

How we protect various user groups

GRI 3-3

Protecting various user groups is an important part of our work to create a safer digital space.

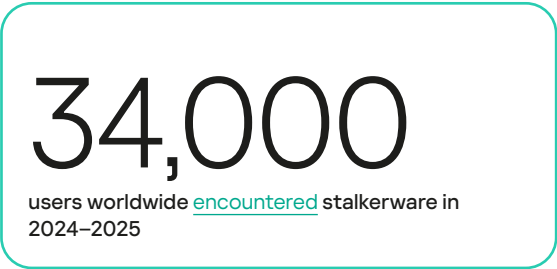
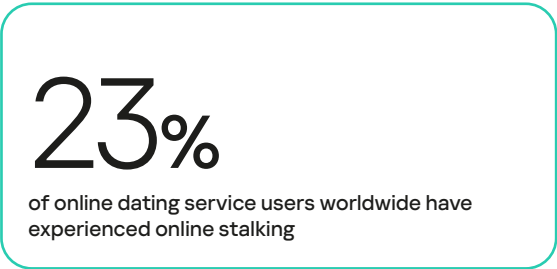
We combat cyberstalking

What is stalkerware and why is it dangerous?

Modern technologies have become an important part of life and help us in many ways, but sometimes they are used to our detriment. One such threat is digital stalking or cyberstalking.

Attackers can install a special kind of application, known as stalkerware, on the victim's smartphone. This software operates covertly and secretly monitors a person through their device: it collects location information, reads correspondence, and gains access to photos and other personal data without the smartphone owner's knowledge. This is a serious problem, both as technical and a social one, as it violates a person's right to privacy and can often be linked to domestic violence.

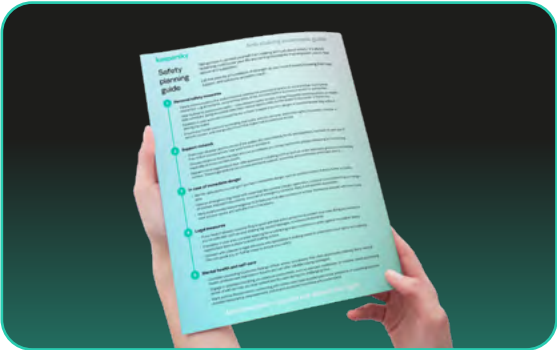
The scale of the problem



Research by Kaspersky shows that digital stalking is an urgent threat.

According to the results of a [global study](#) by the Company¹, approximately one in four users (23%) have experienced some form of digital stalking from a person they were newly dating. The types of abuse varied, with 39% of respondents having reported some form of violence or abuse from a current or previous partner: 10% admitted they had had their location tracked, 10% that their social media accounts or emails had been hacked, and worryingly, 7% having had stalkerware installed on their devices without their consent.

It is very difficult to detect stalkerware without special tools. If you discover a suspicious app, experts advise not to delete it immediately (the stalker might quickly find out it has been deleted), but to seek help from professionals, a crisis center or the police.



We help users protect themselves

Kaspersky has been protecting users from digital stalking for many years, leading the fight against cyberstalking. In 2019, we implemented a stalkerware detection feature in our mobile app. Our [Kaspersky for Android](#) solution scans the device and alerts the user when hidden surveillance apps are detected.

In 2024, we went further and added a new feature – [Who's Spying on Me](#), extending its protection against digital stalking. In addition to the stalkerware detection, the new feature provides protection from offline stalking by detecting suspicious devices tracking the location of a person or object via Bluetooth technology.

In addition to technical solutions against stalking, Kaspersky strongly emphasizes education and cooperation.

In November 2024, we published the [Anti-Stalking Awareness Guide](#), which was created in collaboration with international experts and victims of stalking. The initiative aims to support victims and their families, raise awareness of the problem, and provide practical tools for protection. This guide helps users understand stalking, debunks common myths, and describes the manipulative methods used by stalkers. It focuses on two practical checklists covering both digital and physical security.

¹ The study involved 21,000 people worldwide.

The first checklist includes recommendations for creating a safety plan, a form for documenting incidents, and tips for family and friends who support victims. It was created with the help of:

- Olimpia Coral Melo Cruz, an activist who initiated "Olimpia's Law" in Latin America, which has become the foundation for the fight against digital violence
- Marcela Hernández, co-founder of Red Latinoamericana de Defensoras Digitales, a support network for digital rights defenders
- Janaina Campos, a Brazilian psychoanalyst who works with dysfunctional relationships
- Acacia Diana and Yulia Pavlova, victims of stalking who shared their personal stories to raise awareness among other women

The second checklist, our [Digital Security Guide](#), which was developed by Kaspersky expert Anna Larkina, contains recommendations for protecting personal data, configuring privacy on devices and reducing digital risks that can make a person vulnerable to online harassment. Together, these materials form a holistic approach to supporting victims, encompassing both physical and digital security, and underscore Kaspersky's commitment to creating a safer digital space for everyone.

Additionally, Kaspersky experts regularly share tips on digital security. For example, we recommend using complex, unique passwords and not sharing them, carefully managing privacy on social media, and not disclosing too much personal information online. These simple measures reduce risks and help users feel more confident.

We join forces and help victims

>40

organizations are part of the international Coalition Against Stalkerware, co-founded by Kaspersky

Combating cyberstalking requires the combined efforts of many participants, and Kaspersky actively works to bring stakeholders together. In 2019, we co-founded the international [Coalition Against Stalkerware](#), which today unites more than 40 organizations—from IT companies to law enforcement agencies. Together with our partners, we raise awareness about digital violence and help victims.

Kaspersky participates in international initiatives to combat digital violence, such as Europe's DeStalk project. Another joint project is "Revolutionizing Online Safety: Tackling Technology-Facilitated Abuse to Protect Victims and Survivors of Intimate Partner Violence"¹. In addition to Kaspersky, other international companies, representatives of the academic community, and non-profit organizations are participants. This project is being implemented in partnership with the British agency [UKRI](#) from 2023 to 2026. Kaspersky supports the project by sharing its expertise in combating cyberbullying and stalking, and by participating in additional events.

¹ Research on how to protect victims / survivors of intimate partner violence (IPV) from the risks created by digital technologies.

A safe space for people who need protection

We support the Nizhny Novgorod Women's Crisis Center

We understand every statistic represents real lives, so we strive to participate in initiatives to help victims in real life.

Problem

Women and children who face domestic violence and stalking often need safe shelter urgently. Moreover, sometimes victims do not even have access to their own documents and money. In these circumstances, they have no chance of finding emergency shelter in many regions.

What we did

Since 2022, Kaspersky has supported the Nizhny Novgorod Women's Crisis Center's Safe Apartment project. It offers secret housing that victims can move in to on the same day they apply. Beneficiaries receive basic necessities: accommodations, food, clothing, means of communication, as well as psychological, legal and social assistance. The project imposes no formal barriers, offering help even in the absence of documents.

Result

Over four years, with our support the center has managed to provide shelter and assistance to 32 women with children.



We ensure children's online safety

Creating a safe online environment for children is a priority, and our future depends on it. Kaspersky is working on this both internally and in partnership with ministries, agencies and other organizations around the world.

Why this matters

Children today begin using the internet from a very early age — for study, communication and entertainment. The online environment offers many opportunities for growth, but at the same time, it also carries real risks: threats of fraud, cyberbullying, dangerous content, attempts to manipulate and pressure. Children often encounter these threats before they have time to understand how to resist them, and adults don't always know what exactly is happening to their child in digital spaces.

We believe that technology alone is not enough to protect children online. It's important to understand children's online lives, what they trust, what they fear, and what problems they face. That's why Kaspersky has been conducting surveys on the digital habits of children and parents for many years and then turning knowledge we gain into practical solutions: educational programs, useful materials, and initiatives available to families, schools, and communities around the world.

What does our research say?

One of our key projects in the area of children's digital safety is a regular survey that we use to prepare our annual report on kids' digital interests. [On International Children's Day we issued an analysis](#), covering the period from May 2024 to April 2025, revealing a growing fascination with AI-powered chatbots, the viral rise of Italian brainrot memes like "tralalero tralala," and growing attention to Sprunki — a rhythm-based game combining music and motion. YouTube remains the most popular app among children globally, while WhatsApp overtook TikTok for second place.

We continued to analyze children's digital habits using anonymized data from our [Kaspersky Safe Kids](#) solution. The data show that children are spending more and more time on online games, video platforms, and social platforms, are using mobile devices more often, and are actively interested in gaming and video content.

At the same time, they continue to face key risks: fraud, unwanted content and pressure from unknown users. These findings confirm the need for a comprehensive approach to children's online safety that combines technology-based protection, education, and improved digital literacy among children and parents.

We also studied how attackers exploit the popularity of children's brands. For example, in the [reporting period](#), our experts analyzed threats that use references to well-known games, toys, and cartoons (Minecraft, Roblox, LEGO, Disney, etc.) as bait. The study found that in the first quarter of 2024 alone, the number of such attacks increased by 35% compared to the previous year.

We educate and support children, parents, and teachers

We believe that developing digital literacy should be accessible, clear, and engaging. That is why Kaspersky actively participates in educational and awareness-raising projects.

Easy-to-understand materials for the whole family

To discuss digital literacy and other complex topics in simple terms, we create special publications for children and adults.

- [Cybersecurity Alphabet](#) is an educational book about technology and digital threats, built around the alphabet. It helps children and parents understand new terms and learn safe online behavior. Between 2024 and 2025, we translated the book into 15 languages, and in October 2024, Cybersecurity Alphabet was commercially released in Russian.
- [Digital Schoolbag](#) is a practical guide for parents, offering tips on how to protect children both online and offline: from setting up devices to conversations about safety and trust. The guide is available for free and is aimed at parents without a technical background.

Regional initiatives

Our work to protect children online extends far beyond the borders of one country.

- In **Italy**, as part of the Privacy Tour organized by the Italian Data Protection Authority, we distributed 500 copies of Cybersecurity Alphabet to people participating in educational events.
- In **Germany**, at the largest IT industry exhibition, it-sa Expo&Congress in Nuremberg, participants received 500 copies of these books.
- In **Morocco**, Kaspersky experts participated in a [family day](#) at the Cadi Ayad School in Casablanca, where they spoke to children and parents about digital risks and ways to protect themselves. They also presented Cybersecurity Alphabet. About 50 children and their parents participated in the event.

KidZania: Safety through play and experience

In March 2025, we opened the [Cyber Research Center](#) at KidZania Santa Fe in Mexico. Here, in this renowned entertainment capital, children learn the basics of cybersecurity by playing, completing practical tasks, and learning to recognize digital risks. Kaspersky's Cyber Research Center at KidZania will allow visitors to become cyber investigators, tackling challenges such as digital fraud, online espionage, and identity theft. Children will also develop key skills like critical thinking and problem-solving while learning how to protect their privacy and security on the internet.



Our plans for 2026–2027

- Publish analytical reports and educational materials on children's online safety
- Participate in educational and awareness-raising projects to improve digital literacy among children, parents and teachers
- Open new cyber research centers at KidZania, an educational theme park for kids, in India and the UAE.
- Develop partnerships with international law enforcement organizations, coalitions, and non-profit organizations to combat stalking.