



Brief

Introduction to Social Engineering: Romance Scams

B-2025-03-14a

Classification: TLP:CLEAR

Criticality: Low

**Intelligence Requirements: Social Engineering, Romance Scams, Financial
Extortion**

March 14, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EDT) on March 14, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Introduction to Social Engineering: Romance Scams

ZeroFox's Social Engineering series breaks down aspects of the threat into digestible reports and outlines defensive actions that can be taken to combat it. Part Six of this series takes a deep dive into sextortion and other romance scams: why and how threat actors do it, and how the threat can best be mitigated.

Key Points

- Romance scams are a type of confidence scheme whereby a threat actor seeks to exploit a victim's romantic emotions—usually to achieve a financial objective.
- Romance scams take many forms and are perpetrated by a host of different types of threat actors, from individuals seeking punitive retribution to semi-structured collectives sometimes able to extort millions of dollars in revenue.
- Threat actors conducting romance scams are rapidly incorporating artificial intelligence (AI)-driven technology into their toolsets, augmenting attack techniques during victim selection and initial contact phases through to exploitation.
- Sextortion and romance scam threat actors are very likely to continue evolving their attack techniques in 2025, circumventing security hygiene measures and capitalizing upon the challenges faced by national and international law enforcement (LE) bodies.

| What are romance scams?

Romance scams are a type of confidence scheme whereby a threat actor seeks to exploit a victim's romantic emotions in order to achieve an objective that is usually financially motivated. Upon selecting a target considered vulnerable, a threat actor will attempt to gain trust and affection by fabricating a romantic relationship with them. Various exploitative techniques can then be deployed that seek to gain trust, prolong the relationship, and extract reward (usually monetary) from the victim.

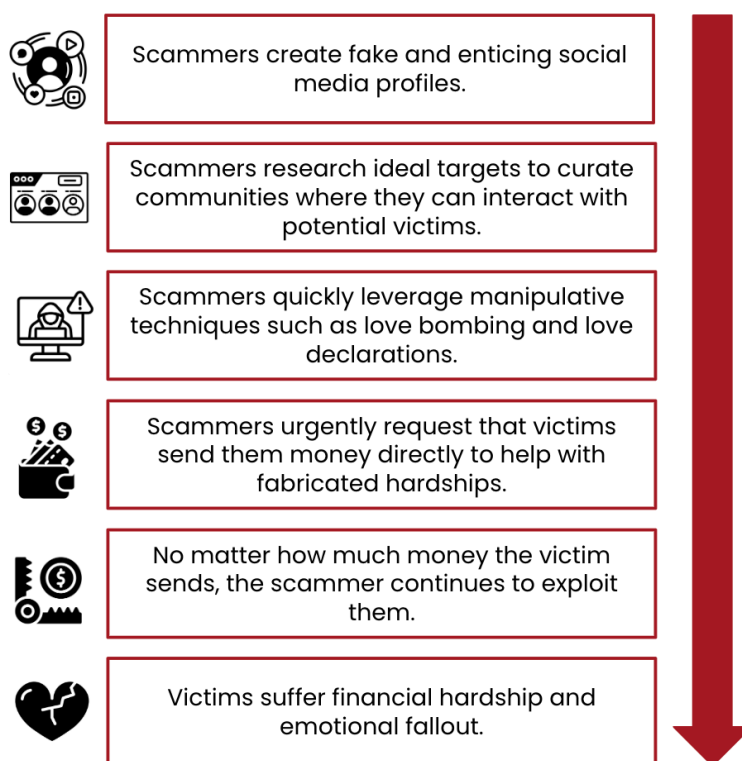
Romance scams take many forms and are perpetrated by a host of different types of threat actors, from individuals seeking punitive retribution to semi-structured criminal gangs that are sometimes able to extort millions of dollars in revenue. Romance scams also vary significantly in timescale, with some intended to achieve results within a few hours and others attempting to establish a high-payoff relationship lasting several years.

Threat actors target specific demographics to yield a high payoff at a low risk. For example, catfishing and impersonation tactics are notably more dangerous to older generations, who often find it difficult to distinguish between legitimate and illegitimate social media accounts. Lonely, divorced, or widowed individuals are also heavily targeted in these schemes, as they are perceived as more likely to be receptive to affection. However, some romance scam techniques, such as fake cryptocurrency investment schemes, are more likely to target younger generations or those with access to an adjacent victim pool of family or friends.

Both the number of romance scams taking place and amount of stolen funds are difficult to quantify. A primary reason for this is underreporting, as research suggests that as little as 3.6 percent of incidents are reported.¹ Romance scams also often evolve into other types of malicious cyber activities, such as impersonation or cryptocurrency-based crime, leading to confusion in categorization. Lastly, as with the majority of cybercrime, many incidents cross international borders, making LE collaboration and coordination difficult.

¹ [hXXps://www.comparitech.com/blog/vpn-privacy/romance-scams/](https://www.comparitech.com/blog/vpn-privacy/romance-scams/)

The threat posed by romance scams towards individuals around the globe is almost certainly growing. The estimated financial cost of romance scams has been increasing year-on-year, despite some reporting suggesting that the total number of incidents is on a downward trajectory.² This is very likely indicative of threat actors opting for fewer but higher effort, higher payoff attacks rather than large numbers of low-effort attacks as has historically been typical of the majority of social engineering attacks techniques.



Confidence–Romance scam overview example

Source: ZeroFox Intelligence

Romance scam stages. While the specific tactics, techniques, and procedures (TTPs) vary, romance scams generally follow an attack chain composed of five fundamental pillars:

- **Victim selection.** The threat actor determines their intentions and desired end state, along with the TTPs that are to be leveraged in order to achieve a favorable risk-payoff ratio. This is conducted adjacent to impersonation-strategy planning.

² [hXXps://www.ic3\[.\]gov/AnnualReport/Reports/2023_IC3Report\[.\]pdf](https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report[.].pdf)

For example, if an attacker chooses to impersonate a celebrity, they will likely seek potential victims in public celebrity fan pages on social media. If an attacker decided to impersonate a fitness influencer, they could seek potential victims within forums used by those seeking weight-loss advice.

Key factors in victim selection include the likely chances of success, the perceived payoff of success, the ease with which appropriate entities or lures can be impersonated, and both the online activity and emotional vulnerability of the potential victim.

- *Initial contact.* Upon selecting a victim, the threat actor will seek to engage. This may be directly, such as by sending messages to the victim's social media accounts or leveraging "wrong number" texts, or indirectly by leaving public comments on the victim's page or otherwise interacting with the victim's online presence. One method scammers commonly use is to initiate contact by pretending to be an old friend that the target briefly met in the past—an exchange likely forgotten by the victim—as a ploy to start a conversation. Scammers will often encourage the victim to make first contact in order to circumvent any privacy protocols in place.
- *Developing a trusting relationship.* Once the victim is engaged, the attacker will attempt to develop an emotional connection. In this stage, a threat actor may use love-bombing to flood the victim with fast-paced and constant attention, straddling a line between achieving manipulation and appearing illegitimate. The extent of success in this stage is highly dependent on prior victim research conducted by the attacker and their ability to align their approach with the victim's emotional needs.

During this stage, the threat actor often employs a combination of both templates and scripts that outline a face-paced, engineered, near-perfect romantic relationship, as well as ad hoc responses to suit the situation. Threat actors leverage readily available tools to produce custom-made, altered, or synthetic media to satisfy any verification requests made by the victim.

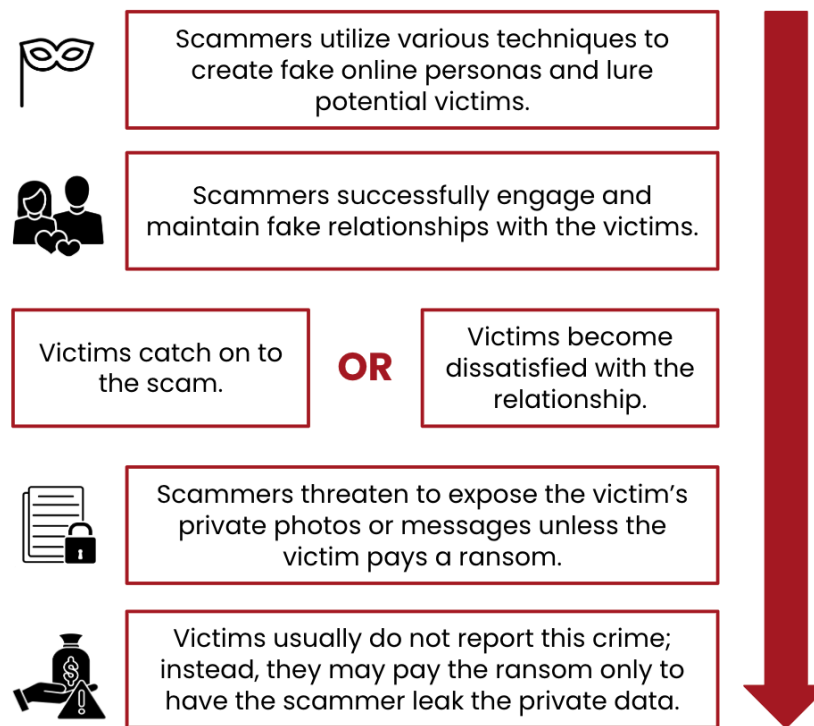
- *Isolation.* Attackers attempt to isolate the victim in order to increase the likelihood of success in subsequent manipulative exploitation. By isolating the victim and encouraging privacy, third parties such as friends, family, or support groups are less likely to raise suspicion or expose the facade.

As the relationship develops, victims often become increasingly intent on meeting in-person, either as part of the natural progression expected from a relationship or borne from a growing skepticism toward the situation. The attacker will often again deploy synthetic or altered media to stave off such requests or begin using excuses such as fictitious personal emergencies or faked frustrations at the continued requests.

- *Exploitation.* Once the victim is deemed sufficiently isolated and manipulated, they will be extorted. This activity can take place at any stage and for an indefinite number of times, depending on the attacker's perceived stability of the relationship and appetite for risk and the victim's level of awareness.

Attackers will fabricate emotionally driven hardships such as basic housing needs, medical care, cellular service, or other emergent suffering to justify their need for money from the victim. The attacker will often seek to foster longevity by beginning with relatively low-risk asks before escalating to higher-payoff requests. Often, the attacker will seek to end the relationship with as high-payoff activity as possible.

Should the victim become aware of the extortion, blackmail is often leveraged as a last-ditch effort. Material gained through the relationship (such as private conversations, secrets and confessions, or explicit images) is often used as leverage, with attackers threatening to share them with the victim's friends, family, or employers. Often, initial demands being satisfied only lead to larger ransoms—or the forcing of the victim to conduct subsequent scamming activity themselves.



Blackmail example overview

Source: ZeroFox Intelligence

Romance Scam Tactics, Techniques, and Procedures

Circumstances vary significantly between individuals, necessitating that threat actors adopt fast-changing TTPs. Even during the course of a single romance scam, the attacker is often required to dynamically respond to human traits such as curiosity, skepticism, and self-preservation. Adaptivity is then required to increase the scam longevity and ensure success. Growing awareness of romance scams and general online security amongst potential victims almost certainly forces threat actors to reevaluate their capabilities and likelihoods of a high-payoff attack.

Beyond the victim, attackers must also adjust to the ever-changing legislative and security landscape. Both local and international LE agencies prosecute cases, while

online private companies such as dating sites and social media platforms have introduced increasingly stringent security protocols.³⁴

As of the writing of this report, these are some of the most commonly adopted and prominent romance scam techniques:

Catfishing. This is a technique whereby the attacker leverages stolen images of other individuals in order to create fake social media profiles. Typically, personal details amounting to a convincing backstory are fabricated in the creation of a fictional online persona. The images stolen—often from an individual perceived as attractive—serve as a face for the persona to mislead victims into falling victim to subsequent malicious activity.

While the catfisher may intend to conduct financial extortion or other fraudulent activities, the majority of instances observed are conducted by attackers seeking to augment their attractiveness during online dating. For example, individuals may have various personal reasons for catfishing activity, such as historical dating struggles caused by insecurities or social awkwardness. Individuals who commit catfishing in this scenario often hope that, upon forming an emotional bond, the victim will be more accepting of their legitimate self. Catfishers are likely to reveal their true identity at this point and reassure victims that a loving relationship can persevere.

Individuals whose media is stolen for use by catfishers may also be a victim themselves. Revenge-motivated or other personal malicious actors can choose to catfish a victim in order to post offensive, sensitive, or private information while pretending to be the victim. This type of catfishing can also do reputational and emotional harm to the affected victims.⁵

Impersonation. While impersonation can be similar to catfishing, the primary difference is that the attacker leverages stolen media and credentials to pretend to be an existing person. This includes fully impersonating aspects of their identity, such as education,

³ [hXXps://kanzlei-herfurtner\[.\]com/romance-scam-money-laundering/](https://kanzlei-herfurtner[.]com/romance-scam-money-laundering/)

⁴ [hXXps://about.fb\[.\]com/news/2025/02/how-avoid-romance-scams-this-valentines-day/](https://about.fb[.]com/news/2025/02/how-avoid-romance-scams-this-valentines-day/)

⁵ [hXXps://www.cybersmile\[.\]org/help-center/catfishing/](https://www.cybersmile[.]org/help-center/catfishing/)

employment history, or geographical locations. Stolen photos and posts further enhance the facade, tricking the victim into believing they are interacting with the impersonated individual. Those with large social media followings or other forms of social prestige are often impersonated online. This includes doctors, celebrities, and military service members.

- *High-Status Professions.* The deliberate and targeted impersonation of an individual in a perceived high-status profession, such as a doctor, allows scammers to present themselves as wealthy, educated, and attractive romantic prospects, capitalizing on the trust and authority associated with their field.⁶ The perceived authority and expertise associated with a doctor can lead to the scammer's requests being perceived as legitimate. In some cases, doctor impersonations can lend credibility to other scam techniques during collaborative scamming operations with multiple threat actors, such as the offering of fake documentation during hospitalization scams.
 - *Hospitalization scams.* These scams are an extension of impersonating a doctor, whereby the primary focus is faking illnesses and injuries to emotionally manipulate victims. Scammers utilize hospitalization scams to convince victims of their hardship, struggle with medical bills, or inability to sustain basic necessities during a hospital stay. These claims can then be augmented by fraudulent documentation, intended to serve as proof. This forms a basis for the scammer to request large funds frequently and can offer longevity, as there could be expensive treatments and medical complications.
- *Celebrities.* While celebrities are often impersonated for legitimate entertainment purposes, threat actors exploit their high-profile images and public personas to conduct romance scams. Using this technique, scammers create a sense of trust, familiarity, and excitement, often leading victims to believe they are interacting with the legitimate celebrity. Due to celebrities' often-significant, highly public online footprint, attackers are often afforded abundant opportunities to steal, misuse, and manipulate their images.

⁶ [hXXps://consumer.ftc\[.\]gov/articles/scammers-use-fake-emergencies-steal-your-money](https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money)

Resilience – Celebrity Social Media Impersonations

- Be aware of fake page verifications (sometimes referred to as blue check marks). Scammers may use emojis, photoshopped images, or other fake symbols to appear verified.
- Become familiar with a platform's standard verification symbol to easily spot fakes.
- Carefully scrutinize any communication or media received from an alleged high-profile individual.



- *Military Service Members.* Scammers impersonate high-ranking military officials due to their esteem and the wide availability of press coverage associated with them. In these cases, attackers often create social media profiles using the official's photos, educational backgrounds, deployment history, awards, and open source information to legitimize their profiles. Scammers often seek romantic relationships with victims and manipulate them into sending money to allegedly cover the cost of flights home from active warzones and various other illegitimate requests.

Resilience – Military Service Member Impersonations

- Military service members do not have to pay for approved leave or any other passes. Be aware of scammers seeking financial assistance under this premise.
- The majority of the time, high-ranking military officials do not have a professional social media presence, and have a minimal personal online footprint.
- Victims should report these crimes to military criminal investigators or law enforcement entities.⁷



Pig Butchering. This is a calculated and malicious investment scam intended to drain finances from its victims.⁸ This is a relatively new scam tactic that combines elements of online-dating fraud and fake cryptocurrency investment schemes. Threat actors are known to have leveraged scamming manuals on how to conduct pig butchering composed of proven standard operating procedures (SOPs) and also to employ malicious apps to further the scheme—some of which are available on legitimate mobile app stores.⁹

- *Wrong number texts.* A common method of initiating a pig butchering scam is for attackers to send a wrong-number text as a way of establishing initial contact. These texts are seemingly accidental and use the guise of trying to reach an old friend who has changed their phone number. When victims respond, this provides

⁷ [hXXps://www.cid.army\[.\]mil/Submit-a-Tip/](https://www.cid.army.mil/Submit-a-Tip/)

⁸ [hXXps://www.aarp\[.\]org/money/scams-fraud/what-are-pig-butchering-scams/](https://www.aarp[.]org/money/scams-fraud/what-are-pig-butchering-scams/)

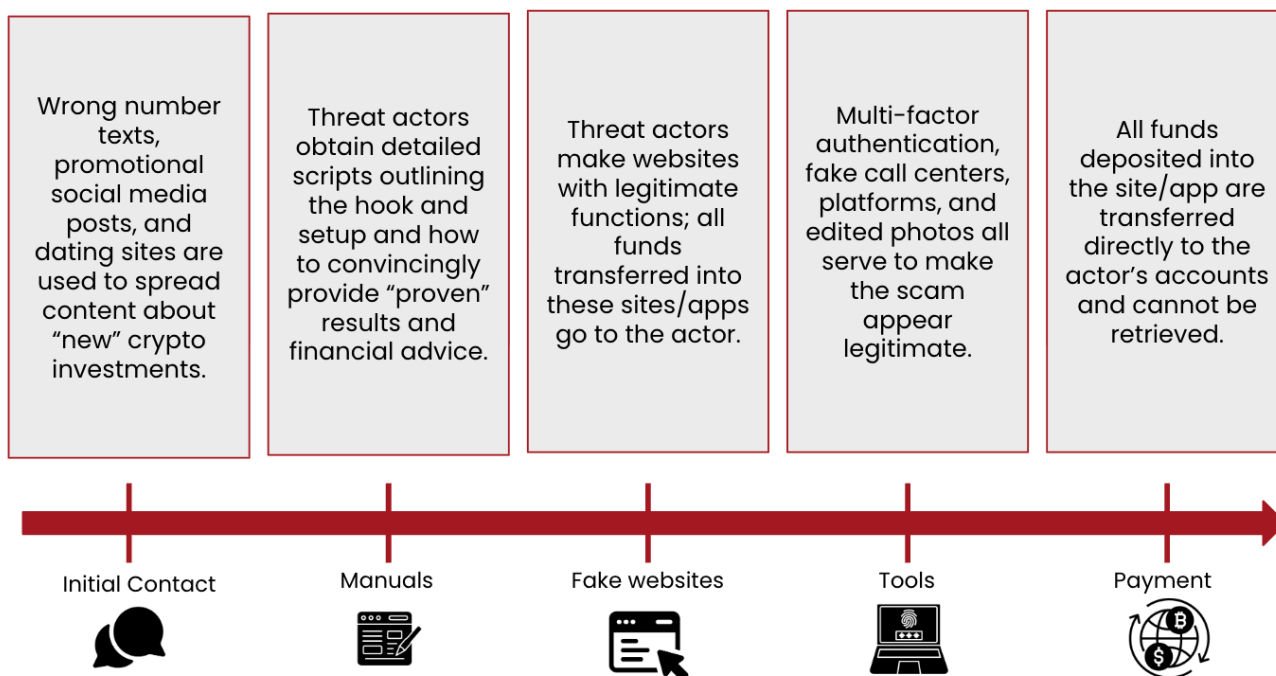
⁹

[hXXps://www.bitdefender\[.\]com/en-us/blog/hotforsecurity/google-sues-crypto-investment-app-makers-over-alleged-massive-pig-butchering-scam](https://www.bitdefender[.]com/en-us/blog/hotforsecurity/google-sues-crypto-investment-app-makers-over-alleged-massive-pig-butchering-scam)

the scammer with an opportunity to lengthen the interaction and later propose the fraudulent cryptocurrency investment scheme.

Pig butchering seeks to introduce a false sense of authenticity while the victim's investments are being deposited directly to the scammer's accounts. Often, victims attempting to withdraw their investments will be notified that a tax bill must first be paid. This is a final attempt by the attacker to extract the victim's funds. Funds conveyed and investments made in this manner are often irretrievable.

Pig butchering can also provide scammers with the opportunity to victimize third parties surrounding an initial victim, such as friends, family, coworkers, and peers. Once a victim has successfully been fooled and believes they are receiving financial returns, they can be encouraged to extend the fabricated opportunity to others. Often, these are individuals perceived as likely to lack a basic understanding of associated technology. However, sophisticated actors are easily able to manipulate tools, results, and websites that can deceive even experienced individuals.



Pig butchering timeline

Source: ZeroFox Intelligence

Sextortion. This is a relatively new form of extortion and sexual exploitation that primarily targets minors. Typically, the threat actor's intent is to solicit and receive child sexual abuse material (CSAM) before blackmailing the victim, and often their parents, promising that the material will be deleted in exchange for payment (often in the form of gift cards).¹⁰ In many cases, the threat actor will either continue extorting the victims or distribute any media obtained, regardless of whether payment is made.

To achieve this, threat actors often adopt online personas of children, studying a victim's interests, friends, and social status before targeting other children through social media accounts. Many schools adopt student-run class accounts intended to provide class updates, which affords threat actors unique access to the personal and school-related digital landscape frequented by potential victims. Fake accounts can then be socially engineered in a manner intended to lower suspicion.

In the creation of a convincing profile, threat actors either use random photos of children or impersonate a real student from the victim's school. In the latter case, the threat actor will use the victim's public following list and that of their class account, mass-following, commenting, and "liking" to interact with every other child from the victim's class or school. This leads to victims assuming that the fake profile belongs to someone that they do not know from their class or to a peer who has made a new account.

Adults are also targeted in sextortion activity, often via traditional phishing methods. In these attacks, threat actors send malicious phishing communications—either en masse or highly targeted toward the victim—claiming to have possession of the victim's login credentials, adult site visitation history, or explicit webcam footage.¹¹ The threat actor can then threaten to publicly distribute this content. As with many other blackmail activities, the threat actor typically does not possess any of the claimed material; instead, they rely on fear and fabricated leverage to intimidate victims.

¹⁰

¹⁰ [hXXps://www.justice\[.\]gov/d9/2023-06/sextortion_crowdsourcing_enticement_and_coercion_2\[.\]pdf](https://www.justice.gov/d9/2023-06/sextortion_crowdsourcing_enticement_and_coercion_2.pdf)

¹¹ [hXXps://www.\[.\]gov\[.\]ukncsc/guidance/sextortion-scams-how-to-protect-yourself](https://www.[.]gov[.]ukncsc/guidance/sextortion-scams-how-to-protect-yourself)

| Artificial Intelligence in Romance Scams

Tools driven by AI technology are rapidly being incorporated into both illicit and legitimate toolsets by malicious actors across the cyber threat landscape. Threat actors conducting various types of romance scam activity are able to enhance and augment their TTPs at various stages of the scam, improving their chances of successful exploitation.¹²

During the victim selection stage of a romance scam, threat actors are able to leverage AI-driven tools to seek a target perceived to be vulnerable. Readily available scraping tools can deliver vast quantities of open-source data from social media platforms, dating websites, and leaked datasets, enabling easier demographic and behavioral analysis. Traditionally and historically, such approaches were not available, leading to an attacker using significantly more resources in target acquisition or selecting a target with less chance of compromise.

During the initial approach stage of a romance scam, AI tools are used in the creation of both inviting profile images and seemingly unique background information used to populate a biography. They can also be used to generate initial messages with a high standard of language and grammar, circumventing any security awareness of traditional phishing red flags that the victim may possess. Highly realistic synthetic media generation tools are able to satisfy demands for voice, location, or video verification, enabling the interaction to continue and offering the attacker more opportunity to appear legitimate.

During relationship development, the attacker often prioritizes building perceived trust. AI chatbots can simulate nuanced conversation and provide detailed responses, mimicking affection, care, and curiosity. Synthetic media tools can also be used to deliver timely proof of claims made relating to the attacker's situation, location, hardships, interests, or day-to-day activities. Techniques such as voice cloning and face swapping can also enable attackers to conduct convincing video calls.

¹² [hXXps://cyberresilience\[.\]com/threatonomics/deepfake-technology-for-live-videos/](https://cyberresilience[.]com/threatonomics/deepfake-technology-for-live-videos/)

When conducting exploitative activity, AI tools can assist in fabricating media to serve as evidence for the need for finances. Falsified photos and videos can be fabricated to depict a hospital stay, debt collector demands, or other adverse situations. Falsified documents can mimic enticing investment opportunities, business proposals, an inheritance inaccessible due to an outstanding tax, or any other written scenario which promises a payout upon the victim's investment.

Resilience – Identifying Synthetic Media

- Look out for visual giveaways, such as skin complexions that are too smooth or wrinkly, unnatural shadows, or inconsistent lighting.
- Listen for speech that is misaligned with lip and overall facial movements, strange background noises, and inconsistent audio quality.
- Consider using open-source deepfake detection tools and reverse image searches to verify suspicious media received.



Threat Actors

An array of different threat actors perceive romance scams as a lucrative, relatively low-risk technique of conducting exploitation. These actors are motivated by a wide range of self-interests, seek different end states, and carry malicious toolkits that vary dramatically in sophistication.

Revenge. Some romance scam activity is conducted by individuals seeking to exert punitive consequences against a target, usually in response to a perceived grievance. In the majority of these cases, the attacker has a personal relationship with the victim. These may be two-way relationships (such as an ex-partner or colleague) or one-way

connections (such as a scorned lover, secret admirer, or cyberstalker). In these cases, the attacker's intent is centered around causing fear, shame, humiliation, or anxiety, and media and information consensually obtained is often used to achieve this.

Financially motivated. Romance scam activity with the intent of obtaining illicit funds is very likely the most widespread motivation. Victim finances are stolen through gift card schemes, wire transfers, cryptocurrency crime, stolen bank information, or the direct payment of bills and services. Both lone individuals and criminal groups operate romance scams with a financial motivation, seeking to profit directly from the exploitation of their victims. These threat actors very likely often run as many scams as they are able to, for as long a period of time as possible, to increase reward. These actors likely engage in subsequent criminal activity needed for both laundering and storage of illicitly gained funds.

Criminal groups. Criminal networks and organizations are a large contributor to the romance scam threat landscape, as these groups often operate with enhanced organization, sophisticated, and proven TTPs. These groups are financially motivated and often commit various other crimes, such as money laundering, human trafficking, identity theft, and other fraudulent activities. The targeting of overseas victims often affords these criminals a relatively permissible legal landscape within which to operate, as they exploit the difficulties encountered by both national and international LE bodies in extradition and prosecution. Many of these groups operate from within the Southeast Asia or Africa regions, where several gangs operate sophisticated scam compounds.

Case Study

The Yahoo Boys are a notable collective that engages heavily in romance scams; they are a loosely connected, primarily West Africa-based criminal entity. A basic online search for "Yahoo Boys" yields numerous results for groups, scam templates, scripts, and fast money-making schemes accessible to any user. Yahoo Boys primarily seek overseas victims, primarily minors located in the United States, Canada, the United Kingdom, Australia, and the Netherlands.

In the 1980s, the Nigerian Letter Scam (or the Advanced Fee Scam) took off, whereby perpetrators convinced often-foreign victims to send money in aid of an alleged Nigerian prince or banker. In the 1990s, this scam evolved to email platforms like Yahoo, which is where the Yahoo Boys moniker originated. As the internet landscape continued evolving and becoming more accessible, the scams evolved as well. The term Yahoo Boy has been prevalent in Nigeria since the late 1990s and was coined to describe Nigerian scammers and their lavish lifestyle. This group is known for flaunting designer fashion, sports cars, and prominent online presences. Over the decades, the influence of Yahoo Boys and scamming enterprises within Nigeria has shaped a subculture amongst Nigerian youth, with the lifestyle becoming emblematic of success within this world of crime.

Numerous notable international LE operations targeting Yahoo Boys perpetrators have been observed in recent years. Often, these are in response to alleged offenses that constitute the sextortion of a minor, many of which lead to severe victim consequences and subsequent public outcry. Some notably large operations have also been successfully targeted, such as the November 2023 indictment of Olamide Shanu and unnamed co-conspirators, who had allegedly received more than USD 2.5 million in Bitcoin transactions amid a large-scale financial sextortion operation.¹³

| Outlook

Romance scams are almost certain to remain a significant threat to both adults and minors, as well as organizations across regions and industries throughout 2025. The threat posed by both low-sophistication individuals motivated by revenge as well as from financially-motivated, semi-organized criminal collectives across the globe is very likely to remain on an upward trajectory as measured by total impact, while there is a roughly even chance that the quantity of incidents will rise.

Threat actors will very likely continue to capitalize upon established techniques to achieve high success rates, and increasing financial payoffs. While impersonation, blackmail, and sextortion will almost certainly persist, new techniques exploiting contemporary social trends and circumventing an ever-growing cyber security

¹³ [hXXps://networkcontagion\[.\]us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf](https://networkcontagion[.]us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf)

awareness are almost certain to emerge. The proliferation of social media platforms and the increasing use of digital technology and internet connectivity by both minors and elderly people is very likely to be seen as a lucrative attack vector exploitable in various types of romance scam and sextortion activity.

Recommendations

- Enable privacy settings on social media accounts to restrict public access to information and photos. Follow the guidance of social media platforms to reduce account exposure.
 - [hXXps://about\[.\]meta\[.\]com/actions/safety/topics/bullying-harassment/stop-sextortion/caregivers](https://about.meta.com/actions/safety/topics/bullying-harassment/stop-sextortion/caregivers)
 - [hXXps://help\[.\]snapchat\[.\]com/hc/en-gb/categories/5685833655188-Safety-and-Security](https://help.snapchat.com/hc/en-gb/categories/5685833655188-Safety-and-Security)
 - [hXXps://help.x\[.\]com/en/safety-and-security](https://help.x.com/en/safety-and-security)
- Be sceptical of connection and message requests received. Look for commonly-used scam tactics before accepting, and report accounts suspected of conducting malicious activity.
- Research all cryptocurrency investment opportunities thoroughly before investing or interacting with users promoting such content.
- Review all social media account terms and conditions for children's accounts, and discuss safety precautions for internet use.
- Maintain open communication with children to encourage them to share unsafe activity or interactions online; educate, spread awareness, and report any incidents.¹⁴
- Protect family members who may be more vulnerable or perceived as low-risk targets, by educating them on how to identify suspicious messages or monetary requests.
- Never share personally identifiable information (PII), personal financial information (PFI), or account login credentials with anyone—especially online.
- Organizations should implement training for employees focusing on awareness of contemporary threats, phishing vigilance, social engineering resilience, and basic cybersecurity hygiene.
- Executives and senior personnel within an organization should ensure that social media profiles are verified to reduce the likelihood of imitation accounts being created.

¹⁴ [hXXps://about.meta\[.\]com/actions/safety/topics/bullying-harassment/stop-sextortion/caregivers](https://about.meta.com/actions/safety/topics/bullying-harassment/stop-sextortion/caregivers)

| Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%