Digital security

Our goal is to protect users against cyberthreats with Kaspersky's products and initiatives.

In today's digital society, technology is ingrained in people's daily lives, with the number of cyberthreats constantly on the rise as a result. You may be exposed to danger while performing simple actions such as exchanging messages, downloading photos, or transferring money online. Threat actors are improving their attack methods as they invade people's personal lives. We are committed to protecting users' interests in the digital realm and making it a place where everyone feels safe.

Kaspersky solutions

>411,000
malicious files detected daily in 2023

~125 million
malicious files found from January to October 2023

>437 million
malware-class attacks blocked from November 2022 to October 2023

33,790,599
malware, adware, and riskware attacks blocked in 2023

135,980,457
malicious email attachments blocked in 2023

709,590,011
attempts to click on phishing links thwarted in 2023

How we protect users against cyberthreats

To counter cyberthreats, we create high-quality products and promote awareness by teaching users the basics of digital literacy and the fundamentals of cybersecurity for corporate clients.

TC-SI-230a.2

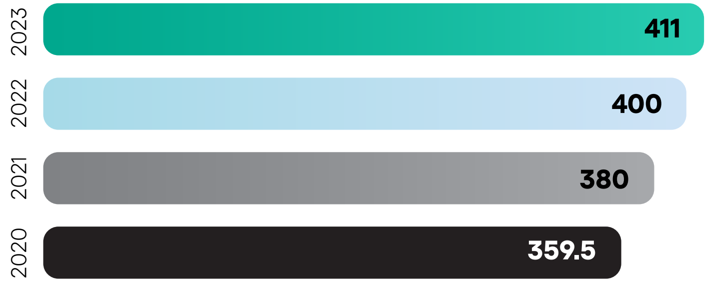
Our solutions protect users against a wide range of cyberthreats, from online fraud to data leaks and targeted cyberattacks. To gain control of computer systems, hackers use various types of malware:

- **Viruses.** Programs that infect files with malicious code. They replicate themselves to spread throughout a computer system.
- **Trojans.** Programs that perform actions that are unauthorized by the user: they destroy, block, modify or copy information, and disrupt the operation of computers or computer networks. One of the key differences between this type of malware is its inability to self-replicate. The first Trojans appeared in the late 1980s and fully lived up to their name, posing as legitimate software.
- **Spyware.** Programs that secretly monitor a user's actions and collect information that hackers can use for their own purposes.
- **Ransomware.** Software that encrypts files and data on a user's computer, after which hackers demand a ransom to restore access to information, claiming that otherwise the user will lose their data. Attackers may also threaten to make compromised data publicly available.
- **Adware.** Advertising-supported software that can create problems on a user's device.
- **Botnets.** Computer networks infected with malware that hackers use for their own purposes.

Users and companies can also fall victim to phishing, scams, phone fraud and DoS attacks.

The modern world has seen a significant increase in the number of cyberthreats as digital technology and the internet evolve. The number of malicious files is growing each year: whereas in 2020 we detected about 360,000 new malicious files per day, in 2023 this figure was already up to 411,000, a 3 percent increase from the year before.

Number of malicious files detected daily by Kaspersky, thousand



Combating cyberstalking

# Objective

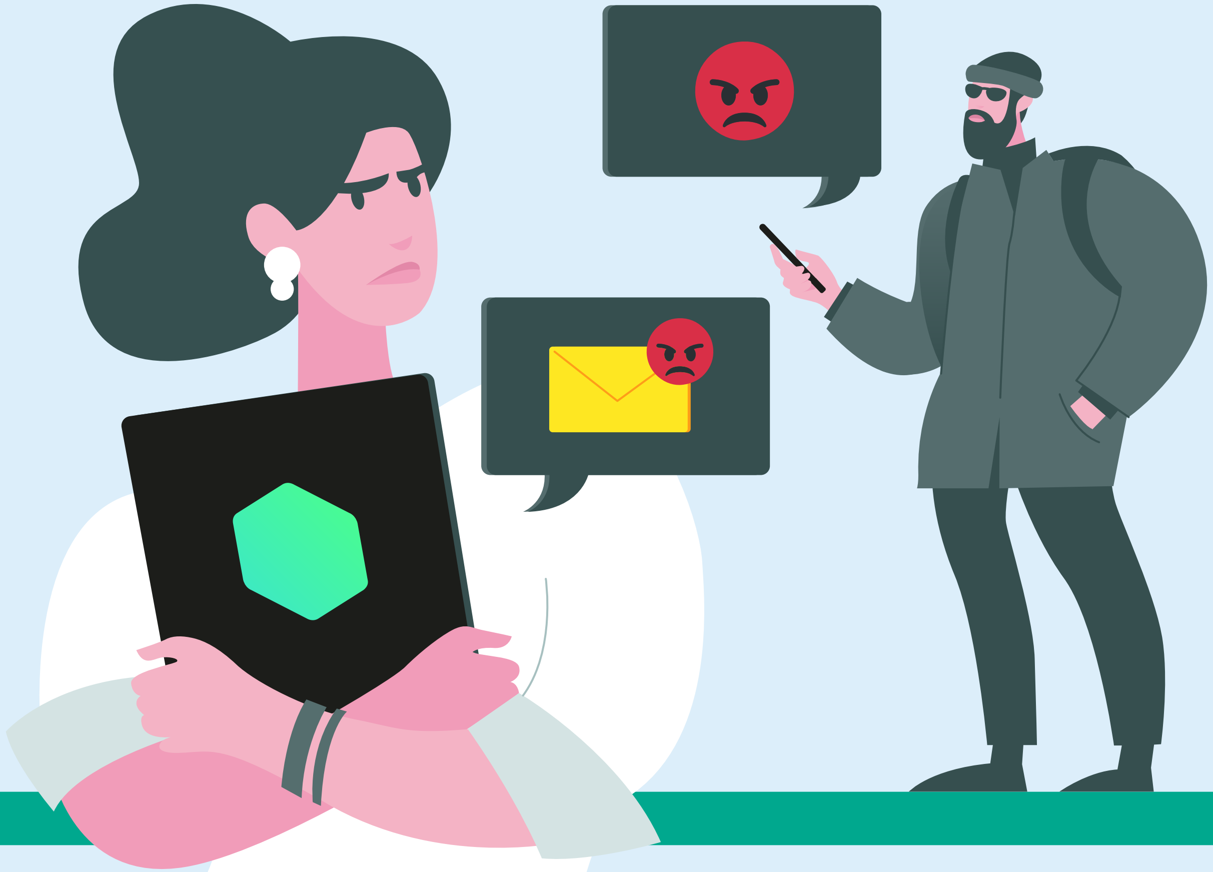
Protect users against digital harassment

Our research shows there has been a steady increase in the number of attacks using digital surveillance software, otherwise known as stalkerware. In 2023, the victims were most often residents of Russia, Brazil and India, but in general this phenomenon has spread throughout the world.

Stalkerware is commercially available software that can be discreetly installed on smartphone devices, enabling perpetrators to monitor an individual's private life without their knowledge. It isn't solely a technical issue; it's also a social problem requiring input from all parties involved in the digital realm to be effectively addressed. We notify users about this threat through our products, including Kaspersky for Android, which offers a solution to protect smartphone data and warn users about the detection of stalker applications on their device. We are also working to address the problem of cyberstalking by partnering with non-profit organizations, industry experts, research companies and government agencies worldwide to offer the TinyCheck digital surveillance tool.

>31,000

users worldwide experienced cyberstalking in 2023 (+5.9% vs. 2022)



# Solutions

GRI 203-1

Take part in projects to protect users against stalkerware

In 2019, Kaspersky co-founded the Coalition Against Stalkerware, an international working group featuring IT companies, non-profit organizations, research institutions and law enforcement agencies, which seek to combat stalkerware and domestic violence.

Today, the coalition includes more than 40 organizations that share their expertise in domestic violence survivor support and perpetrator work, digital rights advocacy, and cybersecurity to address the criminal behavior perpetrated by stalkerware. Users who suspect they are being spied on via a mobile device can seek help on the Coalition's website, which is available in seven languages.

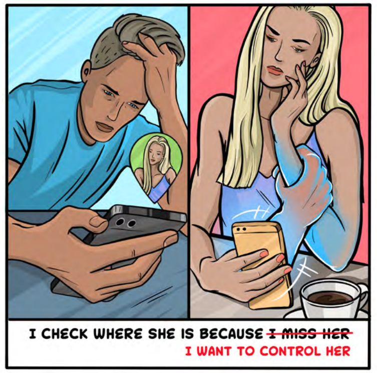
>40

organizations have joined the international Coalition Against Stalkerware co-founded by Kaspersky

Kaspersky also works with the European Network for the Work with Perpetrators of Domestic Violence (WWP EN). In September 2022, we launched the global campaign #NoExcuse4Abuse, which aims to raise public awareness about how people in relationships abuse technology. We believe it is important to refute the myths surrounding this issue and help victims recognize the signs of possible digital abuse. The campaign resulted in the release of comics that show examples of inappropriate behavior in relationships disguised as "caring". The project's main goal is to challenge the arguments and justifications used by abusers in order to deter them from committing violence against their partners.

78,100

reach of the #NoExcuse4Abuse campaign

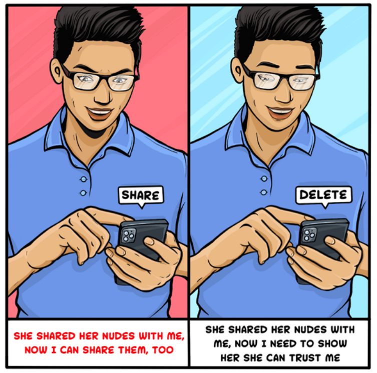


SHE CAN SEE MY PHONE, TOO
SHE'S AFRAID OF WHAT I WILL DO, IF SHE DOESN'T SHOW ME HER PHONE

WE'RE IN LOVE, ~~SO SHE SHOULD HAVE NO SECRETS~~
SO I TRUST HER

CHECKING HER EMAILS ~~ISN'T A BIG DEAL~~
IS CONTROLLING BEHAVIOUR

YOU WANT TO SHOW OFF NUDE PHOTOS OF YOUR HOT GIRLFRIEND
YOU JUST COMMITTED A CRIME


SHARE
DELETE
SHE SHARED HER NUDES WITH ME, NOW I CAN SHARE THEM, TOO
SHE SHARED HER NUDES WITH ME, NOW I NEED TO SHOW HER SHE CAN TRUST ME

Organize research and educational projects against cyberstalking

Kaspersky together with various international companies, the academic community and non-profit organizations is taking part in the study on how to protect victims/survivors of Intimate Partner Violence (IPV) from the risks created by digital technologies together with various international companies, the academic community and non-profit organizations. To participate in this joint study, we have formed a partnership with the UK research and innovation agency UKRI.

The project was launched in 2023, and will continue until 2026. Kaspersky provides support with its expertise in combating cyber violence and stalking, and by participating in additional events.

Notify users about the threat of cyberstalking

Our Company was among the pioneers in the industry to alert users about its solutions for detecting stalkerware on their devices.

In June 2022, Kaspersky launched a portal about TinyCheck, a free and secure open-source tool for non-profit organizations and police departments that work with victims of digital stalking. This solution is installed on a separate external device – a Raspberry Pi microcomputer – instead of a smartphone. TinyCheck can view outgoing internet traffic, analyze it in real time and recognize connections to the control centers of stalkerware developers. At the same time, the solution does not allow the initiators of surveillance to learn about such checks.

In 2022, we expanded our privacy notification functions as part of the launch of a new line of solutions to protect users' digital lives. TinyCheck users now receive a warning not only regarding the presence of stalkerware on their device but also about the potential consequences if they choose to delete the application. This could potentially escalate the situation by alerting the individual who installed it. In addition, the stalking victim should be aware that by deleting the app, they risk deleting important data or evidence that could be used by law enforcement.

DeStalk

From 2021 to 2023, Kaspersky partnered with the DeStalk project, which was launched as part of the EU Rights, Equality and Citizenship program. The project brought together five partner organizations, cybersecurity experts and representatives from research institutions, public organizations and the government.

As part of the DeStalk project, we trained more than 350 professionals who provide assistance to female victims and deal with issues of violence, as well as government officials. They learned effective methods to combat cyberstalking and how to counter other forms of digital gender-based violence. We have also worked hard to provide a wider audience with information about digital violence and how to hinder it.

DeStalk
detect and stop stalkerware and
cyberviolence against women

More than 350 practitioners

addressing gender-based violence were trained as part of the DeStalk project

DeStalk e-learning

As part of the DeStalk project, Kaspersky has developed an electronic training course called The DeStalk e-learning on how to recognize and combat cyber violence and stalkerware in five languages. The goal of the course was to train 80–100 professionals from 20–30 different organizations, including:

- Professionals working with victims/survivors of cyberviolence and stalkerware
- Professionals working with perpetrators of domestic violence
- Public officers working in the field of domestic abuse

The course consisted of four lessons, including theory and testing focused on gender-based cyber-violence, different forms of cyber violence, the topic of cyber-surveillance and stalkerware, working with victims and survivors of violence and/or perpetrators. The electronic course is available on the DeStalk website.

130 people

passed the DeStalk e-learning course

Protection against ransomware

# Objective

Combat ransomware

Our data shows that ransomware attacks are becoming more sophisticated and are causing extensive harm to both companies and users. Targeted (and more complex) attacks on businesses – both enterprises and small and medium-sized businesses – are particularly dangerous. Organizers of targeted attacks carefully select their targets – governments, specific organizations or individual groups of people within a particular enterprise.

Ransomware has remained one of the most pressing cyberthreats of recent years, with attacks becoming increasingly sophisticated. Between November 2022 and October 2023, ransomware Trojans attacked 193,662 unique users, including 52,999 corporate (enterprise) users and 6,351 users from small and medium-sized businesses.

In 2022, Kaspersky discovered two new ransomware cybergroups – RedAlert and Monster. Most recently, their main goal has been to damage as many systems as possible by simultaneously adapting their malicious code to multiple operating systems. In addition, from July to September 2022, we detected two waves of attacks that affected Albanian government e-services using ransomware and wiper malware. The hackers used stolen Nvidia and Kuwait Telecommunications certificates to sign their malware.

Kaspersky solutions

Detected over

74.2 million

attempted ransomware attacks (+20% vs. 2021)

Identified

23,364

ransomware modifications and detected 43 new families from November 2022 to October 2023[1]

Prevented ransomware attacks on the computers of

193,662

unique users from November 2022 to October 2023

[1] Source – https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/28102415/KSB_statistics_2023_en.pdf.

# Solutions

Develop products to protect against ransomware

Kaspersky has developed and published a set of recommendations for users who want to protect themselves and their business against ransomware attacks. Users benefit from our products, which have proven to be highly effective in protecting against ransomware in tests[1]. In particular, three Kaspersky solutions – Kaspersky Endpoint Security for Business, Kaspersky Small Office Security and Kaspersky Standard – successfully passed all the tests, earned 35 out of possible 35 points and earned "Advanced Approved Endpoint Protection" certificate for business security solutions and "Advanced Certified" for consumer product.

Provide the latest cyberthreat intelligence

Kaspersky offers awareness services about modern cyberthreats that will help any organization effectively counter them. Kaspersky Threat Intelligence provides up-to-date technical, tactical, operational and strategic threat intelligence from our world-class analysts and researchers. This has helped Kaspersky become a trusted partner of law enforcement and government organizations around the world, including INTERPOL and various CERT units.

You can request access to this service here.

158

global press releases on cyberthreats were issued by the Company during the reporting period

In addition, the Company regularly conducts special research and surveys, which helps to inform users about the cyberthreats that they may face in real life without even suspecting it. During the reporting period, we shared our findings on:

- Vulnerabilities in popular smart pet feeders, which enable hackers to turn the feeder into a surveillance tool and change the feeding schedule, thereby jeopardizing the pet's health.
- An online fraud scheme that targets pet owners who want to buy imported medications for their pets. Using Telegram channels, scammers defraud people of money and financial information.
- Tourist traps during the summer holidays. Travel experts and cybersecurity specialists warned users about three different scams involving tickets, accommodation and surveys.
- A new campaign to steal cryptocurrency through a fake Tor browser. Under the guise of the Tor browser, hackers distribute the CryptoClipper Trojan on third-party internet resources. When users log into the system, they register in autostart, which is disguised as the icon of a popular app, for example, uTorrent. As soon as the clipper malware finds an address in the clipboard that looks like a crypto wallet, it immediately changes it to an address that belongs to the hacker. More than 15,000 users in 52 countries were affected by the malware campaign.
- Technologies that create deep fake videos. Kaspersky experts discovered that the darknet offers services to create such videos for as much as US$20,000 per minute. Deepfakes can be generated for various purposes, including scams, political manipulation, revenge and cyberbullying.
- Operation Triangulation – a zero-click attack targeting Apple mobile devices via iMessage to run malware gaining complete control over the devices and user data. The final goal was to hiddenly spy on users.
- The latest spam and phishing attacks: statistics and pathways that threat actors exploited in 2023 in a new report.

In addition, we created educational videos to talk about crypto phishing, participated in a webinar on cryptocurrency threat landscape trends in this regard and also published our own research on this topic.

[1] The AV-TEST was conducted in August 2023.

How we uncovered Operation Triangulation

Working together against spyware

In early June 2023, Kaspersky researchers discovered a previously unknown mobile APT campaign targeting iOS devices, which was later named Operation Triangulation. The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data.

Experts found that the embedded spyware transfers information from the victim's device to remote servers without being noticed. The attackers were interested in the owner's microphone recordings, photos from instant messengers, geolocation and data about other actions.

"I have some big news about a cyber-incident we've uncovered. Our experts have discovered an extremely complex, professional targeted cyberattack that uses Apple's mobile devices," **Eugene Kaspersky** wrote in his blog.

If a user is blocked from updating iOS, this is an indirect sign that the Triangulation malware has infected a device, Kaspersky said.

Find out more about Operation Triangulation and how to check your iOS device on Securelist.

What was the result?

We published a comprehensive guide on how to manually check iOS device backups for possible indicators of compromise using the Mobile Verification Toolkit.

Kaspersky developed the free triangle_check utility for computers running Windows and Linux operating systems, which can be used to check if an iPhone is infected with Operation Triangulation malware. To check for the malware using this utility on Windows and Linux, just download the binary assembly, while on macOS you can install it as a Python package.

Apple acknowledged the problem and released updates that eliminate the vulnerabilities.

GRI 203-1

NO MORE RANSOM

To combat malicious actors Kaspersky together with Europol, the Dutch National Police initiated the creation of the No More Ransom initiative in 2016. The initiative provides decryption tools, educates the public about ransomware risks and promotes cybersecurity best practices to counteract this pervasive cyber threat.

Our contribution to the No More Ransom initiative

Working together against ransomware

360,000
downloads of Kaspersky's free decryption tools

39
ransomware families targeted

2 million
victims were able to decrypt their data

The international No More Ransom initiative, co-founded by Kaspersky, provides decryption tools, educates the public about ransomware risks, and promotes cybersecurity best practices to counteract this pervasive cyberthreat.

This initiative represents a unique partnership between governments, law enforcement agencies, antivirus companies and educational institutions.

In March 2023, Kaspersky released a new version of the decryption tool to help victims of ransomware modifications based on previously leaked Conti code.

What was the result?

Our joint efforts have made the digital environment safer, helping hundreds of thousands of users and reducing the overall threat level in the online world.

Kaspersky's free decryption tools, which are available as part of the No More Ransom initiative, have been downloaded more than 360,000 times in the last five years. They can be used to decrypt files locked by 39 ransomware families. These tools provided victims with the means to recover important data without having to comply with the cybercriminals' demands. No More Ransom recently celebrated an important milestone, as more than 2 million users were able to recover data thanks to the initiative.

Training users on the basics of cybersecurity

# Objective

Provide users with self-defense tools

Being able to ensure your own online security is becoming a fundamental skill for individuals in the modern world. By teaching our users the basics of cybersecurity, we are able not only help them recognize potential threats, but also provide them with the tools to protect themselves. In doing so, we are investing in a secure digital future for everyone.

# Solutions

Kaspersky Academy

>8,000

students studied at Kaspersky Academy in 2022–2023

Back in 2010, we launched Kaspersky Academy to scale educational initiatives and make them accessible to everyone. We planned to turn the portal into a global university, able to house all the educational materials related to information security, and managed to implement this project.

At present, Kaspersky Academy speakers include the Company's department heads, leading industry specialists and invited information security experts. In 2022–2023, more than 8,000 students from Russia, Europe, Saudi Arabia, Rwanda and other countries were trained at Kaspersky Academy.

Advantages of Kaspersky Academy:

- It is one of the ways to gain access to content from the Education.kaspersky.com platform.
- It is adapted to two product formats:
  1. Video lessons + tests + certificate.
  2. Video lessons + live broadcasts + tests + final test + certificate.
  3. Online workbook format with auto-check + certificate.
- It allows to track students' results – both intermediate and final.
- It notifies students about upcoming webinars.
- It can quickly customize the training format and collect analytics to suit the customer's needs and project.
- It can manage the duration of students' access to the platform.

Courses launched in 2023:

- "Cybersecurity. Entry level". An updated flagship course for the Russian-speaking audience, which examines all the main aspects of information security. The course targets both IT specialists and students, as well as private users.
- "Cybersecurity for Senior Executives". The course gives students an understanding of cybersecurity as a system and shows how cyber risks affect businesses and how they can be managed.

Key Academic Affairs projects for school and university students in 2023:

SafeBoard offers 15+ areas for IT internships (more than 500 students have enrolled in the program since 2016). Over the eight years this program has existed, more than half of its participants have joined the Company's staff and are now employed, including those at the middle, senior and lead levels

Secur'IT Cup – an annual international competition of student cybersecurity projects (30+ participating countries and more than 2,000 applications from students each year)

Technology Valley – a summer internship for school and college students in Russia (more than 1,200 people registered in 2023 and 45 participants completed in-office internships)

Cyber Generation – a training program for students and recent graduates of Saudi Arabia (91 participants)

Kaspersky Academy Alliance – a special program for universities that integrates cybersecurity expertise and the latest Kaspersky technologies into the student learning process

We work with:

~200 universities

in **42** countries

>60 educational institutions in Russia and the CIS.

Cybersecurity training for non-profit organizations

GRI 203-1

Cybersecurity is crucial for the effective operations of non-profit organizations (NPOs), which rely heavily on digital technologies. Kaspersky regularly conducts training for NPOs to improve their level of protection against constantly evolving online threats. These partnerships help create a safer and more sustainable digital future for everyone.

In 2022–2023, we organized the following training for NPOs:

- **Cyberstalking.** Our leading information security threat researchers conducted two training sessions on the problem of cyberstalking: for the 'Blagie Dela' (Good Deeds) Foundation from Kazan and the Nizhny Novgorod Women's Crisis Center, which provides free psychological and legal support to people dealing with violence and abuse. We also trained the Nizhny Novgorod Women's Crisis Center, on how to use the free open-source tool TinyCheck, which can detect surveillance software installed on a device without notifying the stalker.

- **Doxing**[1]**.** Together with the Singapore Council of Women's Organisations[2], we held a free seminar on combating doxing. Our experts explained how people can reduce the risks of their personal data being misused and protect their own and other people's personal data, introduced the participants to reliable security software and revealed the possible motives of hackers.

- **Cyber-hygiene.** In partnership with the todogood social change platform, we conducted an intensive online course about cyber hygiene as part of the "I Can" program for vulnerable social groups, including women in difficult life situations, people with disabilities and older people. The program's goal is to support individuals in professional retraining, adjusting to online learning and work, navigating socio-cultural shifts, and adopting new technologies. A total of 946 people took the recorded and online intensive course, passed the test and received certificates.

We have also created several cybersecurity projects in partnership with international organizations. In particular, in March 2023, we launched the Kids' Cyber Resilience Project, which aims to educate children on how to keep themselves safe online while helping them build resilience internally in the Asia-Pacific region. This project involves multiple stakeholders, including parents, educators, students, non-profit organizations and government representatives.

- Together with the Center For Cybersecurity, a Singapore-based cybersecurity training organization, and The HEAD Foundation, an international charitable organization that does philanthropic work in education, Kaspersky launched its global **Kids' Cyber Resilience Project** in Singapore with a panel discussion on how a collaborative and proactive approach to online security can benefit children in digital environment.

- **Online seminars on cyber-resilience** were held for educators in the Asia-Pacific (APAC) region in partnership with the Coalition Against Bullying for Children & Youth (CABCY). As part of a series of webinars, we examined the topic of bullying and cyberbullying in more detail. The CABCY helped participants learn more about this complex issue and understand the role of adults in supporting children.

- **Face-to-Face.** A cyber-resilience workshop on basic cyber hygiene for educators from 71 public schools in Valenzuela City was held in September 2023 in collaboration with the Philippine Department of Education Schools Division Office. The workshop aimed to provide teachers with knowledge to effectively help their students become cyber-resilient.

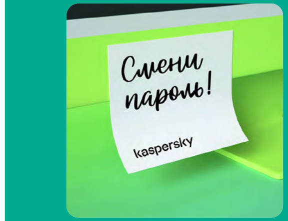
- **Cyber Resilience Day.** In collaboration with Majlis Bandaraya Petaling Jaya (MBPJ) in Malaysia, Kaspersky co-presented an introductory cybersecurity awareness and resilience training session for more than 250 PJ Secondary School learners from 10 public schools. The program aims to educate the participants on how to keep themselves safe online while helping them build resilience internally.

- **Cyber security workshop in India.** In partnership with the Information and Security Analysis Center (ISAC) Foundation, Kaspersky teamed up to deliver a workshop on cyber security hygiene, Indian cyber laws, and dealing with various forms of cybercrimes. Approximately 150 teachers from more than 30 schools participated in the event, which aimed to increase their confidence to share cyber resilience practices with their students as well as improve their capacity to support children to recover from setbacks.

[1] Doxing is the practice of publicly disclosing personal information about people on the internet without their consent.
[2] The Singapore Council of Women's Organisations (SCWO).

Our contribution to improving cyber-hygiene awareness

A podcast aimed at educating people on safeguarding themselves from digital threats



The podcast Change Your Password! is a talk show on various issues surrounding information security hosted by journalist and writer Alexey Andreyev, Kaspersky Chief Security Expert Sergey Golovanov and Kaspersky Chief Technology Expert Alexander Gostev.

The podcast has been airing since 2021 and has – so far – had three seasons. It can be found on every popular podcast platform including Apple Podcasts, Yandex Music, Google Podcasts, VK, Castbox, YouTube.

The hosts of the Change Your Password! podcast discuss key issues in the world of digital security and help listeners understand the impact of current cyberthreats on users and businesses.

Where is personal data leaked?

Why is the Internet of Things dangerous?

Does artificial intelligence offer protection or pose a threat?

Hosts and guest experts from other industries (banking, e-commerce, communications, etc.) provide answers to these and many other questions.

In autumn of 2023, an open recording of the Change Your Password! podcast became the first face-to-face event of the Cryptography Museum Discussion Club. Experts discussed how Russian codes differ from foreign ones, what cryptographic protection modern people need, why quantum computers resemble “apple trees on Mars,” and also answered numerous questions from listeners.

What was the result?

The podcast was listened to

>400,000 times

over three seasons

Over three years, the podcast has evolved into a primary outlet for the most up-to-date information concerning digital threats. Today, Change Your Password! helps listeners create a safer online space for themselves and their businesses.

- The third season of the podcast had been listened to more than 100,000 times as of the end of 2023, and the podcast has been listened to over 400,000 times in total.
- Since 2022, Change Your Password! has regularly been among the top podcasts about technology on Apple Podcasts, as well as in thematic selections from leading media outlets.

Ensuring children's online safety

# Objective

Protect children in the digital world

For several years in a row, the Company has consistently conducted surveys on children's online safety to grasp the impact of the internet on kids, their interests and the potential challenges they may face online.

The 2022 survey conducted by Kaspersky in major Russian cities[1] showed that 77 percent of children aged seven to 10-years-old had been introduced to gadgets before starting school. A new survey conducted by the Company in 2023 revealed that the overwhelming number of primary school students (88%) now have their own phone or tablet. Almost every high school student has his/her own gadget. Starting from middle school, a significant percentage of children spend almost all their free time on gadgets. Parents are concerned about who their children interact with online, whether they encounter aggression and what sites they visit.

88%

of primary school students have their own phone or tablet

Over the past year

55%

of children have come across violent videos or videos with adult content online

29%

of parents do not know what information about their children is publicly available online

"To safeguard children from a diverse range of online threats, a combination of both technical and non-technical protective measures is required. The technical measures include special settings, such as family accounts, parental control programs, antivirus programs and automatic caller ID. Non-technical measures include constant attention to digital awareness, including information security issues. It is crucial to teach children the basics of digital hygiene from a very young age. Over time, this will become more effective than parental restrictions alone."

Andrey Sidenko,
Lead web content analyst and expert on children's online safety, Kaspersky

[1] More than 1,000 pairs of parents and children took part in the survey.

# Solutions

Teach children the basics of cybersecurity

Creating a safe online environment for children is a top priority that will shape our future. Kaspersky is addressing this challenge both on its own and in partnership with relevant ministries, agencies and other international organizations.

To understand how the internet influences young users, what they are interested in and what troubles they may encounter online, Kaspersky has been conducting surveys and studies on children's online safety for several years in a row. Below are a few of them that were presented during the reporting period.

- **"Adults and Children on the internet"** is a series of surveys on children's online safety and a report with the same name. In 2022, Kaspersky commissioned a survey that was conducted by the Online Interviewer company in May–June 2022. The company arranged a total of 2,008 online interviews with 1,004 pairs of parents (or single parents) and children aged three to 18-years in major Russian cities. The survey topics were selected to reflect the situation in various areas of online life. The results, along with comments from a Kaspersky expert on children's online safety, helped adults better understand the interests of young users and showed what needs to be done to make the digital world safer for them.
- **A new survey on children's online safety**. In May–June 2023, Online Interviewer specialists conducted a new study for Kaspersky to find out the latest about children's online safety. They conducted 2,032 online interviews (with a total of 1,016 pairs of parents and children), which revealed the following statistics:
  - 29 percent of parents do not know what information about their children is publicly available on the internet;
  - More than half (55%) of children said they have seen violent videos or videos with adult content on the internet over the past year;
  - A third of parents want their children to work in IT when they grow up, while the share of children who would like to work in this industry in the future is even higher (41%);
  - 30 percent of parents surveyed in Russia are concerned about the problem of children's internet addiction, while more than half of parents (54%) believe that children nowadays are addicted to gadgets and the internet;
  - Most children spend more than an hour a day on the internet starting from the age of seven;
  - More than half of parents (53%) are confident that in 10–15 years touch screens and blackboards will replace the usual teaching tools in schools, 39 percent noted that tablets will replace textbooks and 37 percent believe that voice assistants will be used in teaching in the future.
- **Kids on the web 2023.** Kaspersky regularly conducts global research on children's online safety based on anonymized statistics collected by the Kaspersky Safe Kids solution. The report for 2023 examines the categories of websites that kids visit most often across various platforms, the apps they spend the most time on, and what specifically piqued their interest during the period from May 2022 to May 2023.

We also organized several educational events and projects on cybersecurity for schoolchildren, teachers and parents during the reporting period.

- **"Mom, I'm Going To Be a Blogger!"** In June 2022, Kaspersky launched its own online interactive mini-series called "Mom, I'm Going To Be a Blogger!", 10 two-three minute long video episodes released in 2022. The series, along with the main character Mila, taught children how to safely record vines, avoid scammers, how to distinguish a phishing site from a real one and why it is important to follow netiquette rules on the internet.
- **"Digital Lesson".** In 2022 and 2023, Kaspersky continued taking part in the project "Digital Lesson" conducted by the Digital Economy autonomous non-profit organization with the support of the Russian Ministry of Education and Ministry of Digital Development. In 2022, we also made a series of lessons dedicated to researching cyberattacks, while children were taught about the issues surrounding mobile security in 2023. The latter course was completed more than two million times by learners from grade one to 11. They learned what types of malware exist for mobile devices, how to protect their data on the internet and were also introduced to various cybersecurity professions.

→ For more about the project, please see p. 104

- **"Digital Outreach".** Kaspersky and the Digital Economy autonomous non-profit organization, with the support of the Russian Ministry of Education and Ministry of Digital Development, created a series of short cartoons for children about digital security and privacy. In 2023, this series was added to the useful materials supplement of the national educational project "Digital Outreach".

- **Cybersecurity course for schoolchildren.** In October 2023, Kaspersky gave access to the online course "Information Security Basics" for seventh grade children. The course for learners in grades 8–11 will be available in the near future. It is a practical course that can be used by teachers in computer science classes and as part of extracurricular activities, as well as by parents and learners themselves.

- **Educational events for school children and teachers in Russia and the CIS.** In 2022–2023, more than 150 online and offline events were held for school children and teachers at secondary schools, as well as for parents in 26 regions of Russia and the CIS.

- **Kaspersky Safe Family Spain.** Kaspersky conducted cybersecurity lessons via a special puppet theater play for more than 16,000 Spanish children through its Familia Segura program. It includes the "Kasper, Sky and the Green Bear" initiative, which also aims to improve the cyber awareness of teachers and parents.

- **#ShareAware Hub.** Kaspersky helps parents and children improve their online safety with various tips. The hub provides lots of useful materials, quizzes, research and advice on how to use multimedia on the internet and avoid digital threats.

- **Kids on the internet.** An online safety course developed by Kaspersky. It helps parents to safeguard their children online and build trust. Kids get acquainted with digital literacy and gain online communication skills. It is also intended for anyone who uses the internet and wants to protect themselves and loved ones from modern mobile threats.

- **Hacker:HUNTER.** The Company took part in the production of a series about real cyber incidents. A new season was released in 2023, showing how cybercriminals get children involved in their activities and turn them into hackers, and how law enforcement agencies are combating this issue.

- **Cybersecurity Alphabet.** To help improve the digital awareness of children and their parents, the Company's experts prepared a fun and informative book and poster for children and their parents on how to recognize fraudsters' tricks and learn the importance of staying safe online. The book uses an A to Z approach to introduce readers to new technologies, common cyber risks and tools to protect themselves against them. Cybersecurity Alphabet is available in English for anyone to download on the Company's website. The book and poster will also be available soon in Spanish, Italian, French and Russian.

Cooperate with IT companies and regulators to protect children online

We strive to make the online space for children as safe as possible. Kaspersky is one of founders of the Alliance for the Protection of Children in the Digital Environment, which was created by Russia's largest IT companies in September 2021.

In 2022, Kaspersky, Yandex and VK launched a pilot project as part of the Alliance to identify and block content related to the distribution of child pornography, as well as so-called sexualized content involving minors.

In October 2023, the Alliance held a road show in Kazan called "Your Route Is Ready: Online Safety Paths". At this event Kaspersky shared the results of a study showing that the majority of parents in Russia (87%) are taking measures to protect their children from dangers on the internet. However, it also showcased that only 48 percent of adults themselves follow all the prescribed rules, which reduces the effectiveness of these measures. Our experts reminded parents of the need to be a good example for their children and compiled a checklist with recommendations on what to look for when choosing an appropriate parental control solution.

In December 2023, the Alliance hosted a two-day educational marathon called "Safe Digital" in St. Petersburg, which focused on the guidelines for maintaining online safety. The event was mainly attended by children and teenagers, who had a chance to take part in an IT quiz, special training sessions, roundtables and seminars while parents and teachers discussed digital safety issues. A business program was also organized with IT experts and representatives of the government, business and public organizations. The marathon was attended by the Alliance's founders.

Kaspersky Safe Kids

We are dedicated to safeguarding children from online threats and creating an environment where they can use the internet as safely as possible. To achieve this, we offer our solution Kaspersky Safe Kids – a parental control application that protects children against age-inappropriate content and helps form good digital habits. There is also a free version of this solution available.

Main functions of Kaspersky Safe Kids

Search safely

The application works with search engines and blocks unwanted requests. Once a week, parents receive reports about what their child was searching for online.

Control usage of the application

The basic function blocks applications that are not suitable for children. Usage is also time controlled (you can set time intervals and assign days off).

Control screen time

The application can set the specific number of hours of screen time allowed per day and lock the device if the limit is reached. You can also turn off the device at specific times.

Set a secure perimeter

Thanks to the GPS option, the application sends a notification to parents if their child leaves a designated location (e.g., school).

Monitor potentially dangerous contacts on social media

Parents cannot read their child's messages, but the application notifies them about any correspondence and allows them to see the profile of the person with whom their child is messaging.

In 2023, we updated the Kaspersky Safe Kids solution twice. The new versions have an improved design and interface, new functions for managing screen time, videos with tips on raising children, an easy functional configuration and other useful information for parents. The application can be installed on desktops and mobile devices with all popular operating systems. Children can now request more time from their parents to use the device, and all parents have to do is approve or deny the request.

7
AV-TEST certificates

7
AV-Comparatives certificates

>1 million
downloads worldwide

106 million
harmful websites blocked

Kaspersky Safe Kids testing results

The report released by the independent laboratory AV-TEST in December 2022 indicates that Kaspersky Safe Kids blocked:

- 92% in Windows for potentially inappropriate websites (up from 90% in 2021);
- 87% in Android for for potentially inappropriate websites tested (85% in 2021);
- Almost 100% of the most undesirable category "Adult Content" content is blocked on Windows.

Our contribution to protecting children in cyberspace

Teaching cybersecurity with the “Kasper, Sky and the Green Bear” puppet show

The number of children who use digital technologies is constantly on the rise. At the same time, there are new forms of digital threats spreading throughout cyberspace that are especially dangerous for children due to their lack of experience and knowledge about the threats lurking there. Cyberbullying, sextortion and other types of harassment have become daily problems for children and teenagers, which is why Kaspersky has made it our mission to protect them in the online world.

As part of the Safe Family program, the Company launched the “Kasper, Sky and the Green Bear” initiative in Spain, an adaptation of Marlies Slegers’ book for children aged six to nine years, which introduces them to the digital world and teaches them how to use the internet safely. Kaspersky turned this book into a puppet show that not only educates children, but also seeks to inform teachers and parents that cyberthreats are much more than just a simple virus today.

Thanks to Kaspersky’s efforts, thousands of children, teachers and parents have learned how to use the internet safely. In addition, the “Kasper, Sky and the Green Bear” campaign received the following accolades at the Social Enterprise Awards 2019:

- Best responsibility project for the protection of children
- Best social responsibility project in the field of cybersecurity
- Best responsibility project in the fight against bullying

In addition, Gala Acción Social presented an award to Kaspersky with the distinction “Company with the Best Actions To Protect Children.”

What was the result?

Since its premiere in October 2018, the play has been performed in

106

Spanish schools,

with

146

performances

staged to

16,805

students

35

performances took place during the 22/23 school year,

reaching

3,684

students.

Our achievements

Kaspersky was recognized at the Social Enterprise 2023 awards for its work to combat digital gender-based cyberviolence exercised through stalkerware. The Company received awards in the following categories: “Best Corporate Social Responsibility in the Cybersecurity Sector”, “Best Initiative for the Prevention of Gender-based Violence in the Cybersecurity Sector” and “Best Internet Security Project in the Cybersecurity Sector”. In addition, the organizer of the Gala Acción Social awarded Kaspersky the “Special Prize for the Company with the Best Cybersecurity Initiatives” and “Platinum Company and Company of the Year”.

Our plans for 2024

- Develop partnerships to combat stalking with international law enforcement organizations, coalitions and non-profit organizations;
- Release a new report on the current state of stalkerware;
- Launch a course on cyber hygiene in two languages;
- Conduct the Kids Cyber Resilience project in the CIS and META[1] regions;
- Release an analytical report on children’s online safety with survey data for 2023;
- Publish the Cybersecurity Alphabet and poster in Russian, Spanish, Italian and French.

[1] Middle East, Turkey and Africa.