In fulfilling that mission we aim to become the global leaders in cybersecurity — by securing technology to ensure that the possibilities it brings become opportunities for each and every one of us.

Bring on endless possibilities. Bring on a safer tomorrow.

Eugene Kaspersky, CEO
Our key values that drive our work

Be there for you
We’ll always be there for you, for our customers, partners, prospects & colleagues. We never lose sight of the people we build our solutions for.

Be committed experts
Through our recognized technology expertise, we are committed to providing trust, safety and confidence. We never give up on our mission to make the digital world a safer place. And on this duty we always play fair.

Be cleverly inventive
Focused and ready to act – we share cutting-edge information with customers, partners, colleagues and prospects to keep them ahead of the curve.

Be powered by challenges
We constantly challenge ourselves and the status quo to do what others can’t. We deliver outstanding solutions to overcome obstacles of all kinds, and this is proven across our 25-year history.
Kaspersky at a glance

- Essentials
- Customers
- Geography
- Role in the global IT security community
Founded in 1997
and led by Eugene Kaspersky

Present on six continents in more than 200 countries and territories

Provides innovative IT security solutions and services for businesses and consumers

Facts about us

Essentials

Founded in 1997 and led by Eugene Kaspersky

Present on six continents in more than 200 countries and territories

Provides innovative IT security solutions and services for businesses and consumers

Numbers

> 15 million consumer product activations per year

> 5,000 highly qualified specialists

US $752 million global non-audited IFRS revenue in 2022
Our Next Generation solutions and services are available for a wide range of clients: from individual home users to large and small organizations, including big enterprises, critical infrastructure networks, and governments.

>220,000
Corporate clients worldwide

>400,000,000
Users worldwide are protected by our technologies
We work in a wide range of industry sectors. Our solutions and services successfully protect over 220,000 clients around the world, regardless of size or complexity.

- **Education**: ~6,800 customers in 101 countries
- **Government**: ~5,600 customers in 120 countries
- **Healthcare**: ~3,900 customers in 89 countries
- **Telecoms**: ~2,600 customers in 125 countries
- **Banking & finance**: ~7,900 customers in 119 countries
- **Construction**:
- **Oil & gas**
- **Information**:
- **Retail**:
- **Transport**:
- **Tourism**:
- **Public organizations**:
- **Private companies**:

Our customers

119 countries

~7,900 customers in 119 countries

~3,900 customers in 89 countries

~5,600 customers in 120 countries

~2,600 customers in 125 countries

~6,800 customers in 101 countries
We are an international cybersecurity company

200 countries and territories where we operate

30+ representative regional offices

Africa
South Africa

Asia
Greater China (China, Hong Kong)
Indonesia
Japan
Kazakhstan
Malaysia
Singapore
South Korea

Europe
Czech Republic
France
Germany
Israel
Italy
Netherlands
Portugal
Romania
Russia
Spain
Switzerland
UK

Middle East
Saudi Arabia
Turkey
UAE

North America
USA

Latin America
Brazil
Mexico

Transparency Centers
Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia
Woburn, USA
We participate in joint operations and cybercrime investigations with the global IT security community, international organizations such as INTERPOL, law enforcement agencies and CERTs worldwide.
Global Transparency Initiative

• Key transparency principles
• Global Transparency Initiative pillars
• Independent assessments and certifications
• Bug Bounty Program
Data sent to Kaspersky is crucial for protecting users, it is robustly secured and is not attributed to a specific individual.

We detect and neutralize threats, regardless of their origin or purpose.

We work with international organizations to fight cybercrime.

We are committed to the trustworthy development of our technologies and solutions.

We cooperate with the IT security industry in joint cybercrime investigations.
Launched in 2017, Kaspersky’s Global Transparency Initiative is aimed at engaging the broader information security community and other stakeholders in validating and verifying the trustworthiness of our products, internal processes, and business operations.

It includes a number of actionable and concrete measures:

- **Cyberthreat-related data infrastructure relocation to Switzerland.**
- **Creation of a global network of Transparency Centers in some regions, where Kaspersky’s trusted partners and government stakeholders can review the company’s code, software updates and threat detection rules.**
- **Third-party security assessments of Kaspersky’s engineering and data management practices verify the security of the company’s solutions.**
Global Transparency Initiative pillars

It includes a number of actionable and concrete measures:

- **Vulnerability management program**, under which security researchers can report vulnerabilities or bugs found in our systems for a designated reward.
- **Transparency reports**, in which we publicly share information about the number of requests for user data and technical expertise.
- **Cyber Capacity Building Program** – dedicated training to share security evaluation knowledge with the broader community.
Kaspersky Global Transparency Initiative

Cyberthreat-related user data storage and processing
Malicious and suspicious files received from users of Kaspersky products in Europe, North and Latin America, the Middle East, and also countries in Asia-Pacific region are processed and stored in Switzerland.

Transparency Centers
A facility for customers, partners and government stakeholders to review the company’s code, software updates and threat detection rules, along with other activities.

Independent reviews
Regular third-party assessment of internal processes to confirm the security of Kaspersky’s processes and systems, including:
• Regular SOC 2 audits
• ISO 27001 certifications for the company’s data systems

Bug bounty program
Increased bug bounties up to $100k for the most critical vulnerabilities aim to engage security researchers to supplement the company’s own work in ensuring the security of its solutions.

Transparency reports
Regular updates on how Kaspersky responds to requests from government and law enforcement agencies as well as to personal data-related requests from its own users.
Review options:

- **Blue Piste**
  (both remote & physical)
  An overview of Kaspersky’s transparency practices, products and services, as well as data management practices.

- **Red Piste**
  A review of the most critical parts of the source code, assisted by the company’s experts.

- **Black Piste**
  The deepest review of the most critical parts of Kaspersky’s source code, assisted by the company’s experts.

Kaspersky Transparency Centers

- **Utrecht, the Netherlands**
  Transparency Center

- **Zurich, Switzerland**
  Transparency Center
  Data centers

- **Tokyo, Japan**
  Transparency Center

- **Kuala Lumpur, Malaysia**
  Transparency Center

- **Rome, Italy**
  Transparency Center

- **Madrid, Spain**
  Transparency Center

- **Singapore**
  Transparency Center

- **Woburn, the United States**
  Transparency Center

- **Riyadh, Saudi Arabia**
  Transparency Center

- **São Paulo, Brazil**
  Transparency Center
Kaspersky Global Transparency Initiative: our results in numbers

2 Additional data locations
in Switzerland: globally known as a neutral country, it contains strict data protection regulation.
Here we process and store cyberthreat-related user data from Europe, North and Latin America, the Middle East, and several countries in Asia-Pacific region.

10 Transparency Centers
in Brazil, Italy, Japan, Malaysia, the Netherlands, Singapore, Spain, Switzerland, Saudi Arabia, and the United States

2 Regular third-party independent assessments
confirming the trustworthiness of Kaspersky's engineering practices:
• SOC 2 audit
• ISO 27001 certification

$7.9 mln investment
Since 2018, Kaspersky has invested over $7.9 million in the program, which includes $5.6 million for equipment for the data centers in Zurich.

57 Transparency Center reviews
by public and private stakeholders

55 Bug Bounty report awarded
with total payments equal to $77,450
The Service Organization Controls (SOC) Reporting Framework, a globally recognized report for cybersecurity risk management controls, was developed by the American Institute of Certified Public Accountants (AICPA). Kaspersky successfully passed a comprehensive SOC 2 Type 2 audit in 2023.

The most widely used information security standard prepared and published by the International Organization for Standardization (ISO), the world's largest developer of voluntary international standards. Kaspersky's information security management system has been certified against ISO/IEC 27001:2013 international standard.
Kaspersky is committed to the principles of ethical vulnerability disclosure approach. To ensure the integrity of our products, Kaspersky has been running its public bug bounty program since 2016, and since 2022, it operates on the Yogosha platform. The company also supports the Disclose.io framework, which provides a “Safe Harbor” for vulnerability researchers concerned about the negative legal consequences of their discoveries.

**Rewards**

- **$100,000** for the discovery and coordinated disclosure of severe vulnerabilities (high-quality reports with PoC).
- **$5,000 – $20,000** for the discovery of vulnerabilities allowing different and less severe types of remote code execution.
- **$1,000 – $5,000** for the discovery of bugs allowing local privilege escalation, or leading to sensitive data disclosure.
Threat intelligence and research

• Expertise
• Threat research
• Current advanced persistent threat landscape
• Major discoveries and research
• Targeted attack research
• Enabling a privacy-minded world
Expertise

Our unique team of security experts are at the forefront of protecting people around the world from the most sophisticated and dangerous cyberthreats. This expertise enriches our state-of-the-art protection technologies, making their quality unsurpassed.

>5,000 Highly-qualified specialists
50% of our employees are R&D specialists
35+ Members in our group of elite world-leading security experts - GReAT

Members in our group of elite world-leading security experts - GReAT
>1,000,000,000

cyberthreats
detected by Kaspersky since the company’s inception

7,000,000,000

cyberattacks
detected by Kaspersky in 2022

400,000

new malicious files
detected by Kaspersky every day
Advanced persistent threat landscape in 2022

Kaspersky’s Global Research and Analysis Team (GReAT) is well-known for the discovery and analysis of the most advanced cyberthreats. According to our data, in 2022 the top APT targets were governments and the most significant threat actor was Lazarus.

Top 10 targets

Government
Military
Diplomatic
IT companies
Educational
Telecommunications
Media
Software Development
Manufacturing
Logistics

Top 12 targeted countries

- UAE
- Pakistan
- India
- Turkey
- Ukraine
- Kyrgyzstan
- Russia
- China
- South Korea
- Japan
- Taiwan
- Vietnam

Based on the data up to 31.12.2022
Our major discoveries and research

<table>
<thead>
<tr>
<th>Detection</th>
<th>Active since</th>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sofacy</td>
<td>2014</td>
<td>Cyber-espionage malware platform</td>
<td>A highly sophisticated malware platform exploiting up to three zero-day vulnerabilities</td>
</tr>
<tr>
<td>Duqu 2.0</td>
<td>2015</td>
<td>Complex cyberattack platform</td>
<td>A group believed to be behind the attacks on Sony Pictures Entertainment in 2014 and the Central Bank of Bangladesh in 2016. Responsible for data destruction, money theft as well as conventional cyber-espionage operations against multiple companies around the world</td>
</tr>
<tr>
<td>Lazarus</td>
<td>2016</td>
<td>Cyber-espionage &amp; sabotage, financial attacks</td>
<td>A threat actor attacking state organizations. Project Sauron deliberately avoids patterns, customizing its implants and infrastructure for each individual target, and never reusing them, making traditional indicators of compromise almost useless</td>
</tr>
<tr>
<td>Project Sauron</td>
<td>2016</td>
<td>Cyber-espionage malware</td>
<td>A wiper pretending to be ransomware, using modified EternalBlue and EternalRomance exploits. Some observations point to a link between ExPetr and BlackEnergy APT</td>
</tr>
<tr>
<td>Expety/ Notpetya</td>
<td>2017</td>
<td>Data wiping campaign</td>
<td>An advanced threat actor that hit organizers, suppliers and partners of the Winter Olympic Games in PyeongChang, South Korea, with a destructive network worm. The deceptive behavior of this actor is excessive use of various false flags</td>
</tr>
<tr>
<td>Olympic destroyer</td>
<td>2018</td>
<td>Cyber-espionage malware</td>
<td>As a result of a sophisticated supply chain attack on the popular computer vendor’s software update system, the malware disguised as a software update was distributed to about 1 million Windows computers and signed using a legitimate certificate</td>
</tr>
<tr>
<td>Shadow hammer</td>
<td>2018</td>
<td>Cyber-espionage platform</td>
<td>A technically sophisticated APT framework designed for extensive cyberespionage. Features around 80 malicious modules and includes functionality never before seen in an advanced persistent threat, such as the ability to steal information from printer queues and to grab previously seen files from a USB device the next time it reconnects</td>
</tr>
<tr>
<td>Tajmahal</td>
<td>2019</td>
<td>Cyber-espionage platform</td>
<td>A multi-stage, modular framework aimed at espionage and data gathering. It is leveraging a UEFI bootkit based on Hacking Team’s leaked source code for persistence. Capable of communicating and fetching payloads over multiple covert channels</td>
</tr>
<tr>
<td>Mosaic-regressor</td>
<td>2020</td>
<td>Cyber-espionage platform</td>
<td>A stealthy, sophisticated multi-stage framework incorporating Windows kernel mode rootkit. It is deployed via the ProxyLogon only days following the vulnerability disclosures</td>
</tr>
<tr>
<td>Ghostemperor</td>
<td>2021</td>
<td>Cyber-espionage platform</td>
<td>A highly sophisticated, complex UEFI firmware rootkit we attributed to APT41, which allows the attackers to persistently execute a malware stage on the operating system via a malicious driver</td>
</tr>
<tr>
<td>Moonbounce</td>
<td>2022</td>
<td>Cyber-espionage platform</td>
<td></td>
</tr>
<tr>
<td>Year</td>
<td>2016</td>
<td>2017</td>
<td>2018</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td>ProjectSauron</td>
<td>WannaCry</td>
<td>Zebrocy</td>
</tr>
<tr>
<td></td>
<td>StrongPity</td>
<td>Shamoon 2.0</td>
<td>DarkTequila</td>
</tr>
<tr>
<td></td>
<td>Lazarus</td>
<td>StoneDrill</td>
<td>MuddyWater</td>
</tr>
<tr>
<td></td>
<td>Fruity Armor</td>
<td>BlueNoroff</td>
<td>Skygofree</td>
</tr>
<tr>
<td></td>
<td>ScarCruft</td>
<td>ExPettr/NotPetya</td>
<td>Olympic Destroyer</td>
</tr>
<tr>
<td></td>
<td>Poseidon</td>
<td>Moonlight Maze</td>
<td>ZooPark</td>
</tr>
<tr>
<td></td>
<td>Danti</td>
<td>ShadowPad</td>
<td>Hades</td>
</tr>
<tr>
<td></td>
<td>Dropping Elephant</td>
<td>BlackOasis</td>
<td>Octopus</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Silence</td>
<td>AppleJeus</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy has become a valuable commodity as more and more users understand its importance and the need to change their habits to protect their digital presence. Being not just a cybersecurity firm, but a privacy company, Kaspersky invests in features that enable users to protect their data and digital privacy through educational assets and hands-on tools.

**Anti-doxing course**
Learn what the basic dangers of doxing are and how to protect yourself from it

**Privacy checklist**
An easy to grasp definitive checklist for those who care about their privacy

**Stalkerware protection**
Kaspersky’s consumer security solution offers users best-in-class protection and detection of software used to secretly spy on people

**Privacy Checker**
Instructions on how to set social media accounts and OS privacy levels
Products & solutions

- Kaspersky Cyber Immunity approach
- KasperskyOS-based product portfolio
- Enterprise Solutions
- Industrial Cybersecurity Solutions
- SMB Next Generation Solutions
- MSP Solutions
- B2C Solutions
The overwhelming majority of attacks on a Cyber Immune system are the types that cannot impact its critical function.

Kaspersky’s approach and methodology for developing secure-by-design IT systems

- The architectural approach creates an environment where a vulnerability or bad code is no longer a big deal
- Methodology, technologies and tools for creating Cyber Immune solutions
- **KasperskyOS** – an optimal platform for building Cyber Immune IT systems

The overwhelming majority of attacks on a Cyber Immune system are the types that cannot impact its critical function.
Kaspersky Cyber Immunity areas of application

KasperskyOS-based Cyber Immune solutions have an “innate” protection against the consequences of the intrusion of malicious code and hacker attacks.

They perform functions even in an aggressive environment without additional security features.
KasperskyOS is an effective platform to create Cyber Immune products

Microkernel operating system for IT systems with high cybersecurity demands

- Grants a platform for creating secure-by-design solutions
- Creates an environment that does not allow apps to execute undeclared functions and prevents the exploitation of vulnerabilities
- Provides full transparency, flexible configuration of security policies and control over interactions across the whole system
KasperskyOS-based product portfolio

**Kaspersky IoT Infrastructure Security**
A solution for cybersecure data transfer to digital and cloud business platforms, as well as for infrastructure protection and transparency

- Kaspersky IoT Secure Gateway
- Kaspersky Security Center

**Kaspersky Secure Remote Workspace**
A solution for building a Cyber Immune, functional, and manageable thin client infrastructure with convenient, centralized management

- Kaspersky Thin Client
- Kaspersky Security Center
- Kaspersky Security Management Suite

**Kaspersky Automotive Secure Gateway**
Building reliable IT systems for smart road vehicles

- Kaspersky Automotive Adaptive Platform
- Kaspersky Automotive Secure Broker Framework
- Kaspersky OTA Agent
- Kaspersky Vehicle SOC Agent
- Kaspersky Remote Diagnostic Agent

A solution for building a Cyber Immune, functional, and manageable thin client infrastructure with convenient, centralized management.
Natively integrated platform for OT

Native integration, complete kill chain and intelligence

**Kaspersky Single Management Platform**

**Response examples**
- Security scan and update
- Patching and file execution
- Change node authorization
- Node and process isolation

**Kaspersky Industrial CyberSecurity for Nodes**
- Server
- Workstation
- Portable Scanners

**Kaspersky Industrial CyberSecurity for Networks**
- Server
- Sensor

**Kaspersky at a glance**
- Global Transparency Initiative
- Threat Intelligence and research
- Products & solutions
- Awards
- ESG
- Education
- Sponsorships & Partnerships

**Products & solutions**
- Endpoint protection, detection and response
- Network traffic analysis, detection and response

**Response examples**
- Security scan and update
- Patching and file execution
- Change node authorization
- Node and process isolation

**Kaspersky Network Security**
- Server
- Sensor

**Security Audit**
- Host Telemetry
- Networks Communications
- Incident
- Protection Status
Kaspersky SMB Next Generation Solutions

**Kaspersky Small Office Security**
- As easy as home antivirus
  - Works out of the box, no configuration required
  - Financial protection with Safe Money
  - Unlimited, fast VPN to enjoy global content without compromising on privacy, security or speed
  - Storing all passwords with Password Manager

**Kaspersky Endpoint Security Cloud**
- Rapid protection for limited resources
  - Cloud-based console for flexible, simple administration, no need for additional hardware
  - Protects PCs, laptops, mobile devices and file servers
  - Security for Microsoft Office 365 and 'Shadow IT' control
  - The latest, most up-to-date software - always

**Kaspersky Optimum Security**
- The best enterprise-grade security solution
  - Essential EDR functionality to combat evasive threats
  - Managed protection brings security to a whole new level
  - Reduces your cybersecurity team's workload
  - Cloud-native solution that covers diverse infrastructures
Kaspersky Services for Managed Service Providers

Build services
- Endpoint Protection and hardening
- Vulnerability and Patch Management
- Office365 Protection
- Incident Response
- Security Awareness
- Managed Web and Email Protection
- 24/7 Security Monitoring
- Threat Detection and Response
- Proactive Threat Hunting

MSP
- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365

MSSP
- Kaspersky EDR Optimum
- Kaspersky EDR Expert
- Kaspersky Hybrid Cloud Security
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security for Mail Server
- Kaspersky Security for Web Gateway
- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky Intelligence Reporting

Kaspersky knowledge and expertise
- Automation and integration
  - RMM and PSA Integrations
  - Subscription-based model and LMP
- Knowledge and Expertise
  - Kaspersky Cybersecurity Training
  - Kaspersky Premium Support and Professional Services

Kaspersky at a glance
- Global Transparency Initiative
- Threat Intelligence and research
- Products & solutions
- Awards
- ESG
- Education
- Sponsorships & Partnerships

Kaspersky Premium Support and Professional Services
B2C Solutions: New product portfolio

Our bold new plans cover the full range of customer needs

Complete protection for your digital life

- **PREMIUM SERVICES**
- **IDENTITY**
- **PRIVACY**
- **PERFORMANCE**
- **SECURITY**
Complete protection for consumers’ digital lives

With our diverse collection of security products, we inspire customers to embrace new technologies – because they know we’re guarding them and their families.

Kaspersky B2C Solutions

- **Kaspersky Standard**
  - Win | Android | Mac | iOS

- **Kaspersky VPN Secure Connection**
  - Win | Android | Mac | iOS

- **Kaspersky Password Manager**
  - Win | Android | Mac | iOS

- **Kaspersky Who Calls***
  - Android | iOS
  *Only available in Russia, Kazakhstan and Indonesia

- **Kaspersky Plus**
  - Win | Android | Mac | iOS

- **Kaspersky Safe Kids**
  - Win | Android | Mac | iOS

- **Kaspersky Premium**
  - Win | Android | Mac | iOS
Kaspersky awards

- Overview
- Top 3 metrics
- Recognitions
More than 600 awards*

One of the five biggest endpoint security vendors**.

Kaspersky Internet Security was honored with the Top Rated 2022 annual award by independent test lab AV-Comparatives***.

Kaspersky EDR Expert continually delivers top results: Total Accuracy Rating of 100% in Advanced Security EDR tests of 2022&2023 by SE Labs****; 100% protection from targeted attacks, and Strategic Leader status from AV-Comparatives*****.

*The number includes independent test results of corporate and consumer products during 2013-2022.
**The company was ranked fifth by IDC estimations in Worldwide Consumer Digital Life Protection Market Shares (9 June 2022)
***Kaspersky’s flagship home user security solution – Kaspersky Internet Security – was honored with the annual Top Rated 2022 award for high results in 8 Real-World tests, 2 Malware Protection tests, 2 Performance tests, and Enhanced Real-World test of 2022.
****Enterprise Advanced Security EDR test reports of 2022 and 2023
*****Endpoint Detection and Response test of 2022
Awards

Most Tested*
Most Awarded*
Kaspersky Protection

*Kaspersky.com/top3

As cybersecurity becomes vital to every individual and entity, trust in providers is essential. We protect home users and corporate clients worldwide, and market recognition is very important for us. In 2022, Kaspersky products participated in 86 independent tests and reviews. Our products were awarded 69 firsts and received 73 top-three finishes.

* 86 independent tests were completed by Kaspersky products in 2022 alongside 14 competitors. More than 90 vendors took part in the tests, but only those who participated in 35% or more of the tests had their results represented in the chart.
Recognitions

Kaspersky products are regularly assessed by global research firms, and our cyber protection expertise is proven by the number of recognitions by industrial analysts.

Among those are IDC, Canalys, ISG, Quadrant Knowledge Solutions, Info-Tech, and many others.

In 2023, Kaspersky was noted as the vendor “who shaped the year” in IDC’s Worldwide Modern Endpoint Security Market Shares report.*

ESG

Our company’s mission is to build a safe and sustainable digital world so that people can use technological solutions to improve not only their daily lives but also life on the planet as a whole.

We fulfill this mission by increasing the resilience of the digital space against threats through the creation of Cyber Immunity while paying special attention to social projects and environmental awareness.

Read the first Sustainability (ESG) report covering results for 2021 and mid-2022 as well as key objectives for 2023 [here](#).
Kaspersky’s sustainable development is grounded in five key areas

1. **Ethics and transparency**
   - Source code and process transparency
   - Data protection and the right to privacy
   - Management transparency and business resilience

2. **Safer cyberworld**
   - Critical infrastructure protection
   - Assistance in the investigation of cybercrimes on a global level
   - Protection of users against cyberthreats

3. **Safer planet**
   - Reducing the environmental impact of our infrastructure, business activities and products

4. **People empowerment**
   - Employee care
   - Women in STEM
   - Inclusivity and availability of technologies
   - Talent development in IT

5. **Future tech**
   - Cyber Immunity for new technologies

Learn more about our main accomplishments [here](#).
Education

Despite the rapid development of technology, the human factor still plays a significant role in building a safer digital world. This is why Kaspersky aims to educate people of all ages and professions all around the world about cybersecurity, and create a life-long learning journey for passionate cybersecurity experts.
Education: Cybersecurity is for life-long learning

Kaspersky intends to educate young Internet users about online safety by creating projects such as children’s books on cybersecurity and partnering with schools.

- **School: Primary**
  - Kids Cyber Resilience
  - Kids book

Kaspersky is keen to help young talents to explore the field of cybersecurity and make their future professional journey to IT more vivid.

- **School: Secondary**
  - Tech Valley

As part of our international educational project **Kaspersky Academy**, we promote knowledge of cybersecurity among students and professors worldwide.

- **University**
  - SecurIT Cup
  - SafeBoard

Kaspersky provides a wide range of knowledge on information security for IT professionals, business leaders, top managers and senior executives.

- **Professional**
  - xTraining
Sponsorships & Partnerships

As an innovative global company, Kaspersky cares about future by providing cybersecurity to different industries and by supporting promising talent in various countries.

We contribute to the development of science and contemporary art, help to preserve the world, and provide athletes with the opportunity to reach their full potential.
Kaspersky partners with multiple eSports teams worldwide: Nasr (UAE), Sangal (Turkey), Reckoning (India), and Red Canids (Brazil) to enhance the gaming experience of eSports enthusiasts by providing advanced cyber security measures.

Kaspersky supports talented drivers such as Amna and Hamda Al Qubaisi, the first Emirati female drivers.

Kaspersky was a partner of the Moniker International Art Fair in London, and it supported artists, such as Ben Eine.

Kaspersky is an official cybersecurity partner of the FIDE World Chess Championship.
Bring on the future