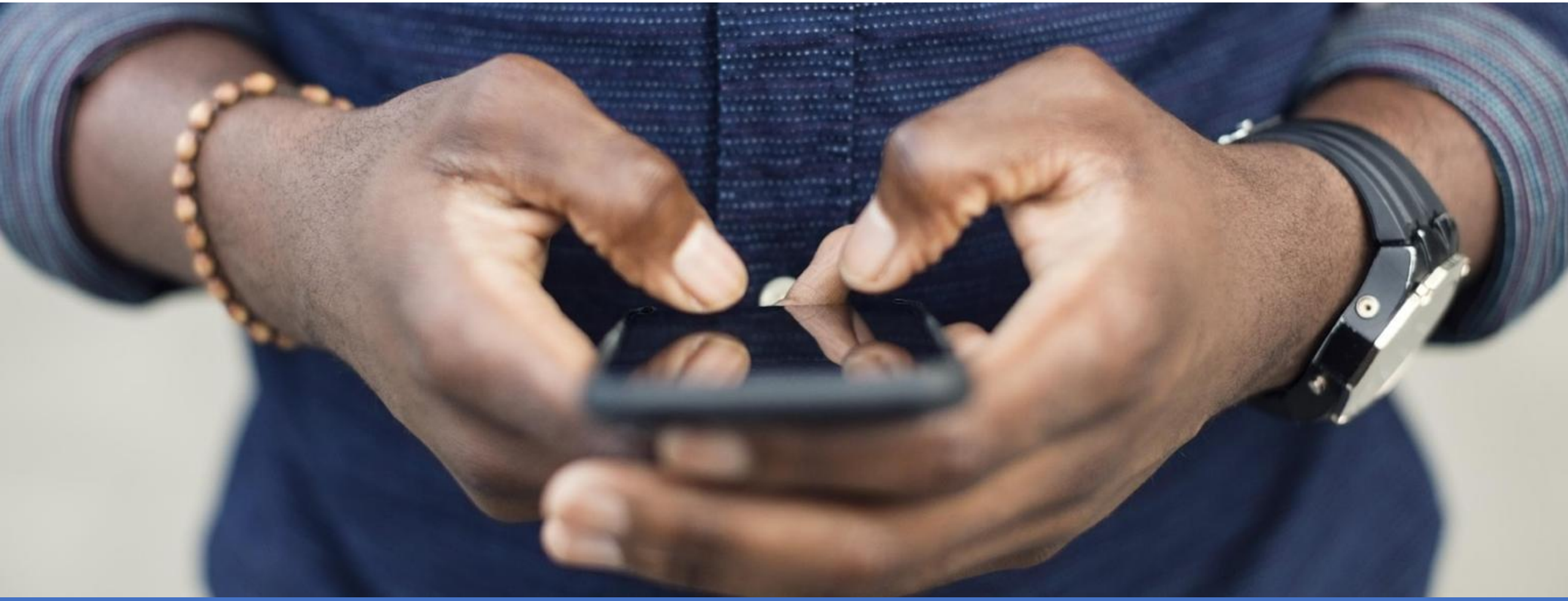


Not Everyone Can Be Friends : An Analysis of the Evolving Process of Cyber Romance Scam and Defensive Strategies

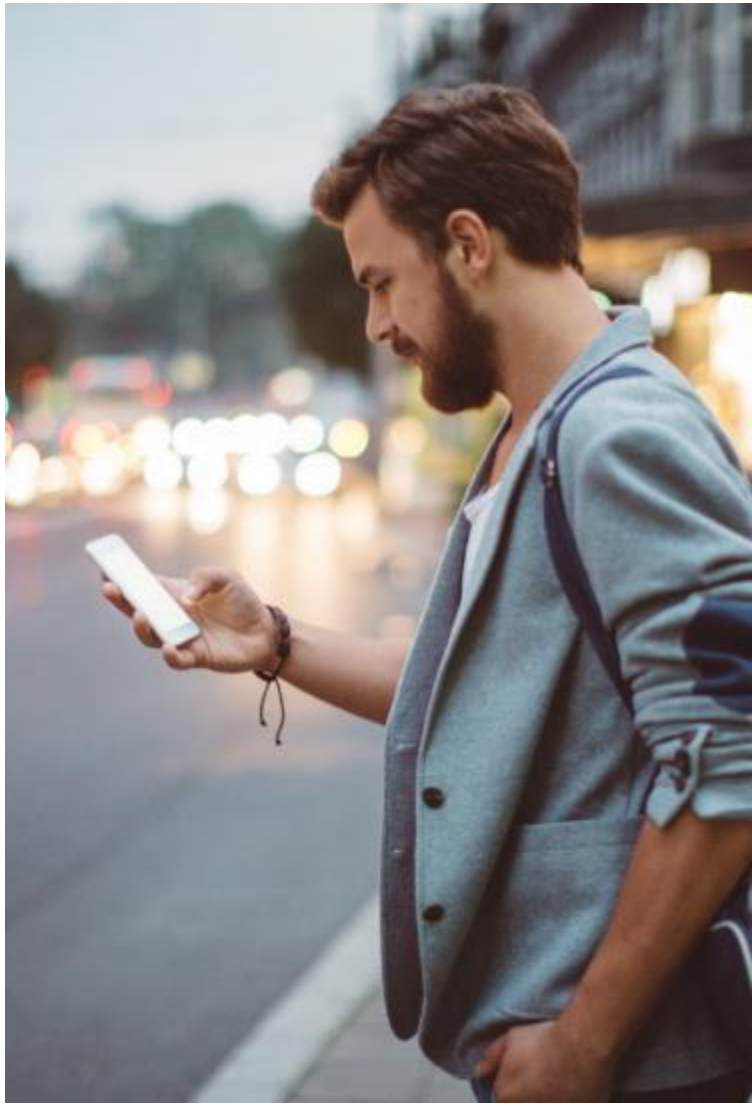
아주대학교 AJOU UNIVERSITY

Department of Global Convergence Management

Young-Jin(Richard) Park

Contents

- ✓ **Introduction**
  - *Background*
  - *Gap & Purpose*
  - *Question*
- ✓ **Research Method**
  - *Digital Ethnographic Analysis*
- ✓ **Research Results**
- ✓ **Practical and Theoretical Contributions**
- ✓ **Research Limitations**
- ✓ **Conclusion**



Introduction

1

Research Background

- **1. Advancements in Technology and Online Scams:**
  - The development of technology and the internet has facilitated the spread of various online scams, and romance scams are no exception (Whitty, 2013).
  - The emergence and rapid advancement of computing systems, coupled with the proliferation and increased efficiency of internet-based platforms, have led to a dramatic rise in online scams over the past decade. This growth is largely attributed to the exponential progress in computer technology and the usability of social media platforms (Wang and Topalli, 2024).
- **2. Dating Apps and the Rise of Romance Scams:**
  - According to the 2024 App Business Report, the global number of dating app users reached approximately 350 million in 2023, marking an increase of 12 million from the previous year. This growth has coincided with a rise in romance scam victims (Curry, D., 2024).



https://www.straitstimes.com/stop-scams

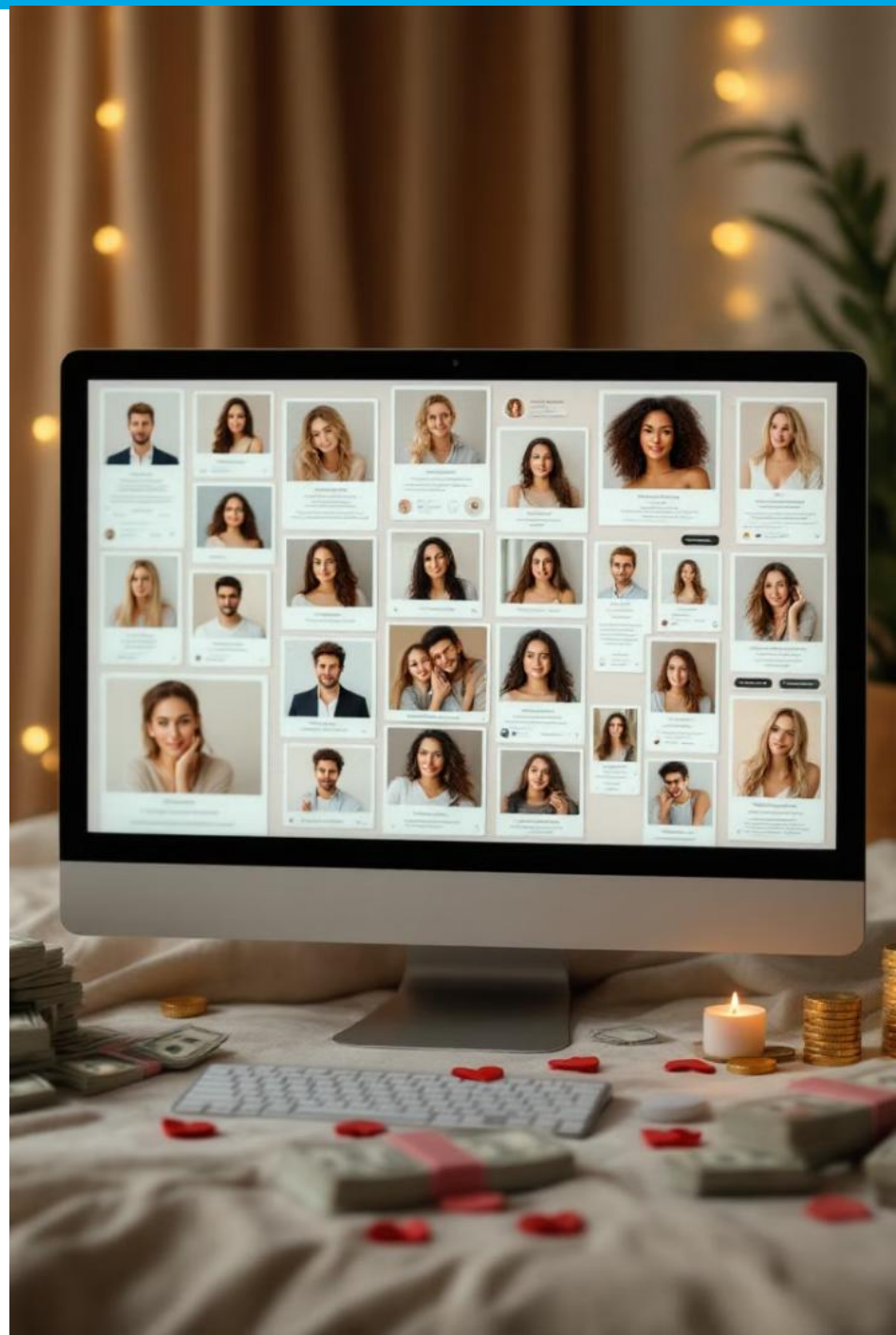
Research Background

- **3. Building Trust Through Messenger Apps:**
  - Scammers use messenger apps like LINE to establish trust, employing sophisticated techniques that blur the lines between friendship and deception. Romance scams are defined as situations where individuals are deceived for financial gain by someone perceived to be in a romantic relationship with them (Buil-Gil and Zeng, 2022).
- **4. International Impersonation and Psychological Manipulation:**
  - Rather than operating scams within a single country, scammers use international impersonation and deception to skillfully manipulate their victims' psychology, leading to financial demands or the theft of personal information (Anesa, 2020).
- **5. The Impact of Romance Scams:**
  - Unlike victims of mass marketing scams, victims of romance scams experience a "double blow." They suffer financial losses as well as severe psychological damage due to the loss of significant interpersonal relationships (Whitty and Buchanan, 2016).



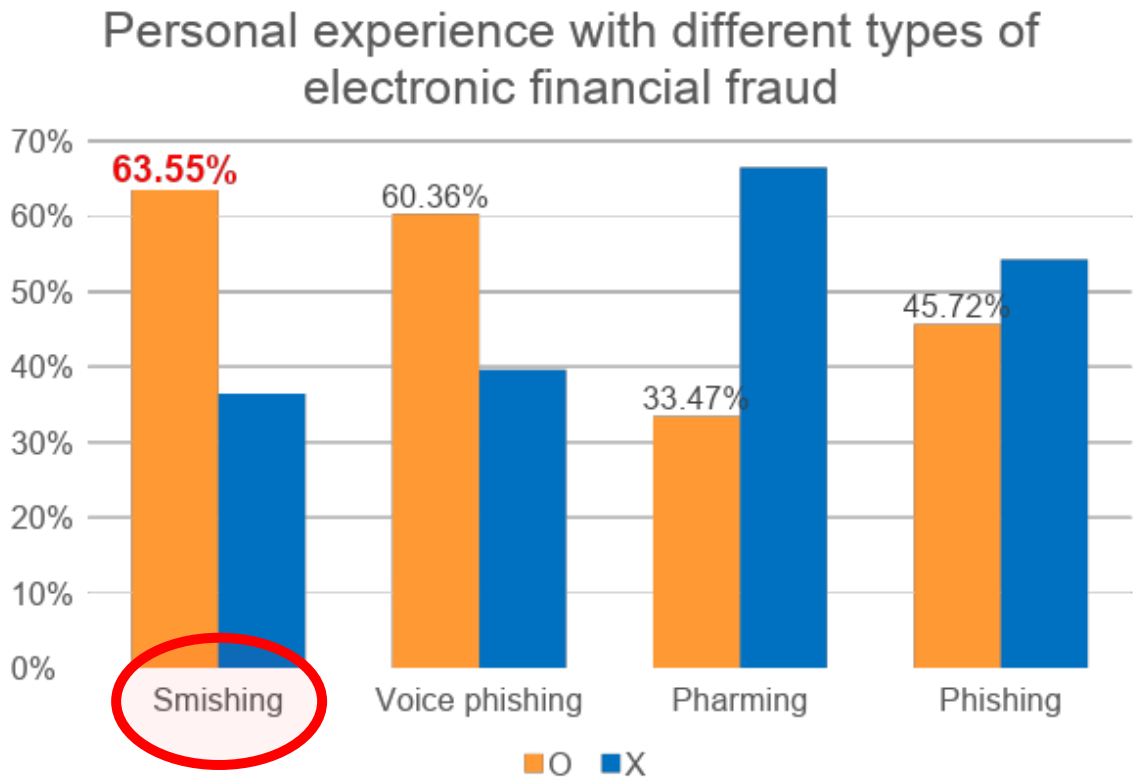
Research Background

- **6. General Approach of Romance Scammers**
  - Romance scammers often pose as potential partners on websites, social media platforms, or online forums, creating attractive personas with appealing profiles and photos to gain the trust and affection of their targets. Once a connection is established, scammers gradually build an emotional bond with the victim, often through regular messages, phone calls, or video chats. They may express love, affection, sexual attraction, and aspirations for a future together. However, their ultimate goal is to systematically exploit the victim financially or obtain personal information for illegal purposes. To achieve these objectives, romance scammers craft elaborate stories designed to elicit empathy and manipulate their victims (Whitty and Buchanan, 2016).



Research Background

- Korea Social Science Data Archive (KOSSDA), Public Awareness Survey on Electronic Financial Fraud, 2022 (1,004 respondents)
- Electronic financial fraud has been increasing overtime through direct phone calls, emails, and text messages.



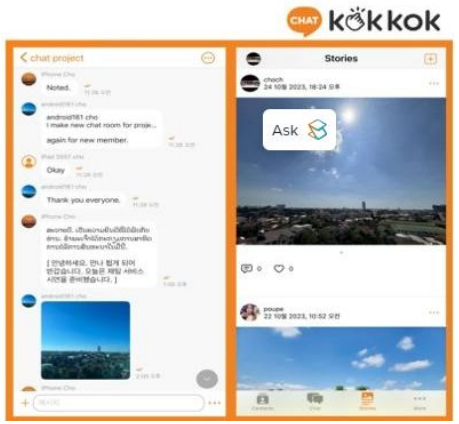
Research Background

- Messaging Apps

Data: Reach (monthly active users) of messaging apps in each given country, among iPhone users in June 2013.
* Pinger doubles when factoring in all iOS devices (iPhone, iPod Touch, iPad)

Onavo Insights, the largest mobile intelligence service, delivers actionable metrics and never-before-seen competitive insights, based on the world's largest mobile panel to drive decision-making and media buying in the world's leading mobile companies. For more Information visit insights.onavo.com





GLOBAL REACH OF MESSAGING APPS

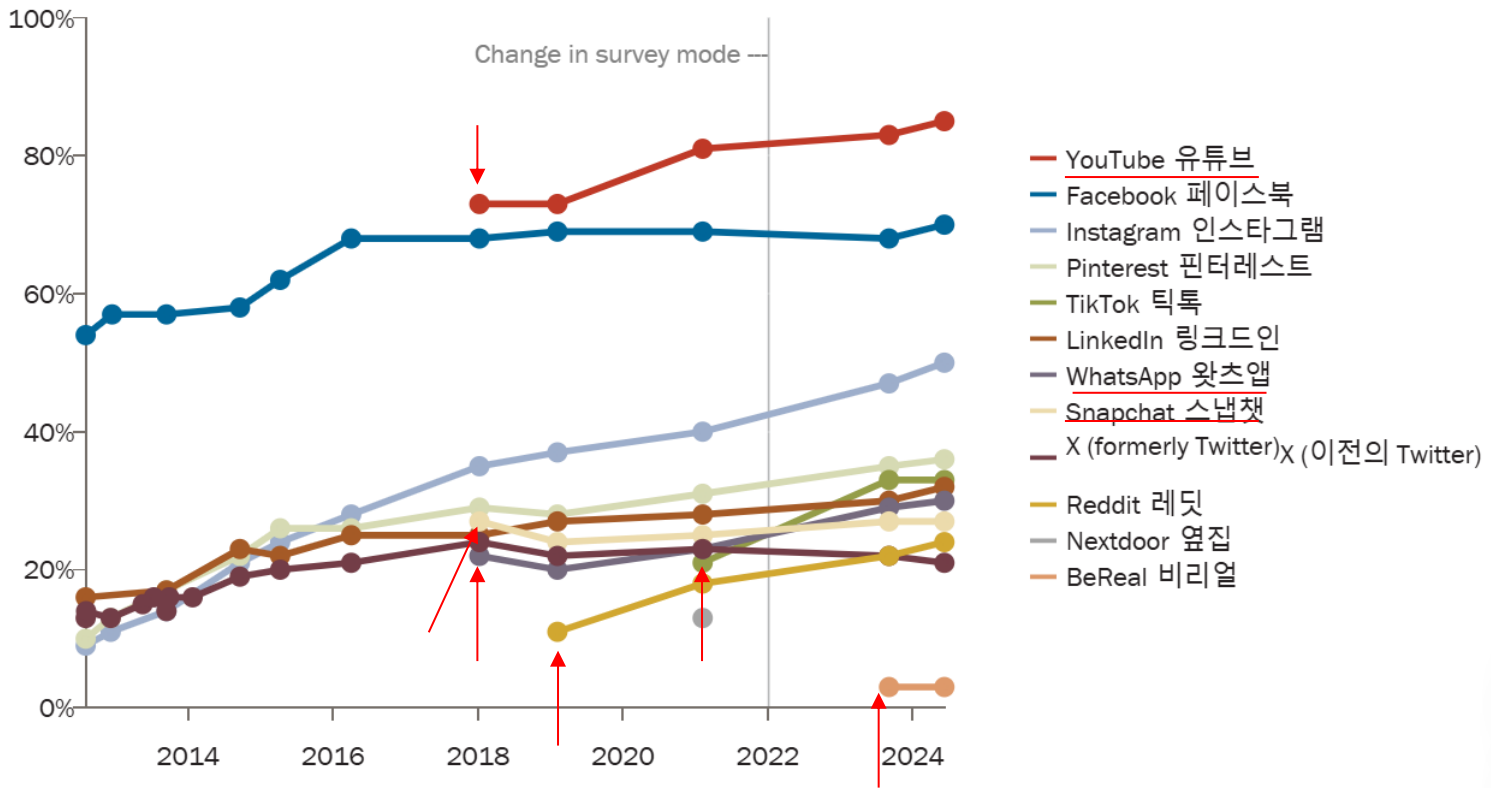
		FB Msngr	KakaoTalk	LINE	Pinger	WeChat	WhatsApp
Anglo		12%	1%	1%	8%*	1%	9%
		17%	1%	2%	-	2%	18%
		15%	-	1%	-	1%	49%
		19%	1%	4%	-	5%	22%
Latin America		29%	-	-	-	-	96%
		32%	-	4%	-	-	90%
		27%	-	26%	-	-	96%
		31%	-	14%	-	-	94%
Europe		29%	-	1%	-	-	91%
		13%	-	44%	-	-	99%
		19%	-	1%	-	-	17%
		33%	-	3%	-	-	93%
E. Asia		-	2%	11%	-	82%	15%
		21%	3%	46%	-	53%	96%
		18%	9%	71%	-	6%	8%
		6%	95%	12%	-	-	3%

Research Background

Social Media Usage

- Source: Surveys of U.S. adults conducted 2012-2024.
- PEW RESEARCH CENTER

- **Note:** Vertical lines indicate mode changes. Public opinion surveys conducted from 2012 to 2021 were conducted via telephone. The 2023 survey was conducted via web and mail, while the 2024 survey was conducted using web, mail, and telephone.



- Data prior to 2018 is unavailable for YouTube, Snapchat, or WhatsApp. Data for Reddit is unavailable before 2019, TikTok before 2021, and BeReal before 2023.
- Source: Surveys of U.S. adults conducted from 2012 to 2024.
- Source: Surveys of U.S. adults conducted 2012-2024. PEW RESEARCH CENTER

Research Gap & Purpose

- Previous studies on romance scams have primarily focused on analyzing the mechanisms of these scams through interviews and questionnaires with victims. While these studies provide valuable insights as qualitative research, there has been a lack of research that uses digital ethnographic methodologies to directly interact with potential scammers, enabling a more detailed exploration of their processes and mechanisms in real-time.

- Preventing scams entirely is becoming increasingly difficult as fraud prevention systems are growing more sophisticated, but no system can fully block all fraudulent pathways. This study aims to delve into the process of romance scams by engaging in actual conversations with scammers via messaging and online messenger apps. This includes following requests, direct message interactions, and friend registration on chatting apps. By analyzing the manipulative intent behind these interactions, the study seeks to identify differences between the observed scam processes and those described in previous research.

Research Questions

- **What psychological tricks and language patterns do scammers use in romance scams, and how can understanding these help us identify and stop them?**
- **What common patterns and manipulation strategies do we see in how scammers and victims interact?**
- **How do scammers use psychological manipulation, and what key factors should we focus on to prevent these scams?**
- How can we design user-friendly tools on apps like LINE, WhatsApp, and Facebook to help people avoid getting scammed?
- What are the best ways to combine psychology and technology, like AI or data analysis, to create stronger defenses against scams on digital platforms?

Research Method

2

Digital Ethnographic Analysis

- Definition:
  - This is a qualitative research methodology that studies human behavior and interactions within digital spaces.
  - It applies traditional ethnographic approaches to digital environments, exploring cultures and practices shaped through online communities, social media, virtual reality, and digital technologies.

"You have to enter the tiger's den to catch the tiger."



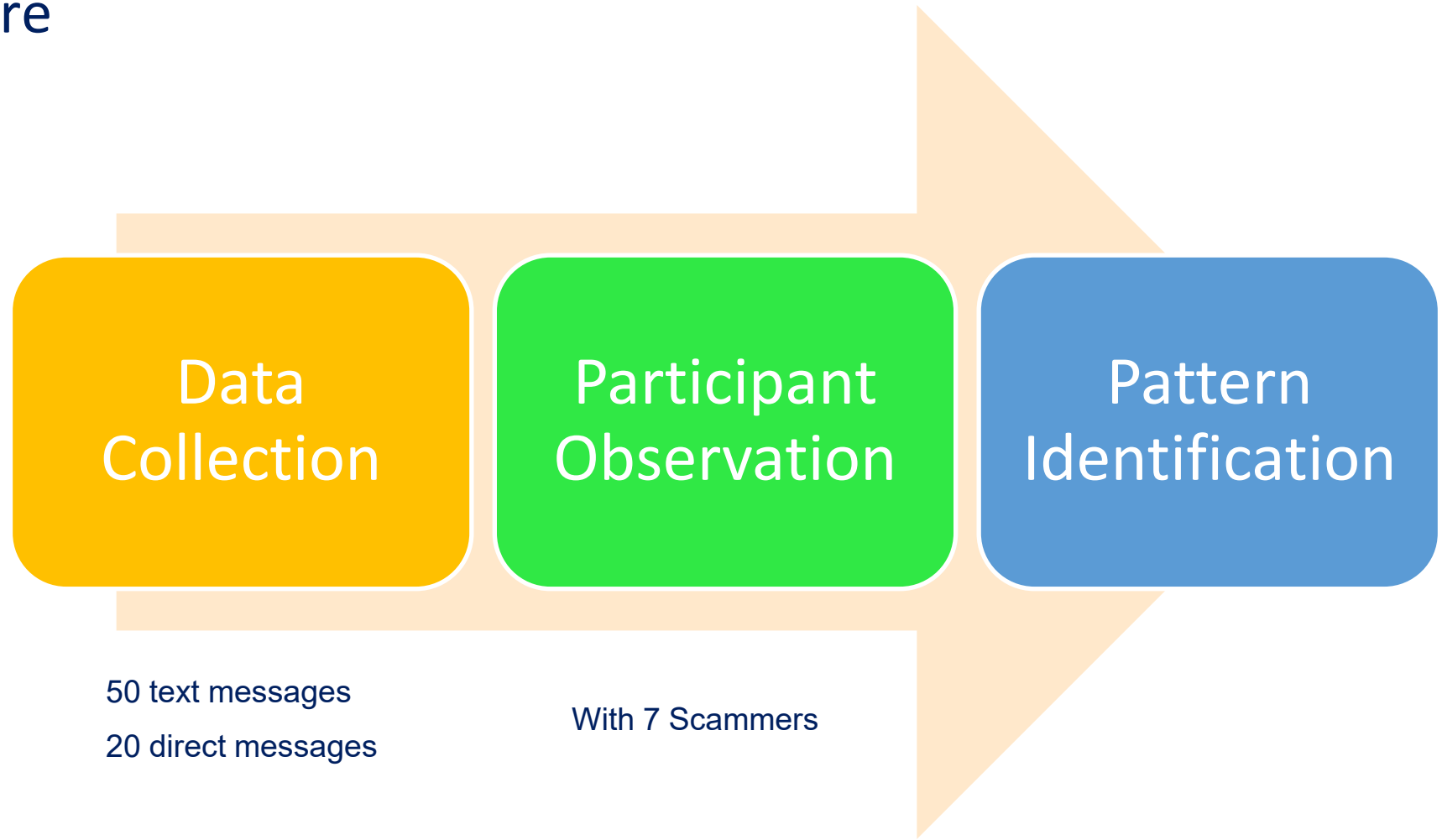
Digital Ethnographic Analysis

- Objective:
  - This study aims to investigate and analyze the interaction patterns, psychological triggers, and standardized processes used by scammers in cyber romance scams through direct communication.

- Methodology:
  - Using digital ethnographic methods, this study involved direct participant observation over a year-long period (October 2023–September 2024).
  - The researchers interacted with 7 unidentified individuals who initiated contact through social messaging platforms and web-based text messages.

Digital Ethnographic Analysis

- Procedure



Research Result

3

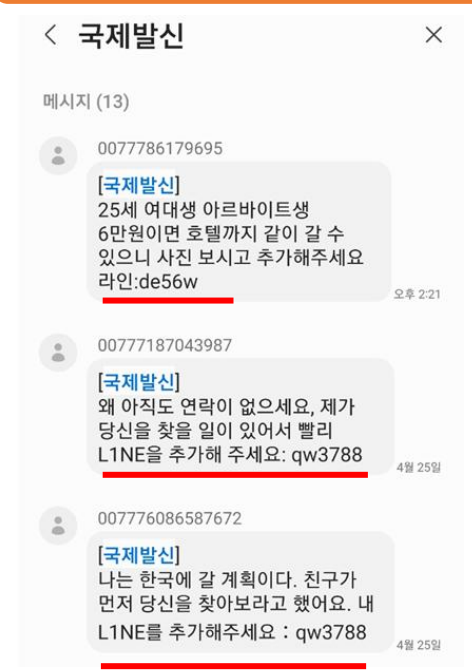
Cyber Romance Scam Process

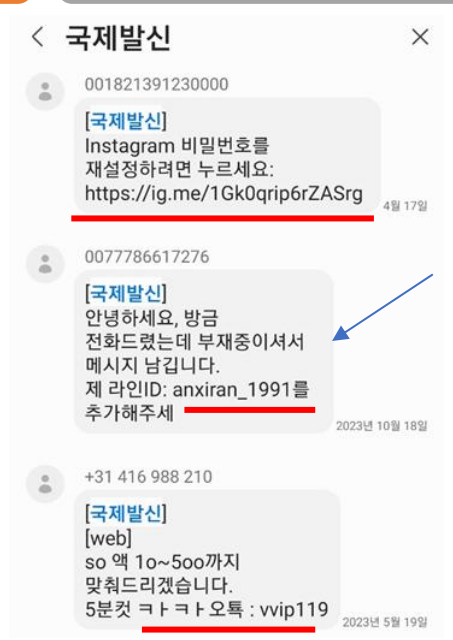
- A type of smishing scam using chat applications
- Type-1

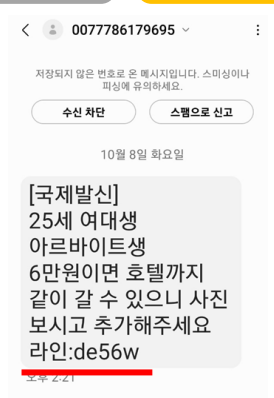
Text Message — International message or Web message

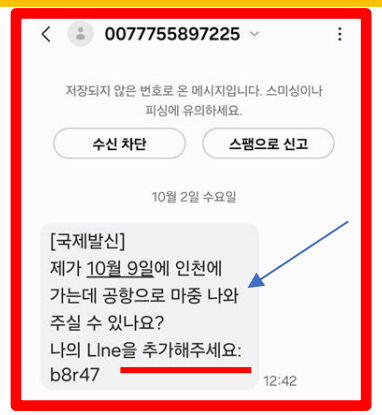
Friend request — 1) Friend request on a chat application → ?
2) Inducing link clicks → X

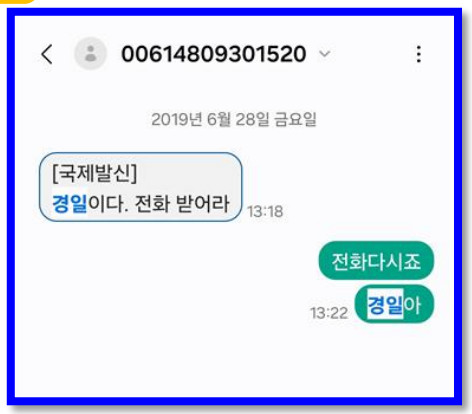
Fraud process — Encouraging registration, investment, and upfront payment











Cyber Romance Scam Process

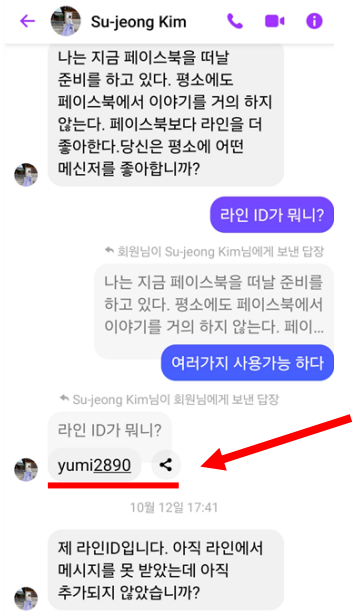
- A type of smishing scam using chat applications
- Type-2

Direct Message Sending direct message on SNS

Friend request Friend request on a chat application

Fraud Process Encouraging registration, investment, and upfront payment



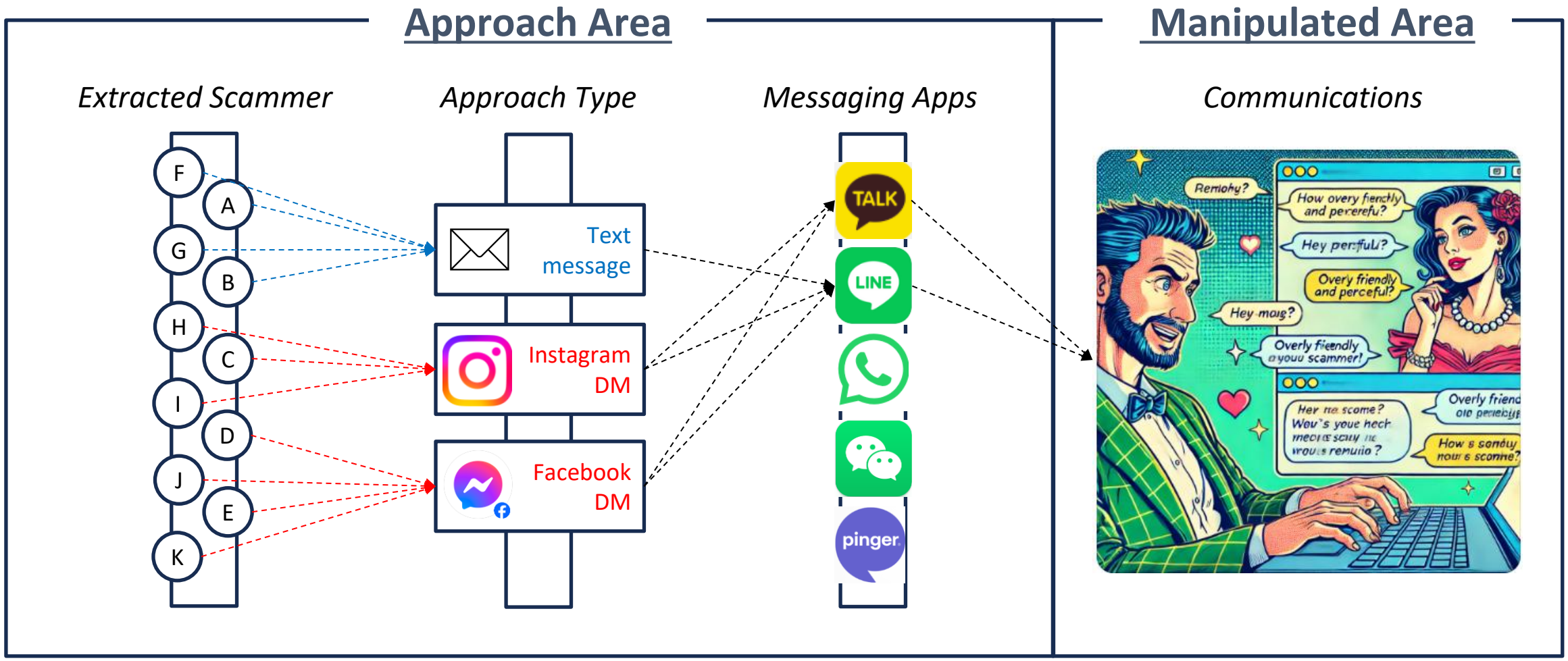






Cyber Romance Scam Process

- Process Understanding



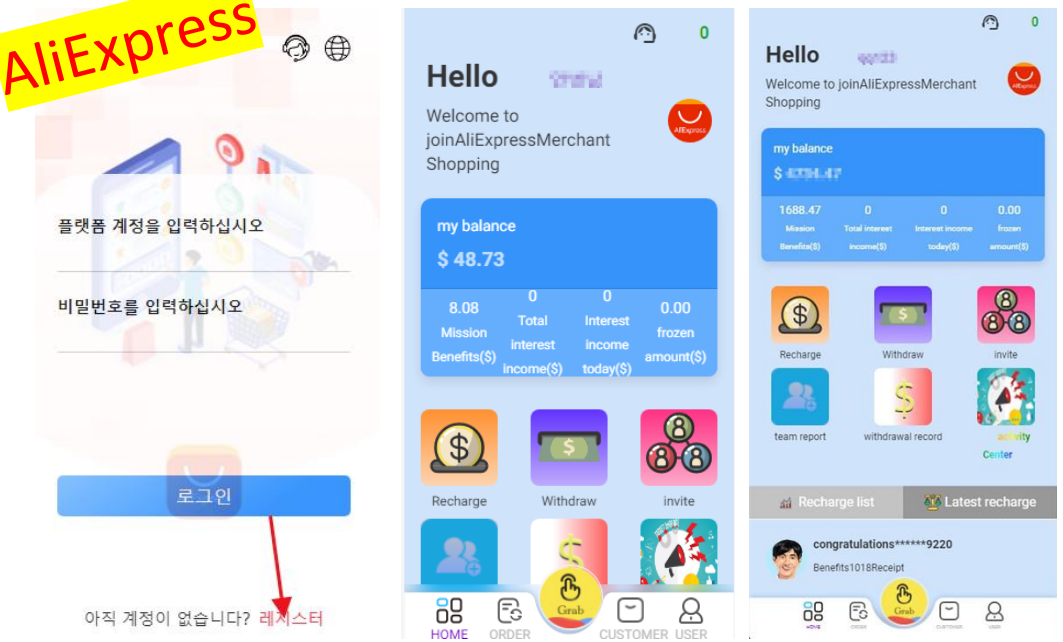
Research Result (Qualitative Study)

#	Contact Method		Used Apps	Initial Requirements	Trust-Building	Continued Fraud	Duration (≒)	Personal Info.		
	Messenger	Method						Gender	Country	Age
1	Text Message	Add ID	LINE	If you don't mind, let's be friends.	Photos Sharing (Hers, Family, Job, Friends)	Foreign Exchange Trading	1.5 Mon.	F	Vietnam	35
2	Text Message	Add ID	LINE	I accidentally reached out to you, but would you be my friend?	Photos Sharing (Hers, Foods, Job, Hobby)	Could you help AliExpress job? (registration)	0.5 Mon.	F	Singapore	35
3	Text Message	Add ID	LINE	Are you going to apply for the part-time job?	An attractive profile photo	Request for personal information(Tel#, Address, etc.)	1 Day	F	Not verified	36
4	Text Message	Add ID	LINE	If you don't mind, let's be friends.	Photos Sharing(Hers,)	Investments in online stores. Click some URL	2 Days	F	Hong Kong	33
5	Instagram	Add ID	LINE	Request to register on the trading platform	Photos Sharing(Daily life), message	Foreign Exchange Trading	0.5 Mon.	F	Singapore	40
6	Instagram	Add ID	LINE	Add me as a friend and let's keep in touch. Do you know Goldman Sachs?	Photos Sharing(Foods, Exercise, Job)	Photo impersonation, Foreign Exchange Trading	4 Days	F	Japan	38
7	Instagram	Add ID	LINE	If you don't mind, let's be friends.	Photos Sharing(Hobby, Shopping)	Photo impersonation, Foreign Exchange Trading	7 Days	F	Japan	37

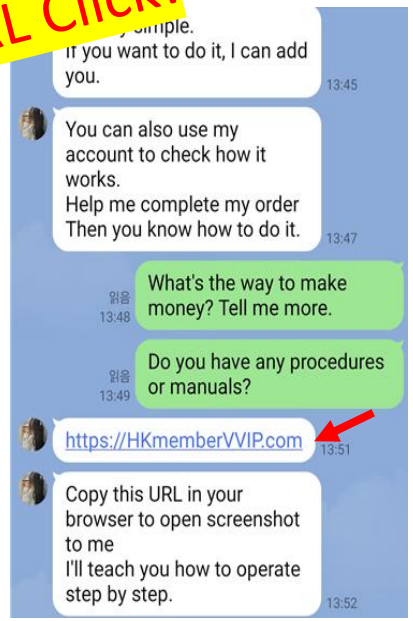
- Reasons for Confirming a Scammer: Requesting personal info., Prompting access to a specific website, Encouraging membership registration, Verified photo impersonation, Click URL, etc.

Research Result (example)

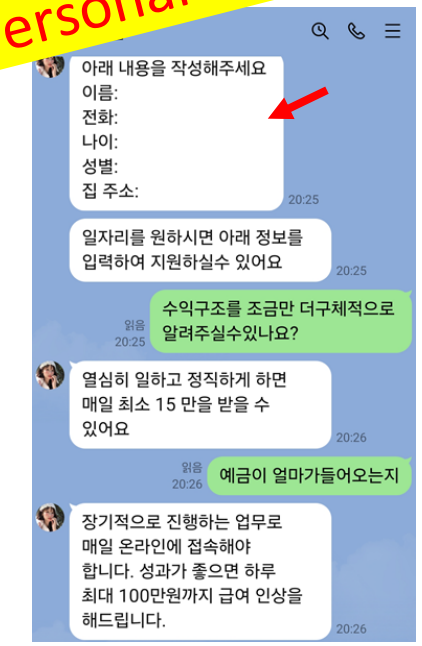
AliExpress



URL Click!

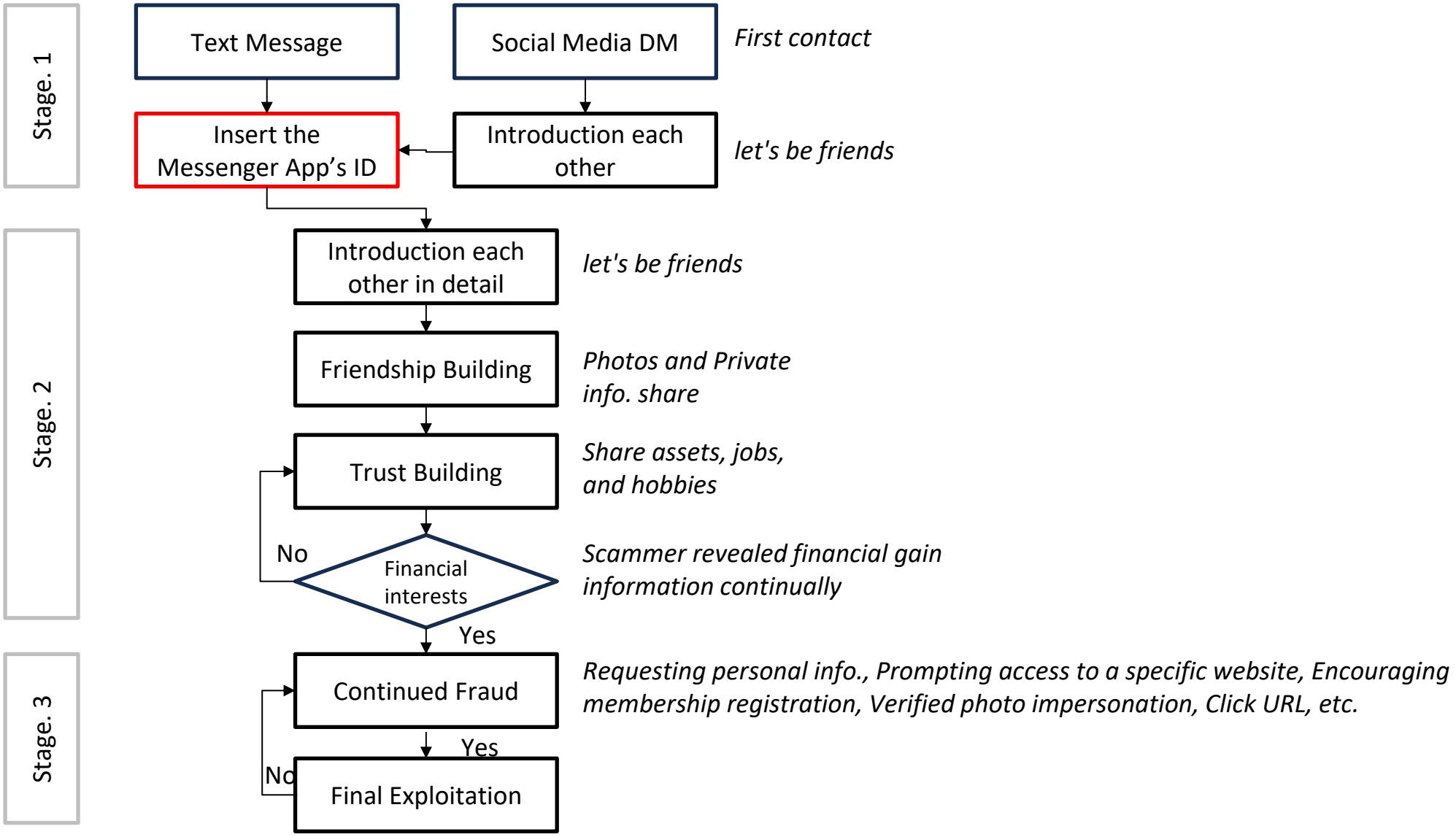


Personal Info.



Advanced Cyber Romance Scam Process

- Standard Process flow



Practical and Theoretical Contributions

4

Practical Contributions

- **Enhancing Security of Messaging Platforms**:
  - Proposes integrating a **preventive alert system** into social media and messaging platforms like LINE and WhatsApp to enable automated **fraud detection and user protection**, ensuring scalability across digital platforms.
- **Policy Recommendations for Digital User Protection:**
  - Provides **policy guidelines** to strengthen digital safety by standardizing and mandating the implementation of fraud prevention systems in collaboration with platform companies.
- **Raising Psychological Awareness and User Vigilance:**
  - Develops an alert system that enhances **psychological vigilance**, helping users recognize scam patterns and avoid potential risks.
  - Offers a **practical framework** for educational programs and awareness campaigns to reduce scam victimization and foster safer user behavior.

Theoretical Contributions

- **Expansion of Digital Ethnography**:
  - This study pioneers the application of digital ethnography to analyze real-time interactions with scammers, adding depth to fraud research
  - Bridges gaps in existing studies by emphasizing detailed interactions rather than retrospective victim accounts.
- **Standardization of Fraud Processes:**
  - Develops a standardized model of romance scam processes for further academic analysis
  - Highlights the interplay between emotional manipulation and linguistic patterns in cybercrimes.
- **Psychological Insight:**
  - Provides a deeper understanding of emotional vulnerabilities exploited by scammers.
  - Identifies recurring psychological triggers, such as loneliness and trust-building narratives.

Research Limitation

5

Research Limitations

- **Sample Size:** The study involved 50 text messages and 20 direct messages, which may limit generalizability across diverse scam scenarios.
- **Limited Platforms**: Focused primarily on LINE, Instagram, and Facebook. Scams on other platforms (e.g., Twitter, WhatsApp) were less explored.
- **Ethical Concerns**: Engaging directly with scammers, although insightful, raises ethical considerations regarding data collection and interaction.
- **Cultural Bias**: The study did not specify the nationality of fraudsters, but changes in fraud strategies due to cultural differences in various countries were not investigated.

Conclusion

6

Conclusion

- This research provides a comprehensive framework for understanding advanced cyber romance scams through digital ethnography.
- The findings have significant implications for fraud prevention, victim support, and platform policy development.
- Despite limitations, the study contributes both practically and theoretically by advancing knowledge of scammer strategies and offering a foundation for future research and technological innovations in cybercrime prevention.





Thank you !

Burujuajin@ajou.ac.kr
8210-8917-8022