INCOGNIA

How to avoid romance scams and increase trust and safety in dating apps

A country of people looking for a match:

Mobile dating apps had over **323 million** users worldwide in 2021[1]

If all dating app users were a country's population, it would be the 4th most populated country globally, behind China, India, and the US.

"The next valentine's day gift is on me!"

The worldwide revenue of dating apps in 2021 came to **$5.61 billion**. That sum could pay for a **$45** gift for all of the **122 million** singles in America.

Globally, revenue from dating services is projected to reach **US$7.88 billion** in 2023, **71%** of which is projected to come from the US alone.

It's a big thing in the US

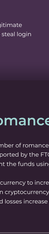
Mobile dating apps had 53 million users in the US in 2020, and 3 out of 10 US adults said they have already used a dating app.[2]

US dating app market share 2021[3]

[1] Business of Apps - Dating App Revenue and Usage Statistics 2022 [2] Statista - Online Dating - United States
[3] Business of apps - Dating App Revenue and Usage Statistics (2022)

The dating scams

Romance scams are rapidly becoming one of the most common forms of cyber-fraud. Victims often think they have found a real, romantic connection only to discover that their "partner" is actually trying to manipulate them into transferring money or disclosing information. Protect yourself by learning all you can about the telltale signs of dating fraud and stay vigilant when meeting new people.



Online dating has the potential to create meaningful relationships, but unfortunately bad actors use the platforms to find vulnerable targets.

Most common dating scams include:

Catfishing
When scammers create fake profiles and pretend to be someone else to trick their victims into sending them money or disclosing personal information.

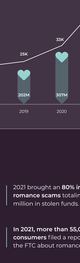
Romance scams
Bad actors build a fake relationship with their victim, often over a long period of time, and consistently ask for money for various reasons such as travel expenses or emergency situations.

Phishing scams
Involve sending messages or links that appear to be from a trustworthy source and ask the victim to enter their login information, which the scammer then uses to access their accounts and steal money and personal information.

Money-laundering scams
Involve ask the victim to receive and then forward large amounts of money, often as part of a larger money-laundering scheme.

Photo scams
Coerce unsuspecting users into sending sensitive information in exchange for intimate images that are never sent.

Malware
Scammers send unsuspecting victims seemingly legitimate websites that actually include malware code used to steal login and financial information.



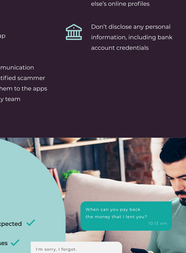
The cost of romance scams

According to the FTC[4], the US saw a record number of romance scams reported in 2021 equaling $547 million in fraud losses. Each occurrence reported by the FTC averaged about $2,400, and 25% of the time, the victim sent the funds using gift cards.

More recently, fraudsters have looked to cryptocurrency to increase their returns. The FTC reports that $139 million of these losses were paid out in cryptocurrency and that when cryptocurrency is the payment method, the average fraud losses increase to approximately $10,000.

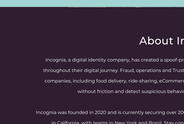
Romance scams are increasing: Growth over five years[4]

The number of reported romance scams grew 3 times over the last five years and the reported losses in 2021 were 6 times what was reported in 2017.



Romance scams and catfishing are on the rise

While 98% of dating app users claim to be truthful



say they have been "catfished" by users pretending to be someone they are not.

2021 brought an **80% increase in romance scams** totaling $547 million in stolen funds.

In 2021, more than 55,000 consumers filed a report with the FTC about romance scams.[4]

According to the FBI, confidence or romance scams cost individuals nearly **$1 billion in 2021,** making it the internet crime with the third highest losses that year.[5]

[4] Federal Trade commission - Reports of Romance Scams Hit Record Highs in 2021 [5] FBI - Internet Crime Report 2021

How does a romance scam work?

01
The scammer creates multiple accounts using fake personal information and starts searching for targets

02
They then invest in establishing an emotional connection with one or multiple legitimate daters

03
Once trust is established with their target(s), the scammer will attempt to manipulate them into sending money, often before they have ever meet in person

04
If successful, the scammer may continue the relationship hoping to receive more payments like this or ghost that user by blocking them or deactivating their account

05
They will likely execute the same scam again by hiding behind a different account and identity

Protecting against romance scams

Protecting users against romance scams is critical for dating apps to maintain trust and safety and avoid brand reputation damage. Verifying the identity of new users is crucial to this effort. In addition to traditional verification methods, dating apps should also leverage location verification software to cross-reference their behavior against the identity documentation they provide.

The FTC provides users with helpful tips to avoid romance scams such as:

- Ask questions and look for inconsistent answers
- Talk to someone you trust about your love interest
- Use an online reverse image search to find out if the person's photos are on anyone else's online profiles
- Think twice before providing any monetary help
- Schedule a video call asap
- Don't disclose any personal information, including bank account credentials
- Be cautious about sharing personal pictures that can be used for bribery
- Stop all communication with an identified scammer and report them to the apps Trust & Safety team

Trust your gut if

- They seem too good to be true
- They declared their love for you much more quickly than you expected
- They asked you for money, perhaps for medical or travel expenses
- They have never met you in person
- They have shared inconsistent information about themselves

Learn more about how to prevent and detect romance scams with location identity by Incognia.

Identity Verification →

About Incognia

Incognia, a digital identity company, has created a spoof-proof Location Identity to silently authenticate customers throughout their digital journey. Fraud, operations and Trust & Safety teams at global gig economy and marketplace companies, including food delivery, ride-sharing, eCommerce and more, use Incognia to authenticate trusted users without friction and detect suspicious behavior to prevent new account fraud and ATO.

Incognia was founded in 2020 and is currently securing over 200M devices. It is a venture-backed company headquartered in California, with teams in New York and Brazil. Stay connected and follow Incognia on **Twitter** and **LinkedIn.**

Visit **incognia.com** to learn more.