Engaging for employees, efficient for managers.

Free trial
k-asap.com

Kaspersky ASAP: Automated Security Awareness Platform

kaspersky bring on the future

Kaspersky
Automated Security
Awareness Platform

Kaspersky ASAP: Automated Security Awareness Platform

82% of all cyber-incidents are caused by human error, with companies losing millions as a result. Traditional training programs are not designed to address this problem, and a new approach is needed. Say hello to Kaspersky ASAP.

Human error is the biggest cyber risk

79%
of employees
admit to having engaged in at least one risky activity within the previous year despite being aware of the risks *

51%
of employees
believe their IT departments should be completely responsible for preventing their employers from falling victim to cyberattacks*

55%
of enterprises
report threats caused by inappropriate IT use by employees**

51%
of small businesses
suffered a security incident due to IT security policies violation by employees**

26%
of employees
say their personal email has the same password as their work account***

Barriers to launching a security awareness program that works

Companies are eager to implement security awareness programs, yet many are unhappy with the process as well as the results. SMBs in particular find it challenging, as they tend not to have the necessary experience or resources.

Inefficient for students	A burden for administrators
Perceived as difficult, boring, irrelevant drudgery.	How to create a program and set goals?
It's all about 'don't' rather than 'how to'	How to manage training assignments?
Knowledge is not retained	How to control the progress
Reading and listening aren't as effective as doing	How to make sure our staff are fully engaged?

* Balancing Risk, Productivity, and Security."Delinea, 2021

** "ITSecurity Economics 2022", Kaspersky

*** https://www.beyondidentity.com/blog/password-sharing-work

Efficient, easy to manage training for organizations of any size

Introducing Kaspersky ASAP, Automated Security Awareness Platform, which sits at the heart of the Kaspersky Security Awareness training portfolio. The platform is an online tool that builds strong, practical cyber-hygiene skills for employees throughout the year.

Launching and managing the platform doesn't require special resources or arrangements, and it includes built-in help at every step of the learning journey towards a safe corporate cyber-environment.

Meaningful content that you can't ignore

One of the most important criteria when choosing an awareness program is efficiency, and with ASAP, efficiency is built into the training content and management. The content is based on the accumulated experience of **25+ years in cybersecurity** expressed in a competency model comprising over **350 practical and essential cybersecurity skills** that all employees should have.

Educate your employees about cybersecurity.
Change their attitude and behavior and protect your business and IT systems.

Efficient training

Consistent	– Well thought-out, structured content – Interactive lessons, constant reinforcement, tests, simulated phishing attacks to ensure skills are applied The content and structure of the training material take into consideration the specifics of human memory, and our ability to absorb and retain information.
Practical & engaging	– Relevant to employees' everyday working life – Skills that can be put to immediate use Examples from real-life situations which employees can personally relate to contribute to better learner engagement, helping information to be retained.
Positive	– Puts a proactive spin on safe behavior – Explains 'why' and 'how to' instead of just the taboos Too many rules and restrictions can cause discontent and disengagement, while explanations and principles aligned with the way people think naturally contribute to adoption and behavioral change.

Easy management

Easy to manage	– Fully automated learning management brings every employee up to the skills level appropriate to their risk profile without any intervention from the platform administrator – Synchronization with AD (Active Directory), SSO (Single Sign-On), Open API (the ability to interact with third-party solutions), online onboarding during the first visit, a FAQ section and tips all make platform management convenient and efficient.
Easy to control	"All-in-one" dashboard & actionable reports: – report on lesson progress – reports on tests and simulated phishing attacks
Easy to engage	The platform automatically sends out invitations and reminders, as well as reports to students and administrators.

ASAP management: simplicity through full automation

Start your program in 4 simple steps

Add users

Use **AD synchronization** or upload .xlsx file or add them manually

Divide users by groups

Divide users manually or using rules based on the desired target level

Launch training

Divide users manually or using rules based on the desired target level, and set the start date for each group

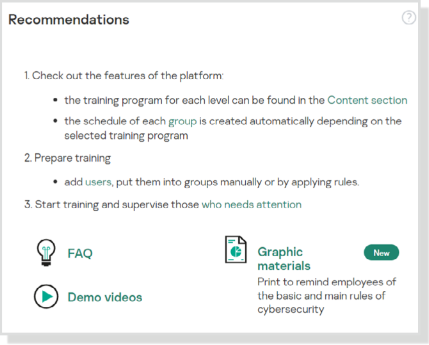
Automated training management done by ASAP

ASAP creates a schedule for each group, for invitations, reminders & other communications – everything happens automatically

A new and improved approach to training

Kaspersky ASAP is changing the way we deliver cybersecurity learning content. Now you can choose whether to assign employees a basic Express course that will help you quickly meet regulatory requirements for cybersecurity training, or refresh their knowledge, or opt for the Main course broken down into complexity levels

Onboarding during first log-in, recommendations, FAQ and demo videos, explaining how platform works from admin and user perspective – everything you need to start the learning process is on the admin main page



Recommendations

1. Check out the features of the platform:
   - the training program for each level can be found in the Content section
   - the schedule of each group is created automatically depending on the selected training program
2. Prepare training
   - add users, put them into groups manually or by applying rules.
3. Start training and supervise those who needs attention

Print to remind employees of the basic and main rules of cybersecurity

Topics covered

Topics covered

Main course	Express course
Email	Email
Passwords & Accounts	Passwords & Accounts
Websites and the Internet	Websites and the Internet
Social media & Messengers	Mobile device security
PC Security	Social media
Mobile Devices	My computer
Protecting confidential data	Protecting confidential data
Personal data	Doxing
GDPR	Cryptocurrency security
Industrial Cybersecurity	Information security when working remotely
Bank card security & PCI DSS	Federal law 152-FZ (for Russia)

Topics are divided into large blocks, covering numerous IT security concepts *.

#Passwords #Phishing #Corporate accounts #Dangerous messages #Bank cards #Ransomware #SocialEngineering #Dangerous Files #Working with browsers #Corporate ethics #Antivirus #Malicious software #Applications #Browser #Confidential information #Storing information #Sending information #Personal data #Internet and the law #European legislation #Business #Dangerous Links #Fake websites #Ransomware sites #Backup #Mobile data #Encryption #Cloud services #Industrial espionage #PCI DSS #Two-factor authentication #Digital footprint #Torrents #Catfishing #Targeted attack #Hashing #Tokens #Pattern locks #Mining #Parental control

* For the latest list of topics and concepts, please check out k-asap.com

Each topic has several levels, detailing specific security skills. Levels are defined according to the degree of risk they help to eliminate – for example, Level 1 is normally enough to protect against the simplest attacks as well as mass attacks. Higher levels need to be studied to learn how to protect against the most sophisticated and targeted attacks.

Example: Skills trained in “Websites and the Internet” topic

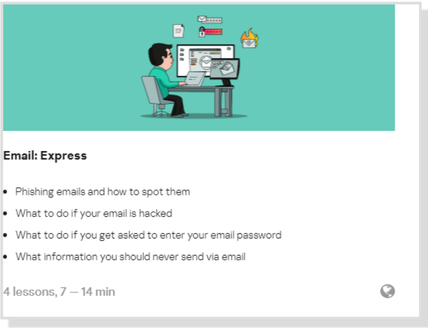
Beginner To avoid mass (cheap and easy) attacks	**Elementary** To avoid mass attacks on a specific profile	**Intermediate** To avoid well-prepared focused attacks	**Advanced*** To avoid targeted attacks
23 skills, including: – Recognize fake pop-ups – Pay attention to redirects – Distinguish genuine download links from fake ones – Recognize executable files found on the web – Be able to determine the authenticity of a browser extension	34 skills, including: – Enter data only on sites with a valid SSL certificate – Use different passwords for different registrations – Recognize fake sites by a number of signs – Avoid numeric links – Recognize invalid network link addresses by fake subdomains	12 skills, including: – Check sharing links before sending – Use software only from trusted manufacturers for torrents – Download legal content only from torrents – Clear browser cookies regularly	13 skills, including: – Recognize sophisticated fake links (including links looking like your company websites, links with redirects) – Check sites using special utilities – Recognize if the browser is mining – Avoid black SEO sites
	+ reinforcement of elementary skills	+ reinforcement of the previous skills	+ reinforcement of the previous skills

ASAP Express course

A short version of the training in audio-video format. Each cybersecurity topic contains several short lessons to help the user grasp basic cybersecurity skills.

- Interactive theory
- Videos
- Tests

Simulated phishing attacks aren’t included in the learning path, but can be assigned separately by the administrator.



Email: Express

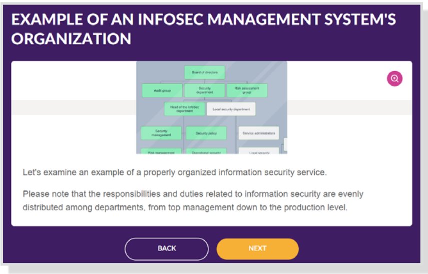
- Phishing emails and how to spot them
- What to do if your email is hacked
- What to do if you get asked to enter your email password
- What information you should never send via email

4 lessons, 7 — 14 min

ASAP main course

The training is based on the specifics of human memory:

- Multimodal content:
  - each unit includes: an interactive lesson, reinforcement, assessment (test and simulated phishing attack, where applicable)
  - all training elements support the particular skill being taught in each unit, so that skills are truly grasped and become part of the new, desired behavior
- Interval learning:
  - training elements follow each other at certain intervals, which eliminates the simple clicking of lessons and improves memory retention. Intervals are based on the Ebbinghaus ‘Forgetting curve’ study
  - repetition builds safe habits and prevents forgetting
- Balanced, structured content relevant to real-life ensures efficiency:
  - packed with real-life examples that highlight the personal importance of cybersecurity for employees
  - the platform focuses on teaching skills, not just providing knowledge, so practical exercises and employee-related tasks are at the core of each module.

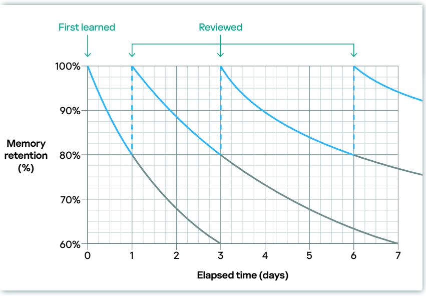


EXAMPLE OF AN INFOSEC MANAGEMENT SYSTEM'S ORGANIZATION

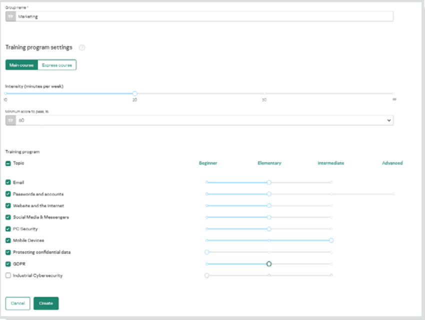
Let's examine an example of a properly organized information security service.

Please note that the responsibilities and duties related to information security are evenly distributed among departments, from top management down to the production level.

Ebbinghaus’ Forgetting Curve



Flexible learning path



Group name *
Marketing

Training program settings

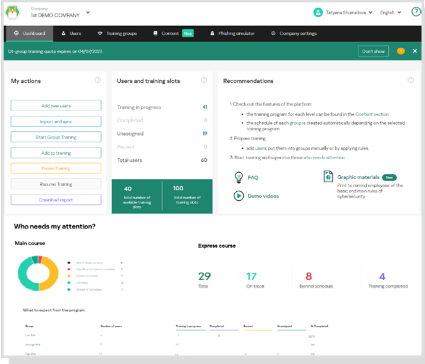
Main course | Express course

Intensity (minutes per week)
10 20 30 ∞

Minimum score to pass, %
80

Training program

Topic	Beginner	Elementary	Intermediate	Advanced
☑ Email				
☑ Passwords and accounts				
☑ Website and the Internet				
☑ Social Media & Messengers				
☑ PC Security				
☑ Mobile Devices				
☑ Protecting confidential data				
☑ GDPR				
☐ Industrial Cybersecurity				



Dt-group training quota expires on 04/07/2023

My actions

Users and training slots

Training in progress	41
Completed	0
Unassigned	19
Paused	0
Total users	60

40 Total number of available training slots

100 Total number of training slots

Recommendations

1. Check out the features of the platform:
   - the training program for each level can be found in the Content section
   - the schedule of each group is created automatically depending on the selected training program
2. Prepare training
   - add users, put them into groups manually or by applying rules.
3. Start training and supervise those who needs attention

Print to remind employees of the basic and main rules of cybersecurity

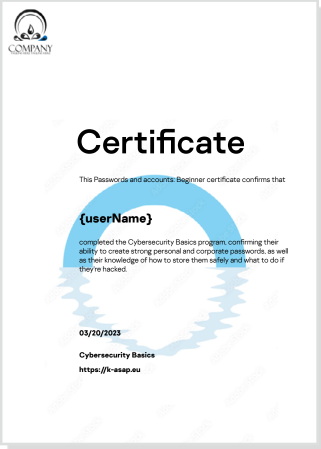
Who needs my attention?

Main course

Express course

29	17	8	4
Total	On track	Behind schedule	Training completed

What to expect from the program



COMPANY

Certificate

This Passwords and accounts: Beginner certificate confirms that

{userName}

completed the Cybersecurity Basics program, confirming their ability to create strong personal and corporate passwords, as well as their knowledge of how to store them safely and what to do if they're hacked.

03/20/2023

Cybersecurity Basics
https://k-asap.eu

Flexible learning

The scope of the training is completely flexible, while retaining the advantages of sequential automated learning management. For each training group you can choose:

- Main or Express course, or a combination of both;
- Topics to train in the main course and/or the Express course which students in the group need to learn;
- The target level you want students to achieve for each chosen topic in the main course.

The learning path will be built automatically by the platform for each group of learners based on these settings.

Do it all from the dashboard

- Everything you need to control and manage training – statistics, summaries of users' activities and progress, training slots, group training, suggestions on how to improve results – can be done from the dashboard. You can download reports in a single click and configure the frequency of reports there too.

Freedom to perform

- Employees can study whenever it's convenient for them, and from any device, with ASAP's mobile-friendly design that makes learning convenient and comfortable.
- Users can access the training portal from personalized links provides in the training invitation or via a single link for all users with Single Sign-On (SSO) technology if it's set-up by administrator.

Customization

The administrator can easily change the program's appearance:

- replace the Kaspersky logo with your company logo in the admin panel, training portal and platform emails;
- customize certificates;
- add personal content to any lesson.

Integration

You can use Open API to interact with third-party solutions – Open API works via HTTP and offers a set of request/response methods.

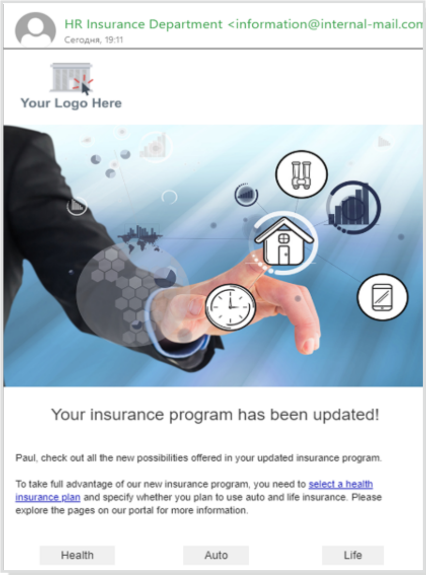
ASAP integrates with Kaspersky KUMA & XDR platforms:
– Admin can see an event in XDR and take the appropriate response, including assigning a training in ASAP
– Automatic enrichment of incident cards with information about the level of awareness of the attacked user

Localization

ASAP is available in 25 languages*. Localization in ASAP goes beyond just translation – text and visuals are not only translated into different languages, they're also adjusted to reflect different cultures and local attitudes.

* Current list of available languages is available on k-asap.com

Example of the editable simulated phishing template and feedback



HR Insurance Department <information@internal-mail.com

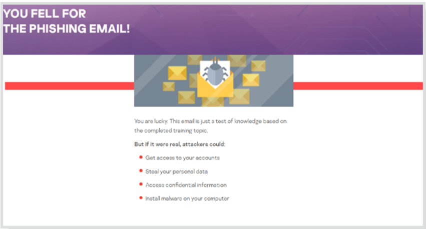
Сегодня, 19:11

Your Logo Here

Your insurance program has been updated!

Paul, check out all the new possibilities offered in your updated insurance program.

To take full advantage of our new insurance program, you need to select a health insurance plan and specify whether you plan to use auto and life insurance. Please explore the pages on our portal for more information.



YOU FELL FOR THE PHISHING EMAIL!

You are lucky. This email is just a test of knowledge based on the completed training topic.

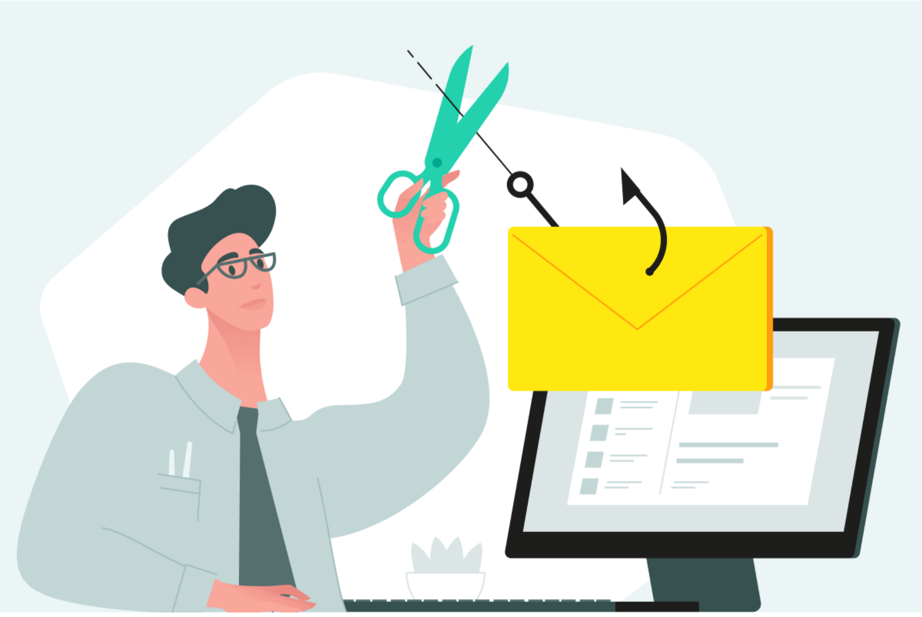
But if it were real, attackers could:

- Get access to your accounts
- Steal your personal data
- Access confidential information
- Install malware on your computer

Simulated phishing campaigns

Phishing campaigns are offered in addition to the main training. They test employees' practical skills in avoiding phishing attacks, and help training managers to quickly identify gaps in users' knowledge and encourage further study of troublesome topics. The phishing campaigns are also an excellent tool for teaching employees how to recognize potentially harmful signs, and putting their knowledge into practice.

The platform comes with ready-made email templates containing phishing examples that can be sent to users in all available languages. The templates are regularly updated and new ones added. You can also create custom emails based on predefined templates.



Try a simulated phishing attack before you start training – check your employees' resilience! It will help employees and management to see the benefits of training.

Employees can also demonstrate their understanding of a topic by not being fooled by a simulated phishing attack, and by reporting phishing mails via the 'Report phishing' tool.

The 'Report phishing' tool demonstrates the level of employees' awareness, removes email from the Inbox, and sends messages not only to platform admin, but also t IT/IT security teams, to help organizations improve their phishing detection and response levels.

Kaspersky Security Awareness – a new approach to mastering IT security skills

Key program differentiators

Substantial cybersecurity expertise
25+ years' experience in cybersecurity transformed into a cybersafety skillset that lies at the heart of our products

Training that changes employees' behavior at every level of your organization
Our gamified training provides engagement and motivation through edutainment, while the learning platforms help to internalize the cybersecurity skillset to ensure that learnt skills don't get lost along the way.

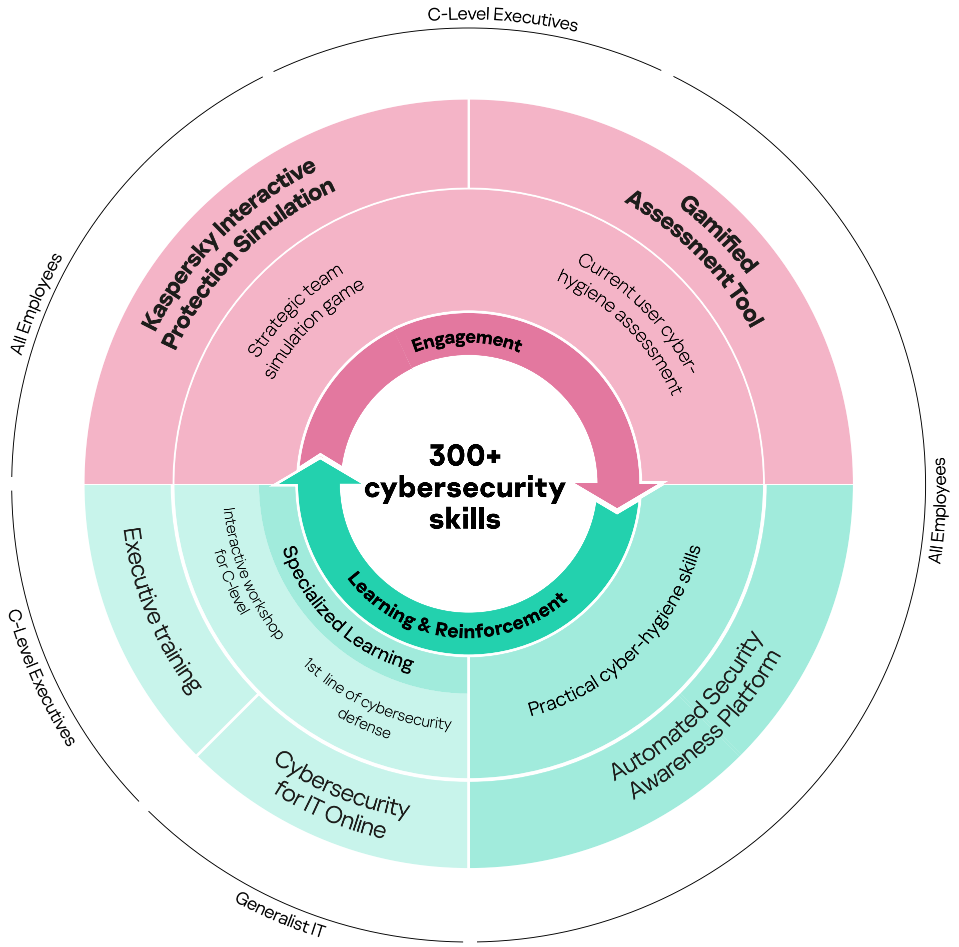
ASAP is a core product in Kaspersky's Security Awareness portfolio.

One flexible training solution for all

Kaspersky Security Awareness has a longstanding international track record of success. Used by businesses of every size to **train over a million employees across more than 75 countries**, it brings together over 25 years of Kaspersky's cybersecurity expertise with extensive experience in adult education.

The portfolio offers a range of engaging training options that increase the cybersecurity awareness of your employees at every level, empowering them to play their part in the overall cybersecurity of your organization.

Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with multiple components. Game-based learning engages senior management, turning them into advocates of cybersecurity initiatives and supporters of building a culture of cybersafe behavior. Gamified assessment helps to define gaps in employee knowledge and motivate them for further learning, while online platforms and simulations equip them with the right skills, reinforced.


C-Level Executives
All Employees
All Employees
C-Level Executives
Generalist IT
Kaspersky Interactive Protection Simulation
Strategic team simulation game
Gamified Assessment Tool
Current user cyber-hygiene assessment
Engagement
300+ cybersecurity skills
Learning & Reinforcement
Specialized Learning
Executive training
Interactive workshop for C-level
1st line of cybersecurity defense
Cybersecurity for IT Online
Practical cyber-hygiene skills
Automated Security Awareness Platform

Kaspersky ASAP free trial: k-asap.com
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