Co-funded by the European Union

FIGHT AGAINST LOVE SCAM

2023-1-DE02-KA210-VET-000151265

Abstract

Fight Against Love Scam (FALS) is a European initiative created to protect and empower adults aged 50+ against online romance fraud. The project brings together partners from Germany, the Netherlands, and Italy to raise awareness and equip adult educators, seniors, and their families with the knowledge and tools to recognize, prevent, and respond to love scams.

Through the creation of a digital guidebook, practical tests, and an online course, FALS promotes online safety, emotional well-being, and active aging. The project also encourages collaboration between educators, social workers, and communities to build stronger support systems around older adults.
By combining education, prevention, and empathy, FALS strives to make the digital world a safer space for everyone.

Project Partners

EUTH WONDERS E.V

IGOR VITALE INTERNATIONAL

ECREC

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Table of Contents

Co-funded by the European Union

A Message from the Project Partners

Dear Reader,

We warmly welcome you to this guidebook, a heartfelt result of our shared commitment across Germany, the Netherlands, and Italy to support and empower one of the most vulnerable segments of our society, older adults navigating the digital world.

Fight Against Love Scam (FALS) was born out of a simple but urgent need: to prevent the emotional and financial harm caused by romance scams, and to equip adult educators, families, and seniors themselves with tools to stay safe online. Too many have been affected in silence and we believe it's time to bring knowledge, care, and community into the spotlight.

This booklet is more than an educational resource; it's a gesture of solidarity and respect. It offers insights, practical guidance, and shared experiences to help recognize warning signs, strengthen digital resilience, and support one another in navigating online relationships.

We hope you find comfort, clarity, and confidence within these pages.

Warm regards,

The FALS Team

EUW (**Germany**)
ECREC (**The Netherlands**)
IVI (**Italy**)

Manual Overview

Content of the manual

The manual contains 3 chapters that formulate the content of the methodology manual:

1. Behind the Mask: Understanding Love Scams
2. Supporting with Care: Good Practices for Educators
3. Digital Defence: Cybersecurity Basics for Beginners
4. Know & Grow: Self-Assessment and Evaluation.

Key elements of the chapters

Chapter 1: An overview of what love scams are, how they happen, and how to recognise and prevent them.

Chapter 2: Practical guidance for adult educators on how to support seniors, recognise psychological vulnerability, and respond to scam incidents.

Chapter 3: Intro to online safety, phishing detection, and platform awareness for non-tech-savvy users.

Chapter 4: A set of short tests to evaluate understanding of love scams, emotional awareness, and digital safety. Includes infographic-based analysis.

About FALS

Co-funded by
the European Union

Introduction

The digital world has opened up countless opportunities for connection but with those opportunities come new forms of risk. One of the most emotionally damaging threats faced by older adults today is the “love scam,” a form of online fraud that preys on vulnerability and trust.

The Fight Against Love Scam (FALS) project was launched as a European collaboration between partners in Germany, the Netherlands, and Italy with a shared mission: to protect, inform, and empower individuals aged 50 and above, and those who support them. Through this manual, we aim to equip adult educators with the knowledge and tools needed to identify the signs of online romance scams, offer psychological and social support, and teach basic cybersecurity practices in an accessible and empathetic way.

This guide is not just a manual, it is a call to action. By raising awareness and building capacity among educators and caregivers, we can prevent harm, support recovery, and promote dignity and safety in digital spaces for older adults.

We invite you to explore the chapters ahead, each designed to help you become a stronger advocate, protector, and educator in the fight against love scams.

FALS OBJECTIVES

- **Raise Awareness among older adults (50+)** about the risks and tactics of online romance scams, helping them to recognize red flags and avoid emotional and financial harm.
- **Empower Adult Educators** by equipping them with knowledge, tools, and methodologies to support seniors in digital spaces and detect early signs of psychological vulnerability.
- **Support Families and Caregivers** by providing practical guidance to help them identify warning signs, communicate with their loved ones, and respond appropriately to suspected scams.
- Promote Digital Safety by introducing cybersecurity basics that help seniors navigate online platforms more securely and avoid high-risk interactions.
- **Build a Sustainable Educational Tool** through the development of a comprehensive guidebook, self-assessment tests, and a digital video course that can be used by adult education centers, social workers, and family members across Europe.
- **Encourage Active Aging and Resilience** by fostering digital literacy and emotional well-being, enabling older adults to remain engaged, independent, and safe in their online interactions.

Target Group

01 Primary Target Group: Older Adults (50+ years old):

- The main beneficiaries of the project. This group is increasingly active online but often lacks the digital literacy or emotional support to protect themselves from romance scams and related online fraud. The project specifically aims to strengthen their awareness, resilience, and digital safety.

02 Adult Educators and Trainers

- Professionals working in adult education, community centers, or digital literacy programs who will be trained and equipped with tools to identify, prevent, and address love scams among older learners.

03 Family Members and Caregivers

- Relatives and close contacts of seniors, who are often the first to notice behavioral changes and can offer emotional or logistical support in case of a suspected scam.

04 Healthcare, Social Workers, Community Centers, NGOs, and Adult Education Institutions

- Professionals who may work with seniors experiencing psychological distress due to scams or vulnerability to online manipulation.
- Entities that can adopt the handbook, training resources, and digital course developed by FALS into their educational or awareness-raising activities.

Behind the Mask: Understanding Love Scams

Co-funded by
the European Union

Agnese Federica Gobbi

Agnese Federica Gobbi, born in Slovenia, holds a bachelor's degree in psychological sciences and techniques and is currently pursuing a master's degree in psychology at the University Guglielmo Marconi in Rome. Since 2022, she has been a valued collaborator at Igor Vitale International s.r.l, where she specializes in audio-video production, photography, content writing, and web page creation. Agnese has actively contributed to more than 15 projects across diverse fields such as hospitality, crafts, ecology, and psychology. Her work has taken her to various parts of Europe, the Overseas Caribbean territories, French Polynesia, Greenland, South Pacific, and regions of Southern and Eastern Asia, showcasing her global perspective and multidisciplinary expertise.

1 INTRODUCTION TO LOVE SCAM

The love scam, also known as the romance scam, represents a form of online fraud in which scammers exploit emotional connections to deceive individuals for financial gain. Rooted in historical deception tactics, such as the “Spanish prisoner” scam of the 16th century, modern romance scams continue to manipulate victims by constructing false relationships and idealized personas. The proliferation of digital communication platforms has provided fertile ground for these schemes, allowing scammers to operate anonymously and expand their reach globally. Victims are often lured by carefully crafted profiles and convincing stories, leading to significant emotional and financial harm (Cemmi, n.d.; Coluccia et al., 2020; Europol, 2023). In recent years, love scams have become more sophisticated, with scammers employing various psychological tactics to establish control over victims and ensure compliance. Understanding the mechanisms and impacts of love scams, as well as recognizing early warning signs, is essential to combating these fraudulent activities.

1.1 What is a love scam

The love scam, known internationally as romance scam, is a type of digital fraud in which scammers manipulate victims to obtain money by leveraging false promises of love via the internet. According to an Italian Supreme Court ruling (n. 25165/2019), individuals who feign romantic interest solely to gain economic or material benefits are prosecutable under Article 640 of the Italian Penal Code (Coluccia et al., 2020 in Cemmi, n.d.). The widespread use of technology has facilitated the rise and evolution of these scams. A study conducted in Italy found that 3% of the population has fallen victim to romance scams, with a higher incidence among women aged 40 to 60. This group tends to idealize relationships and seek intense emotions, making them more vulnerable. However, victimization can also affect professionally successful individuals, such as managers and educators (Cemmi, n.d.; Commissariato di PS, n.d.). Although primarily carried out on digital platforms today, romance scams have ancient roots. One early example is the "Spanish prisoner scam" of the 16th century, targeting wealthy individuals. In this scheme, the scammer posed as a wrongfully imprisoned Spanish noble with a hidden fortune. Pretending to be in despair, he asked for money for his release, promising a portion of his fortune in return.

To make the scheme more enticing, the scammer would mention a beautiful, unmarried daughter, using romantic and familial appeals to evoke empathy and emotional involvement from his victims (Beek, 2016 in Cunha, n.d.; Gillespie, 2017 in Cunha, n.d.). Analyzing the Spanish prisoner scam provides insight into the foundations of the modern romance scam. Despite the centuries passed, the core of the fraud still relies on emotional manipulation. While methods and technologies have evolved, the scheme fundamentally remains unchanged: the scammer builds a trusting relationship, leveraging promises of love and future life together, inducing the victim to surrender money and assets (Cunha, n.d.). This fraud, among the most ingenious and successful of its time, required coordination between different countries, making it difficult to identify and apprehend the scammers. The collaboration between different jurisdictions and logistical complexity allowed these fraudsters to operate with a certain level of impunity, taking advantage of the limited communication and law enforcement capabilities of the time (Gregory & Nikiforova, 2012 in Cunha, n.d.).

Online frauds, including romance scams, encompass a wide range of illicit activities and rely on digital technologies, including social media and dating apps, to attract and deceive victims. Scammers use digital tools like VPNs and RATs to maintain anonymity and access victims' personal and financial information, aiming to create emotional dependence and continuously demand money (EUROPOL, 2023; Wang, 2022).

Romance scams typically follow a pattern in which the scammer builds an emotional bond with the victim through idealized profiles and tragic stories. This process can last months, leading the victim to develop a strong emotional attachment to the virtual scammer, a dynamic that, beyond financial loss, causes significant psychological harm (Whitty, 2015, 2012, 2018, 2013 in Wang, 2022; Dodge, 2016 in Wang, 2022).

1.2 How to recognise the red flags and prevent it

Romance scams employ sophisticated psychological manipulation tactics to establish emotional and financial control over victims. While romance scams are a relatively modern type of cybercrime, they rely on a well-researched series of tactics aimed at exploiting emotional vulnerabilities for financial gain.

Studies have identified recurring strategies that can help individuals recognize and avoid falling victim to romance scams. One notable framework describing these stages was developed by Whitty (in Cemmi, n.d.), who mapped out how romance scams typically evolve across five phases. These stages, which include profiling, preparation, exploitation, sexual abuse, and revelation, demonstrate the deliberate structure and manipulative power that underpin romance scams.

The initial stage (profiling phase) in a romance scam involves creating a false identity tailored to appeal directly to the target. This process often begins with the scammer gathering personal details from the target's social media profiles and online presence, including hobbies, interests, life goals, and personal values.
Using this information, scammers craft personas designed to mirror the target's personality and aspirations. In doing so, they create an appearance of compatibility and shared interests that quickly endear them to the target. Scammers may also claim to live nearby but are temporarily unable to meet due to work, often citing jobs that require international travel, such as military service or high-level business roles. This false but relatable proximity serves to create a sense of trust and commonality, allowing the scammer to deepen their connection with the victim while establishing a convenient excuse for their absence (Whitty, 2015, in Wang, 2022).

Once initial contact is established, the scammer moves into a phase of emotional deepening (phase of preparation). This goes beyond superficial exchanges; the scammer begins to establish what appears to be an intensely affectionate and invested relationship with the target. They employ tactics commonly associated with "love bombing," wherein the scammer floods the target with compliments, expressions of affection, promises of a future together, and continuous attention. The tactic is highly effective, as it appeals to the human need for connection and belonging. Scammers may send altered photographs, romantic messages, and even poems, all intended to strengthen the emotional bond. Over time, they gather personal insights from the target, identifying any gaps in their emotional life that can be manipulated. For instance, a target who feels undervalued may be flattered by the scammer's admiration, while one who feels lonely may become quickly dependent on the constant attention.

By gradually learning about these emotional vulnerabilities, the scammer positions themselves as the answer to the target's unfulfilled needs, creating a reliance that becomes hard to break. This stage can be lengthy, lasting weeks or even months, during which the scammer builds an emotional bond, ensuring the victim feels invested in the relationship. The end goal is to induce emotional dependency, whereby the target becomes deeply attached to the scammer and increasingly willing to fulfil their requests, believing they are essential to the other person's well-being (Commissariato di PS, n.d.).

The scammer now transitions from building trust to extracting financial resources (exploitation phase). Having already established a strong emotional bond, they begin to test the waters by requesting small favours, often framed as urgent needs. The initial requests might seem trivial or reasonable, such as covering a minor emergency expense, and are presented in a way that aligns with the victim's empathetic response to someone they care about. This technique is known as the "foot in the door," where small requests gradually lead to larger financial demands. Once the scammer has successfully received money, they continue to escalate their requests. In some cases, scammers present an elaborate "crisis," such as a sudden health emergency or being defrauded by a business partner, that requires a significant amount of money. Another tactic, referred to as the "door in the face," involves initially asking for a large, unrealistic sum and then reducing the request to something smaller.

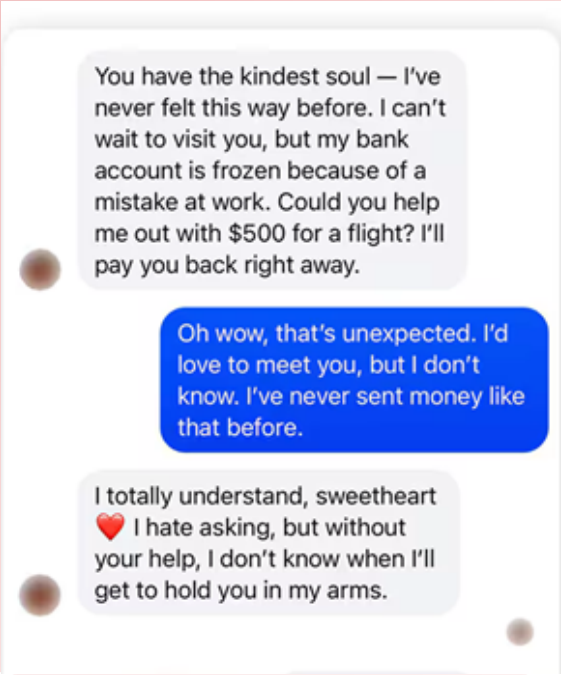
This approach leverages the human tendency to agree to a request after refusing a more demanding one. Scammers may also use ongoing, small requests for everyday expenses, which is common with male victims. Here, the scammer continually requests smaller amounts under the guise of routine needs, such as utility bills or rent, maintaining the illusion of a relationship that will culminate in a real-life meeting (Cemmi, n.d.; Whitty & Buchanan, 2012 in Wang, 2022).

While not present in all cases, some scammers take the manipulation further by introducing a sexual element. In these cases, once a substantial amount of money has been obtained, the scammer pressures the victim to engage in sexual activities via webcam, which are often recorded without the victim's knowledge.

The scammer may then use these recordings to blackmail the victim, threatening to release them unless more money is provided. This tactic inflicts psychological distress and humiliation on the victim, compounding the emotional damage caused by the financial exploitation. It also demonstrates the lengths to which scammers will go to exert control over their victims and maximize financial gain (Whitty & Buchanan, 2012 in Wang, 2022). When the scammer decides they have gained as much as possible from the relationship, they abruptly cut off all contact with the victim, often leaving them in a state of shock and confusion (revelation and abandonment phase). This sudden departure forces the victim to confront the painful reality of the deception. The loss is not only financial but also deeply emotional, as many victims feel as though they have lost a genuine relationship. The aftermath is often accompanied by feelings of shame, humiliation, and betrayal. Victims experience a grieving process similar to losing a loved one, and the psychological impact can be profound, including depression, anxiety, and trust issues. The realization that the relationship was built on manipulation leaves many victims questioning their judgment and self-worth, compounding the emotional toll of the scam (Whitty & Buchanan, 2012 in Wang, 2022).

✦ Examples of a Love Scam Chat Dialogue

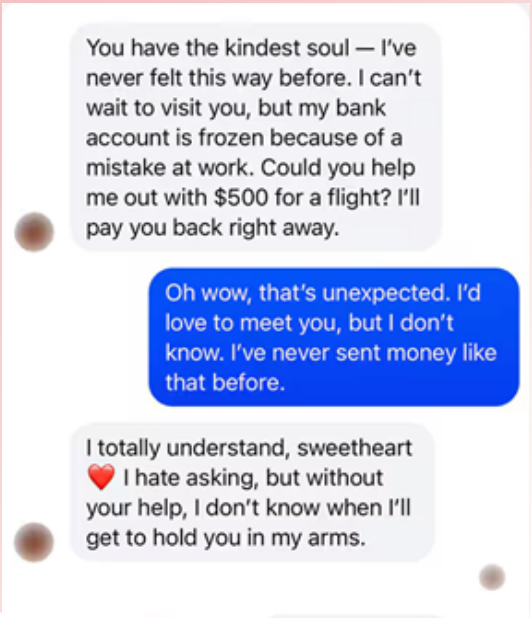
1- Military Scam:



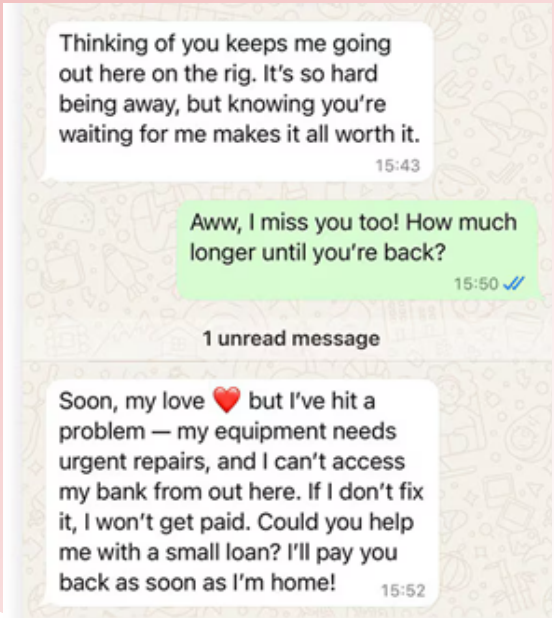
2- Nigerian Scam:

3- Crypto Romance Scam

4- Facebook romance scam

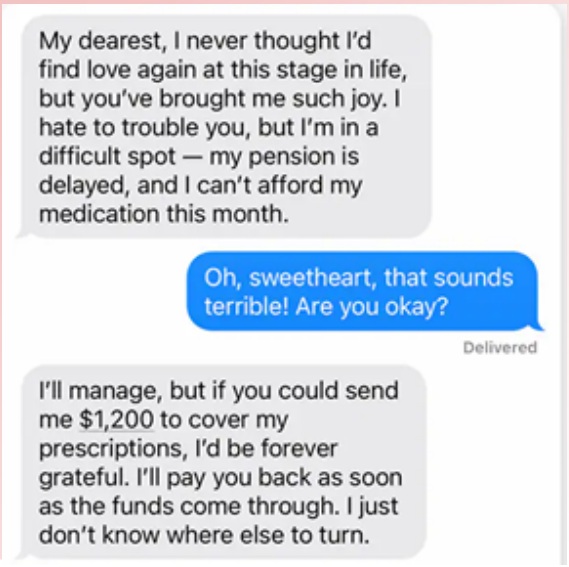


5- Oil rig scam

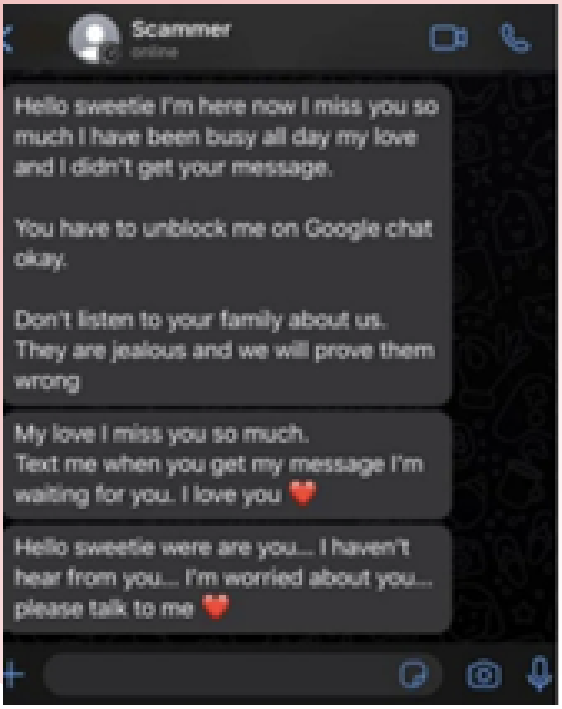


6- Celebrity romance

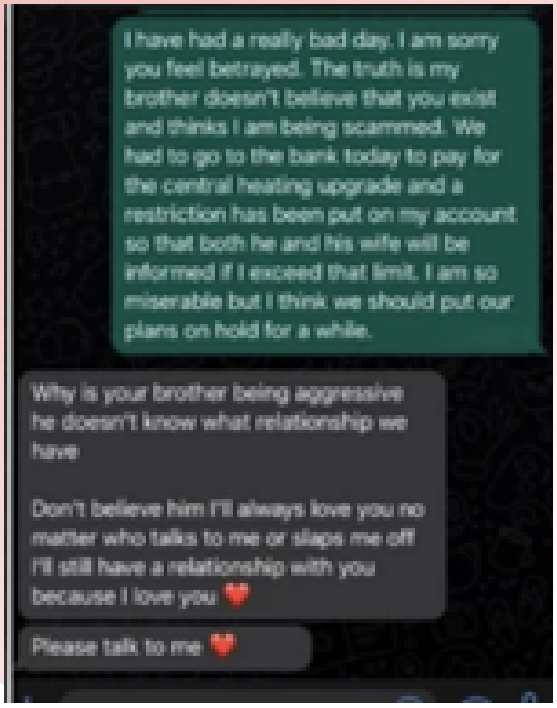
7- Elderly romance scam



8- Example of a scammer



9- Example of a scammer



1.2.1 What is a “sextortion” and how do you recognise it?

Sextortion is a form of sexual extortion, a cybercrime where offenders threaten to distribute intimate images or videos unless the victim complies with their demands (Interpol, 2022; National Crime Agency, 2021 [NCA]; U.S. Immigration and Customs Enforcement [ICE], 2025). In these schemes, perpetrators often use romance or online intimacy to obtain compromising material, later leveraging it for money, sexual favours, or continued exploitation (Wang, 2024).

In regard to love scams, extortion typically emerges after trust has been established online: scammers create false identities on dating sites or social medias, build an emotional connection, and then encourage the sharing of nude images or sexual webcam interactions, sometimes secretly recording them (Kloess et al., 2014). Once obtained, these materials become tools of coercion, with scammers threatening to send them to family, friends, or employers, unless their demands are met (Europol, 2017). In some cases, offenders use the threat of exposure as “implicit blackmail” to maintain control over victims (Whitty & Buchanan, 2012).

Red flags include:

- rapid escalation into sexual conversations or demands (Europol, 2017);
- refusal to engage in normal video calls while insisting on receiving explicit material (Patchin & Hinduja, 2020);
- profiles with stolen or inconsistent photos (Interpol, 2022);
- emotional manipulation or threats of self-harm (Wang, 2024);
- and urging victims to switch quickly from public platforms to private channels (NCA, 2021).

Psychologically, perpetrators use grooming strategies, often using “love bombing” or excessive flattery to lower defences (Coluccia et al., 2020). They may also research victims through social media to intensify threats, making exposure appear imminent (Patchin & Hinduja, 2020). Importantly, sextortion thrives on victims’ shame and silence; research

shows many hesitate to report due to fear of stigma (Cross, 2014; Pietilä & Korhonen, 2024). Recognising the signs early can empower individuals to cut contact and seek professional or law enforcement help.

1.2.2 Case studies on love scam victims

Romance scams have evolved from simple online deceptions into complex criminal networks with global reach, as illustrated by several compelling cases. These examples highlight how romance scams can be both emotionally devastating and financially destructive, targeting vulnerable individuals through emotionally manipulative tactics.

Case study 1

In Italy, a highly organized romance scam network targeted elderly men, primarily in Calabria region. This network was composed of Romanian nationals who employed young women to establish personal, often physical, relationships with their victims. By building a deep emotional bond, these women persuaded the elderly men to transfer significant amounts of money, ostensibly to cover family or health-related emergencies. This case shows how some romance scams extend beyond the online realm, incorporating face-to-face interactions that deepen the scam's impact on the victims. Operating across multiple countries, the network engaged in sophisticated money-laundering practices, distributing the money obtained from victims across various financial channels to avoid detection. This operation generated over one million euros, underscoring the substantial profits that organized romance scams can yield. The multinational scope and structured nature of this scam reveal the challenges authorities face in investigating and prosecuting such cases, especially as these networks often operate across borders (EUROPOL, 2022).

Case study 2

A 53-year-old man, vulnerable after a recent divorce, became a victim of romance fraud when he turned to a dating website to build new connections. He was contacted by a woman who claimed to be from Spain but living in the United States. The woman sent him photos but avoided any real-life or video contact, maintaining communication through phone, Skype, and email. After developing a connection, she began requesting financial assistance, initially citing her inability to afford food and later claiming she needed a passport to visit him. Over time, the victim sent over £15,000 to his supposed partner.

Following police intervention and support from victim services, the man stopped sending money and began receiving emotional and practical assistance. This case illustrates how scammers exploit vulnerable life situations, like divorce, and progress their demands gradually, building trust through consistent but superficial contact (Surrey Police, n.d.).

Case study 3

A 65-year-old widow became a victim of romance fraud after connecting with a man on Facebook who claimed to be an Army officer. Lonely after her husband's passing, she sought companionship and was soon convinced of the man's sincere intentions. The scammer, who only interacted with her through Facebook and phone, claimed he needed money to leave the Army and care for his ill son. The victim, wanting to help, sent £7,500. Shortly afterward, the scammer requested an additional £3,500 to cover medical expenses for his son. However, the bank intervened before the transaction, raising an alert under their banking protocol and preventing further loss. This intervention, along with subsequent police advice, helped the victim understand the situation was a scam. This case highlights the importance of banking protocols and family support systems in protecting vulnerable individuals from scams (Surrey Police, n.d.).

Case study 4

A 66-year-old divorced man living alone became the target of multiple romance scams after joining various online dating platforms. Maintaining contact with several women through email, text, and phone, he was led to believe he was supporting their living expenses, including rent and bills, and even covering flights for visits that never materialized. Over five years, he sent over £100,000 to various scammers. His daughter eventually raised concerns with the police, who intervened. Financial institutions subsequently blocked the man from using money transfer services to prevent further losses. This case exemplifies how prolonged scams can erode financial security and underscores the importance of family involvement and financial monitoring in identifying and stopping such scams (Surrey Police, n.d.).

Case study 5

An investigation into romance scams originating from Nigeria revealed a detailed "playbook" that scammers use to deceive their victims. This playbook provides step by

step guidelines for establishing trust, manipulating emotions, and gradually escalating financial requests. Scammers in Nigeria often target middle-aged or older women who may be single or recently widowed, capitalizing on their potential loneliness and desire for connection. In the early stages, scammers create profiles that appear sophisticated and charming, using flattering photos and engaging in seemingly meaningful conversations. The playbook outlines tactics for building a "whirlwind romance," a strategy meant to replicate the idealized relationships often seen in media. Over time, scammers manipulate the victim into believing in a future together, all the while making increasingly significant financial requests. This playbook highlights the systematic approach these scammers take, and the calculated steps involved in romance scams, emphasizing the professionalized nature of romance fraud as a criminal enterprise (DocumentCloud, n.d.).

Given the persistence of romance scams, certain technological tools are available to help identify fraudulent profiles. Swindlerbuster Face Search, for instance, allows users to perform reverse image searches on photos used in dating profiles. By identifying if an image is connected to multiple names or locations, individuals can better verify the authenticity of online profiles.

1.3 Statistics

The Postal and Communications Police actively monitor the web daily, with specialized personnel overseeing online spaces, especially social media platforms, to prevent and counter criminal behaviours. This specialized division operates a coordinated effort across both national and international levels, leveraging offices throughout the country to manage and investigate incidents related to cybercrime. Among the issues addressed is the "romance scam," or romantic fraud, which saw a staggering increase of 118% in 2021 compared to cases handled in 2020. Although men are generally less affected by this scam, numerous Italian men have been deceived by perpetrators posing as foreign women using social media accounts featuring provocative images, often portraying themselves as models or wealthy heiresses. These scams can result in significant financial losses, with individual cases sometimes amounting to hundreds of thousands of euros. In 2021 alone,

approximately €4.5 million were reported as lost to these scams (Commissariato di Pubblica Sicurezza Online, n.d.). In Europe, romance scams impact between 1% and 3% of the population, with losses demonstrating substantial financial implications across various countries. For instance, Finnish police records from 2020 report 210 incidents, totalling €6.1 million in losses, which surged to €10.4 million by 2023, reflecting the expanding prevalence of these crimes (Pietilä & Korhonen, 2024). The financial impact of romance scams extends across the continent, and the pattern of deception seen in these incidents underscores the importance of public awareness and digital literacy in combatting online fraud.

The platform CybSafe reports that approximately 20% of individuals experience romance scams, with Millennials (18%) and Gen Z (15%) most affected. Despite high victimization rates, only 55% of victims report these scams, and of those who do, 36% reach out to authorities. These statistics highlight both generational differences in vulnerability and reporting behaviors, suggesting a need for targeted preventive strategies and increased support across demographic groups (CybSafe, 2023).

1.4 Victimology of love scam

1.4.1 Psychological consequences of love scam victims

Victimization through cybercrime, such as romance scams, cyberstalking, or fraud, leads to profound psychological impacts that parallel those of similar offline crimes. Victims experience an array of emotional, social, and physiological effects. Research shows that, for instance, victims of cyberbullying suffer similar consequences to traditional bullying, including social anxiety, depression, and a diminished sense of safety (Smith et al., 2008, in Open University, 2024).

Similarly, the distress caused by cyberstalking reflects that of in-person stalking, leading victims to endure high levels of fear, hypervigilance, and stress (Dreßing et al., 2014, in Open University, 2024). Although trolling's effects are less studied, emerging evidence suggests it, too, can contribute to significant psychological harm, indicating a need for

further exploration of its impacts on victims. Romance scams, in particular, have unique and extensive psychological consequences due to the multidimensional nature of their harm. Research shows that romance scam victims experience what Button et al. (2014) call a “double hit,” the financial loss and the emotional devastation that results from the perceived collapse of a genuine relationship. Studies highlight that this emotional betrayal can often eclipse the financial damage, creating profound distress in victims. Button et al. (2014) note that the combination of monetary loss and the emotional betrayal from these scams leads many victims to suffer severe emotional trauma. The work of Whitty and Buchanan (2012; 2016) reinforces this, revealing that victims frequently struggle with shame, guilt, and self-blame, which often deters them from seeking help. Such internalized shame can be amplified by external judgment, as victims are sometimes labeled “naïve” or “gullible” by others (Buchanan & Whitty, 2014, in Open University, 2024).

The psychological impacts of cybercrime victimization are extensive and often lasting. Many victims report experiencing depression, social withdrawal, PTSD-like symptoms, obsessive behaviors, lowered self-esteem, and a deep-seated mistrust of others (Låftman et al., 2013; Sourander et al., 2010; Schneider et al., 2012; Bates, 2017, in Open University, 2024). Victims also frequently report physical symptoms, such as persistent headaches, digestive problems, and sleep disturbances, which further compound their emotional strain and complicate recovery. Coping strategies initially tend toward maladaptive mechanisms, including substance use and avoidance behaviors, before victims can shift toward more positive methods like counseling or participation in advocacy efforts. Yet, recovery is often hindered by societal attitudes, particularly the pervasive issue of victim-blaming. Victim-blaming represents a critical obstacle in the recovery process, especially for cybercrime victims. Victimology research, dating back to Mendelsohn’s early typologies from the 1930s, suggested that victims might play a role in their victimization. However, modern victimology theory generally holds perpetrators accountable, recognizing that factors outside the victim’s control often contribute to their exploitation. Despite this, cybercrime victims frequently face accusations of partial responsibility, often due to deeply ingrained "just-world" beliefs (Lerner, 1980, in Open University, 2024). This belief system suggests that the world operates on a principle of fairness, leading people to

believe that victims must have done something to attract harm. This mindset, often applied to romance scams, implies that victims acted out of greed or gullibility and could have avoided the crime by refraining from online interactions or social media use (Cross, 2015, in Open University, 2024).

This type of victim-blaming can exacerbate the psychological toll on romance scam victims, who already struggle with feelings of betrayal and shame. Many victims report that the most painful aspect of their experience is the judgment and lack of empathy they encounter from family and friends, who may see them as complicit in their victimization. When victim-blaming occurs, it may also reinforce self-blame in the victim, making it difficult for them to seek support or discuss their experiences openly. This lack of support not only hinders emotional healing but can leave victims feeling further isolated and misunderstood, leading to more profound psychological impacts over time (Wang, 2022). Romance scams often lead to profound emotional distress beyond financial loss, leaving victims with feelings of shame, guilt, and social isolation. Many victims may self-blame or feel too embarrassed to report the scam, while some face severe financial consequences, losing life savings or falling into debt. Victims who develop emotional ties with the scammer may experience Stockholm syndrome, feeling sympathy or affection for the perpetrator even after the deception is revealed. This attachment complicates their ability to escape or report the scam (The Debt Advisor, 2023).

1.4.2 Victim profile

Research on the victimology of online romance scams reveals specific demographic and psychological traits that increase vulnerability to such schemes. Studies by Wang (2022) indicate that individuals at a higher risk of falling prey to romance scams tend to be female, middle-aged, and well-educated. Demographic data suggests that 60% of romance scam victims are women, while 40% are men. Among victims, 63% are middle-aged, followed by 21% young adults and 16% elderly individuals. Middle-aged individuals are often targeted due to their financial stability and higher likelihood of using online dating platforms, particularly after life changes such as divorce or the loss of a spouse, which may increase their susceptibility to the promises of companionship presented by scammers.

Personality traits also play a role; individuals with higher levels of trust, impulsivity, and lower self-control are particularly vulnerable. Scammers exploit these characteristics, drawing victims into fabricated romantic relationships through well-crafted narratives that elicit empathy, sympathy, and often a deep emotional attachment (Wang, 2022). The psychological impact of romance scams is profound, often marked by what Button et al. (2014) refer to as a "double hit": financial loss coupled with the emotional devastation of a perceived relationship betrayal.

Victims typically suffer from severe emotional distress, including shame, guilt, and diminished self-esteem. Studies by Whitty and Buchanan (2012, 2016) highlight how these emotional effects can often surpass the distress associated with financial losses, as victims process the betrayal of a relationship they believed to be genuine. Many victims hesitate to seek support or report the crime, fearing criticism or blame from family and friends who may view them as "naïve" or "gullible" (Buchanan & Whitty, 2014 in Open University, 2024). Cross et al. (2016) examined the dynamics of romance scams through the lens of domestic violence theory, exploring how scammers use psychological manipulation to establish control over their victims. According to their findings, romance scam victims often display high levels of trust and vulnerability in online interactions, which makes them more susceptible to emotional manipulation. Scammers build on this trust by presenting a façade of affection, leading the victim to believe in the legitimacy of the relationship. This approach mirrors the tactics of emotional manipulation seen in domestic abuse, where perpetrators create dependence and isolate victims from their support networks. Isolation is a common feature in romance scams, as scammers discourage victims from sharing their relationship details with friends or family. This tactic deepens the victim's emotional involvement and reliance on the scammer, making it increasingly difficult for them to recognize or escape the deception (Cross et al., 2016).

The financial toll on romance scam victims is often severe. Many victims part with substantial savings or sell personal assets to meet the financial demands of scammers. This financial impact, compounded by emotional strain, can lead to a sense of hopelessness and powerlessness. For some, the losses may affect their financial stability for years, adding to the mental health struggles they face. Cross et al. (2016) note that financial exploitation

within these scams can trigger profound feelings of shame and guilt, as victims grapple with the realization of their manipulation. In addition to the financial and emotional toll, romance scam victims report various physical and psychological symptoms associated with trauma. Studies indicate that victims frequently experience symptoms of post-traumatic stress disorder (PTSD), depression, social withdrawal, obsessive behaviors, and an overwhelming sense of mistrust towards others. Physical symptoms, such as headaches, digestive issues, and sleep disturbances, are also common, often exacerbating the emotional toll of the scam. Initially, victims may turn to maladaptive coping strategies, such as substance use or avoidance behaviors, before eventually seeking more constructive support through counseling or advocacy. Yet, recovery is frequently hindered by societal victim-blaming attitudes, which are common in cases of cyber-victimization.

Victim-blaming, a significant barrier to recovery, is rooted in social attitudes and perceptions regarding cybercrime. Early victimology theories, such as Mendelsohn's typologies from the 1930s, posited that victims might play a role in their victimization. Although modern frameworks generally hold perpetrators accountable, cybercrime victims still encounter societal judgment, especially in cases involving romance scams. This judgment is often tied to "just-world" beliefs, which suggest that the world operates on principles of fairness; therefore, victims must have done something to attract harm (Lerner, 1980 in Open University, 2024). Applied to romance scams, this mindset implies that victims could have avoided the scam by staying offline or exercising greater caution, creating a stigma around their experiences (Cross, 2015 in Open University, 2024).

1.4.3 Psychological rehabilitation of the victim of a love scam

Romance scams leave profound psychological and emotional damage. Victims often suffer a "double trauma": financial loss and the collapse of what they believed to be a genuine relationship (Cross, 2014; Cross et al., 2018). Studies show that nearly two-thirds of fraud victims report health or psychological harm that persists long after the scam (Button et al., 2014).

Psychological consequences include acute stress and trauma responses, with some developing PTSD symptoms such as intrusive memories, flashbacks, nightmares, and hyper-vigilance (Coluccia et al., 2020). Depression, shame, and self-blame are common,

with victims often asking how they “could have been so naive” (Whitty, 2018). Many also develop lasting trust issues, doubting their own judgment and struggling to form new relationships (Rege, 2019 in Pietilä & Korhonen, 2024). Victims frequently withdraw socially, embracing feelings of isolation and humiliation (Whitty & Buchanan, 2012). The long road to recovery needs a multi-layered support:

- Trauma-informed counseling, particularly cognitive-behavioral and grief-focused approaches, has shown effectiveness in helping victims reframe their experiences and reduce self-blame (Against Scams, 2024).
- Peer support groups provide safe spaces for survivors to share experiences, validate emotions, and rebuild resilience (AARP, 2021). Online communities also counteract isolation, providing connection and normalisation (AARP, n.d.).
- Understanding the relational and manipulative tactics used by scammers helps survivors shift blame away from themselves and regain self-confidence (Coluccia et al., 2020).
- Social, financial, and community services, ranging from legal advice to digital security training, aid recovery by restoring control and agency (Pietilä & Korhonen, 2024).

Though recovery is gradual, victims often report post-traumatic growth once shame is addressed and supportive networks are in place (Cross et al., 2018; Whitty, 2018).

Supporting with Care: Good Practices for Educators

Co-funded by
the European Union

Salma Alaaelden

Salma is a Project Assistant and Researcher at EUth Wonders e. V. bringing a strong background in economics and over six years of experience in youth work and project management. She has collaborated with organizations worldwide, contributing to initiatives that empower young people and foster intercultural dialogue. Salma contributed to a lot of researches concerning mental health and as a trainer she delivered mental wellbeing workshops through her projects involvements. At EUth Wonders e. V. she plays a key role in the design, coordination, and delivery of Erasmus+ and other international projects, working across the full project cycle ensuring activities are meaningful, inclusive, and aligned with our mission to connect young people across borders and improve their skills and opportunities.

2 GOOD PRACTICES FOR EDUCATORS

2.1 Scope of this chapter

As Romance and love scams targeting older adults are a rapidly growing form of cybercrime in Europe, and lead to a huge social and financial loss and psychological impacts such as social isolation, exploitation of emotional vulnerabilities, and causing financial losses, Educators and youth workers' role becomes crucial in protecting seniors from love-related scams by providing social support, managing psychological vulnerability, and offering clear pathways to these seniors.

According to the importance of the role of youth workers and educators, this comprehensive chapter will provide the necessary information to understand the psychological vulnerabilities that makes victims prone to scamming, the emotional and psychological consequences of love scamming and consequently, this chapter will also equip educators with the knowledge and tools on how to provide social and psychological support to seniors vulnerable to love scams through preventive and responsive measures and to offer useful resources to them in case of the occurrence of a love scam, and to establishing support networks to foster a safe, trusting environment for seniors.

2.1.1 Key objectives and approaches of this chapter:

This chapter focuses on several key objectives aimed at empowering seniors and their support networks to recognize, respond to, and prevent scams. The objectives are:

1. **Identifying psychological, social, and situational vulnerabilities**: Understanding the factors that make seniors particularly vulnerable to scams, including psychological, Social and situational elements, will help in recognizing risk factors and taking preventive actions.
2. **Studying the psychological and emotional impact of love scams on victims**: Analyzing the psychological impacts and mental health problems on victims of love frauds will help us understand and recognize how to support victims after the scam more efficiently as educators.
3. **Real life case studies on love scam situations**: In order to provide a more comprehensive insights on preventive and responding methods to love scams, a few

case studies will be explained and analyzed.

4. **Understanding the important role of youth workers and educators:** This part will explain the different factors that highlight the need of educators in supporting seniors who are prone to love scams.
5. **Providing Guidance for Educators on preventive measures to protect seniors from falling victims to Love Scams**: Identifying the different preventive measures that educators can put in place to ensure that seniors are aware and to save them from potentially falling into love scams.
5. **Providing guidance for educators on how to detect an ongoing scam**: This part will explain how to detect an ongoing scam through behavioural indicators and signs from victims, and how to support the senior victims in such cases.
6. **Providing Step-by-Step Guidance for Responding to Scam Incidents**: Offering a clear, actionable process for seniors and caregivers to follow when they encounter a scam, ensuring they know how to report and handle the situation effectively.
7. **Establishing Long-Term Support Networks:** Creating and strengthening ongoing support systems that can help seniors avoid becoming victims of future scams, promoting education, vigilance, and community connections.
8. **Connecting Educators and Seniors with Essential Resources:** Providing educators, seniors, and their caregivers with the necessary resources and tools for recovery and protection, ensuring they have access to information and support to safeguard against scams.
9. **Practical case studies:** This part will be as a practical exercise with different hypothetical case studies for educators to analyse and explain how they should act in each situation to support senior victims.

These objectives will help seniors stay informed, protected, and resilient against scams, ensuring both immediate and long-term safety.

2.1.2 Approaches

The Educational Focus of this chapter emphasizes a dual approach to protecting seniors from romance scams. First, Preventive Measures will focus on educating older adults and their caregivers about common scam tactics, equipping them with the digital literacy and social support they need to recognize and avoid fraudulent schemes.

Second, Responsive Actions provide clear protocols for intervention and support when a scam does occur, guiding educators through each step—from initial documentation and reporting to emotional and financial recovery resources.

2.2 Recognizing Psychological and social Vulnerability

There is little help and support for senior victims before, throughout, and after the scam process, which not only makes it difficult for senior victims to get timely and professional assistance after experiencing online scams, but also even run the risk of being love scammed again afterward, multiplying the social, psychological, and financial damage.

Before addressing the different measures to prevent or provide support to scammed seniors as educators. And its necessity, it is important to understand first the risk factors that make seniors more susceptible to scams. This is crucial for educators, caregivers, and community leaders because recognizing these factors enables early efficient intervention and provides the opportunity to implement preventive measures before seniors fall victim to fraud.

A variety of psychological, social and situational factors contribute to the vulnerability of older adults, which scammers often exploit. These factors include social isolation, cognitive decline, and emotional need, among others.

✦ **Social Isolation:**

One of the primary factors that increase a senior's susceptibility to scams is social isolation. Many older adults experience a lack of regular social interaction, which can lead to feelings of loneliness and boredom. In some cases, this isolation leads seniors to seek companionship or emotional connection through online platforms. Scammers, aware of this need, often use the guise of online relationships to prey on these individuals, building trust and emotional bonds to manipulate them. Over time, the victim may be persuaded to send money or provide personal information. Combating isolation by encouraging regular social interactions and building supportive community networks is vital in preventing such exploitation.

Cognitive Decline and scam susceptibility:

As people age, they may experience cognitive decline, which includes memory lapses, difficulty processing new information, and a reduced ability to make sound judgments. These cognitive impairments can make it difficult for seniors to recognize red flags associated with scams, such as unsolicited phone calls, phishing emails, or fraudulent investment schemes. Cognitive decline may also diminish a senior's ability to understand the consequences of sharing personal or financial information with strangers. Therefore, it is essential for educators and caregivers to be mindful of a senior's cognitive health and offer strategies for identifying warning signs and avoiding risky situations. Regular mental exercises, routine check-ins, and the use of trusted technology can all help in maintaining cognitive function and preventing scams.

Emotional Need:

Emotional vulnerability is another significant factor that scammers exploit. Seniors may experience a variety of emotional challenges, such as grief, loss of a spouse, or feelings of loneliness. These emotions can lead them to actively seek new relationships or validation, which is an ideal opening for scammers who prey on emotional neediness. Fraudulent individuals may pose as romantic interests, promising affection, companionship, or a sense of belonging. Unfortunately, these scams can result in financial losses, as seniors may be manipulated into sending money or offering other forms of support. Understanding the emotional state of seniors and offering both emotional and social support is key to mitigating these types of scams. Providing access to grief counselling, support groups, and other social resources can help reduce the emotional vulnerability that scammers exploit.

Trusting Nature (gullibility):

Based on multiple studies, people who have a high degree of trust are more likely to be victims of love scams. Many seniors, especially those who have lived through periods of trust and stability, may have a more trusting nature, which can be exploited by scammers. Scammers often play on a senior's desire to be kind and helpful, whether through a supposed charitable cause or a supposed urgent financial need. Seniors may not question the intentions of the individual they are communicating with, making them prime targets for financial fraud. Encouraging a healthy sense of scepticism and advising seniors to always verify requests for money or personal information, even if they come from

seemingly familiar sources, is an important preventative measure.

To sum up, the above are some of the factors that make seniors more prone to scamming. It's worth noting that usually, for a scam to happen, not only one vulnerability exists, there is rather an interplay of psychological, cognitive, and social vulnerabilities that create conditions for exploitation that are severe as what is known as key risk factors that increase the likelihood of being targeted and groomed.

2.3 The psychological impact of love scams on victims

Love scams cause harm beyond financial loss. They often result in deep emotional distress, long-term mental health issues, and social withdrawal. Research consistently identifies this scam type as among the most damaging and profound forms of fraud, particularly for older adults, as victims may continue to experience the psychological effects including shame, insecurity, and trauma up to even a decade after the event.

Below are the different psychological impacts and other impacts the seniors are prone to in case of a love scam occurrence.

✦ **Dual Trauma: Emotional and Financial Loss**

Romance fraud typically comprises what can be described as a "double-hit" which is the emotional betrayal of a perceived intimate relationship, coupled with financial exploitation. These scams often unfold over months, during which the scammer builds a convincing emotional narrative and gains the victim's trust. Consequently, the impact of fraud constitutes not only a financial betrayal but a profound psychological harm where victims experience a profound sense of abandonment, manipulation, and identity confusion, leading to emotional trauma, which is more devastating than the monetary loss.

Empirical findings indicate that financial victims report significantly higher emotional distress than non-financial victims, and that love scam is the type of fraud with the highest emotional toll, and that many of the victims experience emotional abuse, particularly when the grooming was prolonged and involved intimate trust. In these cases, the sudden loss of the "relationship" often leads to symptoms of **adjustment disorder** or **trauma-related conditions**.

Shame and Guilt

After a scam occurs, senior victims frequently blame themselves for being deceived, often internalizing the scam as a personal failure. Shame creates a strong barrier to asking for help, even from their close circle. According to a study that was conducted, many victims avoid telling family or friends, or professionals due to fear of rejection or ridicule. This response can entrench feelings of worthlessness and delay emotional recovery, which is where the educator's role becomes very important to reassure victims, gain their trust and make them feel seen, and to support them to act against the scam.

Depression and Anxiety

Many victims report symptoms of clinical depression, including hopelessness, sleep disturbances, and low energy. Anxiety often co-occurs, especially in relation to finances, privacy, or public exposure. These effects are heightened when the victim has pre-existing emotional vulnerabilities such as grief or loneliness. These symptoms are not temporary as studies indicate long-term psychological damage and increased need for psychosocial support.

Social Withdrawal

After disclosure, senior victims may isolate themselves from peers and community out of embarrassment. Some cut ties with individuals who questioned the relationship or offered warnings when they knew about the fake 'relationship'. This isolation and loss of trust extends to both personal and institutional relationships, contributing to deeper loneliness and re-victimisation risk.

Emotional Attachment and Grief

Victims often form real psychological bonds with the scammer's fabricated persona according to the relationship they have built with them online prior to the scam. When the deception is revealed, many experience grief comparable to the loss of a romantic partner, where victims describe the scammer as their "ideal partner" or "emotional support"—even if the relationship was entirely online. Some victims report a sense of bereavement more intense than the actual financial loss. This is due to the love bombing, false promises of marriage, and constant emotional reinforcement used during the grooming phase.

Loss of Self-Worth and Confidence

Many victims report a diminished sense of personal competence and dignity after the scam. The betrayal often undermines their confidence in decision-making and increases dependence on others. This disempowerment can lead to long-term emotional fragility and reluctance to engage in new relationships or learning opportunities, as well as raising doubts about their identity and social roles.

Fear of Judgment and Disclosure Avoidance

Due to societal stigma, victims are often reluctant to report the scam or seek emotional support. Those who do disclose frequently report unsupportive reactions, which further reinforce guilt and shame. These unsupportive responses lead to further isolation, which contributes to underreporting and decreases their access to support services, making educator sensitivity and role very essential to form a non-judgmental environment promoting disclosure and early intervention.

Re-Victimisation Risk

Victims who fail to recognize or accept the scam, especially those who ignore warnings due to their trusting nature, are at higher risk of being targeted again. This repeated victimisation is linked to emotional denial and the continued belief that the scammer's intention was sincere.

This is even worsened when victims disregard third-party warnings, that's why, Educators must be equipped to gently confront these beliefs while maintaining trust and support.

Physical and Mental Health Decline

In severe cases, psychological stress manifests physically, with victims reporting headaches, sleep disorders, panic attacks, or exacerbation of chronic illnesses. Some experience suicidal ideation, especially for those who are not in a supportive environments, and are faced by shame and guilt from their close circles, and have chosen to be self isolated.

Financial Harm and Dependency

Victims of love scam Reported financial losses that ranged from €50 to over €800,000,

with median losses between €1,000–€10,000 per case. Due to this, many victims suffer long-term economic instability, reduced access to basic needs, and in some cases, become reliant on family or public welfare. Some even lose homes, pension savings, or inheritances, which can permanently change their quality of life.

✦ Long-Term Psychological Effects

Long after the love scam, it was evident that victims may continue to experience ongoing grief and betrayal trauma, avoidance of online communication, distrust in others, impaired interpersonal relationships, and persistent financial and emotional insecurity, low self-esteem, and anxiety up to ten years post-incident.

2.4 Real life case studies on love scam situations:

After understanding the impact of the love scam and the behavioural and social vulnerabilities of senior victims who have potential to be love scammed, this section will mention a few real case studies, to reveal not only the tactics employed by scammers but also the emotional, financial, and psychological toll on victims. These narratives serve as critical learning tools for educators by illustrating how scam dynamics unfold, to spot red flags in real contexts, and highlighting the complex interplay between vulnerability, trust, and deception. The following case studies are grounded in documented incidents from Europe and Australia, with emphasis on their relevance to the behavioral, emotional, and systemic themes discussed in previous sections.

2.4.1 Case Study 1: The French Victim of a Celebrity Impersonation Scam

One of the most widely publicized cases of romance fraud in recent years involved a 53-year-old French woman, Anne, who was scammed with approximately €830,000 by a scammer who pretended to be the actor Brad Pitt. According to news reports and interviews conducted by Euronews and Le Monde, the scam began with Anne being contacted through social media by an individual claiming to be Pitt's mother. This introduction escalated to direct online communication with a fake "Brad Pitt," bolstered by AI-generated photos, fake charity events, and hospital images.

Over the course of more than a year, the relationship deepened, Anne became socially isolated and increasingly distrustful of friends and family who questioned the legitimacy of

the romance, and she transferred money to support what she believed were urgent financial needs linked to medical bills and frozen bank accounts during Pitt's divorce. The scam leveraged both emotional manipulation and technological deception, including the use of AI images and simulated video chats.

After recognizing being scammed, Anna suffered from severe psychological feelings of humiliation, emotional violation, and depression. After the scam was exposed publicly, she endured cyberbullying and ridicule, exacerbating her mental health decline.

2.4.2 Case Study 1: The French Victim of a Celebrity Impersonation Scam

In 2024, Spanish authorities uncovered a transnational scammer also pretending to be Brad Pitt responsible for scamming multiple old women through social media targeted based on psychological profiling.

In this case, the scammer created false personas, complete with convincing narratives of romantic interest and business ventures. Victims were persuaded to invest in fictional film projects or humanitarian efforts supposedly led by Pitt. Collectively, the women were defrauded of over €325,000. Investigators traced the funds through a complex laundering network involving multiple "mule" accounts. Authorities seized a range of digital equipment, documents, and mobile devices used to construct and maintain the deception.

This case illustrates two key educational insights. First, love scams increasingly involve organized criminal networks with transnational reach and digital capabilities. Second, victims often possess a deep emotional commitment to the fabricated relationship, which can impair judgment even in the face of growing suspicion. This reinforces the need for educators to address both cognitive and emotional dimensions in scam prevention programming.

2.4.3 Case Study 3: Veronica Watson and the Consequences of Trust

Veronica Watson, a 59-year-old Australian grandmother, became an international case after being arrested in Brazil for unknowingly smuggling cocaine in 2013. The deception began with a man she met online who claimed to be in need of help delivering documents for an investment. After months of grooming and gaining her trust, he convinced her to

carry a suitcase to Brazil, which contained 5 kg of cocaine. Veronica was then arrested at São Paulo International Airport and spent over two years in prison before being acquitted. The court recognized that she had been a victim of fraud. However, the psychological toll was irreparable, including ongoing anxiety, social stigma, and a loss of trust in her ability.

This case underscores the intersection between romance scams and other forms of criminal exploitation, including drug trafficking and money laundering. It also illustrates how grooming can lead victims not just to financial loss but to life-altering legal consequences. From an educational perspective, it reveals the importance of teaching older adults about not just financial scams, but also "romance and love-based recruitment" into criminal activity.

2.4.4 Case Study 4: Love scam case of Annette Ford

Annette Ford, a 57-year-old woman from Perth, Australia, was love-scammed twice on separate dating platforms. In total, she lost approximately $780,000—her entire life savings. The scams occurred following her divorce, during a period of emotional vulnerability. In both cases, the men she met online professed rapid affection and love bombing, and then, they claimed to be professionals facing temporary financial setbacks due to overseas complications.

Annette sold her home, emptied her pension account, and borrowed money to send to her scammers. She became estranged from her family, who disagreed with her decisions. Following the scam, Annette became homeless and dependent on government support. The psychological aftermath included depression, insomnia, and panic attacks.

Her case includes long-term consequences including economic disempowerment, social isolation, and severe psychological distress. It also demonstrates how prior trauma from divorce can interact with scam exposure to exacerbate emotional vulnerability. For educators, this highlights the need for trauma-informed prevention strategies that are attuned to the layered contexts in which scams occur.

2.4.5 Northern Ireland Man Defrauded of Over £200,000

Another case includes a man from Northern Ireland who also lost more than £200,000 after engaging in a supposed romantic relationship that began on a dating app and continued from 2020 to 2025.

He believed he was in a relationship with a woman he met online, and over two years transferred large amounts of money in response to urgent-sounding requests: legal fees linked to a relative's will; medical bills from a car crash; and a manipulated fake online banking link.

This scam exploited both emotional dependency and technological manipulation. The victim reported that this scam was huge that it almost destroyed his life and left him emotionally and financially devastated. He eventually contacted the Police Service of Northern Ireland (PSNI), which assisted in recovering the funds.

2.4.6 Wrexham Man Scammed Out of £25,000

Moreover, In early 2024, a 65-year-old man from Wrexham, the United Kingdom, was defrauded of approximately £25,000 after joining an online dating site in March 2023 as a result of experiencing a period of loneliness and family estrangement. Accordingly, he engaged with a person via the dating site who moved the conversation to WhatsApp, and was contacting him daily.

Soon after, The scammer requested funds for a deposit to buy a home together and redirected the victim to send money, Apple gift vouchers, jewellery and an iPhone through multiple addresses.

This continued until w January 2021, when the man reported the person to the police. He was deeply impacted as the emotional promise of a "shared future" played a central role in his engagement and loss. He was offered with victim's support calls to move on from the situation.

2.4.7 Conclusions of the above case studies and Educational Implications

These case studies reveal both the diversity of scam tactics and the common emotional

and cognitive patterns that scammers exploit. It can be concluded that although victims span multiple socioeconomic backgrounds and countries, they are unified by psychological themes such as grief, isolation, and idealized romantic narratives. That's where the rule of educators and youth workers comes in, as they must recognize the depth of emotional attachment victims develop, the sophistication of scammer tactics, and the complexity of post-victimization recovery, which includes not only financial damage but also mental health deterioration, and social stigma.

2.5 Real life case studies on love scam situations:

According to the previously explained information on the psychological vulnerabilities of the victims, the impacts, and the insights from the above real life case studies, it becomes clearer that this emerging and fast paced threat of love scams among older adults calls for a coordinated and proactive approach. As frontline actors within community, educational, and social infrastructures, educators and youth workers play a central role as professionals uniquely positioned to identify early warning signs, implement preventive frameworks, and facilitate recovery when victimization occurs. Therefore, due to this important roles, it is important to understand more clearly why educators and youth workers must be involved, and not only the legal authorities or the community.

2.5.1 Educators as gatekeeper of scam awareness and scam prevention

Educators working with older adults, particularly in community centers, and adult education programs, have a great ability to observe early indicators of scam involvement. They are often the first consistent point of contact for older adults outside of family structures due to their ability to objectively observe behavioral shifts, initiate non-threatening conversations, and provide structured learning environments that support early detection.

According to a research study, it was explained that older adults are more likely to disclose scam experiences to educators than to authorities or family, particularly when this **non-judgmental, supportive relationship** exists. This trust places educators in a prime position to initiate preventive conversations, refer to appropriate services, and normalize discussions around scam experiences.

Moreover, according to experimental studies, it was found out that educational activities such as anti-scam games and workshops significantly enhances seniors' scam awareness, reduces susceptibility, and increases self-efficacy in identifying scam tactics, as well as their digital literacy, reducing their dependence on fake online interactions. Also, this educational strategy is considered as the most effective early intervention strategy in financial exploitation. Moreover, educators can function as cognitive scaffolds especially for individuals experiencing early-stage cognitive decline by reinforcing memory, judgment, and critical thinking through routine engagement. These highlight the capacity of educational formats and educators to influence both behavior and mindset in older learners.

2.5.2 Youth Workers as Bridges to Digital Safety and Empathy

Youth workers are critical in fostering intergenerational learning. Older adults frequently lack digital literacy, a key risk factor in love scams. Through mentorship, educators can teach older adults how to recognize fake profiles, report suspicious messages, and manage online privacy settings. Importantly, this exchange also builds emotional resilience through social inclusion and shared purpose—both of which reduce scam susceptibility.

Research also emphasized that preventive efforts must include educational curricula tailored to the vulnerabilities of older populations. This includes the importance of training educators to manage not just informational deficits, but also emotional trauma and cognitive dissonance associated with scam exposure.

2.5.3 Professional Trust and Systemic Access

Educators often hold a position of trust that can encourage victims to disclose sensitive information they may withhold from family or authorities without feeling ashamed or guilty. This places educators in a powerful position after establishing a safe network to guide victims toward reporting pathways, collaborate with law enforcement and legal advocates, and engage support services for mental health and financial recovery.

The educators also have institutional reach through partnerships with libraries, health centers, churches, and senior club networks that can be mobilized for reaching senior citizens and supporting them in such scams through preventive and reactive measures.

2.5.4 Youth Workers as Agents of Intergenerational Empowerment

Youth workers are often overlooked in discussions on elder protection, yet their role is foundational to promoting digital safety and social connection. Youth workers primarily as educators focused on fostering growth and change. This aligns closely with the needs of older adults navigating the unfamiliar online relationships. It was also studied that Intergenerational programs that pair older adults with younger digital mentors have shown promising results in increasing scam detection rates, improving confidence with online tools, and reducing social isolation, which is one of the most potent risk factors for romance scams, as youth workers facilitate these engagements while modeling healthy digital boundaries and critical evaluation of online identities.

2.5.5 Importance of Training and Structural Support

Educators and youth workers are equipped with tools and training that are beneficial in supporting seniors appropriately. This includes:

- Knowledge on scam typologies, grooming tactics, and behavioral cues
- Access to checklists, digital hygiene guides, and referral templates
- Partnerships with law enforcement, mental health providers, and elder financial protection agencies.
- Tools for anonymous reporting and referral pathway.

Based on the above elements, it is evident that in our fast paced word, the educators' role in supporting victims or potential victims in love and romance scams is not only important, but also required, as they have a great impact in applying the different preventive measures, and reactive measures as will be explained further in this chapter.

2.6 Preventive Measures to Protect Seniors from Scammers

To effectively safeguard seniors from possible love scams, it is essential to implement preventive measures that lower the probability of falling into love scams. By providing seniors with the tools and knowledge they need to recognize and avoid scams, as well as fostering a supportive social environment, and improving the victims skills, we can significantly reduce their risk of becoming victims. These measures include building digital literacy and fostering social connections, both of which play critical roles in helping seniors navigate a world that increasingly relies on technology and personal networks.

2.6.1 Digital Literacy Awareness

One of the most important preventive measures for seniors is improving their digital literacy. As technology advances, scammers are constantly adapting their methods to creating roleplays with different scenarios similar to real life, where educators can notice the senior's detection of fake profiles, privacy settings understanding, noticing red flag in online scenarios, and doing reverse images search, and then reflect with them through engaging discussions. Putting the seniors in real life similar situations will help them apply their learning into the real world.

Workshops on Common Scam Tactics:

Providing targeted workshops is an effective way to educate seniors on the most common online scams they may encounter. These workshops should cover the basics of identifying phishing emails, fake profiles on social media or dating sites, AI, and other scams like fake tech support calls. Educators should focus on providing practical examples of these tactics, showing how scammers often use urgent language, promises of rewards, or emotional appeals to manipulate their targets. Educators also should focus on using AI, and how to compare or conclude pictures or texts that are produced by AI tools. The goal of these workshops is to equip seniors with the ability to recognize warning signs and feel confident in their ability to identify potential scams.

Hands-On Training:

Digital literacy extends beyond just understanding what scams are—it's about giving seniors the skills to use technology safely. Hands-on training sessions can teach seniors how to safely use social media, including adjusting privacy settings, verifying identities of people they meet online, recognizing suspicious links or requests for personal information, and seeing the common conversation scripts often used by scammers. For example, they can learn how to spot a phishing email by checking the sender's address, looking for spelling mistakes, or identifying suspicious attachments. Educators can also teach them how to use secure websites (with "https://" in the URL) and how to avoid downloading files from untrusted sources. Additionally, seniors should be instructed on how to report suspicious activity, whether it's a fraudulent email, a scam phone call, or a questionable online profile. To make these training more effective, it is advisable for educators to do exercises and application activities as a part of the training such as creating roleplays with different scenarios similar to real life, where educators can notice

the senior's detection of fake profiles, privacy settings understanding, noticing red flag in online scenarios, and doing reverse images search, and then reflect with them through engaging discussions. Putting the seniors in real life similar situations will help them apply their learning into the real world.

✦ **Community Engagement sessions:**

Awareness sessions should also be offered to provide guidance on the roles of law enforcement, banks and financial security procedures, cybersecurity, and how to act in case of occurrence of a love scam, and procedures. Experts should also be invited to these regular awareness sessions. Moreover, templates to reporting for the different entries should be shared. This all can be included as well in printed handouts and visual aids, to act as a reminder, and to provide reassurance of the senior's next steps in case of scams.

2.6.2 Fostering Social Connection

Another critical preventive measure is fostering social connections. Many scams prey on vulnerable seniors who feel isolated or lonely. Building a sense of community and encouraging social interaction not only helps seniors stay connected but also provides them with the support and resources they need to recognize when something isn't right. This could be done through group discussions, peer support meetings, and buddy systems.

A. Group activities and buddy system

✦ **Group Activities:**

Encouraging seniors to participate in group activities can significantly reduce feelings of isolation, which often lead to vulnerability. Peer-to-peer clubs, hobby circles, and virtual meet-ups are excellent ways to bring seniors together to share common interests and build meaningful relationships. By interacting regularly with others, seniors are less likely to be swayed by scammers seeking to exploit their emotional or social needs. Group activities also provide a safe space for individuals to discuss any suspicious encounters, receive advice from peers, and stay informed about potential scams circulating in the community. For example, a book club or crafting group can be a valuable way to engage seniors in a social environment, promoting both mental stimulation and social well-being.

✦ **Buddy Systems:**

Another effective way to foster social connection and reduce isolation is through the implementation of buddy systems. Pairing seniors together for regular check-ins, sharing experiences, and offering mutual support helps create a sense of camaraderie. When seniors feel more connected to others, they are less likely to fall prey to scams because they have a trusted person to consult when they encounter suspicious situations. A buddy system also provides a way for seniors to stay informed about potential scams, as they can exchange information about recent scams or warning signs they've encountered. Furthermore, the emotional support of a buddy can make seniors feel more secure, reducing the likelihood of them seeking companionship from potentially fraudulent sources.

B. Expanding Social and Emotional Support

In addition to group activities and buddy systems, fostering a wider network of support is essential. Local community centers, senior organizations, and online groups focused on specific interests can help seniors maintain active social lives, reducing the chance of them becoming isolated or emotionally vulnerable. When seniors have a strong social network, they are better equipped to handle situations where they may feel manipulated or pressured, as they can rely on the guidance of trusted friends or family.

Furthermore, providing emotional support for seniors who are grieving, experiencing loneliness, or struggling with other emotional challenges can help prevent scammers from exploiting these vulnerabilities. Offering grief counseling services, therapy groups, and mentorship programs can all be integral in helping seniors manage their emotional well-being, making them less likely to be targeted by scammers looking for an easy mark.

By combining efforts to build digital literacy with strategies to foster social connections, seniors can become more resilient to scams and fraud. Educators, caregivers, and community leaders play a vital role in implementing these preventive measures. Whether through workshops that teach digital safety or through social programs that reduce isolation, these initiatives help seniors maintain their independence and security in a world that increasingly relies on technology and social interactions. Together, these preventive measures create a solid foundation for safeguarding seniors against the ever-growing threat of scams.

2.7 Stopping love scam in early stages based on Behavioral indicators of getting scammed:

After learning the measures that educators can put in place in order to prevent seniors from falling into scams in the future, it's also worth reflecting on the measures that educators should put in place in case of noticing an ongoing love scams on the senior victims. In order to tackle this, the behavioural indicators, some of which were in the above real life case studies, will be mentioned to support educators, youth workers, and caregivers in the early detection of love scams and then, some assessment tools, and measures will be mentioned in order for educators to be informed how to act once a love scam ongoing case is spotted.

2.7.1 Behavioral Warning Signs of senior victims

Preventing harm from romance scams relies not only on broad awareness but on the early identification of behavioural and emotional red flags and signs that indicate an individual may be entering the love scam process. Numerous studies confirm that romance scams typically follow a structured progression from initial contact, to emotional grooming, to financial solicitation, and ultimately social isolation, and each of these phases is marked by specific changes in behaviour, which, when interpreted correctly, can signal the need for timely and targeted intervention. These signed and red flags include the below:

- **Secrecy surrounding new online relationships:**

Victims often hide their communication with the scammer out of fear of judgment or perceived betrayal of their online "partner." This aligns with findings from research studies that noted that victims deliberately avoid disclosure, particularly when emotionally invested.

- **Sudden excessive phone or internet use:**

Victims tend to engage compulsively in digital communication, often appearing emotionally dependent on messaging apps or video chats.

- **Social withdrawal:**

As grooming intensifies, victims may begin avoiding community events, peer gatherings,

and even family interactions. They might also get defensive about online activity. A research study found that scammers thrive on isolating targets from competing sources of influence.

- **Heightened emotional states:**

Victims may experience feelings between euphoria (when they receive messages from the scammer) and anxiety or sadness (when the scammer is absent or requesting money). Also, they may face sudden mood, or behavioural changes. These affective fluctuations should not be dismissed as general mood instability, but rather evaluated in the context of new social attachments.

- **Unexplained financial activity:**

Educators and family members may notice ATM withdrawals, sudden wire transfers, or requests for help with international banking. One of the research studies explains that reduced cognitive monitoring and financial numeracy often precede such transactions.

2.7.2. Educator's role in detecting an ongoing scam and supporting the seniors

Educators and youth workers are uniquely placed to detect these early indicators. Unlike family members who may lack objective insight into the individual's emotional state, educators are often embedded in structured group settings where they can observe changes over time objectively. For example, seniors who become unusually enthusiastic about a new online acquaintance, frequently mention an idealized relationship, or begin withdrawing from community events as mentioned above.

The educators should have a blend of observation and to distinguish behaviors from general aging or mood fluctuation. Educators may utilize brief, non-invasive screening tools in group settings or one-on-one conversations. In case of any doubts, educators can initiate one to one conversation through asking neutral, open-ended questions that avoid confrontation and shame such as, "Have you felt safe and respected in your online interactions?" or "Have you noticed any unusual requests or conversations online?", ""Have you met someone new online recently?" or "Has anyone asked you for a financial

favour or to keep something secret?". These questions allow older adults to reflect without defensiveness. In this way, educators foster an atmosphere of trust rather than intrusion., In case it is noticed that the senior victim is not very responsive to the questions, simulated scenario discussions through using anonymized stories or hypothetical characters can be used where educators can explore and inform the risks without confronting the individual directly. This method has been shown to reduce shame and increase reflective thinking.

Once behavioral signs are noticed and information is confirmed that seniors are enduring a scam, educators should adopt a soft triage model: engage, educate, and evaluate. The engagement phase focuses on listening and showing concern, while affirming that it is a non-judgemental environment. The education phase involves providing general information about online love scams ideally through neutral formats like pamphlets, videos, or anonymized case discussions. This indirect method allows individuals to identify with the patterns described without feeling accused. The evaluation phase, often done informally, involves assessing whether the individual is open to further discussion or support, or whether external referral may be required.

Moreover, Indirect group-based approaches further enhance early detection. When scam education is integrated into regular programming, older adults are more likely to recognize manipulation in their own or others' experiences, and also will feel seen and that they are not alone, making them feel less ashamed, and more open for help. Moreover, having group based settings, and trying to re-engage them in the different activities will help them feel more engaged again with the community, and less engaged with the scammer, leading to finally leaving the scammer.

In summary, educators must treat early behavioral indicators not as isolated curiosities but as potential supporters. By developing observational sensitivity, using informed communication, and embedding scam recognition, they can detect and disrupt romance scams in their early stage before any financial or psychological damage occurs.

2.8 Responsive measures in case a victim falls in a love scam

After studying what measures should be put in order to prevent a love scam, or what educators should do in order to detect that a senior is about to fall in a scam, and to save them from falling into scams in the early stages, this section will analyse the responsive measures to be put in place in case a senior falls completely into a love scam. In this case, it is essential to handle the situation with care, empathy, and a structured approach. These scams are particularly damaging because they prey on the emotional vulnerability of seniors, often leading to significant emotional distress and financial loss. It is important to respond quickly, ensuring that the senior feels supported and empowered to take the necessary steps to recover from the scam. The below are the measures to put in place in case of occurrence of a scam in late stages:

A. Listen and Reassure

The first step in addressing a love scam is to listen to the senior's experience without judgment. Many seniors who fall victim to romance scams often feel embarrassed, ashamed, or even humiliated. They may have invested not only money but also their emotional energy into a relationship that they believed to be genuine. It is crucial to validate their feelings and provide reassurance that they are not at fault. Therefore, the educators must respond with a structured, and trauma informed approach that takes into consideration the victim dignity and psychological stabilization, as mishandling the moment of disclosure may result in re-traumatization or further silence, particularly among seniors, who may already struggle with digital exclusion and generational mistrust of authorities.

Scammers are skilled at manipulating emotions and creating a false sense of intimacy, making it easy for seniors to be taken advantage of. So, it's important that educators validate the victim's experience and to gently explain that they are not alone, and many others have fallen victim to similar scams. Reassure them that these perpetrators are criminals, and their emotional and financial losses are a direct result of fraudulent actions, not their own poor judgment.

Offering empathy and understanding can help alleviate feelings of guilt or embarrassment, which can be barriers to reporting the incident and seeking help. Let the senior know that

they have your full support and that recovery is possible, and do nor blame or interrogate them, or minimize their experience, as this will lead to a very deep emotional harm, and will make them prone to fall into scams over and over again in the future.

B. Document the Incident

Once the senior feels supported, the next step is to help them document the details of the scam. Recording important information will assist law enforcement and consumer protection agencies in their investigation. Encourage the senior to write down the following details:

- **Dates:** Record when the scam first began, when payments were made, and any other significant interactions.
- **Names used by the Scammer:** The name(s) the scammer used, even if they are assumed or fake. This can help authorities track the scammer.
- **Amounts Sent:** Record the amount of money sent to the scammer, as well as any other financial transactions, and their accounts information.
- **Communication Channels:** Document how the scammer communicated with the senior (e.g., email, phone calls, social media, or dating websites).

This documentation is vital, as it provides a clear record of the scam and can serve as evidence for investigations. It will also help in filing reports with appropriate agencies.

C. Report Promptly

The next critical step is to report the scam. Acting quickly is essential to limit further financial loss and assist in the investigation. Guide the senior in reporting the scam to the relevant authorities, such as local law enforcement, consumer protection agencies, or the national hotline dedicated to reporting fraud. Some key places to report a love scam include:

- **Local Law Enforcement:** File a police report as soon as possible. In cases of significant financial loss, local law enforcement can initiate an investigation or connect the victim with the appropriate agency.

- **Federal Trade Commission (FTC):** The FTC is the U.S. government agency responsible for protecting consumers. Seniors can report scams through their website ReportFraud.ftc.gov. The FTC also provides valuable resources on how to protect oneself from future scams.
- **Internet Crime Complaint Center (IC3):** Seniors who were targeted by scammers using online platforms (such as dating websites or social media) can report the scam to the IC3, which is a partnership between the FBI and the National White Collar Crime Center. Visit IC3.gov for more information.
- **National Fraud Hotline:** Countries have Fraud-reporting services that can be used to help authorities investigate and track the scammer. For Example, in the UK, seniors can contact Action Fraud at ActionFraud.police.uk for assistance.
- **Consumer Protection Agencies:** Many states or local municipalities have consumer protection agencies that handle cases of fraud. The trainer should look for the agency in one's country, and refer the victim to it. In Germany, for instance, seniors can contact Verbraucherzentrale Bundesverband (VZBV), which is Germany's central consumer protection agency that provides extensive support for fraud victims, including legal templates, advisory sessions, and digital safety guidance. On the European level, victims can report cross-border digital fraud through the European Consumer Centres Network (ECC-Net) or lodge transnational complaints through the EUROPOL Internet Crime Reporting interface.
- **Financial Institutions and Banks:** Make sure to report the scam to the local bank from which the victim transferred the money to the scammer. This will help in tracking the transfer, and possibly reporting it to bring the victim's money back.
- **Psychological support centres:** victims should also be referred to organisations that offer psychological counseling, victim advocacy, and court accompaniment. For example, in Germany, they can be directed to Weißer Ring, Germany's largest organization for crime victims, which offers free psychological support. Moreover, Cross-border cases involving international scammers can be escalated to the OLAF (European Anti-Fraud Office) or reported via Europol's European Financial and

Economic Crime Centre (EFECC) for potential international tracing.

By reporting the scam promptly, seniors not only protect themselves from further losses but also help law enforcement track down scammers and prevent others from falling victim to similar scams.

2.9 Establishing Long-Term Support Networks:

After assisting the senior victims to report the scammers, it is also critical to follow up with the victim in the weeks and months after disclosure. Studies show that many seniors experience secondary victimization including rejection, disbelief, or ridicule from family or community which can increase trauma and lead to prolonged isolation, re-victimization, or post-traumatic stress symptoms. Therefore, long-term emotional rehabilitation, social reintegration, and empowerment is very vital, and Educators and youth workers are instrumental in this phase, to maintain contact and offer reintegration into community, as well as emotional re-integration.

To offer this, firstly, youth workers and educators should encourage victims to **participate in support groups or peer-led recovery circles** where survivors can share experiences confidentially and without judgment. These groups can be hosted by adult education centers, where they work, or in age-inclusive clubs. This will lower their isolation, and will enforce social integration, as according to research studies, it was found that older adults who participate in structured peer engagement post-scam report significantly improved psychological resilience and reduced vulnerability to repeat offenses.

Another critical component is for educators to provide follow-up through **scheduling check-ins**, and ongoing educational reinforcement. This helps educators to understand the needs of the victims, and makes them feel supported, which will help them to recover emotionally, and re-engage socially. It is also worth noting that throughout all stages of response, the guiding principle must respect the victim's autonomy and dignity, where educators are not investigators or counselors but trusted allies in a recovery journey that may involve multiple professionals. Their role is to affirm the victim's experience, reconnect them with agency, and ensure they are not left to navigate the aftermath in isolation.

Moreover, Educators can encourage victims to join **group therapy,** trauma-informed counseling, and narrative reconstruction exercises, as they have been shown to help rebuild identity and agency. For example, in Germany, survivors may access such services through local public health insurers (e.g., AOK, TK), or organizations such as Weißer Ring, which offer specialized counseling for crime-related trauma. Municipal senior centers and health networks can also serve as access points for non-stigmatizing mental health services.

Digital reintegration is another key element of long-term recovery. Many victims become fearful of engaging with digital tools again, thereby increasing their isolation. Educators and youth workers can help restore confidence by offering digital re-onboarding workshops, designed to teach online safety, privacy settings, scam identification, and communication boundaries. This will be particularly effective in helping seniors re-engage with the digital world in a safe and supportive manner.

Another crucial point is to do **guiding and informative toolkits and workshops for the families and friends** of these victims, where open dialogue is encouraged, and information on how to react and support the seniors in order to improve their healing journey, as well as how to go through the difficult conversations. This will ensure offering an environment for the victims that doesn't blame or shame the victims, but rather to support them.

Finally, reintegration must include **empowerment opportunities**, where they are encouraged to speak up about their experience as they are more trusted by their fellow seniors. Victims who transition into educators, advocates, or peer supporters often report a stronger sense of control and healing. Community platforms should also allow survivors to share their stories anonymously in newsletters, public forums, or awareness campaigns transforming personal harm into communal protection. Such participatory recovery not only benefits the individual but reinforces collective vigilance against fraud.

In sum, self sustained recovery is not a linear process but a circular one, requiring continued emotional support, structured digital rehabilitation, robust institutional coordination, and meaningful social participation. The educator's role in this journey is

both facilitative and restorative, helping victims not only move beyond the scam but toward a stronger, more resilient person.

2.10 Practical Case studies

Based on the previous sections outlining scam detection, psychological impacts, the educator's role, and intervention strategies, the following practical scenarios are provided to help educators and youth workers apply key learning outcomes. Each case represents a common, real-world situation and is accompanied by reflective questions to assess judgment, communication strategies, and ethical sensitivity.

2.10.1 Case Study 1:

Anna, 71, has become quite active on Facebook over the past few months. During a coffee break at your community center workshop, she excitedly shares that she's met "a wonderful widower". "He really gets me," she says, "it's like he knows exactly what I'm feeling." She adds that he might come to visit soon, and Lately, she's been asking questions about international banking.

Reflective Questions:

- What signs suggest Anna may be at risk?
- What specific signs suggest that Anna may be vulnerable to a romance scam?
- How would you approach a non-confrontational, trust-building conversation to explore more about the scammer without provoking shame?
- What educational tools or peer discussion strategies could you use to help Anna critically reflect on her situation?
- If Anna remains adamant, how could you build a safety net without removing her autonomy?

2.10.2 Case Study 2:

Walter, 78, has recently started skipping sessions in your senior discussion group. When he does attend, he sits quietly and avoids eye contact. You notice he's spending a lot of time texting, visibly anxious. One day, you overhear him mention that he's sending money to help a "friend" he met online get a passport to join him in Germany.

Reflective Questions:

- What behavioral red flags in Walter align with known indicators of scam involvement?
- How would you open a dialogue that is respectful, trauma-informed, and avoids triggering defensiveness?
- What support resources or partnerships could you activate (e.g., legal aid, scam helplines)?
- How can you maintain Walter's dignity and autonomy while encouraging protective action?

2.10.3 Case Study 3:

You receive a phone call from Lara, the daughter of Maria, one of your long-time participants. Lara is upset and worried: "My mother just sent €5,000 to some man she's never met! He says he's in the military and stranded overseas. She thinks they're in love—it's madness!" Lara is furious and insists her mother is being foolish. She wants you to confront Maria and convince her to stop.

Reflective Questions:

- How would you approach Maria to preserve her trust while gently surfacing concerns?
- What strategies from trauma-informed care could you use to reduce shame and create a safe space for disclosure?
- How would you engage Lara in a supportive, non-coercive way, helping her understand the emotional dimensions of such scams?
- What role can you play in helping both parties find common ground for recovery and future protection?

Digital Defense: Cybersecurity Basics for Beginners

Co-funded by
the European Union

Jim Boelhouwer

I am an accomplished Project Manager and IT expert with a passion for continuous learning and achieving outstanding results. With a strong background in managing complex projects and a deep understanding of IT systems, Jim brings a wealth of expertise to every endeavor he undertakes.

I have impressive track record of successfully leading and delivering high-profile projects in the IT industry. My extensive experience spans various domains, including software development, infrastructure implementation, and system integration. My ability to effectively manage cross-functional teams and align project objectives with organizational goals has consistently resulted in on-time and within-budget project completions.

3 Cybersecurity Basics for Beginners

3.1 Key components of security awareness

In the previous chapter it is explained which tactics and methods criminals use to approach vulnerable older people to rob them financially.

One part of how these tactics and methods are exploited is via the use of digital communication. We are more and more connected to each other by a digitized world. This means that vulnerable older people need to be aware of the risks this brings along. Receiving emails or starting chat conversations can be the start of a process of financial exploits.

Security awareness is the understanding and recognition of potential cybersecurity threats and best practices for protecting sensitive information and systems. It involves educating people about various aspects of cybersecurity to reduce the risk of security breaches and data loss. The key components of security awareness are;

a. Phishing attacks and how to identify them
b. Password security and strong authentication
c. Safe use of removable media
d. Social engineering tactics
e. Proper use of social media and email
f. Cloud security best practices

3.2 Phishing attacks and how to identify them

Phishing attacks are fraudulent attempts to obtain sensitive information like usernames, passwords, credit card details, or other personal information by disguising as a trustworthy entity. Attackers typically use deceptive emails, text messages, or websites that appear legitimate to trick recipients into revealing their data or clicking malicious links that lead to malware installation. Here's an overview of common types of phishing attacks and how to identify them.

A. Phishing attacks

Types of Phishing Attacks:

- **Email Phishing:** This is one of the most widespread forms of phishing. Attackers use emails to impersonate trusted organizations or individuals, aiming to trick recipients into sharing sensitive data or clicking on malicious links.

- **Spear Phishing:** A more targeted version of phishing that involves tailoring emails to specific individuals or organizations.

- **Smishing (SMS Phishing):** Attackers use text messages containing malicious links or phone numbers to harvest personal information or infect devices with malware.

- **Vishing (Voice Phishing)**: This involves phone calls to impersonate trusted individuals. With AI-powered voice replication, these calls can sound highly realistic.

- **Clone Phishing**: Attackers create duplicates of legitimate emails, replacing original links with malicious ones.

- **Pop-Up Phishing**: Malicious pop-ups on websites that can trigger downloads of malware or redirect users to fake sites.

- **Evil Twin Phishing**: Attackers create fake Wi-Fi hotspots to intercept data from users who connect to them.

B. How to Identify Phishing Attacks

To identify them, look for unusual sender information, urgent or threatening language, requests for personal information, suspicious links and attachments, and generic greetings. Be extra cautious of emails that seem too good to be true, such as offers for free products or services.

Suspicious Email Characteristics:

- Requests for sensitive information (e.g., passwords, credit card details)
- Urgent or alarming messages creating a sense of panic
- Unfamiliar or slightly altered sender email addresses

- Spelling and grammar mistakes
- Generic greetings instead of personalized ones

- **Link and Attachment Red Flags**:
- Shortened or masked URLs hiding the actual destination
- Mismatched link text and actual URL (hover to check)
- Unsolicited attachments, especially from unknown senders

Content Warning Signs:
- Offers that seem too good to be true (e.g., free gift cards)
- Unexpected account-related alerts or problems
- Requests to verify or update account information via email

Technical Precautions:
- Check for HTTPS in website URLs, especially for sensitive transactions
- Be wary of duplicate Wi-Fi hotspots in public places
- Use pop-up blockers and be cautious of browser notification requests

By staying vigilant and following these guidelines, you can significantly reduce the risk of falling victim to phishing attacks. Remember, legitimate organizations will never ask for sensitive information via unsolicited emails or messages.

3.3 Password security and strong authentication

Password security and strong authentication are crucial components of cybersecurity in today's digital landscape. To ensure the protection of online accounts and sensitive information, it's essential to implement robust security measures.

3.3.1 Strong Passwords

Creating strong passwords is the first line of defense against unauthorized access. A strong password should:
- Be at least 10 characters long
- Include a mix of uppercase and lowercase letters, numbers, and symbols

- Avoid common words or easily guessable sequences

To create a strong password from a phrase, you can use several techniques. One popular method involves using the first letter of each word in the phrase, possibly adding numbers or symbols, and ensuring the password is of sufficient length.

Here's a breakdown of methods:

1. Acronyms:
- Take the first letter of each word in your chosen phrase.
- For example, the phrase "My favorite color is blue" could become "Mfcib".
- Consider adding numbers or symbols to make it stronger, like "Mfcib12!".

2. Substitution:
- Replace letters with similar-looking numbers or symbols (e.g., "a" with "@", "e" with "3").
- For example, the phrase "I love cats" could become "1 l0v3 c@ts".

3. Misspellings and Capitalization:
- Deliberately misspell words in your phrase, or capitalize some letters to create a unique combination.
- For example, "The quick brown fox" could become "Th3 q!ck br0wn f0x" or "ThE qUiCk bRoWn FoX".

4. Combining Techniques:
- You can combine acronyms, substitutions, misspellings, and capitalization for an even stronger password.
- For instance, using the phrase "This is a test" could become "T!s!s@t3s7t".

3.3.2 Best Practices for Password Management

Best practices for a strong password policy include setting a minimum password length, requiring a mix of characters (uppercase, lowercase, numbers, symbols), and encouraging the use of passphrases or password managers. To enhance password security:

- Use unique passwords for each account
- Change passwords regularly, ideally every 3 months
- Consider using a password manager to securely store and generate complex passwords
- Avoid sharing passwords or using easily guessable information

3.3.3 Multi-Factor Authentication (MFA)

Strong authentication goes beyond passwords by implementing multi-factor authentication. MFA requires at least two identity components to verify a user's identity. These components typically include:

1. Something the user knows (e.g., password or PIN)
2. Something the user has (e.g., smartphone or hardware token)
3. Something the user is (e.g., biometric data like fingerprints or facial recognition)

Enabling MFA on all accounts where possible significantly increases security by adding an extra layer of protection.

3.3.4 Strong Authentication Techniques

Strong authentication aims to verify user identities robustly and prevent unauthorized access. Some key aspects of strong authentication include:

- Not relying solely on shared secrets or symmetric keys
- Repelling credential phishing and impersonation attempts
- Using hardware-based cryptographic tokens, such as FIDO keys or smart cards, for the highest level of security

3.3.5 Benefits of Strong Authentication

Implementing strong authentication practices offers several advantages:

- Enhanced protection against credential theft and unauthorized access

- Reduced risk of successful phishing attacks
- Improved compliance with regulatory requirements
- Increased trust in user identities and overall system security

By combining strong passwords with multi-factor authentication and following best practices you can significantly improve your cybersecurity posture and protect sensitive information from potential threats.

3.4 Safe use of removable media

The use of removable media devices such as USB flash drives, external hard drives, SD cards, etc. has become prevalent due to their compact size and high storage capacity. However, these same features that make them user-friendly also make them attractive targets for cybercriminals looking to steal sensitive information.

According to a study by IBM Security, human error was responsible for more than 90% of security incidents involving removable media devices. Common mistakes such as misplacing or losing these devices can lead to unauthorized access or theft of confidential data.

Moreover, malicious attacks such as malware infections through infected USBs are becoming increasingly common.

Approximately 560,000 new pieces of malware are detected each day, according to Astra Security and DeepStrike. This figure represents a significant volume, adding to the already vast number of malware programs in existence, which exceed 1 billion.

To ensure the safe use of removable media, follow these best practices:

1. Use trusted devices only:
    - Never connect found or unknown removable media to your computer.
2. Implement security measures:
    - Install and maintain up-to-date anti-virus software that actively scans removable media when connected.

- Disable autorun and autoplay features on your computer to prevent automatic execution of malicious code.
- Encrypt all removable media devices to protect data if lost or stolen.
- Apply strong password protection to removable media devices.

3. Handle data properly:
   - Keep personal and work data separate.
   - Securely delete sensitive data from removable media after use.
   - Limit the use of removable media to only when necessary and authorized.
4. Maintain physical security:
   - Never leave removable media unattended, store securely when not in use.
   - Disable unnecessary wireless services like Bluetooth and Wi-Fi on devices.
5. Regular maintenance:
   - Conduct routine scans of removable media for malware.
   - Perform regular audits and monitor removable media usage to detect suspicious activities.

By following these guidelines, you can significantly reduce the risks associated with using removable media while still benefiting from its convenience and portability.

3.5 Social engineering tactics

Social engineering is the psychological manipulation of people to gain access to confidential information or to get them to perform actions that may not be in their best interest. Next to the already mentioned phishing types of tactics there are also the following tactics:

- Baiting: offering something enticing (like free software) that contains malware or compromises security when accessed.
- Quid pro quo: promising a benefit in exchange for information or action, like offering free IT support that installs malware.
- Scareware: using fear tactics to manipulate victims into acting, such as fake virus alerts.
- Watering hole attacks: compromising websites frequently visited by the target to deliver malware.

In the next 2 paragraphs we will go into more detail about two well-known types of social engineering: romance scam and pig butchering scam.

3.5.1 Romance scam

A **romance scam** is a confidence involving feigning romantic intentions towards a victim, gaining the victim's affection, and then using that goodwill to get the victim to send money to the scammer under false presentences or to commit fraud against the victim. Fraudulent acts may involve access to the victim's money, bank accounts, credit cards, passports, e-mail accounts, or national identification numbers or forcing the victims to commit financial fraud on their behalf. These scams are often perpetrated by the fraud factory operated by the organized criminal gangs who work together to take money from multiple victims at a time. Pig butchering scams (PBS or PB Scam) is an increasingly rampant and widespread type of romance scam which usually also entails the high yield investment program (HYIP) scam. We will discuss this kind of scam in a separate paragraph.

Stolen images

Romance scammers create personal profiles using stolen photographs of attractive people for the purpose of asking others to contact them. This is often known as catfishing. Often photos of unknown actresses or models will be used to lure the victim into believing they are talking to that person. US military members are also impersonated, as pretending to serve in the military explains why the scammer is not available for an in-person meeting.

Because the scammers often look nothing like the photos they send to the victims, the scammers rarely meet the victims face to face or even in a video call. They deceive their intended victims by making plausible-sounding excuses about their unwillingness to show their faces, such as by saying that they cannot meet yet because they are temporarily traveling or have a broken web camera.

Tricking the victim

Scammers are very adept at knowing how to "play" their victims – sending love poems, sex games in emails, building up a "loving relationship" with many promises of "one day we will be married". Scammers ask their victims many questions but share little about themselves.

They often shower the victims with compliments.

Communications are exchanged between the scammer and victim over a period, sometimes months or even an entire year, until the scammer feels they have connected with the victim enough to ask for money. Scammers prey on the victims' false sense of a relationship to lure them into sending money.

These requests may be for gas money, bus or airplane tickets to visit the victim, medical or education expenses. There is usually the promise the scammer will one day join the victim in the victim's home.

Victims may be invited to travel to the scammer country; in some cases, the victims arrive with asked-for gift money for family members or bribes from corrupt officials, only to be beaten and robbed or murdered.

The scam usually ends when the victim realizes they are being scammed or stops sending money. However, people are often slow to believe the reality, and the stigma of falling for such deception may deter them from reporting fraud to the police. Many victims, even when confronted with strong evidence, cannot bring themselves to believe that the person who seems so loving in text messages is instead a criminal scammer. They may react angrily or violently against anyone who objects. Banks can lock down the victim's money, especially when financial abuse of an elder is suspected.

Criminal groups

Criminal networks defraud lonely people around the world with false promises of love and romance. Scammers post profiles on dating websites, non-dating social media accounts, classified sites and even online forums to search for new victims. The scammer usually attempts to obtain a more private method of communication, such as an email or phone number, to build trust with the victim.

Because the scammers are working in groups, someone in the group can be online and available to send e-mail or text messages to the victim at any hour. The rotation between different scammers, all claiming to be the same person, is difficult to detect in text-based

messages, whereas it would be obvious if a different person showed up for a face-to-face meeting or in a video or telephone call.

3.5.2 Pig butchering scam:

Pig-butchering scams originated in 2016 or earlier as a regional scam in China, originally finding their victims on same-sex dating sites before expanding to opposite-sex dating sites as well. The term "pig butchering" arises from an analogy comparing the initial phase of gaining the victims' trust to the fattening of pigs before slaughtering them.

The modus operandi later spread throughout southeast Asia at the height of the covid pandemic. In Cambodia, once a prosperous gambling town, many local gambling gangs transformed casinos into scam operations center, performing pig-butchering scams. This was likely a result of a lack of casino attendance on account of the covid pandemic and the Cambodian government cracking down on commercial gambling. Many operations are also run from areas of Myanmar which are outside central government control because of the civil war, with one important hub being the town of Myawaddy, near the border of Thailand. According to the UNHR Office, hundreds of thousands of people have been trafficked and are trapped in scam centers in Cambodia and Myanmar, with other operations being run from Laos, the Philippines and Thailand. Many of the groups that run pig-butchering scams are overseas Chinese criminal syndicates based in Southeast Asia, who traffic ethnic Chinse and others into fraud factories and force these people to commit the fraud.

Pig-butchering scams gained international momentum through the exploitation of online dating apps and social media platforms. Scammers crafted elaborate fake identities to establish romantic or emotional connections with victims, thus marking a departure from conventional financial scams by integrating psychological manipulation. This early phase of these scams primarily targeted local populations but quickly expanded as digital connectivity grew.

The scams evolved significantly with the integration of sophisticated techniques, including the creation of fake online investment platforms and the use of social engineering. With

the wider use of platforms like WhatsApp and Telegram, random persons can be targeted just by starting an accidental conversation. A key aspect of this evolution was the use of cryptocurrency for transactions, which appealed to scammers due to its difficulty to trace and recover. The scams' globalization can be attributed to the increased ubiquity of digital interactions and the rising popularity of cryptocurrencies, which provided a new avenue for such fraudulent activities on a global scale.

✦ Criminal groups

Pig-butchering scams involve a series of meticulously planned steps to deceive and exploit victims, typically focusing on cryptocurrency investment fraud.

1. **Gaining trust:** Scams often begin with casual conversations initiated by the scammer, who may pretend to have received the victim's contact details accidentally or through a mutual acquaintance. These initial interactions are designed to build trust and may involve the use of attractive profile images to lure victims.
2. **Introducing the investment:** As trust is established, the scammer introduces the victim to a fraudulent investment scheme, promising significant returns in a short period. The scammers use persuasive tactics and counterfeit investment portfolios to convince victims of the scheme's legitimacy.
3. **Collecting money:** After persuading the victim to invest, scammers collect funds, often through digital payment platforms or cryptocurrencies, to complicate tracking and tracing of the transactions.
4. **Disappearance of the scammer:** Once a substantial amount has been collected, or when victims attempt to withdraw funds, scammers become unreachable, delete their online presence, or create new identities, leaving the victims with no way to recover their funds.

Furthermore, the scammers develop fake brokerage websites and mobile applications to add legitimacy to their scheme, making it difficult for victims to distinguish them from genuine platforms.

3.6 Proper use of social media and email

Social media is, of course, far from being all bad. There are often tangible benefits that follow from social media use. Many of us log on to social media for a sense of belonging, self-expression, curiosity, or a desire to connect. Apps like Facebook, Instagram, WhatsApp, Telegram and Twitter allow us to stay in touch with geographically dispersed family and friends, communicate with like-minded others around our interests, and join an online community to advocate for causes dear to our hearts.

We each must come to our own individual decisions about social media use, based on our own personal experience. Grounding ourselves in the research helps us weigh the good and bad and make those decisions. Though the genie is out of the bottle, we may find, as Shakya and Christakis put it, that "online social interactions are no substitute for the real thing," and that in-person, healthy relationships are vital to society and our own individual well-being. We would do well to remember that truth and not put all our eggs in the social media basket.

General Guidelines:

- Maintain privacy by reviewing settings regularly
- Think before posting - content can remain online indefinitely
- Be respectful and considerate in all interactions
- Verify information before sharing to avoid spreading misinformation
- Remember that your digital footprint affects your personal and professional reputation

Security Awareness:

- Be cautious with links and attachments
- Verify sender addresses before responding to suspicious emails
- Never share sensitive information unless you're certain of security
- Use encryption for sensitive communications
- Use strong, unique passwords and enable two-factor authentication

3.7 The introduction of Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to the development of computer systems capable of performing tasks that typically require human intelligence. These tasks include learning,

problem-solving, decision-making, and understanding natural language. AI encompasses a wide range of techniques and approaches, from simple rule-based systems to complex machine learning models. Here's a more detailed look on the core concepts:

- **Mimicking Human Intelligence:** AI aims to create machines that can perform tasks that humans usually do using their intelligence.
- **Learning and Problem-Solving:** AI systems can learn from data, identify patterns, and make decisions based on that learning.
- **Diverse Applications:** AI is used in various fields, including healthcare, finance, education, and transportation.
- **Machine Learning:** A core component of modern AI, where algorithms learn from data without explicit programming.
- **Natural Language Processing:** Enables machines to understand and interact with human language.
- **Computer Vision:** Allows machines to "see" and interpret images and videos.

Examples of AI in Use:

- **Voice Assistants:** Like Siri or Alexa, which understand and respond to voice commands.
- **Recommendation Systems:** Used by online platforms to suggest products or content based on user preferences.
- **Self-Driving Cars:** Utilizing AI for navigation and decision-making in autonomous vehicles.
- **Fraud Detection:** Employing AI to identify suspicious transactions in financial systems.

In essence, AI is a rapidly evolving field with the potential to transform various aspects of our lives. The same principles apply to romance scams, in which AI-generated personas posing as the scammer's friends, family or colleagues interact with the victim to validate the relationship and ease their doubts. These interactions simulate social proof, making it harder for victims to question inconsistencies.

3.7.1 Initial contact

The credibility of a scammer's profile is crucial in the early stages of romance fraud, as it helps determine whether a target engages with a fake persona. While scammers traditionally stole images from real users, reverse image searches and photo forensics could be used to expose these deceptions. However, through the integration of LLMs and deepfake image generation, fraudsters can now easily mass-produce synthetic personas that closely mimic real users. These profiles are designed to bypass detection mechanisms on social media, dating platforms and professional networks while effectively deceiving victims.

The scale of AI-driven profile creation is vast. For example, Meta reportedly removed billions of fake accounts in 2024 (this included any account that the firm believed had been created with malicious intent or for non-human entities). The surge in AI-generated fraudulent profiles forced dating platform Tinder to expand its identity verification programme in 2024, rolling out enhanced measures in the US and the UK. These measures require users to submit government-issued IDs and self-recorded videos. However, they may not be sufficient to tackle the increasing sophistication of generative AI, with the technology posing challenges to KYC checks and other identity verification processes.

AI-generated profiles do not operate in isolation. Fraudsters can combine synthetic personas with automated outreach, creating high-volume pipelines in which thousands of realistic profiles simultaneously deploy LLM-generated messages. As discussed in the previous section, fraudsters are likely to leverage LLMs in the initial outreach rather than later interactions. This is because:

- The first message requires minimal personalisation, making them easy to generate at scale.
- Sending out introductory messages is highly repetitive work, making automation a high priority for fraudsters looking to increase efficiency.
- LLMs perform best in structured, low-context scenarios, making them particularly suited to this stage.

This means that AI is already well-positioned to enhance the early-stage scalability of romance scams. Fraudsters can deploy the technology across multiple platforms, relying

on LLM-generated messages to initiate conversations efficiently. Once a victim engages, scammers can then transition to manual intervention or refined AI-assisted interactions to sustain deception.

As AI-generated profiles and outreach become more sophisticated, traditional detection methods such as profile verification and text-based anomaly detection may struggle to keep pace, necessitating adaptive countermeasures.

3.7.2 Relationship-building

Once fraudsters have established initial contact, they transition into the relationship-building phase, in which they seek to deepen emotional engagement and establish trust with their targets. AI-driven tools have enhanced scammers' ability to scale and personalise deception, but they have only a limited capacity to automate this phase. Unlike initial outreach, which benefits from generic scripting and large-scale automation, relationship-building requires adaptability, emotional intelligence and tailored responses to victim interactions.

A key distinction between AI-driven and human-led deception is adaptability. Human scammers can dynamically adjust their narratives based on victims' responses, ensuring conversations remain emotionally engaging and progress towards financial exploitation. While LLMs can generate procedurally accurate scam messages, they struggle to maintain continuity and in-depth personalisation across extended interactions. Without human oversight, AI-generated messages risk tone inconsistencies, contradictions and repetitive phrasing, which can weaken credibility over time. The United Nations Office on Drugs and Crime[29] reports that while AI is already being used in cyber-enabled crimes, most scams still rely on human oversight to maintain credibility and manage complex interpersonal dynamics.

However, AI can enhance this phase in several ways:

Scam script optimisation: fraudsters can use LLMs to refine scam scripts, testing different phrasing and emotional appeals to maximise engagement.

- **Multilingual chat assistance:** translation allows scammers to engage victims in multiple languages with improved fluency.
- **Automated relationship management:** AI tools can help fraudsters manage multiple victims simultaneously, providing suggested responses and engagement strategies while minimising inconsistencies across conversations.

While LLM-generated text facilitates scalable and personalised engagement, deepfake media provide an additional layer of authenticity, making fraudulent personas more convincing and increasingly difficult to verify. AI-powered voice cloning tools allow scammers to generate content that mimics speech patterns, accents and emotional inflections, reducing the need for direct human interaction. Similarly, fraudsters can use AI-generated video to fabricate visual proof of identity, enabling them to bypass verification requests and deepen trust with potential victims. Although fully autonomous deepfake interactions remain technically challenging, scammers already exploit pre-recorded synthetic video content, allowing them to maintain a deception for longer.

Recent high-profile cases highlight the growing impact of deepfake deception. A UK engineering firm reported in January 2024 that criminals used a deepfake video to successfully impersonate senior executives, facilitating a $25 million corporate fraud. In October 2024, romance scammers employed deepfake-generated visuals to deceive victims into believing they were in genuine relationships, ultimately extracting $46 million from them. Though more recent cases have focused on the role of deepfakes in romance scams, the underlying tactics are expanding across other domains, including investment fraud.

Advancements in AI inpainting technology, which seamlessly integrates generated content into existing images or videos, have further enhanced the realism of these deceptive materials, making detection increasingly difficult for both humans and automated systems. As AI develops new capabilities, its role in fraudulent relationship-building will likely evolve, blending automated deception with strategic human oversight to maximise the effectiveness of scams.

3.7.3 Grooming

As a relationship deepens, fraudsters shift from general trust-building to highly targeted psychological manipulation. This stage, commonly referred to as grooming, involves escalating emotional dependence and isolating the victim from external influences to increase their vulnerability to financial or personal exploitation. AI enhances and personalises this process by analysing a victim's online behaviour, monitoring their emotional state and adapting communication patterns, potentially in real time. By automating these manipulative techniques, AI allows fraudsters to optimise deception at scale, making their tactics more sophisticated and efficient, as well as harder to detect.

AI-powered systems can rapidly gather and analyse data from multiple sources, including social media and public records, to create a comprehensive psychological profile of potential victims. Traditionally, such profiling required extensive manual effort, but AI can automate and refine this process within seconds, enabling scammers to identify and prioritise highly vulnerable targets. AI-driven profiling is well-documented in social engineering, particularly in spear phishing attacks, which tailor messages to exploit individuals' fears, desires or insecurities.

Fraudsters can extend this AI-driven profiling into real-time behavioural analysis, tracking a victim's responses, engagement patterns and emotional cues. By processing ongoing conversations, AI can help scammers dynamically adjust their tone, timing and messaging to create an illusion of genuine connection. This allows for a gradual yet highly calculated deepening of emotional reliance on the scammer's fabricated persona.

AI's ability to create immersive online environments further strengthens the grooming process by reinforcing the scammer's fabricated identity and reducing victims' scepticism about the process. Research into AI-driven political and marketing persuasion has shown that models can micro target individuals with tailored messaging, thereby increasing their engagement and shaping their beliefs. The same principles apply to romance scams, in which AI-generated personas posing as the scammer's friends, family or colleagues interact with the victim to validate the relationship and ease their doubts. These interactions simulate social proof, making it harder for victims to question inconsistencies.

Additionally, the type of AI-powered content creation and bot-driven amplification often

observed in political influence campaigns can flood online spaces with reinforcing narratives. This ensures that when a victim searches for their partner's name, they find fabricated testimonials, fake profiles or AI-generated articles that strengthen the scam's credibility. Just as public figures can use AI to steer public discourse and reinforce political narratives, fraudsters can exploit it to curate an artificial digital network that isolates the victim.

3.7.4 Execution

As trust deepens, fraudsters escalate from emotional manipulation to financial exploitation, leveraging the victim's attachment to justify requests for payment. This phase often involves fabricated crises such as medical emergencies, logistical complications or legal troubles, all of which are designed to create urgency and pressure the victim into sending money. Gift cards remain a common method of financial extraction, featuring in 24% of reported romance scam cases, but cryptocurrency and bank transfers result in significantly higher losses per victim. Reports indicate that losses from romance scams have surged in recent years, costing the UK public more than £80m per year. In Australia, reported losses exceeded AU$23 million in 2024, with AI playing a significant role in this increase.

Beyond timing and scale, AI helps fraudsters engage in sophisticated deceptions, fabricate financial legitimacy and streamline money laundering, making financial extraction subtler and more effective. One concerning development relates to AI's ability to fabricate financial credibility. Like many other criminals, romance scammers use shell companies to hide their illicit gains. Fraudsters now use generative AI to forge convincing financial statements, legal documents and synthetic identities to bypass financial institutions' checks. As discussed, criminals increasingly use AI-generated synthetic identities to bypass KYC verification, allowing them to open fraudulent bank accounts and facilitating money laundering at scale. Their AI-generated identities can infiltrate legitimate financial networks in ways that traditional fraud monitoring systems increasingly struggle to detect.

AI is also playing a critical role in the rise of 'pig butchering' scams, one of the most

lucrative forms of financial extraction in romance fraud. In these schemes, scammers groom victims over weeks or months before introducing them to fake cryptocurrency or investment platforms, on which they are tricked into making increasingly large deposits. Fraudsters increase the credibility and realism of these fake investment sites by not only copying code from real investment platforms but also using AI to generate content for them. They also deploy AI-powered chatbots as fake investment advisors to guide victims through the platform, ensuring that even sceptical users feel reassured by fabricated market trends and personalised guidance. These chatbots further entrap victims by embedding malicious links in their communications, directing them towards other fraudulent schemes and deepening their financial losses.

Cryptocurrency scam revenues reached an estimated $12.4 billion in the US in 2024, with pig butchering scams accounting for a significant share of these losses. Meanwhile, AI-assisted coding tools have reduced the technical skill required to launch fake investment platforms, allowing scammers to mass-produce fraudulent sites with minimal effort.

As AI continues to automate deception and streamline fraud operations, pig butchering scams are becoming increasingly intertwined with romance fraud. The ability to create hyper-personalised, AI-driven investment scams makes these schemes even more insidious, harming victims both financially and psychologically.

3.7.5 Exit or Escalation

As romance scams reach their final phase, fraudsters either abruptly disappear after extracting payments from their victims or escalate their deception to extract even more. AI enables ever more complex exit strategies, prolonging victim exploitation through techniques such as deepfake blackmail and impersonation scams.

As the Federal Trade Commission recently reported, a rising tactic involves AI-powered impersonation of law enforcement or financial recovery services. In this type of scam, fraudsters contact victims with false promises of financial restitution, posing as police officers, financial regulators or investigators to claim that they can help recover lost funds for a fee.

3.8 Romance Scam Case Study of Sarah Thompson

Background

Sarah Thompson, a 58-year-old widow from Portland, Oregon, lost her husband of 30 years to cancer in 2022. After a year of grieving, her adult children encouraged her to try online dating as a way to reconnect socially. With limited dating experience in the digital age, Sarah created a profile on a popular dating site in March 2023.

Initial Contact

Within two weeks of joining the platform, Sarah received a message from "William Pierce," who claimed to be a 62-year-old American civil engineer working on a contract in Malaysia. His profile featured photos of an attractive, silver-haired man with a warm smile. William expressed that he was also widowed and looking for companionship.

Their conversations quickly moved from the dating platform to email and WhatsApp, which should have been the first red flag. William was attentive, romantic, and seemed deeply interested in Sarah's life. They communicated daily through messages and occasional voice calls, though William always had excuses for why video calls weren't possible—poor internet connection, busy work schedule, or time zone differences.

Relationship Development

Over the next two months, William built an emotional connection with Sarah through:

- Daily good morning and goodnight messages
- Sharing personal stories about his deceased wife and children
- Discussing future plans to meet and possibly build a life together
- Sending occasional gifts (flowers, chocolates) to Sarah's home
- Expressing deep romantic feelings relatively quickly

The Financial Requests

Approximately three months into their relationship, William's financial requests began:

1. **Initial Request:** William claimed his project was delayed due to equipment failure. He needed $3,000 to replace parts and couldn't access his funds due to "banking issues abroad." Sarah, concerned about his situation, sent the money via wire transfer.
2. **Escalation:** After expressing tremendous gratitude, William announced the project was nearly complete, and he would be returning to the U.S. within weeks. However, he then claimed he had a medical emergency (appendicitis) and needed $7,500 for surgery not covered by his insurance. Sarah, now emotionally invested, borrowed against her retirement to send the funds.
3. **Crisis Situation:** Just before his supposed return to America, William claimed he had been in an accident at the work site. He needed $15,000 for medical expenses and to resolve a legal dispute with the local company to release his passport. He promised to repay everything upon his return.

Red Flags Sarah Missed

Looking back, Sarah identified several warning signs she had overlooked:

- William's reluctance to video chat
- Inconsistencies in his stories about family and work
- His knowledge of engineering seemed vague when pressed for details
- Photos never showed him in Malaysia or at work sites
- All conversations steered toward their relationship or his problems
- His writing contained grammatical errors inconsistent with a native English speaker
- Reasons why he couldn't access his own substantial funds became increasingly elaborate

The Turning Point

Sarah became suspicious when William's demands increased and his stories grew more complex. When she mentioned visiting him in Malaysia, he strongly discouraged it. Her daughter, concerned about her mother's financial situation, insisted on reviewing William's communications and recognized the patterns of a romance scam.

To confirm their suspicions, Sarah's daughter conducted a reverse image search on William's photos, discovering they belonged to a retired professor in Canada who had no

connection to the scammer.

Resolution and Aftermath

Sarah ultimately lost approximately $25,500 to the scammer before cutting contact. When confronted, "William" initially denied the deception, then became aggressive before disappearing entirely. Sarah reported the scam to:

- Local police
- The FBI's Internet Crime Complaint Center (IC3)
- The dating platform where they met
- Her bank and financial institutions

While she was unable to recover the lost funds, the experience led Sarah to:

- Join a support group for romance scam survivors
- Work with a financial advisor to rebuild her retirement savings
- Become an advocate for romance scam awareness in senior communities
- Develop healthier boundaries in relationships

Psychological Impact

Sarah experienced significant emotional trauma from the scam:

- Deep shame and embarrassment
- Trust issues in new relationships
- Depression and anxiety
- Financial stress from the losses
- Grief over the relationship she thought she had

Key Lessons

This case highlights several important aspects of romance scams:

1. Scammers target vulnerable individuals, particularly those who have experienced recent loss
2. They build emotional connections before making financial requests

3. They isolate victims from support networks that might identify the scam
4. They create urgency and emotional pressure around financial requests
5. They have plausible explanations for why they cannot video chat or meet in person

Prevention Strategies

From Sarah's experience, several prevention strategies emerge:

- Never send money to someone you haven't met in person
- Insist on video calls early in online relationships
- Research the person's information and photos
- Discuss new relationships with trusted friends or family
- Be wary of relationships that progress unusually quickly
- Question why someone with claimed resources needs your financial help
- Be skeptical of repeated emergencies and crises

Conclusion

Sarah's case is representative of thousands of romance scams that occur annually. While she lost significant money, the emotional impact of the betrayal proved even more devastating. Through therapy and support groups, Sarah has rebuilt her life and now helps others recognize the warning signs of romance scams before they lose their savings—or their hearts to skilled manipulators.

Know & Grow: Self-Assessment and Evaluation.

Co-funded by
the European Union

4 Self-Assessment and Evaluation

4.1 Self Assessment tests on Chapter 1: Understanding love scams

1. What is the primary goal of a love scam?
   A) To find genuine romantic partners
   B) To exploit emotional connections for financial gain
   C) To promote healthy online relationships
   D) To provide dating advice

Correct answer: B

2. Which historical scam is the love scam said to be rooted in?
   A) Ponzi scheme
   B) The “Spanish prisoner” scam
   C) Pyramid scheme
   D) Nigerian prince scheme

Correct answer: B

3. What is the initial phase in Whitty's framework for the stages of a romance scam?
   A) Preparation phase
   B) Profiling phase
   C) Exploitation phase
   D) Revelation phase

Correct answer: B

4. In romance scams, the tactic of overwhelming the target with affection and attention is known as:
   A) Guilt-tripping
   B) Crisis creation
   C) Love bombing
   D) Financial exploitation

Correct answer: C

5. Which of the following is a common red flag in romance scams?
A) Requests to meet in person immediately
B) Limited or vague personal details on the scammer's profile
C) Clear and consistent life stories
D) Public social media presence
Correct answer: B

6. According to studies, which group is more likely to fall victim to romance scams?
A) Young adults aged 18-25
B) Elderly men over 70
C) Middle-aged women aged 40-60
D) Teenagers
Correct answer: C

7. What type of payment method is commonly requested by scammers in love scams?
A) Personal checks
B) Cryptocurrency or gift cards
C) Credit card payments
D) Direct deposit into a bank account
Correct answer: B

8. How do scammers often attempt to prevent victims from recognizing the scam?
A) By meeting victims frequently
B) Through video calls only
C) By asking victims to avoid sharing their relationship details with others
D) By encouraging victims to report them
Correct answer: C

10. Which of the following is a recommended preventive measure against romance scams?
A) Sending money quickly to avoid losing the relationship
B) Keeping details private and conducting background checks on new contacts
C) Avoiding friendships and relationships altogether
D) Ignoring any feelings of suspicion
Correct answer: B

9. What is often the psychological impact on victims of romance scams, according to Button et al. (2014)?

A) Relief and satisfaction
B) Only financial loss without emotional impact
C) Severe emotional trauma and financial loss (Correct)
D) Feeling more secure
Correct answer: C

4.2 Self Assessment tests on Chapter 2: Good Practices for Educators

1. What is one of the main reasons scammers target socially isolated seniors?
A) They are more likely to invest in risky stocks
B) They are eager to learn new technology
C) They are usually wealthy
D) They are emotionally vulnerable and seek connection
Correct answer: D

2. Which factors most often contribute to a senior's vulnerability to love scams?
A) High income and lack of social media experience
B) Trusting nature, cognitive decline, and emotional need
C) Free time, and good family support
D) They are usually wealthy
Correct answer: B

3. What tactic do scammers often use to emotionally groom their victims?
A) Strict legal language
B) Promises of early inheritance
C) Love bombing and emotional reinforcement
D) Mocking their loneliness
Correct answer: C

4. What is a dual trauma often faced by love scam victims?
A) Emotional betrayal and financial loss
B) Legal trouble and health decline
C) Family conflict and embarrassment
D) Technology misuse and job loss
Correct answer: A

5. Which consequence can persist years after the scam if they were not offered proper support?
A) Improved judgment
B) Long-term trauma and avoidance of relationships
C) Better online habits
D) Better self esteem
Correct answer: A

6. Why do seniors often avoid reporting scams?
A) They do not understand how reporting works
B) They are not emotionally impacted
C) They fear shame, ridicule, or judgment
D) They want to protect the scammer
Correct answer: C

7. Why are educators often more effective than family in early scam detection?
A) They have legal authority to investigate
B) They restrict online use
C) Seniors feel less judged and more comfortable confiding in them
D)They live with the seniors
Correct answer: C

8. What role can youth workers play in reducing seniors' vulnerability to scams?
A) Report scams to banks on seniors' behalf
B) Offer intergenerational digital mentoring and empathy
C) Remove seniors from online platforms
D) Replace educators in all workshops
Correct answer: B

9. What is the primary reason digital literacy is emphasized in scam prevention?
A) To reduce susceptibility to online fraud tactics
B) To make seniors spend more time online
C) To teach them to create blogs
D) To avoid needing police intervention
Correct answer: A

10. Why are “buddy systems” effective in preventing scams?
A) They reduce travel costs for educators
B)They limit phone calls
C) They monitor internet use
D) They give seniors someone to confide in about suspicious activity
Correct answer: D

11. What should educators prioritize when designing scam-prevention workshops? A) Complex technical language and long sessions
B) Shame-based cautionary tales
C) Accessible, interactive methods on emotional and digital awareness
D) Telling seniors to stop using technology
Correct answer: C

12. Which behaviour is an early warning sign of an ongoing romance scam?
A) Volunteering more often
B) Increased family visits
C) Attending digital literacy classes
D)Sudden secrecy about a new online relationship (Correct)
Correct answer: D

13. Which is NOT a recommended detection method?
A) Direct confrontation
B) Trust-building conversations
C) Emotional engagement
D) Observing behavior
Correct answer: A

14. What is “triage” in scam response strategy?
A) Blaming the victim
B) Evaluate, accuse, report
C) Ignore, watch, analyze
D) Engage, educate, evaluate
Correct Answer: D

15. How should educators handle emotionally invested seniors in active scams?
A) Use scare tactics
B) Use anonymized scenarios and guided questions
C) Insist they report the scam immediately
D) Alert their family without consent
Correct Answer: B

16. How can educators help reduce post-scam isolation?
A) Encourage secrecy
B) Reconnect victims with safe social activities and support groups
C) Monitor their social media
D) Cut off internet use
Correct Answer: B

17. Why should educators involve the families of victims sensitively?
A) To blame them
B) To increase pressure
C) To hand over responsibility
D) To build support and reduce victim shame
Correct Answer: D

18. Why are partnerships with libraries, health centers, and community hubs critical in scam prevention?
A) They reduce paperwork
B) They replace the educator’s work
C) They help reach seniors and provide trusted environments
D) They can enforce legal action
Correct Answer: C

4.3 Self Assessment tests on Chapter 3: Cybersecurity Basics for Beginners

1: What is the primary characteristic of a phishing attack?
a) Installing malware through USB devices
b) Exploiting software vulnerabilities
c) Deceiving individuals into revealing sensitive information through fraudulent communications
d) Physically breaking into computer systems
Correct Answer: C

2: How does spear phishing differ from regular phishing?
a) It uses phone calls instead of emails
b) It targets specific individuals or organizations with personalized attacks
c) It only targets government agencies
d) It uses physical mail instead of electronic communication
Correct Answer: B

3: What is pretexting in social engineering?
a) Sending mass emails to random recipients
b) Creating a fabricated scenario to engage victims and steal information
c) Using technical exploits to gain system access
d) Installing keyloggers on target computers
Correct Answer: B

4: Which scenario best describes a baiting attack?
a) Leaving infected USB drives in parking lots for employees to find
b) Sending threatening emails demanding payment
c) Making phone calls pretending to be IT support
d) Creating fake social media profiles
Correct Answer: A

5: What is tailgating in the context of social engineering?
a) Following someone's online activity
b) Monitoring network traffic
c) Following someone through a secure door without proper authorization
d) Copying someone's keystrokes
Correct Answer: C

6: What does "vishing" refer to?
a) Visual phishing through fake websites
b) Viral phishing through social media
c) Video phishing through fake video calls
d) Voice phishing using phone calls
Correct Answer: D

7: Which psychological principle do social engineers commonly exploit?
a) Technical complexity
b) Network protocols
c) Authority and trust
d) Encryption algorithms
Correct Answer: C

8: What is a watering hole attack?
a) Poisoning actual water supplies
b) Compromising websites frequently visited by target organizations
c) Attacking water utility companies
d) Using water-themed phishing emails
Correct Answer: B

9: What characterizes a quid pro quo social engineering attack?
a) Offering something in exchange for information or access
b) Threatening legal action
c) Using only technical methods
d) Targeting only executives
Correct Answer: A

10: What is reverse social engineering?

a) Engineering social networks backwards

b) When the attacker positions themselves as helpful and waits for the victim to contact them

c) Reversing the effects of social engineering

d) Using social media in reverse chronological order

Correct Answer: B

11: Which of the following is a red flag that may indicate a social engineering attempt?

a) Requests for software updates

b) Urgent requests for sensitive information with threats of consequences

c) Regular private communications

d) Scheduled meetings with known people

Correct Answer: B

Sources

AARP. (n.d.). Romance scams. https://www.aarp.org/money/scams-fraud/

AARP. (2021). AARP VOA ReST program: Healing after fraud. AARP Fraud Watch Network. https://www.aarp.org/fraudwatchnetwork

AARP. (n. d.). Emotional Support for Victims of Fraud. https://states.aarp.org/maryland/emotional-support-for-victims-of-fraud#

Against Scams. (2024). The importance of trauma therapy for scam victims. https://againstscams.org/importance-of-trauma-therapy-for-scam-victims-2024

Action Fraud. (n.d.). Romance fraud. https://www.actionfraud.police.uk/

Action Fraud. (2025, January 30). Our research and statistics on romance fraud – Action Fraud claims advice. https://www.actionfraud.org.uk/research-and-statistics-on-romance-scams-fraud/

Ayoobi, N., Shahriar, S., & Mukherjee, A. (2023, September 5). The looming threat of fake and LLM-generated LinkedIn profiles: Challenges and opportunities for detection and prevention. arXiv. https://doi.org/10.1145/3603163.3609064

BBC News. (2024, May 7). How a 'Brad Pitt' scam broke my mum's heart. https://www.bbc.com/news/articles/ckgnz8rw1xgo

Berry, K. (2024, November 24). Scams: 'I was duped by Martin Lewis deepfake advert'. BBC News. https://www.bbc.co.uk/news/articles/clyvj754d9lo

Boulat, P.-A., & Wake, P. (2024, May 15). Can AI-generated deepfakes compromise know your customer (KYC) authentication? techUK. https://www.techuk.org/resource/can-ai-generated-deepfakes-compromise-know-your-customer-kyc-authentication.html

Sources

Brady, S. (2024, February 20). Tinder bolsters ID verification amid surge in AI scams. Verdict. https://www.verdict.co.uk/tinder-bolsters-id-verification-amid-surge-in-ai-scams/?cf-view&cf-closed

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391-408. https://doi.org/10.1177/0004865814521224(Original work published 2014)

Commissariato di P.S. (n.d.). Truffe romantiche - Romance scam. Polizia di Stato. https://www.commissariatodips.it/consigli/per-i-cittadini-e-i-ragazzi/truffe-romantiche-romance-scam/index.html

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020.). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. Clin Pract Epidemiol Ment Health, 16 https://doi.org/10.2174/1745017902016010024

Cross, C. (2014). Love hurts: the costly reality of online romance fraud. The Conversation.

Cross, C., Dragiewicz, M., & Richards, K. (2016). Understanding romance fraud: Insights from domestic violence theory. Cyberpsychology, Behavior, and Social Networking, 19(7), 419-423. https://doi.org/10.1089/cyber.2016.0729

Cross, C., & Layt, R. (2021). “I suspect that the pictures are stolen”: Romance fraud, identity crime, and responding to suspicions of inauthentic identities. Social Science Computer Review, 40(4), 1043–1058. https://doi.org/10.1177/0894439321999311

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: The need to rethink current romance fraud prevention messaging. Crime Prevention and Community Safety, 24(1), 30–41. https://doi.org/10.1057/s41300-021-00134-w

Sources

Cunha, H. S. (n.d.). Why are romance scams so powerful? https://www.newcastle.edu.au/__data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf

CybSafe. (2023). Romance scams: The stats, and what they mean for your organization. https://www.cybsafe.com/blog/romance-scams-stats-for-organizations/

Daily Mail. (2024, June 1). British grandmother arrested in Brazil for smuggling cocaine. https://www.dailymail.co.uk/news/article-14718249/Grandmother-Veronica-Watson-Brazil-drugs.html

Dellinger, A. J. (2019). Anatomy of a scam: Nigerian romance scammer shares secrets. Forbes. https://www.forbes.com/sites/ajdellinger/2019/11/25/anatomy-of-a-scam-nigerian-romance-scammer-shares-secrets/

Dogma. Truffe sentimentali: I segnali e come difendersi. https://www.dogma.it/it/news/truffe-sentimentali--i-segnali-e-come-difendersi

Eberhart, C. (2023, May 26). Who is watching you? AI can stalk unsuspecting victims with 'ease and precision': Experts. Fox News. https://www.foxnews.com/us/who-is-watching-you-ai-can-stalk-unsuspecting-victims-ease-precision-experts

Europol. 13 arrested in Italy for tricking elderly in love. https://www.europol.europa.eu/media-press/newsroom/news/13-arrested-in-italy-for-tricking-elderly-love

Europol. How not to fall for the "lover boy" scam. Europol. https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/how-not-to-fall-for-lover-boy-scam

Sources

Europol. (2023). Spotlight report: Online fraud schemes. https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf

Europol. (2017). Online sexual coercion and extortion as a crime affecting children. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/sites/default/files/documents/online_sexual_coercion_and_extortion_as_a_form_of_crime_affecting_children.pdf

Federal Bureau of Investigation. (2024, December 3). Criminals use generative artificial intelligence to facilitate financial fraud. https://www.ic3.gov/PSA/2024/PSA241203

Federal Trade Commission. (2023). Romance scammers' favorite lies exposed. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

Federal Trade Commission. Report fraud. https://reportfraud.ftc.gov/

Federal Trade Commission. Avoiding online romance scams. https://www.consumer.ftc.gov

Finney, G. (2023). Project Zero Trust. Cybersecurity Insights. https://www.cybersecurityinsights.com/project-zero-trust

Fintech Global. (2025, February 13). Banks face heightened reputational and financial risks as romance scams surge. https://fintech.global/2025/02/13/banks-face-heightened-reputational-and-financial-risks-as-romance-scams-surge/

Goodwin, L. (2024, December 19). 'AI deepfake romance scam duped me out of £17k'. BBC News. https://www.bbc.co.uk/news/articles/cdr0g1em52go

Sources

Gozzi, L. (2025, January 15). French woman duped by AI Brad Pitt faces mockery online. BBC News. https://www.bbc.co.uk/news/articles/ckgnz8rw1xgo

Howard, R. (2023). Cybersecurity First Principles: A Reboot of Strategy and Tactics. John Wiley & Sons. https://www.wiley.com/en-us/Cybersecurity%2BFirst%2BPrinciples%3A%2BA%2BReboot%2Bof%2BStrategy%2Band%2BTactics-p-9781394173099

Internet Crime Complaint Center (IC3). (n.d.). Romance scams. https://www.ic3.gov/

Interpol. (2022). Interpol report on sextortion trends. International Criminal Police Organization. Retrieved from https://www.interpol.int

Kollmorgen, A. (2025). AI-driven romance scams likely leading to higher losses. Choice. https://www.choice.com.au/electronics-and-technology/internet/using-online-services/articles/romance-scams-and-how-to-avoid-them

Kloess, J. A., Beech, A. R., & Harkins, L. (2014). Online child sexual exploitation: prevalence, process, and offender characteristics. Trauma, violence & abuse, 15(2), 126–139. https://doi.org/10.1177/1524838013511543

Lee, Y., & Gelman, B. (2023, November 27). The dark side of AI: Large-scale scam campaigns made possible by generative AI. Sophos News. https://news.sophos.com/en-us/2023/11/27/the-dark-side-of-ai-large-scale-scam-campaigns-made-possible-by-generative-ai/

Magramo, K. (2024, May 17). British engineering giant Arup revealed as $25 million deepfake scam victim. CNN. https://edition.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk/index.html

Sources

Mattackal, L. P. (2025, February 14). Crypto scams likely set new record in 2024 helped by AI, Chainalysis says. Reuters. https://www.reuters.com/technology/crypto-scams-likely-set-new-record-2024-helped-by-ai-chainalysis-says-2025-02-14/

Narang, S. (2024, February 14). Pig butchering scam: How Bitcoin, Ethereum, Litecoin and spot gold (XAUUSD) investments are used in romance scams to steal hundreds of millions. Tenable. https://www.tenable.com/blog/pig-butchering-scam-bitcoin-ethereum-litecoin-spot-gold-xauusd-romance-scam

National Cyber Security Centre. (2024, January 24). The near-term impact of AI on the cyber threat. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

National Crime Agency [NCA]. (2021). Sextortion threat report. NCA Cybercrime Unit. https://www.nationalcrimeagency.gov.uk

Newcastle University. (n.d.). Online dating scam victims: Psychological impact analysis. https://doi.org/10.54097/ehss.v4i.2740

Newman, L. H., & Burgess, M. (2024, September 30). The pig butchering invasion has begun. Wired. https://www.wired.com/story/pig-butchering-scam-invasion/

Newman, L. H., & Burgess, M. (2025, February 13). The loneliness epidemic is a security crisis. Wired. https://www.wired.com/story/loneliness-epidemic-romance-scams-security-crisis/

Nielson, S. J. (2023). Discovering cybersecurity: A technical introduction for the absolute beginner. Apress. https://doi.org/10.1007/978-1-4842-9560-1

Patchin, J. W., & Hinduja, S. (2020). Sextortion Among Adolescents: Results From a National Survey of U.S. Youth. Sexual abuse : a journal of research and treatment, 32(1), 30–54. https://doi.org/10.1177/1079063218800469

Sources

Patel, M. (2025). Cybersecurity for beginners: Learn practical skills to defend against cyber threats and prepare for certification exams. Michael Patel. ISBN-13: 9798227516435.

pen University. (2024). The psychology of cybercrime. https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-4

Pietilä, E. & Korhonen, H. (5.06.2024). The harsh realities of romance scams. https://nordicwelfare.org/popnad/en/artiklar/the-harsh-realities-of-romance-scams/

Policija.si. (n.d.). Romance scams. Slovene Police. https://www.policija.si/eng/prevention/internet-security/romance-scams

Rege, A. (2009). Tainted love: A systematic literature review of online romance scam research. Interacting with Computers, 21(5-6), 427–437. https://doi.org/10.1016/j.intcom.2009.06.006

Rogiers, A., et al. (2024, November 11). Persuasion with large language models: A survey. arXiv. https://doi.org/10.48550/arxiv.2411.06837

Sanction Scanner. (2024, September 16). How generative artificial intelligence launders money. https://www.sanctionscanner.com/blog/ais-dark-side-how-generative-artificial-intelligence-launders-money-863

ScamWatch. (2024, August 15). Online dating and romance scams. https://www.scamwatch.gov.au/types-of-scams/online-dating-and-romance-scams

SciSpace. (n.d.). Online romance scams: Relational dynamics and psychological insights. https://scispace.com/papers/online-romance-scams-relational-dynamics-and-psychological-5cckseevfj

Sources

Shea, S., & Krishnan, A. (2024). How AI is making phishing attacks more dangerous. TechTarget. https://www.techtarget.com/searchSecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

Shepardson, D. (2024). Consultant fined $6 million for using AI to fake Biden's voice in robocalls. Reuters. https://www.reuters.com/world/us/fcc-finalizes-6-million-fine-over-ai-generated-biden-robocalls-2024-09-26/

Statista. (2025,). Number of fake accounts removed by Facebook per quarter worldwide as of Q1 2025. https://www.statista.com/statistics/1013474/facebook-fake-account-removal-quarter/

Stockwell, S., Hughes, M., Swatton, P., Zhang, A., Hall, J., & Kieran. (2024, November). AI-enabled influence operations: Safeguarding future elections. CETaS Research Reports.

Surrey Police. Romance fraud. Surrey Police. https://www.surrey.police.uk/romancefraud

Tech Report. Romance scam statistics. https://techreport.com/statistics/cybersecurity/romance-scam-statistics/

The Debt Advisor. (2023). Romance scams: A growing threat to both men and women. https://www.thedebtadvisor.co.uk/romance-scams/

The Guardian. (2024). Spanish police arrest five people over fake Brad Pitt scam. https://www.theguardian.com/film/2024/sep/23/spanish-police-arrest-five-people-over-fake-brad-pitt-scam

Sources

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

U.S. Federal Reserve. (2024). Synthetic identity fraud: Generative AI toolkit for payments fraud detection. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

U.S. Immigration and Customs Enforcement. (10.02.2025). Sextortion. https://www.ice.gov/features/sextortion#

United Nations Office on Drugs and Crime. (2024). Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

U.S. Federal Reserve. (2024). Synthetic identity fraud: Generative AI toolkit for payments fraud detection. https://fedpaymentsimprovement.org/wp-content/uploads/sif-toolkit-genai.pdf

Wang, C. (2022). Online Dating Scam Victims Psychological Impact Analysis. Journal of Education, Humanities and Social Sciences, 4, 149-154. https://doi.org/10.54097/ehss.v4i.2740

Wang, F. (2024). Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. International Review of Victimology, 31(1), 91-116. https://doi.org/10.1177/02697580241234331 (Original work published 2025)

Sources

Whitty, M. T., & Buchanan, T. (2016). Do you love me? Psychological characteristics of romance scam victims. Psychological Characteristics of Romance Scam Victims - PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5297105/

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: Causes and consequences of victimhood [PDF]. University of Warwick. https://wrap.warwick.ac.uk/id/eprint/81382/1/WRAP_whitty__buchananpsychological_impact_romance_scam_final_version.pdf

Whitty, M. & Buchanan, T.. (2012). The Online Romance Scam: A Serious Cybercrime. Cyberpsychology, behavior and social networking. 15. 181-3. 10.1089/cyber.2011.0352.

Wrexham.com. (2024, February13). Wrexham man conned out of £25k in romance scam. https://wrexham.com/news/warning-issued-after-wrexham-man-conned-out-of-25k-in-romance-scam-247088.html

Yeung, J. (2024, October 15). Deepfake romance scam raked in $46 million from men across Asia, police say. CNN. https://edition.cnn.com/2024/10/15/asia/hong-kong-deepfake-romance-scam-intl-hnk/index.html

Zhang, D., et al. (2024, February 9). IP-Adapter inpainting: Controllable inpainting with IP-Adapter. arXiv. https://arxiv.org/html/2502.06593v1

Zvelo. (2023, November 8). The role of AI in social engineering. https://zvelo.com/the-role-of-ai-in-social-engineering

Zvelo. (2023, November 8). The role of AI in social engineering. U

Connect with US!

This manual was developed collaboratively by the FALS project coordinators; EUW (Germany), ECREC (The Netherlands), and IVI (Italy).

To stay connected, and in case of any inquiries, comments, or suggestions, Please feel free to reach out to us through the following channels.

ECREC (The Netherlands)

Phone
+31 70 200 2595

Email
info@ecrec.eu

Website
https://ecrec.eu/

EUW (Germany)

Phone
+49 176 55030502

Email
projects@euthwonders.org

Website
www.euthwonders.org

IVI (Italy)

Phone
+39 329 599 7585

Email
igorvitaleinternational@gmail.com

Website
https://www.igorvitale.org/

Co-funded by the European Union