SECURITY GUIDE

Security Tips for Dating Apps

Interlira Risk Consultancy | interlira.com

INTERLIRA Risk Consultancy

Technology made it easier to find a love, or just someone to hang around with. However, **those who are looking for a relationship and use apps for that, need to be careful not to fall for scams** and even become a victim of kidnapping.

In São Paulo, the Anti-kidnapping Division of the Department of Strategic Police Operations (Dope), a unit specialized in kidnapping by the São Paulo Civil Police, has informed that this is a growing trend with more and more cases every year.

According to the Military Police, the victims' profile is:

- Usually older, financially successful men;
- People over 40 years old;
- Single or married;
- Merchants or businessowner.

Most criminals attract their victims through Tinder, with **seductive messages and a request to meet as soon as possible**.

According to police, the victims are chosen according to the information it provides directly or indirectly, such as photos and profession. **The main targets are those who post photos on international trips and next to luxury cars.**

TYPES OF SCAMS

VERIFICATION SCAM

In this type of fraud, **scammer contacts the victim and requests a code that was sent to her phone.** However, this number is actually the key to access the Facebook account, Snapchat, WhatsApp or even the bank account. Scammers also use bots that contact matches with a fake profile and automatically send them account verification links.

Criminals seek to take advantage of a Tinder profile verification tool in order to demonstrate that the photos belong to a real person's profile and not a fake account.

FAKE PROFILES

This type of scam is more trivial. Criminals create fake profiles, with photos taken from image banks with models or sexually suggestive positions.

After the match, the phone number is asked so that the scammer and the victim can “get to know each other better”, where they use social engineering to collect personal information.

"CATFISH"

In this strategy, bandits do not focus on stealing information or money, but the objective is to gain the trust of their victims and exploit this for their benefit, by asking for money and valuable gifts.

Despite sounding harmless, catfish can cause quite a bit of anguish in victims, as fakers can take their lies very far and make the person on the other side of the screen fall in love with them.

"SEXTORTION"

Sending sensual messages and photos (sexting) is quite common, but it can be dangerous. This material can be used by scammers for extortion, with threats of disclosure if a cash or cryptocurrency payment is not made.

This type of scam can cause a lot of pain and anguish for victims, especially women.

FINANCIAL ROMANCE SCAMS

This scam is more complex both to detect and to apply. In them, **scammers manage to go further, taking fraud from the virtual world to the real world**.

They are real people, with real profiles, but with hidden interests, who use Tinder to leverage their scams.

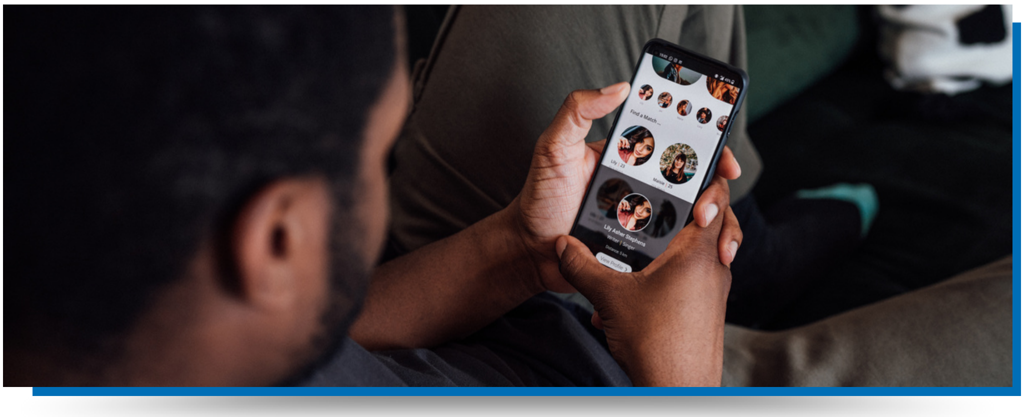
RECOMMENDATIONS TO AVOID TRAPS

I. ON YOUR PROFILE

- Use the abbreviated name or nickname;
- Reduce personal information you make available such as “I love dogs”, as they are particular characteristics that can attract the scammer to the victim’s sentimental side;
- Avoid putting information about your occupation;
- Do not use photos that show international travel and expensive items;
- When you are no longer using the app, delete or hide your profile; This prevents your location from continuing to be shared without you knowing;
- Use the app’s built-in chat. This keeps your information logged and protected.

II. DURING THE CONVERSATION

- Search or ask for the person's profile on other social networks, such as Instagram and Facebook;
- Search the photos on Google. You just need to take the person's photo to Google search (https://images.google.com) and choose the option "find the source of the image". Then choose all sizes. If it is someone fake, it's possible that the photo appears several times as a result;
- Watch for signs that may indicate manipulation of the image: irregular edges or shadows and low resolution are indications of montage or removal of photos from other profiles;
- Profiles without a photo or with images available in banks: this increases the chance of being a fake profile;
- Take your time. Get to know the person better before agreeing to meet. Also, chat via video call before meeting the person.
- Make sure your match has online identity verification, ensuring they are who they say they are;
- Never send money or financial information.



III. DURING THE DATE

- Set the date during the day;
- Choose a public, busy place outside a risk region. Do not arrange to meet on the street, at the person’s door or on quiet streets;
- Let friends/family know where, when and with whom you're going out;
- Arrange an emergency call: ask a trusted person to call you to find out how the situation is. If they doesn’t get an answer, they can take action or even call for help;
- If the person changes the meeting point at the last minute, the recommendation is to cancel;
- Limit alcohol consumption and do not leave drinks or personal items unattended;
- Be aware of possible warning signs from the other person: if they spend a lot of time on their cell phone, if they are answering messages when talking to you, if they are looking outside, if they are worried about the time. These are all indications that a crime can happen.
- Have your cell phone charged and always with you;
- Go with your own transport and leave if you feel uncomfortable;

❗ If you don’t feel safe, ask for help on the platforms or call police authorities (190). And if you fall for a scam, don't hesitate in registering the occurrence at the police station.

LEARN MORE ABOUT OUR SERVICES

INTER LIRA Risk Consultancy

To visit our website, **click here**.

To follow us on LinkedIn, **click here**.

To contact us, **click here**.