

Romance Scam Research Center

SOCIAL TECHNOLOGY AND SAFETY FOUNDATION

LIVING EVIDENCE SYNTHESIS

Prevention and Intervention

Prevention and Intervention for Romance- and Relationship-Linked Online Scams: Evidence Synthesis

Reviewed evidence supports a layered, stage-aware prevention and intervention approach that emphasizes earlier recognition triggers linked to concrete verification behaviours, development and controlled evaluation of small-scale interactive education prototypes, complementary platform- and financial-sector mitigations, and strengthened, nonjudgmental victim support. High-quality qualitative and mixed datasets document staged grooming processes and identify recognition triggers that can be operationalized in messaging and practice. Prototype educational tools (including an immersive VR exercise and mock-platform prototypes) demonstrate feasibility and strong immediate usability or engagement signals in very small pilot samples but lack longitudinal behavioural or retention outcome data. Platform- and financial-sector proposals—such as account re-verification, mass-message blocking, AI-enabled transaction monitoring, and exchange-side inducement-detection—are repeatedly recommended as complements to education; some operational interventions show promising signals (for example, a financial-intelligence warning-letter program) but existing detection methods face documented high false-positive rates and adaptation limits. Authors consistently call for rigorous evaluations (including controlled tests of education formats), ethical assessment of automated/paternalistic measures, external

validation of detection datasets and workflows, and longitudinal tracking of offender trajectories and intervention impacts.

Published Aug 30, 2026	Updated Aug 30, 2026	Synthesis version 66
------------------------	----------------------	----------------------

PUBLICATIONS	EVIDENCE STATEMENTS	CITED SOURCES	SYNTHESIS VERSION
23	89	23	66

Reviewed evidence supports a layered, stage-aware prevention and intervention approach that emphasizes earlier recognition triggers linked to concrete verification behaviours, development and controlled evaluation of small-scale interactive education prototypes, complementary platform- and financial-sector mitigations, and strengthened, nonjudgmental victim support. High-quality qualitative and mixed datasets document staged grooming processes and identify recognition triggers that can be operationalized in messaging and practice. Prototype educational tools (including an immersive VR exercise and mock-platform prototypes) demonstrate feasibility and strong immediate usability or engagement signals in very small pilot samples but lack longitudinal behavioural or retention outcome data. Platform- and financial-sector proposals—such as account re-verification, mass-message blocking, AI-enabled transaction monitoring, and exchange-side inducement-detection—are repeatedly recommended as complements to education; some operational interventions show promising signals (for example, a financial-intelligence warning-letter program) but existing detection methods face documented high false-positive rates and adaptation limits. Authors consistently call for rigorous evaluations (including controlled tests of education formats), ethical assessment of automated/paternalistic measures, external validation of detection datasets and workflows, and longitudinal tracking of offender trajectories and intervention impacts. [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#) [\[6\]](#) [\[7\]](#) [\[8\]](#) [\[9\]](#) [\[10\]](#) [\[11\]](#) [\[12\]](#) [\[13\]](#) [\[14\]](#) [\[15\]](#)

Stage-aware framing and the staged grooming model

Multiple high-quality qualitative syntheses and stage-model studies document a recurring grooming trajectory in which scammers develop rapport and trust before initiating monetary extraction; these staged descriptions motivate prevention that foregrounds recognition cues earlier in the interaction timeline rather than relying on single admonitions. [\[1\]](#) [\[2\]](#) [\[3\]](#)

Because these stage-based descriptions are grounded in victim accounts and mixed qualitative datasets, prevention frameworks that map interventions to interaction stages (for example, recognition prompts before first transfers) are repeatedly recommended across the literature as a way to close the gap between suspicion and protective action. [\[1\]](#) [\[3\]](#) [\[2\]](#)

Recognition triggers and prevention messaging

Empirical work that collected large numbers of self-reported victim recognition moments shows that triggers cluster into themes—additional money requests, communication features, failed verification, offender actions, and third-party involvement—and that many victims only notice these triggers after loss, creating a prevention gap that stage-aware messaging seeks to close by linking each trigger to a concrete verification action. [\[3\]](#)

Reviewed studies support shifting awareness content from abstract admonitions (for example, 'don't send money') toward stage-linked, behavior-focused triggers that recommend specific verification steps or pause-to-check actions, because simple slogans can misrepresent grooming dynamics and encourage self-blame. [\[3\]](#) [\[12\]](#) [\[10\]](#)

Education, interactive prototypes, and experiential approaches

Interactive prototypes (for example, a mock dating-platform exercise and an immersive VR game) demonstrate feasibility and strong immediate usability/engagement metrics in small pilot samples, suggesting potential to improve user attention and experiential learning, but sample sizes are very small, internal-consistency on some education measures was limited, and longitudinal behavioural or retention outcomes remain untested. [\[4\]](#) [\[5\]](#)

Prototype evaluations reported above-average usability scores in a very small HeartGuard VR pilot (mean SUS = 79.75) alongside limited internal consistency for an education measure and explicit calls within the prototype literature for larger, follow-up studies to establish retention and real-world behaviour change. [\[5\]](#)

Platform- and financial-sector mitigations

Authors recommend platform-level measures to complement education, including account-creation phone collection with periodic re-verification, requiring multiple profile images and human-image checks, and automated controls such as suspending accounts that send mass messages or flagging abusive phrases and external-link redirects. [\[6\]](#)

Financial-sector proposals include AI-powered fraud detection and real-time transaction monitoring and exchange-side approaches (for example, using small inducement payments to detect ongoing scams). An Australian financial-intelligence letter intervention that warned people who had transferred money to typical scam countries was followed by most recipients making no further transfers, indicating potential for targeted financial-sector actions; however, authors also highlight ethical and operational considerations for aggressive automated prevention (for example, flagged or delayed transactions) that require further empirical and ethical assessment. [\[7\]](#) [\[8\]](#) [\[9\]](#)

Detection features, linguistic analysis, and operational constraints

Linguistic and structural similarities across scam messages have been proposed as usable warning templates to discourage disclosure of personal data or joining suspicious financial schemes, and discourse-analytic work aims to translate message features into public-facing indicators for awareness and training. [\[16\]](#) [\[17\]](#) [\[18\]](#)

Implemented forensic and automated detection approaches face documented constraints: at least one reviewed study explicitly describes existing detection methodologies as having high false-positive rates and weak adaptation to changing tactics, which limits operational confidence without further validation and robustness testing. [\[6\]](#)

Tailored victim support, vulnerable groups, and ethical cautions

Authors caution against unconditional paternalistic measures (for example, blanket account or payment blocking) because such actions can undermine victim agency; instead, conditional and ethically evaluated interventions are proposed (thresholds based on unaffordable repeated losses or assessed impaired decision-making), requiring explicit empirical development and ethical assessment. [\[19\]](#)

Qualitative work identifies people with acquired brain injury as a group with documented, specific needs: survivors and close others call for simple, repeated one-to-one interactive training, mock-scam exercises, central resources, and improved professional awareness; hearing from other survivors is also reported as effective for reducing denial and encouraging help seeking. The evidence base also documents broader calls for immediate referral to counselors informed about romance scams and for law-enforcement interactions that avoid judgment or ridicule. [\[15\]](#) [\[20\]](#)

Methodological patterns, evidence gaps, and prioritized future work

Authors also identify urgent topical gaps that should inform future prevention work: updating advice for AI-enabled deception (deepfakes defeat reverse-image search), developing empirically tested victim-support interventions (including ABI-tailored approaches), and longitudinal tracking of offender trajectories and intervention impacts to understand long-term effectiveness. [\[13\]](#) [\[14\]](#) [\[15\]](#) [\[21\]](#)

Independent audits of the reviewed literature further emphasize three priority items supported by multiple records: updating prevention advice for AI-enabled deception because synthetic images can defeat reverse-image searches; conducting longitudinal research to track offender trajectories and intervention impacts over time; and assessing the ethical implications of automated, transaction-level prevention or paternalistic blocking measures. [\[13\]](#) [\[7\]](#) [\[14\]](#) [\[21\]](#)

The literature also highlights the need for coordinated multidisciplinary research combining psychological, technological, and criminological perspectives and for co-designed, context-sensitive pilot testing of interventions with explicit outcome measures; co-design work documents stakeholder-driven development of intervention content, measures, and sustainability plans through

20 hours of hybrid focus-group engagement. [\[22\]](#) [\[11\]](#) [\[23\]](#)

However, explicit evidence that recommended co-designed pilot testing uniformly includes ethical oversight is not provided in the cited co-design and review records, so any requirement for mandatory ethical oversight should be framed as a recommended best practice pending explicit, supporting evidence. [\[22\]](#) [\[11\]](#) [\[23\]](#)

References

1. [Whitty, MT. \(2013\). Anatomy of the online dating romance scam DOI](#)
2. [Whitty, MT. \(2013\). The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam DOI](#)
3. [Cross, C. \(2023\). "I knew it was a scam": Understanding the triggers for recognizing romance fraud DOI](#)
4. [Dickerson, S.; Apeh, E.; Ollis, G. \(2020\). Contextualised Cyber Security Awareness Approach for Online Romance Fraud DOI](#)
5. [Lea, Octavia; Shepherd, Lynsay A.; Szymkowiak, Andrea \(2024\). HeartGuard VR: Immersive Romance Scam Education DOI](#)
6. [Vedhanayagam, Priya; Singh, Moulik; Dadhania, Arora Preksha; Ikram, Sumaiya Thaseen \(2026\). Forensic footprints in digital love: Unveiling romance scams with Maltego and machine learning DOI](#)
7. [Krause, David \(2025\). The Deceptive Allure: Understanding and Combating Cryptocurrency Pig Butchering Scams DOI](#)
8. [Griffin, John M.; Mei, Kevin \(2024\). How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering DOI](#)
9. [Thiel, C. \(2020\). Love scam in cyberspace DOI](#)
10. [Wang, Fangzhou \(2023\). Essays on the Rationality of Online Romance Scammers DOI](#)
11. [Lazarus, S.; Whittaker, JM.; McGuire, MR.; Platt, L. \(2023\). What do we know about online romance fraud studies? A systematic review of the empirical literature \(2000 to 2021\) DOI](#)
12. [Kassem, R.; Carter, E. \(2023\). Mapping romance fraud research – a systematic review DOI](#)
13. [Cross, C. \(2022\). Using artificial intelligence \(AI\) and deepfakes to deceive victims: the need to rethink current romance fraud prevention messaging DOI](#)

14. [Fletcher, Rachel; Tzani, Calli; Ioannou, Maria \(2024\). The dark side of Artificial Intelligence – Risks arising in dating applications DOI](#)
15. [Gould, Kate R.; Carminati, Jao-Yue J.; Ponsford, Jennie L. \(2021\). “They just say how stupid I was for being conned”. Cyberscams and acquired brain injury: A qualitative exploration of the lived experience of survivors and close others DOI](#)
16. [Dreijers, G.; Rudziša, V. \(2020\). Devices of Textual Illusion: Victimization in Romance Scam E-Letters DOI](#)
17. [Lee, KF; Chan, MY; Ali, Afida Mohamad \(2024\). Drawing on social approval as a linguistic strategy: A discourse semantic analysis of judgement evaluation in suspected online romance scammer dating profiles DOI](#)
18. [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](#)
19. [Sorell, T.; Whitty, M. \(2019\). Online romance scams and victimhood DOI](#)
20. [Whitty, MT.; Buchanan, T. \(2015\). The online dating romance scam: The psychological impact on victims – both financial and non-financial DOI](#)
21. [Barnor, J. \(2024\). The charade of discreetness: Exploring the paradoxical lifestyles of romance fraudsters DOI](#)
22. [Thumboo, Sharen; Mukherjee, Sudeshna \(2024\). Digital romance fraud targeting unmarried women DOI](#)
23. [Chew, Kimberly Ann; Ponsford, Jennie Louise; Gould, Kate Rachel \(2025\). “This is a lifesaver”: co-designing a novel cyberscam psychosocial recovery intervention framework for people with acquired brain injury 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/prevention-and-intervention-for-online-romance-scams-evidence-synthesis>