Kaspersky Security Awareness

Computer-based training programs for all organizational levels

2019

kaspersky

Learn more on
kaspersky.com/awareness

The effective way to build 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 generally fail to inspire and motivate the desired behavior.

People are the weakest link in the cybersecurity chain:

52% **of companies** regard employees as the biggest threat to corporate cybersecurity*

60% **of employees** have confidential data on their corporate device (financial data, email database, etc.)**

30% **of employees** admit that they share their work PC's login and password details with colleagues**

23% **of organizations** do not have any cybersecurity rules or policies in place for corporate data storage**

The solution:
Convert human frailties into strengths by capitalizing on our ability to learn, and make employees your new first line of defense.

Why are customers not happy with existing awareness training programs?

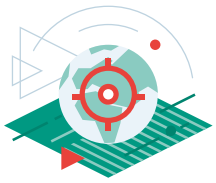
Not efficient:
- Training is perceived by employees as boring, far removed from actual working life, and an irrelevant drudge
- It's all about 'don't' rather than about 'how to'
- Reading and listening isn't as efficient as doing

An administrative burden:
- Difficult to manage and control the training process
- Difficult finding new ways of engaging and motivating employees to learn

* Research: "The cost of a data breach", Kaspersky Lab, Spring 2018.

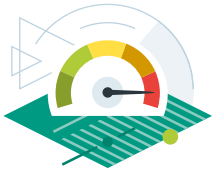
Kaspersky Security Awareness – a new approach to learning

Key program differentiators



Role-based, targeted training
- Learn what you need to know, based on your role and risk profile
- Real-life examples and skills that can be put to immediate use
- Learning by doing

Human-centric
- Training that's structured in line with the way people naturally think
- Putting a positive, proactive spin on safe behavior
- Information and skills that are easy to digest and retain, thanks to methodologies based on the specifics of human memory



Continuous incremental learning
- From the simple to the more complex
- Expanding and applying previously acquired knowledge in new contexts

Easy to manage and control
- Online
- Automated learning management
- Invitations and motivational emails sent automatically with individual recommendations for every student

** "Sorting out a Digital Clutter". Kaspersky Lab, 2019.

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:

$1,057,000
per enterprise – the average financial impact of data breaches caused by inappropriate IT resource use by employees*

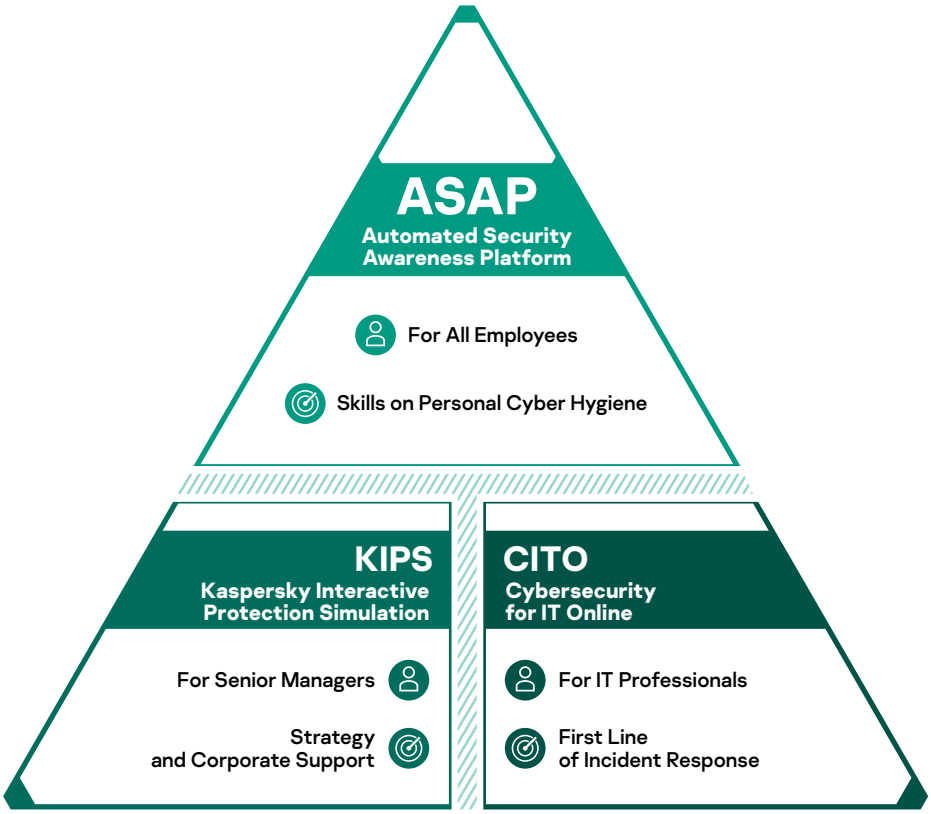
$101,000
for every SMB – the financial impact of attacks caused by phishing/social engineering **($1.3M per enterprise)****

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

Kaspersky Security Awareness training

Kaspersky offers computer-based training products that combine expertise in cybersecurity with best-practice educational techniques and technologies. This approach changes users' behavior and helps create cybersafe environment throughout the organization.

Different training formats for different organizational levels



* Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives . Kaspersky Lab, 2018

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

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

Kaspersky Security Awareness Products description

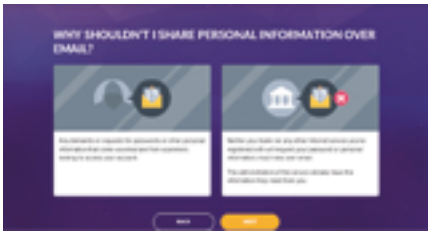
ASAP offers easy-to-set training objectives, a well-balanced predefined learning path, real-life relevance and actionable reporting ensuring program appreciation and value for employees and management alike.

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 9 languages: English, German, Italian, French, Spanish, Russian, Arabic, Portuguese and Dutch*.

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!



1. Kaspersky Automated Security Awareness Platform (ASAP)

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:

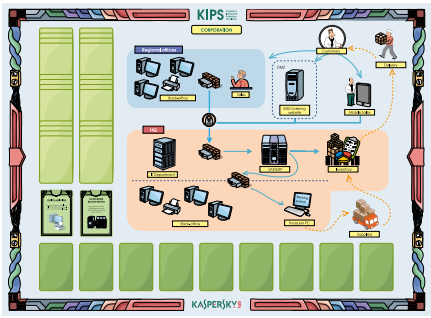
- **Simplicity through full automation:** The program is very easy to launch, configure and monitor, and ongoing management is fully automated – no administrative involvement required.
- **Efficiency:** program content is structured to support incremental interval learning with constant reinforcement. The methodology is based on the specifics of human memory to ensure knowledge retention and subsequent skills application.
- **Flexible licensing:** the per-user licensing model can start from as little as 5 licenses.

* As of July 2019

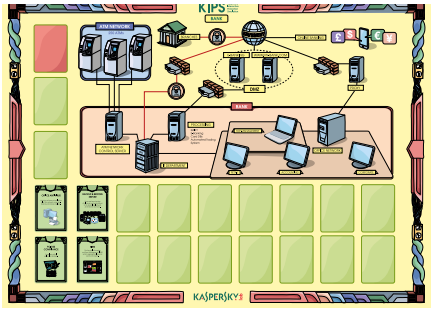
KIPS training is targeted at senior managers, business systems experts and IT professionals, increasing their awareness of the risks and security problems of running modern computerized systems

Some of KIPS scenarios:

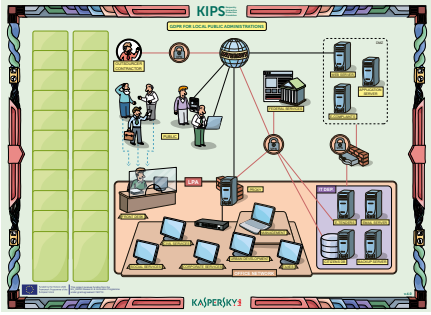
Corporation



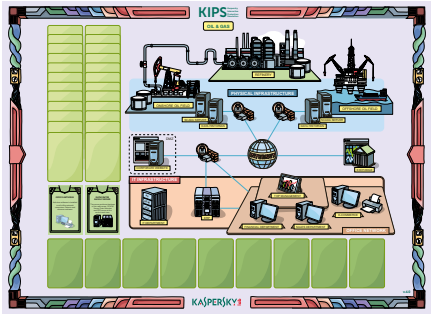
Bank



Local Public Administrations (LPA) NEW!



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

2. 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 cyber-threats, 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/ Local Public Administrations:** 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.

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 to corporate 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 take be spread over the course of a year. The recommended rate of progress is 1 exercise per week – each exercise taking from 5 up to 45 minutes to complete.

3. 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.

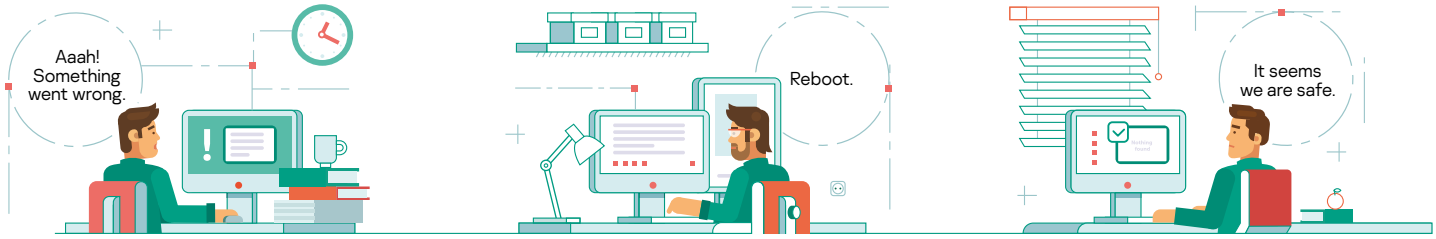
The course consists of 4 modules:

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

This course equips IT professionals with practical skills including:

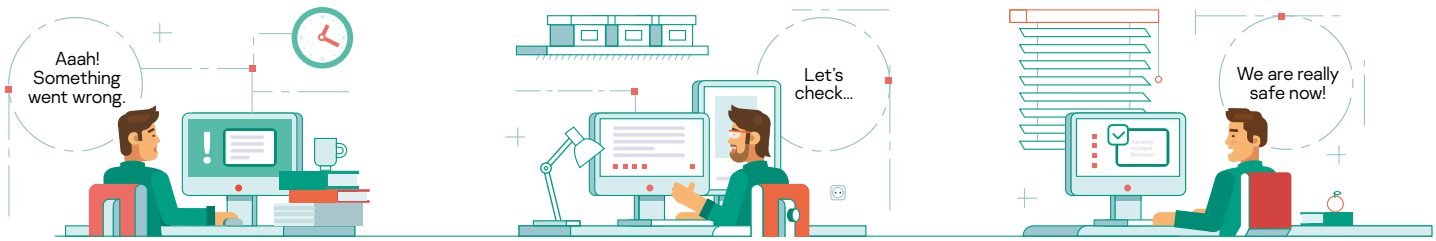
- How to recognize a possible attack scenario in an ostensibly benign PC incident
- How to collect incident data for handover to IT Security
- Hunting out malicious symptoms – cementing the role of all IT team members as the first line of security and defense.

Now



User **IT Support/Admins** **IT Security**

Should be

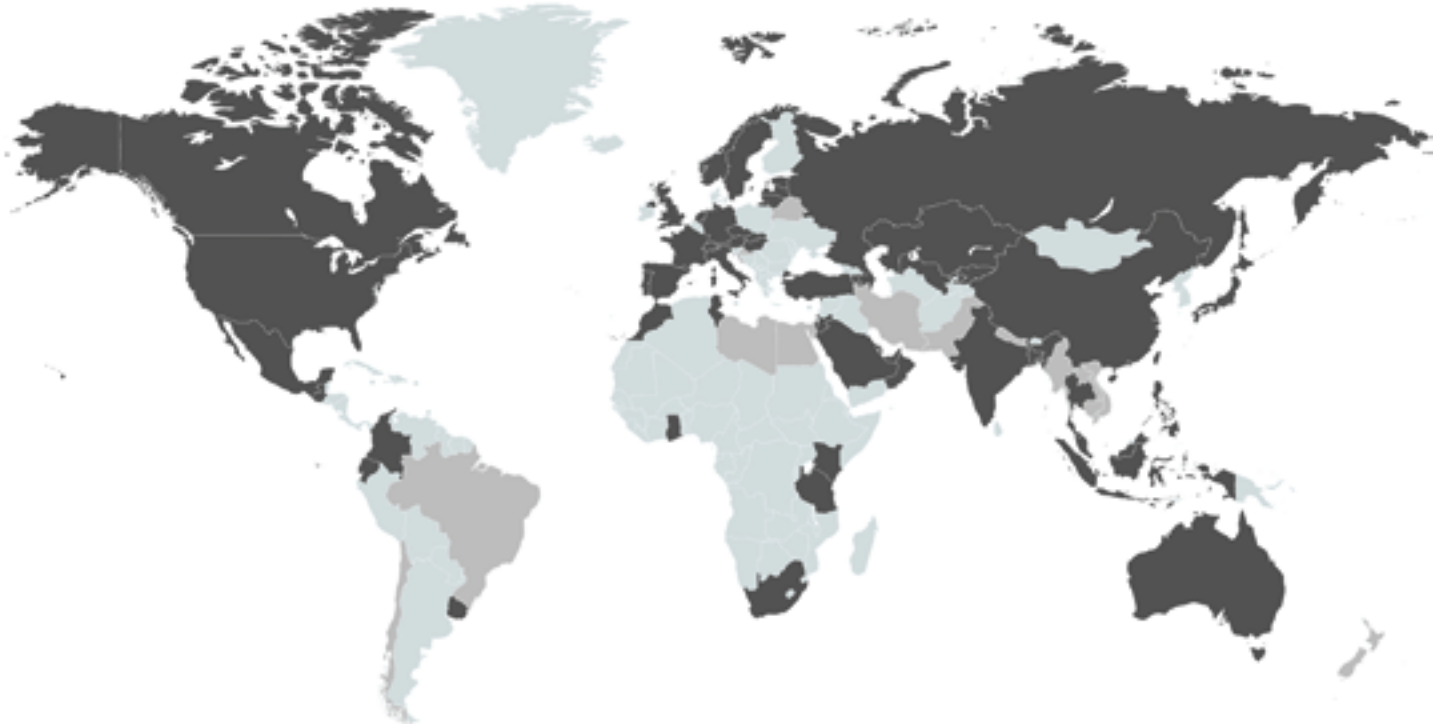


User **IT Support/Admins** **IT Security**

Kaspersky Security Awareness worldwide

75
countries

250,000
trained employees



As of March 2019

Commercial use or major event
Participated in online tournament

Created with mapchart.net

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
IT Security News: business.kaspersky.com

www.kaspersky.com

kaspersky **BRING ON THE FUTURE**