RQ3 Thematic analysis

Table 1: Themes for user identification cues and related strategies

Define strategies based on cues, choose three colors:
Color 1: highlights observed strategies with no prior work
Color 2: highlights observed strategies where prior work already exists
Color 3: highlights empty cells where there is no strategy

Identify the strategies from the current identification and map those to fraud categories.

Fraud category	Identification theme (more heuristic)	Strategy
	Parent theme: Linguistic red flags	
	1.1. identified grammatical error in brand name	
	1.2. unconventional language use	
	1.3. excessive grammatical errors in sentence	
	1.4. unprofessional and unclear message	
	Parent theme: Account hacking extortion	
	1.5. financial extortion for account recovery	

	1.6.	OTP extortion for account recovery	
	1.7.	tiktok account banned	
	1.8.	account hacked	
	1.9.	unauthorized changes to account settings	
	Parent theme: Account discrepancy		
	1.10.	suspicious user account name	Reverse google search scammer
	1.11.	email domain name discrepancy	
	1.12.	no company logo	
	1.13.	using renowned company logo	
	1.14.	lack of TikTok presence	
	1.15.	multiple fake accounts	
	1.16.	profile picture mismatch	Reverse image search to verify profile pic
	1.17.	different country phone number	
	1.18.	lack of internet presence	
Impersonation	1.19.	slight difference in account names **(impersonation)**	
Impersonation	1.20.	difference in number of followers for creator and scammer profiles **(impersonation)**	
Impersonation	1.21.	found their profile impersonated	

	(impersonation)	

Table 2: Mapping Lure technique themes, victim fall categories, identification cues

What is driving the strategies - is it the fraud category or the lure technique?
Add sankey diagram for visual representation
Perform correlation of themes
Check for other video-format studies on scams. Specifically look at Elissa's work on image-based abuse.https://arxiv.org/abs/2411.09751
https://arxiv.org/pdf/2406.05520

Lure technique	Victim fall	Identification	Strategies
Fake rewards (money) (39)	Small amounts and mass targeting Enterprising fraudsters	**Account hacking extortion** ● financial extortion for account recovery ● OTP extortion for account recovery ● tiktok account banned ● account hacked ● unauthorized changes to account settings	
Emotional manipulation and trust exploitation (38) - Exploit user compassion (11) - Exploit user vulnerable emotional state (11) - Exploit user trust in content creator (8) - Exploiting need for luxury (4)	Visceral appeals	**Account hacking extortion** ● financial extortion for account recovery ● OTP extortion for account recovery ● tiktok account banned ● account hacked ● unauthorized changes to	

- Urgency manipulation (2) - Exploit parent concern for children (1) - Show interest in user profile (1)		account settings **Account discrepancy** ● suspicious user account name (Strategy: reverse google search scammer) ● email domain name discrepancy ● no company logo ● using renowned company logo ● lack of TikTok presence ● multiple fake accounts ● profile picture mismatch (Strategy: Reverse image search to verify profile pic) ● different country phone number ● lack of internet presence ● slight difference in account names (impersonation) ● difference in number of followers for creator and scammer profiles (impersonation) ● found their profile impersonated (impersonation)	
Creator exploitation (25) - increase followership promise (7) - fake collab promise (6) - grow account (4) - exploit user desire to be verified (4)	Authority and legitimacy		

- fake promise of contract (3) - pay for endorsed product (1)			
Low cost deception (20) - Low product price (19)	Small amounts and mass targeting Enterprising fraudsters		
Deceptive digital identity and marketing (20) - fake company account (6) - fake product (5) - fake celebrity video (4) - professional looking online presence (4) - fake influencer testimonial (1)	Small amounts and mass targeting Enterprising fraudsters	**Linguistic red flags** ● identified grammatical error in brand name ● unconventional language use ● excessive grammatical errors in sentence ● unprofessional and unclear message **Account discrepancy** ● suspicious user account name (Strategy: reverse google search scammer) ● email domain name discrepancy ● no company logo ● using renowned company logo ● lack of TikTok presence ● multiple fake accounts ● profile picture mismatch (Strategy: Reverse image search to verify profile pic) ● different country phone number ● lack of internet presence ● slight difference in account names (impersonation)	

		• difference in number of followers for creator and scammer profiles (impersonation) • found their profile impersonated (impersonation)	

Identification of scams - themes

1. Linguistic red flags (6)

1.22. identified grammatical error in brand name
1.23. unconventional language use
1.24. excessive grammatical errors in sentence
1.25. unprofessional and unclear message

2. Account hacking extortion (14)

2.1. financial extortion for account recovery
2.2. OTP extortion for account recovery
2.3. tiktok account banned
2.4. account hacked
2.5. unauthorized changes to account settings

3. Account discrepancy (38)

3.1. suspicious user account name (**Strategy:** reverse google search scammer)
3.2. email domain name discrepancy
3.3. no company logo
3.4. using renowned company logo

3.5. lack of TikTok presence
3.6. multiple fake accounts
3.7. profile picture mismatch (**Strategy:** Reverse image search to verify profile pic)
3.8. different country phone number
3.9. lack of internet presence
3.10. slight difference in account names **(impersonation)**
3.11. difference in number of followers for creator and scammer profiles **(impersonation)**
3.12. found their profile impersonated **(impersonation)**

Theme	Count
found their profile impersonated	15
email domain name discrepancy	4
lack of tiktok presence (4) lack of internet presence (2) no company logo (1)	7
multiple fake accounts	4
suspicious user account name (3) slight difference in account names (1)	3
using renowned company logo	3
lack of internet presence	
difference in number of followers for creator and scammer profiles	2
profile picture mismatch	2
different country phone number	1

4. Scammer communication pattern (46)

4.1. generic communication template (16)
4.2. ghosted victim (6)
4.2.1. no response to user's emails (1)
4.3. pressured to buy product/service (5) + excessive notifications (3)

4.3.1. undue pressure to take specific action (1)

4.4. requested to connect outside TikTok (4)

4.5. Pleasing users (6):

4.5.1. exaggerating user's importance (3)

4.5.2. repeated reassurance from scammer (1)

4.5.3. immediate contact with user after follow (2)

4.5.3.1. immediately follow back user account

4.6. unfulfilled promise (3)

4.7. scammer gaslighting user (3)

Theme	Count	Percentage
generic communication template	16	8
ghosted victim	5	2
requested to connect outside tiktok	4	2
pressured to buy product/service	4	2
excessive notifications	3	2
exaggerating user's importance	3	2
unfulfilled promise	3	2
scammer gaslighting user	2	1
repeated reassurance from scammer	1	0
undue pressure to take specific action	1	0
no response to user's emails	1	0
immediate contact with user after follow	1	0

5. Product and pricing misrepresentation (20)

5.1. duped with poor quality product

5.2.

5.3. never received product

5.4. requested extra shipping cost

5.5. cheaper products available online
5.6. exploitative return policy
5.7. product description mismatched with advertised used
5.8. excessive price for service
5.9. made exaggerated claims
5.10. unrealistically low price

Theme	Count
duped with poor quality product (8) **product description mismatched with advertised used (4)**	12
cheaper products available online (4) **unrealistically low price (1)**	5
never received product	4
excessive price for service (3) **requested extra shipping cost (1)**	4

6. Unauthorized transactions and monetary requests (27)

6.1. specific way of payment
6.2. requested money
6.3. unauthorized purchase on user's account
6.4. unauthorized extra fee
6.5. offered services for a fee
6.6. requested bank details
6.7. requested tiktok virtual money in exchange for money

7. Manipulative content (8)

7.1. difference in video quality of content **(impersonation)**
7.2. re-uploading creator's content **(impersonation)**
7.3. using celebrity video as bait
7.4. fake tiktok live

7.5. deepfake using AI
7.6. recurring instances of same content in different names

8. Past experience and collective action (19)

8.1. past experience with scam
8.2. Informed by people

9. Impersonation related scam identification pattern (17)

9.1. found their profile impersonated

Lure Techniques - reasoning themes:

1. **Fake rewards (money) (39)**
2. **Emotional manipulation and trust exploitation (38)**
   - Exploit user compassion (11)
   - Exploit user vulnerable emotional state (11)
   - Exploit user trust in content creator (8)
   - Exploiting need for luxury (4)
   - Urgency manipulation (2)
   - Exploit parent concern for children (1)
   - Show interest in user profile (1)
3. **Creator exploitation (26)**
   - increase followership promise (8)
   - fake collab promise (7)
   - grow account (4)
   - exploit user desire to be verified (4)
   - fake promise of contract (3)
   - pay for endorsed product (1)

4. **Low cost deception (20)**
   - Low product price (19)
   - Fake promise of energy saving (1)
5. **Deceptive digital identity and marketing (20)**
   - fake company account (6)
   - fake product (5)
   - fake celebrity video (4)
   - professional looking online presence (4)
   - fake influencer testimonial (1)

Advice related themes:

Transaction related advice (15)

1. use paypal to make transactions (1)
2. compare the deal or price on TikTok with those offered outside (1)
3. beware of livestreams advertising cheap selling products (1)
4. beware of low priced products (3)
5. Beware of ads for exaggerated claims about products (e.g., the world's heaviest bracelet) (5)
6. Research products and sellers before buying (8)

Advice on scammer profile and communication style (10)

1. look for grammatical errors (1)
2. beware of fake investment opportunities (2)
3. avoid collab with specific companies (1)
4. beware of emotional appeal scams (2)
5. beware of fake followers on the social media page of the company (1)
6. beware of fake success stories (2)
7. avoid paying for collab products (1)

Security related advice (10)

1. avoid sharing personal info to get gift cards (1)
2. avoid sharing personal info with strangers (2)
3. verify information (2)
4. beware of email domain name discrepancy (1)
5. avoid URLs from unknown emails (1)
6. avoid URLs from cashapp fake profiles (1)
7. Verify that email addresses match the company website (e.g., .com vs. .co) (2)

Advice specific to romance scam (8)

1. avoid sharing personal info with strangers (2)
2. excuse made by romance scammer to extract money (4)
3. beware of romance scammers asking for money (2)

Redressal related themes:

Internet search 4

- Searched internet 1
- Learn about scam 1
- Refer to reddit for guidance 1
- Google reverse search scammer 1

Community support 4

- Urged followers to report scam 3
- Followers informed creator 1

In-platform measures 27

- Create new account 3
- Use security measures 2
- Ignore scams 1
- Share evidence in tiktok video 12
- Cancelled item 2

- Block scammer 7

Report to entity 35

- Report to instagram 1
- Report to tiktok 12
    - Issues with tiktok redressal 10
- Reached out to scammer 4
- Report to payment vendor 6
- Suggestions for tiktok 1
- Reached out to legitimate vendor 1

Victim Fall Categories:

```
"Victim_1": "Psychological manipulation" - finance (20)

"Victim_2": "Exploiting desires",- manipulation(9))

"Victim_3": "Trust exploitation", account (28)

"Victim_4": "Financial deception",finance (4)

"Victim_5": "Product deception", shopping (14)

"Victim_6": "Social media manipulation", finance (4)
```

	shopping	romance	finance	edu	account	manipulation	ai-scam	health-scam
Victim_1	1	3	20	0	1	7	0	0
Victim_2	0	0	2	0	3	9	0	0
Victim_3	3	0	13	0	28	6	1	1
Victim_4	2	0	4	0	0	2	0	0
Victim_5	14	0	0	0	6	4	0	0
Victim_6	2	0	4	0	2	2	0	0

Appendix:

Identification of scams themes

Parent code	Child code list
	excessive notifications
	generic communication template
	suspicious user account name
	past experience with scam
	duped with poor quality product
	found their profile impersonated
	unfulfilled promise
	received counterfeit product
	never received product
	no response to user's emails
	specific way of payment
	requested extra shipping cost
	requested money
	difference in communication between scammer and original creator
	informed by people
	scammer gaslighting user
	immediately follow back user account
	cheaper products available online
	exploitative return policy
	immediate contact with user after follow
	product description mismatched with advertised used
	excessive price for service

Account hacking extortion	financial extortion for account recovery
	lack of internet presence
	requested to connect outside TikTok
Linguistic red flags	identified grammatical error in brand name
Linguistic red flags	unconventional language use
Linguistic red flags	excessive grammatical errors in sentence
Account hacking extortion	OTP extortion for account recovery
	Reverse image search to verify profile pic
	recurring instances of same content in different names
	ghosted victim
Linguistic red flags	unprofessional and unclear message
	email domain name discrepancy
	no company logo
	difference in video quality of content
	difference in number of followers for creator and scammer profiles
	exaggerating user's importance
	duping creator's product
	using renowned company logo
	made exaggerated claims
Account hacking extortion	tiktok account banned
	unauthorized purchase on user's account
	lack of tiktok presence
	undue pressure to take specific action

	unauthorized extra fee
	offered services for a fee
Account hacking extortion	account hacked
Account hacking extortion	unauthorized changes to account settings
	multiple fake accounts
	reverse google search scammer
	requested bank details
	repeated reassurance from scammer
	profile picture mismatch
	deepfake using AI
	pressured to buy product/service
	requested tiktok virtual money in exchange for money
	fake tiktok live
	re-uploading creator's content
	unrealistically low price
	slight difference in account names
	using celebrity video as bait
	different country phone number