Kaspersky Enterprise Cybersecurity

Kaspersky Security Awareness

Gamified training programs for all organizational levels

www.kaspersky.com
#truecybersecurity

An effective way of building cybersafety across an organization

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

Inadvertent employees' errors are responsible for the most of cybersecurity incidents in organizations today:

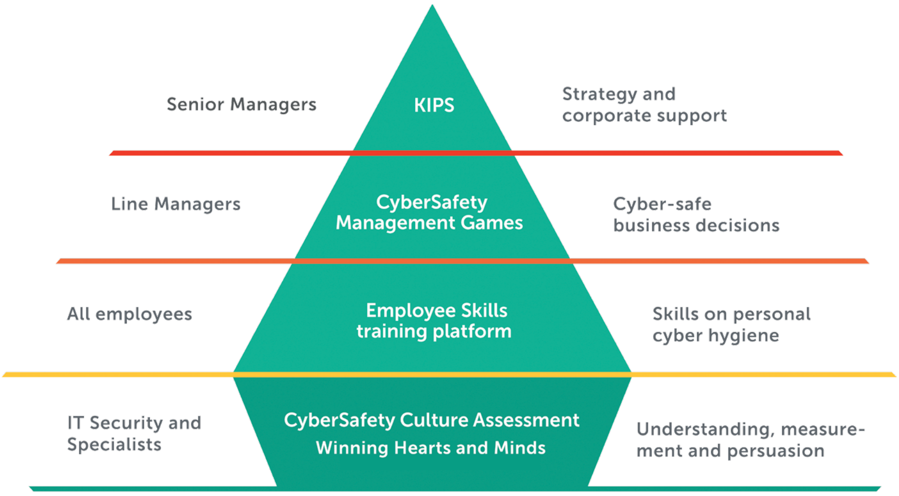
- IBM reported in 2015, that the percentage of the internal **breaches caused by human errors exceeds 95%**[1];
- **75% of the U.K. large organizations** and 31% of small businesses **suffered staff related security breaches** in 2015[2];
- **Average financial impact** of an incident involving careless actions of employees is **$865,000 per breach**[3];
- **Average cost of phishing attacks is up to $400 per employee per year** (other types of cyberthreats are excluded from this count)[4];
- Insurance from incidents caused by human errors, mistakes and negligence are reported to be **covered by only 25% of the cyber insurance plans** (while risks caused by external cyber criminals are covered by 84% of insurance plans, and risks from malicious or criminal insiders are reported to be covered in 75% of cases)[5].

Analysis has shown that the majority of existing Cyber Security Awareness training programs are ineffective:

- Reading policy documents and instructions is boring, too technical, too skeptical, i.e. full of treats and "Don't", without showing examples of safe behavior;
- People are not motivated to learn (only 22% believe they can be targeted by criminals);
- Employees do not see IT Security as partners and always try to bypass them;
- There is a lack of measurements on awareness, besides "how many people got trained".

Program Benefits and Advantages

Kaspersky Lab has launched a family of computer-based training products that utilize modern learning techniques and address all levels of the organizational structure. Our training program has already proved its effectiveness.


Senior Managers
KIPS
Strategy and corporate support
Line Managers
CyberSafety Management Games
Cyber-safe business decisions
All employees
Employee Skills training platform
Skills on personal cyber hygiene
IT Security and Specialists
CyberSafety Culture Assessment
Winning Hearts and Minds
Understanding, measurement and persuasion

Kaspersky Security Awareness portfolio is designed to ideally fit Enterprises objectives and preferences:

- **Builds behavior and doesn't just give knowledge:** the learning approach involves gamification, learning-by-doing, simulated attacks, etc. It results in strong behavioral patterns and produces a long-lasting effect;
- Creates **specific behavior for different organizational levels**: Senior managers, Line/ Middle managers, Average employees; considers their particular needs, time and format limitations;
- **Highly measurable and easy to manage** due to its computer-based nature. Can be administered by IT Security or HR teams. Kaspersky Lab provides proven implementation methodology, best practices and methodical and technical support;
- Based on immense **Kaspersky Lab cybersecurity grounds and R&D power**.

[1] IBM 2015 Cyber Security Intelligence Index.

[2] 2015 Information Security Breaches Survey. HM Government in association with InfoSecurity Europe and PwC.

[3] "Business Perception of IT Security: In The Face of an Inevitable Compromise", Kaspersky Lab, 2016.

[4] Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.

[5] 2015 Global Cyber Impact Report. Ponemon Institute LLC.

KIPS Training to Create a Strategic Support

KIPS training is targeted at business system experts, IT people and line managers, and increases their awareness of the risks and security problems of running modern computerized systems.

Kaspersky Interactive Protection Simulation (KIPS) is an exercise that places teams into a simulated business environment facing a series of unexpected cyber-threats, while trying to maximize profit and maintain confidence. The idea is to build a cyber defense strategy by making choices from amongst the best pro-active and re-active controls available.

Every reaction made by the teams to the unfolding events changes the way the scenario plays out, and ultimately how much profit the company makes… or fails to make. Balancing engineering, business, and security priorities against the cost of a realistic cyber-attack, the teams analyze data and make strategic decisions based on uncertain information and limited resources. If that sounds realistic, it should do, because each of the scenarios is based on real-life events.

KIPS is a dynamic awareness program based on “learning by doing”:

- Fun, engaging and fast (2 hours)
- Team-work builds co-operation
- Competition fosters initiative & analysis skills
- Gameplay develops understanding of cybersecurity measures

> **“What does emerge from the exercise, though, is that some of the first and most basic strategic decisions you take, such as security audits and training, password changes and patch management, will help enormously with the incident responses you may have to make later on.”**
>
> Mark Jenkins · December 16, 2015 · ICT Qatar

Scenarios available (all exist as KIPS Live and KIPS Online; 10 languages are supported)

Corporation	Protecting the enterprise from Ransomware, APTs, automation security flaws.
Bank	Protecting the financial institutions from high-profile APTs, attacking their ATMs, management servers and business systems.
e-Government	Protecting the public web servers from attacks and exploits.
Industrial	Protecting Industrial Control Systems and critical infrastructure.

Each scenario focuses on the respective threat vectors, allows discovering and analyzing the typical mistakes in building the cybersecurity and incident response procedures in the corresponding industry.

Cybersafety Management Games to Ensure Cybersafe Business Decisions

This highly interactive workshop (combination of computer-based and instructor-led) motivates line managers on the importance of cybersecurity for their jobs and provides managers with competence, knowledge and attitudes essential to maintain secure working environment in their divisions.

Organizations are taking steps to address cyberthreats by setting up IT security structures and training compliance. But is this enough?

- Does knowledge gained at training really drive employees' behavior? Or is it something else?
- Does business efficiency have to be sacrificed to achieve security?
- Do security officers feel that there are too few of them to reach every ear in their fight for cyber safety?

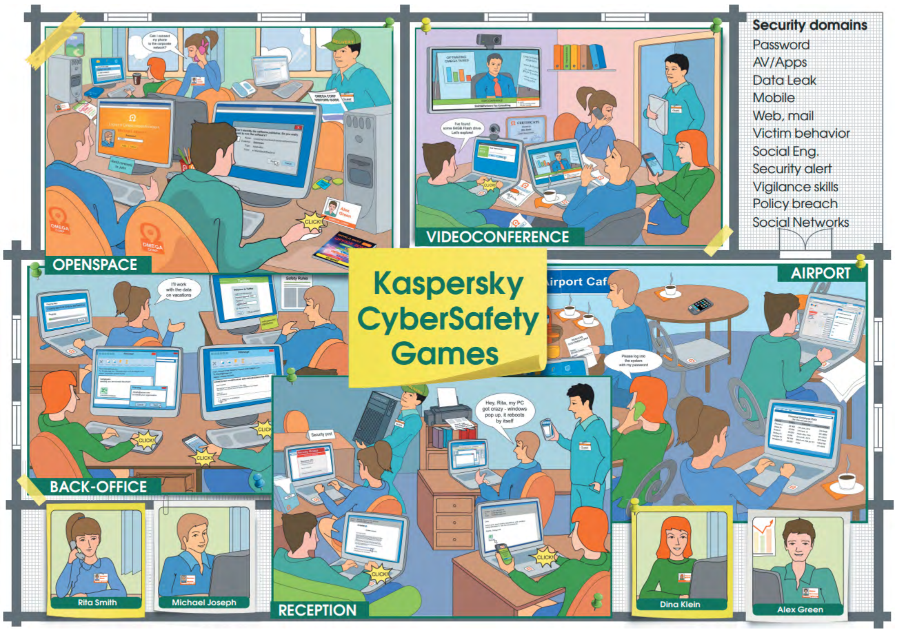
These challenges can only be addressed by engaging **line managers in making organizations cyber secure, without sacrificing efficiency. Only they** interact with employees on a daily basis and make business decisions. The answer lies in making cyber-safety the mandatory ingredient of everyday decision-making.

Kaspersky CyberSafety Management Games provide managers with **competence, knowledge and attitudes** essential to maintain secure working environment in their divisions:

- **Understanding:** Inner adoption of cybersecurity measures as an important yet uncomplicated set of actions
- **Monitoring:** Seeing everyday working process through the cybersafety lens
- **Cyber-Safe Decision Making:** Cybersecurity considerations as an integral part of business processes
- **Reinforcement and Inspiration:** Influential leadership and helpful advice to employees

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

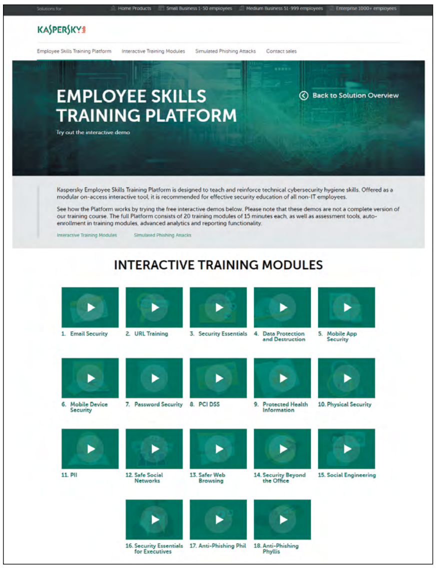
- Ease of delivery – awareness trainers do not have to be security experts;
- Ease of scheduling – modular short training sessions can be run at convenience of employee's schedule.



The platform is available in 27 languages as for February 2017.

Using the platform, and based on the Best Practice Guide from Kaspersky Lab, customers will be able to establish and implement a powerful, continuous and measurable cybersecurity education plan, running employees from simple to complicated lessons, and varying security domains to train according to the threat landscape and people skills.

Check www.kaspersky.com/demo-sa for our interactive demo!


Solutions for:
Home Products
Small Business 1-50 employees
Medium Business 51-999 employees
Enterprise 1000+ employees
KASPERSKY lab
Employee Skills Training Platform
Interactive Training Modules
Simulated Phishing Attacks
Contact sales
Back to Solution Overview

EMPLOYEE SKILLS TRAINING PLATFORM

Try out the interactive demo

Kaspersky Employee Skills Training Platform is designed to teach and reinforce technical cybersecurity hygiene skills. Offered as a modular on-access interactive tool, it is recommended for effective security education of all non-IT employees.

See how the Platform works by trying the free interactive demos below. Please note that these demos are not a complete version of our training course. The full Platform consists of 20 training modules of 15 minutes each, as well as assessment tools, auto-enrollment in training modules, advanced analytics and reporting functionality.

Interactive Training Modules   Simulated Phishing Attacks

INTERACTIVE TRAINING MODULES

1. Email Security
2. URL Training
3. Security Essentials
4. Data Protection and Destruction
5. Mobile App Security
6. Mobile Device Security
7. Password Security
8. PCI DSS
9. Protected Health Information
10. Physical Security
11. PII
12. Safe Social Networks
13. Safer Web Browsing
14. Security Beyond the Office
15. Social Engineering
16. Security Essentials for Executives
17. Anti-Phishing Phil
18. Anti-Phishing Phyllis

Employee Skills Training Platform to Build Cyber Hygience Skills

It is important to build on the skills and knowledge so access to an online skills platform is essential to work through typical scenarios and situations and gain greater knowledge and understanding of the potential threats and how to deal with them. Online learning allows employees to practice and learn through an interactive learning portal.

Interactive Training Modules

- Fun and short
- Based on exercises with a knock-on effect
- Auto-enrollment reinforces skills
- 20+ modules covering all security domains

Knowledge Assessment

- Includes predefined or random assessments, customer-defined questions, and customizable length
- Covers various security domains
- Vast questions library and randomization exclude cheating

Simulated Phishing Attacks

- 3 types of phishing attacks of various difficulty, all based on real-life cases
- Teachable moments appear every time employees open phishing emails
- Customizable templates
- Auto-assignment in training modules for those who failed the simulated attack

Reporting & Analytics

- Provides statistics for the organization as a whole or by department, location, position, as well as on individual level
- Monitors employees’ level of skills and its dynamics
- Supports data export to a number of formats or to customer’s LMS

Focus

Assessment looks at security culture from different perspectives:

- Organizational (managerial) level
- Personal (Employee) level
- Expertise available
- Security Assurance as a process

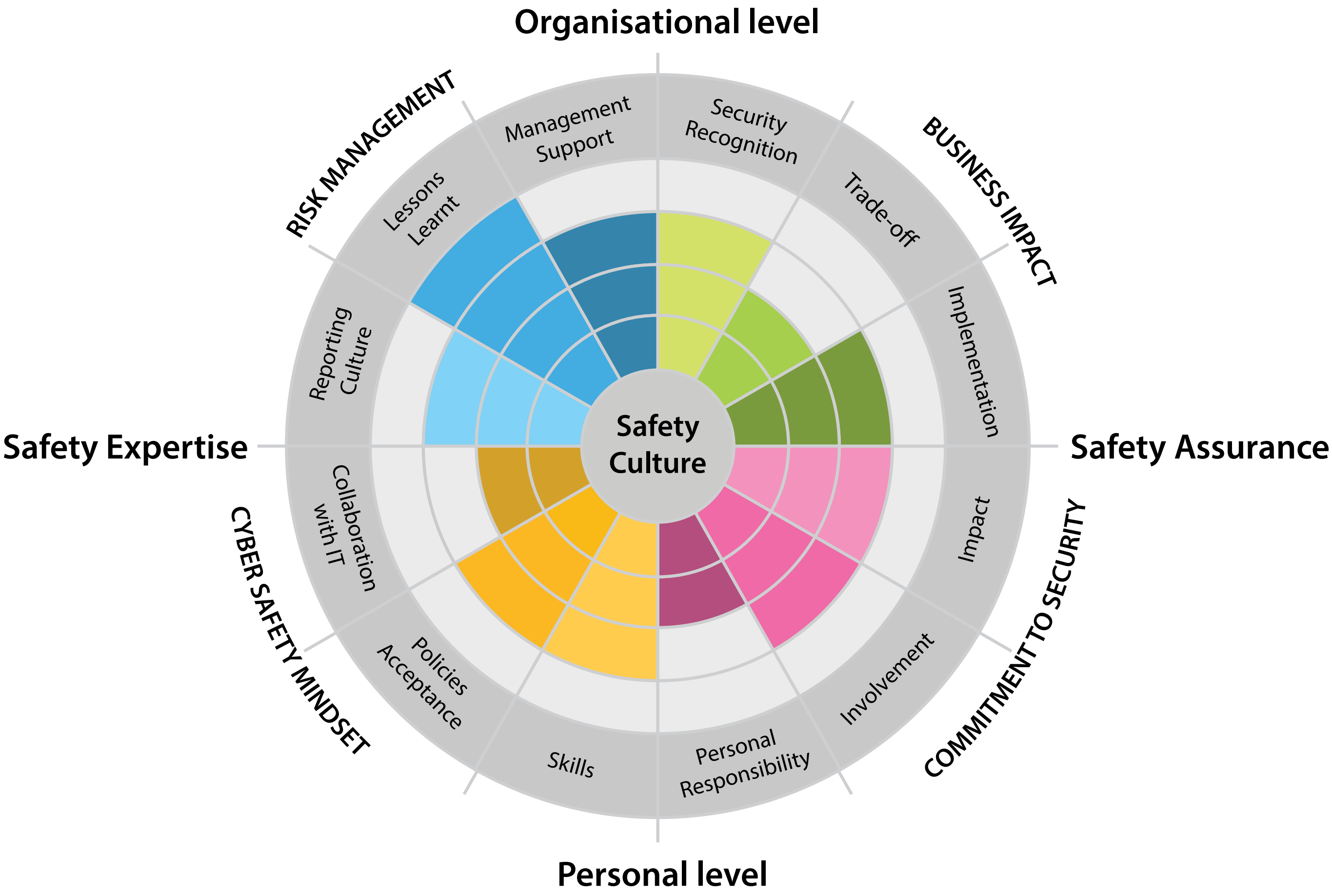
CyberSafety Culture Assessment

CyberSafety Culture Assessment analyses actual everyday behavior and attitude toward the cybersecurity at all levels of the enterprise, showing how employees in your organization perceive different aspects of cybersecurity.

Assessment results can be used to understand the misbalances and areas to focus on, to justify and align priorities in the internal and external activities of the Security department, including awareness and trainings, internal PR and information sharing, collaboration principles while working with business.

CyberSafety Culture includes domains, which will be assessed and measured altogether, organization-wide. The assessment results are the basis for discussion of the role and place of cybersecurity in supporting the business efficiencies:

- CyberSafety Mindset (perception of security & policies),
- Risk Management (guidance, feedback, improvements),
- Commitment (people’s attitude and behavior on security),
- Business Impact (the balances between security and business efficiency).



Please note that cybersafety culture report is not an assessment of the technical security maturity level of the enterprise, nor is it a measurement effectiveness of the security department.

The CyberSafety Culture report shows how average employees see / feel cybersecurity in their minds; what do they think about the culture, habits, rituals, daily practice for cybersecurity related aspects; what is their personal perception of different aspects of the culture of making the company secured from the cyber threats. Such perception results from various company practices and units, not just a result of security or risk management department activity.

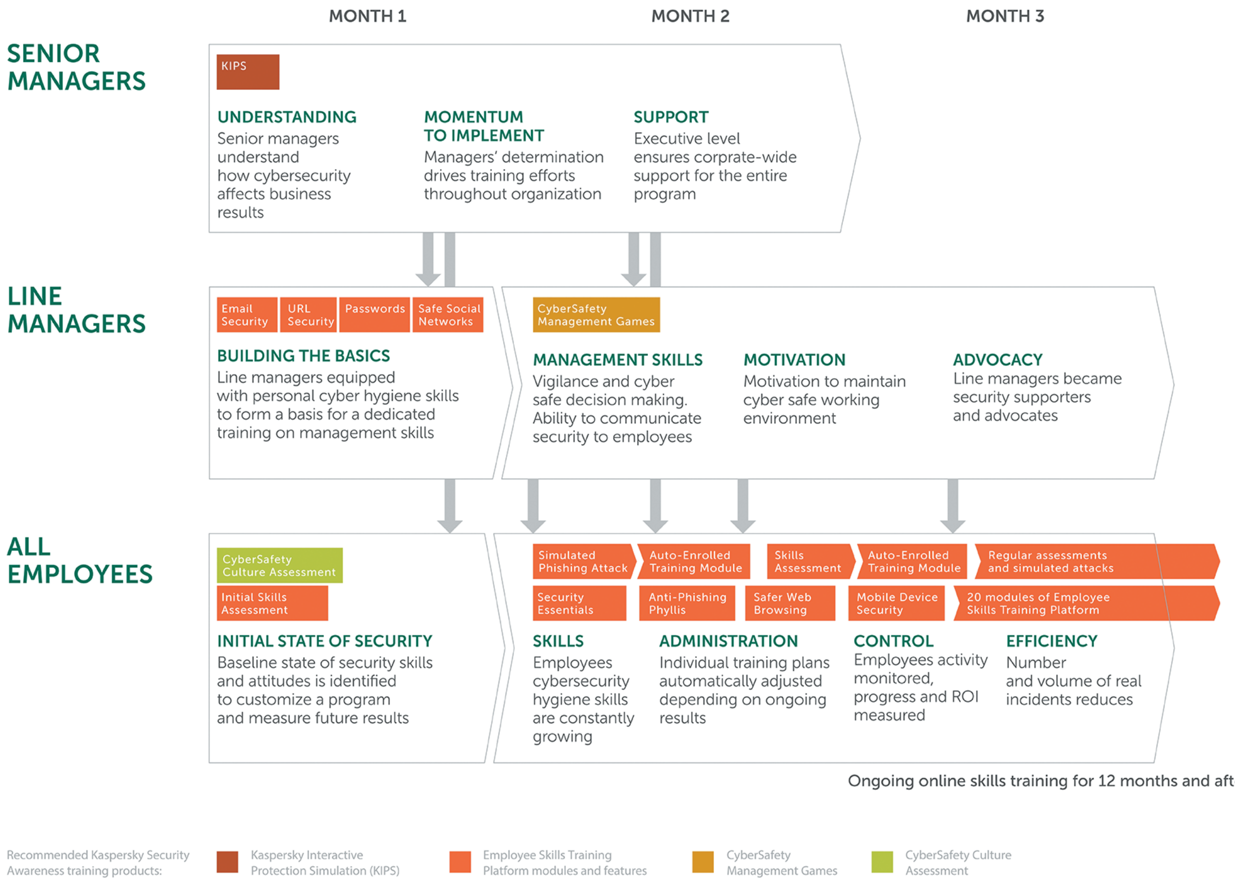
The Assessment is performed as a cloud-based survey. It takes about 15 minutes to complete for an employee, average 2 weeks to run the survey though all employees.

After the survey the customer receives a consolidated report.

Implementation Methodology: Quick Launch and Cumulative Effect

Below is a recommended sequence of educating employees with Kaspersky Security Awareness Products (“Best Practice Guide” is also available to our customers). We provide detailed instructions and methodical support to customers, ensuring that our trainnig products are easy to implement and manage and deliver as much value as they potentially can.

Cumulative Effect – Each Training Supports the Others



MONTH 1 | MONTH 2 | MONTH 3

SENIOR MANAGERS

KIPS

UNDERSTANDING
Senior managers understand how cybersecurity affects business results

MOMENTUM TO IMPLEMENT
Managers’ determination drives training efforts throughout organization

SUPPORT
Executive level ensures corprate-wide support for the entire program

LINE MANAGERS

Email Security | URL Security | Passwords | Safe Social Networks

BUILDING THE BASICS
Line managers equipped with personal cyber hygiene skills to form a basis for a dedicated training on management skills

CyberSafety Management Games

MANAGEMENT SKILLS
Vigilance and cyber safe decision making. Ability to communicate security to employees

MOTIVATION
Motivation to maintain cyber safe working environment

ADVOCACY
Line managers became security supporters and advocates

ALL EMPLOYEES

CyberSafety Culture Assessment

Initial Skills Assessment

INITIAL STATE OF SECURITY
Baseline state of security skills and attitudes is identified to customize a program and measure future results

Simulated Phishing Attack | Auto-Enrolled Training Module | Skills Assessment | Auto-Enrolled Training Module | Regular assessments and simulated attacks

Security Essentials | Anti-Phishing Phyllis | Safer Web Browsing | Mobile Device Security | 20 modules of Employee Skills Training Platform

SKILLS
Employees cybersecurity hygiene skills are constantly growing

ADMINISTRATION
Individual training plans automatically adjusted depending on ongoing results

CONTROL
Employees activity monitored, progress and ROI measured

EFFICIENCY
Number and volume of real incidents reduces

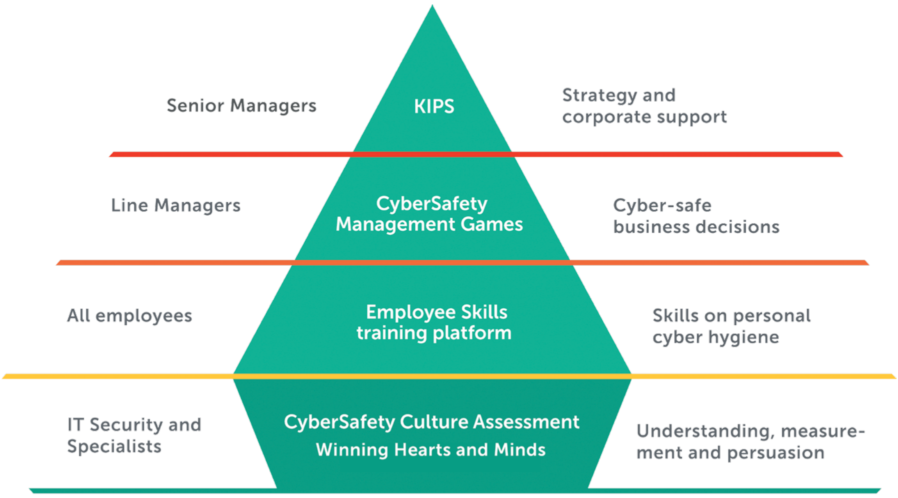
Ongoing online skills training for 12 months and after...

Recommended Kaspersky Security Awareness training products:

- 🟥 Kaspersky Interactive Protection Simulation (KIPS)
- 🟧 Employee Skills Training Platform modules and features
- 🟨 CyberSafety Management Games
- 🟩 CyberSafety Culture Assessment

Kaspersky Security Awareness Training Products

Interactive Protection Simulation training is a part of Kaspersky Security Awareness portfolio, based on CyberSafety Culture methodology. Cyber Safety Culture development by set of awareness trainings with gamification, for all levels of the organization structure, managed by Security and HR teams.


Senior Managers
KIPS
Strategy and corporate support
Line Managers
CyberSafety Management Games
Cyber-safe business decisions
All employees
Employee Skills training platform
Skills on personal cyber hygiene
IT Security and Specialists
CyberSafety Culture Assessment
Winning Hearts and Minds
Understanding, measurement and persuasion

Comprehensive But Simple and Straightforward

- Wide range of security issues
- Familiar environments
- Engaging training process
- Practical exercises
- Language suitable for non-IT people

Business Benefits

as much as
93%
probability of using the knowledge in the daily work

up to
90%
decrease the number of incidents

50-60%
reduce the cyber risk monetary volume

more than times
30x
provide ROI from investment into the Security Awareness

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**