

Catfishing and Romance Scams

How to Identify and Avoid Them

What are catfishing and romance scams?

Catfishing is luring prey into a relationship by means of a fictional online persona ... for purposes of exploitation (getting money, stealing identity, money laundering). This is done on dating sites but also other social media (Facebook, Instagram, etc.), as well as, and more and more, in person.

Romance scammers are highly motivated, extremely SKILLED, manipulative con artists and often criminals. There are scripts the scammers can follow, and yes you can google them, although many are skilled enough to make modifications to adapt to their prey's vulnerabilities. Romance scammers create false intimacy to build trust with their prey so that they feel comfortable complying with the scammer's exploitation. For many scammers, their job and therefore their ability to provide for their extended family, depends on their ability to successfully exploit their prey, in some cases in order to fulfill quotas.

Love bombing is when someone you've just met showers you with attention and affection for purposes of false intimacy used to gain trust, control and exploitation. The love bomber might shower you with compliments, gifts and make profound declarations of love quickly. They might even say that they have never been this way with anyone else, which can make you feel even more special. It can feel like someone finally values, appreciates, or "gets" you. It usually feels really good, passionate, exciting and even intoxicating, but it's actually a form of emotional manipulation. Love bombing may seem loving, but underneath the behavior is a desire to control; it's a common form of emotional abuse that goes unrecognized.

What are the top catfishing romance scams?

Financial

- **Money** to be provided via a specific method to pay an unexpected debt or to pay for "an emergency situation," such as a child/grandchild's surgery, claiming that the situation prevents them from being able to visit you until it's resolved and that for a variety of reasons they don't have access to the funds.
- **Credit**, either opening a credit card, taking out a loan or establishing a line of credit in YOUR name for their use.
- **Gift cards**, purchasing high quantities and then providing the card numbers.
- **Investments** in a guaranteed high yield or once in a lifetime "investment." They may pay you a small return at first to support the idea that there is actually an investment and that it is fruitful and later ask you to add to your investment, after which you will not receive any further returns and you will instead be told that you lost your entire investment.
- **Money transfers**, receiving it then wiring it overseas. This transaction is money laundering, of stolen or "dirty" money, and wire fraud, which may sound harmless but both are legally punishable crimes.
- **Cryptocurrency**, purchasing tokens that will be held in the scammer's existing crypto account supposedly for "ease." Once it's in their account, it is inaccessible by anyone other than the account holder after that.

Identity theft

- **Information, especially financial**, to be used for identity theft.

Blackmail (revelation of information)

- **Personal information**, especially financial, including passwords, as well as private photos.

In all cases, as long as the prey voluntarily complies with the scammer's requests, no crimes are committed by the scammer. Sometimes scammers are criminals but not in regard to their romance scams. Money laundering and wire fraud are voluntarily committed by the prey and are punishable crimes.

Know your boundaries and NEVER vary from them for ANY reason!

Know your values and boundaries and NEVER compromise on them. **If a request is made for you to do anything that makes you uncomfortable, especially in regard to sending or posting photos, say NO! Accept NO LIES ... not one ... and NEVER, ever do any monetary transaction or share personal, especially financial, information!** If your boundaries are crossed, a lie is substantiated or a request for any personal information or financial transaction is made STOP communicating with the scammer IMMEDIATELY!

Keep in mind that the catfisher just met you and nobody that you just met should ever ask you for anything financial. The person they are portraying is not real and neither is their "emergency situation," "investment," "need for assistance" or need for any of your personal information!

How can you avoid being prey to a romance scam; what are the signs you may be being scammed?

- **Be careful what you post and make public online.** Scammers can use details shared on social media and dating sites to better understand and target you. Also, the scam may be identity theft, protect your personal information.
- **Be wary of long distance and overseas relationships.**
- **Research** the person's photo and profile using online searches to see if the image, name, or details have been used elsewhere. Google all information they provide: name, email address, phone number, address (verify on a county assessor site), everything. Also use socialcatfish.com. You can consider running a background check. Many sites used to be free but are now behind a paywall. It may be worth paying for a report! If you have photos, try using <https://images.google.com>. (Select the camera image to upload an image.) It works better on buildings than it does for headshots.
- **They often claim to be self-employed** in an industry (oil and gas) or have a job (architect or construction) that they say has either previously required them to work outside the country or is about to. Working on an oil rig or serving in the military are often cited.
- **Ask what their job is.** Does it have a website? If not, why not?
- **Ask to see their social media presence** to verify who they are? Beware if they have none. **Ask them what their address is**, especially if the claim to live in the U.S.? They may ask what yours is – do not give it to them. Say that you asked him.
- **They will create "false" intimacy**, very quickly, in order to create immediate trust by asking personal questions, showing care/concern, eventually stating that they have found "the one," referring to you. They will claim they are deleting their profile because you are the one they have been looking for. Many scammers claim that it has been years since their spouse has passed away that they just opened themselves up to meeting someone and that you are exactly what they have been looking for.

- They will cautiously declare their love, and state that they have held back because they didn't want to scare you away. Once they declare their love, they will "love bomb" their prey. They do not love you!!! They do not know you, and you do not know them! In fact, they aren't even who they say that they are and, in fact, are creating a fake persona for you.
- Go slowly and ask lots of questions.
- Beware if the individual seems too perfect and/or something seems "off" about them. It is!!
- Pay attention to the details of the stories you are being told – look for inconsistencies or lies. It is not skeptical or distrusting, but smart and safe to do so! Again, you don't know them!
- They may try to impress you with their financial stability/wealth by asking questions that they can then answer with fabulous answers to impress you. For example, they might ask if you like fast cars – well, I have 5 fast cars. Or perhaps, ask "What kind of car do you have?" and then reply that they will buy you a newer, more expensive car. Another might be, "What kind of home would you like to live in?" followed by stating the their home has extravagant features.
- They may play on your sympathy by saying that they need financial assistance, perhaps for a refrigerator, if only their parents.
- Beware if they quickly ask you to leave a dating service or social media site to communicate directly. Stay on the platform. The scammer then has your contact information, which of course you can then block. If you go off the platform, the scammer can then delete their profile and not be tracked.
- Beware if they won't meet in person ... supposedly due to travel. In fact, if they immediately say they have to travel, tell them that you will communicate with them only after they have set up a day/time to meet in person have returned and you have met!
- Beware if the individual promises to meet in person but then always comes up with an excuse why he or she can't. If you haven't met the person after a week or so, for whatever reason, you have good reason to be suspicious.
- Beware if they refuse to video chat OR if they will video chat but always "need" to initiate the meeting or ask you to "jump" into a meeting they already have going. Also, if the video is always "blurry" and/or the voice/mouth are out of sync, it is likely video that has been stolen from the person used to create the fake profile and then manipulated with the scammer's voice over.
- Beware if the individual attempts to isolate you from friends and family or requests inappropriate photos or financial information that could later be used to extort you.
- NEVER do monetary transactions of any kind or share financial information with anyone you have only communicated with online/phone or have known a short time, no matter how close you feel to them.

Have a strategy:

- Screen print their profile immediately, 1) so you can remember what it said and 2) in case you need to report it someday.
- Get as much information as you can in your initial communication: name, where they live, employment, social media presence etc, ... BE BOLD! Verify as much as possible. If they ask for you address, tell them that you will let them know that after you have verified their address.
- Ask for a video Zoom or Facetime meeting PRIOR to meeting in person. YOU initiate the meeting, do not let them create the meeting or ask you to jump on an open meeting. If the person is not real, the video will be blurry, almost as though underwater, and the video and

audio will not match – even if they claim to be in the same neighborhood. That just hastens identifying the scam. If they initiate the meeting it facilitates their ability to use modified video from their end, as well as to record your image as video.

- **Require that they meet you in a public place within the first week** or wait until they “return” home and can meet to communicate any further – a scammer will NEVER meet you. Even if they schedule an in person meeting, it doesn’t mean that it will happen. If an unscheduled event/trip causes the meeting not to happen, stop communicating until the meeting can happen in person. NO exceptions! They are skilled!
- **Share as little information as possible.** During your initial communication, and prior to a scheduled first in-person meeting, they will do their best to create “false” intimacy by asking a lot about you. This is so that they can learn more about you personally to be used to create further false intimacy and your vulnerabilities for future exploitation. Don’t be too eager to fully answers questions. Provide partial answers to questions such as “What do you like to do?” Don’t deliver the full list answer but instead one or two things you enjoy. Then ask them for their answer. This prevents them from being able to say that everything you said is what they like.
- **Watch out for questions that imply concern for you,** such as: “Have you eaten today? What have you eat? and Are you taking care of yourself?”
- **When you meet someone in person, always let someone know who you are with and where you are going,** as well as what time you will call them to either say you are still with the person or to let them know you are home and safe
- **Always meet in public and be in control of your own transportation.** Know your limits so that you do not become impaired. Don’t leave drinks or personal items unattended. If you feel uncomfortable, leave immediately
- **Always trust your gut!!!** If something feels off, it is!!!

What can you do if you feel that you are communicating with a scammer and/or have been scammed?

If possible, try to do this prior to the scammer knowing that you are on to them.

- **If you shared financial information and/or passwords, contact the credit bureaus to report possible fraud.** Contact Equifax: (866) 640-2273, press 1 then 4. You can activate a fraud alert, put a security freeze on your accounts and request a credit report. Equifax will notify Experian and TransUnion for you.
- **Contact any appropriate financial institutions** (banks, credit card companies) and change your account numbers and passwords.

1. Stop communication with the scammer immediately!

Block their phone number for messaging and calls. Do not respond to another message or answer another phone call. They WILL try to gaslight you, to convince you to continue communicating with them, by telling you that you have misunderstood or made a mistake or created false story about them or even that you are an awful person to doubt or ghost them. The scammer will be desperate to reengage you as they have invested time and energy into luring you toward their scam and are also extremely skilled at getting their prey to reconsider and give them a second chance. DO NOT!!!

2. Report the scammer

Contact the app, social media platform or website through which you met the person. If you met them locally in person, report them to your local law enforcement agency. In either

case, if you feel at personal risk, contact your local law enforcement agency immediately!
File a report at [i3c.gov](https://www.ic3.gov) (per the FBI) and the Federal Trade Commission (FTC).

If at any time you doubt yourself about knowing that you communicating with a scammer,
remember that the scammer is likely on a computer, in an internet café or call center,
communicating with 2 dozen or more people at the same time, asking the same questions and
sending the same photos, poems, special songs, etc. You are NOT special to them; you are ONE
OF MANY!