The Comfort Zone Video Research Part 1

Demographics of Women Most Vulnerable to Online Dangers

Online dangers such as romance scams, identity theft, and other cybercrimes affect women across various demographics, but certain groups are disproportionately at risk due to a combination of social, psychological, and technological factors. Below is a summary of the most vulnerable demographics, supported by current research and statistics.

Middle-Aged Women (Ages 45–54 and 50+)

- **Romance Scams:** Multiple sources indicate that middle-aged women-particularly those aged 45–54 or with an average victim age around 50-are among the most frequent victims of romance scams[591020]. These women not only report more cases but also tend to lose more money per incident compared to men or other age groups[2012].
- **Retail and Social Media Scams:** Women in this age range are also the most likely to fall for retail scams, especially those propagated via social media and online forums[5].

Older Women (Ages 65+)

- **General Online Scams:** Older women are particularly vulnerable to a wide range of online scams, including identity theft and financial fraud, due to factors such as social isolation, longer life expectancy, and sometimes lower digital literacy[1317].
- **Financial Losses:** While men in this age group may lose more per incident in some scam categories, women are more frequently targeted and may be more likely to report or recognize victimization[13].

Women from Minority and Marginalized Groups

- **Cybercrime and Identity Theft:** Women who are Black, Indigenous, or people of color (BIPOC) face higher risks of financial impact from cybercrimes and are more likely than white women to have their accounts hacked or identities stolen[2].
- **Non-Financial Cybercrimes:** These women are also more frequently targeted for non-financially motivated crimes, such as cyberstalking, online harassment, and the use of their identity in nonconsensual deepfake pornography[2].

Women with Lower Digital and Financial Literacy

- **Global Perspective:** Across both developed and developing regions, women with lower digital and financial skills are more susceptible to scams, including social engineering, phishing, and identity theft[7].

- **Barriers to Reporting:** Lower literacy and social norms can also discourage women from seeking help or reporting cybercrimes, increasing their vulnerability[7].

Younger Women (Ages 18–39)

- **Phishing and Online Shopping Scams:** Contrary to the stereotype of digital natives being more savvy, women aged 18–39 have high click rates on phishing emails and are susceptible to online shopping and social media scams[38].

- **Underreporting and Awareness:** Young women may underestimate their risk, leading to underreporting and repeated victimization[8].

Summary Table: Most Vulnerable Demographics

Demographic Group	Primary Risks	Notable Factors
Middle-aged women (45–54, 50+)	Romance scams, retail scams	High average losses, frequent targeting
Older women (65+)	General scams, identity theft	Isolation, longer lifespan, lower digital skills
BIPOC and marginalized women	Identity theft, cyberstalking	Higher financial impact, non-financial crimes
Women w/ low digital literacy	Phishing, social engineering	Less access to education, less likely to report
Younger women (18–39)	Phishing, online shopping scams	High click rates, overconfidence in skills

Key Findings

- **Romance scams:** Women are more likely than men to be victims, with middle-aged women especially at risk and suffering higher average financial losses9102012.
- **Identity theft:** Women, particularly those from minority backgrounds or with lower digital skills, face higher risks27.
- **Online harassment and cyberviolence:** Women report higher rates of cyberviolence, harassment, and nonconsensual use of their identity online42.
- **Digital literacy:** Lower digital and financial literacy significantly increases vulnerability, especially among older and marginalized women7.

Conclusion

While all women face some risk from online dangers, the most vulnerable are:

- Middle-aged and older women,
- Women from minority or marginalized backgrounds,
- Those with lower digital or financial literacy,
- And, in certain scam types, younger women who overestimate their cyber-savvy.

Scammers adapt their tactics to exploit the specific vulnerabilities of these groups, making targeted education, support, and improved digital literacy crucial for reducing risk275.

Citations:

1. https://bbbmarketplacetrust.org/wp-content/uploads/2025/02/New-Insights-research-report.pdf
2. https://www.occrp.org/en/news/report-minorities-and-women-are-more-likely-victims-of-cyber-crime
3. https://sosafe-awareness.com/company/press/digital-natives-more-likely-to-open-harmful-phishing-emails-than-their-older-colleagues/
4. https://proprivacy.com/blog/women-and-online-scams-latest-statistics-2022

5. https://www.cyberdaily.au/security/11967-research-middle-aged-women-most-likely-to-fall-for-retail-scams

6. https://www.malwarebytes.com/press/2024/09/25/malwarebytes-research-reveals-10-of-romance-scam-victims-lose-more-than-10000

7. https://www.cgap.org/blog/break-bias-evidence-shows-digital-finance-risks-hit-women-hardest

8. https://www.gridware.com.au/blog/research-finds-young-people-most-likely-to-be-scammed/

9. https://www.reddit.com/r/PurplePillDebate/comments/kep5qw/are_women_more_likely_than_men_to_be_victims_of/

10. https://pmc.ncbi.nlm.nih.gov/articles/PMC5806049/

11. https://www.scamwatch.gov.au/research-and-resources/scam-statistics

12. https://fintech.global/2024/07/30/men-more-likely-to-fall-victim-to-romance-scams-while-women-lose-more/

13. https://www.rbcwealthmanagement.com/en-us/insights/scams-targeting-older-adults-are-on-the-rise-and-women-are-particularly-vulnerableheres-how-you-can-help

14. https://www.sciencedirect.com/science/article/pii/S2949791424000058

15. https://www.cityoflondon.police.uk/news/city-of-london/news/2024/june/heavy-hearts-and-empty-wallets-more-than-94.7-million-lost-to-romance-fraud-in-the-last-year/

16. https://search.proquest.com/openview/8589497f15ae8ea542d6cb3249e7abff/1?pq-origsite=gscholar&cbl=18750

17. https://www.healthyagingpoll.org/reports-more/report/experiences-scams-among-older-adults

18. https://www.statista.com/statistics/1481218/us-online-dating-service-users-scams-by-gender/

19. https://www.ukfinance.org.uk/press/press-releases/over-half-those-looking-love-online-vulnerable-romance-scams

20. https://www.bbc.com/news/business-47176539

Answer from Perplexity: pplx.ai/share

Online Dangers Middle-Aged Women Are Most at Risk For

Middle-aged women face a distinct set of online dangers, shaped by both gendered dynamics and their life stage. The most significant risks include:

1. Technology-Facilitated Gender-Based Violence

- Middle-aged women are especially vulnerable to tech-based abuse, which includes threatening, intimidating, bullying, harassing, humiliating, or coercive behaviors conducted via digital platforms. This abuse is often more severe and longer-lasting for women, with a greater psychological impact than for men[1].
- Sexual harassment and stalking are the most commonly reported forms of technology-facilitated violence. Tactics include unwanted messages, image-based abuse (such as the sharing of intimate photos without consent), doxing (the public release of personal information), and cyberbullying[2].

2. Online Sexual and Gendered Abuse

- Women are more likely to be targets of online sexual harassment, sexism, misogyny, and even sexual assault facilitated through digital means. This can include explicit messages, non-consensual sharing of images, and online defamation[1][2].
- The rise of deepfake technology has increased the risk of manipulated images or videos being used to harm reputations or coerce victims[2].

3. Identity Theft and Impersonation

- Middle-aged women, particularly those with lower digital literacy, are at risk of identity theft and impersonation, which can lead to financial loss and reputational harm[2][3].

4. Online Scams and Fraud

- While not detailed in the specific search results, it is well-established that middle-aged women are frequent targets of romance scams and other financial frauds, often facilitated through social media or dating platforms.

5. Psychological and Social Impact

- Prolonged exposure to online abuse can lead to increased fear for personal safety, depression, and other mental health concerns. Middle-aged women may experience these effects more acutely due to the severity and persistence of the abuse[16].

6. Exclusion and Digital Disadvantage

- Although more pronounced in older women, digital exclusion and lower digital skills can still affect middle-aged women, increasing their vulnerability to scams, misinformation, and exploitation[3].

Summary Table: Key Online Dangers for Middle-Aged Women

Danger Type	Examples/Tactics
Tech-based gendered violence	Harassment, stalking, doxing, deepfakes, sextortion
Sexual and gendered abuse	Explicit messages, image-based abuse, misogyny
Identity theft and impersonation	Account hacking, fraudulent profiles
Online scams and fraud	Romance scams, phishing, financial fraud
Psychological and social impact	Anxiety, depression, fear for safety
Digital exclusion (for some)	Lower digital skills, increased scam risk

Middle-aged women are at heightened risk for a spectrum of online dangers, particularly those rooted in gendered abuse, sexual harassment, and technology-facilitated violence. These risks are exacerbated by social attitudes, digital skill gaps, and the evolving tactics of perpetrators[1][2][3].

Citations:

1. https://www.esafety.gov.au/women/online-risks-for-women

2. https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women
3. https://www.age-platform.eu/the-complex-gender-face-of-digital-exclusion-in-old-age/
4. https://www.france24.com/en/technology/20250308-women-s-and-girls-rights-at-risk-from-uptick-in-online-abuse-says-new-un-report
5. https://pmc.ncbi.nlm.nih.gov/articles/PMC10880227/
6. https://pmc.ncbi.nlm.nih.gov/articles/PMC8954843/

Answer from Perplexity: pplx.ai/share

Yes, there are support groups and specialist services available for women who have experienced technology-facilitated violence. These services are provided by women's rights NGOs, domestic and sexual violence organizations, legal aid groups, and coalitions focused on digital safety.

Types of Support Available

- **Specialist Women's Rights NGOs:** Many NGOs offer counseling, advocacy, and technical support specifically for victims of technology-facilitated violence. These organizations are recognized for their specialist expertise and are considered essential for effective victim support[38].
- **Domestic and Sexual Violence Services:** Traditional domestic violence and sexual assault support services have increasingly adapted to address technology-facilitated abuse, offering both in-person and remote assistance[49].
- **Coalitions and Networks:** Initiatives like the Coalition Against Stalkerware bring together support organizations, security experts, and advocacy groups to share resources and provide technical help to victims of digital abuse[5].
- **International Programs:** Organizations such as UNFPA run global initiatives (e.g., Making All Spaces Safe) that provide survivors with access to social, health, and justice services tailored to technology-facilitated gender-based violence[7].
- **Legal and Psychological Counseling:** Support often includes legal advice, help with reporting to authorities, and psychological counseling to address the trauma associated with online abuse[8].

Access and Barriers

- Many victims do not report incidents due to lack of information, mistrust in institutions, or dissatisfaction with previous responses. However, support services are working to improve accessibility and awareness, including through digital literacy programs and online reporting mechanisms[8].
- National helplines and online complaint systems are increasingly being equipped to handle cases of technology-facilitated violence, ensuring victims can seek help confidentially and safely[8].

Summary

Women experiencing technology-facilitated violence can access support through:

- Women's rights NGOs and domestic violence organizations
- Specialist coalitions like the Coalition Against Stalkerware
- International initiatives (e.g., UNFPA's Making All Spaces Safe)
- National helplines and online reporting platforms

These support groups provide counseling, legal advice, technical assistance, and advocacy, helping survivors recover and navigate the complex challenges of digital abuse[3][4][5][7][8].

Citations:

1. https://help.unhcr.org/portugal/where-to-seek-help/survivors-of-violence/
2. https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women
3. https://rm.coe.int/gec-pc-evio-2024-5-gec-cdpceviodiscussionpaper11sep24-2749-5696-6410-1/1680b1cbf3
4. https://www.anrows.org.au/publication/technology-facilitated-abuse-a-survey-of-support-services-stakeholders/
5. https://www.eeagender.org/the-synergy-network/news/how-can-we-fight-tech-facilitated-violence/
6. https://giwps.georgetown.edu/wp-content/uploads/2024/06/Technology-Facilitated-Gender-Based-Violence.pdf

7. https://www.unfpa.org/TFGBV
8. https://www.undp.org/sites/g/files/zskgke326/files/2024-12/undp-executive-summary-en.pdf
9. https://bdigital.ufp.pt/bitstream/10284/10169/1/2021.%20Remote%20support%20to%20victims%20ofVAW%20and%20DV%20during%20t
10. https://techsafety.ca/files/WSC0701-Tech-Safety-Report-FINAL-EN-web.pdf

---

Answer from Perplexity: pplx.ai/share

Yes, there are online communities and forums where women can share their experiences with technology-facilitated violence, although these spaces often prioritize privacy and safety due to the sensitive nature of the discussions.

Examples and Initiatives

- **Community of Practice on TFGBV:** As highlighted in reflections from the SVRI Forum, there is a growing "Community of Practice" dedicated to technology-facilitated gender-based violence (TFGBV). This community brings together researchers, advocates, and survivors to share experiences, knowledge, and support in a safe environment[3]. While some aspects are research-focused, these spaces often include survivor voices and peer support.
- **Workshops and Forums:** Events such as "The Virtual is Real: A Forum Addressing Technology-Facilitated Gender-Based Violence" provide opportunities for women to connect, share stories, and build solidarity. These forums, sometimes organized by organizations like UNFPA, may have online components or lead to the creation of ongoing online networks[13].
- **Women's Rights and Digital Safety NGOs:** Many NGOs and advocacy groups create private online support groups or forums for survivors of online abuse. While not always publicized for security reasons, these spaces are often accessible through referral or after contacting the organization directly[35].
- **Peer Support and Survivor Networks:** The need for survivor-centered spaces is widely recognized. Research and advocacy groups emphasize the importance of survivor-led conversations and peer support networks, which can take the form of moderated online forums, closed social media groups, or messaging platforms[38].

Privacy and Safety Considerations

Because technology-facilitated violence often involves stalking, harassment, and doxing, these online communities usually:

- Require vetting or invitations to join
- Are moderated by professionals or trained survivors
- Emphasize confidentiality and digital security

How to Find These Communities

- Contact women's rights NGOs, digital safety organizations, or domestic violence services for recommendations or referrals to online support groups.
- Look for announcements from major forums (like SVRI or UNFPA) about ongoing online communities or follow-up networks after public events[1][3].
- Some organizations may advertise closed Facebook groups, encrypted chat channels, or forums on their websites, but access is controlled to protect participants.

Summary

While there is no single, universally recognized public forum for sharing experiences with technology-facilitated violence, multiple online communities, support groups, and survivor networks exist-often linked to NGOs, advocacy groups, or global initiatives. These spaces are designed to provide solidarity, share resources, and amplify survivor voices in a secure environment[3][1][8].

Citations:

1. https://www.unfpa.org/events/the-virtual-is-real
2. https://www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech
3. https://www.svri.org/navigating-the-complex-terrain-of-tfgbv/
4. https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf
5. https://www.unfpa.org/TFGBV
6. https://blogs.icrc.org/law-and-policy/2024/01/04/online-violence-real-life-impacts-women-girls-humanitarian-settings/
7. https://www.unwomen.org/sites/default/files/2022-10/Accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls-en_0.pdf

8. https://www.svri.org/topic-specific-research-agendas/technology-facilitated-gender-based-violence-global-shared-research-priorities/

9. https://www.weforum.org/stories/2015/02/how-to-tackle-gender-based-violence-online/

10. https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-Submission_UNFPA.pdf

---

Answer from Perplexity: pplx.ai/share

Yes, there are several initiatives aimed at educating middle-aged women-and other vulnerable adults-about online safety. These efforts are delivered by governments, NGOs, and online safety organizations, often as part of wider digital literacy or media literacy campaigns.

Notable Initiatives

- **UK Government Media Literacy Strategy:** The UK has invested over £1 million in projects to boost media literacy among vulnerable and hard-to-reach groups, including elderly and middle-aged women. This includes funding for workshops, training courses, and online learning specifically designed to help people spot disinformation, avoid scams, and protect themselves from online abuse. Charities like Internet Matters and Glitch deliver workshops and training for vulnerable and marginalized women, focusing on media literacy and tackling online abuse5.

- **Netsafe (New Zealand):** Netsafe provides free support, advice, and education to people of all ages to promote safe and positive online experiences. Their resources and programs are accessible to middle-aged women and cover topics such as online scams, privacy, and digital wellbeing2.

- **Community-Based Digital Skills Training:** Initiatives like the Leeds Older People's Forum offer digital media skills training both online and in community centers. While some programs specifically mention older adults, they are often open to middle-aged women as well, recognizing the need for lifelong digital learning5.

- **NGO and Charity-Led Workshops:** Organizations such as Glitch run workshops tailored to the needs of marginalized women, including those who are middle-aged, to help them recognize and respond to online threats, abuse, and misinformation5.

- **Best Practice Frameworks:** Resources like the Australian eSafety Commission's Best Practice Framework for Online Safety Education provide guidelines and resources that can be adapted for different age groups, including adults and middle-aged women, to ensure effective online safety education4.

Key Features of These Initiatives

- Focus on media and digital literacy, including recognizing scams, misinformation, and digital abuse.
- Community-based and accessible both online and offline.
- Tailored content for vulnerable and marginalized groups, including women.
- Support from government funding, NGOs, and local organizations.

Summary

Middle-aged women can access a growing range of online safety education initiatives, from government-funded media literacy projects to NGO-led workshops and community digital skills training. These programs aim to empower women with the knowledge and skills needed to navigate online risks safely and confidently[245].

Citations:

1. https://www.mdpi.com/2227-7102/12/10/715
2. https://netsafe.org.nz
3. https://www.unicef.org/eap/media/10946/file/Evaluating%20Online%20Safety%20Initiatives.pdf
4. https://www.esafety.gov.au/educators/best-practice-framework
5. https://www.gov.uk/government/news/help-for-vulnerable-people-to-spot-disinformation-and-boost-online-safety
6. https://assets.publishing.service.gov.uk/media/5a8222f2e5274a2e8ab57aed/Internet_Safety_Strategy_green_paper.pdf
7. https://www.internetmatters.org/about-us/policy-and-research/projects-and-programmes/
8. https://www.sciencedirect.com/science/article/abs/pii/S0160791X21002980

Answer from Perplexity: pplx.ai/share

The Role of Social Media in the Prevalence of Romance Scams Among Women

Social media plays a significant and multifaceted role in the prevalence of romance scams targeting women. Here's how:

1. Easy Access to Personal Information

- Women often share personal details, photos, interests, and even information about friends and family on social media platforms. Scammers exploit this openness to craft highly convincing fake profiles and tailor their approach to the victim's preferences and vulnerabilities, making their schemes more effective147.

2. Initial Contact and Grooming

- Romance scammers frequently initiate contact through popular social media sites like Facebook and Instagram, as well as dating apps. They analyze victims' profiles and self-descriptions to develop approaches that resonate emotionally, often contacting the victim first with personalized messages157.

3. Emotional Manipulation and Trust Building

- Scammers use social engineering tactics-such as love bombing, flirty messages, and promises of a future together-to quickly build trust and emotional bonds. Social media's instant messaging and constant connectivity make it easier for scammers to maintain ongoing, intimate contact, deepening the victim's emotional investment2367.

4. Fabrication of Elaborate Personas

- Social media enables scammers to create and maintain multiple fake identities, complete with photos, fabricated backstories, and even networks of fake friends. These personas are used to establish credibility and authenticity in the eyes of their targets37.

5. Expansion of Victim Pool

- The global reach of social media platforms allows scammers to target women across geographic boundaries, increasing the number of potential victims and making it harder for law enforcement to track and stop these crimes67.

6. Escalation to Financial Requests

- Once trust is established, scammers use the emotional connection to manipulate victims into sending money, often under the guise of emergencies or investment opportunities. Social media's private messaging features make it easier for scammers to escalate these requests without scrutiny246.

7. Underreporting and Stigma

- The emotional manipulation involved, combined with the public nature of social media, can lead to shame and underreporting among women who fall victim, further fueling the cycle of abuse and making it difficult to gauge the true scale of the problem6.

Summary Table: Social Media's Role in Romance Scams

Mechanism	Impact on Romance Scams Targeting Women
Access to personal information	Enables tailored, convincing scams
Platform for initial contact	Facilitates easy, direct outreach to potential victims
Emotional manipulation	Builds trust and deepens emotional investment
Fake personas and networks	Increases scammer credibility and authenticity
Global reach	Expands pool of potential victims
Private messaging	Allows for escalation and secrecy
Stigma and underreporting	Hinders detection and prevention efforts

In summary:
Social media platforms are central to the success and spread of romance scams targeting women, providing scammers with tools to identify, contact, groom, and manipulate victims at scale, while also making detection and prevention more challenging1234567.

Citations:

1. https://www.cybercrimejournal.com/pdf/Koppetal2015vol9issue2.pdf
2. https://www.moonstone.co.za/the-dark-side-of-digital-romance-how-pig-butchering-scams-are-targeting-daters/
3. https://lynxtech.com/blog/romance-scams-a-hidden-danger-in-the-digital-dating-world/
4. https://www.kaspersky.com/resource-center/threats/beware-online-dating-scams
5. https://consumer.ftc.gov/articles/what-know-about-romance-scams
6. https://pmc.ncbi.nlm.nih.gov/articles/PMC7254823/
7. https://www.scamwatch.gov.au/types-of-scams/online-dating-and-romance-scams
8. https://www.ice.gov/about-ice/hsi/news/hsi-insider/romance-scams-protect-yourself
9. https://www.mastercard.com/news/perspectives/2025/what-to-know-about-romance-scams/
10. https://drpress.org/ojs/index.php/EHSS/article/download/2740/2634/2687
11. https://www.staffordshire.police.uk/news/staffordshire/news/2024/february/warning-as-romance-scammers-continue-to-target-vulnerable-and-lonely/
12. https://www.newcastle.edu.au/__data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf
13. https://www.malwarebytes.com/press/2024/09/25/malwarebytes-research-reveals-10-of-romance-scam-victims-lose-more-than-10000
14. https://www.ukfinance.org.uk/press/press-releases/over-half-those-looking-love-online-vulnerable-romance-scams
15. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams
16. https://pmc.ncbi.nlm.nih.gov/articles/PMC5806049/

17. https://www.sciencedirect.com/org/science/article/pii/S1745017920000183
18. https://www.sciencedirect.com/science/article/pii/S2949791423000441
19. https://globalcyberalliance.org/love-at-a-cost/
20. https://www.sciencedirect.com/science/article/pii/S2949791423000131

Answer from Perplexity: pplx.ai/share

Psychological Factors Making Women More Susceptible to Romance Scams

Research identifies several psychological and situational factors that increase women's vulnerability to romance scams:

1. Loneliness and Social Isolation

- Women experiencing loneliness or social isolation-often due to life transitions like divorce, retirement, or bereavement-are more likely to be targeted and fall victim to romance scams[4]. These conditions heighten the desire for companionship, making emotional manipulation by scammers more effective.

2. Emotional Vulnerability and Search for Meaning

- Victims are often emotionally vulnerable or searching for meaning in their lives, which scammers exploit by offering affection, attention, and the promise of a meaningful relationship[2].

3. Impulsivity and Sensation Seeking

- Romance scam victims tend to score higher on impulsivity and sensation-seeking traits. This means they are more likely to make quick decisions under emotional pressure and respond to urgent requests from scammers without thorough consideration[1][2].

4. High Trust and Compliance

- Women who are more trusting, benevolent, and inclined to comply with perceived authority figures are at greater risk. Scammers often present themselves as authoritative or trustworthy figures, leveraging this tendency to gain compliance with requests, including sending money[1][2].

5. Addictive Disposition

- Some victims exhibit addictive tendencies, becoming deeply invested in the ongoing narrative of the scam. The emotional highs and lows can create a cycle similar to gambling addiction, making it difficult for victims to disengage even when warning signs appear1.

6. Denial and Commitment to Consistency

- Many victims struggle to accept they are being scammed, even when presented with evidence. A strong psychological need to maintain consistency with prior commitments leads them to continue the relationship and comply with requests, despite doubts24.

7. Lower Cybersecurity Awareness

- Individuals who believe they lack cybersecurity knowledge are more likely to be victimized, as they may not recognize warning signs or know how to verify the authenticity of online contacts1.

8. Life Transitions and Recent Loss

- Significant life changes-such as the loss of a loved one, divorce, or retirement-can increase susceptibility by creating emotional needs that scammers are adept at exploiting4.

9. Romantic Idealization

- Strong romantic beliefs, such as the idealization of love or the notion of a perfect partner, are linked to increased risk. These beliefs can cloud judgment and make individuals more receptive to a scammer's advances5.

Summary Table: Key Psychological Factors

Factor	How It Increases Susceptibility
Loneliness/social isolation	Heightens need for connection and emotional support
Emotional vulnerability	Makes manipulation and love-bombing more effective
Impulsivity/sensation seeking	Leads to quick, less-considered decisions

High trust/compliance	Increases likelihood of believing and helping scammer
Addictive disposition	Creates difficulty in breaking off the relationship
Denial/need for consistency	Keeps victims engaged despite warning signs
Low cybersecurity awareness	Reduces ability to spot scams
Life transitions/loss	Amplifies emotional needs and openness to new contacts
Romantic idealization	Encourages belief in scammer's fabricated persona

In summary, women are more susceptible to romance scams when they experience loneliness, emotional vulnerability, impulsivity, high trust, addictive tendencies, denial, low cybersecurity awareness, significant life changes, and strong romantic idealization. Scammers skillfully exploit these psychological factors to build trust, manipulate emotions, and ultimately defraud their victims[1][2][4][5].

Citations:

1. https://pmc.ncbi.nlm.nih.gov/articles/PMC5806049/
2. https://theconversation.com/brad-pitt-online-romance-fraud-shows-how-victims-are-influenced-by-complex-psychological-factors-247875
3. https://www.sciencedirect.com/org/science/article/pii/S1745017920000183
4. https://www.finextra.com/blogposting/27754/the-definitive-guide-to-prevent-romance-scams
5. https://www.sciencedirect.com/science/article/pii/S2949791423000131

Answer from Perplexity: pplx.ai/share

Yes, specific life events can make women more vulnerable to romance scams. Research and victim reports consistently highlight the following life circumstances as increasing susceptibility:

- **Bereavement and Widowhood:** Women who have recently lost a spouse are particularly vulnerable. The emotional impact of bereavement can lead to loneliness and a heightened desire for companionship, making them prime targets for scammers who exploit their need for connection[156].

- **Divorce or Relationship Breakdown:** Women going through a divorce or the end of a significant relationship may experience emotional upheaval and seek new relationships online, increasing their risk of falling victim to romance scams[135].

- **Loneliness and Social Isolation:** Life stages or events that lead to increased isolation-such as children leaving home (empty nest), retirement, or relocation-can leave women feeling lonely and more open to online advances from strangers[235].

- **Major Life Transitions:** Any significant transition, such as retirement or moving to a new area, can disrupt social networks and routines, making women more susceptible to the emotional manipulation used by romance scammers[35].

- **Recent Trauma or Loss:** Women with a history of trauma, insecure attachment, or low self-esteem-often stemming from earlier life events or abusive relationships-are more likely to form intense emotional bonds with scammers, mistaking manipulation for genuine affection[5].

- **Periods of Increased Online Activity:** Times of year when people are more likely to feel lonely, such as between Christmas and Valentine's Day, see a spike in romance scam activity, as scammers take advantage of seasonal vulnerabilities[2].

In summary, women are most at risk of romance scams during or after events that cause emotional vulnerability, loneliness, or significant change in their lives. Scammers deliberately seek out those experiencing these circumstances, knowing they are more likely to respond to offers of affection and companionship[12356].

Citations:

1. https://www.reddit.com/r/PurplePillDebate/comments/uebm4w/why_are_women_more_likely_to_be_victims_of/

2. https://www.staffordshire.police.uk/news/staffordshire/news/2024/february/warning-as-romance-scammers-continue-to-target-vulnerable-and-lonely/

3. https://globalcyberalliance.org/love-at-a-cost/

4. https://www.ukfinance.org.uk/press/press-releases/over-half-those-looking-love-online-vulnerable-romance-scams

5. https://www.buckley-law.com/articles/romance-scams-elderly/

6. https://www.reddit.com/r/aspergers/comments/1fbpxuc/why_are_women_more_likely_to_fall_for_online/

7. https://pmc.ncbi.nlm.nih.gov/articles/PMC7254823/

8. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed

---

Answer from Perplexity: pplx.ai/share

Life Transitions That Make Women More Vulnerable to Romance Scams

Certain life transitions significantly increase women's vulnerability to romance scams, primarily because these events often lead to emotional upheaval, loneliness, or social isolation-conditions that scammers are adept at exploiting.

Key Life Transitions Linked to Increased Risk

- **Bereavement (Loss of a Loved One):**
- Women who have recently lost a spouse or partner are at heightened risk. The emotional impact of bereavement can create a strong desire for companionship, making them more susceptible to scammers offering affection and support[2][3][6].

- **Divorce or Relationship Breakdown:**
- Women experiencing a recent divorce or separation may feel isolated or eager to rebuild their social and romantic lives. Scammers exploit this vulnerability by presenting themselves as understanding and attentive partners[2][3][6].

- **Retirement:**
- Transitioning into retirement can disrupt daily routines and social circles, leading to increased feelings of loneliness and more time spent online-both factors that can make women more likely to respond to online advances from strangers[3].

- **Children Leaving Home (Empty Nest):**
- When children move out, women may experience a sense of loss or emptiness, increasing their openness to new relationships and online interactions[3].

- **Relocation or Moving to a New Area:**
- Moving away from established support networks can lead to social isolation, making women more likely to seek connection online[3].

- **Health Challenges or Caregiving Responsibilities:**

- Health issues or the demands of caregiving can restrict social engagement, increasing reliance on online communication and the risk of encountering romance scammers[3].

Why These Transitions Matter

Scammers specifically target individuals going through these transitions because:

- **Emotional vulnerability** makes victims more open to new relationships and trusting of strangers.
- **Loneliness and isolation** can cloud judgment and increase the desire for companionship.
- **Disrupted routines** often mean more time spent online, where scammers are most active.

Supporting Evidence

- Studies and expert analysis consistently show that people undergoing significant life transitions-especially bereavement and divorce-are more susceptible to romance scams[1,2,3,6].
- Middle-aged and older women, who are more likely to experience these transitions, are frequently targeted and tend to report higher financial and emotional losses from such scams[3,6].

In summary:
Life transitions such as bereavement, divorce, retirement, children leaving home, relocation, and health challenges make women more vulnerable to romance scams by increasing emotional need, loneliness, and online activity-all factors that scammers exploit[1,2,3,6].

Citations:

1. https://globalcyberalliance.org/love-at-a-cost/
2. https://www.moodys.com/web/en/us/kyc/resources/insights/swipe-left-on-fraud-risk-detecting-and-deterring-romance-scams.html
3. https://www.finextra.com/blogposting/27754/the-definitive-guide-to-prevent-romance-scams
4. https://www.ukfinance.org.uk/press/press-releases/over-half-those-looking-love-online-vulnerable-romance-scams

5. https://www.newcastle.edu.au/__data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf

6. https://www.buckley-law.com/articles/romance-scams-elderly/

7. https://www.sciencedirect.com/science/article/pii/S2949791423000131

Answer from Perplexity: pplx.ai/share

Safety Measures for Women to Protect Against Romance Scams During Life Transitions

Life transitions-such as bereavement, divorce, retirement, or moving-can increase emotional vulnerability, making women prime targets for romance scams. Here are concrete safety measures to help protect yourself during these periods:

1. Guard Your Personal Information

- **Limit what you share online:** Avoid posting personal details (like your full name, address, place of work, or daily routines) on social media and dating profiles. Scammers use this information to build convincing stories and manipulate you56.

- **Set social media to private:** Only allow people you know to follow or friend you. Regularly review your followers and remove anyone you don't know personally56.

2. Recognize Red Flags

Be alert for these common scam tactics:

- **Quick requests to move off dating platforms** (to WhatsApp, email, etc.)-scammers want to avoid detection by site moderators35.

- **Too good to be true profiles:** Overly attractive photos, vague or inconsistent details, and professions that require frequent travel (military, oil rig, etc.) are common scammer hallmarks5.

- **Love bombing:** Excessive flattery and rapid declarations of love or commitment35.

- **Excuses to avoid meeting in person:** Canceled plans, claims of being abroad, or last-minute emergencies35.

- **Requests for money or financial help:** Any request for money, gift cards, or help with "emergencies" is a major red flag3578.

3. Verify Identities

- **Reverse image search:** Use tools like Google's reverse image search to check if their profile photos appear elsewhere on the internet (often linked to other identities or scam reports)15.
- **Ask specific questions:** Request details about their local area or experiences. Scammers often can't provide convincing answers to specific or personal questions5.
- **Request real-time video calls:** Be wary if they refuse or make excuses to avoid video chats or sharing candid, real-time photos9.

4. Involve Trusted People

- **Share your experience:** Talk to a trusted friend or family member about your new online relationship. Outsiders can often spot red flags that are harder to see when emotionally involved57.
- **Listen to concerns:** If loved ones, your bank, or authorities warn you about a relationship, take their advice seriously7.

5. Never Send Money or Share Financial Details

- **Never send money to someone you haven't met in person:** No matter how convincing the story, this is the most common way victims are exploited78.
- **Don't share financial or sensitive information:** Never provide your bank details, passwords, or copies of personal documents8.

6. Pause and Reflect

- **Take your time:** Don't let anyone pressure you into making quick decisions about your relationship or finances. Genuine partners will respect your boundaries and timeline7.

7. Use Reputable Platforms

- **Stick to well-known dating sites:** These platforms often have better security and fraud detection measures than informal social media or messaging apps14.

8. Educate Yourself

- **Stay informed:** Learn about common scam tactics and keep up to date with new trends in online fraud. Awareness is a powerful defense56.

Summary Table: Key Safety Measures

Safety Measure	Why It Matters
Limit personal info online	Reduces scammer's ability to manipulate you
Recognize red flags	Early detection prevents deeper emotional/financial harm
Verify identities	Exposes fake profiles and stories
Involve trusted people	Provides objective perspective and support
Never send money/share financial info	Prevents direct financial loss
Pause and reflect	Counters emotional manipulation and pressure tactics
Use reputable dating platforms	Lowers risk of encountering scammers
Stay informed	Keeps you prepared for evolving scam tactics

In summary:
Staying vigilant, involving trusted people, limiting what you share online, and never sending money are critical steps to protect yourself from romance scams-especially during emotionally vulnerable life transitions13578.

Citations:

1. https://globalcyberalliance.org/love-at-a-cost/
2. https://www.ice.gov/about-ice/hsi/news/hsi-insider/romance-scams-protect-yourself

3. https://www.aarp.org/money/scams-fraud/romance/

4. https://www.finextra.com/blogposting/27754/the-definitive-guide-to-prevent-romance-scams

5. https://www.rbcroyalbank.com/en-ca/my-money-matters/money-academy/cyber-security/cyber-security-for-business/how-to-protect-yourself-from-romance-scams/

6. https://www.mcafee.com/learn/romance-scams/

7. https://nedbankprivatewealth.com/insights/how-to-stay-safe-from-romance-scams/

8. https://www.secretservice.gov/investigations/romancescams

9. https://www.bankerslife.com/insights/life-events/romance-scams-6-tips-to-prevent-financial-ruin/

Answer from Perplexity: pplx.ai/share

How Women Can Verify the Identity of Someone They Meet Online

Verifying the identity of someone you meet online is essential for safety, especially in the context of dating and potential romance scams. Here are practical, expert-backed steps women can take:

1. Search for a Digital Footprint

- **Google their name and details:** Look up their full name, workplace, school, and other personal information. Cross-check these details across multiple sources to see if they're consistent and legitimate456.

- **Check social media profiles:** Review their social media accounts for authenticity. Look for a history of posts, interactions with friends, and photos over time. A lack of any digital footprint is a red flag45.

2. Use Reverse Image Search

- **Google Reverse Image Search:** Upload their profile photos to Google Images or similar tools to see if those images appear elsewhere-such as stock photo sites or unrelated social media profiles. This can reveal if their photos are stolen or used in multiple places56.

3. Ask for Real-Time Interaction

- **Video calls:** Request a video chat early in your conversations. Scammers often avoid video calls or make excuses to not appear on camera[15].

- **Voice calls:** Speaking on the phone can also help, but video is more reliable for confirming appearance and identity[1].

4. Verify Details in Person (When Safe)

- **Meet in public:** Arrange to meet in a public place. Subtle checks, like matching their appearance to their photos or noting the name on a credit card, can provide extra reassurance[1].

- **Ask for corroborating information:** If comfortable, you can ask for social media handles, or even see a driver's license in person. Never ask or send ID images online, as this can be risky for both parties[14].

5. Watch for Red Flags

- **No online presence:** If you can't find any information about them online, be cautious[45].

- **Inconsistent stories or evasiveness:** If their details don't add up or they avoid direct answers, this is a warning sign[5].

- **Refusal of video or in-person meetings:** Consistent avoidance of real-time interaction is a major red flag[5].

6. Use Platform Verification Tools

- **Check for verification badges:** Some dating apps offer ID or photo verification features. Verified profiles are generally safer, but still use caution as verification is not always mandatory or foolproof[23].

Summary Table: Verification Steps

Step	What to Do	Why It Matters
Search digital footprint	Google name, check social media	Confirms consistency and authenticity
Reverse image search	Upload profile photos to Google Images	Detects stolen or fake photos

Video/voice call	Request a real-time video chat	Confirms appearance and liveness
Meet in public	Compare appearance, check subtle details	Adds another layer of verification
Use app verification	Look for verification badges	Indicates some level of screening
Watch for red flags	Note avoidance, inconsistencies, no presence	Helps spot potential scams

In summary:
Women can protect themselves by cross-checking online information, using reverse image searches, insisting on video calls, meeting in public, and leveraging app verification features. Always remain alert to red flags and never share sensitive documents or financial information online[1][2][3][4][5][6].

Citations:

1. https://www.reddit.com/r/datingoverforty/comments/1d79b5n/how_do_you_verify_identity_of_someone_from_old/
2. https://regulaforensics.com/blog/online-dating-identity-verification/
3. https://www.incognia.com/use-case/online-dating-identity-verification
4. https://www.forbes.com/sites/alysonkrueger/2014/04/30/the-best-ways-to-research-someone-you-meet-online/
5. https://www.aura.com/learn/how-to-spot-a-scammer-on-a-dating-site
6. https://www.snbonline.com/about/news/how-to-detect-an-online-romance-scam
7. https://www.esafety.gov.au/lgbtiq/learning-lounge/meeting-online/impersonation-catfishing-identity-theft

---

Answer from Perplexity: pplx.ai/share

Does Facebook Use Information from Private Groups for Advertising Algorithms?

Direct Use of Private Group Content

Facebook does not allow advertisers to directly target users based on the *specific content* they share within private groups. The platform does not make private group posts or discussions available for ad targeting through its official advertising tools234. This means that what you write or share inside a private group is not directly scanned and used for ad personalization in the same way as public posts or profile information.

Indirect Use: Group Membership and Behavioral Inference

However, Facebook does use *behavioral signals*-including group membership and engagement-as part of its broader profiling and ad targeting system. Here's how this works:

- **Ad Preferences and Inferred Interests:** Facebook assigns users "ad preferences" based on their activity across the platform, which can include joining or engaging with groups. These inferred interests are then used to categorize users for advertising purposes, sometimes even relating to sensitive topics16. For example, if you join a group about a specific health condition or political topic, Facebook may infer your interest in that area and show you related ads16.

- **Advertiser Targeting:** Advertisers can target users based on these inferred interests, but not by directly selecting members of a specific private group through Facebook's ad manager16.

- **Third-Party Tools:** Some third-party tools (like LeadEnforce or Phantom Buster) claim to allow advertisers to scrape group member data (even from private groups) to create custom audiences for ads234. However, this practice is not officially sanctioned by Facebook, may violate its terms of service, and can pose privacy and ethical concerns4.

Sensitive Data and Privacy Concerns

Research shows that Facebook labels a significant portion of its users with potentially sensitive ad preferences, often inferred from their activity without explicit consent16. While these preferences can be based on group engagement, the actual content of private group discussions is not directly used for ad targeting.

Summary Table: Facebook Group Data and Advertising

Data Type	Used by Facebook for Ads?	Notes
Private group content	No	Not directly scanned for ad targeting
Group membership/engagement	Yes (indirectly)	Used to infer interests for ad preferences
Third-party group data scraping	Not officially	Possible via external tools, but violates Facebook's terms

Conclusion

- Facebook does not directly use the information people share in private groups for advertising algorithms.
- The platform does use signals like group membership and engagement to infer interests, which can be used for ad targeting[16].
- Some third-party tools can scrape group member data for ad targeting, but this is not officially supported and may breach privacy rules[234].

In summary, while your private group discussions are not directly used for ads, your participation in those groups can influence the types of ads you see through inferred interests and ad preferences.

Yes, your understanding and Perplexity's summary are spot on. While Facebook private groups offer a degree of controlled access and privacy compared to public posts, they are **not absolutely private or inherently "safe" in the truest sense of the word, especially for highly sensitive information and vulnerable individuals.**

Here's a breakdown of why and what it means for your course:

Why Facebook Private Groups Aren't Fully "Safe":

1. **Facebook's Access (The Big One):**
   - As Perplexity stated, **Facebook (Meta) retains access to all content posted in any group, private or not.** Their algorithms scan content for policy violations, and

theoretically, their employees could access it under certain circumstances (e.g., legal requests, investigations). This means true confidentiality from the platform itself doesn't exist.

2. **Member Behavior & Trust:**

- **Screenshots & Sharing:** A member can easily screenshot posts or copy text from a private group and share it outside the group. There's no technical way to completely prevent this. The "privacy" relies heavily on the trust and integrity of all members.

- **Malicious Intent:** Someone could join a private group under false pretenses to gather information, troll, or exploit members. While admins can vet, it's not foolproof.

- **Accidental Sharing/Misunderstanding Rules:** Members might not fully understand the group's privacy expectations or accidentally share information inappropriately.

3. **Technical Vulnerabilities & Data Breaches:**

- While Facebook invests heavily in security, no platform is immune to bugs, vulnerabilities, or large-scale data breaches that could expose group content, however unlikely for a specific group's data.

4. **Admin Power & Responsibility:**

- The safety and privacy of the group heavily depend on proactive, diligent admins who set clear rules, vet members, monitor discussions, and remove problematic content or individuals. This is a significant responsibility.

5. **Changes in Facebook Policy:**

- Facebook's terms of service and privacy policies can change, potentially impacting how group data is handled in the future.

What This Means for Your Course & Your "Safe Community":

1. **You Can Still Teach About FB Groups (Realistically):**

- Many grieving individuals will seek support in Facebook groups because they are accessible and widely used. It would be unrealistic to ignore them.

- Your role is to educate your students on **how to engage with Facebook groups as safely as possible**, understanding the inherent limitations.

2. **Your Teaching Points for FB Groups Should Include:**

- **Understanding the Limits of "Private":** Explain what we just discussed – Facebook's access, risk of member sharing.

- **How to Vet a Group:** Look for clear rules, active and engaged admins, a focus on supportive interaction, how long the group has existed, and the general tone of discussions.

- **Personal Sharing Boundaries:** Advise caution about sharing extremely sensitive personal identifying information (PII) even in private groups. Encourage them to think about what they would be comfortable with if it were somehow shared outside the group.

- **Using Facebook's Privacy Settings:** Remind them to manage their own overall Facebook privacy settings.

- **Recognizing Red Flags:** Teach them to spot signs of an unsafe group (e.g., lack of moderation, prevalence of spam/scams, members being attacked, pressure to buy things).

- **The "Screenshot Rule":** Assume anything posted could potentially be screenshotted.

3. **Positioning YOUR Community (The Comfort Zone) as a Safer Alternative/ Complement:**

- This is where your own dedicated community space gains even more value. You can highlight how it offers a different level of privacy or control because it's not on a massive social media platform where data is the core business model.

- While no online space is 100% invulnerable, a platform like The Comfort Zone, when used for a private, paid community, offers:
- **Less Data Mining:** The platform's business model is usually selling access to the platform, not monetizing user data in the same way Facebook does.

- **More Control for You:** As the owner, you have more direct control over members, content, and the environment.

- **Higher Barrier to Entry (Potentially):** If it's linked to a paid course or membership, there's a financial commitment, which can deter casual troublemakers.

- **Focused Purpose:** The community is solely dedicated to your specific topic, unlike Facebook which is a multi-purpose platform.

4. **Transparency is Key:** Be honest with your students about the pros and cons of different online spaces.

In summary: You're right. Facebook private groups offer a layer of privacy but are far from foolproof "safe spaces." Your course will equip students with the knowledge to navigate them wisely and understand the risks. This also strengthens the value proposition for the dedicated, more controlled community space you plan to offer. You're not saying "never use Facebook groups," but rather "here's how to use them more safely, and here's an alternative we're building together that aims for an even higher level of trust and focus."

Catfishing Victimization Among Bereaved Women

No specific research or statistics directly quantify the number or proportion of bereaved women who are victims of catfishing. Available data focuses on broader victim demographics and general vulnerability factors.

Key findings from available research:

- **Women are more likely than men to be victims of catfishing.** Some sources report that up to 85% of catfishing victims are women69.
- **Catfishing frequently targets emotionally vulnerable individuals,** including those experiencing grief or recent loss, but no studies directly measure rates among bereaved women specifically26.
- **Romance scams and catfishing are on the rise:** In 2021, romance fraud losses in the US reached $956 million, with women representing the majority of victims9.
- **Older adults, including widows, are disproportionately affected financially:** Victims aged 70+ lost a median of $9,000 per incident, far higher than younger groups59.
- **Bereavement increases vulnerability:** While not specific to catfishing, studies note that bereaved individuals-especially widows-experience significant emotional distress, which may increase susceptibility to online scams8.

Summary Table: Catfishing Victim Demographics

Group	Percentage of Victims	Notable Trends
Women	Up to 85%	Most likely to be targeted69
Men	~15%	More likely to perpetrate catfishing69
Bereaved Women	Not specified	Higher vulnerability, but no direct statistics

Older Adults (70+)	Not specified	Highest median financial losses[5][9]

Conclusion:
While bereaved women are likely at elevated risk of being catfished due to emotional vulnerability, **no direct statistics currently quantify this subgroup**. The majority of catfishing victims are women, and older women (including widows) suffer the greatest financial losses, but more targeted research is needed to determine the exact prevalence among bereaved women

Common Tactics Used by Catfishers Targeting Bereaved Women

Emotional Manipulation and Rapid Intimacy

- Catfishers often "love bomb," showering victims with affection and attention to quickly build trust and emotional bonds, making bereaved women-who may be seeking comfort-especially vulnerable[3][4][5].

- They may mirror the victim's interests and values, creating a false sense of compatibility[3].

Exploiting Vulnerability

- Catfishers target emotional pain, offering empathy and understanding to gain trust, then gradually escalate the relationship[6].

- They may claim to have experienced similar losses to appear relatable and deepen the emotional connection.

Fake Identities and Stolen Photos

- Scammers use stolen or AI-generated photos to create convincing online personas, sometimes posing as attractive or successful individuals[7].

- They may pretend to be someone from the victim's past or a new romantic interest, often with a compelling backstory[7].

Avoiding Real-Life Contact

- Catfishers avoid video calls or in-person meetings, making excuses or canceling plans repeatedly to maintain the deception[4][5][6].

- They often ask to move conversations off dating platforms to less regulated channels[6].

Financial Requests and Blackmail

- After establishing trust, scammers invent emergencies (medical, travel, legal) and request money, sometimes starting with small gifts and escalating to larger sums[467].
- Some may solicit intimate photos and later use them for extortion or blackmail[48].

Isolation and Gaslighting

- Catfishers may encourage victims to distance themselves from friends and family, increasing dependency on the scammer and making it harder for others to intervene[3].
- They manipulate victims into doubting their own judgment, making them more susceptible to ongoing deception[3].

Summary Table: Tactics and Red Flags

Tactic	Description
Love bombing	Overwhelming affection and attention early on
Mirroring	Imitating interests and values
Fake identity/photos	Using stolen or AI-generated images and stories
Avoiding real contact	Excuses to avoid video calls or meetings
Financial/emergency requests	Requests for money after building trust
Soliciting intimate photos	Later used for blackmail or extortion
Isolation and gaslighting	Undermining support networks and distorting reality

Bereaved women may be especially at risk due to their emotional state and desire for connection, making these tactics particularly effective

https://vpnalert.com/resources/catfishing-statistics/

The website above has some alarming facts and figures with regards to catfishing-statistics from just a few years ago. It's likely that the figures given in this article have significantly increased since then.

I won't go into detail of all of them but what I@m about to tell you next will give you some idea of the huge amounts of money being extorted through catfishing...

Romance scams and catfishing are on the rise: In 2021, romance fraud losses in the US reached $956 million, with women representing the majority of victims but research suggests that only 2.8% of romance scams were reported in 2021. The total loss was projected to surpass $526 billion if all romance scams had been reported. (Source)

The average loss to online catfish scammers increases with age. In 2021, people aged 70 and older reported the highest individual median loss to catfish scammers at $9,000.

Age Median reported losses 50 to 59 $4,000 60 to 69 $6,000 70 and over $9,000 (Source)

Long-Term Emotional Impacts of Catfishing on Bereaved Women

Profound Emotional Distress

- Victims often experience intense feelings of betrayal, heartbreak, and humiliation after discovering the deception, which can be especially severe for bereaved women seeking connection and support235.

Trust Issues and Relationship Difficulties

- Catfishing can shatter a victim's ability to trust others, making it difficult to form new relationships-romantic or otherwise. This mistrust can persist for years and extend to friends and family235.

Anxiety, Depression, and PTSD

- Long-term psychological effects may include chronic anxiety, depression, and symptoms similar to post-traumatic stress disorder, driven by the emotional violation and loss456.

Social Isolation and Withdrawal

- Shame, embarrassment, and fear of judgment often lead victims to withdraw from social situations, increasing feelings of loneliness and isolation, which can be particularly acute for those already grieving35.

Loss of Self-Esteem and Identity

- Many victims struggle with self-doubt, low self-esteem, and even identity crises, questioning their judgment and feeling exploited or foolish for having been deceived35.

“Double Whammy” Trauma

- Bereaved women may experience a compounded sense of loss: mourning both the original bereavement and the betrayal of the catfishing scam, sometimes described as a “double whammy” of trauma2.

These impacts can linger long after the incident, affecting mental health, social life, and the ability to trust and connect with others

There are currently **no widely available courses specifically focused on online safety and digital wellbeing for bereaved women**. Most bereavement training courses, such as those from Winston's Wish, Flexebee, and others, focus on understanding grief, supporting the bereaved, and providing compassionate care, but do not address digital safety or catfishing risks123568.

Your proposed course would fill a unique gap by combining bereavement support with practical digital safety skills tailored for bereaved women-a need not met by existing offerings

Having basic protection in place from anti-virus software and firewalls isn't enough to support your safety, in an environment where criminals are becoming more sophisticated all the time.

For example, have you noticed that many of the scammer emails you receive now are way more sophisticated than scammer emails of years past?

Not only is the language more grammatically correct, but they are also using graphics and email layouts very similar to the companies that they're trying to portray in order to get you to click on a link and submit personal information.

The Rise of Phishing

Phishing has been a persistent problem in the cybersecurity landscape for some time. The chances are that this issue will continue to plague the digital landscape in the years to come.

Cybercriminals have proven that there are no limits to what they're willing to do to get their hands-on valuable consumer data. **In the years to come, phishing strategies will only become more intelligent.**

With more people spending the majority of their time online for work and play, there's no doubt that criminals will find plenty of inspiration in the digital world to help them cheat their victims out of their information.