KASPERSKY lab

Kaspersky Security Awareness

Computer-based training programs for all organizational levels

www.kaspersky.com/awareness
#truecybersecurity

The effective way to build cybersafety across your organization

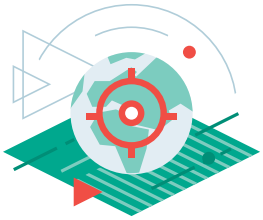
More than 80% of all cyber-incidents are caused by human error. Enterprises lose millions recovering from staff-related incidents – but the effectiveness of traditional training programs intended to prevent these problems is limited, and they generally fail to inspire and motivate the desired behavior.

Why are customers not happy with existing awareness training programs?

- Unsure how to set goals and plan education
- Training takes too much time to manage
- Reporting does not help in goal tracking
- Employees don't 'buy into' the program → so don't develop the skills

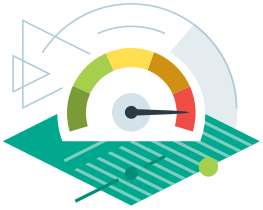
Kaspersky Security Awareness – a new approach to learning

Key program differentiators



Setting objectives & choosing a program

- Goal-setting based on global data
- Benchmarking against world/ industry averages

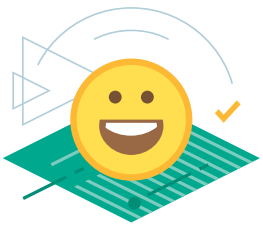


Learning management

- Automated learning
- Self-adjusting learning paths
- Calculation of time spent

Reporting & analytics

- Actionable reports anytime
- On-the-fly analysis of potential for improvement



Program efficiency & appreciation

- True gamification
- Competition & challenge
- Overload prevention

Effective Security Awareness

Staff training at all levels is essential in raising security awareness across the organization and motivating all employees to pay attention to cyberthreats and countermeasures – even if this is not perceived as a specific part of their job responsibilities.

Employee errors are responsible for the majority of cybersecurity incidents in organizations today.

Human error can be a major organizational cyber-risk, even when traditional awareness programs are in place:

$1,155,000 per enterprise – the average financial impact of attacks caused by careless/uninformed employees*

$101,000 for every SMB –the financial impact of attacks caused by phishing/ social engineering **($1.3M per enterprise)***

Up to $400 per employee per year – the average cost of phishing attacks**

---

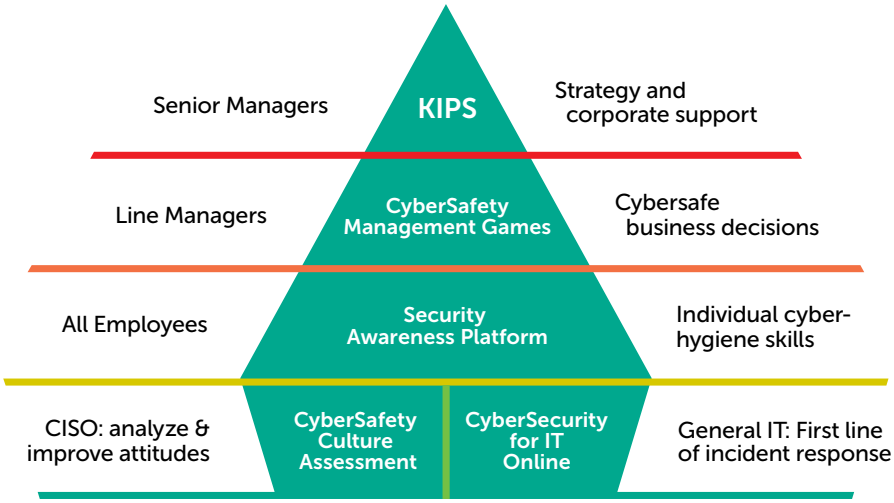
* Report "Human factor in IT security: How Employees are Making Businesses Vulnerable from Within", International, June 2017

** Calculation based on Ponemon Institute "Cost of Phishing and Value of Employee Training", August 2015

Kaspersky Security Awareness training

Kaspersky Lab has launched a family of computer-based gamified training products that utilize modern learning techniques and address all levels of organizational structure. This approach helps create a collaborative cybersafety culture which engenders a self-sustaining level of cybersecurity throughout the organization.

Different training formats for different organizational levels



An approach that delivers proven results

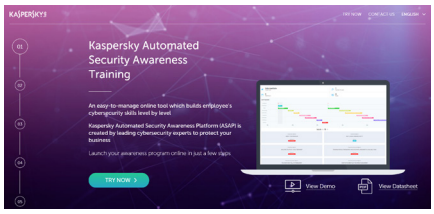
Up to
90%
reduction in the total number of incidents

At least
50%
reduction in the financial impact of incidents

An amazing
86%
of participants would definitely recommend the program to others

Employees are a key focus for cyber-attackers

As businesses become more aware of the threat of cyberattacks, technical defenses are becoming stronger. It's far more difficult to hack into corporate networks than it used to be. Because of this, hackers are creating new methods of accessing secure data. These efforts are being directed at the new weakest link in corporate cybersecurity - employees.



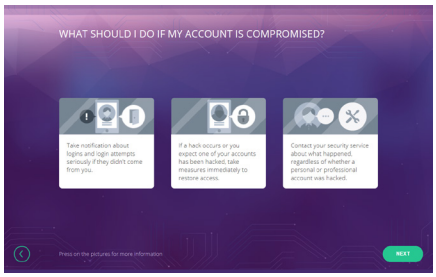
ASAP offers easy-to-set training objectives, a well-balanced predefined learning path, real-life relevance and actionable reporting ensure program appreciation and value for employees and management alike.

Each topic comprises different levels, developing specific security skills. Levels are defined according to the degree of risk they help eliminate. Level 1 addresses behavior in the face of straightforward and mass attacks. Higher levels provide awareness training when faced with the most sophisticated and targeted attacks.

The platform is available in 7 languages: English, German, Italian, French, Spanish, Russian and Arabic*.

ASAP is ideal for MSPs and xSPs – training services for multiple businesses can be managed through a single account, and licenses can be purchased on a monthly subscription basis.

Trial a fully functional version of Kaspersky ASAP at asap.kaspersky.com - see for yourself just how easy it is to set up and manage your own corporate security awareness training program!



Security awareness training - building cybersafe workforce behavior

Online interactive training through two separate platforms, addressing the differing needs of growing businesses and large enterprises while catering for a range of current employee cybersafety skills-levels.

Kaspersky Automated Security Awareness Platform (ASAP) for Growing Businesses.

A new holistic approach to online educational programs, based not just on knowledge but on 'pattern perception', empowering employees to behave safely, even when faced with completely new threats.

Automated learning management

- The platform takes just 10 minutes to launch - it's quick and easy to load your user-list, divide users into groups and set a target level for each group, based on risk levels.
- The platform itself then builds an education schedule for each group, providing interval learning with constant reinforcement, offered automatically through a blend of training formats, including learning modules, email reinforcement, tests and simulated phishing attacks.

Actionable reporting, available anytime

- Follow your learners' progress through the user-friendly dashboard, providing live data tracking, trends and forecasts
- Receive recommendations on how to boost results

Universal training curriculum

- A comprehensive range of key cyber-security topics are covered - all offered at different levels, from absolute beginner to advanced.

Key benefits:

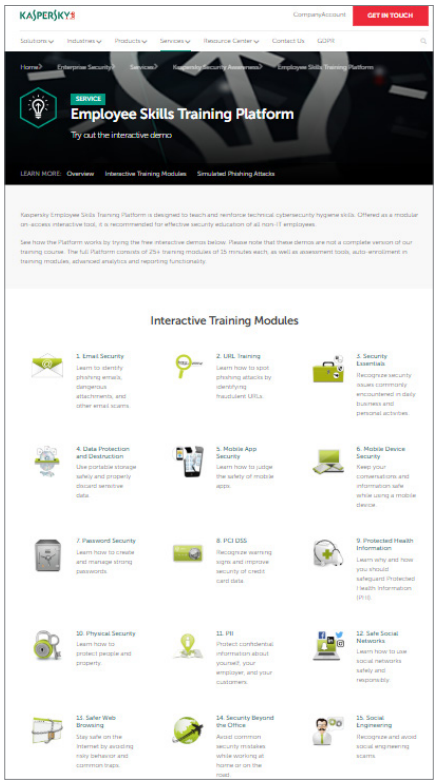
Simplicity through full automation: The program is very easy to launch, configure and monitor, and ongoing management is fully automated –no administrative involvement required.

Effectiveness: program content is structured to support micro-learning, keeping training sessions focused and bite-sized to deliver high levels of knowledge retention and subsequent skills application.
Flexible licensing: the per-user licensing model can start from as little as 5 licenses.

*Arabic will be added during 1H2019

Using the platform, and based on the recommendations provided with platform documentation, you can establish and implement a powerful, continuous and measurable cybersecurity education plan, encouraging employees to move from simple to complex security concepts, in line with their roles and responsibilities and the prevailing threat landscape.

The Employee Skills Training Platform covers all major security domains and provides advanced assessment tools and functionality for simulated phishing attacks, as well as comprehensive reporting capabilities.
The platform is available in 34 languages.
See our interactive demo at
www.kaspersky.com/demo-sa



EMPLOYEE SKILLS TRAINING PLATFORM for Enterprise Businesses

Through typical scenarios and situations, cyber-attack simulations, individual tasks and guidance, the platform builds an understanding of potential threats and provides the skills needed to deal with them. Online gamified learning allows employees to practice and learn through an interactive study portal.

Interactive Training Modules

- Fun & short
- Based on exercises with a knock-on effect
- Auto-enrollment reinforces specific skills
- 33 modules cover all areas of security

Knowledge Assessment

- Includes predefined or random assessments, customer-defined questions, and customizable length options
- Covers a comprehensive range of security scenarios
- A vast library of randomized questions ensures no cheating

Simulated Phishing Attacks

- 3 types of phishing attack with a range of templates and levels of challenge
- 'Teachable moments' which appear whenever employees open phishing emails
- Customizable templates
- Auto-assignment of training modules, covering knowledge gaps identified through simulated attack performance

Reporting & Analytics

- Results are broken down by department, location and job function, as well as presented at individual level
- Monitors employee skills levels and dynamics
- Supports data export to your LMS in various formats

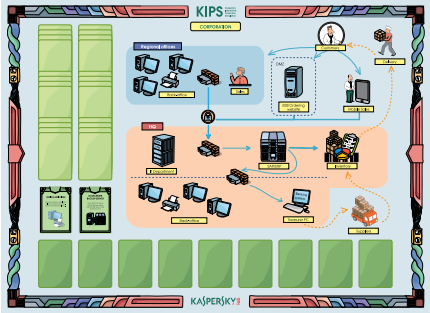
Key benefits:

- **Time-saving.** Only training directly relevant to the individual role is undertaken - specific training modules can be assigned based on the employee's role and expertise level.
- **Gamification and interactivity:** no dull explanations - just interactive learning by doing.
- **Provides concrete skills, not just knowledge:** combines educational materials and tests with simulated real-life situations.
- **Provides data for benchmarking:** compare your corporate performance with that of the industry overall.
- **No additional resources needed:** training can be conducted in the customer workplace – no additional skills/training/resources required.

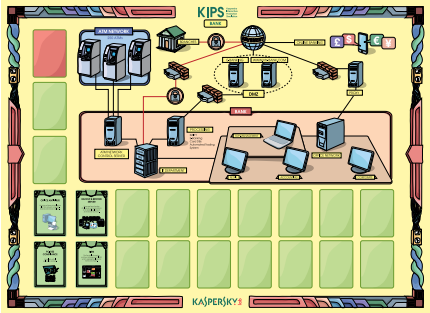
KIPS training is targeted at senior managers, business systems experts and IT professionals, increasing their awareness of the risks and security problems of running modern computerized systems

Some of KIPS scenarios:

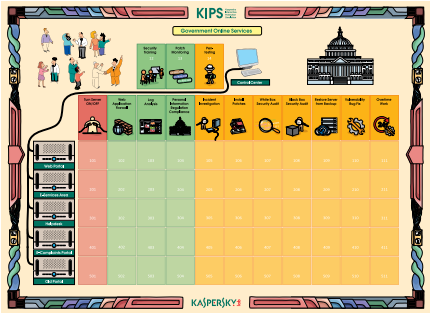
Corporation



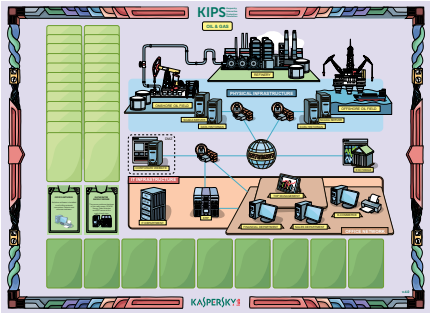
Bank



e-Government



Oil & Gas



KIPS online:

- Perfect for global organizations
- Up to 300 teams simultaneously
- Different teams can choose a game interface in different languages
- A trainer leads each session via WebEx

Kaspersky Interactive Protection Simulation (KIPS) training encourages strategic understanding and support

What is KIPS?

KIPS – is a team roleplay game that simulates a business environment where participants are tasked with handling a series of unexpected cyberthreats, while trying to maximize profits and maintain market confidence.

The idea is to build a cyberdefense strategy by making choices from among the best pro-active and re-active controls available.

KIPS is outstandingly effective because:

- It delivers a fresh workable approach to cybersecurity
- It's fun, engaging and fast (2 hours)
- It builds co-operation through teamwork
- It fosters initiative & analysis skills through competition
- It allows discoveries and mistakes in building cybersecurity and cybersafe behavior to be made and analyzed safely through gameplay

The KIPS experience:

- Be prepared for emerging threats – learn how criminals operate technically, (threat intelligence) and understand their goals
- See how to combine incident response with incident prevention
- See what happens when you forget to configure security controls properly
- Watch out for simultaneous alerts from security, IT and business standpoints

Industry-related scenarios available

(all exist as KIPS Live and KIPS Online – 10 languages are supported)

- **Corporation:** Protecting the enterprise from Ransomware, APTs, automation security flaws etc.
- **Bank:** Protecting financial institutions from high-profile APTs attacking ATMs, management servers and business systems.
- **e-Government:** Protecting public web servers from attacks and exploits.
- **Power Station/Water Plant:** Protecting industrial control systems and critical infrastructure.
- **Transport:** Protecting passenger and -freight carriage against Heartbleed, ransomware and APT.
- **Oil & Gas:** Exploring the influence of a range of threats – from website defacement to current ransomware and sophisticated APTs.

Each scenario demonstrates to participants the true role of cybersecurity in terms of business continuity and profitability, highlighting emerging challenges and threats and typical organizational errors when building their cybersecurity, while promoting cooperation between commercial and security teams – a cooperation which helps maintain stable operations and sustainability against cyberthreats.

CyberSafety Management Games
educating and motivating of line managers

- Combines gamification with comprehensive coverage of security topics, examples, explanations and exercises,
- Powered by purpose-built CyberSafety Management Games software, supporting an easy-to-manage training delivery process,
- Divided into short modules, running a total of 4 hours.

CyberSafety Management Games – ensuring cybersafe business decisions

This highly interactive workshop (a combination of computer-based and instructed learning) focuses line management on the importance of cybersecurity in their jobs and provides the competence, knowledge and outlook essential to maintaining secure working practices in their divisions.

The biggest challenge for the Security Team is all too often how to engage management - the people who interact with employees on daily basis and make business decisions.

That's why Kaspersky Lab has developed a **training program aimed at specifically converting line/middle management into cybersecurity supporters and advocates.**

Kaspersky CyberSafety Management Games provides managers with:

- **Understanding:** Internal adoption of cybersecurity measures as an important yet straightforward set of actions
- **Monitoring:** Seeing everyday working processes through the cybersafety lens
- **Cybersafe Decision Making:** Cybersecurity considerations as an integral part of business processes
- **Reinforcement and Inspiration:** Delivering influential leadership and guidance to departmental teams.

Can be licensed as "Train-the-trainer" for enterprise training centers, giving key deployment benefits:

- Ease of delivery – awareness trainers do not have to be security experts.;
- Ease of scheduling – short modular training sessions fit around the employee's work schedule.

Cybersecurity IT training targeting service desk specialists, general IT security & local service administrators

Training format

Training is 100% online – participants just need an internet connection/ access incorporating LMS and a Chrome browser.

Each of the 4 modules comprises a short theoretical overview, practical tips and between 4 and 10 exercises – each practicing a specific skill and demonstrating how to use IT Security tools and software in everyday work.

Study is intended to be spread over the course of a year. The recommended rate of progress is 1 exercise per week – each exercise taking between 5 and 45 minutes to complete.

Cybersecurity for IT Online

Interactive training for all those involved in IT, building strong cybersecurity and first-level incident response skills

Creating a strong corporate cybersecurity posture is impossible without the systematic education of all relevant employees. Most enterprises provide cybersecurity education and training on two levels – expert training for IT Security teams and security awareness for non-IT employees. Neither of these approaches works for the many IT staff not directly involved in security, but ideally placed to make specific and very important contributions to corporate cybersafety.

First-line incident response

Kaspersky Lab offers first-on-the-market online skills training for generalist Enterprise IT professionals.

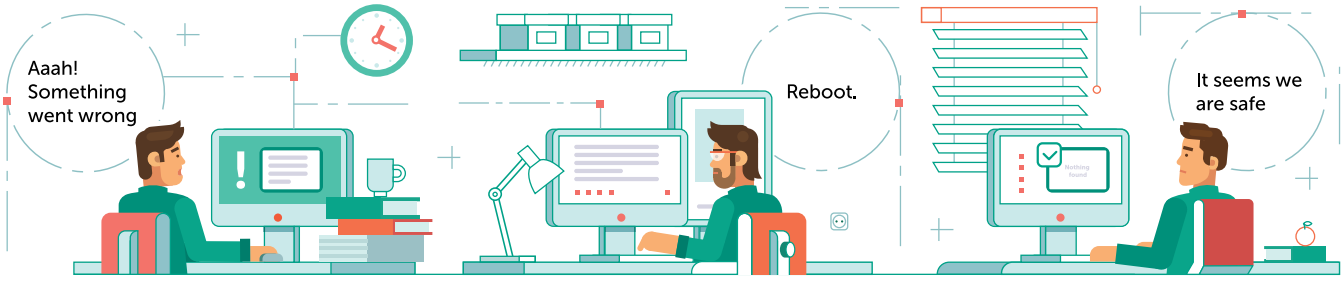
The course consists of 4 modules:

- Malicious software
- Potentially unwanted programs and files
- Investigation basics
- Phishing incident response

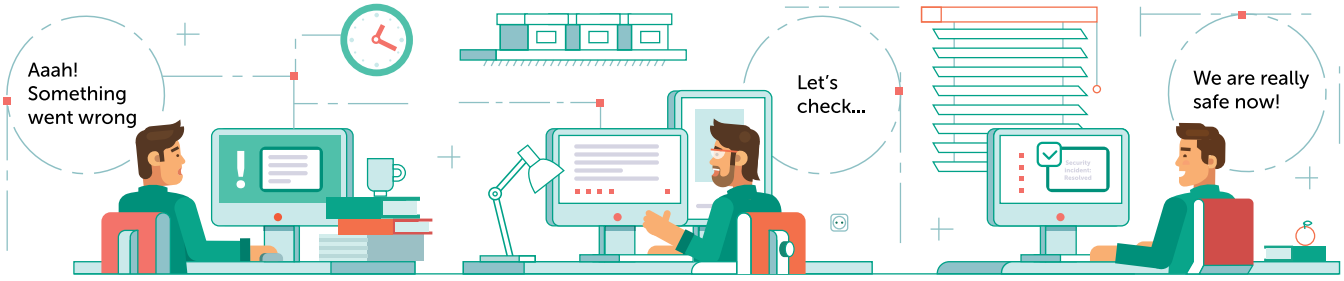
This course equips IT professionals with practical skills including:

- How to recognize a possible attack scenario in an ostensibly benign PC incident
- How to collect incident data for handover to IT Security
- Hunting out malicious symptoms – cementing the role of all IT team members as the first line of security and defense

Now



Should be



This assessment looks your at security culture from different perspectives:

- Organizational (managerial)
- Individual (employee)
- Expertise availability
- Security Assurance as a process

Assessment is through a cloud-based survey completed by employees in around 15 minutes. It takes an average of 2 weeks to run the survey though all employees.

The customer receives a consolidated report of survey findings.

CyberSafety Culture Assessment

CyberSafety Culture Assessment analyzes current everyday behavior and attitudes towards cybersecurity at all levels of the enterprise, revealing how employees perceive different aspects of cybersecurity.

Assessment results can be used to recognize imbalances and areas for greater focus, justifying and aligning priorities in the internal and external activities of the Security Department, including awareness and training, internal PR, information sharing and business collaboration.

CyberSafety Culture includes the assessment of areas of knowledge, measured together, organization-wide. Assessment results form a basis for discussion of the role of cybersecurity in supporting business efficiencies:

- CyberSafety Mindset (perception of security & policies)
- Risk Management (guidance, feedback, improvements)
- Commitment (attitudes and behavior towards security)
- Business Impact (the balance between security and business efficiency)

Please note that Cybersafety Culture reporting is not an assessment of the maturity level of technical security in the enterprise, nor is it a measurement of the effectiveness of the Security Department.

The CyberSafety Culture report reveals how employees perceive cybersecurity, how they view the culture, habits, rituals and daily practice of cybersecurity, and their personal perception of different aspects of corporate security. This perception is engendered by diverse corporate practices and units, not just security or risk management departmental activity.

Kaspersky Security Awareness training programs:

New approach — proven effectiveness

More than
30x
ROI in security awareness

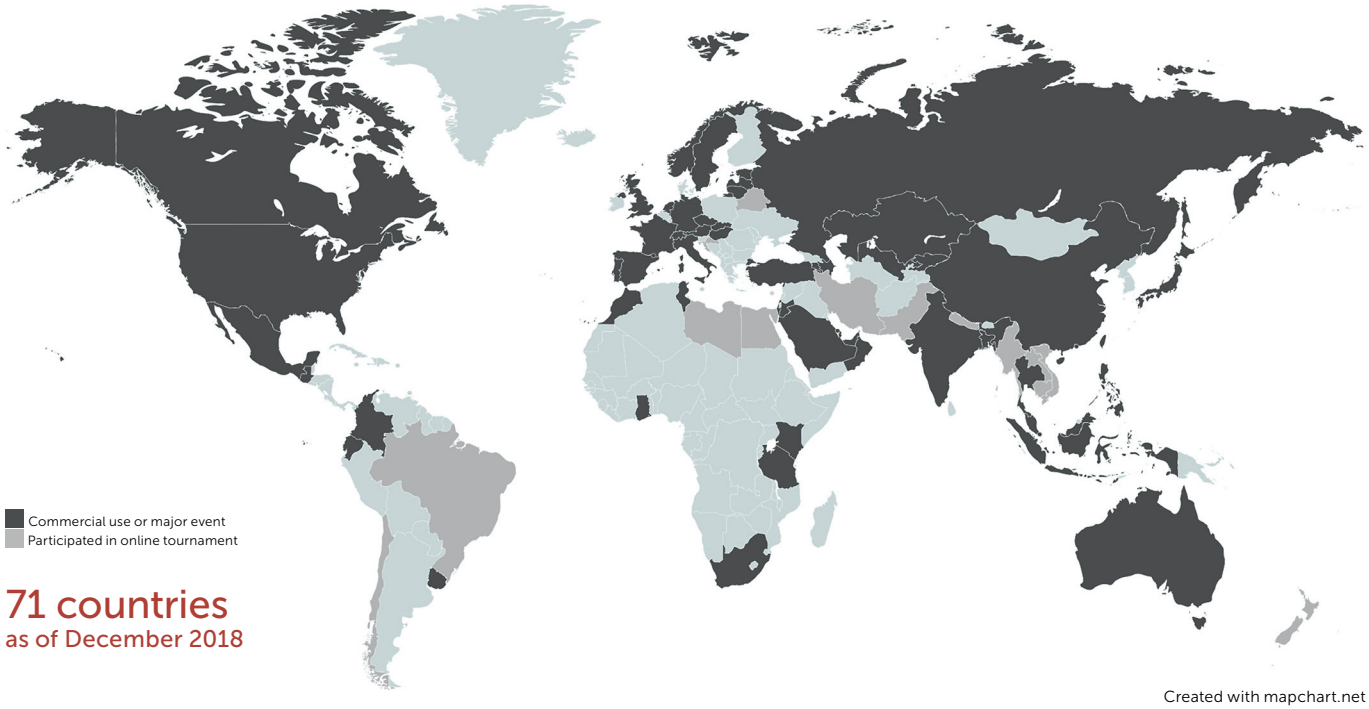
Up to
90%
Reduction in the total number of incidents

Minimum of
50%
Reduction in the financial impact of incidents

Up to
93%
Probability that knowledge will be applied in everyday work

An amazing
86%
Of participants willing to recommend the experience

Kaspersky Security Awareness Worldwide



71 countries
as of December 2018

Created with mapchart.net

www.kaspersky.com

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Kaspersky Security Awareness: **www.kaspersky.com/awareness**
Product demo: **www.kaspersky.com/demo-sa**