

Kaspersky ASAP: Automated Security Awareness Platform

Efficiency and ease of management for organizations of any size

www.kaspersky.com/awareness
#truecybersecurity

Kaspersky ASAP: Automated Security Awareness Platform

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.

Human mistakes as the biggest cyber risk today

\$83,000 per SMB

Average financial impact of attacks caused by careless/uninformed employees¹

\$101,000 per SMB

Financial impact of attacks caused by phishing/ social engineering¹

\$400 per employee per year

Average cost of phishing attacks (other types of cyberthreats are excluded from this count)²

52% of all organizations

Named careless actions of employees/ users as the biggest issue in their IT Security strategy¹

Barriers for launching efficient security awareness program

While companies are eager to implement security awareness programs, not many of them are happy with both process and results. Small and medium businesses, which usually do not have experience and dedicated resources, are particularly challenged.



No clue how to set goals and plan education



Training takes too much time to manage



Reporting doesn't help in goal tracking



Employees don't appreciate program → don't get skills

Even organizations with dedicated awareness teams often struggle to achieve a real improvement in user behavior as a result of security awareness training.

Many companies choose between one-time educational effort (like "all about cybersecurity in 1 hour") and well-structured professional training programs of which, however, they only use some basic functions and instruments. Typically this consists of a number of waves of simulated phishing attacks per year plus a few overview lessons, because other program elements are too difficult to run and manage. Either way, employees do not get strong skills needed to create a sustained state of security for their organization.

¹ "Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", Kaspersky Lab and B2B International, June 2017

² Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.

Efficiency and ease of awareness management for organizations of any size

Kaspersky Lab is introducing Automated Security Awareness Platform which forms the core part of Kaspersky Security Awareness training portfolio.

The Platform is an online tool building strong and practical cyber-hygiene skills of employees throughout a year. Launching and managing the Platform doesn't require specific resources and arrangements, and it provides the organization with built-in help in all steps of the journey towards safe corporate cyber environment:

Step 1:



Setting training objectives and justifying a program

- Set goals in comparison to the global benchmarking
- Choose balance between target level of security competence for each group of employees and total learning time required to get employees to this level

Step 2:



Ensuring all employees are trained up to their best needed level

- Use automated learning management which pulls every employee up to the security skill level appropriate to their risk profile
- Make sure acquired skills are reinforced to prevent obliteration
- Train people in individual, own pace manner to avoid over-training and rejection

Step 3:



Monitor progress with actionable reporting and analytics

- Get live tracking of data, trends and forecasts
- Use real-time forecast of achieving the annual training goal
- Address issues before they become problems (e.g., you know which organizational units need more attention and can influence their results)
- Benchmark your interim results against global KL data

Step 4:



Guarantee training appreciation and thus efficiency

- Engage employees into training with gamification and competition
 - Ensure training is relevant to people's everyday life
 - Offer an opportunity to compare individual results with others
 - Prevent overload
-

Program management: simplicity through automation

Start program in 10 minutes

- Set objectives based on world/ industry averages
- Start training
- Pay only for active users (those who are learning)

Platform adjusts to individual pace and learning abilities of each employee

- Platform automatically ensures user learns and passes tests on basics before going to study further
- Management does not need to spend time on individual progress analysis and manual adjustments

Benefit from specific learning paths for each risk profile

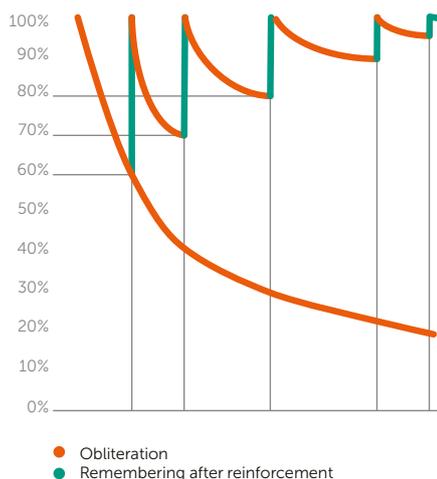
- Use automated rules to assign employees to a certain group based on the desired educational target level. Target level depends on the risk the particular user poses to the company. Higher the risk, higher the target education level should be, e.g. IT, or accountants typically represent a higher risk than most office workers
- Each group of users study the material only to the extent that they really need without spending too much working time on training

Get actionable reports anytime

- Enjoy dashboards with all information needed to estimate progress
- Get suggestions on what to do to improve results
- Compare results with world/ industry benchmarks

The Ebbinghaus Forgetting curve

Repeated reinforcement helps building strong skills.



Training efficiency: continuous micro learning

Skills increase level by level, from the easiest to more advanced. Platform automatically re-assigns more learning to those who failed to complete a previous level. This ensures strong skills retention and prevents obliteration.

Micro learning

- Content is especially structured for micro learning (2 to 10 minutes), avoiding dull and tedious long lessons.

Comprehensive set of tools on each security topic

- Each level includes: Interactive lesson and video → reinforcement → assessment (test or simulated phishing attack)

Each topic comprises 4 levels, detailing specific security skills. Levels are defined according to degrees of risks they help eliminate: Level 1 is normally enough to protect from easiest and mass attacks while to protect from the most sophisticated and targeted attacks, one needs to reach level 4

Training topics*

- Email / phishing
- Web browsing
- Passwords
- Social networks & messengers
- PC security
- Mobile devices
- Confidential data
- Personal data
- GDPR
- Social engineering
- Security at home and on travel

Example: Skills trained in “Web browsing” topic

Beginner to avoid mass (cheap and easy) attacks	Elementary to avoid mass attacks on a specific profile	Intermediate to avoid well-prepared focused attacks	Advanced to avoid targeted attacks
<p>13 skills, including:</p> <ul style="list-style-type: none"> – Set up your PC (updates, antivirus) – Ignore obviously malicious websites (those which ask to update software, optimize PC performance, send SMS, install players, etc.) – Never open executables from websites 	<p>20 skills, including:</p> <ul style="list-style-type: none"> – Sign-up/Login with trusted sites only – Avoid numeric links – Enter sensitive information on trusted sites only – Recognize signs of a malicious website 	<p>14 skills, including:</p> <ul style="list-style-type: none"> – Recognize faked links – Recognize malicious files and downloads – Recognize malicious software 	<p>13 skills, including:</p> <ul style="list-style-type: none"> – Recognize sophisticated fake links (including links looking like your company websites, links with redirect) – Avoid black-SEO sites – Log out when finished – Advanced PC setup (turn off Java, adblock, noscript, etc.)
	+ reinforcement of the elementary skills	+ reinforcement of the previous skills	+ reinforcement of the previous skills

Key subjects covered in the topic: Links, Downloads, Software installations, Sign-up & Login, Payments, SSL

* Final list of training topics may be changed.

Languages

In the Autumn 2018 Platform is available in the the following languages*:

- English
- German
- Italian
- Russian

Next following:

- Arabic
- French
- Spanish

New languages are being added regularly to guarantee deep and efficient education for all regions.

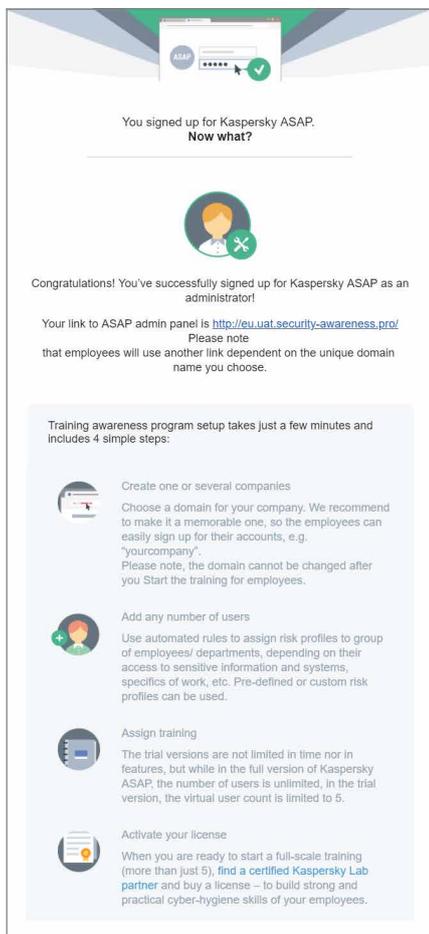
Gamification and relevance to real life to ensure efficiency

The Platform's content is based on simulation principles showing real life events and highlighting personal importance of cybersecurity for employees. Platform focuses on training skills, not just giving knowledge, thus practical exercises and employee-related tasks are at the core of each module.

Modules combine different types of exercises to keep users interested and alert and to motivate them to learn and acquire safe behavior.

Visual style and texts are not only translated to different languages, but are adjusted to reflect cultures and local attitudes.

Simulation-based tasks and excersices to build practical skills and keep users entertained and motivated



You signed up for Kaspersky ASAP.
Now what?

Congratulations! You've successfully signed up for Kaspersky ASAP as an administrator!

Your link to ASAP admin panel is <http://eu.uat.security-awareness.pro/>
Please note that employees will use another link dependent on the unique domain name you choose.

Training awareness program setup takes just a few minutes and includes 4 simple steps:

- Create one or several companies**
Choose a domain for your company. We recommend to make it a memorable one, so the employees can easily sign up for their accounts, e.g. "yourcompany".
Please note, the domain cannot be changed after you Start the training for employees.
- Add any number of users**
Use automated rules to assign risk profiles to group of employees/ departments, depending on their access to sensitive information and systems, specifics of work, etc. Pre-defined or custom risk profiles can be used.
- Assign training**
The trial versions are not limited in time nor in features, but while in the full version of Kaspersky ASAP, the number of users is unlimited, in the trial version, the virtual user count is limited to 5.
- Activate your license**
When you are ready to start a full-scale training (more than just 5), find a **certified Kaspersky Lab partner** and buy a license – to build strong and practical cyber-hygiene skills of your employees.



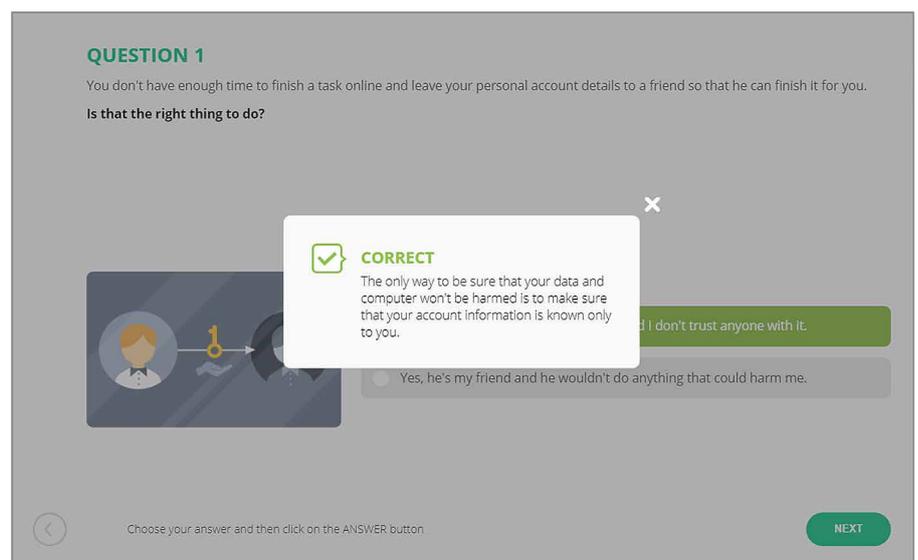
WHAT IS THE MOST VALUABLE AND IMPORTANT THING WE WILL LEARN?

We will find out which passwords provide reliable protection and which security measures should be adopted to prevent scammers from stealing passwords.

We will determine:

- ▶ How to tell which passwords are reliable and which aren't
- ▶ How to come up with a complex password
- ▶ Where to store passwords, ensuring they will not be lost or stolen
- ▶ What can happen if you give your password to someone
- ▶ When to change your password
- ▶ Why passwords to corporate accounts should never be used elsewhere

NEXT



QUESTION 1

You don't have enough time to finish a task online and leave your personal account details to a friend so that he can finish it for you.

Is that the right thing to do?

CORRECT

The only way to be sure that your data and computer won't be harmed is to make sure that your account information is known only to you.

I don't trust anyone with it.

Yes, he's my friend and he wouldn't do anything that could harm me.

Choose your answer and then click on the ANSWER button.

NEXT

* The final order and timing of localizations may be changed



Kaspersky® Security Awareness

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 cybersecurity culture which engenders a self-sustaining level of cybersecurity throughout the organization.

up to **90%**

Reduction in the total number of incidents

not less than **50%**

Reduction in the financial impact of incidents

up to **93%**

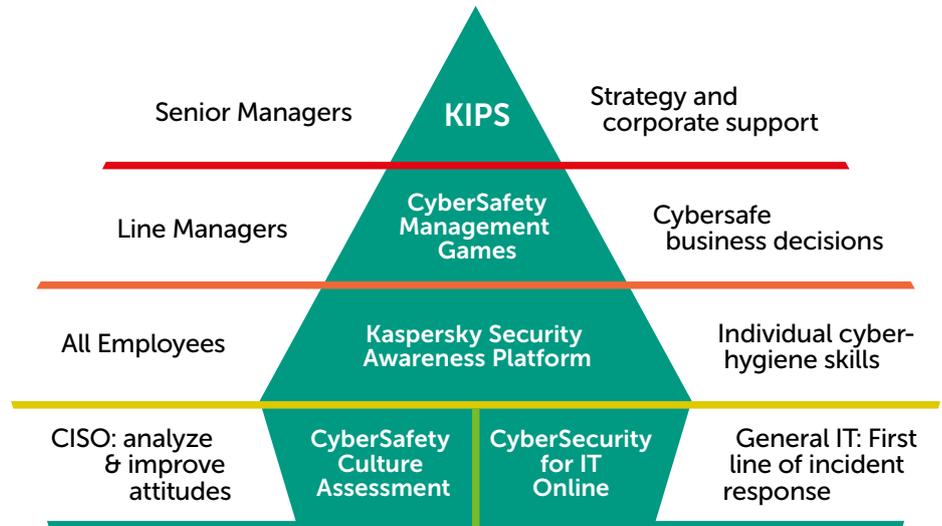
Probability that knowledge will be applied in everyday work

more than **30x**

ROI from investment in security awareness

amazing **86%**

Of participants willing to recommend the experience



Setting objectives & choosing a program

- Setting goals based on global data
- Benchmarking against world/industry averages

Learning management

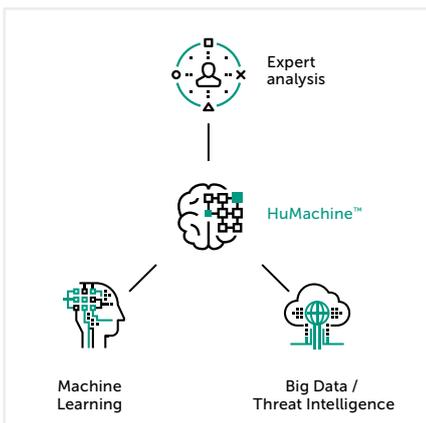
- Learning automation
- Self-adjusting learning path
- Calculation on time spent

Reporting & analytics

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

Program efficiency & appreciation

- True gamification
- Competition & challenge
- Overload prevention



Kaspersky Lab
 Enterprise Cybersecurity: www.kaspersky.com/enterprise
 Cyber Threats News: www.securelist.com
 IT Security News: business.kaspersky.com/

#truecybersecurity
 #HuMachine

www.kaspersky.com

© 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.