A COMPANY TO SAVE THE WORLD

KASPERSKY lab

2014 Citizenship Report

OUR GREATEST STRENGTHS SHOULD SERVE OTHERS, NOT JUST US

My dear friends,

This year our company turns 18 years' old – an age that in much of the world marks the transition from childhood to adulthood. So we're joining the big boys club, and as a grown-up company, we've decided to publish our first corporate social responsibility report. That doesn't mean we haven't done socially-oriented and charitable projects before, but now we can look back at what we've achieved previously as well as outlining our priorities for the future.

Our company has always been driven by a higher purpose: our ultimate goal is to save and protect the world from all cyberthreats, and make the use of computers and other digital and networked devices safe and secure for everyone across the world. It's not an easy task, since cyberthreats are becoming increasingly sophisticated and everything around us – from elevators to power grids and from washing machines to blast furnaces – is becoming computerized and running on networks. The share of the economy that's online is growing across the globe. There are many risks and they are growing too, but I believe we have a lot to offer in order to tackle them.

There are many things that we're doing well already: we provide best-in-class protection to people; businesses and communities; we help tackle cybercrime on a national and international level; we share our expertise and cooperate closely with INTERPOL and Europol as well as with law enforcement organizations in various countries. By working together with foundations, universities, and non-profit organizations, we help tackle the problems plaguing the Internet, train more people in the basic skills of personal information security, and help more young technology professionals develop their expertise. In addition, of course, we are a successful and profitable company. However, as our in-house survey has shown, the majority of Kaspersky Lab employees chose to work here because we are not just about business. In the words of one of the heroes of this report, North American employee Nichol Goldstein, "this is about much more than just a pay-check."

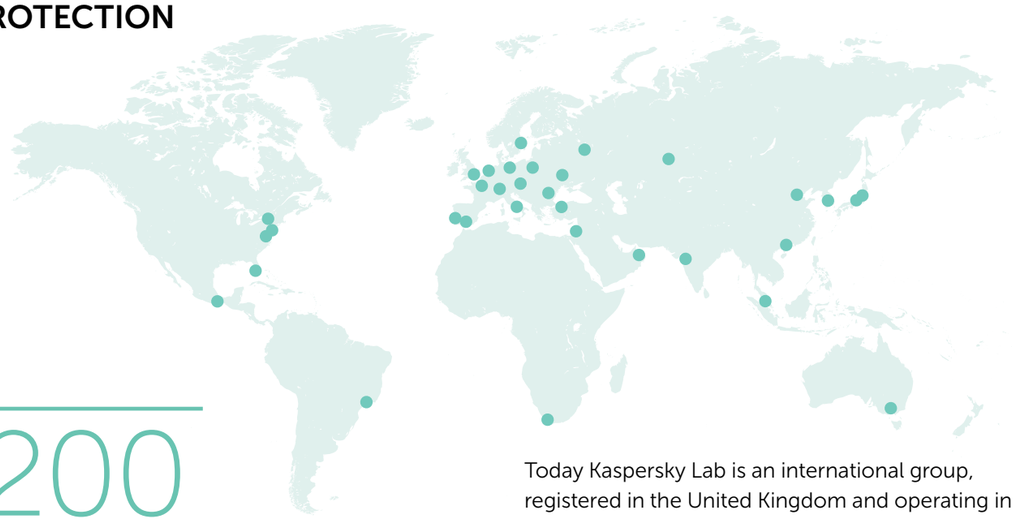
We want to use our strengths – the things that we are good at – to make the world a better place. Our own communities are a good place to start. So this report is our first experience at preparing a systematic account of our efforts at being socially responsible.

Thank you!

Yours Sincerely, Eugene Kaspersky,
Chairman and CEO, Kaspersky Lab

Kaspersky Lab is a global privately held company, founded in 1997. It is ranked among the world's top four providers of security solutions for endpoint users. At Kaspersky Lab we are driven by a mission to save the world from cyberthreats. We succeed in this by enlightening, enabling and empowering our customers to secure the things in life that hold real worth.

WORLDWIDE PROTECTION



200

KASPERSKY LAB IS OPERATING IN ALMOST 200 COUNTRIES AND TERRITORIES WORLDWIDE

Today Kaspersky Lab is an international group, registered in the United Kingdom and operating in almost 200 countries and territories worldwide. It has 34 representative territory offices in 31 countries across 5 continents. Kaspersky Lab currently employs more than 3,000 highly qualified specialists and this number is growing by about 7% a year.

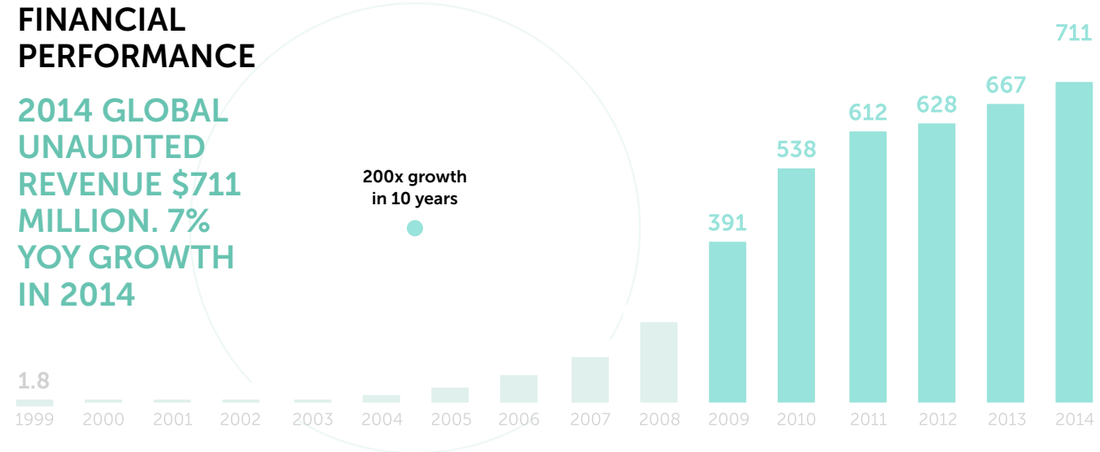
UNIQUE EXPERIENCE

Kaspersky Lab's Global Research and Analysis Team (GReAT) provides company-wide leadership in anti-malware research and innovation. The security analysts in the team are based around the world, each contributing a unique set of skills and expertise to the research and development of solutions to combat increasingly complex malicious codes.

The company's sustainable growth is based on developing innovative technology to address market-specific needs. From inception, Kaspersky Lab's technology is built to take advantage of the best threat intelligence ecosystem in the world. It allows customers to be better protected and more informed.

FINANCIAL PERFORMANCE

2014 GLOBAL UNAUDITED REVENUE $711 MILLION. 7% YOY GROWTH IN 2014



TECHNOLOGY AND OEM PARTNERS

Kaspersky Lab has about 120 global technology OEM and pre-installation agreements with companies including Microsoft, Cisco Meraki, Juniper Networks, Alcatel Lucent, Blue Coat, Check Point, D-Link, Clearswift, Netgear, ZyXel, Alt-N, Parallels, Lenovo, Facebook, Qualcomm, BAE Systems, H3C, Trustwave, Vertu, ASUS, Samsung, Toshiba, Stormshield, Openwave Messaging and General Dynamics.

WHAT IS CORPORATE CITIZENSHIP?

Eugene Kaspersky once said: «We are here to save the world.» This may sound excessively dramatic to some, but at Kaspersky Lab really feel this way. To anyone who asks what we do; we save humanity from cyberthreats! The company's core business operations have already set high standards for social responsibility, and we try our best to live up to them.

Our understanding of social responsibility is close to the idea of corporate citizenship. As a corporate citizen, Kaspersky Lab feels very much part of this world, and feels it has a responsibility to make it better and safer. In practical terms, that means creating real changes for the better in the parts of social life for which we feel responsible.

Social responsibility was never an artificial concept for Kaspersky Lab. But we don't like talking about it too much — because creating a better, safer world has always felt like something natural and obvious, something that is embedded into Kaspersky Lab's DNA. We do not have to divide our business activities into «things we do to make money» and «things we do to benefit society.» Instead, our business is to protect the tangible and intangible assets of individuals and organizations in cyberspace, using our innovative products. We invest millions in R&D to make sure Kaspersky Lab solutions provide reliable protection for our users. This has always been more than just business. We take a much broader view of our purpose as a corporate citizen in the world.

Today, we're all living on the threshold of a new reality, a reality in which the Internet plays a central role. Within the next few years, the majority of people on Earth will become connected to a common digital cyberspace through multiple devices. This new world offers a wealth of great opportunities. However, unfortunately it is not as safe as we'd like it to be. We are preyed upon in cyberspace by malware and criminals who are out to get our personal information and money; facing us with psychological pressure and other threats.

We made the decision to protect this new, necessary and universally useful world from threats, make it happier and brighter and make people's experiences safer. Clearly, achieving this objective takes more than just the production of quality defensive technologies so we are making use of all our expertise, discoveries, ideas and experience to make the cyberspace of the future safe and inspiring. We are standing on guard for the online world, using multiple social initiatives, as well as actively fighting the bad guys who want to exploit others.

Kaspersky Lab's corporate social responsibility (CSR) budget is split between charitable and socially significant initiatives:

37%	26%	20%	17%
CHARITY AND VOLUNTEER NITIATIVES	EDUCATIONAL PROJECT	GLOBAL PROJECTS AND ANTI-CYBERBULLYING PROJECTS	DISASTER RELIEF

We know every nook and cranny, including the darkest recesses, of the digital world, so we know that we can make a real difference. We come to work at Kaspersky Lab every day, aiming to give everyone on the planet the opportunity to benefit from new technologies without having to worry about the security of their personal data, finances or reputation. And so, the concept of Digital Citizenship naturally became the core of Kaspersky Lab's socially responsible activities. It has united projects aiming to keep people safe in the global network.

We believe that education and enlightenment are the best weapons to fight cybercriminals and other sources of digital threat. We help people to better understand the threats they may face online, and share the tools they can use to protect themselves from these threats. We know that smart and «environmentally responsible» behavior online can reduce our vulnerability to threats and pressures. Knowledge is power, and we want as many people as possible to have the power to protect themselves. This is the purpose of our research and educational and security awareness initiatives.

The knowledge and tools we share are the result of hard work by our R&D team. Everyday our R&D experts toil to identify new threats and analyze online user behavior, offering algorithms to make people less vulnerable on the Internet. Our analysts also explore threats against businesses, alerting more than 270,000 companies around the world to potential dangers and providing them with the algorithms they need to do business securely. Our Chairman and CEO, Eugene Kaspersky, is widely regarded as one of the world's most highly respected experts in cybersecurity. He has made it his mission to inform decision-makers about threats and how to defend against them, warning and protecting those who set society's agenda: political leaders, corporations, and popular movements.

We also fight for a safer digital world in a literal sense — by helping to catch cyber criminals and cooperating with INTERPOL, Europol, and law enforcers in many countries.

One of the most important areas of our work is protecting children online. We are working on both technological solutions and educational/social projects for children and their parents. Cyberbullying has become a real threat to kids and teenagers around the world and in 2015 we launched a serious, dedicated program to counter it.

A human perspective is key to everything we do. We appreciate and value people above all else. We create technology for people. We share knowledge and expertise with people. We do not have software protection devices, instead we have people who protect other people.

Kaspersky Lab supports children's institutions, people with disabilities, young talent and many others; we also donate money and software licenses to charitable foundations, and we are actively developing volunteer projects around the world. Our employees often initiate charitable and volunteer projects themselves. We do not have any formal programs because every project that we are working with is different. Each project has a unique face and is inspired by a specific person who wants to make the world better, stirring his or her colleagues to do likewise.

For its work over the last three years (2012-2014) Kaspersky Lab North America has been awarded with the Gold Impact Award for its commitment to strengthening local communities through volunteerism and giving. This is the second consecutive year that Kaspersky Lab North America has won this award.

PEOPLE WHO PROTECT PEOPLE

Our people are our number one asset. Any company working on innovative products will share this view. This is vital in an age when real value is created in people's heads rather than on an assembly line. It is therefore not surprising that businesses have started talking about investing in human capital alongside "conventional" investments like R&D or marketing. We'd rather not tell this story using the language of numbers alone. Our employees call Kaspersky Lab "a company for people," and the positive impact of this attitude reaches far beyond the boundaries of our offices. That is what matters the most.

OUR TEAM

There is a universal formula to ensure the success of any startup: put together a team of enthusiasts and offer customers a product or service that takes quality to a whole new level. Eugene Kaspersky chose this path in 1997. Today Kaspersky Lab is a global corporation with offices in 31 countries around the world, and yet it still has a team of enthusiasts working for it, and its products are peerless in terms of their quality (according to independent tests results).

Recruiting and developing people that are passionate about their work has been at the core of the company's HR policy for the past 18 years. A market-leading compensation package, personal and professional development programs, a comfortable working space, and the freedom to take the initiative are all essential components of this policy. However, there is another component most other progressive companies will never be able to offer their employees, no matter how much they want to. Every day, when employees come to work at Kaspersky Lab, they are saving people from real threats. There are few things more inspiring.

31

MORE THAN 3000 KASPERSKY LAB'S EMPLOYEES WORK IN 31 COUNTRIES AROUND THE GLOBE

6k

6,000 HOUSE PLANTS COVER 15,000 SQUARE METERS OF KASPERSKY LAB'S MOSCOW HEADQUARTERS

78%

EMPLOYEE SATISFACTION LEVEL AT KASPERSKY LAB (BASED ON A 2013 EMPLOYEE ENGAGEMENT SURVEY)

VOLUNTEER MOVEMENT

For most people, dealing with life's daily problems and challenges means they have little energy left to help others. With that in mind, the fact that we have such a large number of employees involved in social and volunteer projects is something we are proud of at Kaspersky Lab. We are proud that the company gives people both the incentives and the strength to share their energy with the world. What are the projects? Nothing out of the ordinary. For example, several times a year employees in our offices around the planet donate blood. They volunteer to help children who have survived cancer. They leave the office to clear a local stream of garbage. They make blankets for the homeless. They travel hundreds of kilometers to an orphanage to teach new skills to orphans. They do a great number of other simple things to make the world around them a little better. No doubt they would have done those things anyway; Kaspersky Lab simply brought them together.

CHARITY

Kaspersky Lab has never published a formal report on its charity projects before. We regularly help various foundations and get involved in a large number of charity events. Both Kaspersky Lab's management and our employees see this as a personal matter. However, as an international company, we must make our charitable work public. We are happy to do this in the hope that you will also take notice of the charities we are helping. Here are some facts about Kaspersky Lab's key charity initiatives and projects. Kaspersky Lab is an active partner of the Gift of Life Foundation – a leading Russian charity that helps children struggling with tumors and serious blood conditions. We take part in all of its events, including the World Children's Winners Games – a sporting tournament for children who have survived cancer.

$35,500

KASPERSKY LAB'S TEAM COLLECTED $35 500 TO HELP THE JAPANESE RED CROSS AFTER TSUNAMI DISASTER OF 2011

115

KASPERSKY LAB HANDED OVER 115 PIECES OF HARDWARE AND 1021 LICENSES TO VARIOUS CHARITIES, ORPHANAGES AND SCHOOLS IN 2014

We provide help wherever it's needed. One of the most memorable examples of how we have helped is following the Japanese disaster of 2011. Kaspersky Lab was among the first companies to donate to the Japanese Red Cross – we transferred $250 000 straight away. Since then we have financed humanitarian aid and purchased and delivered 5,000 radiation detectors to affected areas. Wanting to do more, and after a request from our employees, we organized a fundraiser. Every Kaspersky Lab office across the world took part, and everyone – from top-managers to interns - donated. Our team collected $35,500 and the company added twice that sum, then transferred it all to the Japanese Red Cross.
The partnership between Kaspersky Lab and Ferrari bore some unexpected fruit in 2014. Kaspersky Lab was approached by charity Make-A-Wish with a request to help a boy who was fighting cancer meet Ferrari's star F1 racer Fernando Alonso. Kaspersky Lab worked hard to help and was thrilled to invite 14 year-old Michael and his father to be our guests at the Italian Grand Prix at the legendary Monza Autodrome.
"Ice fever" gripped the world in August 2014, with dozens of videos cropping up on YouTube showing very famous, mildly famous, vaguely familiar and completely unknown people pouring buckets of iced water over their heads. So one Monday, Kaspersky Lab joined in with a flash mob: more than 100 Kaspersky Lab employees accepted the Ice Bucket Challenge, and lined up outside the office to pour ice and ice water over themselves in unison. We not only transferred money on behalf of everyone who took part – more than US$1,000 – to the ALS Association, we also helped out the Perspective and Gift of Life foundations – two foundations we have been supporting for years – by sending RUB1 million (about US$ 27,000) to each of them too.

ONE OFFICE'S DEDICATION TO SERVICE, AND THE PEOPLE WHO HELP MAKE IT POSSIBLE

Nichol Goldstein grew up in a family that was not particularly rich. In fact, their circumstances were so constrained that her parents couldn't even afford Christmas presents for the kids. However, a miracle would happen every Christmas Eve, and Nichol always received a gift. Local people would buy presents for children from underprivileged families. A fair number of years have gone by since then, yet Nichol still remembers those moments, and believes that it's her turn to «do good deeds.» She didn't know it at first, but many employees in Kaspersky Lab North America shared the same desire to do good for their community and go well beyond what is required of them. This drive and passion from all involved is what makes Kaspersky Lab NA's local programs successful today.

FINDING HER PLACE

Kaspersky Lab's North America office opened in Woburn, MA in 2005, and Nichol Ashworth-Goldstein has been working there for almost seven of its 10 years. A large bulletin board hangs on the wall next to her workplace, detailing all the charitable and social projects overseen by Kaspersky Lab employees in the past 12 months. There are too many to count at a single glance. To the uninitiated, this may look like the HQ of a volunteer organization. But it is just our office.

Nichol says, «Together with the HR department, I offered an opportunity to all local staff. If they wanted to, they could join our Events Committee here in the Woburn office and, since then, we've had many volunteers from many different departments. Together we think about how we can help those in need,» Nichol says. «Our volunteer events can be fairly simple things that don't require any great experience or investment; a lot of them are just nice to do in your spare time. The management team here really believes in the importance of giving back to the community as well. In fact — they believe in it so deeply that, when Jessica Bird (Sr. HR Generalist and one of the longstanding members of the Events Committee) recommended a volunteer paid time-off program as an employee benefit, they immediately said YES! Now, thanks to Jessica, our employees get 3-paid days off each year to spend doing charity work.»

No charity event or activity takes place at Kaspersky Lab's North America office without this amiable and energetic young woman. Nichol, a Kaspersky Lab Executive Assistant, is engaging colleagues in all kinds of socially significant initiatives, inspiring others with her genuine desire to help those who need it most — the elderly, the sick, children, people with disabilities and other disadvantaged people.

«Initiatives like these are very important for several reasons,» says Chris Doggett, Head of Kaspersky Lab North America, who studied information systems management at Boston University. «First of all, it is one of our sacred duties, to take care of local communities, supporting programs that help other people survive and live a full life. Second, corporate philanthropy is not only useful to the people you are helping (which alone is a valid reason for its existence), it also serves to reinforce the company's connections with the community. We try to take care of our own employees, but also the people around us. Moreover, this helps to build stronger ties within the company, because we do all of this together.»

Nichol and the Events Committee have done a lot to make sure no employee of Kaspersky Lab North America remains indifferent to social projects. Most importantly, the more projects they do, the more people want to take part.

«I have colleagues come up to me all the time to say, „I really like what we are doing! You know, I also have this idea for this charity... and another idea..." And they start to tell me what else we could be doing. It was after so many people started doing this that I had the idea of setting up our Events Committee, which meets early in the year as a small action group to decide which projects we are going to work on in the New Year.»"

A GREAT JOB

As she looks at the photos on the bulletin board, Nichol recalls the highlights with genuine enthusiasm:

«Collecting donations is all well and good, but my favorite activities are those where we have to do things with our hands,» Nichol says laughing. «For example, we've helped the zoo near our office for the past two years. Last year, we cleared an emergency exit for the zoo. We had to pick up our shovels and literally get our hands dirty. In fact, I always feel that if I sweat while working, I must be doing a good job for a good cause! The soreness you feel the next day is like your body telling you, „Job well done!"».

Nichol's other favorite project is working for the Boston Food Bank — a project that has helped many families. Every day, residents in the Commonwealth of Massachusetts, the state where Kaspersky Lab's North America office operates,

donate food for those who cannot afford it. Nichol and her colleagues sort the food donated at the Food Bank. Last year, they sorted 4,419 kilograms of food in four hours, putting together 5,923 servings of food: enough to feed a family of four for a whole year!

«Here is a US$733 check,» Nichol points out a bright pin in the upper corner of the bulletin board. «This is how much we collected in donations on 'Pink Day' in October — a day spent honoring those in our lives who have suffered from cancer.» On that day, Nichol came around the office with a cart full of homemade treats (made by six different employees, each of whom made 50 delicious pieces of pastry or candy!) The employees who wore pink that day could buy a treat for as little as $1, while those who did not wear pink had to pay at least $2 for a treat. All the proceeds were transferred to the American Cancer Society.

Kaspersky Lab North America also holds regular events. For example, in a good St. Valentine's Day tradition, elderly people in Woburn receive greeting cards containing good wishes, poems and dedications signed by Kaspersky Lab employees. In another local tradition, Kaspersky Lab gathers donations for Christmas presents for the disadvantaged families of Woburn.

KINDNESS WITHOUT BORDERS

You can see the signs of Nichol and her NA Kaspersky Lab colleagues across the whole of Greater Boston — one of the largest metropolitan areas in North America, and home to more than four million residents. However, we also work on smaller-scale projects targeting locals in the much smaller city of Woburn, which is home to our NA office.

«I have been with Kaspersky Lab for many years now — I feel like the office is my home! I love the people who work here, our corporate culture and management style, and I really value the fact that all of our employees have the opportunity to do more here than just earn their salaries. Our office has been supporting charitable initiatives for years, and I am especially pleased to see colleagues from Kaspersky Lab's other regional offices adopt our practices and learn from our experiences. One more reason to be proud of working with Kaspersky Lab is that we help to develop and support the community on a global scale, to make the world around us better. We really are here to save the world, in more ways than one.»

65k

WOBURN, MA EMPLOYEES HAVE DONATED MORE THAN US$ 65,000 TO ALL KINDS OF CHARITY PROJECTS SINCE 2011

A STORY WHICH SHOWS MONEY ISN'T EVERYTHING (OR MORE PROOF OF THIS OLD MAXIM)

Marina Alekseeva joined the Kaspersky Lab team in 2008, becoming HR Director in 2012. We believe she is the perfect person to answer a few questions about why a job at Kaspersky Lab is a dream position for so many people, how we choose people to become part of our team, and how we support an environment where people protect other people.

Marina, what is the first thing people experience when they start a new job at Kaspersky Lab?
I came here after working for a bank, and I found it stunning how quickly everything gets resolved and how everything is focused on delivering results. That was seven years ago and certainly a lot has changed since. Kaspersky Lab today is a large global company, and yet, it has been able to stay healthy and not succumb to the diseases typical in mature corporations. I believe that the main impression a new employee is likely to get is that he or she will definitely not be bored here.

To what extent does Kaspersky Lab's HR policy contribute to this?
Our corporate DNA directly influences and is supported by our HR policy. It is comprised of four key elements.
- First, we are creating an environment that helps employees reach their potential and find self-realization as professionals. We are focused on the long-term development of competencies. In practical terms, that means that Kaspersky Lab employees don't just have to meet all the requirements of their position, they need to be ready for any challenge the next day may bring.
- Second, we offer competitive working conditions in the broadest sense of the word. From salary, social packages and comfortable offices, to material aid and an eventful corporate life. We objectively evaluate the market and develop a strategy that makes our working conditions attractive for high-level, highly motivated and high-achieving professionals.
- Third, during the recruitment process, we not only look at the knowledge and skills of the candidate, we make a forecast about whether the person will be successful in our team, whether their beliefs and competencies match the company's expectations and corporate culture. We pay special attention to young specialists.
- And finally, the fourth component of the HR policy that permeates our entire company is a human

perspective on everything we do. It is often the case with large corporations that people are overlooked in favor of systems, structures, and processes. We, on the other hand, put people first.
All of this together creates a unique environment in which there is always room for development, room to move forward and room to change."

Formalized processes are needed in global corporations to ensure a uniform quality of management across all the regions in which a corporation does business. How difficult is it to combine this need with our HR policy?
"HR policy is more of a local than a global function. It is affected to a large extent by the cultural, legal, and market specifics of a given country. For example, our global employee compensation policy is ahead of the market. Kaspersky Lab employees both in England and in China get generous health coverage for their region and the specifics of coverage in different countries are as different as the English and Chinese cultures. However, a common approach and a global HR policy are important for providing a standard level of quality and cost savings for the business. The thing is, the company doesn't evaluate people based on their sex, nationality or the country they live in. The only thing that matters is the results they produce."

How did this kind of corporate culture emerge?
"This is a culture that is the natural extension of the management's world view. The management of any company would claim that people are the most important thing to its business. However at Kaspersky Lab it's true. We recently ran focus groups on our corporate values. Employees in all of the focus groups, employees said that "our company is a company for the people." This is reflected in the way people receive detailed employment records from HR, as well as the way Eugene Kaspersky himself interacts with employees. I must be quite different from other HR professionals because I am proud that our corporate culture has not been created by HR. HR professionals at other companies are often proud of the opposite, saying, "It was us who created the [corporate] culture here." I am pleased to be working with a company where we did not need to create a culture, there was a great culture at Kaspersky Lab to begin with. Our task is just to support it."

What qualities do people building their careers at Kaspersky Lab have in common?
"First of all, they all enjoy their work because they do what they love, that's how we get both expertise and quality. Secondly, they care about the overall outcome and they can work in a team to achieve a common result. Thirdly – you could call it an enterprising spirit. This means that people can propose ideas, solutions and are ready to accept responsibility for them. This sounds very simple, but believe me people like that are hard to find. An enterprising spirit is a rare thing in a corporation. There are pure entrepreneurs, but it's hard for them to be a part of a corporation, because they run their own businesses, and there are people who prefer to be a "link in the chain." The majority of our success stories are people somewhere in the middle - they want to work in a team and they also have something of a free spirit."

I must be quite different from other HR professionals because I am proud that our corporate culture has not been created by HR

How successful is the Kaspersky Lab HR Policy overall? How would you rate it?
"An HR policy's effectiveness is evaluated within several parameters that eventually influence the company's business results: the readiness of employees to complete their tasks today and tomorrow, the motivation of employees to achieve the company's goals, and the attractiveness of our company to potential candidates. There are also parameters like the level of employee satisfaction with HR's services, and in terms of finance we are analyzing the cost effectiveness of HR. We've already learnt how to evaluate some of these parameters and we are satisfied with the results – for example the employees' engagement level and satisfaction with HR's services. We are now learning how to evaluate some of the others."

Could you share a special secret — what's the key factor in the success of Kaspersky Lab's HR policy?
Our secret is very simple. People come to work with us because we are not just making money, we are saving the world and we are fighting cybercrime. For many at Kaspersky Lab it is important to have the opportunity to have an input into this. People today do not want to simply work at a company that makes money. People want to do something that makes a difference."

If global business used the amount of disseminated knowledge as a measure of a company's social significance, we would have reached an impressively high score. However, humanity has yet to find an easy way to measure knowledge. We do not share knowledge to win performance points. On the contrary, some information you just have to share if you know it could help save someone from serious trouble. We teach people – children and adults alike – how to stay safe in the digital environment. We educate companies on how to avoid falling victim to cyber criminals. We teach national governments to protect their citizens from cyber terrorists. We train experts who can go on to teach others in our stead. We use a huge amount of the company's resources to disseminate knowledge and still believe this is the right thing to do. Knowledge is the foundation and the driving force of our business. The more you share your knowledge, the more knowledge you get in return, and the greater the demand for new knowledge. This is how the technological progress of our civilization works, and we want Kaspersky Lab to be part of it.

GLOBAL EXPERTISE

Kaspersky Lab has a very high concentration of unique competencies in preventing and fighting cyber threats; we track the condition of the global information environment in real time, on a daily basis, and we know pretty much everything that is going on in the cyber world. Making this knowledge available to all the stakeholders is a matter of principle to us.

The Kaspersky Lab Global Research and Analysis Team (GReAT) has become the core repository of our expertise in the field. GReAT comprises top-notch security experts who analyze new and complex cyberthreats. Over the last few years, GReAT's combination of expertise, passion and curiosity has led to the discovery of several infamous cyberespionage and cybersabotage campaigns, including Flame, Gauss, RedOctober, NetTraveler, Icefog, Careto/The Mask, Darkhotel, Regin, Cloud Atlas, Epic Turla, Equation and Duqu 2.0. With this in mind, it makes sense that GReAT is sought out by international organizations, national and regional law enforcement agencies around the world,

(including INTERPOL, Europol, The National High Tech Crime Unit (NHTCU) of the Netherlands' Police Agency) and Computer Emergency Response Teams (CERT) to help investigate cybercrime. Major IT companies including Adobe, Google and Microsoft receive information about the vulnerabilities of their products from GReAT on a regular basis.

We also share our expertise with the professional community. A significant example is that the company has organized, for six consecutive years, the global annual Security Analyst Summit (SAS) – an event that brings together the world's best IT security professionals to share their expertise with international organizations, law enforcers and businesses. The event provides two full days of learning opportunities and networking with industry experts and covers all aspects of the global threat landscape. In 2015 more than 250 delegates from 23 countries attended the conference.

The Kaspersky Security Network (KSN) is a complex distributed infrastructure dedicated to processing depersonalized cybersecurity-related data from millions of voluntary participants around the world. By participating in Kaspersky Security Network, users of Kaspersky Lab security products around the world contribute to building a safer Internet environment. We use this data to ensure quick reaction times to new and advanced threats to maintain the highest level of protection for all of Kaspersky Lab's users, as well as to enhance the usability of our products. KSN is just one of the sources we use to improve our expertise and make sure it stays up-to-date. That's one more thing about knowledge – you lose it if you stop learning.

42

THE GREAT COMPRISES 42 UNIQUE EXPERTS ON CYBER THREATS

80

MILLIONS VOLUNTARY PARTICIPANTS ARE CONNECTED TO KASPERSKY SECURITY NETWORK CLOUD INFRASTRUCTURE

40

INFORMATION ON NEWLY EMERGING THREATS AND THEIR SOURCES IS AVAILABLE TO ALL KSN USERS IN 40 SECONDS

EDUCATIONAL PROJECTS

The company has organized, for five consecutive years, the global annual Security Analyst Summit (SAS) — an event that brings together the world's best IT security professionals to share their expertise with international organizations, law enforcers and businesses.

The Kaspersky Academy is a project designed to support and develop young cybersecurity talent. We are looking for accomplished young people to give them the opportunity to show their worth, while enhancing their knowledge and skills. Kaspersky Lab also organizes Cybersecurity for the Next Generation, an annual conference that gives undergraduate students from different countries the opportunity to get to know peers and IT security professionals, share their knowledge, ideas and experience, and gain in-depth practical knowledge on how to start building their careers. The Kaspersky Academy also runs a program for those interested in doing an internship at Kaspersky Lab.

In 2015 The Security Startup Challenge (SSC) was launched. It is a mentor-driven acceleration program, developed and implemented by the Kaspersky Academy, in partnership with venture industry leaders. SSC provides startups with access to cutting-edge business, cybersecurity and cross-industry expertise from around the world.

Hundreds of thousands of users and subscribers visit Kaspersky Lab's web resources, which are published to educate about cybersecurity. Eugene Kaspersky's personal blog is available in 10 different languages and receives up to 20,000 unique visitors a month. Kaspersky Lab's corporate blog has a monthly audience of close to 400,000 readers, which makes it one of the world's most popular online resources dealing with cybersecurity.

PROTECTING CHILDREN AND ADOLESCENTS

One more thing about knowledge. It's a powerful tool that could be used both in the name of good and to do harm. Words can save and words can kill – literally. One of the key social issues in the digital environment now is, from our point of view, the danger for those who can't yet protect themselves. Cyberbullying is a pressing issue for families coping with the challenges of the digital world today. It is obvious that problems such as cyberbullying make people feel less safe online. It is the mission of our company to make the Internet a safer place, which is why we decided to invest in research into cyberbullying and help organizations that are successfully fighting against it. By raising awareness of the issue and educating parents and children we aim to help them to feel empowered in the face of online threats.

Half of all parents worry that their children could fall victim to cyberbullying, according to a joint study by Kaspersky Lab and B2B International, an international research firm. Their concern is justified. For example, in Russia, the consequences of bullying are often so serious that 58% of the time parents or educators have to become involved to help the targeted child. We have accepted the challenge to raise awareness about this issue globally.

We initiated a discussion about cyberbullying as a pervasive problem at Mobile Congress, Barcelona in spring 2015, engaging leading international experts in the talks. "The core problem is that our communication tools have hugely evolved over the past decades, yet the development of literacy skills [with regard to these tools] is not keeping up," said Janice Richardson, Senior Advisor at European Schoolnet. To combat this very serious threat, we have launched several social projects intended to teach both children and their parents how to resist and counter social pressure on the web and social media.

The Kaspersky Lab Anti-cyberbullying Educational Portal offers a large number of free resources that will help parents better understand how to protect their children from cyberbullying and its horrible consequences.

Another project launched in 2015 is "Words Can Save" – An interactive campaign to raise awareness of the dangers of cyberbullying. This is an interactive portal where users are invited to meet and communicate with two characters, Kate and Mike, via their smartphone or by means of voice recognition. Both children are victims of cyberbullying by their peers. Their lives are at stake and they have considered harming themselves. The goal is to persuade them not to give up on life, and the results can then be shared via social networks to educate others.

One other initiative, Familia Segura, was launched in Spain in 2014; it includes stage plays which aim to teach children about cyberbullying, as well as master classes for parents. This format has proved so popular that we are planning to replicate this project in other regions. In 2014 we also ran our first joint project with European Schoolnet (a network of ministries and departments of education across Europe). We donated EUR1 from the sale of some Kaspersky Lab products in Europe to support the Insafe Helpline Fund Call Center, which was set up to answer questions from kids who have found themselves to be cyberbullying targets. We collected EUR30,000 through these efforts – enough to help 9,000 children in 2015.

800,000

TEENAGERS ARE TARGETED IN FACEBOOK CYBER BULLYING ATTACKS EVERY YEAR IN THE US ALONE

18%

OF ALL PARENTS HAVE BEEN DOING NOTHING AT ALL TO PROTECT THEIR CHILDREN FROM THE CYBER BULLYING THREAT

50%

OF VICTIMS DO NOT SAY ANYTHING TO THEIR PARENTS

HOW ONE UNPLEASANT STORY TURNED ORDINARY POLICE OFFICERS INTO CYBER COPS

Police officers are usually the ones to impose fines, but in October 2012 in Manchester, it was the police themselves who were fined the hefty sum of ? 120,000. How were they at fault? A memory stick, which contained data about a thousand criminals, was stolen from the home of a law enforcement officer. Unbelievably, the data was stored unencrypted! The UK authorities gave the matter some thought, and decided to spend money on educating police officers about the basics of IT security to make sure similar incidents never happen again. Today, cybersecurity training centers are up and running at police departments around the world. So where do cyber cops get their training and how does it work?

Let us, for example, take a look at the Indian megalopolis of Mumbai (formerly the City of Bombay). The Mumbai Cyber Lab opened there 11 years ago, and now offers a 6-day course in online crime investigation, at the end of which students take a mandatory online test. The police departments themselves pick the candidates to take the course and the «chosen» are more than happy to gain new knowledge which can put them on a fast-track career path. The Mumbai Police already have a «Cyber Squad.» Cyber Squad officers take regular refresher courses at the Cyber Lab and attend workshops, for example, on «hacker ethics,» in order to get a better insight into hacker psychology. Every year, Mumbai Police organize a Cyber Security Week, during which police officers and IT companies talk to university and high school students, their parents, bankers and high-ranking police officials about cybersecurity issues.

Japan has also decided to get serious about bringing its police up to date on digital technology. The authorities made the decision after police arrested four innocent people who were accused of creating and distributing a so-called «terror virus» which sent mass emails threatening terror attacks all across Japan. Investigators later discovered that the virus had infiltrated the suspects' computers and turned them into bots. The likely creator of the virus was eventually discovered and placed in custody. However, the police came to the correct conclusion after this setback. Cyber crime investigation experts at Tokyo's Metropolitan Police are currently training police officers from other parts of Japan about how the Internet works, the methods used to hack into wireless and Wi-Fi networks, and how malware is used to take remote control of computing devices and smartphones.

Cyber Squad officers take regular refresher courses at the Cyber Lab and attend workshops, for example, on «hacker ethics,» in order to get a better insight into hacker psychology

It goes without saying that US law enforcement agencies and departments across the nation have a full complement of cyberpeace and enforcement officers and just about every government agency now has a cybersecurity division. The Feds and the FBI, are making a tremendous effort to investigate cybercrime. The US Department of Justice has an active Computer Crime and Intellectual Property Section (CCIPS), and there is a whole National Cyber Security Division within the US Department of Homeland Security. The National White Collar Crime Center, a non-profit with expertise in cybercrime analysis and investigation, provides relevant training to police and law enforcement and security agency officers.

The European Union is not far behind. Europol has joined forces with the European College for Police (CEPOL) to offer training to police officers across the European Union, to improve their awareness of cybersecurity issues. One of these training sessions was provided in Sweden and Finland in October 2014. Estonian police received training in how to effectively search for cyber-evidence and how to carry out a cybercrime investigation in November 2014. CEPOL also runs online training in cybersecurity and cybercrime prevention and investigation for senior police officers.

But let us go back to the United Kingdom. As the old English adage goes «every cloud has a silver lining,» and the unfortunate incident with British police officers not only helped to identify a problem with their training, but also became a strong incentive to search for ways to address this problem. The UK police authorities took the matter very seriously, and when Kaspersky Lab UK approached the City of London Police with an offer to provide training for police officers, it was readily accepted. A joint project between Kaspersky Lab and the City of London Police was born — a series of exclusive training sessions in cybersecurity fundamentals designed for the City of London Police officers.

The first ten City of London Police officers came to Kaspersky Lab's Moscow Headquarters in February 2014. Their cybersecurity trainers were Global Research and Analysis Team professionals, who gave them much more than just the underlying theory — they took part in three-weeklong hands-on training sessions that were so effective that the City of London Police Academy has since incorporated them into their curriculum.

So, you can't go wrong by taking a page out of the UK police's book. If you get into trouble, don't get too upset: a brilliant idea might just come out of a bad experience.

The first ten City of London police officers came to Kaspersky Lab's Moscow Headquarters in February 2014

THE STORY OF MAURIZIO ABBA, WHO HASN'T SAVED THE WORLD YET, BUT IS SAVING IT LITTLE BY LITTLE EVERY DAY

This is a highly regular and ordinary story. No, no, our hero is a good guy and an excellent expert in his field. His name is Maurizio Abba. And he even won a prize at the CyberSecurity for the Next Generation 2014, a conference for undergrads organized by Kaspersky Lab. All of this is true. However, he hasn't done anything truly great yet. He has not saved the world from a horrible catastrophe, has not prevented the spread of a highly destructive virus, not has he discovered a hackers' syndicate. This is, we repeat, an ordinary story. You won't believe how great it is. But we will attempt to explain.

EDUCATIONAL PROJECTS

When does our story begin? In 1995 in Turin, when Maurizio Abba was born. He spent his childhood years in Torre Pellice, a small town on the French-Italian border. When little Maurizio turned seven, his dad gave him his old computer as a birthday present, and a window into the pixellated world of Space Invaders along with it. After learning to use a laser cannon to protect himself against invaders from other planets, Maurizio decided he would definitely become a videogame developer.

He came very close to living his dream as a high school senior. After reading all of the available information on game coding, Maurizio teamed up with a buddy to create alternative versions of Tetris and Pac-Man. However, nothing came of it. The teenage Maurizio reached the conclusion that he preferred regular software, without any graphics or embellishments.

That was in 2008; which was also the year Kaspersky Lab organized its first security conference for undergraduate students, under a slightly different name: IT Security for the New Generation. Kaspersky Lab came up with an event format to bring together undergrads, experts and university professors to discuss the burning issues of cybersecurity and promote a culture of data protection. Kaspersky Lab provided grants for the best young scholars at the conference to allow them to continue their research.

However, we left our hero at a point when he was still not even contemplating cybersecurity but had decided to become a software developer. After graduating from high school, Maurizio enrolled in the IT Program at Turin Polytechnic.

He did not stay long in his home country. He has always had a certain wanderlust, and was always attracted to new countries and new experiences. He spent one year of his five-year program taking courses in Shanghai, and another in Nice. Maurizio became a very good software coder at university, and did his Bachelor's thesis on artificial intelligence. However, his priorities changed once again. One day, Maurizio was in his dorm room trying to set up a Wi-Fi connection, which can be pretty patchy at student residence halls. At some point, he became curious about the difference between protected and unprotected connections. He decided to figure out how they worked, as well as looking into secure networking methods. He started to explore what information security experts did in their jobs, and found their work fascinating. Maurizio decided to do his final graduation thesis on cyber security.

At the same time, Maurizio enrolled in EURECOM, a graduate engineering school in France. It was there he started working on Web Honeypots 2.0: An Analysis of Exploitation Behaviors on the Web, under the guidance of his professor. Honeypots is the name for fake unprotected websites that are created specifically to be attacked. His research of the website cracking technology used by hackers saw Maurizio come first in the regional round of CS for The Next Generation, before going on to Stockholm to win first prize for best elevator pitch-style presentation at the Seventh Conference.

"I wanted to find out what hackers were doing after they infiltrated a website," Maurizio says. "Maybe they'd just post their own photos or try to break into other websites? I found this topic incredibly fascinating; I guess that's why I won." Maurizio Abba thinks writing the best elevator pitch was easy – "it's essentially just like an article for a science journal."

"You start out by writing down everything that comes into your head. Then you realize that you have written a thesis instead of an article. Then you start picking out the key ideas, the main concepts, and you keep doing that until all you have is an A4 page. The presentation time is very limited, but there is so much to say! This conference gave me a unique opportunity to meet some awesome people from different countries on an informal basis. I am still in touch with some of them.

HELPING TO PROTECT HIS MOTHER

Maurizio is living and working in London now, in his first job at Lastline, a US company analyzing complex malware. There is a lot of work and long hours – the company is very small, practically a startup with many larger competitors. However, this is something he has dreamt of.

"I have chosen this job over doing a doctorate degree because I wanted to make something that even people without a solid understanding of technology could use to ensure their security. People like my Mom. She is not very computer savvy, she keeps saying: "My boy's working in London at some kind of a security company." However, she is much savvier now than she used to be. She used to say things like: "Hey, I got an email telling me to transfer 500 Euros. And I did. I did the right thing, didn't I?" Maurizio believes that cyber security experts will be in demand for a long time to come.

"Everybody knows what happened to Sony recently: a major company, an entertainment giant was hacked by some guys. We used to think that war is assault rifles and tanks. However, it is enough to have an old computer and a malicious mind to wage cyber war! I think the time has past when computer security was something done by weirdoes living in a basement. Now the importance of this topic can no longer be disputed ."

Unfortunately, Maurizio is right – the world is not getting any safer. And yet, at events like CyberSecurity for the Next Generation, we see increasing numbers of young people genuinely interested in cyber security and concerned about saving the world. This is a good reason to be optimistic.

HOW ADULTS NEARLY FORGOT ABOUT THEIR CHILDREN WHILE TRYING TO PROTECT THEIR ONLINE WALLETS

One child in three (for those with access to the Internet) has encountered social harassment online. This issue is nowhere near as significant in the adult world. In fact, cyberbullying does not even make it into the top 10 online threats highlighted by adult Internet users. So how is it possible that we don't know what dangers our children are facing, and how can we change this?

Teenagers have been terrorizing one another for as long as there have been teenagers. You will certainly have found yourself in situations at school, or even outside, when older or stronger kids would terrorize those who were younger and weaker. Generally though, it all ended when everybody went home. In today's online world, when a child is at home and alone with a gadget connected to the Internet, the worst is often about to begin. Cyberbullying knows no physical boundaries. The victim is alone, with the whole world seemingly against them. Surviving this kind of ordeal would be hard even for adults.

In 2002, Canadian teenager Ghyslain Raza made a video of himself for fun pretending to be a Star Wars character swinging a golf ball retriever as if it were a light saber. One of his classmates uploaded the video to the Internet without Raza's permission, where it went viral and was seen by millions.
The video looks perfectly innocent. However, for Raza, who was overweight at the time of the video, life soon became hell. Online harassers humiliated and insulted him, suggesting he should commit suicide, while the media immediately dubbed him the Star Wars Kid.
He lost all of his friends and had to change schools, while his parents had to hire a psychiatrist and sued the parents of the classmate who posted the video. "No matter how hard I tried to ignore the hateful messages, I felt like a total loser, and my life did not seem worth living," Ghyslain said in an interview 10 years after the first recorded cyberbullying incident. ("'Star Wars Kid' speaks out" www.macleans.ca)

Some modern parents are convinced they know what perils are lurking online. They know from their own experience that shocking content can be found online, and that you can make questionable acquaintances or lose a lot of money on a credit card, and they want to protect their children from these threats. But it is unlikely they have been harassed on social networks. And when they eventually do find out what is happening to their child, sometimes it is too late.

Cyber bullying victims almost never turn to adults for help because they are afraid they'll be subjected to an even worse punishment ; having their computer or mobile phone privileges taken away. Fear of losing access to the virtual world forces cyber bullying victims to hide their problems until they can take no more.

We at Kaspersky Lab started thinking about how we could make the situation better. Unfortunately, we cannot protect every single potential cyber bullying victim. However, as security experts, we can teach people to fight cyber bullying and give them the tools to defend themselves.

63%

OF TEENS AGED 11 TO 19 SEE ONLINE SAFETY AS ONE OF THEIR FUNDAMENTAL RIGHTS

54%

OF CHILDREN AROUND THE WORLD SAY THEY ARE SERIOUSLY WORRIED ABOUT CYBER BULLYIN

The time to sound the alarm came a long time ago: as many as 70% of all teens in China have been subjected to cyberbullying, 53% in Singapore, 48% in Russia and 39% in Germany (according to the Microsoft OnLine Bullying Survey)

TYPES OF CYBER BULLYING

Every cyber bullying incident is unique, but we've identified several key varieties of cyber aggression

Slander

Alienation (isolation). Excluding someone from online communities

Flaming. Exchange of angry, cruel or rude messages by users on public and private online forums

Happy Slapping. Videotaping actual physical abuse of the victim and distributing the footage online

Impersonating the Victim. The predator impersonates the victim and sends messages or distributes questionable information in the victim's name to ruin their reputation

Text wars/text attacks. Harassing or bullying the victim by sending a large number of small text messages or emails

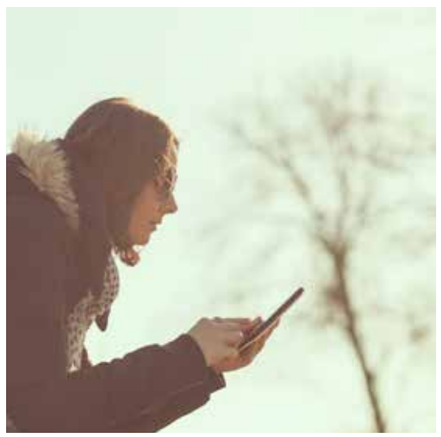
Trolling. Aggressive attacks designed to provoke the victim into retaliatory aggression

Cyberbullying is a complicated problem which cannot be solved with just a technological solution, but requires a complex approach, a very important part of which is raising the mutual awareness of kids and their parents. Kaspersky Lab offers mature technology in its flagship consumer protection products, e.g., Parental Control for Windows and OS X that can prevent children from visiting undesirable websites or disclosing personal information and can monitor the appearance of selected words, such as abusive language, on social networking sites, IMs and so on.

Alas, even the best software cannot rid the world of violence. How should parents react if they find signs of cyber bullying attacks against their child? What can children do when they find themselves victims of these attacks? We realized that even experts had no easy answers , so we decided to take things further.

The kids.kaspersky.com project offers an emergency response and aid to anyone who faces cyberbullying. Here we put together all the essential information about the problem, offering expert advice for adults, as well as creating an interactive educational game for kids that can prepare them for situations in which they are subjected to social pressure.

In 2003, 13 year-old Ryan Patrick Callahan killed himself after he could no longer bear the attacks by his former friends who set out to prove he was gay. After his son's death, Ryan's father found messages he had exchanged with a girl who used to be his girlfriend but who broke up with him over the attacks. "I am going to do it tomorrow, you'll read about it in the paper," Ryan wrote to those who bullied him, and his tormentors responded with, "This is gonna be a lot of fun!" This was the first known incident of 'bullycide', in which the bullying victim died.



Edutainment is a great idea for the offline as well as the online world. In 2014, our Familia Segura initiative was launched in Spain. And finally, our efforts to fight cyberbullying have started to get government support at a national level. Our first joint project with European SchoolNet has brought excellent results.

It is hard to say how much effort and how much time we are going to have to spend to remove cyber bullying as a global online threat. But we are going to see this through. Join us, and together we will make the Internet a safe environment even faster.

Find out more about the issue of cyberbullying and ways to defend against it at www.wordscansave.me.

TECHNOLOGY THAT DOES MORE THAN WE EXPECT

We give our customers — both individuals and huge corporations — great confidence in their devices. We cover all existing platforms and currently have 38 versions of our most popular products. What difference does this confidence make to people's lives? What difference does it make that they can afford to not think about the dangers, and focus on their own business and pleasure? You can probably decide for yourselves. However, some of our products and solutions go far beyond simply protecting personal or corporate data. They do not fit the standard ideas of business logic. And we want you to know about them.

10 MOST POPULAR KASPERSKY LAB PRODUCTS WHICH CAN BE USED / TRIED FOR FREE

Kaspersky Internet Security for Android — a powerful protection solution for the most popular mobile operating system

Kaspersky Safe Browser for iOS, Kaspersky Safe Browser for Windows Phone — browsers that can block dangerous online resources and enable the user to filter content

Kaspersky Security Scan — a quick computer scan for viruses and other threats on Windows

Kaspersky Virus Scanner — an easy-to-use tool to check Mac devices for viruses, Trojans and more

Kaspersky QR Scanner — a mobile app for secure QR code scanning

Kaspersky Rescue Disk — a tool to recover a system after a critical virus attack

Kaspersky Virus Removal Tool — a utility to clean a computer of viruses and other threats on Windows

Kaspersky Password Manager — an app for the secure storage of passwords, allowing them to be synchronized across all the user's devices including Windows, OS X, iOS and Android.

Phound! — a utility for Android that helps to find lost or stolen devices, or block them remotely if needed.

Kaspersky Threat Scan for Android — a tool that detects vulnerabilities that can result in the theft of financial or personal data from a mobile device.

People can try nearly all of our products for free. This is common practice in the mass consumer market, but can be very effective when it comes to protective software. For the majority, protective software is not thought of as essential, because most people have very little idea of just how vulnerable they actually are in the cyberworld. However, many agree to try it out for free, and this often becomes the first lesson in cybersecurity for those who have never thought about it.

People can use a whole range of our solutions for free, for an unlimited amount of time. All of these solutions are compatible with each other. The fact that even those who cannot pay for our protection still use it is very important to us.

CRITICAL INFRASTRUCTURE PROTECTION

The early pioneers and philosophers of digital technology could never have predicted that the essential facilities and infrastructure, which now support daily life, can be controlled by software linked to a single network. Even modern armies are unable to defend these facilities and infrastructure. Hacking and other attempts to compromise industrial systems that control infrastructure are methods used for terror attacks, unfair competition and political struggle. The leaders of the world's major powers are getting serious about tackling this problem, and Kaspersky Lab is already actively developing a suite of solutions capable of protecting critical infrastructure at all levels — from PC networks down to embedded devices.

KasperskyOS — a secure operating system in development by Kaspersky Lab with security specifically to protect embedded connected devices, such as smart meters, programmable logic controllers (PLC) and medical devices, in environments where cyber security is a top priority, including the Internet of Things and the Industrial Internet of Things.

Kaspersky Security System — a platform allowing access control rules according to a given security policy, able to classify the informational resources and configure the interaction between the different components of a protected system. It is available as a main component of KasperskyOS and an embeddable OEM component to manufacturers and vendors of comprehensive IT solutions.

Kaspersky Endpoint for Business — Kaspersky Lab's flagship corporate product approved by leading developers of automatic control systems (Siemens, Rockwell Automation, Emerson) as a defensive solution.

Kaspersky Industrial Protection Simulation — training system which teaches the key cyberthreats to large industrial facilities and ways to defend them.

Kaspersky Industrial Security — a specialized product intended for critical infrastructure protection. It includes Endpoint protection from cyberthreats and Network monitoring to inform security officer about all incidents within the network.

35%

MALICIOUS ATTACKS ACCOUNT FOR 35 PERCENT OF THE CAUSES OF INCIDENTS IN INDUSTRIAL NETWORKS

PROTECTING CHILDREN IN THE CYBERWORLD

49

DEVICES ARE CURRENTLY PROTECTED BY KASPERSKY SAFE KIDS SOFTWARE

Many people have a nasty surprise when they see how fast their children become immersed in the cyberworld. The life of children in this environment is mostly hidden from the eyes of parents, especially when children are using mobile devices, and there are few ways to effectively protect them from the negative impacts. It would be no great exaggeration to describe this as a problem for the whole of civilization as well as individual families. We firmly believe that it is our duty as cybersecurity experts to help parents protect their loved ones from any threat – and we are doing this already. Kaspersky Safe Kids offers what we believe is the most thorough system for protecting children against online dangers, without restricting them from the best things the cyber environment has to offer.

Kaspersky Safe Kids is a multi-platform solution for Windows, OS X, iOS and Android managed through the My Kaspersky portal. Our developers set the goal of not only protecting children from cyberthreats, but to providing a healthy way to learn and grow in the modern world, combining online and offline environments. Below are just some of the key features included in this solution:

— **Kaspersky Safe Kids goes far beyond the customary boundaries of familiar parental controls.** Now adults can manage kids' access to various gadgets and categories of apps, in addition to blocking inappropriate or undesirable content.

— **Kaspersky Safe Kids teaches children to behave responsibly in the cyber world,** helping them develop the habit of carefully managing information about themselves and their families.

— **Kaspersky Safe Kids always keeps you connected to your children.** No matter what devices you and your children use, you will always have information about their online activity.

In other words, our products offer a serious addition to the process of raising children, and the development of their relationships with parents.

A STORY OF VITAL TECHNOLOGY THAT WE DON'T NOTICE UNTIL IT SUDDENLY BREAKS DOWN

Hollywood screenwriters have run out of ideas. Every year, they come up with new ways to end the world, and civilization as we know it, in one fell swoop. Violent tectonic shifts, meteor strikes, uprisings of robots or great apes, epidemics — they've tried it all, several times over. However, there's an excellent plotline that screenwriters tend to overlook: a computer virus can destroy the essential infrastructure critical for modern human activity and everyday life. In reality, we are just a few steps away from seeing this scenario play out, with dire consequences. The real (rather than imaginary) threat to our civilization is that people responsible for critical infrastructure don't always know how serious this problem is.

AN UNEXPECTED SCENARIO

However, you have to hand it to Hollywood: some 20 years ago, stories with heroes saving the real world from virtual threats were, for a short time, the height of fashion. The bad guy in Hackers, a 1995 movie, came up with the idea of using malicious code to cause oil tankers to capsize at sea. «Good hackers» were able to save the day that time. Evil computer whizzes faced a few more defeats on the silver screen, and then Hollywood decided it had done its job. However, year after year, digital technology rapidly takes over essential aspects and areas of our lives, yet, the threat of shady characters breaking into the control system of a nuclear reactor or something equally important has apparently not become one of humanity's biggest fears. A meteorite impact is so much more spectacular and easier to get your mind around.

Everything started to change in 2010. One summer day, antivirus expert Sergey Ulasen found traces of an unusual online virus. The malicious code looked exactly like a legitimate piece of software (which meant it went unnoticed by antivirus software) and was capable of taking over any system it infected. Experts sounded the alarm, but their efforts to find out where the virus, which became known as Stuxnet, had come from and how it was spreading were futile. By the fall of 2010, the Iranian authorities announced that nearly half of all the top secret facilities in the nation's nuclear program were out of commission after control systems used in uranium enrichment centrifuges were infected by Stuxnet.

Kaspersky Lab experts were among the first to «figure out,» or «decipher,» the new virus. Their conclusions were shocking: Stuxnet was written by software coders of the highest caliber in order to take over specific elements of strategic infrastructure. Its proliferation around the world was just a side effect.

«Stuxnet does not steal money, it does not send out spam or steal confidential data. This piece of malware was created to control, in a literal sense, large industrial facilities, whole plants,» Eugene Kaspersky wrote in his blog at the time. «Only a short while ago, we were only fighting cyber criminals and online bullies, but now, I'm afraid, the time is coming for cyber terror, cyber weapons and cyber wars.»

Everything started to change in 2010. One summer day, antivirus expert Sergey Ulasen found traces of an unusual online virus

WHAT CEOS DO NOT SAY

This essentially means that power plants, chemical factories, oil refineries, nuclear facilities and transport infrastructure are all at risk

Alas, Eugene Kaspersky has been proven right. Since 2010, the list of new attacks against strategic infrastructure has been growing steadily. However, planned hacker attacks are just part of the problem. In September 2014 alone, there were more than 13,000 instances of accidental viral infection of computers running complex technological systems used by Siemens, Rockwell, Wonderware, General Electric, Emerson and others. This essentially means that power plants, chemical factories, oil refineries, nuclear facilities and transport infrastructure are all at risk.

"Many people will find it strange, but actually, breaking into a system that controls, for example, reactor units, is very easy. In fact, breaking into it is easier than breaking into a well-protected computer or a smartphone," says Sergey Ulasen, who is now a Kaspersky Lab expert. "People still think that if their system has no direct Internet connection, and watchful security guards do not allow unauthorized personnel to approach the facility, there is no threat. However, this is no longer the case and hasn't been the case for years. We all expose ourselves to great risks unless we finally get our act together and securely protect elements of critical infrastructure."

The reasons for this sorry situation are obvious. The majority of industrial equipment is still controlled by aging operating systems that offer minimal data protection. The upgrade or re-installation of these systems involves the risks posed by equipment downtime and standard protection tools for computer systems will not work. As a result, the management of infrastructure components often simply ignore this issue altogether.

Inadequate data encryption, weak password safekeeping methods, a lack of reliable ways to run upgrades, and poorly qualified employees are the most obvious vulnerabilities hackers actively take advantage of when they take over various systems.

To make matters worse, operators often tend to try and conceal incidents of unauthorized access to critical infrastructure systems, to avoid damaging their reputations.

WHERE TO GO FOR HELP?

The situation really is quite dire. Recent data from Kaspersky Security Network suggests that more than 17% of all industrial systems have been targeted and intentionally infected. However, even the most technologically advanced developed nations are only just starting to address this problem at the national governmental level. The market for IT protection of critical infrastructure is just beginning to take shape, and Kaspersky Lab has become one of the frontrunners, capable of providing effective contemporary protection for strategic facilities.

17%

17% OF ALL INDUSTRIAL SYSTEMS HAVE BEEN TARGETED AND INTENTIONALLY INFECTED

Kaspersky Lab clearly cannot save the world from cyber terrorists on its own. The company is offering ways to preinstall the Kaspersky

Security System as a stand-alone module in real-time operating systems offered by other vendors. Kaspersky Lab is also actively involved in helping to refine and improve international security standards for strategic facilities by sharing its knowledge with the staff of companies and organizations managing critical infrastructure.

KASPERSKY lab