Romance Scam Research Center

SOCIAL TECHNOLOGY AND SAFETY FOUNDATION

LIVING EVIDENCE SYNTHESIS

Attack Methods and Offender Strategies

Attack Methods and Offender Strategies: How Romance- and Relationship-Based Offenders Identify, Groom, Deceive, and Exploit Targets

Across the reviewed evidence, relationship-based online frauds are described as multi-stage deceptions that commonly use fabricated or impersonated social-media profiles—including Facebook and Instagram—to attract targets, present narrative-style profile content emphasizing self- and desired-partner descriptions while excluding non-narrative demographic fields, sustain communication over multiple letters or conversations, and escalate to financially framed extractions such as fake investment schemes or emergency/crisis scenarios. One analysis examined seven scam letter sets containing 18–23 letters each. Another study analyzed a two-year corpus of 53 authentic conversations between a romance scammer and the victim-author. Reported deception types in the reviewed material show fake investment schemes as the most common (54.2%) and emergency scenarios as the second most common (43.0%). The literature also notes limited scholarly attention to fraudsters’ communication strategies and factors influencing those strategies.

Published Aug 31, 2026 Updated Aug 31, 2026 Synthesis version 67

PUBLICATIONS	EVIDENCE STATEMENTS	CITED SOURCES	SYNTHESIS VERSION
26	275	26	67

Across the reviewed evidence, relationship-based online frauds are described as multi-stage deceptions that commonly use fabricated or impersonated social-media profiles—including Facebook and Instagram—to attract targets, present narrative-style profile content emphasizing self- and desired-partner descriptions while excluding non-narrative demographic fields, sustain communication over multiple letters or conversations, and escalate to financially framed extractions such as fake investment schemes or emergency/crisis scenarios. One analysis examined seven scam letter sets containing 18–23 letters each. Another study analyzed a two-year corpus of 53 authentic conversations between a romance scammer and the victim-author. Reported deception types in the reviewed material show fake investment schemes as the most common (54.2%) and emergency scenarios as the second most common (43.0%). The literature also notes limited scholarly attention to fraudsters' communication strategies and factors influencing those strategies. [5] [2] [1] [4] [6] [7]

Staged progression and experimental confirmation

Independent analyses support components of a stage-like sequence in relationship-based fraud. One study analysed seven scam letter sets, each containing 18–23 letters. A separate finding reports that a fake profile functions as a key initial mechanism for attracting and connecting with potential romance-fraud victims. Another study compiled a corpus of 53 conversations between romance scammers and the author, collected over a two-year period (2021–2023). [2] [8] [6]

Controlled sequential-communication experiments and offender-facing interaction studies provide process-level confirmation that money requests typically follow extended rapport-building rather than appearing at first contact, and that offenders adapt some communicative features in response to perceived reward signals from targets. Authors of these experimental studies caution about sample and identifiability limits, but the findings align with corpus-based observations of staged escalation. [7] [9] [6]

Profile construction and target selection

Offenders commonly create idealized, formulaic, or stolen-photo personas aimed at maximizing perceived credibility and fit with target preferences; comparative profile-corpus studies report narrower vocabulary, recurring personal-attribute adjectives (e.g., 'honest', 'loving'), and frequent use of first-person constructions consistent with template reuse. These linguistic and corpus findings also report frequent claims of high-status occupations (military, executive, medical) to justify later requests. [1] [10]

Case analyses and complaint datasets show that 80% of the offenses were linked to romance scams, and that offenders used Facebook and Instagram to impersonate people and to create fake profiles that advertise attractive individuals or make initial approaches on social networks. One study experimentally used known scammer profiles alongside verified genuine profiles that were matched by gender and age. [5] [12] [11]

Grooming mechanics and persuasion techniques

Qualitative message-corpus studies, thematic analyses of victim testimonials, and discourse-analytic work identify a recurrent set of persuasion techniques used during grooming: personalization, reciprocity and commitment appeals, manufactured crises and urgency framing, invocation of apparent authority figures, progressive intimacy ('love-bombing'), and repeated small requests (photographs, minor gifts, contact details) used as early compliance probes. These techniques are typically combined and sequenced to normalize requests and reduce critical evaluation. [13] [2] [14]

These techniques are typically combined and sequenced to normalize requests and reduce critical evaluation; multiple observational studies note that small earlier compliance acts (information, gifts) commonly precede larger monetary requests and that crisis narratives are frequently used at the point of extraction. [3] [2]

Extraction pathways and investment-hybrid (pig-butchering) variants

Final extraction commonly employs framed emergencies (medical, travel/customs, legal) and, in a large share of recent samples, investment narratives. Studies of pig-butchering and related hybrid romance–investment schemes document a pattern in which offenders first build prolonged trust and later steer victims toward fraudulent trading or investment platforms showing apparent early returns; victims then face escalating deposit requests and withdrawal obstacles. [4] [15] [16] [17]

Empirical sources and convicted-case analyses report diverse cash-out channels in practice—including gift cards, money-transfer services, bank transfers, and cryptocurrency wallets—and document that escalation from small initial transfers to large sums is a commonly reported trajectory in victim accounts. [3] [5] [18]

Organizational modes and offender perspectives

Operational modes vary across contexts: documentary analyses of convictions and investigator interviews describe structured, role-specialized groups with distinct functions (account/identity creation, chat/grooming personnel, technical support, and cash-withdrawal or money-movement roles). These organizational findings are based on court judgments, investigator reporting, and multi-site qualitative descriptions. [19] [20] [21]

The batch includes offender-facing research from Ghana: an ethnographic study using interviews and observations of Ghanaian romance-fraud offenders (methods described) and a hotspot survey that sampled 320 respondents from validated Ghanaian internet romance fraud hotspots. A separate survey of 397 respondents found 303 (76.4%) reported having engaged in some form of cybercrime. [23] [22] [24]

Methodological patterns, limitations, gaps, and future directions

The evidence base is methodologically heterogeneous: high-value contributions include PRISMA-guided reviews, crime-script and correspondence analyses, offender interviews, court-file documentary studies, controlled sequential-communication experiments, and blockchain forensics.

This diversity enables triangulation of recurring tactics but also produces evidence-specific limits to inference because many studies use small, purposive, geographically bounded samples or rely on self-selected complaint datasets. [25] [2] [5] [7] [8]

Important evidence gaps identified by authors include: (a) systematic, ethically approved offender interview studies across diverse jurisdictions to explain motives and decision rules; (b) larger authenticated datasets that link conversation transcripts to confirmed payment flows (including blockchain tracing where relevant); (c) cross-platform comparative research to test whether persuasion repertoires vary by platform or scam subtype; and (d) longitudinal or experimental replication to measure attacker adaptation and tactic effectiveness. [26] [4] [7] [16]

Where evidence supports it, authors recommend combining offender-facing qualitative work, larger authenticated conversation-to-transfer datasets (including blockchain tracing for crypto-enabled schemes), and replication of sequential-communication experiments with larger, better-validated samples to strengthen causal inference about tactic effectiveness and offender adaptation. Cross-disciplinary approaches—linking discourse analysis, behavioral experiments, and forensic tracing—are repeatedly proposed. [7] [8] [16] [6]

References

1. Lee, KF.; Chan, MY.; Mohamad Ali, A. (2022). Self and desired partner descriptions in the online romance scam: a linguistic analysis of scammer and general user profiles on online dating portals DOI
2. Dreijers, G.; Rudziša, V. (2020). Devices of Textual Illusion: Victimization in Romance Scam E-Letters DOI
3. Whitty, MT. (2013). Anatomy of the online dating romance scam DOI
4. Lim, A.; Choi, KS. (2025). Modus Operandi and Blockchain Analysis of Romance Scams: Cryptocurrency-Driven Victimization DOI
5. Soares, Adebayo Benedict; Lazarus, Suleman; Button, Mark (2025). Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud DOI
6. Faber, P. (2024). The Frames of Romance Scamming DOI
7. Wang, Fangzhou; Dickinson, Timothy (2024). Hyperpersonal feedback and online romance fraud: an empirical examination DOI

8. Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging DOI
9. Dickinson, T.; Wang, F.; Maimon, D. (2023). What Money Can Do: Examining the Effects of Rewards on Online Romance Fraudsters' Deceptive Strategies DOI
10. Annadorai, Kalaivani; Krish, Pramela; Shaari, Azianura Hani; Kamaluddin, Mohammad Rahim (2020). Mapping Computer Mediated Communication Theories and Persuasive Strategies in Analysing Online Dating Romance Scam DOI
11. Whitty, MT. (2019). Who can spot an online romance scam? DOI
12. Grace Carvalho Fernandes, S.; BASTOS DO NASCIMENTO, V.; Castelo Branco Do Nascimento, V. (2023). Romance Scam: Victim Manipulation and Human Trafficking DOI
13. Wang, F.; Topalli, V. (2022). Understanding Romance Scammers Through the Lens of Their Victims: Qualitative Modeling of Risk and Protective Factors in the Online Context DOI
14. Anesa, Patrizia (2020). Lovextortion: Persuasion strategies in romance cybercrime DOI
15. Cross, C. (2023). Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud DOI
16. Wang, F.; Zhou, X. (2022). Persuasive Schemes for Financial Exploitation in Online Romance Scam: An Anatomy on Sha Zhu Pan (□□□) in China DOI
17. Botha, Johannes George; Singh, Kreaan; Leenen, Louise (2025). Analysis of a Cryptocurrency Investment Scam: Pig Butchering DOI
18. Yosiandra, Syakira Yuniar; Sakariah, Dewi Saraswati (2024). Unveiling the Romance Scam Scheme: Psychological Manipulation and Its Impact on Victims DOI
19. Choi, SW.; Lee, J.; Choi, YJ. (2024). Unveiling the Patterns of Romance Scams in South Korea DOI
20. Lee, Hyejin; Boo, Minseo (2025). Analyzing the Evolving Modus Operandi of Romance Scams via Court Judgments: Crime Script and Policy Implications DOI
21. Luo, Qiaoyu; Zhao, Yun (2025). Butcher or be butchered: understanding the unwitting recruitment by cybercrime groups in China DOI
22. Abubakari, Yushawu (2024). Modelling the modus operandi of online romance fraud: Perspectives of online romance fraudsters DOI
23. Toku, L.; Otu Offei, M. (2023). The client's consent strengthens the 'Gamers' hand; The deterrence theory's perspective of the Internet romance fraudsters. DOI

24. Obeng, Charles; Kumah, Paul Kwasi; Asiedu, Hubert Bimpeh; Obeng Senior, Felix Awuah (2024). Understanding Cybercrime in Developing Economies: Insights from Agona Swedru, Ghana DOI
25. Bilz, A.; Shepherd, LA.; Johnson, GI. (2023). Tainted Love: a Systematic Literature Review of Online Romance Scam Research DOI
26. Yoshida, Yutaka (2025). Therapeutic but toxic spaces: Romance fraud victimization from a psychosocial perspective DOI

This AI-assisted synthesis is based on reviewed evidence records. It may contain errors or omissions. Follow the publication and DOI links, consult the original works, and make your own judgment about the evidence.

About this document

This living evidence synthesis was produced through AI-assisted analysis of approved RSRC publications. Claims are linked to supporting evidence and checked for source consistency. It may change as the corpus is updated. Readers should consult the cited publications when making research, policy, or practice decisions.

Current web version: https://romancescamresearch.org/research-insights/attack-methods-and-offender-strategies-how-offenders-identify-approach-groom-deceive-and-exploit-targets