KASPERSKY lab

Employee Skills Training Platform

www.kaspersky.com/demo-sa
#truecybersecurity

Employee Skills Training Platform

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 skills how to deal with them. Online learning allows candidates to practice and learn through an interactive learning portal.

Platform - is a part of Kaspersky Security Awareness training programs

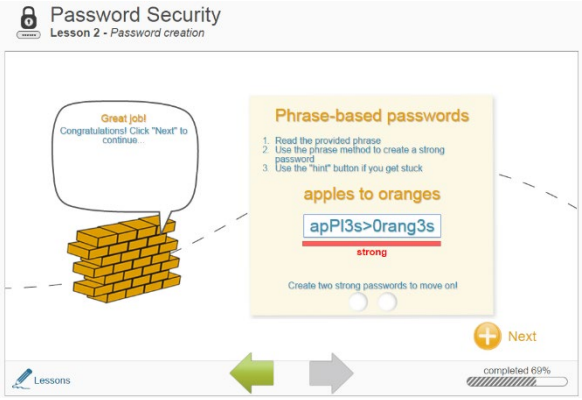
Easy and effective solution for cybersecurity

- **Setting objectives &choosing a program:** setting goals based on KL global data; comparison with world/ industry average
- **Learning management:** learning automation; self-adjusting learning path; calculation of time spends
- **Reporting & analytics:** actionable reports anytime; on-the-fly analysis of what can be improved
- **Program efficiency & appreciation:** true gamification competition & challenge; preventing overload

Key components of the Employee Skills Training

1. Interactive training modules:

- Fun and short
- Based on exercises with a knock-on effect
- Auto-enrollment reinforces specific skills
- 29[1] modules covering all areas of security



2. Knowledge Assessment

To determine the in-depth skills, knowledge and training needs of the user. Covers various security domains, includes predefined or random assessments, customer-defined questions, and customizable length.

3. Simulated phishing attacks

Ready-to-go customizable templates of phishing emails of various difficulty. When employees receive and click on the phishing, they get the teachable moment, and can be auto-assigned to the relevant training module.

4. Analytics & Reporting

Results by Campaign, Group, Device Type, Repeat Offender, Location

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

1 As of October 2017

Assess

Evaluate your employees' knowledge and your organization's susceptibility with our customizable assessments and simulated attacks, as well as Teachable Moments that provide tips and practical advice for employees who fall for mock phishing and USB attacks. These brief exercises explain the dangers of actual attacks and help motivate employees to participate in follow-up training.

Educate

Choose from a full menu of interactive training modules that are key to educating your employees about security threats in the workplace and beyond. These 10- to 15-minute modules help users understand potential risks and how to safeguard corporate and personal assets.

Our Auto-Enrollment feature allows automatically assign training to employees who fall for simulated phishing attacks and those users who don't exhibit a desired level of proficiency on predefined knowledge assessments.

Reinforce

Remind employees about best practices by bringing messaging into the workplace with Security Awareness Materials designed to reinforce your training and encourage knowledge retention. Share articles, display posters and images, and reward participants with security-minded gifts.

Measure

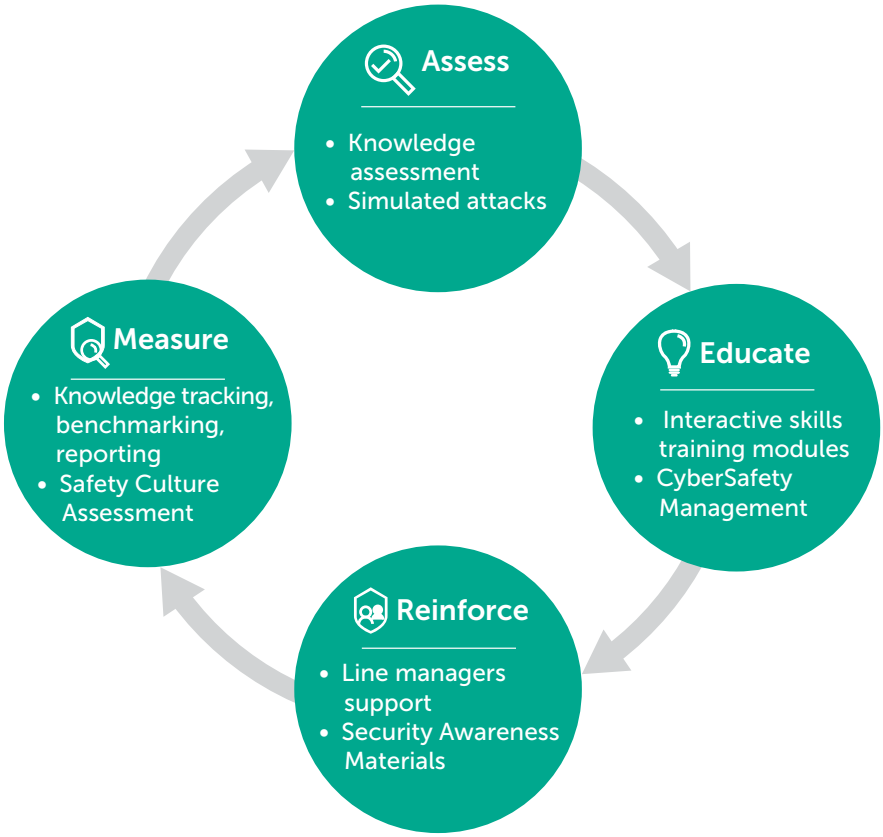
Gather powerful analytics about your organization's strengths and weaknesses, evaluate results, and plan future training accordingly prior to repeating the four-step cycle.

Methodology

Our customers have enjoyed benefits in many areas, including reduced successful phishing attacks (up to 90%), reduced malware infections (up to 95%), lower helpdesk call volumes, increased reporting of incidents by employees, and an overall improved security posture.

These results are achieved by implementing Continuous Security Training Methodology and cybersecurity education solutions. Our Continuous Security Training Methodology includes four key steps: Assess, Educate, Reinforce, and Measure.

These components can be used independently, but are most effective when combined, which delivers a 360-degree approach to security awareness and training. You can deliver these steps via our Security Education Platform, which is purpose-built for information security officers and enables seamless execution of your program.



With our solutions, security officers can easily implement, manage and monitor education campaigns, and measure success with comprehensive reporting capabilities. In the first steps of this methodology security officers use Knowledge assessment, to understand user's knowledge level and awareness materials to raise awareness of the program. Then they utilize simulated phishing attacks to assess user vulnerability to attack and motivate them to complete training. The resulting assessment data is used to prioritize critical training topics. Interactive software training modules on selected topics are then assigned and progress as well as completion is tracked. Auto-Enrollment feature will automatically assign respective interactive training modules to users who didn't gained the limit of correct answers. This user-centered approach can result in as much as a 90% training completion rate

1. Interactive Training Modules

- **The General Data Protection Regulation (GDPR)** – Employee will learn why the GDPR was developed by lawmakers; how the GDPR classifies personal data; what type of organization the GDPR applies to; what is considered a data breach; key data security and data privacy guidelines; four key areas to increase compliance and decrease risk: accountability; data mapping; detecting and reporting exposure; data erasure.
- **Introduction to phishing** – Provides a brief but instructive look at the best practices related to identifying and handling suspicious emails.
- **Avoiding dangerous links** – Gives users practical guidance on how to find out a URL's actual destination and examines common visual cues that can help users determine whether a website is legitimate or dangerous.
- **Avoiding dangerous attachments** – Helps users understand why they should treat any email attachment with a healthy suspicion, and how to handle these types of messages.
- **Data entry phishing** – Explains the dangers associated with malicious data entry forms and helps users understand why they should be wary of any email that includes a request for credentials or other sensitive information.
- **Email protection tools** – Learn how to protect yourself from phishing scams in combination with email defense tools.
- **Email security on mobile devices** – Identify and avoid phishing emails on mobile devices
- **Spear phishing threats** – Recognize and avoid targeted phishing attacks.
- **Security Essentials** – Training on the basics of the cybersecurity. User will learn the most common threats and mistakes in the daily life.
- **Security Essentials for Executives** – Recognize and avoid threats encountered by senior manager at work and at home.
- **URL Training** – Employees learn how to examine a URL, understand the origin of the link, and identify fraudulent or malicious URLs in this interactive game.
- **Email Security** – Users learn to spot phishing traps in emails and recognize fake links, attachments and information in this interactive game.
- **Anti-Phishing Phil** – In this character-based game, employees learn how to examine a URL, understand the origin of the link, and identify fraudulent or malicious URLs.
- **Anti-Phishing Phyllis** – In this character-based game, users learn to spot phishing traps in emails and recognize fake links, attachments and information.
- **Password Security** – Users are given tips and tricks to create stronger passwords, to use a password family to aid in password recall and to safely store passwords.
- **Safe Social Networks** – Educate your users about types of "impostors" that can be found online, implications of very public social networks, and how to spot scam messages on social networks.
- **Protecting Against Ransomware** – Brief training module on how to recognize and prevent ransomware attacks.
- **Mobile Device Security** – Teach users how to secure their smartphone from theft, create PINs, keep communications private, and avoid dangerous apps.
- **Mobile App Security** – Learn how to research app components and the implications of dangerous permissions, which can help them judge the reliability and safety of mobile applications prior to downloading.
- **USB Device Safety** – An often-overlooked threat – end users need to be aware of the risks associated with flash drives and other IoT items powered via USB ports.
- **Physical Security** – Learn how to prevent and correct physical security breaches, and get the best practices that will help keep people, areas and assets secure
- **Security Beyond the Office** – Educate employees about using free Wi-Fi safely, risks of using public computers, and safeguards for company equipment and information at home and on the road.
- **Safer Web Browsing** – Users will learn the difference between browser content and website content, how to avoid malicious virus pop-ups, the importance of logging out of web sites, form auto-complete risks, and how to spot other common website scams.
- **Social Engineering** – Employees will learn to recognize common social engineering tactics and practical tactics to avoid attacks and get insight into how social engineers think.

- **Personally Identifiable Information (PII)** – Educate employees about the different types of PII, guidelines for identifying, collecting, and handling PII, actions to take in the event of a PII breach and tips and techniques for improving overall PII security.
- **Payment Card Information Data Security Standard (PCI DSS)** – Users will learn to understand PCI-DSS requirements, identify PCI-DSS compliance, manage records and accounts as well as to recognize and act upon security breaches.
- **Data Protection and Destruction** – Teach everyone about the different types of portable electronic devices and removable storage media, the pros and cons associated, best practices for securing these devices and securely disposing of data.
- **Protected Health Information (PHI)** – (U.S. only) Interactive training to educate employees why and how they should safeguard PHI to meet HIPAA, HITECH and Omnibus compliance regulations including best practices for using, disclosing, transmitting and storing PHI.
- **Travel Security** – Explore how to keep data and devices safe when working in airports, in hotels, at conferences, and in other public spaces.

2. Knowledge Assessment

Ideal for early and ongoing assessment exercises including:

- establishing a baseline measurement of employees' understanding of critical cybersecurity topics (including phishing);
- assessing beyond the phish to evaluate vulnerabilities related to mobile devices and mobile apps, data management, physical security, and more;
- identifying areas of susceptibility from the organizational level down to the individual level;
- tracking progress and targeting existing and emerging areas of concern.
- We have 2 types of predefined assessments: covering certain areas of cybersecurity and broad assessments. Above this there is a possibility:
- to build your own assessments using our library of questions
- to create your own questions, define new categories and use them into assessments

Auto-enrollment feature for automatically assignment of appropriate models for those who failed the assessment.

3. Simulated Phishing Attacks

Allows you to create groups, design a simulated phishing email, and send it directly to your users. Should users click on the simulated phishing link, download an attachment or enter information into a landing page, they will receive a "just-in-time" training message. Everyone who falls for t attack will experience a "teachable moment" during which the employee is humbled by what could have been a critical mistake and therefore making them more receptive to follow-on training.

Simulated phishing attack tool:

- Up-to-date template library of phishing emails
- Huge list of fake phishing domains
- Library of Teachable moment (landing pages for users who failed the attack)
- Easy creation of phishing campaign
- Phishing emails and teachable moments are fully customizable
- Comprehensive scheduling of the campaign
- Detailed reporting for cyber security specialists and management that could be exported for separate usage
- Auto-enrollment feature

4. Analytics & Reporting

While employees are being trained, the platform is simultaneously collecting and tracking key metrics. Platform captures each employee's interaction with training modules, mock attacks, and knowledge assessments. Security officers will instantly have detailed information not only about who completed which assignments, but also in which concepts they are strong or weak, and how they have improved over time.

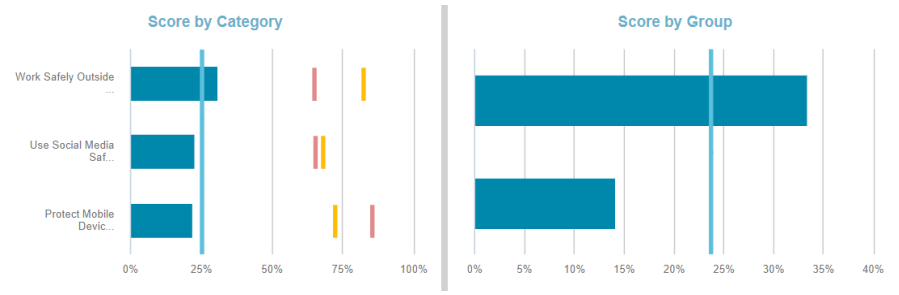
All user data can be characterized, filtered and reported using administrator-defined fields including job function, location, department, hire date, etc.

The Knowledge Assessment report includes industry benchmark data to better understand how users are performing against others in their industry. This report enables customers to better understand organizational risk and where to focus training efforts by knowing how employees' cybersecurity awareness knowledge compares to that of other end users in their industry and around the world.

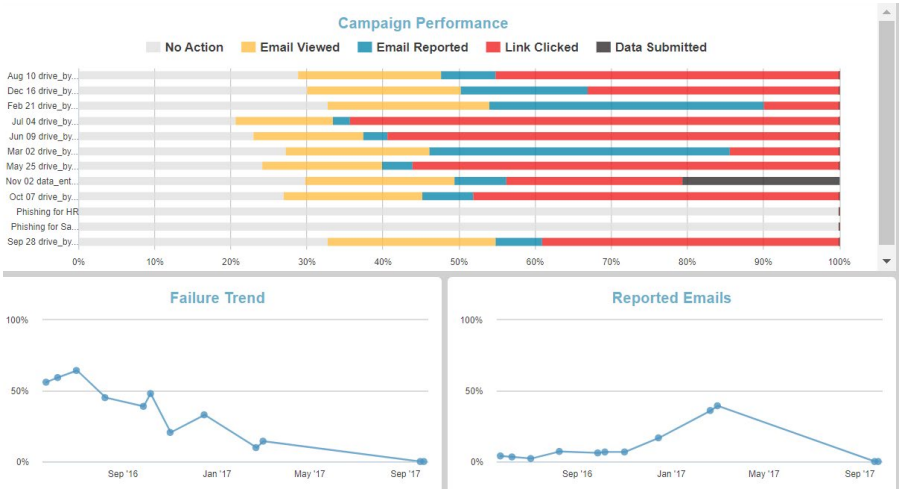
Phishing simulation report allows to compare personal data with the average failure rate among all clients

Compare your performance to benchmark reports

The Knowledge Assessment report includes industry benchmark data to better understand how users are performing against others in their industry.



Track Awareness Program progress



Reports can be generated in CSV, Word, Excel or PDF formats that Administrators can easily modify, pivot or filter to support their desired business analytics.

Languages supported

Kaspersky Employee Skills Training Platform supports a consistent set of 28[2] languages across all training modules (except for the PHI module, which is only available in American English).

Arabic, Bulgarian, Chinese (simplified & traditional), Czech, Danish, Dutch, English (UK & US), Finnish, French (France & Canada), German, Hebrew, Hindi, Hungarian, Icelandic, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Russian, Slovak, Spanish (Spain & Latin America), Swedish, Thai, Turkish, Vietnamese.

A note about translations: Bulgarian, Czech, Danish, Finish, Icelandic, Hebrew, Hindi, Norwegian, Polish, Slovak, Thai, Vietnamese are available on a limited selection of modules.

Available configurations

Implementation options

Configuration / features included	Anti-Phishing	Multi-Topic	**Full**	Training Modules only
Individual modules / lessons	3	All (20+)	**All**	All
Simulated phishing attacks	Yes	Yes	**Yes**	-
Training Auto-enrollment after Phishing attacks/Assessments	Yes	Yes	**Yes**	-
Manual Training Assignments	-	Yes	**Yes**	*)
CyberStrength knowledge assessment	-	-	**Yes**	-
Detailed reports	Yes	Yes	**Yes**	*)
Delivery form	Cloud	Cloud	**Cloud**	On-premises**)
Content updates delivery	Immediate	Immediate	**Immediate**	Annually
Minimum number of users	250+	150+	**50, 100+**	250+
Recommended to use when	Phishing and Knowledge assessment features are critical, cloud data storage security measures provided by Kaspersky Lab are satisfactory.			In-house data storage is a must.

* Availability to implement and exact functionality depends on the functionality of LMS.

** Delivery requires customers to have an LMS compatible with SCORM 1.2 specifications. Most of modern LMSs are compatible.

2 As of October 2017

Try out Platform demo !

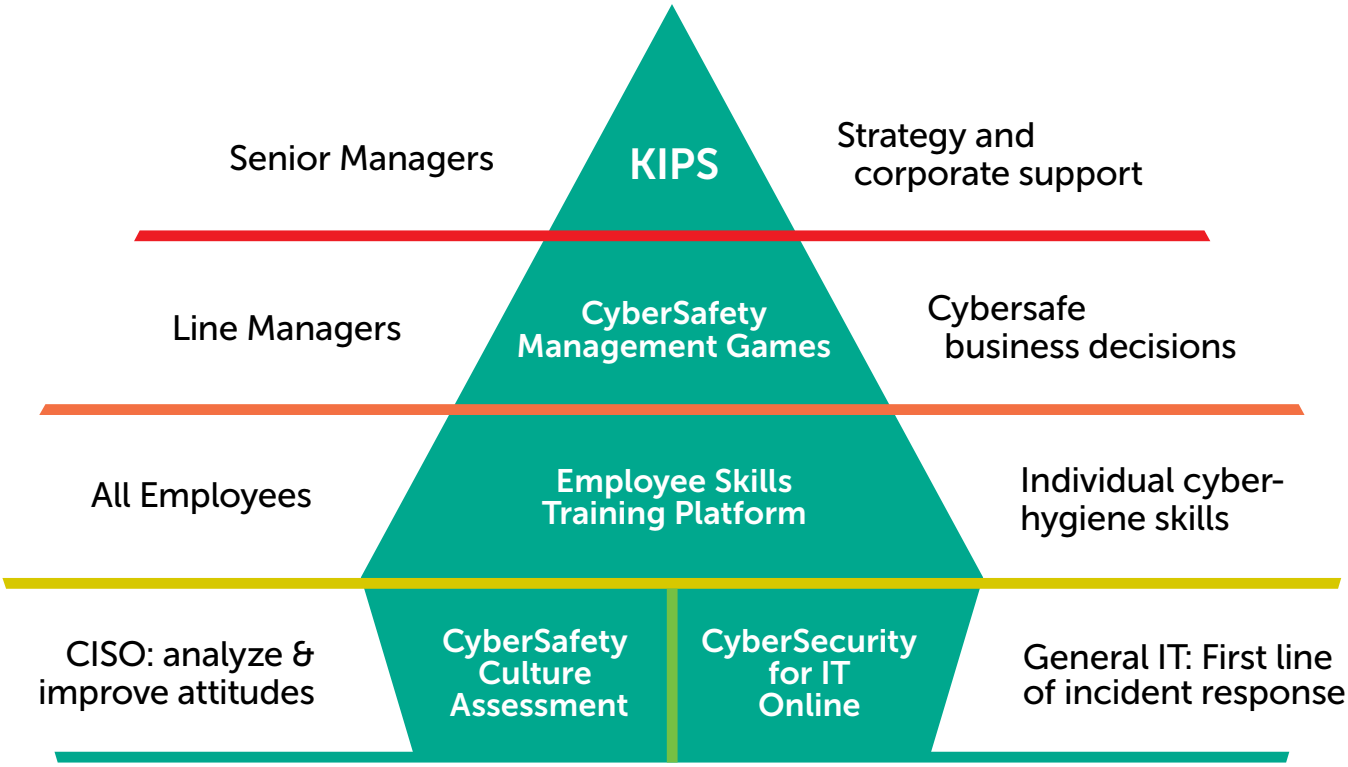
www.kaspersky.com/demo-sa

Free interactive demo of training modules and simulated phishing attacks (available on local websites as well)

Contact your local Kaspersky Lab office or our partners for more information (including administrative features' demo, pricing, etc.)

Kaspersky® Security Awareness

Kaspersky Lab has launched a family of computer-based training products that utilize modern learning techniques and address all levels of organizational structure. This approach helps create collaborative CyberSafety Culture which ensures a self-sustained state of cybersecurity throughout the organization.



Setting objectives & choosing a program

Setting goals based on KL global data

Comparison with world/ industry average

Learning management

Learning automation

Self-adjusting learning path

Calculation of time spends

Reporting & analytics

Actionable reports anytime

On-the-fly analysis of what can be improved

Program efficiency & appreciation

True gamification

Competition & challenge

Preventing overload

up to
90%
Reduction in the total number of incidents

not less than
50%
Reduction in the financial impact of incidents

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

more than
30x
ROI from investment in security

amazing
86
Of participants willing to recommend the experience

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**