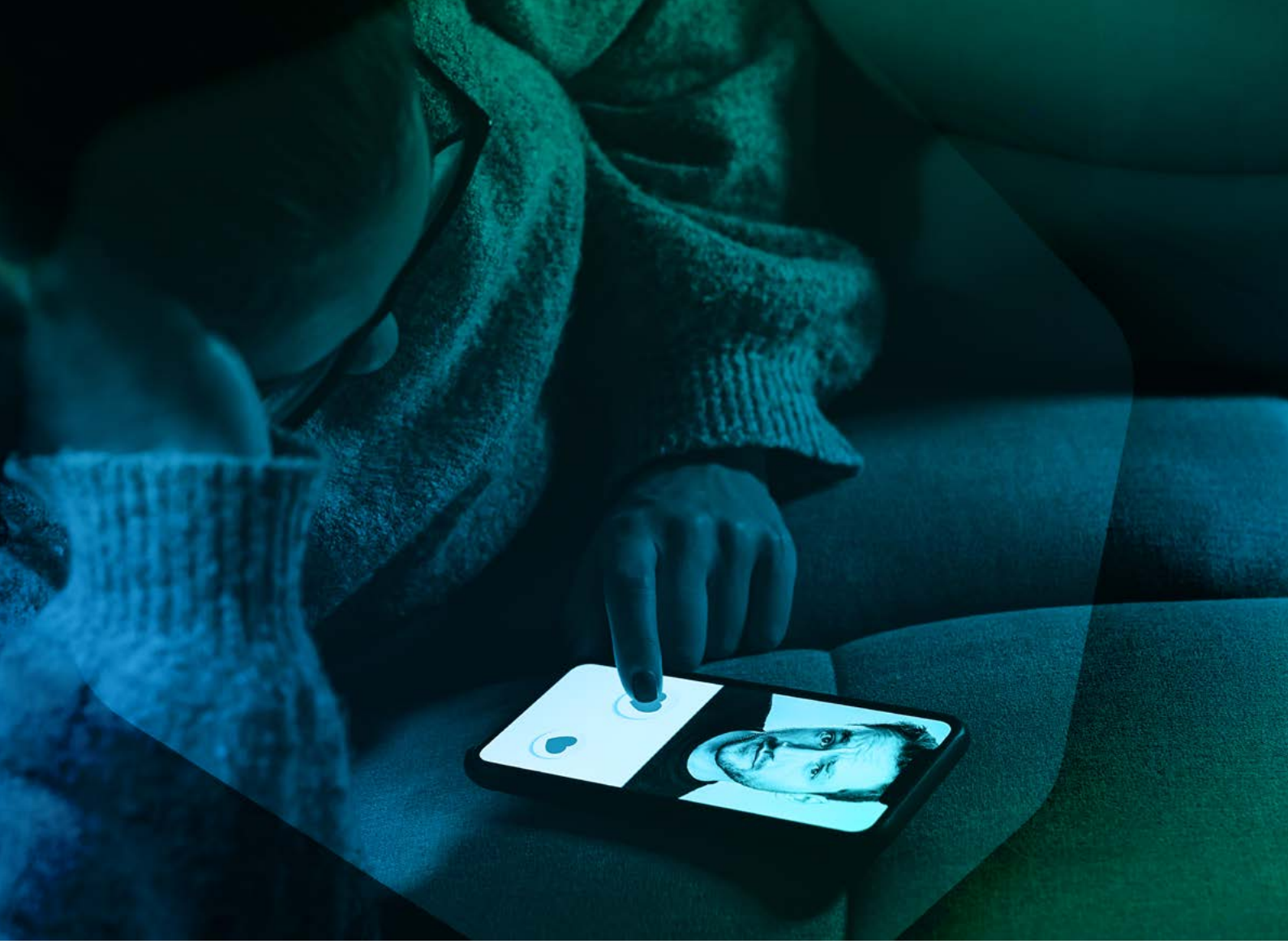


Is technology making relationships more risky?

Top three threats to watch out for

kaspersky.com
Kaspersky official blog

kaspersky BRING ON THE FUTURE

Is technology making relationships more risky? Top three threats to watch out for

Stalking, blackmailing with intimate images or sensitive information, and spreading false rumors have long been threats when it comes to dating and relationships. The advent of social media and AI technologies has significantly amplified these dangers.

Today, meeting partners online has become commonplace, and due to how dating apps and messaging services work, it's easy to develop trust quickly. This often leads to the sharing of personal information and intimate images without real-world knowledge of the person. As a recent **global study** by Kaspersky shows, a quarter (25%) of respondents have shared images of themselves with people they are dating or chatting to, with the number rising amongst 25–34-year-olds to 39%. Notably, 20% of males surveyed have sent nude images to individuals they have never met in real life, basing their actions on perceived trust within the relationship.

Unfortunately, this openness can be exploited, especially when relationships go astray or when individuals with malicious intent are involved from the start.

As a cybersecurity company, Kaspersky provides protection against a wide range of digital threats. However, some dangers –such as grooming and doxing, stalking, bullying or the misuse of intimate images – extend beyond the capabilities of technology alone. This is why public education is crucial, and we as a purpose-driven organization are committed to raise awareness about these threats and empower people to protect themselves. Among our various initiatives, this report serves to highlight the three most critical threats in romantic relationships that have been amplified by technology today:

1. Intimate Image Abuse: when private images spiral out of control

In May 2024, Kaspersky surveyed 9,033 people – one of the largest polls to ever be conducted on the subject – revealing the extent to which explicit images are captured, stored, and shared on smart devices. The findings correlate with the widespread issue of intimate image abuse (IIA), also known as 'revenge porn,' with nearly half (47%) of respondents reporting that they have either experienced (7%) or know someone

In Europe, the three most affected countries by stalkerware in 2023 were Germany (577), France (332), and the United Kingdom (271)

Everyday technologies like GPS tracking, smart home devices, and especially social media are opening new avenues for abusers to monitor and control others.

who has survived this form of online 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.

This growing normalization of sharing intimate images has become a critical societal issue, with the public now seemingly aware of the risks. Yet, younger age groups, in particular, are still prepared to share their most intimate images without acknowledging the potential long-term vulnerabilities.

2. Stalkerware: when legitimate technology is abused

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 a victim'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.

In 2023, **Kaspersky data** reveals 31,031 unique individuals around the world were affected by stalkerware, an almost six percent year-on-year increase (5.8%) of the 29,312 users affected in 2022. The figures reverse the downward trend of 2021, confirming digital stalking continues to be a global problem. In Europe, the three most affected countries by stalkerware were Germany (577), France (332), and the United Kingdom (271).

But stalkerware is just the tip of the iceberg; everyday technologies like GPS tracking, smart home devices, and especially social media are opening new avenues for abusers to monitor and control others. In our culture of oversharing, nearly everything about a person can be found online. In fact, a substantial 34 percent of respondents in **our survey** view Googling or checking social media accounts of someone they recently started dating as an acceptable form of due diligence. This behavior is creating a false sense of entitlement to monitor others and empowering abusers with easy access to personal information.

3. Deepfakes: when fakes become indistinguishable from reality

Deepfakes, powered by artificial intelligence (AI) to generate highly realistic images, videos, or audio recordings, are expected to become increasingly prevalent tools of abuse in relationships. In the past, 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. The technology has developed rapidly in the last five years, with various open-source tools freely available now, allowing anyone with basic programming skills to create deepfakes. This trend makes deepfake technology one of the most dangerous tools of the future.

The first and most obvious area where deepfake immediately found its place was pornography. Celebrities were the first to suffer from this, but

now even ordinary individuals are affected by it. In the context of relationships, deepfakes may be used to **blackmail victims** by threatening to release compromising fake content unless they comply with the abuser's demands. This can include threats to share fake nude photos or videos, which may force the victim to stay in the relationship or fulfill other coercive demands.

David Emm, Principal Security Researcher, Global Research and Analysis Team, Kaspersky, elaborates: "Intimate image abuse, stalkerware and deepfakes are dramatically expanding the scope and severity of relationship abuse in our connected world. Through our very own personal devices, perpetrators can exert control, monitor their victims' every move, and inflict emotional and psychological harm from anywhere, often without the victim's knowledge. The surge of AI and deepfake technologies further intensifies these threats, as anyone can create compromising content and distribute it without consent. This not only wreaks havoc on victims, but also complicates effort to seek justice. As technology evolves, it's crucial for individuals to be vigilant about the personal information and images they share online, be aware of the signs of manipulated media, and prioritize privacy settings on social media and dating apps."

Education: from a behavioral and technological standpoint

Consent is not a one-time agreement

Unfortunately, victim blaming remains a pronounced issue in our society. As our **survey** shows, 50% of respondents believe that if you've shared an image of yourself, it is your fault if it ends up in the wrong hands. However, blaming victims perpetuates harmful myths, adds to their trauma, and distracts from the real problem: the actions of those who misuse or distribute these images without consent. The emphasis should be on educating about consent and holding abusers accountable, rather than shaming individuals for engaging in private, consensual behaviors.

Despite significant progress in legislation and efforts by NGOs against IIA, it's still important to understand that once an image is shared, it is virtually impossible to fully control its spread or ensure its deletion. Pictures may be released by mistake or if the device or accounts get hacked. There needs to be greater awareness that consent for private pictures is an ongoing process, not a one-time agreement, requiring continuous respect and reaffirmation. In fact, 30% of men surveyed believe receiving an intimate image grants them ownership, complicating issues of consent and highlighting a prevalent misunderstanding about digital privacy and respect.

Generally, it's always important to think twice before you post, gauge whether the person can be trusted and remain cautious because even if you take all precautions, things can still go wrong.

Education of boys and men

The majority of intimate image abuse and cyberstalking incidents are perpetrated by men, often reflecting deeper societal issues related to power, control, and a lack of respect for boundaries and consent. Addressing this problem requires targeted education in schools, workplaces and communities to teach boys and men about the impact of online harassment, the legal consequences of such actions, and the importance of recognizing and valuing consent both online and offline.

30% of men surveyed believe receiving an intimate image grants them ownership

By fostering a culture of accountability and respect, combined with clear messaging that these behaviors are unacceptable, we can begin to shift attitudes and reduce the prevalence of online abuse perpetrated by men.

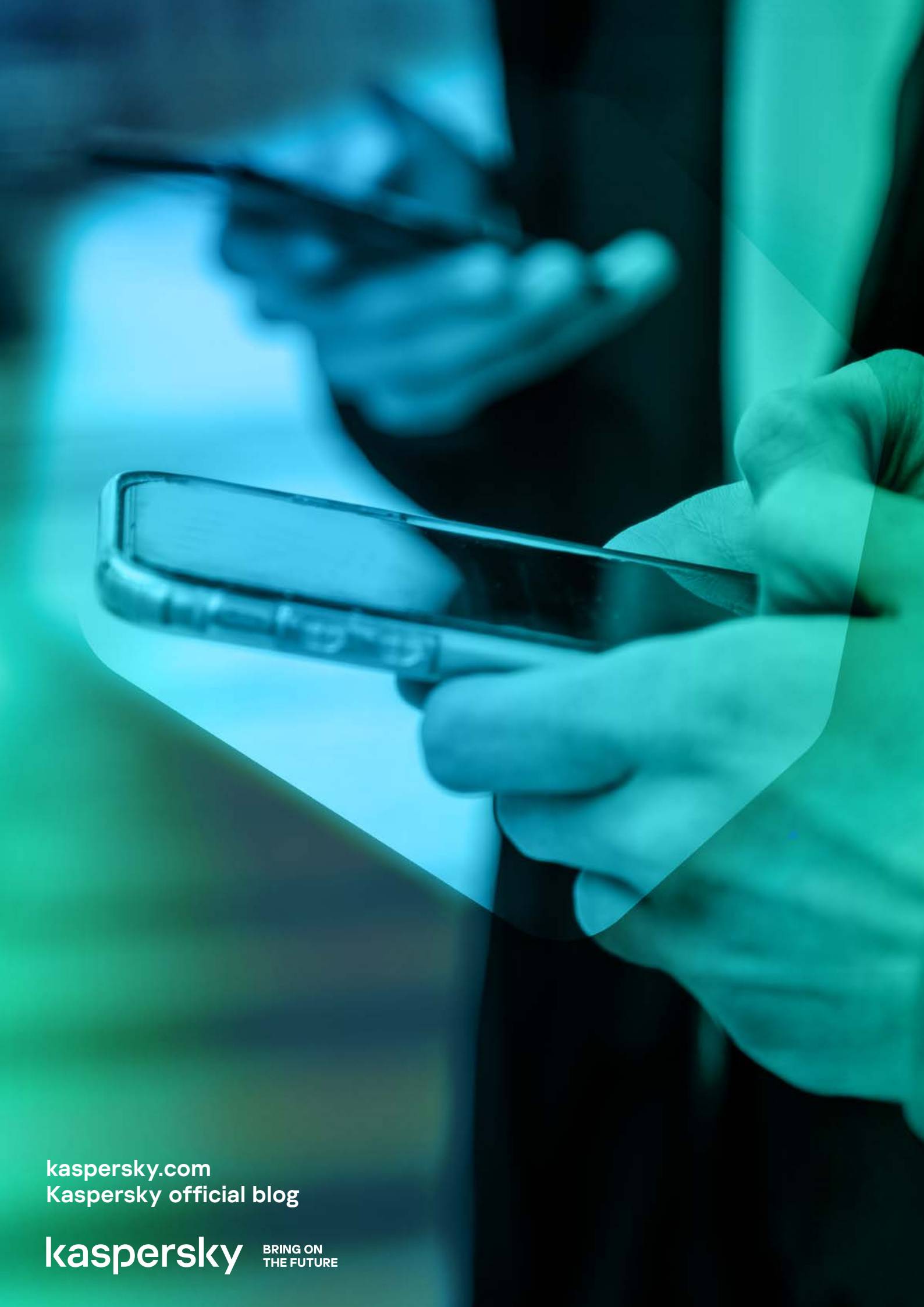
Digital literacy to minimize risks

There is also a plethora of technical dimensions that individuals should take into account to protect themselves from online abuse. For instance:

- In the case of distribution of intimate images and deepfakes on social media, individuals can report them to the platform to take down the content. Many of these platforms are using advanced AI technologies such as image recognition and digital fingerprinting, which can automatically detect intimate images, enabling platforms to track and prevent their spread once reported by the affected individual.
- 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
- Understand which messengers are safe and which have end-to-end encryption
- 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
- Install a reliable IT security solution like **Kaspersky Premium** on your devices and scan them regularly. However, in cases where stalkerware may have already been installed, the solution should only be installed once the risk to the victim has been assessed, as the abuser may notice the use of cybersecurity. The following warning signs may indicate the presence of stalkerware:
- Fast-draining battery due to unknown or suspicious apps using up its charge
- Newly installed applications with suspicious access to use and track your location, send, or receive text messages and other personal activities.
- Checking if your “unknown sources” setting is enabled, it may be a sign that unwanted software has been installed from a third-party source.
- In case of the presence of stalkerware, do not erase the stalkerware, change any settings or tamper with your phone. 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. It is best to reach out to a local support organization: to find one close to you, check the **Coalition Against Stalkerware** website.

Sources:

- **The Naked Truth: How intimate image sharing is reshaping our world**
- **The State of Stalkerware in 2023**
- **How real is deepfake threat?**



kaspersky.com
Kaspersky official blog

kaspersky BRING ON THE FUTURE