KASPERSKY lab

EMPLOYEE SKILLS TRAINING PLATFORM

www.kaspersky.com/demo-sa

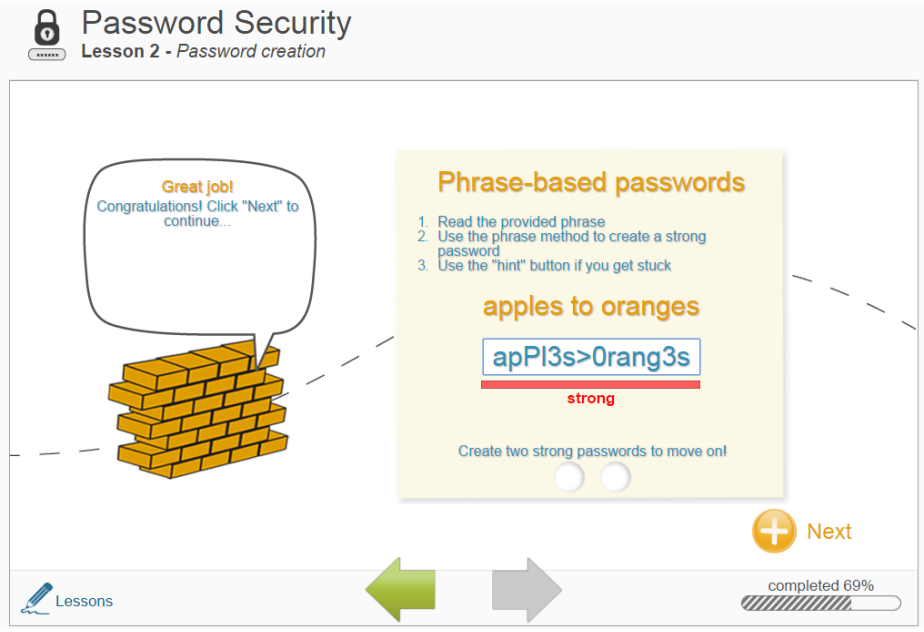
KASPERSKY LAB PRESENTS ITS EMPLOYEE SKILLS TRAINING PLATFORM, DEVELOPED IN PARTNERSHIP WITH WOMBAT SECURITY TECHNOLOGIES AND BUILT ON WOMBAT'S AWARD-WINNING TRAINING SOFTWARE.

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 candidates to practice and learn through an interactive learning portal.

Key aspects of the Employee Skills Training

- **Online Training Modules**: Security Essentials and Security Essentials for Executives, Anti-Phishing, Data Protection and Destruction, Email Security, Safe Social Networks, Physical Security, Mobile App Security, Mobile Devices Security, Safer Web Browsing, Security Beyond the Office, Social Engineering, URL Training, Passwords, Personally Identifiable Information (PII), Protected Health Information (PHI), Safe Online Payments (PCI DSS), Protecting Against Ransomware, USB Device Safety, Travel Security.
- **Skills Assessment**: To determine the in-depth skills and training needs of the user. Covers various security domains, includes predefined or random assessments, customer-defined questions, and customizable length,
- **Simulated attacks**: Ready-to-go customizable templates of phishing emails of various difficulty. When Employee receives and clicks on the phishing, he gets the teachable moment, and can be auto-assigned to the relevant training module,
- **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.

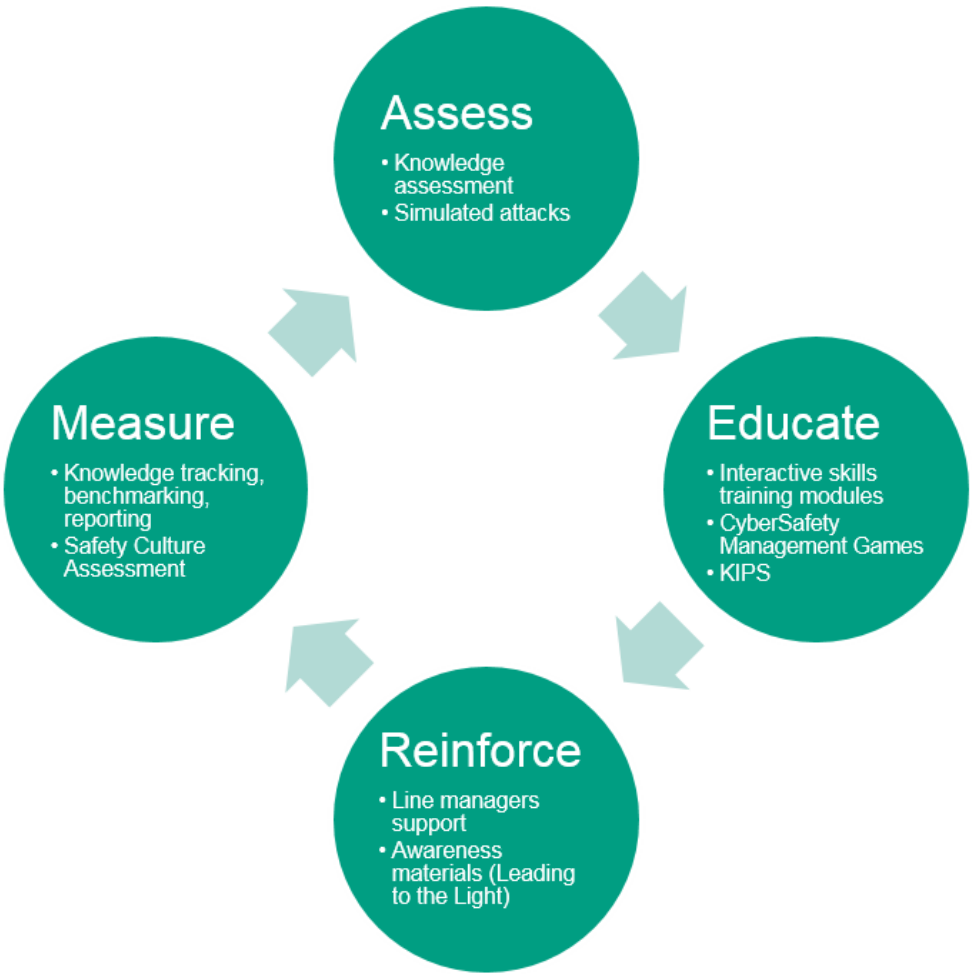


Methodology

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



- **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, smishing, 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 you to 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 CyberStrength® 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.

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 **CyberStrength®**, our knowledge assessment, to understand user knowledge and awareness materials to raise awareness of the program. Then they utilize simulated 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 and completion is tracked.

Our unique **Auto-Enrollment** feature can be used to assign interactive training modules to CyberStrength users as well as every user who falls for a simulated attack. This user-centered approach can result in as much as a 90% training completion rate.

Assessments

- **Phishing Attacks** allows you to create groups, design a simulated phishing email, and send it directly to your users. Should a user click on the simulated phishing link, download an attachment or enter information into a landing page, he/she will receive a "just-in-time" training message. Everyone who falls for the 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.
- **CyberStrength** allows you to create customized knowledge assessments to test end user knowledge of cybersecurity topics.

Interactive Training Modules

- **Security Essentials** – Training on the basics of the cybersecurity. User will learn the most common threats and mistakes in the daily life.
- **Security Essentials: Executive** – 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.

Languages supported

العَرَبِية
čeština
Deutsch
English(UK)
English(US)
español
Español
français
français
עִבְרִית
Magyar
Íslenska
italiano
日本語
한국어
Nederlands
Norsk
polski
português
русский
Slovák
svenska
ภาษาไทย
Türkçe
tiếng Việt
简体中文
繁體中文

Available configurations

Our recommendations on choosing the configuration are (the below table shows the detailed comparison of the configurations):

1. Anti-Phishing Suite – If you are primarily focused on reducing phishing/malware attacks;
2. Multi-topic Suite – If you see phishing as important, but also are interested in training across other areas – mobile device/app, data protection, PII/PCI, physical security, passwords, and you know already which of those areas are most weak/important;
3. Full platform – All of the above + also you want to be able to assess/understand what the other risk areas are so you can target and prioritize your training efforts.

	Anti-Phishing	Multi-topic	Full
Simulated phishing attacks	Yes	Yes	Yes
Auto-enrolment of training modules	Yes	Yes	Yes
Manual Module Assignments	-	Yes	Yes
CyberStrength (knowledge assessment tests)	-	-	Yes
Training modules included	3	All*	All*
Language support	Full	Full	Full
License term	1 year	1 year	1 year

* All modules means all currently and all then-available modules

Proof of Concept

For evaluation purposes, and for a separate fee, Kaspersky Lab will manage a 30-day Anti-Phishing Assessment and Training Cycle using mock phishing attack service, URL training module and Email Security training module. This project is comprised of 3 steps:

Step 1: Assess Susceptibility to Attack

Kaspersky Lab will deliver a simulated phishing attack campaign to establish a realistic baseline of your organization's vulnerability against attack using our PhishGuru service. In addition to determining vulnerability, employees who fall for these attacks will experience a teachable moment where they are instructed how to avoid future vulnerability.

Step 2: Assign Anti-Phishing Training Modules

Kaspersky Lab will assign training modules to users who failed initial simulated attacks, including our URL Training module and Email Security training module. The assignment will be sent via email to users who fell for the simulated phishing attack, giving them 30 days to take the training modules.

Step 3: Re-Assess Vulnerability

At the end of the 30-day period, Kaspersky Lab will deliver a second simulated phishing attack campaign to the entire group of users including in the initial attack in #1 above. The results from the two campaigns will be analyzed and a final report provided to the customer.

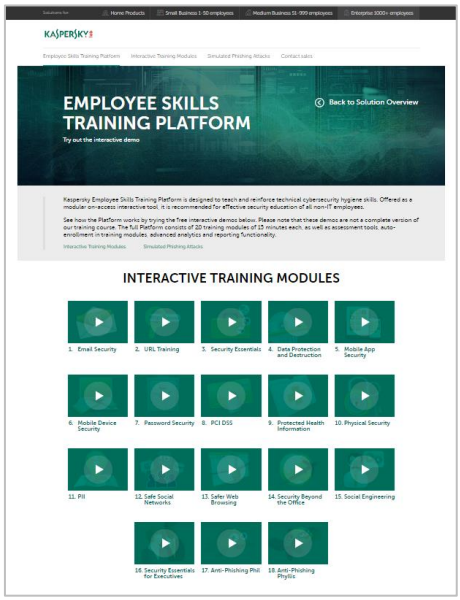
Customer Responsibility

Customer will appoint a project lead who will be the primary point of contact for the Kaspersky Managed Services project manager. The point of contact will provide Kaspersky Lab information and assistance needed to complete the POC.

Deliverables

We will provide a final report showing the vulnerability and the improvement.

Try out Platform demo!



www.kaspersky.com /demo-sa

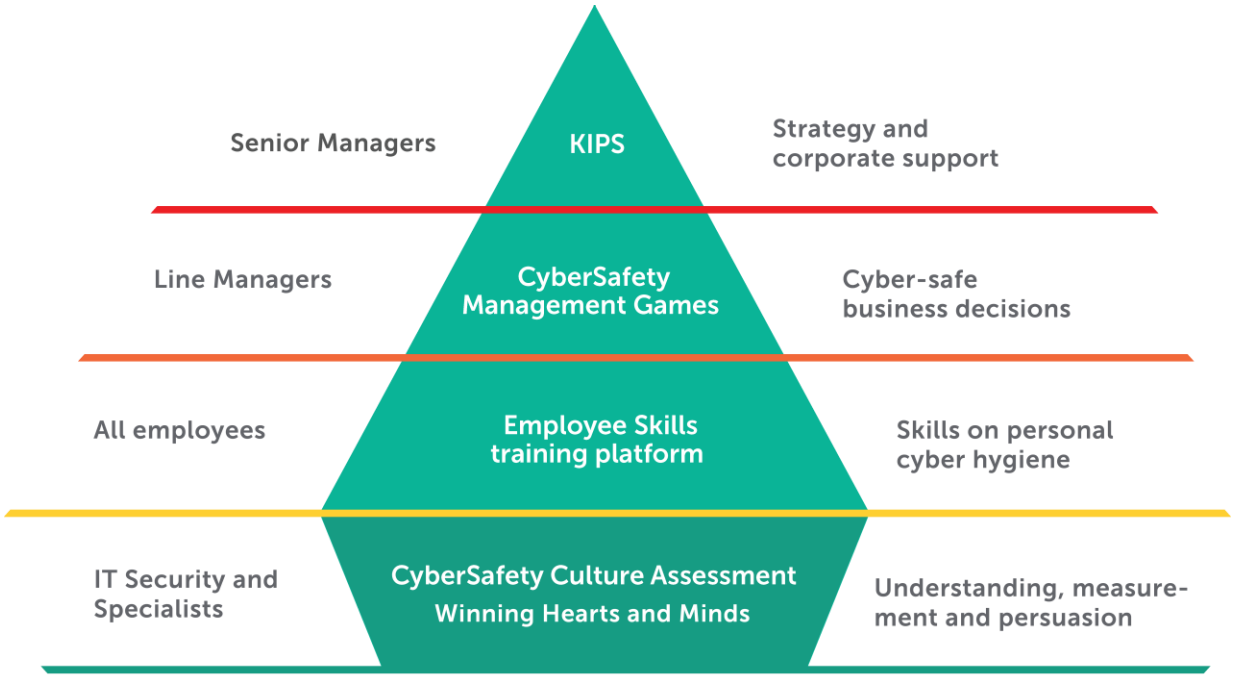
Try our free interactive demo of training modules and simulated phishing attacks.

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

Kaspersky Security Awareness Training Products

Employee Skills training platform is a part of Kaspersky Security Awareness portfolio, based on CyberSafety Culture methodology. CyberSafety Culture is a set of values and attitudes that drives people's behavior, on an individual or corporate level.

We help customers develop a CyberSafety Culture, under the management of their security and HR teams, through a set of awareness training programs. The training programs utilize gamification and address all levels in the organization structure.



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
- Decrease the number of incidents by up to 90%
- Reduce the cyber risk monetary volume by 50-60%
- Translate the cybersecurity from IT-jargon to business language, and get business management involvement
- Get measurable cybersecurity awareness program results
- Provide ROI from investment into the Security Awareness more than 30x times