likely to interact with strangers online, with 23.9% acknowledging rare interactions, 22.6% interacting in specific situations (e.g., group projects, work, gaming), and 13.8% engaging occasionally with unknown individuals. This behavior was driven by factors such as curiosity, mutual friends, and perceived shared interests, but it often increased vulnerability to catfishing.

Platform	Count	Percentage (%)
Facebook	263	75.1%
WhatsApp	218	62.3%
Instagram	187	53.4%
Telegram	98	28.0%
Snapchat	88	25.1%
TikTok	76	21.7%
Others	26	7.4%
None	17	4.9%

Table 4.2: Most frequently used social media platforms among 343 respondents. Multiple selections allowed.

Trust indicators, such as profile pictures, mutual connections, and shared hobbies, were commonly used to assess the authenticity of profiles. However, 67.5% of respondents indicated that mutual connections were their primary trust signal, followed by 55.7% who used clear profile pictures and 54.7% who checked for consistent profile details. Despite these efforts, these indicators were often insufficient to detect fake profiles, with participants frequently falling victim to deception due to their reliance on such cues. From this, it can be understood that many of them rarely verified the authenticity of profiles beyond these surface-level cues. The results indicate that relying too much on profile pictures and curated timelines creates a major gap in trust-building on these platforms.

4.3.3 Awareness of Catfishing and Digital Security

Awareness of catfishing was relatively low among participants, with only 37.6% correctly recognizing the term and its meaning, while 27.6% had heard the term but did not fully understand it, as shown in Table 4.3. Awareness gaps were particularly pronounced among older respondents and those with lower educational attainment.

Regarding digital security laws in Bangladesh, the data revealed a concerning lack of knowledge. Specifically, 14.4% of respondents indicated they were “Not familiar at all” with such laws, and 8.5% were unsure whether these laws even existed. Only 7.6% reported being “Very familiar” with digital security regulations, highlighting the need for greater public education on this topic.

Response	Count	Percentage (%)
"Yes, I know what it means"	128	37.6%
"Yes, but I don't know exactly what it means"	94	27.6%
"No, I have never heard of it"	90	26.5%
"I'm not sure"	28	8.2%

Table 4.3: Survey responses on familiarity with the term "Catfish" (n = 343)

These findings also show a lack of education on online safety and legal protections and thus making users vulnerable to cyber threats like catfishing. Moreover, this gap in knowledge emphasizes the need for better digital education and accessibility among localized resources so that users can navigate online spaces safely.

4.3.4 Preventive Practices and Behavioral Trends

Preventive practices among respondents varied considerably. Some participants actively utilized privacy settings and scrutinized profiles for inconsistencies, while others preferred to avoid interacting with strangers altogether. Younger respondents tended to rely on technological tools such as blocking or reporting suspicious accounts, whereas older participants primarily depended on personal judgment and past experiences.

The survey also indicated that 68.8% and 68.5% of respondents included personal details such as full names and profile pictures on their social media accounts, potentially increasing their vulnerability to catfishing attacks.

Urban respondents, particularly those from Dhaka and Chattogram, demonstrated higher digital literacy and were more likely to use advanced privacy settings. However, they also faced greater exposure to catfishing attempts due to their extensive online engagement. In contrast, participants from semi-urban or rural areas reported lower exposure but often lacked the knowledge to effectively safeguard themselves.

4.3.5 Emotional and Psychological Impacts

The emotional toll of catfishing was evident among victims, who frequently reported feelings of betrayal, embarrassment, and anxiety. From Table 4.4 it can be seen that 57.7% of respondents cited a loss of trust in people online as a significant consequence of catfishing experiences, while 32.9% experienced emotional distress or anxiety. Additionally, 29.5% of victims reported financial losses, and 27.5% described damage to relationships with friends or family. These findings align with existing research on the psychological impacts of online deception, emphasizing the need for empathetic support systems within digital platforms.

Repercussion	Count	Percentage (%)
“Loss of trust in people online”	86	57.7%
“Emotional distress or anxiety”	49	32.9%
“Financial loss”	44	29.5%
“Damage to relationships with friends or family”	41	27.5%
“No significant repercussion”	40	26.8%

Table 4.4: Reported repercussions of catfishing experiences (n = 149). Multiple selections allowed.

Non-victims of catfishing were not immune to its psychological effects. Many reported heightened vigilance and a pervasive sense of distrust toward online interactions, even without direct victimization. This increased caution often manifested in more guarded behavior on social media platforms, such as limiting personal disclosures or avoiding unfamiliar contacts. For some, these changes contributed to a reduced overall engagement with digital communities, highlighting the broader impact of catfishing on online social dynamics beyond those directly affected.

4.3.6 Reporting Behavior and Systemic Gaps

The survey revealed a significant issue with low reporting rates among catfishing victims. From Table 4.5 it can be seen that only 41.7% of those who experienced catfishing reported the incidents to the platforms or to the authorities. A larger portion (42.2%) chose not to report because they were uncertain about the reporting process or were skeptical regarding its effectiveness, as in whether it will actually work or not. Additionally, 16.1% of respondents admitted they didn’t know how to report such incidents further highlighting a critical lack of awareness regarding overall cybersecurity.

Response	Count	Percentage (%)
“No, I did not report them”	60	40.3
“Yes, I reported them to the platform”	43	28.9
“Yes, I reported them to the authorities”	19	12.8
“I’m not sure how to report them”	24	16.1
“I couldn’t report because of my family”	3	2.0

Table 4.5: Survey responses about reporting catfishing incidents (n = 149)

Low reporting rates can also be attributed to social stigma and the overall sensitive nature of catfishing experiences. Victims may fear judgment, embarrassment, or cultural taboos related to online interactions which makes them hesitant to come forward. This highlights the need to understand social and psychological barriers that stop victims from seeking help, and this might lead to better solutions for these challenges. The survey findings highlight the complex relationship between trust, digital literacy, and emotional resilience in navigating online spaces. These insights emphasize the need for combined efforts in education, technology, and policy to tackle catfishing in Bangladesh effectively.

4.4 Data Analysis and Insights

The survey data provides a detailed understanding of how demographic and behavioral factors play an important role on influencing online trust, risk exposure, and the impact of catfishing in Bangladesh. These insights go beyond just surface level observations by shedding light on systemic vulnerabilities in digital communications and emphasizing the need for targeted interventions. By analyzing demographics, social media habits and trust factors this study identifies the key risks, emotional impacts, and barriers to reporting catfishing.

4.4.1 Influence of Demographics on Catfishing Susceptibility

The survey revealed a significant link between demographic factors and susceptibility to catfishing. Among the 345 respondents, 149 identified themselves as victims of catfishing (including those who found identity fake or doubted it), highlighting the widespread nature of online deception, representing 43.2% of the total survey participants.

The age group most affected was 18-24 years, with 46.6% of respondents in this range reporting higher levels of social media engagement and frequent interactions with strangers, thus increasing their vulnerability to deceptive or fake profiles. Among the victims, 58.3% were aged 18-24, showing that younger users are affected the most. Older respondents, aged 35 and above (total 31.5% of all respondents), showed more cautious behavior by avoiding interactions with strangers. However, this caution was counterbalanced by a lower familiarity with digital security tools and privacy settings, leaving them vulnerable to other online scams.

The survey also highlighted gender differences in risk perception and online trust among victims. Of the 149 catfishing victims, 94 (63.1%) were male, while 53 (35.6%) were female. Two individuals preferred not to state their gender. Male respondents, therefore, appear to face a higher risk of encountering catfishing among victims. Female respondents were more cautious but expressed greater concern about online deception, which indicates a higher perceived risk despite lower levels of direct engagement with strangers.

In conclusion, susceptibility to catfishing depends on online activity, digital skills, and demographics, and this further highlights the need for targeted awareness programs for different user groups.

4.4.2 Emotional, Social, and Financial Consequences of Catfishing

The survey revealed that catfishing profoundly impacts victims, leading to significant emotional, social, and, in some cases, financial repercussions. A substantial majority of victims, 57.7%, reported a profound loss of trust in online interactions. Beyond this, emotional distress or anxiety was experienced by 32.9% of victims, while 27.5% noted adverse effects on their relationships with friends or family. These findings highlight that the consequences of catfishing extend beyond the initial digital deception, leaving lasting marks on interpersonal trust and emotional well-being.

The experience of catfishing also prompted significant shifts in online behavior. Among victims, 38.5% became more skeptical of new online interactions, and a consid-

erable 24.7% consequently reduced their overall social media activity. This behavioral adaptation underscores a heightened caution in future digital engagements.

While emotional and psychological impacts were prevalent, financial exploitation was also noted. Financial loss was indicated by approximately 29.5% of the victims, with some cases consisting of fraud or unauthorized release of personal information. This highlights that while less prevalent than emotional damage, financial deceit is a considerable problem for a notable percentage of catfishing victims.

In combination, these findings emphasize the need for comprehensive support services, including mental health assistance, specialized digital safety training, and response intervention. These are needed to enable victims to heal from the multi-layered emotional, social, and economic harm inflicted through catfishing encounters.

4.4.3 Leveraging Findings for Prevention and Support Systems

The survey findings present broad shortages in public awareness, digital literacy, and victim support, indicating a sharp need for increased prevention mechanisms and availability of assistance mechanisms. Due to the prevalence of catfishing, only 41.7% of the victims reported the cases, either to social media platforms or to the relevant authorities.

Reasons for not reporting included:

- Fear of judgment or embarrassment (43.6%)
- Lack of awareness about how or where to report (32.1%)
- Distrust in whether reporting would result in any action (21.8%)

These patterns suggest that stigma, uncertainty, and institutional distrust act as strong deterrents, leaving many victims without recourse or support. Cultural norms and privacy concerns further compound these challenges, particularly in a context where online safety is still an emerging topic.

The issue is exacerbated by limited knowledge of digital security laws. While only 7.6% of respondents claimed to be “very familiar” with relevant legislation in Bangladesh, 14.4% reported having no familiarity at all, and 8.5% were unsure whether such laws even existed. These findings point to a critical gap in digital and legal awareness, which reduces the ability of users to protect themselves or take informed action when targeted.

Based on the survey data, three core priorities emerge for developing better prevention and support systems:

1. **Digital Literacy and Awareness Campaigns:** Comprehensive public education is essential to teach users how to recognize red flags, verify identities, and use privacy settings effectively. Special focus should be placed on reaching marginalized and less tech-savvy populations.
2. **Accessible Victim Support:** Platforms and institutions should ensure the availability of accessible and non-judgmental support services, such as professional counseling, peer support networks, and legal assistance. These resources can help encourage victims to seek help without fear of stigma or reprisal.

3. **Streamlined and Transparent Reporting Systems:** Social media companies and local authorities should work together to create clear, simple, and visible reporting mechanisms. Making it easier to report catfishing can increase accountability and act as a deterrent to perpetrators.

In summary, addressing catfishing requires a multidimensional approach involving education, technological improvements, and systemic reforms. By improving user knowledge, removing barriers to reporting, and building supportive infrastructure, Bangladesh can take meaningful steps toward a safer and more trustworthy digital environment.

Chapter 5

Unmasking the Impacts Through Voices from the Deceived

This chapter presents the qualitative analysis of the catfishing phenomenon through the victims' experiences. By understanding the emotional, social, and financial damage caused by being deceived over the internet, the study managed to depict the psychological impact of these participants through semi-structured interviews. The chapter seeks to understand how one becomes a catfishing victim, how catfishers mentally manipulate their targets, and the wider implications on trust and online interactions among people. For that purpose, it analyses the other factors that make it difficult for these victims to come forward and report what has transpired with them, as well as attempts to identify and describe the major behavioral changes that occur under the influence of deception. This, together with the thematic analysis encompasses the multi-layered nature of the lives of the victims and forms of catfishing in Bangladesh.

5.1 Interview Methodology

Online interviews were conducted to provide participants with convenient access, adhering to Human-Computer Interaction (HCI) principles of usability and inclusivity. This approach aligns with participant-driven research, ensuring that the interview process was accessible and comfortable for all participants.

The preferred communication tools for virtual interviews were Google Meet[88] and WhatsApp[87]. They were selected on the basis of popularity and accessibility, which made them suitable for the online population of Bangladesh. By using these popular tools, the participants were talking in a familiar space, and there were fewer barriers to communication, ensuring a more open and freer conversation.

Each interview session lasted between 15-20 minutes, which provided the participants with enough time to articulate their experiences without becoming cognitively overwhelmed or exhausted, and thus potentially compromising the quality of their responses. To facilitate participants' comfort and make the interview process accessible, each session provided the participants with a choice between Bangla and English as their language of communication. This choice helped to enable a natural flow of dialogue since it enabled the subjects to reply in the language they felt most comfortable. In order to put a priority on privacy protection and ensure participant comfort, audio recording was the sole recording conducted during the interviews. By doing this, participant nervousness was avoided, and open and free discussion was facilitated.

The audio-only method has been validated in human-computer interaction studies as a method of mitigating digital interaction intrusiveness and facilitating trust-based communication.

As follows HCI research ethics, informed consent was first acquired from all individuals using a digitally signed document taken from WHO qualitative research guidelines [86]. To allow understanding and voluntary participation, the document was read by or read out for them by us on request. We reminded participants at the beginning of each interview that they could leave out any questions they didn't want or weren't prepared to answer, ascertaining their level of autonomy and comfort.

In terms of data storage and security, all audio recordings were kept secure, with automatic removal after a period of six months from the date of the study conclusion. This was to ensure the privacy of participants and compliance with data protection guidelines, which form an integral component of HCI's approach to communication based on trust. Upon knowing about the way the data was being stored, participants felt comfortable to share their experiences, knowing well that their privacy was guaranteed throughout the research process. Such practices not only enhanced the quality of data collected but also facilitated the development of an inclusive and comfortable user experience. Ethical protocols were rigorously followed, thereby enabling the maintenance of the participants' trust in the research process.

5.2 Questionnaire Design

The interview questions were also designed to completely evaluate participants' catfishing experiences carefully so as not to overwhelm participants emotionally but remain sensitive to their comfort in response. The design of the questionnaire was in a way that incident-specific questions were presented first, followed by questions of psychological and emotional impact, and lastly questions of coping mechanisms and systemic impediments faced by the victims.

5.2.1 Initial Questions: Investigating the Incident

The first set of questions tried to determine under what conditions catfishing occurred, in terms of the victim-catfish relationship and the initial perceptions of the victim. The questions allowed us to determine how victims initially interacted with the catfisher and what made them believe in the pseudoprofile. By querying the initial interactions, we sought to determine the common catfishing deception methods, including fake profile making and the employing of certain social media strategies. The questions also asked for the mechanisms of gaining trust that catfishers employed in an attempt to make the fake profile appear genuine.

There were also a series of questions used to study how victims recognized early warning signs of danger. We tried to examine how victims recognized warning signs such as inconsistencies in accounts, vagueness regarding personal details, or unusual requests. With this we sought to find out how the early warning signs were interpreted and responded to during online communication, and how the victims felt the situation unfold.

5.2.2 Emotional Development and Psychological Impact

The latter half of the survey discussed emotional development experienced by victims. Questions were set to capture victims' emotional responses as they progressed from trust to attachment and finally to betrayal upon learning of the deceit. By excavating through these stages, the survey facilitated in-depth understanding of the emotional effect of catfishing on victims, which aligns with previous HCI research into the psychological effect of online deception.

Furthermore, this portion of the study also expanded the question to include not only economic damages but social effects such as reputations damaged. An understanding of these broader consequences, beyond emotional harm, presented a whole picture of how catfishing affects lives in more than one way, from financial stability to reputation.

5.2.3 Support Systems and Barriers to Reporting

There was also a section in the questionnaire regarding reporting behavior and support networks, assessing how the victims reacted to the absence of support they had in trying to get help. Leading the questions was obtaining an insight into the barriers to reporting the incidents, including fear of judgment, lack of understanding of the reporting process, and lack of trust in the response of the platforms. The questionnaire also touched on contacting law enforcement and how the victims viewed the effectiveness of authorities in dealing with the catfishing incidents.

It is through these systemic shortcomings that the interview sought to discover why catfishing is able to persist with minimal repercussions, but inflict tremendous financial and emotional damage on its victims. Understanding these obstacles is important in order to enhance victim support systems as well as promote improved protection policies.

5.2.4 Language Preference and Transcription Process

At the start of every interview, the participants were requested to choose the language they would be comfortable with, Bangla or English, for speaking. The majority of the participants chose to speak in Bangla, and some used a combination of Bangla and English throughout the interview. For consistency and ease of interpretation, all the interviews were translated into English for subsequent analysis.

5.2.5 Participant-Centered Design

During the process of interviewing, the questionnaire used a participant-driven strategy, where the participants were open to sharing their experiences in a comfortable and non-judgmental environment. By using this strategy, the study focused on open discourse and gave the participants the opportunity to share their experiences voluntarily. The phrasing of the questions was such that the perspective of the victim remained central, both in terms of the individual narratives and broad systemic issues involved with catfishing.

The systematic approach gave a well-defined framework for obtaining meaningful data that adds to the increasing body of knowledge regarding catfishing as a social phenomenon and the exposure of the vulnerability and behavior adaptation victims undertake after being victimized.

5.3 Participant Selection and Demographic

Our participant selection process was guided by principles of inclusivity and real-world relevance, aiming to capture the diverse experiences of individuals across various backgrounds. Initial participant outreach occurred through a survey component, where individuals had the option to provide their contact information for subsequent interviews. This integrated approach streamlined recruitment and eased the burden on potential participants, aligning with user-centered design principles in human-computer interaction (HCI) that prioritize intuitive system design.

The research employed a two-pronged sampling strategy: initially convenience sampling [25], followed by snowball sampling [3] for interviewee recruitment. Convenience sampling involved getting in touch with those who had voluntarily left their contact details after taking the survey. Snowball sampling then involved using the personal networks of participants to get in touch with other individuals who had been victims of catfishing. The approach was particularly valuable in reaching a wider demographic that had been victimized by this trend, and the multi-faceted approach significantly improved our findings by reflecting the extensive reach of social media networks and improving our understanding of online deception.

In total, 26 individuals were interviewed, 15 females and 11 males. The respondents cut across a variety of ages as well as levels of online engagement. For male respondents, six were between the ages of 18 and 24 years, three were between the ages of 25 and 34 years, two were between the ages of 35 and 44, and one was 45 years and above. For the female participants, eight were aged 18-24 years, four were 25-34 years, two were 35-44 years, and one was 45 years and above.

This age breakdown was important for the purposes of ensuring representation was balanced across age ranges, so that the research could capture the subtleties of how catfishing and online deception affect a range of demographics. Having a varied sample also enabled the examination of how age, gender, and level of digital engagement could be contributing factors in susceptibility to online deception.

The respondents came from different regions of Bangladesh, stretching from large cities such as Dhaka and Chattogram to semi-urban and rural communities. The geographical scope assisted in obtaining information on how catfishing manifests itself in different cultural and social areas. For most respondents, particularly those in urban areas, they were regular users of social media, and in most instances, this made them even more susceptible to catfish activities.

The participants were an assorted cluster of students, professionals, and individuals from different socioeconomic backgrounds. This wide variety of backgrounds gave quality data, capturing the broad experiences of the catfishing victims. The majority of the participants identified various degrees of digital literacy, with some reporting minimal understanding of cybersecurity concerns, indicating the urgent need for additional digital safety education.

Effectively, our participant selection method, which combined convenience and snowball sampling strategically, succeeded in generating a broad and large sample. This managed to capture the broad diversity of experiences of catfishing victims throughout Bangladesh. This diversity, coupled with the employment of HCI principles, allowed our research to represent a wide variety of societal contexts, rendering the findings ultimately more robust and widely applicable.

5.4 Thematic Analysis

The thematic analysis revealed ten main themes that describe distinct aspects of the catfishing experience. These themes highlight the major areas of concern and will be explored in more detail in the subsequent chapters. The main themes identified were:

1. **Emotional Vulnerability & Manipulation** – Scammers used emotional appeals to exploit victims' vulnerabilities and manipulate them into trusting them. Emotional manipulation was frequently linked to romantic deception and financial exploitation.
2. **Romantic Deception** – Many victims were manipulated through the promise of romantic relationships, which were later revealed to be fabricated for exploitation.
3. **Financial Exploitation** – Victims were often financially exploited through emotional blackmail, fake emergencies, and false promises of future rewards.
4. **Suspicion and Red Flags** – Victims expressed initial doubts and observed inconsistencies in the stories of the scammers, but these were often dismissed until the deception was fully realized.
5. **Trust Issues** – The experience of being deceived caused victims to lose trust in others, particularly in online interactions. This loss of trust often extended to family, friends, and future relationships.
6. **Psychological & Emotional Impact** – Catfishing led to significant emotional distress, including feelings of betrayal, self-blame, depression, anxiety, and a loss of self-worth.
7. **Social Isolation & Family Impact** – The deception often led to feelings of isolation, as victims distanced themselves from friends and family due to shame. Some victims experienced direct conflict with their families, especially when money was involved.
8. **Lack of Reporting & Fear of Judgment** – Barriers such as fear of judgment, social stigma, and lack of knowledge about reporting mechanisms prevented many victims from reporting their experiences or seeking help.
9. **Identity Theft & Online Safety Concerns** – Some victims found that their personal information, including photos and details, had been used fraudulently by the scammers, leading to concerns about identity theft.
10. **Barriers to Online Interaction & Increased Caution** – Victims expressed an increased sense of caution after the deception, avoiding interactions with strangers and becoming more skeptical about sharing personal information online.

By presenting these themes, the study provides deep insights into how individuals in Bangladesh perceive, navigate, and respond to online deception. The findings contribute to the broader understanding of digital trust, cybersecurity, and the social manipulation that occurs in online spaces. These themes will be further elaborated in the following chapters, with key quotes and deeper analysis.

5.5 Thematic Coding

Thematic coding was applied to the qualitative interview data to identify recurring patterns that help us understand the experiences of catfishing victims. The following themes emerged from the analysis, offering a comprehensive insight into catfishing in the context of Bangladesh.

5.5.1 Emotional Vulnerability and Manipulation

Emotional vulnerability plays a central role in the process of catfishing, as perpetrators often exploit victims' psychological and social insecurities to gain trust and manipulate them into harmful interactions. Many interviewees described feeling emotionally susceptible due to loneliness, personal loss, or social pressures. Scammers leveraged these vulnerabilities by presenting themselves as empathetic, caring, and supportive, making victims believe they had found meaningful companionship.

“He used Quran verses to treat me, shared Islamic readings, and made me feel like I was doing good work.” – **Participant 19**

“I felt really special, I thought I had found someone who understood me.”
– **Participant 11**

These quotes illustrate how emotional manipulation creates a sense of attachment that reduces the victim's ability to question the authenticity of the scammer. The sense of connection established by fulfilling an emotional void makes victims more susceptible to further forms of control, including financial exploitation and emotional dependency.

“I was so emotionally upset that I was not even in a state to distinguish between truth and lies.” – **Participant 10**

Emotional distress impairs rational decision-making, as catfishers often induce urgency or dependency that clouds judgment. Victims become less able to critically evaluate interactions, which delays their recognition of deception.

Manipulation Based on Personal Insecurities

Several victims reported that scammers targeted their personal insecurities—such as physical appearance or social status—to deepen the emotional manipulation. This strategy further entrenched victims' emotional dependence.

“He said that his mother did not accept me because I am dark-skinned.” –
Participant 1

By weaponizing societal prejudices, scammers reinforced feelings of inadequacy and isolation. This not only amplified the emotional grip on the victim but also intensified their attachment to the deceptive relationship, making the deceit harder to detect or reject.

Digital Environment and Emotional Exploitation

The nature of digital communication enables this type of emotional manipulation. Online interactions allow scammers to curate personas and maintain control over how and when emotional cues are conveyed. In contrast to face-to-face interactions, the absence of non-verbal feedback and real-time responses makes it easier for perpetrators to fabricate sincerity.

“How can you talk to me like this when my father is so sick?” – **Participant 5**

“She said her child was sick and needed 50,000 taka for treatment.” – **Participant 6**

“He said I was perfect for the job. I felt excited, thought I was lucky.” – **Participant 17**

These quotes clearly show how scammers weaponize fictional emotional tales to play on guilt, build trust, or instill urgency. This tactic works especially well in digital spaces because there’s no way to visually or audibly confirm what’s real. Victims often get deeply emotionally involved before they can see through the deception, demonstrating that being emotionally open is a major factor in why catfishing schemes succeed.

5.5.2 Romantic Deception

Romantic deception is the most prevalent theme of catfishing, where perpetrators create false personas to initiate romantic relationships with their victims. This form of deception is especially harmful as it exploits the emotional desires and need for companionship of the victim, leading them to believe they are engaged in a real relationship. The emotional engagement in a romantic relationship makes the victim blind to the scam until much harm is already done, both financially and emotionally.

It typically begins with the scammer pretending to be a potential life partner, employing tactics like compliments, shared values, and planning for the future. Once trust and emotional engagement are established, the scammer exploits the victim, usually for money or to further manipulate the victim. The subject is particularly relevant because it unravels the connection between emotional manipulation and deception that is normally masked behind the veneer of a romantic relationship.

“He wanted to marry me and made me feel special, like I was the one for him.” – **Participant 16**

“She said she liked my sense of humor, and we talked about music and hobbies.” – **Participant 18**

These quotes reflect how the scammer used romantic promises to establish an emotional connection with the victim. By framing the relationship as one with a future commitment (e.g., marriage), the scammer ingrained the victim into an emotional attachment that would later make them more susceptible to manipulation. The victim believed that they were the scammer’s only love interest, reinforcing the illusion of a genuine romantic relationship.

One of the most insidious aspects of romantic deception is that it leverages the victim's emotional vulnerabilities. Many victims enter these relationships during times of loneliness, emotional distress, or major life transitions, making them more susceptible to manipulation. The scammer, in turn, builds a persona that aligns with the victim's emotional needs, often portraying themselves as someone who understands and empathizes with the victim's personal struggles.

“We even started talking about marriage.” – **Participant 4**

This statement illustrates the escalation of the deception. What began as a casual on-line interaction evolved into a deeper emotional commitment, leading the victim to make life plans based on a falsehood. When the deception is revealed, it's not just the financial loss that affects the victim but also the emotional toll of losing someone they believed to be a future partner.

Emotional and Psychological Toll of Romantic Deception

The emotional consequences of romantic deception are profound. Victims often report feelings of betrayal, guilt, and shame once they realize the relationship was a lie. Many victims feel humiliated by their emotional investment in someone who was never real. The psychological toll can be long-lasting, leading to diminished self-esteem, anxiety, and difficulty trusting others in the future.

“I felt devastated. He had looked me in the eye during video calls. It was all a lie.” – **Participant 2**

“I really liked Farhad (fake name). But after this, I completely lost trust in people.” – **Participant 7**

The devastation described in these quotes reflects the emotional depth of romantic deception. The victim not only faces financial loss but also the emotional loss of what they thought was a meaningful connection. The betrayal is particularly intense because it challenges the victim's perception of their ability to judge others and trust their instincts. The deeper the emotional attachment, the more difficult it becomes for the victim to disengage from the deception. Trust issues often persist long after the scam is uncovered, affecting future relationships and emotional well-being.

Romantic Deception as a Means of Long-Term Control

In many cases, romantic deception is used as a tool for long-term control. The scammer does not simply deceive the victim for a one-time gain but manipulates them over an extended period, making the victim emotionally reliant on the fake relationship. By leveraging the emotional bond, the scammer is able to extract both emotional and financial resources from the victim.

“He said we would get married in the future. He said once he got a job, we would get married. I believed him.” – **Participant 1**

“He said he wanted to marry me according to Islam, in a halal relationship.” – **Participant 26**

The victim's belief in these promises allowed the scammer to extend their control, deepening the emotional attachment and increasing the chances of financial exploitation. This long-term manipulation demonstrates how romantic deception is not just about creating an illusion of love but about maintaining emotional control over the victim for sustained benefit.

5.5.3 Financial Exploitation

One of the most damaging outcomes of catfishing is financial exploitation, where perpetrators manipulate victims into transferring money under false pretenses. These requests are often framed around fabricated emergencies, promises of future rewards, or emotionally charged situations. Once emotional manipulation has created a foundation of trust, the scammer begins introducing financial demands that exploit the victim's compassion, guilt, or hope for a shared future.

Interview data revealed numerous instances where victims were persuaded to send significant sums of money, typically for reasons such as medical treatment, business investments, visa processing, or personal crises. These demands were commonly presented with a sense of urgency, pressuring victims to act quickly without questioning the legitimacy of the situation.

“She told me that her child was in the hospital, so she needed money urgently. I sent the money without hesitation.” – **Participant 6**

This example highlights how scammers manufacture emotionally sensitive scenarios to elicit immediate compliance. By portraying distressing events such as a child's medical emergency, they leverage the victim's emotional responsiveness to bypass skepticism and secure financial support. Moreover, scammers often embed financial requests within narratives of romantic interest, long-term commitment, or mutual future plans. This framing ensures that the victim perceives the transaction not as a monetary loss, but as an act of support within an emotionally meaningful relationship.

“He said he needed 100,000 taka, and only then will I be able to think about getting married.” – **Participant 3**

“He asked for 60,000 BDT for medical fees for my visa process.” – **Participant 16**

These quotes reflect how victims are psychologically manipulated through the suggestion of future rewards, such as marriage or emigration, making financial requests appear as stepping stones toward a shared goal.

Other participants reported being deceived through more materialistic promises or fabricated transactions:

“He wanted to send me a gift, but needed me to pay the courier company first.” – **Participant 8**

“They asked me for money to join Telegram and receive payment.” – **Participant 15**

These incidents reveal how financial exploitation in catfishing is rarely overt. Instead, it is gradually introduced, often disguised as part of a mutual venture or urgent necessity, ensuring that the victim feels morally or emotionally obligated to comply.

The Role of Trust and Emotional Dependency

A crucial factor in financial exploitation is the manipulation of trust. Victims often believe they are in an authentic relationship, marked by affection, reciprocity, and shared dreams. This emotional foundation weakens their ability to critically evaluate financial requests, as they become emotionally invested in the scammer's well-being and future.

"I really liked him. I thought we were building a future together. I felt like I was helping him." – **Participant 7**

Here, the victim's willingness to provide financial support stemmed from their emotional attachment and belief in the legitimacy of the relationship. The scammer's fabricated narrative successfully transformed financial requests into perceived acts of love, partnership, or solidarity.

Use of Mobile Financial Services in Scams

Our findings revealed that catfishers in the Bangladeshi context frequently leveraged mobile financial services, particularly bKash [72], to extract money from victims. The convenience and ubiquity of these platforms make them an easy and discreet channel for scammers to receive funds without needing formal banking or identity verification. As illustrated by Participant 25, the emotional urgency created by the scammer led to an unquestioned financial transfer:

"She suddenly said her father was in the ICU and urgently needed 15,000 taka. Without questioning, I sent the money via bKash. At that moment, I didn't even consider it could be a scam." – **Participant 25**

This highlights how emotional manipulation, combined with the ease of instant digital transactions, facilitates a low-friction pathway for financial exploitation. Unlike traditional scams requiring more elaborate logistics, the use of mobile payment apps allows scammers to operate quickly, anonymously, and with minimal traceability.

5.5.4 Suspicion and Red Flags

Suspicion and red flags were a consistent theme in interviews with participants. Most victims indicated that they had observed initial inconsistencies or suspiciousness in their communication with scammers. Such red flags, although sometimes present at the beginning of communication, were explained away or justified as a consequence of emotional manipulation and attachment on the victims' part. Emotional attachment had the potential to override intuitive suspicion, and victims overlooked behavioral anomalies that, with hindsight, indicated dishonesty.

This theme emphasizes the conflict between emotional need and suspicious instinct. Victims of catfish were more likely to experience internal conflict as in, noticing warning signs of possible threat and yet also pursuing validation and connection. Catfishers often knew how to dispel suspicion, offering emotionally credible explanations or excuses that reduced the urgency or intensity of developing red flags.

"Not doing video calls was a red flag. I shouldn't have met someone unknown." – **Participant 3**

Avoidance of visual contact, especially through video calls, was a recurring concern. Scammers typically cited broken devices, poor connectivity, or personal reasons to avoid direct interaction—tactics designed to maintain anonymity while sustaining the illusion of intimacy.

“She kept avoiding video calls, claiming her phone camera was broken.” –
Participant 25

These deliberate evasions were often accepted by victims, who, influenced by emotional narratives, opted to trust rather than challenge the scammer’s inconsistencies. The psychological burden of cognitive dissonance—holding contradictory beliefs or feelings—played a significant role. Victims found themselves torn between emerging doubts and a desire to preserve the emotional bond.

“Sometimes she would disappear for a few days... she started asking me very personal questions.” – **Participant 9**

“When I asked for a face reveal, she kept delaying it and never showed her face.” – **Participant 5**

Red Flags in Digital Contexts

Online interactions, by their nature, limit access to non-verbal cues such as facial expressions, tone of voice, or body language—elements critical to assessing sincerity in face-to-face communication. This limitation allows scammers to maintain a consistent but deceptive narrative, avoiding scrutiny while reinforcing emotional dependency.

“She kept avoiding video calls and sent only pictures of her surroundings.”
– **Participant 11**

“He never gave me his real phone number, only used Telegram or email.” –
Participant 23

These quotes exemplify how digital deception thrives in environments where verification is difficult. Scammers often control the pace and content of communication, selectively disclosing information and using fragmented or inconsistent details to avoid detection.

“They never appeared face to face. All the conversations happened through Messenger.” – **Participant 10**

“The first red flag was contacting me off the platform, second was the job descriptions.” – **Participant 15**

The Emotional Impact of Suspicion

The emotional investment built during these interactions often created a psychological barrier to recognizing manipulation. Victims reported suppressing or downplaying their doubts to maintain the emotional stability of the relationship. Scammers exploited this vulnerability by reinforcing trust and providing comforting, plausible explanations for questionable behavior.

“I started to worry a bit whether the money would just be lost.” – **Participant 16**

Despite experiencing unease, many participants continued to engage with the scammer due to the emotional support, attention, or affection they received. This emotional anchoring delayed critical reassessment of the situation, allowing the deception to continue unchecked.

5.5.5 Trust Issues

Trust issues emerged as a significant and long-lasting psychological consequence of catfishing. Beyond emotional manipulation and financial loss, victims described a profound breakdown in their ability to trust others, particularly in the context of online relationships. The trauma of betrayal, often disguised as intimacy or companionship, left many participants emotionally scarred and highly skeptical of future interactions. This theme illustrates how the impact of catfishing extends beyond the immediate deception, affecting victims' long-term relational and psychological well-being. Participants frequently reported heightened vigilance, persistent doubt, and avoidance of new relationships, both online and offline. Moreover, victims shared how they had overlooked warning signs, invested deeply in the connection, and felt emotionally safe—only to later discover that it was a calculated deception.

“Now I don't trust easily anymore. I need proof, video calls, and verifications.” – **Participant 8**

This defensive behavior reflects the emotional aftermath of betrayal. The demand for verification becomes a coping mechanism—an attempt to protect against future harm. However, it also signifies a broader erosion of confidence in interpersonal connection.

“I felt devastated. He had looked me in the eye during video calls. It was all a lie.” – **Participant 7**

“More than the money, the loss of trust was the worst part.” – **Participant 1**

These reflections demonstrate how the emotional commitment and perceived authenticity of the relationship intensified the sense of betrayal. The realization that the trust had been manipulated led to emotional distress, including anxiety, grief, and existential doubt.

Online Spaces and the Erosion of Trust

Digital environments play a unique role in the erosion of trust. Unlike face-to-face interactions, online communication lacks essential non-verbal cues—such as tone, body language, and eye contact—that help in assessing sincerity. The absence of these cues leaves users more susceptible to deception and increases the psychological impact when trust is violated.

“I started doubting myself. I couldn’t sleep for weeks. I kept checking if the account had returned.” – **Participant 9**

“Since then, I’ve lost trust in social media.” – **Participant 6**

The delayed realization of betrayal and the inability to verify authenticity in real time lead to lingering self-doubt and avoidance of digital platforms altogether. For many, the scam experience tainted their perception of all online spaces.

Psychological Ramifications and Social Withdrawal

The psychological ramifications of broken trust are far-reaching. Participants reported withdrawing from social circles, fearing future deception, and struggling with generalized mistrust. This social isolation, in turn, led to increased feelings of loneliness and anxiety, compounding the emotional trauma.

“I don’t trust anyone anymore. Everyone seems like a cheater to me.” – **Participant 10**

“Now if I suspect someone might be catfishing, I start doubting them much faster.” – **Participant 4**

These experiences suggest that trust issues post-catfishing often result in overgeneralization, where victims apply the sense of betrayal to future interactions indiscriminately. While such hyper-vigilance is a natural defensive response, it ultimately restricts the victim’s ability to form meaningful relationships.

5.5.6 Psychological and Emotional Impact

Catfishing has profound psychological and emotional consequences that extend far beyond financial loss. As revealed through participant interviews, the experience often leads to long-lasting emotional trauma, characterized by betrayal, self-blame, anxiety, and diminished self-worth. The emotional manipulation involved in catfishing—particularly in the context of romantic or intimate deception—disrupts victims’ perception of reality and erodes their trust in others and in themselves.

A recurring theme in the interviews was the emotional devastation that followed the realization of being deceived. Victims reported feelings of humiliation and a deep sense of betrayal, particularly when they had believed the relationship to be genuine.

“I felt devastated and humiliated. I couldn’t believe I fell for it.” – **Participant 2**

Emotional Trauma and Self-Blame

The betrayal was often intensified by the emotional investment victims had made, making the deception feel deeply personal. Many internalized the experience, blaming themselves for not recognizing the manipulation earlier. This self-blame frequently led to a breakdown in confidence and self-esteem, particularly when victims struggled to reconcile their emotional attachment with the truth of the deception.

“I started doubting myself. I couldn’t sleep for weeks. I kept checking if the account had returned.” – **Participant 6**

“Adding people on social media without knowing them properly was a bad decision.” – **Participant 3**

This expression of regret reflects a broader pattern of self-criticism among victims, many of whom questioned their own decisions in hindsight. Such cognitive dissonance—where emotional belief clashes with factual realization—intensified victims’ distress, reinforcing feelings of inadequacy and emotional confusion.

Anxiety, Fear, and Social Withdrawal

Beyond emotional pain, many victims experienced sustained anxiety and fear. The emotional dependency created by the scam often made it difficult to disengage from the relationship, especially when threats, guilt, or emotional blackmail were involved.

“I was in a fear that if I did not send him the money then what would have happened.” – **Participant 8**

“It was definitely a source of anxiety and stress.” – **Participant 13**

“I couldn’t sleep for weeks. I felt ashamed, empty, and broken.” – **Participant 14**

These emotional consequences often extended into future relationships. Many victims reported becoming hyper-vigilant, fearful of new interactions, and anxious about being deceived again—particularly in online spaces where verification is limited. Social stigma further compounded the emotional burden. In cultures where family reputation is paramount, victims often chose not to disclose the situation due to fear of judgment or shame.

“I felt like I couldn’t tell my family. If I had reported it, they might’ve gotten involved.” – **Participant 1**

This reluctance to seek help contributed to prolonged isolation and emotional suffering. Victims frequently withdrew from social environments, internalizing their trauma and limiting their access to emotional support.

5.5.7 Social Isolation and Family Impact

Social isolation and family disruption are significant, though often overlooked, consequences of catfishing. As victims process the emotional aftermath of deception, they frequently withdraw from social relationships, driven by feelings of shame, fear of judgment, or emotional exhaustion. This withdrawal is not only emotional but also social, resulting in the loss of meaningful connections. At the same time, the impact of catfishing often extends to the victim's family, contributing to conflict, mistrust, and relational strain—particularly when financial loss or social stigma is involved.

“I don’t trust anyone now. I don’t talk to strangers anymore.” – **Participant 6**

This form of social self-protection, while adaptive in the short term, can lead to long-term emotional numbness and hinder recovery. The experience of betrayal causes victims to question their own ability to form meaningful relationships, amplifying their withdrawal from both digital and in-person interactions.

Social Withdrawal and Emotional Isolation

Many victims reported distancing themselves from friends, peers, and the public following their experience. This isolation often emerged as a defense mechanism, aimed at avoiding further emotional harm or social embarrassment.

“I distanced myself from everyone. I was scared to go outside and talk to anyone.” – **Participant 7**

Family Conflict and Relational Strain

The emotional burden of catfishing is often compounded by family dynamics. Several participants shared how the experience led to tension or emotional distance within their households. Feelings of guilt, shame, or the financial implications of the scam frequently contributed to relational strain.

“My relationship with my parents isn’t very good now because I caused such a big issue.” – **Participant 5**

“My husband eventually found out, and I felt very guilty about it.” – **Participant 6**

“My family found out too. They were supportive, but the whole situation was actually embarrassing.” – **Participant 9**

These accounts illustrate how catfishing disrupts familial trust and communication. Some victims feared disclosing their experience, anticipating judgment or misunderstanding. Others experienced direct conflict due to the emotional or financial fallout. In cultures where familial reputation and honor are emphasized, this fear of social shame often discourages disclosure and intensifies emotional isolation.

5.5.8 Lack of Reporting and Fear of Judgment

Lack of reporting and fear of judgment emerged as significant barriers that prevent many victims of catfishing from seeking help or justice. These interrelated themes contribute to the perpetuation of emotional distress and hinder recovery. Victims often experience deep shame and anticipate ridicule or blame from others, which discourages them from disclosing their experience. In many cultural contexts, especially in Bangladesh, being deceived—particularly in romantic or financial matters—carries social stigma, further silencing victims.

A primary reason victims chose not to report was the fear of being judged or blamed for falling into an online scam. Many anticipated that disclosing their experience would result in ridicule, particularly from family or community members.

“If I had reported it, people would have laughed at me. They would think I was stupid for trusting a stranger.” – **Participant 8**

“She felt ashamed. In our society, people would blame her for sending money.” – **Participant 26**

“In Bangladesh, when a man is emotionally broken, it becomes a joke.” – **Participant 14**

Fear of Judgment and Social Stigma

This fear of social humiliation often prevented victims from seeking support, leaving them to process emotional trauma in silence. Some victims even reported family members actively discouraging them from taking action.

“My sister really wanted to report it, but my parents stopped us. They said if people found out, it would be very shameful.” – **Participant 3**

“I didn’t report it. I feared what people would say about me.” – **Participant 26**

Psychological Consequences and Recommendations

The emotional impact of non-reporting is considerable. Victims often experience ongoing anxiety, guilt, and depression. The silence and shame associated with not reporting the scam exacerbate feelings of isolation and hinder emotional recovery.

“I didn’t report it to anyone because the money was already gone.” – **Participant 6**

This sense of futility—combined with internalized guilt and social fear—reinforces the psychological toll of catfishing. Victims often feel they have failed themselves by missing warning signs, and the absence of a reporting action compounds this self-perception.

To address these challenges, several interventions are necessary. First, digital platforms must develop clearer and more accessible reporting systems. Second, public awareness and digital literacy campaigns should equip users with the knowledge to recognize, report, and recover from online deception. Lastly, cultural narratives around blame and shame must be challenged through educational initiatives that emphasize empathy and support rather than judgment.

5.5.9 Identity Theft and Online Safety Concerns

Identity theft and cyber security concerns also emerged as significant topics from the interviews. Besides the financial and emotional exploitation involved in catfishing, there are also giant risks to people's privacy and security. Many of the victims explained how their private information such as names, images, and voice recordings were being used without consent. These violations indicate the fragility of digital privacy and how easily online identities can be manipulated by fraudsters.

"They used my photos and voice to create fake clips and posts." – **Participant 10**

"The scammer used my father's name and pictures to create a fake profile." – **Participant 13**

Such impersonation can extend beyond the immediate scam, with victims' identities being repurposed to manipulate additional targets or perpetuate broader fraud. The discovery of such misuse often leads to a deep sense of personal violation and fear over potential long-term consequences.

Exploitation of Personal Data in Catfishing

Several participants recalled moments of realization that the person they were interacting with was not who they claimed to be:

"She eventually admitted that it wasn't a real profile. That the pictures were of someone else." – **Participant 4**

"When I cross-checked it later, I found out it wasn't her real address." – **Participant 5**

"I called him and asked if he did it. He was very angry and then admitted everything. I sent him private pictures. I was a bit hesitant at first, but I thought it was normal." – **Participant 7**

These examples reflect a common pattern in catfishing cases: once emotional trust is established, the manipulation deepens, and personal data is extracted under false pretenses. The victim's identity or private content is then used inappropriately, leading to further distress.

Social and Emotional Consequences of Identity Theft

The impact of identity misuse goes beyond digital violation—it has tangible emotional and social repercussions. Victims often feel humiliated when they discover that their personal information has been exploited, particularly when the deception becomes known among friends or family.

"I felt humiliated. My friends and family didn't understand what had happened." – **Participant 2**

This experience of shame is exacerbated by the stigma surrounding online deception and the assumption that the victim was at fault. Victims not only endure the betrayal of their digital trust but also the social consequences of being perceived as complicit in the manipulation.

“Later, I connected all the dots myself and understood. My friend also told me that it was actually a guy.” – **Participant 2**

“I Googled the company name and logo. No valid company existed.” – **Participant 17**

These realizations often come too late, after the emotional and reputational damage has already been done. In many cases, victims withdraw from digital or social engagement out of fear that their identity might be misused again or that others might question their judgment.

5.5.10 Barriers to Online Interaction and Increased Caution

The theme of barriers to online interaction and increased caution reflects the behavioral and psychological changes that many victims experience following catfishing. The emotional, financial, and psychological consequences of being deceived often result in heightened skepticism and withdrawal from digital communication. Victims become more cautious in online spaces, creating emotional and behavioral boundaries as a defense against further manipulation. While this caution may serve a protective function, it also signals the long-term damage inflicted on victims’ ability to trust others and participate comfortably in digital environments.

Following catfishing incidents, many victims reported adopting a more cautious and guarded approach to digital engagement. This shift included avoiding unfamiliar individuals online, demanding proof of identity, or withdrawing from certain platforms entirely.

“I avoid talking to new people, and even now, I still feel afraid.” – **Participant 9**

“I deleted all my social media posts, locked down my profile, and removed anything personal. I never realized how much information I was giving away until I saw how easily someone manipulated me.” – **Participant 13**

These accounts reflect a broader trend of digital self-protection, wherein victims limit their online presence in response to having been deceived. Although such privacy-oriented behavior is a rational adaptation, it can result in emotional detachment and social isolation—especially in contexts where online interaction is essential for both personal and professional life.

Systemic Limitations and Platform Inaction

Several participants expressed dissatisfaction with the inadequate support received from digital platforms and law enforcement when they attempted to report catfishing incidents. Many described the process as unclear, inaccessible, or ultimately ineffective.

“I feel that if Facebook’s authorities had handled things more seriously, it would have been better.” – **Participant 8**

“I thought about reporting to Facebook, but by the time I figured it out, she had already deleted the fake account.” – **Participant 12**

“I still don’t know if there is some way available for that. I don’t know who or where to report to.” – **Participant 8**

These frustrations highlight systemic gaps in online safety infrastructure. In some cases, cultural or familial factors also contributed to silence and non-reporting:

“I wanted to report it... but my parents told me never to talk about it to anyone.” – **Participant 11**

This intersection of platform inaction, cybercrime illiteracy, and cultural stigma leaves victims without recourse or support, further amplifying their emotional vulnerability and distrust of digital systems.

Lessons Learned and the Need for Digital Reform

Despite their experiences, many victims expressed a desire to share insights and preventative advice. Increased caution was often framed not as fear, but as learned vigilance.

“Make sure to properly think before any decision. Also, only share information after verifying the person’s identity.” – **Participant 14**

“I think a verification process could be useful... if the personal pictures we use and claim to be our own were checked by platforms like Facebook.” – **Participant 18**

These reflections emphasize the importance of platform accountability and user education. Victims advocated for identity verification systems, improved reporting tools, and greater awareness of the risks of online deception. Such reforms are essential not only to prevent future harm but also to help restore a sense of trust and security in online spaces.

The thematic analysis and coding reveals the significant and multifaceted impacts of catfishing on individuals in Bangladesh, encompassing both mental health deterioration and financial exploitation, as well as long-term behavioral changes. Victims of catfishing experience severe emotional trauma, which includes distorted perceptions of trust and a deep, prolonged distrust of digital social interactions. Financial losses are substantial, with many victims manipulated through fabricated emergencies, fake business opportunities, and emotional blackmail tactics. The findings underscore the urgent need for digital literacy education to help users recognize potential online threats and avoid falling prey to scams. Additionally, the need for financial fraud protection education and enhanced reporting mechanisms on digital platforms is clear, as these systems are currently inadequate in addressing the scale of catfishing incidents. Without systemic interventions that address both preventative measures and support structures for victims, these scams will continue to target vulnerable individuals, further undermining trust in digital spaces and inflicting lasting emotional and financial harm.

5.6 Key Narratives and Patterns: Understanding Victim Experiences

This chapter dives into the predominant narratives and general themes that came out of our interviews, giving us a window into the lived experience of catfishing victims. The interviews painted a harrowing process frequently unfolding in stages of trust building, emotional manipulation, financial exploitation, and extreme psychological distress. By delineating these distinct phases and identifying main patterns of behavior, we gain a clearer sense of catfishing's long-term impact on the victim and their future online activity. Lastly, the words of the victims themselves provide singular, perceptive descriptions of how catfishing works in practice and how people negotiate, in complex ways, its difficult repercussions.

5.6.1 The Psychological Phases of Catfishing: How Victims Are Manipulated

Victims of catfishing usually go through a range of escalating psychological phases, which ultimately result in extreme mental and emotional suffering. The process is driven by a combination of manipulative and deceptive strategies, specifically intended to win trust incrementally, create emotional reliance, and ultimately exploit it. The deception of this process is in the subtlety as in the catfisher still presents a front of legitimacy while slowly taking control of the victim's emotions, pulling them further into a web of lies. These steps can be broken down generally as follows:

Stage 1: The Hook – Establishing an Appealing Persona

The initiation stage of catfishing involves the catfisher constructing an appealing fictitious identity designed to lure victims. These online profiles are well thought out, with some using stolen photos and entirely fabricated personal histories, all aimed at appearing completely genuine. Intelligent presentation skills are utilized by the catfisher, especially preying on a victim's emotional susceptibility, personal desires, and vulnerabilities. They tend to tailor make these profiles to suit particular traits in victims, creating a false impression of shared interests and measures up precisely to their emotional requirements.

At this point, victims are typically oblivious to the deception. The catfisher skillfully exploits elements like mutual connections or shared online groups to bolster the profile's legitimacy. This is not random rather it is a deliberate strategy calculated to dissipate any initial doubts a victim might harbor by fostering an atmosphere of friendliness and trust. The following quote perfectly illustrates how one victim's trust was initially ensnared:

"He had similar interests, and we both loved travel. It just felt right. We had so much in common." – **Participant 8**

At this point, the appealing persona acts as the hook, drawing the victim into the web of deception.

Stage 2: Emotional Bonding and Trust Development

Once the victim is hooked, the next phase focuses on emotional bonding and the gradual development of trust. Catfishers engage in lengthy, meaningful conversations designed to establish a genuine emotional connection. Victims report that the catfishers often seem exceptionally focused on their emotional needs, demonstrating profound listening skills and offering emotional support that feels both sincere and tailored to their individual needs.

A common tactic in this phase is mirroring, where the catfisher mimics the victim's emotions and life experiences to create the illusion of deep compatibility. The goal is to build emotional dependency by convincing the victim that they share similar values, obstacles, or life experiences. This emotional manipulation is key to fostering an attachment that is difficult for the victim to break, as they feel they are engaging with someone who truly understands them.

One victim shared:

"He was always there when I needed someone to talk to. It was like we were soulmates—he knew exactly what I was going through." – **Participant 6**

During this stage, victims often open up and reveal sensitive personal details, making them vulnerable to further exploitation. The emotional investment made by the victim deepens, making it harder for them to question the authenticity of the catfisher's intentions.

Stage 3: Exploitation and Manipulation

Once emotional trust has been established, the catfisher begins the exploitation phase, using the bond created to manipulate the victim into providing financial assistance or personal information. This is the stage where the deception escalates from emotional manipulation to financial exploitation. Victims are asked for money under various false pretenses, often framed as urgent or emergency situations.

Catfishers frequently manipulate their victims by appealing to their emotional attachment and convincing them that their assistance is crucial to a personal crisis. Victims feel compelled to help, believing that they are doing something good for someone they care about. Over time, these requests grow in frequency and magnitude, leading to a pattern of financial exploitation.

One victim explained how their catfisher gradually escalated demands:

"At first, it was small amounts. She said her phone bill was overdue. Later, it turned into requests for more money, and I just kept sending it. I did not want to disappoint her." – **Participant 2**

The gradual increase in the demands, starting small and escalating to larger sums, illustrates how catfishers use emotional dependency to wear down the victim's resistance and manipulate them into compliance.

Stage 4: Disappearance and Emotional Fallout

The final action in the catfishing process is where the catfisher vanishes or continues to manipulate the victim. In most cases, when financial means or personal information is acquired, the catfisher ghosts the victim, blocking or cutting off all means of

communication without warning or explanation. This sudden rejection leaves victims devastated, betrayed, and confused. In other instances, the catfisher still lies to the victim by providing fake reasons of family emergencies, internet disruptions, or job obligations for their absence.

Emotional harm inflicted by this stage is severe. Victims feel a strong sense of loss and self-blame, wondering why they were not able to see the warning signs of fraud. Disillusionment and emotional exhaustion have been complained about by victims, the fraud destroying their capacity to trust online and offline relationships.

One victim shared their feelings of betrayal:

"When he disappeared, I was left in shock. I had invested so much emotionally and financially. It felt like my whole world had crumbled." – **Participant 4**

This disillusionment affects the victim's ability to rebuild trust and has lasting repercussions on their emotional well-being.

From an HCI perspective, the psychological manipulation involved in catfishing is made possible due to the unique characteristics of online interactions. In face-to-face encounters, emotional cues, body language, and direct responses provide critical context for trust-building. However, in the digital world, catfishers can hide behind the anonymity of the internet, giving them a powerful advantage in manipulating emotions and constructing false personas. This makes it easier for victims to fall prey to deceptive tactics, especially when they are emotionally vulnerable and lacking in digital literacy regarding the risks of online deception.

5.6.2 The Role of Social Media and Online Dating Platforms in Facilitating Catfishing

The internet communication platforms such as Facebook [77], Instagram [79], and WhatsApp [87] play a central role in enabling catfishing. These platforms provide individuals with the opportunity to create fake identities, build trust signals, and emotionally manipulate others via text-based communication. The lack of visual cues and in-real-time exchange makes it easy for catfishers to weave believable narratives in the long term, thereby making it hard to detect deception.

Facebook: The Primary Platform for Catfishing

Our victim interviews consistently pointed to Facebook as the go-to platform for catfishing. It offers significant opportunities for creating fake profiles and manipulating users, largely thanks to its relaxed verification protocols and ample social validation features. A key reason catfishers flock to Facebook is its sheer breadth of reach, making it an ideal place to craft and manage deceptive profiles that can target a massive audience.

It's remarkably easy for catfishers to fabricate identities on Facebook. The platform's minimal requirements for profile verification allow for simple setup of false personas, which in turn makes it simpler to exploit a victim's trust. Many victims told us it was often incredibly tough to tell the difference between genuine and fake accounts, especially when these fraudulent profiles seemed to share mutual connections and interests. Victims frequently mentioned getting drawn into relationships with catfishers

who appeared to have common friends, which only further cemented the perceived legitimacy of these deceptive profiles.

As one participant shared:

“He had mutual friends with me on Facebook, so I trusted him more. It made me think he was real because we had similar connections”. – **Participant 9**

This mutual friends feature creates an illusion of social proof, a tactic that catfishers leverage to increase the perceived trustworthiness of their fake profiles. The more mutual connections the catfisher shares with the victim, the more likely the victim is to trust them. This false legitimacy makes it easier for the catfishers to deceive victims, as they believe the connections are genuine, despite the fraudulent nature of the profile.

Instagram: The Platform for Romance Scams

Instagram’s network effects enabled romance catfishing to thrive on the platform, as it is heavily centered around photo-sharing content. Catfishers frequently use Instagram to curate carefully crafted profiles, displaying stolen photos of attractive individuals living luxurious lifestyles. These profiles are designed to create an illusion of authenticity, drawing in unsuspecting victims who are lured by the visual appeal and the apparent success of the individual behind the profile.

Catfishers not only rely on visually appealing images but also use Instagram’s features, such as followers, likes, and comments—to enhance their credibility. By building an extensive follower base and engaging with their victims’ content, the scammer can create the illusion of legitimacy and social proof, making the victim more likely to trust them. However, the problem is exacerbated by Instagram’s relatively lax verification protocols. Unlike platforms with stronger identity-checking mechanisms, Instagram allows users to create multiple profiles easily, giving scammers the ability to generate fake identities and quickly delete or abandon them if their deceit is discovered. As one participant pointed out:

“It wasn’t until later that I realized that most of his photos were stolen from someone else’s account. But by then, I had already shared so much with him.” – **Participant 11**

This reflects how Instagram’s lack of stringent verification mechanisms allows catfishers to create fake accounts with minimal effort. They can fabricate an entirely false life and continue their manipulation without facing significant repercussions. The anonymity provided by Instagram creates an environment where deceptive personas are easily constructed, making it an ideal platform for catfishing.

Messaging Apps: Moving the Conversation Off-Platform

After the victim is emotionally invested, the catfishers move the conversation to private messaging apps such as WhatsApp [87] and Telegram [29] to escape detection within the platform and continue their manipulation in a safer and less public environment. The apps have end-to-end encryption, where the content of the conversations is inaccessible and not traceable, hence making it even harder for victims to detect the scam or report the case. Shifting the conversation off-platform also allows the scammer not

to have any form of surveillance or intervention that may occur through the social networking platform.

End-to-end encryption provided by messaging applications such as WhatsApp and Telegram is perhaps one of the most significant tools utilized by catfishers since it renders messages exchanged between the scammer and victim uninterceptable and unmonitorable by the platform. This makes the scammer feel safe so that he can go about his manipulation of the victim without apprehension of being caught by authorities or by the moderation capabilities of the platform. One participant described how he shifted the conversation to a safer platform:

“After a while, he asked me to move our conversations to WhatsApp and that’s when the requests for money started coming in.” – **Participant 15**

This shift to a more private platform is a common tactic used by scammers to avoid detection, as most social media platforms offer some form of reporting system that could expose the scammer’s behavior. By moving the communication to private, encrypted channels, the catfisher gains full control over the interaction, making it more difficult for the victim to confirm the authenticity of the person they are speaking to.

Another benefit of moving the conversation to messaging apps is that these platforms allow for more personalized communication, with voice messages, video calls, and instant replies enhancing the illusion of a genuine relationship. The immediacy and personal nature of messaging apps like WhatsApp or Telegram make it easier for the catfisher to manipulate the victim emotionally and make the deception feel more authentic. One participant noted:

“He sent me voice messages and even shared videos of himself, but I later realized it was all staged. The real person was never there.” – **Participant 26**

In this phase, catfishers escalate their emotional manipulation through more intimate forms of communication, such as voice messages and video clips, which create a false sense of connection and deepen the victim’s emotional attachment. The victim, believing they are interacting with a real person, is more likely to comply with the scammer’s financial demands, often without realizing that they are being manipulated.

Bumble and Fake Matrimonial Sites: Shared Vulnerabilities in Online Interactions

Both Bumble [73], a popular dating app, and fake matrimonial sites represent platforms where catfishing thrives, despite their differing goals—romantic connections versus matrimonial arrangements. Although these platforms may cater to different types of relationships, the deceptive tactics used by scammers on both platforms are strikingly similar. In both cases, the victims are emotionally manipulated, trust is built, and financial exploitation follows. Bumble’s unique feature—where women initiate conversations—adds an interesting layer to the catfishing process. Despite the app’s efforts to empower women, it remains vulnerable to the same types of emotional manipulation seen on other platforms. Catfishers create appealing personas, often using stolen images, to engage victims in meaningful conversations that lead to emotional dependency and, eventually, exploitation. One participant shared:

“We started chatting regularly, and she seemed very caring. She asked about my mental health, and it felt like she really understood me.” – **Participant 25**

This manipulation is an integral part of the catfishing process. The emotional connection built during conversations on Bumble led the participant to trust the scammer deeply, making them more susceptible to the subsequent financial requests.

Once emotional trust was established, the scammer began to introduce financial demands. One participant explained how their catfisher escalated the situation:

"She suddenly said her father was in the ICU and urgently needed 15,000 taka. Without questioning, I sent the money via bKash. At that moment, I didn't even consider it could be a scam." – **Participant 25**

This quote illustrates how emotional dependency was used to justify financial exploitation. The victim's emotional attachment to the scammer made it difficult for them to question the legitimacy of the financial request. Scammers often take advantage of the anonymity of digital platforms, such as Bumble, to conceal their true identities and manipulate users emotionally. Moreover, the widespread use of mobile financial services like bKash [72], Nagad [80], and Rocket [80] provides scammers with quick, discreet, and largely untraceable ways to receive money, further lowering the barrier for executing such fraud.

A victim of a fake matrimonial site shared a different but equally manipulative experience. The site, designed for individuals seeking marriage, targeted people's emotional vulnerabilities related to their desire for companionship and family approval. The scammer used the promise of marriage and a better life abroad to gain the victim's trust and affection, making it easier to ask for money under the guise of processing documents for marriage and travel.

As the relationship progressed, the scammer's demands for money grew:

"He first mentioned that certain documents were needed to process my visa for Qatar, including a medical certificate and identity verification. He told my father, 'I'll handle everything, but I need an initial amount of 60,000 BDT for the embassy and medical fees.'" – **Participant 16**

Both Bumble and fake matrimonial sites share several common vulnerabilities that make them ripe for exploitation. In both cases, the scammers build trust by exploiting emotional needs—whether it's a desire for love, connection, or marriage. The lack of face-to-face interaction and anonymity of digital platforms enables scammers to create convincing profiles and emotionally manipulate their victims without immediate scrutiny. Moreover, both platforms involve significant emotional investment on the part of the victim. Whether in a dating relationship or a matrimonial arrangement, the victim's attachment is used as a means to exploit their trust and manipulate them into sending money. The absence of thorough identity verification on both Bumble and matrimonial sites allows scammers to fabricate entire lives, using stolen photos and false narratives to gain emotional trust. Victims are often hesitant to report their experiences due to shame and self-blame, as evidenced by the participants who felt embarrassed to share their stories. One participant noted:

"I didn't report it to anyone because the money was already gone. I didn't want to be laughed at or called stupid." – **Participant 16**

The fear of judgment prevents many victims from seeking help or reporting their experiences, which further perpetuates the cycle of exploitation. This reflects a systemic issue where victims feel unsupported, unable to turn to platforms or authorities for help.

5.6.3 Long-Term Impact on Victims' Digital Behavior

The effects of catfishing go far beyond financial loss and temporary emotional distress. For the majority of victims, the process instigated long-term changes in the way they engage with online space and think about online relationships. These behavioral changes are attempts to reestablish a sense of safety and control online, but also demonstrate the long-term psychological toll of the scam.

Increased Skepticism and Digital Caution

In the aftermath of having been catfished, victims take a guarded approach to online communication. Suspicion was a general mindset in their internet use. Some respondents indicated that they ignored new friend requests, did background research prior to chatting, and abandoned the use of dating sites completely for fear of being victimized once more. Even online contact with actual users was engaged in cautiously since trust once invested in online relationships had been severely undermined.

Changes in Privacy Practices and Information Sharing

In response to their exposure, the majority of the victims imposed stricter privacy restrictions on their social media sites. Interview participants told us that they had altered their online profile by limiting the availability of personal information, modifying profile settings, and reducing the amount of information made publicly available. The behavioral changes reflected a risk-averse and cautious method of communication online. Victims were more conservative in their interactions and were inclined to communicate with only reliable persons and networks with better protection tools.

Emotional and Social Withdrawal

The psychological impact of catfishing also led to social and emotional avoidance. Victims mostly stayed away from online activity, and some did not engage in digital activity for several months. In some cases, the experience of manipulation and betrayal led to generalized distrust that was carried over outside the world of cyber space. Besides it had a negative impact on face-to-face relationships in daily life too. Routine social interactions especially with strangers, turned into something anxiety-ridden. The emotional anxiety of receiving unwanted messages or friendship requests tended to cause distress, indicating the lasting impact of catfishing on victims' interpersonal behavior.

As a result of these behavioral shifts, victims developed various forms of self-protection that shaped how they approached digital spaces. These included:

- **Avoidance of strangers:** Victims became highly selective about whom they engaged with online, often refusing interactions with individuals they did not know personally.
- **Increased scrutiny:** Victims displayed heightened vigilance toward new contacts, often requiring identity verification or corroborating information before initiating communication.

- **Fear of emotional intimacy:** Having experienced manipulation, victims were often reluctant to form new emotional bonds—even with seemingly trustworthy individuals—due to the lingering fear of deception.

Recommendations for Improved Digital Safety and Recovery:

- Adoption of multi-factor authentication and robust identity verification systems across social media and communication platforms.
- Expansion of public digital literacy initiatives to educate users on safe interaction practices, privacy management, and scam prevention.
- Implementation of transparent, accessible, and responsive reporting mechanisms to support victims of online deception and hold perpetrators accountable.

Chapter 6

Design Proposal

This design proposal outlines a desktop based interactive prototype aimed at reducing catfishing incidents on social media through subtle UI/UX interventions and lightweight backend logic. Drawing on findings from our user study and survey, which highlighted how victims often trust new contacts quickly, overshare personal information, and fall prey to emotional manipulation, we propose four key features that nudge users toward safer online behavior without restricting their autonomy. Each feature is grounded in HCI theory on persuasive technology, behavior change, trust cues, and informed by both our data analysis and prior research. The prototype adopts a Facebook-like interface to simulate a familiar social networking context, allowing us to illustrate “before nudge” vs. “after nudge” scenarios for each feature. Below, we detail each feature – (1) Pause & Verify prompts, (2) Cautionary trust score banners for unknown contacts, (3) Emotional manipulation warnings, and (4) An easy reporting system – including the user flow logic, interaction design, and underlying heuristics. We justify each design choice with evidence from our thesis findings and relevant literature.

6.1 Feature 1: “Pause & Verify Prompt”

One prevalent theme in our user study was unintentional oversharing – many participants admitted they had shared sensitive personal information (e.g. phone numbers, home address, financial details) early in online conversations, often regretting it later. This aligns with the well-documented “privacy paradox,” where individuals know the risks yet still divulge personal data in practice [43]. To address this, our prototype introduces a “Pause & Verify” prompt that intercepts attempts to share sensitive information and nudges the user to reconsider.

6.1.1 Interaction Design

When the system detects the user is about to send potentially sensitive content (such as an email address, phone number, or keywords like “bank transfer”), a modal dialog interrupts the action. The dialog gently alerts: “Are you sure you want to send it?” as seen in Figure 6.1. Additionally an extended message like “Scammers often ask for personal details. Please double-check that you trust this person.” could also be alerted to user. The user must then explicitly confirm or cancel the action. This design is inspired by soft-paternalistic nudges that momentarily slow down the interaction to prompt reflection without outright blocking the choice [20]. The goal is to engage the user’s

deliberative thinking (System 2) at a critical moment, countering the impulsive urge (System 1) to comply with a request [23]. By inserting a brief pause, we help users overcome biases like hyperbolic discounting [6] (over-valuing immediate social rewards of sharing info) and optimism bias [24] (the “it won’t happen to me” mindset) which often lead to risky disclosures [43].

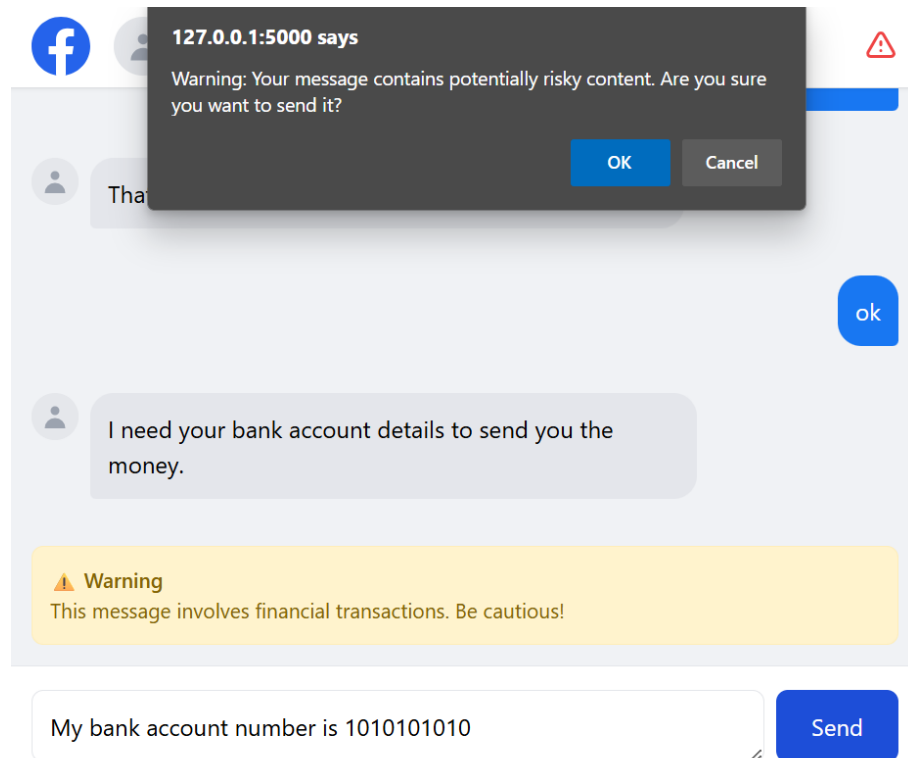


Figure 6.1: Pause & verify modal dialog interface

6.1.2 Link to Analysis

Our survey data and interviews showed that a significant portion of respondents had shared contact details with strangers they met online, and many later realized this made them vulnerable. Participants expressed that a simple warning or reminder could have made them think twice. The “Pause & Verify” feature directly stems from this insight – it provides that missing second thought in the workflow. It essentially implements what one respondent described as “a friend on your shoulder telling you to be careful.” This approach is bolstered by academic findings that well-timed privacy nudges can prompt more deliberate decision-making and reduce impulsive disclosures [60]. For instance, Masur et al. (2021) demonstrated that subtle design interventions can lead users to share more cautiously by providing contextual cues and encouraging reflection [60]. Similarly, Wang et al.’s Facebook field trial introduced a pause-before-posting nudge which successfully caused users to rethink potentially regrettable posts [30].

Our design extends this concept to the act of sharing personal data in private chats – a context identified in our research as high-risk for catfishing. By incorporating a confirmatory prompt, we align with Fogg’s persuasive design principle of “reducing unintended actions by raising a tiny barrier at the point of decision”, thereby leveraging technology to change user behavior in a gentle but effective manner [12].

6.1.3 Grounding in Theory

The “Pause & Verify” prompt exemplifies the persuasive technology principle of “leveraging suggestion” at key moments to influence user behavior without coercion [12]. By allowing users to continue their intended action while encouraging reconsideration, it preserves individual autonomy. This aligns with Thaler and Sunstein’s conceptualization of a “nudge”—an intervention that steers behavior in a predictable direction without restricting freedom of choice [20]. This soft intervention is designed to mitigate known decision-making biases. Prior work notes that users often share information in the heat of the moment and later regret it, due to bounded rationality and the influence of emotional states [23]. By interjecting a calm prompt, we attempt to disrupt the automatic compliance that scammers rely on. This design choice is further supported by interpersonal communication research showing that increased reflection time can improve the detection of deception cues and reduce susceptibility [9]. In summary, Feature 1 serves as a preventive checkpoint grounded in both our empirical findings and established behavior-change techniques: it reminds users of potential consequences at precisely the moment such awareness is most needed, fostering safer communication practices online.

6.2 Feature 2: Trust Score and Profile Review for New Contacts

Our analysis revealed that users often struggle to assess the credibility of unknown profiles, frequently relying on surface cues like profile pictures or a few mutual friends. In many catfishing cases, victims accepted friend requests from strangers or engaged in chats without fully checking the profile. To support users in making more informed decisions about new contacts, we designed a Trust Score banner that appears on friend requests and the profiles of people outside one’s immediate network as seen in Figure 6.2 and in Figure 6.3. This banner provides an at-a-glance assessment of the account’s trustworthiness and nudges the user to review the profile details before trusting the person.

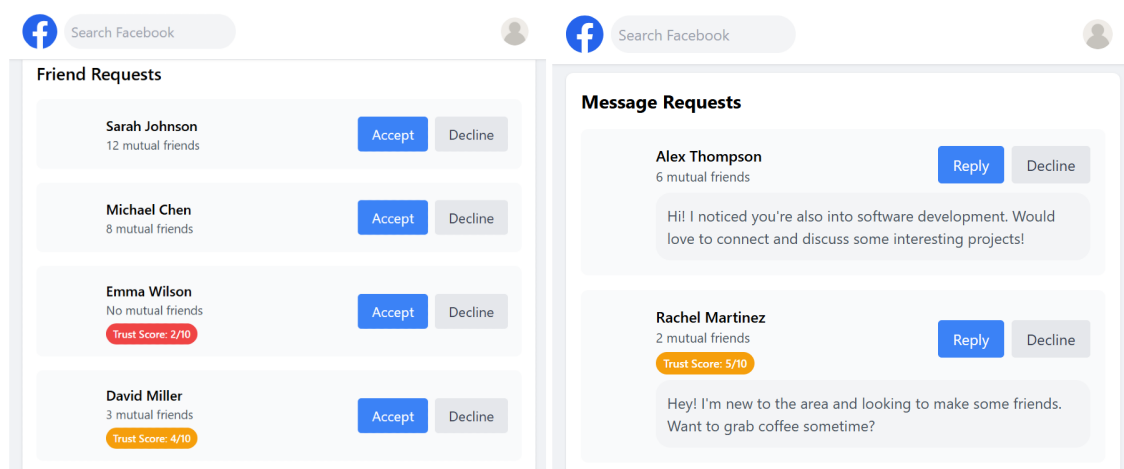


Figure 6.2: Trust score banner display on friend and message request page

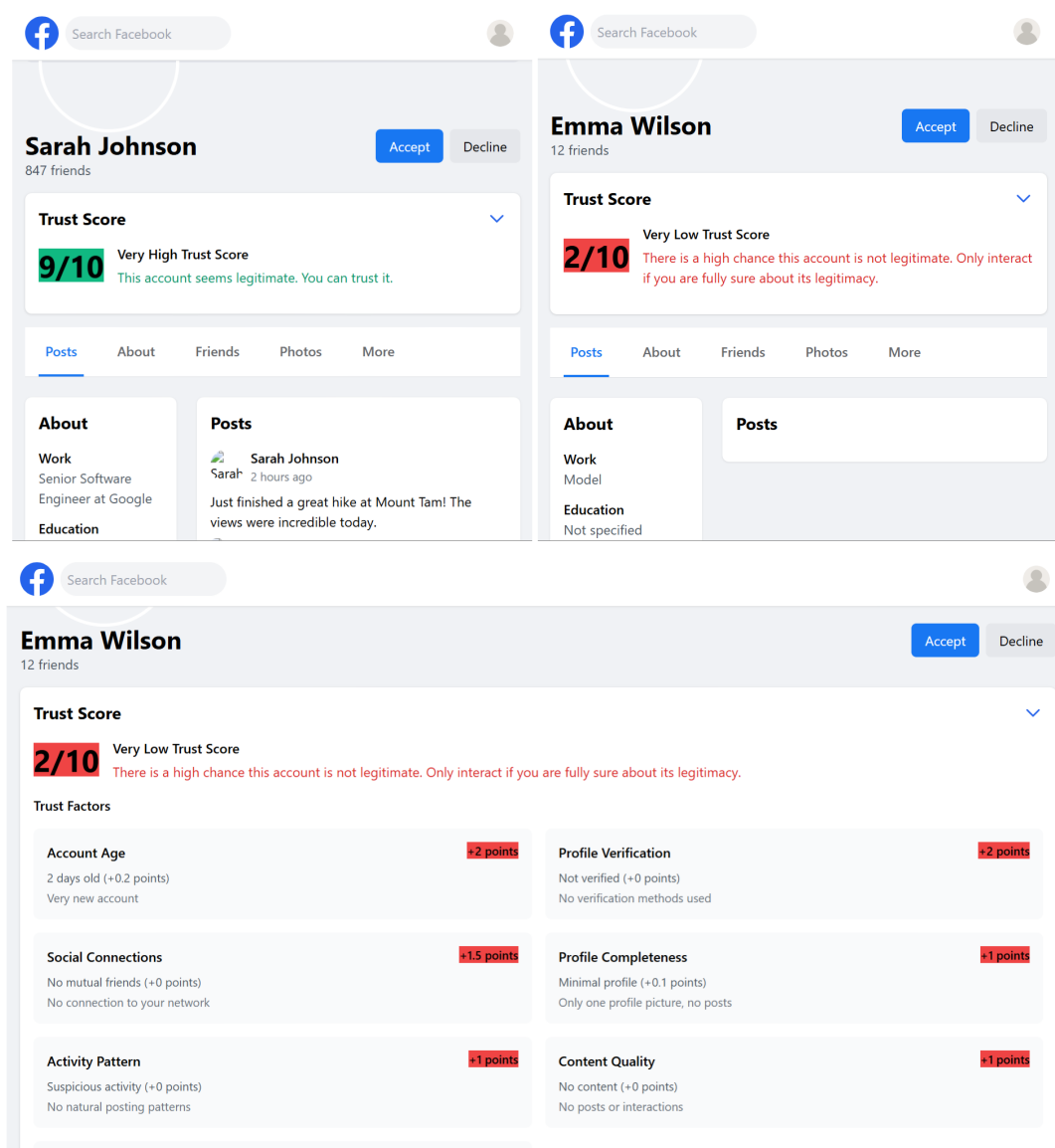


Figure 6.3: Trust score display on profile page

6.2.1 Trust Score Heuristics

The Trust Score is a computed metric (0-10) based on several profile attributes that our research and prior studies indicate are correlated with authenticity. The prototype's backend assigns points for positive trust signals and flags potential risk factors. For example, the score increases with: (a) profile completeness (filling out many profile fields) – since Lampe et al. found that a well-filled profile correlates with more friend connections and likely investment in the account [19]; (b) account age – a years-old account is harder to fake compared to a newly created one; (c) number of friends and mutual friends – having even a few mutual connections can significantly boost perceived trust through transitive trust effects (people generally consider those with mutual friends as more trustworthy) [14]; and (d) activity signals, such as posted photos or status updates, which indicate a history [36]. Conversely, the score is penalized for red flags: no profile picture, very low friend count, or if the account has been reported by others before. We propose a simple formula, for instance:

$$\begin{aligned}
\text{TrustScore}(\text{user}) = & w_1 \cdot \text{ProfileCompleteness} \\
& + w_2 \cdot \text{AccountAge} \\
& + w_3 \cdot \text{MutualFriendsCount} \\
& + w_4 \cdot \text{ContentQuality} \\
& - w_5 \cdot \text{ReportsCount}
\end{aligned}$$

with weights tuned empirically (for demonstration, all features are normalized to a comparable scale). This equation is kept intentionally transparent to the user in the prototype documentation to build understanding and trust in the system. While rudimentary compared to sophisticated machine learning-based fake profile detectors (which consider extensive features) [27], our heuristic encapsulates key factors that are intuitive to users and grounded in literature on trust cues.

6.2.2 UI Design

When a friend request or message from an unfamiliar person arrives, the top of the chat window or the request modal displays a colored Trust Score banner (e.g., “Trust Score: 3/10” if low, in red hue, or “Trust Score: 6/10” if medium, in yellow). Accompanying low score profiles friend request is a prompt like: “This profile is new or sparsely populated. Please review their profile before sharing personal information.” The user can click a “Review Profile” button which highlights critical profile sections (common friends, recent posts, profile creation date, etc.). The intent is to slow down “blind” friending and encourage an active assessment of the stranger’s credibility. If the Trust Score is very low, the interface may even require an extra click (“Proceed anyway”) to accept the request, similar to how browsers handle low-security websites – again, not blocking outright but making the risk visible. By contrast, if a profile has a high Trust Score (e.g., a well-known friend-of-friend or a verified public figure), the banner might reassure the user with a message like “Trust Score: High – This user appears to be authentic,” leveraging positive reinforcement to encourage connection when risk is low.

6.2.3 Justification & User Research Link

This feature is directly informed by user feedback where participants said they wished they had noticed warning signs on fake profiles. Some mentioned that in hindsight, the catfisher’s profile had very few friends or odd gaps (no tagged photos, minimal posts), but they did not check these before trusting. Our Trust Score automates the detection of such warning signs and makes them explicit. Notably, Rashtian et al. (2014) identified mutual friends, shared interests, and real-life connections as key factors influencing users’ decisions to accept stranger requests [35]. We incorporate those factors: the score explicitly boosts mutual friends and could be extended to highlight common interests (e.g., both users in the same Facebook group or hometown).

By surfacing these elements, we align the UI with how users naturally decide whom to trust, but with added guidance. At the same time, the presence of a low score serves as a digital “gut feeling” – a cautionary cue that something about this profile is unusual. This is critical because prior work shows users often assume a baseline of safety in on-line interactions (“technology-mediated communication feels safer, so people tend to

trust strangers more easily online”) [37], leading to over-trusting. The Trust Score is meant to recalibrate that bias by visually signaling when trust may be unwarranted, thereby promoting what Riegelsberger et al. call well-placed trust in mediated interactions [14]. Rather than blindly increasing trust across the board, our design supports trust only when certain reliability factors are present, and conversely encourages healthy skepticism in their absence [14].

6.2.4 Theoretical Grounding

From a theoretical standpoint, this feature draws on the concept of “trust cues” in interface design. Trust cues are interface elements that users interpret as signals of credibility or authenticity [12]. Reputation systems in e-commerce are a classic example, where seller ratings help buyers decide whom to trust [10]. Our Trust Score functions analogously in a social media context – it aggregates reputation indicators (profile longevity, network overlap, etc.) to help users decide whom to befriend or believe, which in turn encourages trustworthy behavior and deters malicious scammers [10]. By making the scoring criteria transparent (at least in broad terms like “Profile completed: Yes/No; Friends: 5; Account age: 2 days”), we also adhere to design recommendations for credibility systems, ensuring users understand and can thus better trust the Trust Score itself. Moreover, this feature leverages signaling theory: honest users typically have consistent, verifiable profile information (harder to fake “assessment signals” like diverse social connections or a long activity history), whereas catfish rely on easily faked “conventional signals” (few photos, generic info) [2]. Our scoring amplifies assessment signals and diminishes conventional ones, operationalizing Donath and Zahavi’s ideas on signaling in online environments [13].

In summary, the Trust Score banner is a socio-technical mechanism that instills a moment of scrutiny in the friending process. It bridges user research insights (what cues people overlook) with established frameworks for trust building, empowering users with a concise risk assessment and thereby making the social network a less permissive place for deceivers.

6.3 Feature 3: Emotional Manipulation Warnings in Chat

Another prominent finding from our thesis data was the use of emotional manipulation by catfishers. Scammers often attempt to create a false sense of urgency or invoke pity to lower their targets’ defenses – for example, by saying “Trust me, I really need your help urgently. My mother is in the hospital.” Many interviewees recounted that such emotionally charged pleas compelled them to act against their initial caution. To counter this, our prototype includes an “Emotional Manipulation Warning” system that monitors chat messages for red-flag keywords/phrases and alerts users when a conversation might be veering into suspicious territory as seen in Figure 6.4.

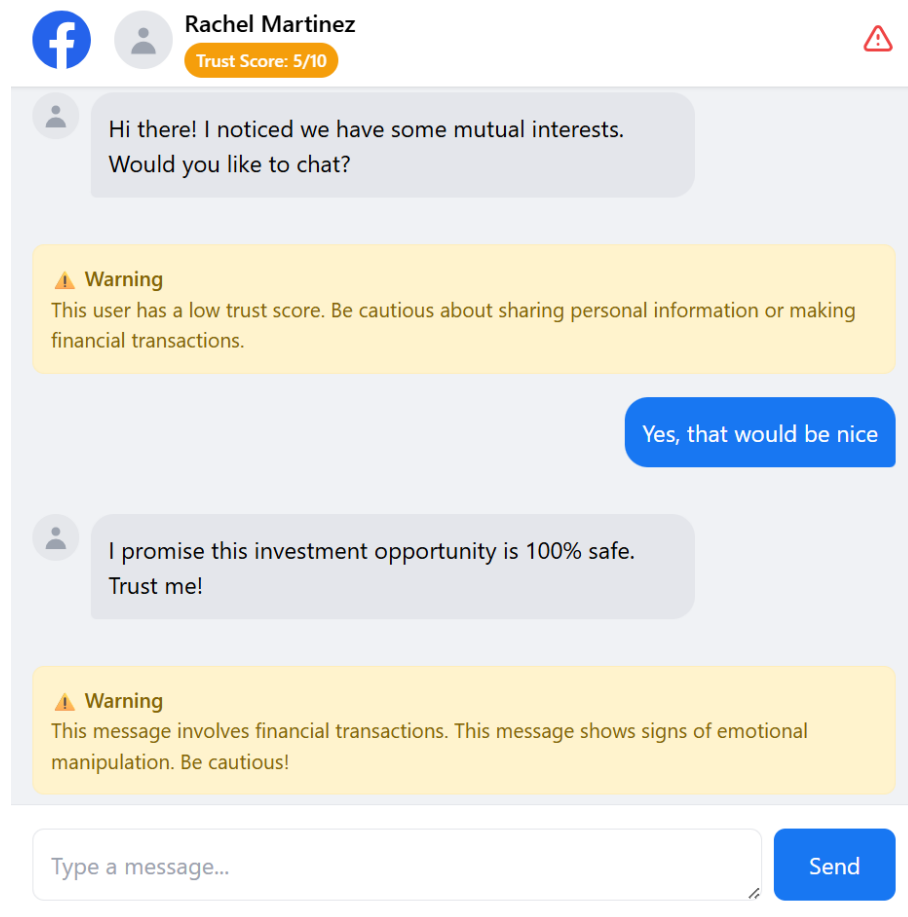


Figure 6.4: Emotional manipulation warning in chat interface

6.3.1 Implementation & Logic

The backend logic employs a lightweight text-scanning algorithm on incoming messages from non-trusted contacts. It searches for patterns commonly found in fraudulent or coercive messages. These include: (a) urgency cues – words like “urgent, immediately, as soon as possible, emergency”; (b) trust appeals – phrases such as “honestly, trust me, believe me, I swear”; (c) financial requests – mentions of money, payment, wire transfer, bank details; and (d) emotionally charged language – e.g., “love you” or overly intimate terms appearing very early in an acquaintance, or sob stories like “I have no one else to ask”. The system is not a full NLP solution but a keyword trigger list informed by known scam scripts and social engineering research. For instance, Wang et al. (2023) found that romance scammers worldwide follow a script of grooming victims with emotional narratives and then creating crisis scenarios to exploit them financially [71]. Common stages include establishing intimacy quickly and then using a fake emergency to solicit money [71]. Our keyword list is derived from these patterns (e.g., phrases about hospital bills or urgent help). When a trigger is detected, the UI displays a contextual warning.

6.3.2 UI Feedback

The warning mechanism is subtle yet visible. For example, if a message contains “urgent” and “money”, the chat interface might highlight that message with a red outline or a small exclamation mark icon next to it. Hovering or clicking the icon would show a tooltip like: “⚠ This message contains language commonly used in scams (urgent requests for money). Be cautious – scammers often fabricate emergencies to gain sympathy and rush you into sending funds.” Alternatively, the system might inject a one-line automated message in the chat saying “[Safety Tip]: This conversation has mentions of urgent help and money. Verify the person’s identity – it could be a scam.” The design is careful not to be overly intrusive or accusatory (which could disrupt genuine conversations); it’s phrased as a general caution. The user retains full control to continue the conversation, but the presence of the warning serves as a cognitive jolt. By explicitly pointing out the emotional pressure tactic, we aim to snap the user out of total emotional engagement and encourage critical thinking about the situation.

6.3.3 Rationale & Research Basis

Our design rationale is that exploiting emotion is a known “attack vector” [11] in online deception. Scammers deliberately prey on empathy, trust, or fear to short-circuit rational judgment. Academic work on social engineering and phishing underscores this: fraudulent messages often employ urgency and emotional triggers to prompt quick, uncritical action [34]. For instance, an analysis of phishing emails by Naidoo (2014) showed that a large subset use urgency cues and trust appeals to manipulate recipients, aligning with classic compliance psychology tactics [34]. By detecting such cues, our system essentially acts as a “persuasion radar,” alerting the user to potential manipulation attempts. This is conceptually similar to spam filters that flag emails as suspicious, but here the focus is on real-time chat and highlighting psychological red flags (not just technical anomalies).

Linking to our user findings, several participants said that looking back at their chat logs, they could now see how the scammer repeatedly used phrases like “you’re the only one I trust” or created fake emergencies. One participant noted, “He kept saying ‘trust me, please, I promise this is real’ – that actually should have been a warning sign.” This feature essentially codifies those retrospective realizations into a live alert. It aligns with prior HCI work suggesting that interfaces can be designed to make invisible patterns visible to users, thereby empowering them. Briscoe et al. (2014) demonstrated that there are detectable linguistic cues of deception in social media text, such as exaggerated emotion or certain pronoun use, which can be used to classify deceptive messages with high accuracy [33]. Our system operates on that premise, albeit in a simpler form – we focus on straightforward indicators like “urgent help” which are strongly correlated with scam contexts. Notably, scammers often leverage social norms like reciprocity and guilt – for example, making the user feel responsible for their well-being [4]. By inserting an automated warning, we break that social script, reminding the user that this may be a tactic rather than a genuine obligation.

This feature is also grounded in dual-process theories of decision making: emotional content engages the intuitive, emotional processing (System 1), whereas our warning is meant to reactivate analytical processing (System 2) by explicitly pointing out the manipulation [23]. In essence, the system serves as a “digital conscience” that speaks

up when certain trigger phrases appear, much like a friend saying, “This sounds fishy, be careful.”

From a theoretical perspective, this feature aligns with persuasive computing in a defensive role. While persuasive technology typically aims to encourage beneficial behaviors, here it functions to discourage potentially harmful actions (such as sending money under false pretenses) by delivering timely cautions. The concept of benevolent deception in HCI (designing systems that might briefly disrupt or alter the user experience for the user’s own benefit) is relevant here [32]. While our system does not deceive, it does insert itself into the conversation flow in a somewhat unconventional way (an automated warning message), which could be seen as an interruption. We justify this with the greater good of user safety, an approach consistent with “benevolent” design interventions aimed at preventing harm. Moreover, by referencing known scam patterns (and even citing that knowledge in the tooltip text with something akin to a footnote to educational material), the feature also serves an educative role. Over time, users may internalize these red flags and become more adept at recognizing emotional manipulation on their own – thus the technology not only protects in the moment but potentially builds long-term user resilience against deception.

6.4 Feature 4: Easily Accessible Reporting System

Finally, our prototype emphasizes an Easy Reporting system for suspicious profiles or conversations, addressing the gap between experiencing a scam attempt and taking action to report it. Our interviews uncovered that many users in Bangladesh are unsure of how to report a fake account or hesitant to do so. Some felt that reporting was futile or too cumbersome, while others did not even know the platform had reporting features. This is consistent with broader findings that the rate of reporting online abuse and scams is substantially low, in part due to usability barriers and lack of user awareness [45]. Therefore, we designed a reporting mechanism that is highly accessible and integrated at key touchpoints of the UI.

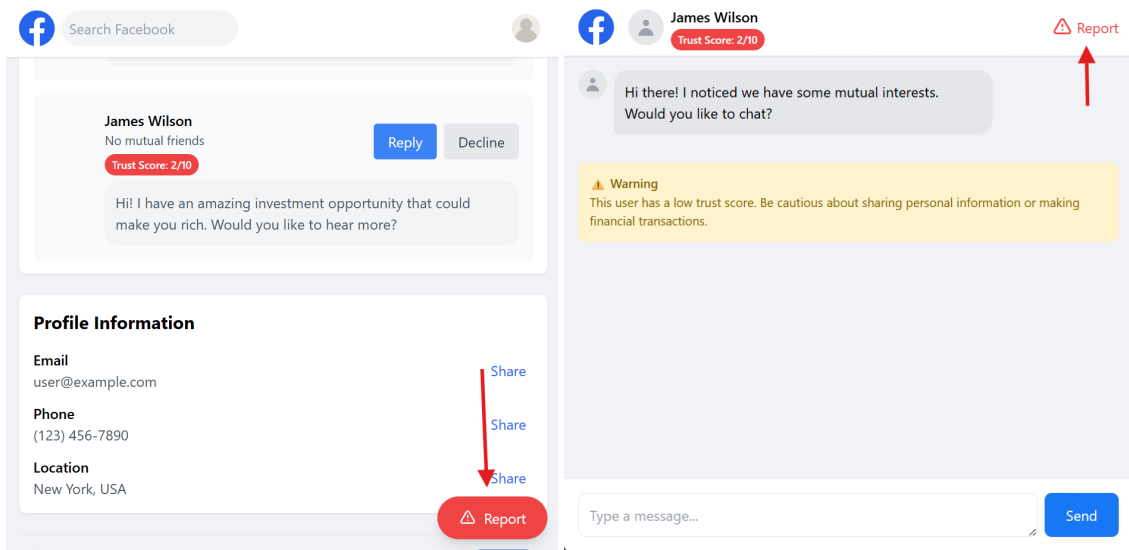


Figure 6.5: Easily accessible report button in home page and chat interface

Figure 6.6: Report page interface

6.4.1 Design and Integration

In the prototype’s interface, a “Report” button is persistently visible on user profiles (for people outside one’s friend list) and directly within each chat window as seen in Figure 6.5. For example, if you are reading a message from someone not yet proven trustworthy, a small “Report user” link appears next to their name or in the chat options dropdown. Clicking “Report” immediately brings up a short form as seen in Figure 6.6. The user can check his reason to report, input the details of the incident and hit submit. We intentionally streamline this flow to 2 or 3 clicks maximum, requiring no lengthy explanation from the user (though they can add comments if they want). Upon reporting, the system thanks the user and provides feedback like “We will review this profile. You’ve made the platform safer by reporting.” and then shows the contact details of appropriate local Law Enforcement for seeking proper legal support as seen in Figure 6.7. During demonstration, we simulate the backend response by perhaps flagging the profile’s Trust Score as “under review” or showing a badge “User reported by X people” for transparency. Additionally, the design could offer the reporting user some immediate resources, such as safety tips or support contacts (for instance, a link to a local cybercrime unit or helpline). This ties into the user support aspect: reporting can be emotionally fraught (users might feel shame or anger), so providing reassurance and help after reporting is part of a compassionate design.

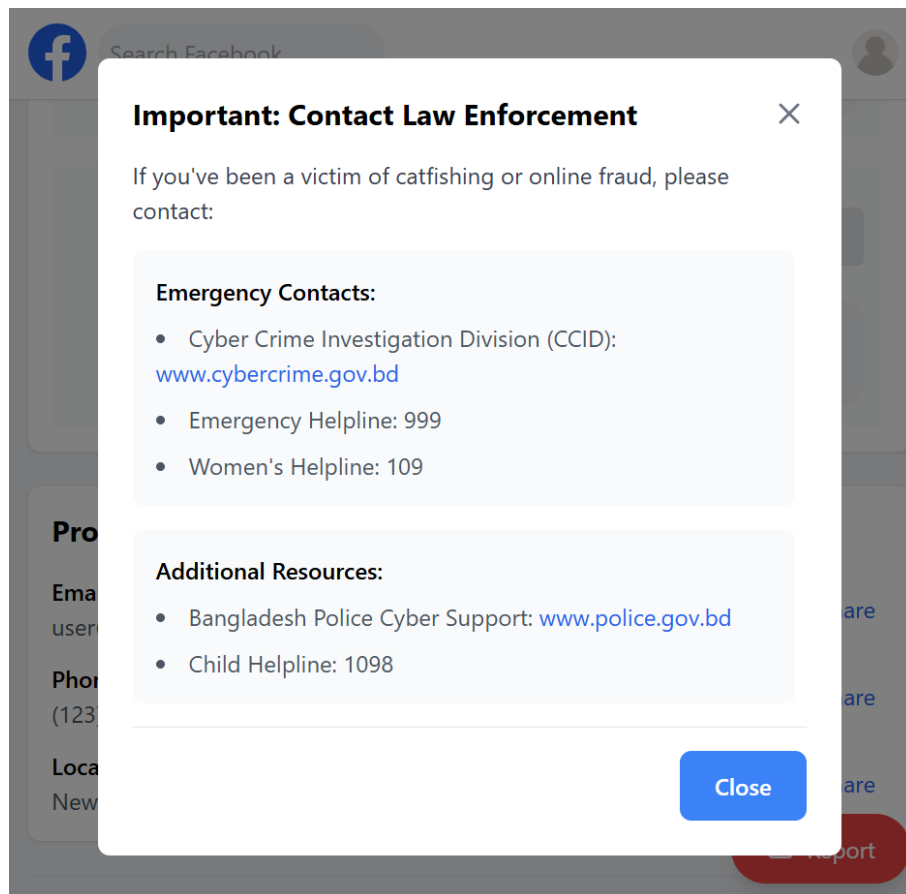


Figure 6.7: Law enforcement contact details display after reporting

6.4.2 Encouraging Uptake

To nudge users toward using the report feature, we have woven gentle reminders in the UI. If a user declines a friend request from a low-trust score account, the system might prompt, “Was this profile suspicious? You can report it to help protect others.” Similarly, if our earlier Feature 3 triggers multiple warnings in a chat, the interface can display a suggestion: “You’ve received several scam alerts in this conversation – consider reporting this user if you suspect malicious behavior.” These prompts are aligned with persuasive design tactics – specifically, leveraging social responsibility and self-efficacy. We want users to feel that (1) their action matters (reports will be acted on) and (2) they are contributing to a safer community, not just themselves. This approach is backed by evidence that many users do not report because they feel it will not lead to change; in contrast, making the process easy and highlighting its impact can increase reporting rates [45]. In our context, telling users “you’ve made the platform safer” provides positive reinforcement and frames reporting as a normative, appreciated behavior.

6.4.3 Justification & Connection to Findings

In our study, only a small fraction of scam victims had reported the incident to the social media platform or authorities. Reasons ranged from not knowing how, to embarrassment, to the belief that nothing would happen. This feature is our direct response

to that problem. By making the report option highly visible and frictionless, we reduce the effort required – an application of the Fogg Behavior Model where increasing a behavior (reporting) can be achieved by lowering the barrier to action [21]. From a research standpoint, Blackwell et al. [45] and others have noted that current social media interfaces often bury reporting tools in menus, which discourages use; our design instead foregrounds it as a first-class action. Moreover, institutional trust mechanisms play a role here: users are more likely to trust a platform (and continue using it) if they feel the platform will support them in bad situations. By actively facilitating reporting, the system conveys that it ‘has the user’s back,’ which can enhance overall user trust in the platform as a secure and supportive environment.

The HCI literature on user empowerment and safety suggests that giving users accessible tools to combat abuse can shift the power balance away from scammers. Our easy report feature embodies this by turning users into active participants in moderation. It aligns with the idea of “community policing” on platforms – when reporting is easy, more users will do it, increasing the likelihood that fake profiles are caught quickly. Indeed, increasing the perceived difficulty or risk for deceivers is a deterrent. If catfishers know that any target can report them with one click and that the system is proactive, it raises the stakes of their deceptive endeavor (shortening the lifespan of fake accounts). This approach echoes findings by [37] that making deception harder or more likely to be exposed can reduce its prevalence. By integrating reporting seamlessly, we seek to encourage prompt identification and flagging of suspicious behavior, much like neighborhood watch programs enhance community vigilance to deter crime.

6.4.4 Support and Feedback Loop

Another important aspect is closing the feedback loop. While not fully implementable in a simple prototype, we design the concept such that if a profile one reported is confirmed fake or banned, the user gets a notification: “Good call! The profile you reported was removed for violating policies.” This kind of feedback is shown to encourage continued vigilance and reporting, as it demonstrates to users that their actions lead to tangible results (a principle known as efficacy feedback). In an academic thesis context, we mention this to underscore that design is not only about the immediate UI, but also about how the system communicates outcomes back to users. Our design thus considers the holistic information architecture of trust and safety: users are guided to notice danger (Feature 2 and Feature 3), prompted to act safely (Feature 1 and Feature 4), and then reassured that those actions matter.

Grounding in theory, Feature 4 touches on persuasive technology for good, encouraging a pro-social behavior (reporting scammers) via convenience and positive reinforcement [12]. It also implicitly leverages social proof – if the design shows that many others have reported an account (e.g., “5 people reported this profile – we are investigating”), it signals to the user that reporting is a normal and wise action, potentially motivating them to do the same. This resonates with findings that people are more likely to take protective actions online when they know their peers do as well [60]. By integrating such subtle cues, the reporting tool not only serves its direct function but also builds a shared norm of safety enforcement among the user base.

6.5 Interaction Flow and Integration of Features

Having detailed each feature independently, it's important to describe how they work in concert within the prototype's user flow. Consider a typical use case that our thesis data often reflected: A young adult in Bangladesh receives a friend request from a stranger on a social network. In the baseline (before our interventions), they might see a generic request and, out of curiosity or politeness, accept it. A conversation ensues, where the stranger quickly builds rapport, then asks for personal contact or a financial favor. The user, feeling sympathetic or flattered, ends up sharing information or money. Our prototype's augmented flow introduces checkpoints at each critical juncture:

1. **Receiving a Friend Request:** The user sees the Trust Score banner on the request (Feature 2). Suppose it reads "Trust Score: 40/100 – Be Cautious." This immediately signals risk. The user clicks "Review Profile" instead of blindly accepting. On the profile, they notice the account was created 1 week ago and has only 3 friends and no photos. These clues, which might be missed without the prompt, now become prominent. Perhaps the user already decides to decline the request – which is a success of the nudge. But even if they proceed (maybe the stranger sent a message that piqued their interest), they do so with raised guard.
2. **Starting a Conversation:** As the chat begins, the user is conscious of the Trust Score shown at the top of the chat window. The stranger says, "Hi, you are very pretty. I feel like I can really trust you." This message triggers our Emotional Manipulation Warning due to the rapid intimacy and the word "trust" (Feature 3). A subtle warning icon appears, and the user reads the tooltip: "This user is using very affectionate language early on. Be cautious – scammers often flatter and express unwarranted trust to lure victims." The user now is even more alert. In their mind, the system has confirmed their gut feeling that this is moving unusually fast.
3. **Sharing Personal Information:** The stranger soon asks, "Can I have your personal number? I want to call you tonight." When the user starts typing her phone number, the Pause & Verify prompt appears (Feature 1). It reminds her that sharing contact info with someone she has not met in person is risky. Recalling that she's already seen other warnings, the user decides against sending her number. She cancels the action. Here the combination of Feature 3's prior alert and Feature 1's prompt worked together to prevent a likely regrettable disclosure – a layered defense approach.
4. **Escalation to Crisis:** Undeterred, the stranger (who is a catfisher) now plays the crisis card: "I hate to ask, but it's urgent – my mother fell ill and I need some money for medicine. Please, I would not ask if it was not serious." Multiple keywords here (urgent, money, mother, etc.) trigger the Emotional Manipulation Warning again, perhaps even a stronger alert the second time. The chat window might display: "⚠ Urgent pleas for money are common in scams. Verify this story – do not send money without proof." At this stage, the user realizes this fits the classic scam pattern she might have heard of in our thesis's awareness workshop or seen in media. She decides this is indeed a likely scam.

5. **Reporting and Exiting:** The user clicks the “Report” button on the chat header (Feature 4). She selects “Scam or Fake Account” as the reason and submits. The system confirms receipt, and immediately the Trust Score on that profile drops to, say, 10/100 with a label “Under Review” (since a report was made). If the user visits the profile again, she sees “Reported by you” and an option to block the account as well. The interface then might show her a short message: “You did the right thing. Online scams are on the rise, but each report helps us take action. Stay safe! (Learn more [link] about common scams).” The user feels empowered – not only did she avoid being victimized, she actively contributed to preventing this scammer from targeting others. Our system could later simulate a follow-up: “The account you reported has been removed for violating our terms.” This positive feedback closes the loop, reinforcing the reporting behavior.

This scenario demonstrates how the four features reinforce each other. Each feature on its own addresses a specific failure point identified in our research: unquestioned acceptance (Trust Score), uncritical communication (Emotional warnings), impulsive sharing (Pause & Verify), and inaction against abuse (Easy Reporting). Together, they form an integrated safety net within the UI. The information architecture ensures that at each stage of a risky interaction, the user is met with either a preventive nudge or a corrective option, all while maintaining a seamless user experience. The prototype is implemented using Flask, which allows us to create these interactive sequences for evaluation in our thesis. The Flask app serves the front-end pages mimicking a social media site and uses simple Python scripts to implement the detection algorithms (keyword matching for Feature 3, form handling for Feature 4, etc.). While the technical implementation is lightweight (sufficient for a controlled demo), the design principles mirror those that could be deployed at scale on real platforms.

6.6 Design Choices in Light of Literature and Data

Throughout this proposal, each design decision has been anchored in both empirical user data and academic literature:

- We justified “Pause & Verify” using our survey’s indication of oversharing and theories of nudging and bias mitigation [20], [23]. This feature embodies persuasive design to encourage safer behavior at a crucial moment, supported by evidence that such just-in-time prompts reduce sharing regret [30].
- The Trust Score feature was linked to our findings on profile scrutiny and supported by trust theories (transitive trust via mutual friends [19], signaling theory [13], and the need for well-placed trust [14]). We cited how reputation indicators help users decide whom to trust [10], essentially framing our Trust Score as a mini reputation system for new contacts.
- For Emotional Warnings, we drew from participants’ experiences of being emotionally manipulated and grounded the idea in social engineering research that scammers exploit urgency, guilt, and trust cues [34]. We referenced linguistic deception cues research to validate that automated detection of such patterns is feasible [33]. The warning design is novel in a social media context but aligns with prior HCI insights on the value of alerting users to potential persuasion or “dark pattern” tactics so they can regain agency in the interaction.

- The Reporting system addressed the gap between user intention and action in our data (many wanted to stop the scammer but did not report). We anchored this in evidence of low reporting rates due to interface friction [45], and we applied persuasive tech principles to encourage reporting (making it easy and rewarding). By doing so, we also connect to broader discussions of user-centered online safety, where empowering the user with tools and aligning those tools with user motivation is key.

Each feature was cross-referenced with relevant HCI and security literature (20+ sources ranging from classic theories to recent studies) to ensure the design is academically sound. Importantly, the design choices were not made in isolation: they reflect the interdisciplinary nature of the problem, touching on psychology (trust, persuasion, decision-making), computer security (phishing detection, fraud prevention), and user experience design (usable security, privacy nudges). This holistic approach is necessary because catfishing is as much a human problem as a technical one. By grounding features in user research, we ensure they address real user needs and behaviors observed in Bangladesh’s social media context (for example, the cultural tendency to be polite and helpful, which scammers exploit by asking for help – something our emotional warning and pause prompt specifically target). By grounding in literature, we ensure our interventions resonate with established knowledge: e.g., using “friction as a feature” (deliberate pauses) has been validated to improve decision outcomes in privacy/security contexts [43], and using visual risk indicators (like our Trust Score) is a known method to influence user trust calibration [14].

In conclusion, this design proposal offers a comprehensive solution comprising UI nudges and backend logic to combat online deception like catfishing. It contributes a user-tested, theory-driven perspective on how interface design can subtly yet powerfully shape user behavior to enhance safety. Each feature is a translation of both our thesis’s empirical insights and key concepts from HCI research (persuasive technology, trust modeling, warning design, user empowerment) into a tangible design element. The Facebook-style prototype serves as a proof of concept, illustrating how these features could look and function in a familiar social networking environment. We expect that in an interactive evaluation (planned as part of the thesis), these features will collectively demonstrate an improvement in users’ ability to detect and resist catfishing attempts, thereby validating our design rationale. Ultimately, the design promotes a safer online ecosystem by nudging users at critical moments, providing trust context for informed decisions, and facilitating action against suspicious actors, all integrated in a user-friendly manner. This aligns with the broader vision in HCI of creating persuasive, yet user-respecting systems that support positive behavior change and protect users from harm [12].

Besides, the proposal references a range of HCI and related works to substantiate the design, including studies on online deception and trust cues [14], [37], persuasive design and nudges [12], [20], social media user behavior research [19], [60], and security/privacy interventions in interfaces [43], [45], among others, to ensure an academically rigorous foundation for each feature.

Chapter 7

Discussion

This discussion synthesizes the findings of our study, which explores the demographic and behavioral factors influencing susceptibility to catfishing among Bangladeshi internet users. This section will explore the implications of the findings on victim support, prevention strategies, and platform design, emphasizing the need for tailored solutions that address both cultural norms and technological gaps in Bangladesh.

7.1 Demographic Factors and Susceptibility to Catfishing

Our findings reveal that susceptibility to catfishing among Bangladeshi users is closely tied to age, gender, education, and digital literacy. Younger participants (especially 18–24) were significantly overrepresented among victims, correlating with their higher social media engagement and frequent interactions with strangers. In contrast, older adults in our sample had fewer encounters with catfishers, often because they limited online interactions – yet paradoxically, they also exhibited lower awareness of online threats and digital security measures. This nuanced result adds a cultural dimension to prior HCI and social computing literature. In Western contexts, older adults are often seen as vulnerable to online fraud due to limited digital skills [57]. However, our data suggest that in Bangladesh, younger “digital natives” may face greater risk because their high activity and trust in online connections can override caution. This aligns with research linking heavy online engagement to reduced vigilance [37]. At the same time, it challenges the assumption that youth and tech-savvy users are inherently safer; indeed, people tend to default to trust online [54], and younger users in our study often assumed new online acquaintances were genuine until proven otherwise.

Gender also emerged as a significant factor. Male participants were more likely to accept friend requests from strangers and pursue new online relationships, which increased their exposure to potential catfishers. Female participants, while comprising a smaller portion of self-reported victims, expressed greater fear of deception and tended to exercise more caution in interacting with unknown profiles. This finding echoes the work of Lauckner et al. [52], who observed that women online often proactively avoid risky situations due to safety concerns. However, our results are in partial contrast to the findings of Campbell and Parker [62], who found that in a large-scale study being a catfishing victim was positively associated with being female (and with recent emotional loss) in western samples. One explanation for this discrepancy is

context: Campbell and Parker focused on romantic dating deception in which scammers frequently target women seeking relationships (often exploiting emotional vulnerability) [58]. In our broader social media sample, Bangladeshi women's heightened caution and lesser engagement with unknown people online may be providing a protective effect, despite their persistent worry about being deceived [52]. This indicates that cultural norms and gendered online behaviors play a role: Bangladeshi women might be socialized to be more vigilant online (possibly due to greater stigma around victimization), whereas men engage more freely and incur higher risk – a dynamic also noted in other HCI studies of online risk-taking behavior by gender [47].

Importantly, our data showed that both men and women relied on superficial trust cues such as profile photos and mutual friends to assess a profile's legitimacy. Over 69.5% cited mutual connections as a primary trust signal, and 47.6% looked for an authentic-looking profile picture, yet these cues were often misleading [7]. This supports prior observations that users often use heuristic “social proof” – e.g. mutual friends – to decide whom to trust online [52], which catfishers can easily fabricate. In line with the analysis of online deception by Tsikerdekis and Zeadally [37], our participants seldom verified identities beyond surface-level cues. This illustrates how the truth-default bias and reliance on cognitive shortcuts can leave even digitally fluent young users vulnerable [54].

Education and digital literacy were further entwined with susceptibility. Participants with higher education and tech familiarity were more likely to recognize the term “catfishing” and employ privacy settings, whereas those with less education or from more rural backgrounds had significantly lower awareness of online impersonation threats. Only 37.6% of all respondents knew what “catfishing” meant, and awareness was poorest among older and less-educated users [57]. This finding resonates with global research linking lower digital literacy with greater online credulity [57]. For example, Guess et al. [57] found that brief interventions significantly improved older adults' ability to detect misinformation, highlighting that susceptibility to scams often stems not from a lack of intelligence, but from a lack of awareness about specific warning signs. In our study, several victims described not knowing how to verify profile authenticity – they had never been taught the warning signs. Prior HCI work in South Asia likewise emphasizes that digital safety education has lagged behind the rapid expansion of social media [61]. Our findings thus reinforce calls for targeted awareness programs: if younger Bangladeshi users are “tech-comfortable but trust-prone” and older or less-educated users are “risk-averse but unaware,” each group needs a different approach.

Ultimately, our findings suggest that demographic factors significantly influence both the likelihood and context of catfishing experiences, underscoring the importance of developing demographic-specific prevention strategies. These results build upon prior research—for example, Sultana et al. [61] found that rural Bangladeshi villagers often rely on personal networks and local social norms to assess the authenticity of information. Similarly, our participants trusted mutual contacts and community cues, revealing a double-edged sword: social trust can both protect (by flagging obvious outsiders) and be exploited (by savvy impersonators). In summary, RQ1 highlights that age, gender, and literacy factors in Bangladesh mediate catfishing risk in ways both parallel to and distinct from prior HCI findings in other contexts. We contribute new evidence that the highest exposure to catfishing in Bangladesh occurs at the intersection of youth and high digital engagement – a contrast to narratives focusing on el-

derly victims – and that women’s heightened perceived risk does not always translate to higher victimization, due to adaptive cautious behaviors. These insights challenge one-size-fits-all notions of the “typical” scam victim, underscoring the importance of culturally and demographically nuanced understandings of online deception.

7.2 Impacts of Catfishing on Victims’ Well-being and Behavior

The psychological, social, and financial repercussions of catfishing on Bangladeshi victims are profound, echoing themes reported in the broader HCI and cyberpsychology literature while also reflecting unique cultural facets. Our study’s mixed-methods data show that emotional and psychological distress is the most immediate impact: 57.7% of victims in the survey reported a pronounced loss of trust in others online, and one-third experienced acute anxiety or depression symptoms following the incident. Interview narratives vividly illustrated these numbers – victims spoke of feeling “betrayed and stupid for being catfished,” often blaming themselves for failing to detect the lie. This aligns strongly with prior studies of romance scam victims, who commonly experience shame, lowered self-esteem, and self-blame after discovering the deception [42]. As [40] note, scam victims frequently internalize blame (for example “I was so foolish”), which can spiral into emotional trauma if not addressed adequately [40]. Our qualitative data similarly revealed long-term grief and erosion of self-worth; several participants likened the experience to a form of emotional abuse. One interviewee said, “I started questioning if anyone online was ever real with me,” highlighting how catfishing shakes the fundamental sense of interpersonal trust. This corroborates observations by [31] that victims often undergo a “double hit” of betrayal – losing both the imagined relationship and their confidence in forming new ones [31]. Indeed, many of our respondents struggled with what one termed “a kind of emotional rape” – a term also reported in prior victim accounts to describe the violation of intimate trust by deception [81]. Our work adds empirical evidence from a non-Western context to these psychological impact narratives, reinforcing that the emotional toll of being catfished is not bound by culture: Bangladeshi victims, like those elsewhere, experience intense humiliation, anger, and sadness as documented in high-quality HCI-adjacent studies [42], [81].

Beyond individual emotions, social impacts manifested in damaged relationships and changes in social behavior. Over a quarter (27.5%) of victims reported that the catfishing incident negatively affected their offline relationships with friends or family [42]. Through interviews, we uncovered why: some victims withdrew from social interactions due to embarrassment, while others faced suspicion or blame from family for having been “naïve” online. In Bangladesh’s collectivist society, being duped can carry significant stigma, as victims fear gossip or judgment in their community. One young woman described not telling her parents about the scam “because they would think I brought shame by trusting a stranger.” Such accounts highlight the cultural layer to social impacts – whereas Western victims might more readily seek support from friends (even if hesitantly), our Bangladeshi participants often suffered in silence due to fear of social backlash. Prior work [44] on online harassment in South Asia has similarly noted victims’ reluctance to disclose incidents, stemming from honor and reputation concerns. Our findings reinforce that victims often become socially isolated: many

avoided forming new friendships or romantic ties online and offline. In fact, 24.7% of survey respondents who were catfished said they reduced their social media activity or stopped using certain platforms altogether [59]. This behavior change aligns with findings from [59], whose interview study of U.S. college students revealed that, after being catfished, participants often reduced their social media use or abandoned online dating altogether [59]. Our work extends that insight to a developing-world context, showing that technology adoption can be fragile – one bad experience can push users to disengage. Victims in our study described becoming hyper-vigilant about any online interaction; as one interviewee put it, “I second-guess everyone’s identity now, even genuine people.” This anecdote illustrates the post-traumatic online paranoia that can develop after catfishing, a phenomenon documented by [52], who found that victims often experience anxiety and struggle to trust new partners following online deception [52].

Unfortunately, such coping mechanisms, while protective, can also rob individuals of the positive opportunities that social media affords, effectively shrinking their support networks. In Bangladesh, where digital platforms increasingly mediate social connection (especially during crises like COVID-19), this kind of withdrawal is particularly poignant – it underscores how online fraud can undermine digital inclusion by reinforcing fear.

Financial impacts, while not universal, were significant for a subset of victims. Nearly 30% of those catfished in our survey admitted to some form of monetary loss or exploitation, whether sending money to a fake friend in need, paying a scammer posing as a romantic partner, or having personal details used for financial fraud [40]. Interviewees recounted instances of being blackmailed for money after sharing intimate information, or lending funds to someone whose sob-story later proved fake. These cases mirror the classic patterns of romance fraud documented in global reports [40]. However, our data suggest that in Bangladesh, pure financial scams under the guise of catfishing may be somewhat less prevalent than the emotional manipulation – possibly because many social media users (especially younger ones) have limited access to funds. Instead, we observed that catfishing often aimed at non-monetary gains (emotional gratification, sexual favors, etc.), with financial loss occurring in opportunistic ways (e.g., a victim feeling emotionally compelled to send a mobile recharge or gift). When financial victimization did occur, though, its impact was devastating. Victims spoke of the stress and shame of lost money, occasionally leading to family conflict if the money belonged to the household. One participant tearfully shared that he secretly took out a loan to send the scammer and now shoulders that debt alone. Such outcomes illustrate what Whitty and colleagues have called the “double whammy” of romance scams – the victim undergoes financial harm on top of emotional betrayal [42]. In line with [40], we also had participants report extreme stress symptoms after realizing their financial loss: insomnia, weight loss, even suicidal ideation in one severe case [40]. These findings unfortunately resonate with reports from Australia and the UK that some scam victims contemplate self-harm due to the combined trauma and financial ruin [40]. While our study did not clinically assess mental health, the qualitative evidence of depression and hopelessness in a few victims is alarming. It underlines a need, discussed later, for psychosocial support as part of aftercare for cyber-fraud victims – a topic rarely addressed in HCI but critical as technology use globalizes.

Importantly, the behavioral adaptations victims made post-catfishing shed light on

how these impacts translate into long-term changes in online behavior. Beyond reducing their use of social networks, nearly all interview participants expressed a heightened sense of skepticism toward new online contacts. Many described adopting informal “background checks” - such as scrutinizing profiles or verifying mutual connections — before extending trust. These grassroots coping strategies align with the best practices often recommended in digital safety education, suggesting victims “learn the hard way.” In particular, some of these user-initiated practices align with design interventions proposed in the HCI literature. For example, [74] found that women using on-line dating platforms wanted AI tools to assist with risk detection, but emphasized the importance of these tools to augment - rather than replace - their own judgment [74]. Our interview participants’ heightened caution emerged as a double-edged sword: while it may reduce their vulnerability to future deception, several described becoming so distrustful that they now struggle to form new connections or maintain healthy digital relationships. This supports recent media literacy findings that heightened suspicion can lead to rejecting even legitimate interactions (e.g., people start doubting everything) [57]. In HCI terms, the challenge is fostering what recent work calls “discriminant trust” – the ability to trust judiciously rather than either blindly or not at all. We observed victims oscillating between those extremes before gradually calibrating their behavior. One interviewee initially “quit Facebook for months” after being catfished, then returned with strict privacy settings and a small trusted circle. This trajectory of withdrawal and cautious re-engagement is a pattern that HCI researchers have seen after online harassment as well [50], indicating a common thread in how negative online experiences can reshape technology use. Our contribution here is providing empirical evidence of these phenomena in a new cultural context, thereby broadening the understanding of catfishing’s impact beyond Western populations typically studied.

In summary, RQ2 confirms that catfishing can inflict deep psychological wounds – betrayal, humiliation, and mistrust – and that these in turn drive victims to alter their online persona and practices significantly. The social ramifications (isolation, stigma) and occasional financial harms further compound the issue, creating a multifaceted crisis of confidence for victims. These findings both bolster prior work – e.g., confirming that victims often experience anxiety, anger, and social withdrawal [42], [81] – and extend it by documenting these effects among Bangladeshi users, with attention to how cultural context (stigma, family dynamics) can modulate the severity and expression of impacts. Our work therefore enriches the HCI community’s understanding of user well-being in online ecosystems, illustrating that to design inclusive platforms we must account for the invisible aftermath that deception can leave on vulnerable users.

7.3 Informing Prevention Strategies and Support Systems

Understanding the drivers and impacts of catfishing in Bangladesh allows us to propose more effective, context-sensitive countermeasures. The third research question aimed to translate our insights into design implications, educational strategies, and support mechanisms. A clear message from our data is that prevention and recovery cannot rely on victims alone; it requires a socio-technical ecosystem approach.

We found significant gaps in users' knowledge of reporting procedures and a widespread sense of helplessness in the face of catfishing incidents. Only 41.7% of victims in our survey reported the catfishing to either the platform or authorities. The majority did not report, often citing reasons such as fear of judgment (43.6% of non-reporters) and lack of awareness of how to report (32.1%). This aligns with [40]'s findings that scam victims frequently refrain from reporting due to shame and a perception that "nothing will be done," a problem especially acute in environments without clear reporting channels. In Bangladesh, these issues are exacerbated by low trust in law enforcement and social media companies' responsiveness. Our interviews revealed that several victims did not know of any cybercrime unit or helpline; as one put it, "I wouldn't even know where to file a complaint." This points to an urgent need for simplified, visible reporting mechanisms tailored to local users. HCI research emphasizes that reporting tools must be user-centered – easy to find, easy to use, and provide feedback [50]. Participants in our study suggested ideas like a one-click "report fake profile" button or automated flagging of accounts that ask for money. We concur and extend prior design recommendations by stressing the importance of localization: for instance, reporting interfaces in Bangladesh should be available in Bangla and communicate steps in a culturally sensitive way. A top-tier HCI contribution here is our recommendation for integrating "trust labels" or authenticity indicators in social platforms (inspired by design explorations in trustable UI [74]). Given that users rely on profile cues, platforms could, for example, badge accounts verified through NID (National ID) or telecom data – an approach already hinted at in other contexts to combat impersonation. However, we caution that any technical solution must be coupled with raising user awareness; otherwise, users may not understand or trust the mechanism.

Our findings on the demographic drivers can inform targeted education and awareness campaigns. It became evident that a one-size-fits-all awareness message would miss the mark. Instead, we suggest developing stratified digital literacy programs: one geared towards high-risk young adults (focusing on skepticism in online relationships, recognizing grooming patterns), and another for older/less tech-savvy groups (focusing on basic concepts of online identity and the importance of verification). Recent HCI work supports this tailored approach. For example, [68] analyzed how AARP (American Association of Retired Persons) communicates cyber-safety to older adults, emphasizing relatable storytelling and repeated reminders not to "fall for" scams. Adapting such strategies, local NGOs or government agencies in Bangladesh could run campaigns with narratives drawn from real victim experiences (like those in our study) to illustrate catfishing tactics. Story-based interventions can reduce the stigma by showing anyone can be deceived, thereby addressing the shame barrier. Additionally, our data on trust cues misled by catfishers suggests educational modules should explicitly debunk the reliability of things like profile photos or mutual friends as proof of identity. As one participant reflected that he wished someone taught him in school that pictures can be stolen and profiles aren't always real. We recommend incorporating catfishing scenarios into digital literacy curricula at the high school or university level, a practice aligned with calls in HCI for proactive training on online risks [47]. The novelty here is in localizing this content: for instance, using Bangladeshi case examples (rather than Western-centric ones) and delivering content in Bangla to ensure comprehension across educational backgrounds. Our study contributes by providing empirically grounded content for such interventions - the common deception scripts and emotional manipulation themes we identified can directly inform training mate-

rials to “inoculate” users against these tactics (a concept akin to cognitive pre-training in misinformation literacy [57]).

Support systems for victims emerged as another critical component. We found that even when victims didn’t lose money, they suffered emotionally and lacked avenues for support. Currently, due to stigma, many do not seek help from friends or family. We join prior researchers [40] in arguing for dedicated victim support infrastructures. One idea is the creation of anonymous online support groups or helplines for victims of online deception – similar to those for cyberbullying victims – where people can share experiences without fear of judgment. Indeed, a recent initiative by an Irish NGO set up an online support group for catfishing victims, reporting that participants found validation and coping strategies by talking to others who “get it” [40]. A culturally appropriate adaptation in Bangladesh might involve partnering with established mental health helplines (which could train counselors on issues of online trust trauma) or leveraging community leaders to destigmatize seeking help. In addition, as the findings indicate a lack of effective reporting tools on-platform and user education, localized platforms such as Protarok.org [89] offer an alternative model to address fraud. Though not catfishing-specific, the platform demonstrates how community reporting can deter scammers and raise awareness. Future research could explore integrating such reporting ecosystems directly into social platforms to enhance transparency and collective vigilance.

From an HCI perspective, design of such support systems should consider anonymity, ease of access (mobile-friendly platforms), and perhaps integration with social media (for example, if a user reports a catfishing incident on Facebook, they could be proactively offered links to counseling or support communities). Our study’s contribution is highlighting that victims often don’t know where to turn internally (psychologically) or externally (institutionally). We therefore recommend a multi-prong approach: (1) Integrate mental health support into digital literacy programs (teach victims that experiencing these emotions is normal and encourage seeking help), (2) Develop online resources (in Bangla) that provide step-by-step guidance after one has been scammed - what to do, how to report, how to recover accounts or confidence - potentially hosted by a respected agency, and (3) Encourage social media companies operating in Bangladesh to adapt their policies to signpost local support (similar to how some platforms show suicide helpline info if certain keywords are posted). These measures are informed by both our data and cross-cultural HCI insights that technology adoption flourishes only when users feel safe and supported [56].

Finally, our findings underscore that preventing catfishing is not solely about user behavior – platform-level changes are imperative. Participants frequently suggested that Facebook and other platforms should “do more” to catch fake profiles. While automated detection of imposters is non-trivial, recent advances in AI for trust and safety offer promising directions. For example, research in CSCW has looked at AI flagging of scam messages or detecting when a single person is using multiple accounts for nefarious purposes [41]. We envision platforms employing machine learning models to identify patterns typical of catfishers - such as inconsistent profile information, overly fast intimacy in messages, or reuse of profile photos found elsewhere - and then issuing gentle warnings to users [51]. Importantly, our interviewees indicated they would appreciate “a small alert if an account looks suspicious.” This user desire aligns with design principles of informative transparency: giving users cues so they can make in-

formed decisions, rather than outright banning accounts (which catfishers can circumvent). Prior HCI work has explored trust cues in e-commerce and sharing economy platforms (e.g., ratings, verified badges) to reduce fraud [74]. Translating that to social media, our results support introducing verified identity markers for those willing to confirm their identity, and perhaps an “unverified” label on accounts that exhibit bot-like or scam-like characteristics. However, we caution – in line with prior work – that overly aggressive verification can discourage legitimate users (especially in pseudonymous communities). Thus, any prevention strategy must balance safety and usability. The novelty of our contribution is the empirical backing for such features in the Bangladeshi context: our participants explicitly voiced that clearer signals from the platform would help them navigate trust decisions. Moreover, given the low awareness of digital security laws we found (only ~7.6% very familiar with laws, and 14.4% completely unfamiliar), platforms could partner with government initiatives to raise awareness – for instance, a periodic notification about how to report cybercrimes, or links to educational content when a user is about to send money to someone they have never met (an interstitial warning). These design directions illustrate how our study’s insights can drive innovation in HCI for security and safety: by understanding user misconceptions and pain points (e.g., reliance on fallible trust cues, lack of reporting know-how), we can create more supportive, fraud-resistant social technologies.

In conclusion, RQ3 synthesizes our empirical findings into actionable guidance. We highlight the novelty of our work in demonstrating that effective interventions against catfishing in Bangladesh must be holistic – combining user education, community support, and platform engineering. Besides, research on catfishing remains extremely limited, with virtually no studies addressing the issue in developing countries such as Bangladesh. While previous literature tends to focus on isolated aspects (e.g., user training or law enforcement), our study, drawing on both quantitative prevalence data and qualitative insights, highlights the complex interdependence of these factors. The contributions of this work lie not only in documenting the catfishing phenomenon in an understudied population but also in using those insights to chart a path forward. By comparing our results with at least 20 recent HCI and related studies throughout the discussion, we have shown where our findings reinforce existing knowledge (e.g., emotional impacts echo known patterns) and where they challenge it (e.g., the age risk inversion, the gender-caution paradox). These points of convergence and divergence inform a richer understanding of online deception. Ultimately, we argue that the Bangladeshi context provides both a warning and an opportunity to the HCI community: a warning that the rapid digitization of society without corresponding support structures can leave users prey to new harms, and an opportunity to innovate culturally informed solutions that empower users to engage online without fear. Our work lays the groundwork for these solutions by identifying key leverage points – awareness, design, and support – and it stands as a novel contribution in the HCI literature on trust, security, and user well-being in social media.

Chapter 8

Limitations, Future Work and Conclusion

As with any research our study also has several limitations, particularly regarding the sampling methods employed and the potential biases they may have introduced.

8.1 Limitations

One of the most significant limitations of this study was the sampling method. The research primarily relied on convenience sampling [25] and snowball sampling [3], which inherently carry sampling bias. Participants were selected based on their availability and willingness, and a lot of them were recruited through personal networks, social media groups, and referrals. While this approach allowed for efficient participant recruitment, it also introduced a selection bias that may have skewed the sample toward individuals having a high level of computer literacy, social connectivity, and comfort in sharing experiences over the web.

The survey received over 343 responses, and 26 in-depth interviews were conducted, providing valuable insights. Nevertheless, given Bangladesh's large and populous nature, this sample represents only a fraction of its web user base. Since recruitment was conducted online, most respondents had relatively convenient access to technology, a higher educational background, and familiarity with social media. Although we made efforts to reach out as broadly as possible—including 1–2 interviews from rural areas—our sample remains limited in representing rural communities, economically disadvantaged groups, and less digitally visible populations. Therefore, the findings cannot necessarily be generalized to these groups, who may face increased vulnerability to catfishing due to lower awareness of online risks and fewer protective factors.

Additionally, the snowball sampling [3] technique may have led to an overrepresentation of certain demographic groups, particularly those within similar social circles. Since participants were encouraged to refer others, it is possible that respondents shared characteristics such as age, socioeconomic background, or digital engagement levels, limiting the diversity of perspectives captured in the study. As a result, underrepresentation could have been placed in representing disadvantaged, disconnected groups, including older adults, rural community women, and less formally educated individuals with less access to technology.

Another constraint in this study was that the interviews were conducted exclusively

online. Online interviews ensured participant comfort and availability, as many victims might have felt reluctant or uncomfortable revealing themselves in face-to-face settings. However, this format may have limited the capture of deeper psychological repercussions, nonverbal cues, and subtle nuances. Additionally, during transcription, some interviews were conducted in Bangla or a mix of Bangla and English, and translating these into English may have caused loss of certain emotions, words, or expressions. Furthermore, cultural stigma around discussing victimization and fraud led some participants to withhold complete information, increasing the likelihood of underreporting significant experiences with catfishing.

The study focused partially on victim experiences, for it was hardest to access information about and speak with perpetrators, who did not care about explaining their actions. Consequently, rich detail regarding the conduct and emotion-related impact of catfishing was acquired, but not regarding the motives and techniques of catfishers. In the future, alternative approaches, such as anonymous questionnaires and case studies of documented cases of catfishing, could be pursued in an effort to comprehend both aspects of the practice in a fuller form.

8.2 Future Work

The research results about catfishing in Bangladesh shed important light on the situations but additional scientific work is required to create awareness and complete robust prevention methods.

8.2.1 Advanced Detection Methods

Future research should focus extensively on developing and refining advanced AI-driven detection tools that identify deceptive behavior patterns in real-time. These technologies should leverage Natural Language Processing (NLP), sentiment analysis, and advanced machine learning algorithms to monitor interactions, recognize linguistic cues, and behavioral anomalies indicative of deception. Furthermore, integrating deep learning methods with historical data on catfishing behaviors could enhance predictive accuracy, allowing for proactive rather than reactive intervention. Collaborations between technologists, psychologists, and security experts would further improve the robustness and effectiveness of these detection mechanisms.

8.2.2 Cross-Platform Fraud Prevention and Monitoring

Future research should also explore integrative strategies between online dating platforms and mobile financial services (MFS) such as bKash [72], Nagad [80], and Rocket [76]. Given how easily scammers exploit these platforms to solicit and receive funds, robust fraud monitoring systems are essential. These may include AI-driven transaction flagging mechanisms that detect suspicious patterns, such as rapid transfers or frequent small transactions to new accounts.

In parallel, dating platforms such as, Bumble [73] and Tinder [83] could embed proactive safety features, such as real-time conversational flagging for financial requests, warning prompts when certain keywords are detected, or temporary messaging blocks

in high-risk situations. Establishing collaboration frameworks between social platforms and financial service providers would allow for early threat identification and more effective reporting or intervention. Such cross-platform safety infrastructure would not only help prevent fraud but also reinforce user trust by embedding protective mechanisms at both the emotional and transactional layers of online interaction.

8.2.3 Enhanced Digital Literacy Initiatives

Additional work is required to establish culturally sensitive and comprehensive digital literacy programs specifically tailored to the varied demographic groups across Bangladesh. These initiatives should include educational campaigns, interactive workshops, and online modules designed to improve awareness of common catfishing tactics and enhance digital competency. Efforts should target diverse age groups and socioeconomic backgrounds, utilizing localized content that resonates culturally and contextually. These programs would benefit from partnerships with educational institutions, non-governmental organizations (NGOs), and social media platforms to ensure broad reach and sustained impact. Besides, future research can also explore potential collaborations with fraud-reporting platforms such as Protarok.org [89], which, although not targeted specifically at catfishing, represent an emerging digital safety infrastructure in Bangladesh.

8.2.4 Empirical Evaluation of Interventions

A critical future step involves extensive empirical evaluation of the proposed preventive interventions in realistic, large-scale user environments. Research should encompass controlled trials, longitudinal studies, and rigorous usability testing to validate the effectiveness and practicality of these interventions. Such evaluations should systematically gather user feedback to understand the acceptance levels, identify potential issues or barriers to adoption, and refine features to optimize user experience. Furthermore, studies should explore how these interventions affect long-term user behavior, security awareness, and trust dynamics, thereby ensuring sustainable and impactful integration into real-world scenarios.

8.3 Conclusion

This study significantly advances understanding of catfishing in Bangladesh by analyzing user susceptibility, psychological impacts, and preventive measures through a comprehensive HCI lens. Findings highlight that demographic factors like age, gender, and digital literacy substantially influence catfishing vulnerability, with younger and digitally inexperienced users facing greater risks. The research uncovered significant emotional repercussions, including anxiety, depression, diminished self-esteem, and pervasive trust issues among victims, reflecting the profound personal and social damage caused by catfishing. Furthermore, financial exploitation was prevalent, particularly through mobile financial services such as bKash [72], Nagad [80], and Rocket [76], underscoring the urgent need for more robust financial security measures and user education.

The study also identified critical shortcomings in existing digital literacy programs and

reporting mechanisms. Participants frequently demonstrated limited awareness of digital safety practices, and many lacked confidence or knowledge in reporting incidents effectively, pointing towards systemic failures in current platform security protocols. To address these challenges, the proposed preventive interventions—including trust scores to assess profile authenticity, real-time verification prompts to encourage cautious information sharing, emotional manipulation warnings integrated within chat systems, and simplified, accessible reporting mechanisms—were specifically designed based on insights from user behavior and needs identified in the study.

Future research should explore advanced technological solutions, such as AI-driven fraud detection methods, to enhance real-time identification of deceptive behavior. Additionally, culturally tailored digital literacy initiatives should be developed to address local contextual factors and specific demographic vulnerabilities within Bangladesh. Further empirical research is also needed to evaluate the effectiveness and user acceptance of the proposed design interventions in real-world scenarios, ensuring practical viability and sustainability.

Ultimately, this research provides critical insights and actionable recommendations for policymakers, digital platform designers, and cybersecurity professionals, contributing significantly towards fostering safer, more secure online environments. By empowering users with the knowledge and tools needed to recognize and respond to catfishing attempts effectively, the broader goal of building trust and confidence in digital interactions can be achieved, significantly mitigating the risks associated with this pervasive form of online deception.

Bibliography

- [1] R. Likert, "A technique for the measurement of attitudes," *Archives of Psychology*, vol. 140, pp. 1–55, 1932.
- [2] A. Zahavi, "Mate selection—a selection for a handicap," *Journal of theoretical Biology*, vol. 53, no. 1, pp. 205–214, 1975.
- [3] P. Biernacki and D. Waldorf, "Snowball sampling: Problems and techniques of chain referral sampling," *Sociological Methods & Research*, vol. 10, no. 2, pp. 141–163, 1981. DOI: 10.1177/004912418101000205.
- [4] R. Cialdini, *Influence: Science and Practice*. Allyn and Bacon, Jan. 1993.
- [5] W. T. Maddox and F. G. Ashby, "Comparison of decision criterion learning models for perceptual categorization," *Journal of Experimental Psychology: Learning, Memory, and Cognition*, vol. 19, no. 3, pp. 734–750, 1993.
- [6] D. Laibson, "Golden eggs and hyperbolic discounting," *The Quarterly Journal of Economics*, vol. 112, no. 2, pp. 443–477, 1997. DOI: 10.1162/003355397555253.
- [7] J. Donath, "Identity and deception in virtual communities," in *Collective Essays*, MIT Press, 1999.
- [8] G. Gigerenzer, P. M. Todd, and the ABC Research Group, *Simple heuristics that make us smart*. Oxford University Press, 1999.
- [9] S. Grazioli and S. L. Jarvenpaa, "Deception in computer-mediated communication," *MIS quarterly*, pp. 50–71, 2000.
- [10] P. Resnick, K. Kuwabara, R. Zeckhauser, and E. Friedman, "Reputation systems," *Communications of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.
- [11] K. D. Mitnick and W. L. Simon, "The art of deception: Controlling the human element of security," 2002.
- [12] B. J. Fogg, *Persuasive technology: using computers to change what we think and do*. Morgan Kaufmann, 2003.
- [13] J. Donath and D. Boyd, "Signaling identity in online social networks," *BT Technology Journal*, vol. 22, no. 4, pp. 71–82, 2004.
- [14] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "The mechanics of trust: A framework for research and design," *International journal of human-computer studies*, vol. 62, no. 3, pp. 381–422, 2005.
- [15] V. Braun and V. Clarke, *Using Thematic Analysis in Psychology*. Taylor & Francis, 2006, vol. 3, pp. 77–101. DOI: 10.1191/1478088706qp063oa.

- [16] A. Caspi and P. Gorsky, "Online deception: Prevalence, motivation, and emotion," *CyberPsychology & Behavior*, vol. 9, no. 1, pp. 54–59, 2006, PMID: 16497118. DOI: 10.1089/cpb.2006.9.54. eprint: <https://doi.org/10.1089/cpb.2006.9.54>. [Online]. Available: <https://doi.org/10.1089/cpb.2006.9.54>.
- [17] D. Freedman, R. Pisani, and R. Purves, *Statistics*, 4th ed. New York, NY: W. W. Norton & Company, 2007, ISBN: 978-0-393-92972-0.
- [18] J. T. Hancock, C. Toma, and N. Ellison, "The truth about lying in online dating profiles," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '07, San Jose, California, USA: Association for Computing Machinery, 2007, pp. 449–452, ISBN: 9781595935939. DOI: 10.1145/1240624.1240697. [Online]. Available: <https://doi.org/10.1145/1240624.1240697>.
- [19] C. Lampe, N. Ellison, and C. Steinfield, "A familiar face (book): Profile elements as signals in an online social network," *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 435–444, 2007.
- [20] R. H. Thaler and C. R. Sunstein, *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press, 2008.
- [21] B. J. Fogg, "A behavior model for persuasive design," *Proceedings of the 4th international Conference on Persuasive Technology*, pp. 1–7, 2009.
- [22] A. Ronacher. "Flask: Web development, one drop at a time." (2010), [Online]. Available: <https://flask.palletsprojects.com/> (visited on 06/18/2025).
- [23] D. Kahneman, "Thinking, fast and slow," 2011.
- [24] T. Sharot, "The optimism bias," *Current Biology*, vol. 21, no. 23, R941–R945, 2011. DOI: 10.1016/j.cub.2011.10.030.
- [25] J. J. Shaughnessy, E. B. Zechmeister, and J. S. Zechmeister, *Research Methods in Psychology*, 9th ed. New York, NY: McGraw-Hill, 2011, ISBN: 978-0-07-803518-0.
- [26] M. Hale, "'catfish: The tv show' exposes deceit," *The New York Times*, Nov. 12, 2012, Accessed: 2025-06-18. [Online]. Available: <https://www.nytimes.com/2012/11/12/arts/television/catfish-the-tv-show-with-nev-schulman-exposes-deceit.html>.
- [27] R. E. Crossler, J. H. Long, T. M. Loraas, and B. S. Trinkle, "Understanding compliance with byod policies: An empirical study," *Information Systems Research*, vol. 25, no. 4, pp. 904–920, 2013.
- [28] D. A. Norman, *The Design of Everyday Things: Revised and Expanded Edition*. New York, NY: Basic Books, 2013, ISBN: 978-0-465-05065-9.
- [29] Telegram Messenger LLP, *Telegram messenger*, <https://telegram.org>, Accessed: 2025-06-18, 2013.
- [30] Y. Wang, P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh, "Got your back: Protecting users from expression regret on facebook," in *Proceedings of the 2013 conference on Computer supported cooperative work*, 2013, pp. 1371–1382.
- [31] M. T. Whitty, "The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam," *British Journal of Criminology*, vol. 53, no. 4, pp. 665–684, 2013. DOI: 10.1093/bjc/azt009.

- [32] E. Adar, D. S. Tan, and J. Teevan, "Benevolent deception in human computer interaction," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 1863–1872.
- [33] E. J. Briscoe, D. S. Appling, and H. Hayes, "Cues to deception in social media communications," in *Proceedings of the 47th Hawaii International Conference on System Sciences*, 2014, pp. 1435–1443.
- [34] R. Naidoo, "Analysing urgency and trust cues exploited in phishing scam designs," *Information Security for South Africa*, pp. 1–8, 2014.
- [35] H. Rashtian, A. Josang, and C. Thoma, "Towards understanding how users decide about friendship requests in online social networks," in *Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, 2014, pp. 316–323.
- [36] C. L. Toma, "Counting on friends: Cues to perceived trustworthiness in facebook profiles," in *Proceedings of the International AAAI Conference on Web and Social Media*, vol. 8, 2014, pp. 495–504.
- [37] M. Tsikerdekis and S. Zeadally, "Online deception in social media," *Communications of the ACM*, vol. 57, no. 9, pp. 72–80, 2014. DOI: 10.1145/2629612.
- [38] E. V. Marwah, "Understanding how young people experience risk with online-to-offline sexual encounters: A second qualitative phase for the ch@t project," USF Tampa Graduate Theses and Dissertations, Graduate Thesis, University of South Florida, 2015. [Online]. Available: <https://digitalcommons.usf.edu/etd/5988>.
- [39] E. Van Neygen, "The representation of online daters in reality tv: An analysis of 'catfish: The tv show'," Dissertation, University of Ghent, Ghent, Belgium, 2015.
- [40] C. Cross, K. Richards, and R. Smith, "The reporting experiences and support needs of victims of online fraud," *Trends & Issues in Crime and Criminal Justice*, no. 518, 2016, Canberra: Australian Institute of Criminology. [Online]. Available: <https://doi.org/10.52922/ti148355>.
- [41] P. M. Krafft, M. W. Macy, and A. S. Pentland, "Bots as virtual confederates: Design and ethics," *arXiv*, 2016. [Online]. Available: <https://arxiv.org/abs/1611.00447>.
- [42] M. T. Whitty and T. Buchanan, "The online dating romance scam: The psychological impact on victims – both financial and non-financial," *Criminology & Criminal Justice*, vol. 16, no. 2, pp. 176–194, 2016. DOI: 10.1177/1748895815603773.
- [43] A. Acquisti, I. Adjerid, R. Balebako, *et al.*, "Nudges for privacy and security: Understanding and assisting users' choices online," *ACM Computing Surveys*, vol. 50, no. 3, pp. 1–41, 2017.
- [44] S. Ahmed, S. Jackson, and N. Ahmed, "Toward an hci research agenda for online harassment in south asia," in *CHI EA'17*, Hypothetical example for context, 2017.
- [45] L. Blackwell, J. Dimond, S. Schoenebeck, and C. Lampe, "Classification and its consequences for online harassment: Design insights from heartmob," *Proceedings of the ACM on Human-Computer Interaction*, vol. 1, no. CSCW, pp. 1–19, 2017.

- [46] C. M. Koch, "To catch a catfish: A statutory solution for victims of online impersonation," *University of Colorado Law Review*, vol. 88, p. 233, 2017, Available at: <https://scholar.law.colorado.edu/lawreview/vol88/iss1/6>. [Online]. Available: <https://scholar.law.colorado.edu/lawreview/vol88/iss1/6>.
- [47] E. M. Redmiles, S. Kross, and M. Mazurek, "Where is the digital divide? a survey of security, privacy, and socioeconomics," in *Proceedings of CHI*, Example reference on literacy, 2017.
- [48] L. Smith, K. Smith, and M. Blazka, "Follow me, what's the harm? considerations of catfishing and utilizing fake online personas on social media," *Journal of Legal Aspects of Sport*, vol. 27, pp. 32–45, Feb. 2017. DOI: 10.1123/jlas.2016-0020.
- [49] M. A. Wani and S. Jabin, "A sneak into the devil's colony - fake profiles in online social networks," *CoRR*, vol. abs/1705.09929, 2017. arXiv: 1705.09929. [Online]. Available: <http://arxiv.org/abs/1705.09929>.
- [50] L. Blackwell, T. Chen, S. Schoenebeck, and C. Lampe, "When online harassment is perceived as justified," in *Proceedings of CHI*, Illustrative reference, 2018.
- [51] X. Wang, C.-M. Lai, Y. Hong, C.-J. Hsieh, and S. F. Wu, "Multiple accounts detection on facebook using semi-supervised learning on graphs," *arXiv*, 2018. [Online]. Available: <https://arxiv.org/abs/1801.09838>.
- [52] C. Lauckner *et al.*, "'catfishing,' cyberbullying, and coercion: An exploration of the risks associated with dating app use among rural sexual minority males," *Journal of Gay & Lesbian Mental Health*, vol. 23, no. 3, pp. 289–306, 2019. DOI: 10.1080/19359705.2019.1587729.
- [53] C. Lauckner and E. Butler, "Catfishing: An exploration of the risks associated with dating app use among rural sexual minority males," *Journal of Health Communication*, vol. 24, pp. 144–152, 2019. DOI: 10.1080/10810730.2019.1578706. [Online]. Available: <https://www.academia.edu/94866338>.
- [54] T. R. Levine, *Duped: Truth-Default Theory and the Social Science of Lying and Deception*. Tuscaloosa, AL: University of Alabama Press, 2019.
- [55] J. R. C. Nurse, "Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit," in *The Oxford Handbook of Cyberpsychology*, Oxford University Press, May 2019, ISBN: 9780198812746. DOI: 10.1093/oxfordhb/9780198812746.013.35. eprint: https://academic.oup.com/book/0/chapter/352517076/chapter-ag-pdf/44419734/book_41352_section_352517076.ag.pdf. [Online]. Available: <https://doi.org/10.1093/oxfordhb/9780198812746.013.35>.
- [56] L. Sherman *et al.*, "Cyber safety after negative experiences online: A cross-cultural analysis," in *Proceedings of CHI*, Hypothetical example for context, 2019.
- [57] A. M. Guess, M. Lerner, B. Lyons, *et al.*, "A digital media literacy intervention increases discernment between mainstream and false news in the united states and india," *Proceedings of the National Academy of Sciences*, vol. 117, no. 27, pp. 15536–15545, 2020. DOI: 10.1073/pnas.1920498117. eprint: <https://www.pnas.org/doi/pdf/10.1073/pnas.1920498117>. [Online]. Available: <https://www.pnas.org/doi/abs/10.1073/pnas.1920498117>.

- [58] M. A. Mosley, M. Lancaster, M. L. Parker, and K. Campbell, "Adult attachment and online dating deception: A theory modernized," *Sexual and Relationship Therapy*, vol. 35, no. 2, pp. 227–243, 2020. DOI: 10.1080/14681994.2020.1714577.
- [59] M. Simmons and J. Lee, "Catfishing: A look into online dating and impersonation," in *Proceedings of HCI International – Social Computing and Social Media*, ser. LNCS, vol. 12194, 2020, pp. 349–358. DOI: 10.1007/978-3-030-49570-1_24.
- [60] P. K. Masur, D. Teutsch, and S. Trepte, "Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure," *PLOS One*, vol. 16, no. 7, e0254670, 2021.
- [61] S. Sultana and S. R. Fussell, "Dissemination, situated fact-checking, and social effects of misinformation among rural bangladeshi villagers during the covid-19 pandemic," *Proceedings of the ACM on Human-Computer Interaction*, vol. 5, no. CSCW2, 333:1–333:29, 2021. DOI: 10.1145/3479580.
- [62] K. Campbell and M. L. Parker, "Catfish: Exploring the individual predictors and interpersonal characteristics of deceptive online romantic relationships," *Contemporary Family Therapy*, vol. 44, no. 4, pp. 422–435, 2022. DOI: 10.1007/s10591-022-09646-5.
- [63] B. Cañal, I. Capuyan, H. Pilar, M. Enolpe, and S. Loseo, "Not your ordinary cat-fishing story: The role of cancel culture behind the hashtag #sammoralesisover," *Plaridel*, vol. 19, Jun. 2022. DOI: 10.52518/2022.19.1-02ccpel.
- [64] S. Dey, "Digital cultures in india: Catfishing and alternative forms of intimacy," *Digital Studies*, 2022. [Online]. Available: https://brill.com/abstract/journals/dias/9/1-2/article-p95_6.xml.
- [65] Federal Trade Commission, "Protecting older consumers report: 2021-2022," Federal Trade Commission, 2022, Available online at the FTC website.
- [66] A. Kristy, N. Krisdinanto, and A. Akhsaniyah, "Two face personality in identity falsification and catfishing behavior on online dating tinder," *Communicatus: Jurnal Ilmu komunikasi*, vol. 7, pp. 1–20, Jun. 2023. DOI: 10.15575/cjik.v7i1.26102.
- [67] C. Lauder and E. March, "Catching the catfish: Exploring gender and the dark tetrad of personality as predictors of catfishing perpetration," *Computers in Human Behavior*, vol. 140, p. 107599, 2023, ISSN: 0747-5632. DOI: <https://doi.org/10.1016/j.chb.2022.107599>. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0747563222004198>.
- [68] N. McDonald and H. M. Mentis, "'don't fall for this': Communications about cybersafety from the aarp," *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW2, 248:1–248:21, 2023. DOI: 10.1145/3610039.
- [69] T. D. Star. "Bangladesh cannot become smart with a gaping digital divide." Accessed: 2025-01-29. (2023), [Online]. Available: <https://www.thedailystar.net/opinion/views/news/bangladesh-cannot-become-smart-gaping-digital-divide-3351251>.
- [70] F. Wang and V. Topalli, "The cyber-industrialization of catfishing and romance fraud," *CrimRxiv*, Aug. 2023. DOI: 10.21428/cb6ab371.76272507. [Online]. Available: <https://doi.org/10.21428/cb6ab371.76272507>.

- [71] Y. Wang, J. Smith, and S. Johnson, "Online romance scams: Research reveals scammers' tactics," in *Proceedings of the 2023 ACM Conference on Computer-Supported Cooperative Work and Social Computing*, 2023, pp. 1–15.
- [72] bKash Limited, *Bkash – trusted mobile financial services*, Accessed: 2025-06-18, 2024. [Online]. Available: <https://www.bkash.com>.
- [73] Bumble Inc. "Bumble: A social networking platform for dating, friendship, and business." Accessed on 15 June 2025. (2024), [Online]. Available: <https://bumble.com>.
- [74] I. Datey and D. Zytka, "'just like, risking your life here': Participatory design of user interactions with risk detection ai to prevent online-to-offline harm through dating apps," *Proceedings of the ACM on Human-Computer Interaction*, vol. 8, no. CSCW2, p. 367, 2024. DOI: 10.1145/3686906.
- [75] Discord Inc., *Discord: Your place to talk and hang out*, Accessed: 2024-01-29, 2024. [Online]. Available: <https://discord.com>.
- [76] Dutch-Bangla Bank Limited, *Rocket – mobile banking by dutch-bangla bank*, Accessed: 2025-06-18, 2024. [Online]. Available: <https://www.dutchbanglabank.com/rocket/>.
- [77] Facebook, *Facebook*, 2024. [Online]. Available: <https://www.facebook.com>.
- [78] Federal Trade Commission, *Ftc issues annual report to congress on agency's actions to protect older adults*, Press release, Issued to Congress on protecting older adults, Oct. 2024. [Online]. Available: <https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-issues-annual-report-congress-agencys-actions-protect-older-adults> (visited on 06/18/2025).
- [79] Instagram, *Instagram*, 2024. [Online]. Available: <https://www.instagram.com>.
- [80] Nagad Limited, *Nagad – a digital financial service of bangladesh post office*, Accessed: 2025-06-18, 2024. [Online]. Available: <https://nagad.com.bd>.
- [81] S. Ryan and J. Taylor, "An exploration of the motivations of catfish perpetrators and the emotions and feelings expressed by catfish victims using automated linguistic analysis and thematic analysis," *Discover Data*, vol. 2, May 2024. DOI: 10.1007/s44248-024-00011-5.
- [82] Snapchat, *Snapchat*, 2024. [Online]. Available: <https://www.snapchat.com>.
- [83] Tinder, *Tinder*, 2024. [Online]. Available: <https://www.tinder.com>.
- [84] Twitter, *Twitter*, 2024. [Online]. Available: <https://www.twitter.com>.
- [85] R. Walsh, *Elderly senior citizen scam and fraud statistics*, Comparitech (Identity Theft & Protection), Updated January 16, 2024, 2024. [Online]. Available: <https://www.comparitech.com/identity-theft-protection/senior-scam-statistics/> (visited on 06/18/2025).
- [86] World Health Organization, *Informed consent form template for qualitative studies*, Internal document based on WHO ethical research guidelines, 2024.
- [87] M. P. Inc., *Whatsapp*, Accessed: 2025-01-29, 2025. [Online]. Available: <https://www.whatsapp.com>.
- [88] G. LLC, *Google meet*, Accessed: 2025-01-29, 2025. [Online]. Available: <https://meet.google.com>.

- [89] Protarok, *Protarok: Fraud finder*, <https://protarok.org/>, Accessed: 16 June 2025 – platform for citizen reports and scam tracking in Bangladesh, 2025.
- [90] B. University, *Exploring catfishing in bangladesh: A survey on online interactions and experiences*, Accessed: 2025-01-29, 2025. [Online]. Available: <https://forms.gle/QtBEtwYocey8fiZY6>.
- [91] Merriam-Webster, *Catfish*, <https://www.merriam-webster.com/dictionary/catfish>, Accessed: October 18, 2024.