KASPERSKY lab

Kaspersky ASAP: Automated Security Awareness Platform

Efficiency and ease of management for organizations of any size

www.kaspersky.com/awareness
asap.kaspersky.com
#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 employees[1]

$101,000 per SMB
Financial impact of attacks caused by phishing/social engineering[1]

$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 strategy[1]

Barriers to launching an efficient security awareness program

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

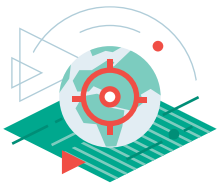
[2] Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.

Efficiency and ease of awareness management for organizations of any size

Introducing the Automated Security Awareness Platform, which forms the core of the Kaspersky Security Awareness training portfolio.

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

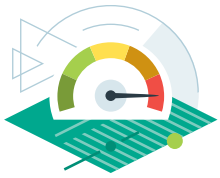
Step 1:



Setting training objectives and justifying a program

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

Step 2:



Ensuring all employees are trained up to their appropriate level

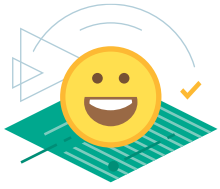
- Use automated learning management which pulls every employee up to the security skills level appropriate to their risk profile
- Make sure acquired skills are reinforced to prevent obliteration
- Train people in an individual manner at their own pace to avoid over-training and rejection

Step 3:

Monitor progress with actionable reporting and analytics

- Get live tracking of data, trends and forecasts
- Use real-time forecasts to achieve the annual training goals
- 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 Kaspersky Lab data

Step 4:



Guarantee training appreciation and thus efficiency

- Engage employees with practical interactive exercises
- Provide learning scenarios that are relevant to participants' everyday working lives
- Avoid knowledge overload and training fatigue

Program management: simplicity through automation

Start your program in just 10 minutes

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

Platform adjusts to the individual pace and learning abilities of each employee

- The platform automatically ensures that the 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

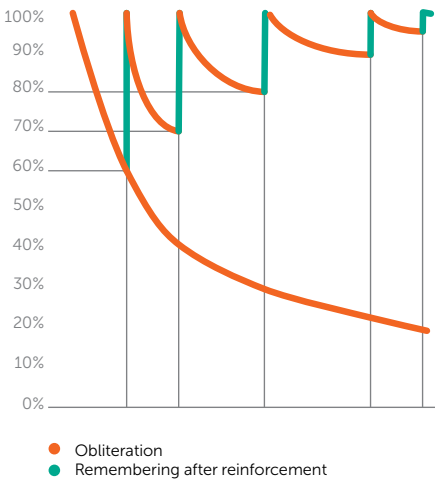
- Use automated rules to assign employees to a certain group based on their desired educational target level. This target level depends on the risk the particular role poses to the company. The higher the risk, higher the target education level should be, e.g. IT, or accountants typically represent a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

Get actionable reports anytime

- Enjoy dashboards with all the 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 build strong skills.



Training efficiency: continuous micro-learning

Skills increase level by level, from the easiest to the more advanced. The Platform automatically re-assigns more learning to those who fail 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 several levels, detailing specific security skills. Levels are defined according to degrees of risk 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 study the next levels.

Training topics*

- Email
- Web browsing
- Passwords
- Social networks & messengers
- PC security
- Mobile devices
- Confidential data
- Personal data/GDPR
- Social engineering
- Security at home and during 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
13 skills, including: – 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	**20 skills, including:** – Sign-up/Login with trusted sites only – Avoid numeric links – Enter sensitive information on trusted sites only – Recognize the signs of a malicious website	**14 skills, including:** – Recognize faked links – Recognize malicious files and downloads – Recognize malicious software	**13 skills, including:** – Recognize sophisticated fake links (including links looking like your company websites, links with redirects) – Avoid black-SEO sites – Log out when finished – Advanced PC setup (turn off Java, adblock, noscript, etc.)
	+ reinforcement of 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

As from Autumn 2018, the Platform is available in the following languages*:
- English
- German
- Italian
- Russian

Followed by:
- Arabic
- French
- Spanish

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

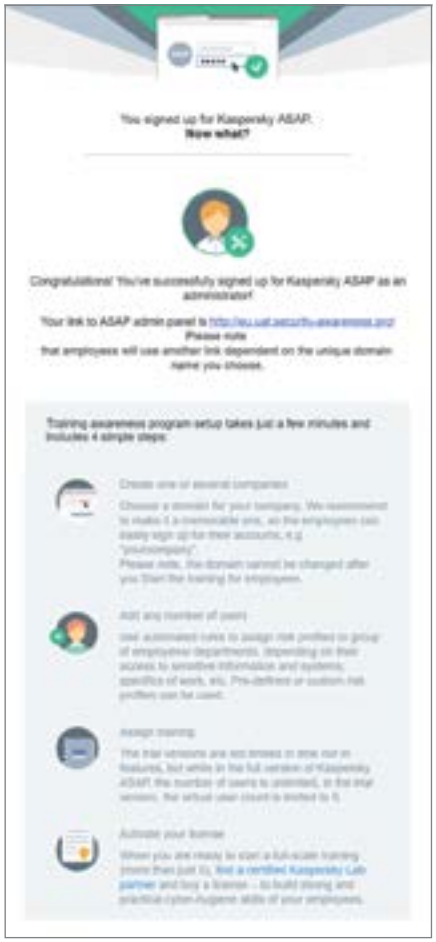
Gamification and relevance to real life ensures efficiency

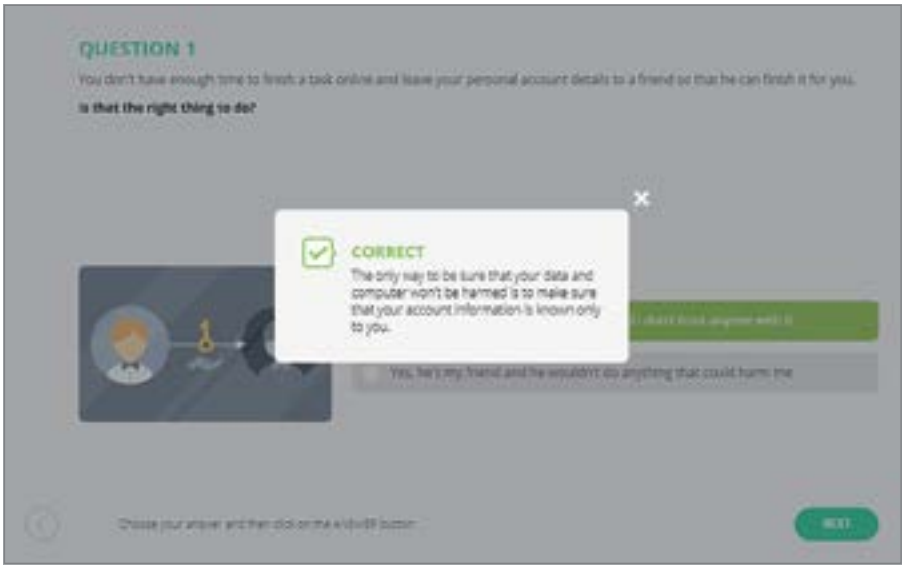
The Platform's content is based on simulation principles showing real life events and highlighting the personal importance of cybersecurity for employees. The Platform focuses on training skills, not just providing knowledge, so practical exercises and employee-related tasks are at the core of each module.

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

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

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





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

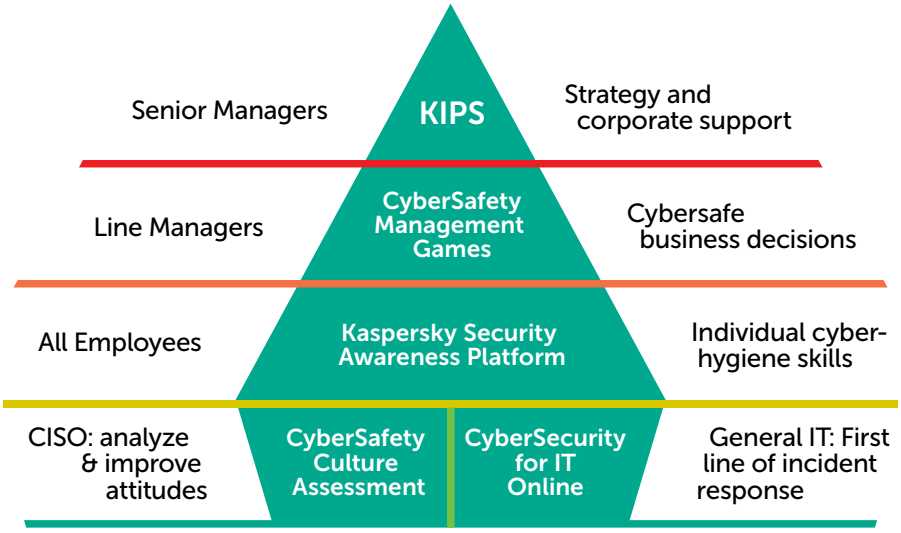
up to
90%
Reduction in the total number of incidents

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

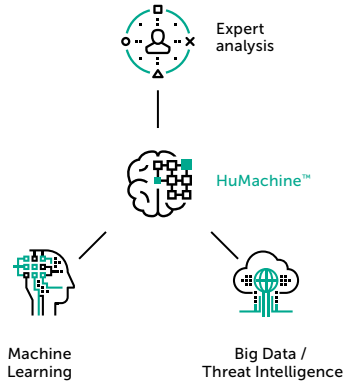
- Learning automation
- Self-adjusting learning path
- Calculation on time spent

Reporting & analytics

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

Program efficiency & appreciation

- Practical engaging exercises
- Prevent overload and training fatigue
- Deliver high level of knowledge and skills retention



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

#truecybersecurity
#HuMachine

www.kaspersky.com