# Digital Dating Dangers

kaspersky

# Intimate Image Abuse

The sharing of intimate images has become a normal part of day-to-day dating life. Whilst great news for allowing us to form connections and bonds, many people are seemingly unaware or unconcerned about the associated risks. Research shows us that younger age groups, in particular, are still prepared to share their most intimate images without concern for the potential long-term dangers of relinquishing control.

In May 2024, Kaspersky surveyed 9,033 people revealing nearly half (47%) of respondents have either experienced (7%) or know someone who has survived this form of online abuse. Intimate Image Abuse (IIA) is particularly pronounced among younger generations, with 69% of 16-24-year-olds and 64% of 25-34-year-olds reporting such experiences.

But it doesn't have to be all doom and gloom – there are plenty of steps we can take to make this a positive and safe experience, which enhances our dating journey.

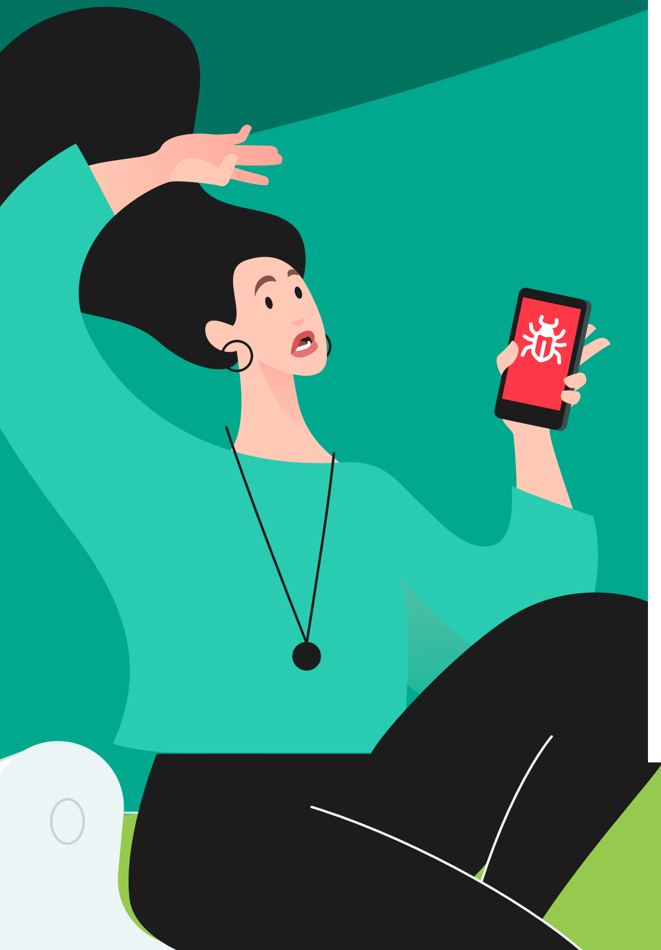
## Top tips for keeping yourself safe:

- **Think before you post.** Be mindful of who you share your data with and when. Always consider how the content you share online might be interpreted and used by others.
- **Understand** which messengers are safe and which have end-to-end encryption. However, keep in mind that although encryption keeps it secure in transit, this doesn't stop someone who receives it from sharing it with others.
- If you think you are a victim of IIA, **keep evidence and report** it to the police and platforms where you believe your data is available.
- Always **check the permission** settings on the apps you use to minimize the likelihood of your data being shared or stored by third parties – and beyond – without your knowledge.
- **Use a reliable security** solution like Kaspersky Password Manager to generate and secure unique passwords for every account; resist the temptation to reuse the same one.
- **Utilise StopNCII.org** or other online tools to help protect intimate images from being shared online across some of the most widely used platforms in the world .

kaspersky

# Stalkerware

Stalkerware, by its nature, often happens within relationships because it typically requires physical access to a device. Stalkerware products are typically marketed as legitimate anti-theft or parental control apps on smartphones, tablets, and computers, but in reality, they are very different. Installed without the knowledge or consent of the person being tracked – they operate stealthily and provide a perpetrator with the means to gain control over someone's life. Usually, these apps are not shown in the list of installed apps in a phone´s settings, which makes them hard to spot.



## Whether you are a victim of stalkerware or not, these tips can help you to better protect yourself generally:

- Protect your phone with a strong password that you never share with your partner, friends, or colleagues.
- Only download apps from official sources, such as Google Play or the Apple App Store.
- Block installation of third-party apps.
- Check apps installed on your device regularly and remove any that you no longer need.
- Install a reliable IT security solution like Kaspersky Premium on devices and scan them regularly. However, in cases where stalkerware may have already been installed, the solution should only be uploaded once the risk to the victim has been assessed, as the abuser may notice the use of cybersecurity.

*Victims of stalkerware may be victims of a larger cycle of abuse, including physical.*

*In some cases, the perpetrator is notified if their victim performs a device scan or removes a stalkerware app. If this happens, it can lead to an escalation of the situation and further aggression. This is why it is important to proceed with caution if you think you are being targeted by stalkerware.*

- **Reach out to a local support organization:** to find one close to you, check the Coalition Against Stalkerware website.
- **Keep an eye out for the following warning signs:** these can include a fast-draining battery due to unknown or suspicious apps using up its charge, and newly installed applications with suspicious access to use and track your location, send, or receive text messages and other personal activities. Also check if your "unknown sources" setting is enabled, it may be a sign that unwanted software has been installed from a third-party source.
- **Do not try to erase the stalkerware, change any settings or tamper with your phone prior to developing a safety plan:** this may alert your potential perpetrator and lead to an escalation of the situation. You also risk erasing important data or evidence that could be used in a prosecution. Take steps to determine what course of action makes the most sense for your current situation prior to making changes that could lead to an escalation in behavior from a potential perpetrator. Seek help from a survivor support organization.

kaspersky

# Deepfakes

Deepfakes, powered by Artificial Intelligence (AI) are being increasingly used to generate highly realistic images, videos, or audio recordings, and are expected to become prevalent tools of abuse in relationships/dating.

Previously, the quality of such fakes was low, and they could easily be detected by the naked eye; now a deepfake has become much more difficult to spot and making deepfake technology one of the most dangerous tools of the future. Deepfakes are increasingly being used to blackmail victims with the threat of releasing compromising fake content unless they comply with the abuser's demands.

## Whilst technology now makes it easy for someone to create a deepfake, the following steps could help minimize your risks:

- Be careful what images and audio you share or post online, and how available that is to other people.
- Be mindful of what you're looking at – check for obvious clues of fakes, such as:
  - something that looks odd, or objects that are misplaced
  - non-matching earrings
  - watch or bracelet doesn't look right
  - background items out of place
  - distorted background items
  - too many fingers.
- Try a reverse image search, to see if you can identify the source of the picture.
- Check file metadata, to see if this reveals anything about the source of the image.
- Upload the picture to an AI system, to see if it is flagged as AI.
- Think before you share/forward on images – don't be a part of the problem.

## What to do if you're worried about a child in the context of any of these issues:

- **Discuss the risks:** Have open conversations about the potential consequences of sharing intimate images, including the possibility of them being shared without consent.
- **Encourage trust and communication:** Make sure children feel comfortable discussing any online experiences or pressures they may face.
- **Teach digital literacy:** Educate children about secure ways to use technology, including the importance of privacy settings and understanding that images shared online can be permanent.
- **Use parental controls:** Implement tools and apps that monitor and restrict the sharing of sensitive content.
- **Set clear rules:** Establish family guidelines for internet and phone use, emphasizing respect for privacy and the importance of consent.
- **Model responsible behaviour:** Show by example how to engage responsibly with technology and online sharing.