Cybersafety skills for employees at every level

# Kaspersky Security Awareness

kaspersky bring on the future

Learn more at kaspersky.com/awareness

# Kaspersky Security Awareness

## Build a culture of cybersafety throughout your organization

More than 80% of all cyber-incidents are caused by human error. By building a culture of cybersafe behavior, together with fundamental cybersecurity skills and awareness, throughout your organization, you can reduce the attack surface as well as the number of incidents you have to deal with. The best way to achieve the changes in behaviour that solve 'the human factor' problem in cybersecurity is through training that uses the latest techniques and technologies in adult education and delivers the most relevant and up-to-date content.

### The human factor – the most vulnerable element of cybersecurity

Cybersecurity solutions are rapidly developing and adapting to complex threats, making life more difficult for cyber criminals who are turning to the most vulnerable element of cybersecurity – the human factor.

**55% of corporations** report IT security policy violations by their own employees*

**43% of small businesses** report that IT security policy violations by employees cause security incidents **

**Data leaks** are the most common security issue most often **caused by employees** (22%) and attackers (23%).*

**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***

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

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

The highly engaging and effective training solutions boost the cybersecurity awareness of your staff so that they all play their part in the overall cybersafety of your organization. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with multiple components.

Continuous learning cycle


**Engagement/ motivation**
- Why do I need this?
- Cognition

**Starting point**
- Am I aware?
- What do I know and where are the gaps?

**Learning**
- Micro learning
- Continuous learning
- Adaptivity

**Consolidation**
- Did I get it right?
- Do I remember this?
- Do I act accordingly?

## 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 change 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.

* "IT Security Economics 2022" Kaspersky

** Report "IT Security Economics 2021", Kaspersky.

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

# Fueling motivation for effective security awareness

**Employees make mistakes. Organizations lose money...**

**$52.887**
**per enterprise organization**
The average cost of a cyberattack caused by inappropriate IT resource use by employees*

**30%**
**of malware breaches**
happen via emails with fake links and attachments**

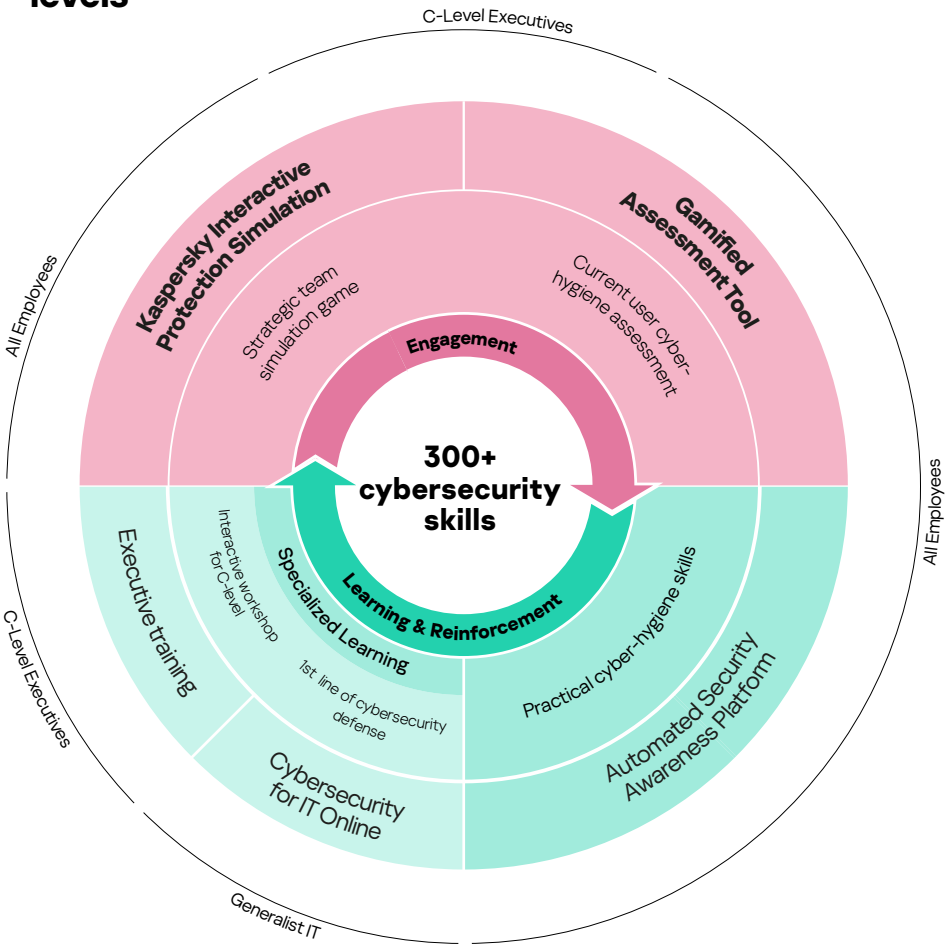
**79%**
**of employees**
admitted to having engaged in at least one risky activity within a year despite being aware of the risks***

**$164**
**per record**
The average global cost for breaches involving between 2,200 and 102,000 records****

**42% of respondents**
**working in companies with more than 1000 employees**
said that the majority of training programs they attended were useless and uninteresting*****

Changing employees' behavior is your biggest cybersecurity challenge. People are generally not motivated to acquire skills and change their habits, which is why so many educational efforts turn into little more than an empty formality. Effective training consists of different components, takes into account the specifics of human nature and the ability to assimilate the acquired skills. As cybersecurity experts, Kaspersky knows what cybersafe user behavior looks like. Using our insights and expertise, we've added learning techniques and methods to immunize our customers' employees against attacks while giving them the freedom to perform without constraints.

## Different training formats for different organizational levels




* "IT Security Economics 2022" Kaspersky
** Data Breach Investigation Report, 2022
*** «Balancing Risk, Productivity, and Security», Delinea 2021
**** Cost of a Data Breach, 2022. IBM
***** Capgemini "The digital talent gap"

# Kaspersky Security Awareness solutions

**Engagement & motivation**

Employees aren't always keen on compulsory training, and when it comes to cybersecurity, many consider it to be too complicated or boring, or believe that it has nothing to do with them. Without the motivation to learn, the learning outcome is unlikely to be very positive. Another challenge for those tasked with education is involving business executives in training, even though their mistakes can cost the company just as much as everyone else's. This is where gamification comes in – because it's so engaging, it's the most effective way to encourage your staff to overcome their initial resistance to training.

**76%** of CEOs admit to bypassing security protocols to get something done faster, sacrificing security for speed*.

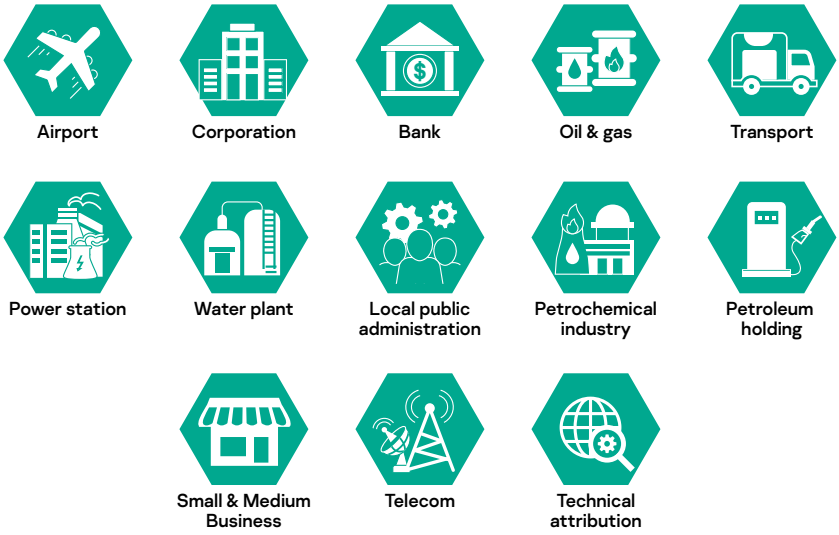
**62%** of managers admit that miscommunication regarding IT security within their organization led to at least one cybersecurity incident**

**KIPS training** is targeted at senior managers, business systems experts and IT professionals, to increase their awareness of the risks and challenges associated with using all kinds of IT systems and processes.

## Kaspersky Interactive Protection Simulation (KIPS): cybersecurity from a business perspective

KIPS is a 2-hour-long interactive team game that establishes an understanding between decision-makers (senior business, IT and cybersecurity officers) and changes their perceptions of cybersecurity. It presents a software simulation of the real impact that malware and other attacks have on business performance and revenue. It forces players to think strategically, anticipate the consequences of an attack, and respond accordingly within time and money constraints. Every decision affects all business processes – the main goal is to keep things running smoothly. The team that finishes the game with the most revenue, having found and analyzed all the pitfalls in the cybersecurity system and responded appropriately, wins.

## 13 industry-related scenarios
(with more being added all the time)




Each scenario demonstrates the role of cybersecurity in terms of business continuity and profitability, highlighting emerging challenges and threats and the typical mistakes that organizations make when building their cybersecurity. It also promotes cooperation between commercial and security teams, which helps maintain stable operations and sustainability against cyberthreats.

## KIPS is available in two flavors

The very popular KIPS Live option creates an indescribable atmosphere of excitement and enthusiasm thanks to the face-to-face competitiveness on-site. It's a great tool for engaging and building a culture of cybersecurity within an organization.

In the KIPS Online version users can interact with a large number of participants from anywhere. Perfect for global organizations or public activities, KIPS Online can be combined with KIPS Live to add remote teams to the on-site event.

- Up to 300 teams (= 1000 trainees) simultaneously, from any location.
- Different teams can choose a game interface in different languages.
- Customers can personalize pre-installed scenarios by determining the number and types of attacks in the game from the library.
- Another benefit of the online version is getting statistics on the players' choices, data about teams' actions in certain situations and a benchmark of player actions in relation to the previous game.

## KIPS for enterprises

Customers with a license that allows them to play KIPS as often as they like during the license period can play with the predefined settings, or personalize the game scenario every time they play, choosing and combining different attacks from the library. This functionality changes the game every time, making it even more interesting.

* https://www.forbes.com/sites/louiscolumbus/2020/05/29/cybersecuritysgreatest-insider-threat-is-in-thec-suite/?sh=466624f87626

** https://www.kaspersky.com/blog/speakfluent-infosec-2023/

**Starting point**

People are usually unaware of their level of incompetence, which makes them particularly vulnerable. They need to be tested, and they need to receive detailed and clear feedback on their level of cybersecurity competence for further training to be effective. This also ensures that time isn't wasted on material that is already familiar.

## **Gamified Assessment Tool**: a quick and exciting way to assess employees' cybersecurity skills

Kaspersky Gamified Assessment Tool (GAT) lets you quickly estimate the levels of your employees' cybersecurity knowledge. The engaging, interactive approach eliminates the boredom often found in classic assessment tools. It takes employees just 15 minutes to go through 12 everyday situations related to cybersecurity, assessing whether the character's actions are risky or not and expressing the level of confidence in their response.

After completion, users receive a certificate with a score that reflects their cybersecurity awareness level. They also get feedback on every zone, with explanations and useful tips.

GAT's gamified approach motivates employees while at the same time demonstrating that by resolving certain cybersecurity situations, there may be gaps in their knowledge. This is also useful for IT/HR departments to gain a better understanding of the cybersecurity awareness levels in their organization – and can serve as an introductory step to a wider education campaign.

**Learning**

Our online learning platform is the core of the awareness program. It contains **more than 300 cybersecurity skills** covering all the major IT security topics.
Each lesson includes cases and real-life examples so that employees can feel the connection to what they have to deal with in their everyday work. And they can use these skills immediately after the first lesson.

## **Kaspersky Automated Security Awareness Platform**: efficiency and ease of training management for organizations of any size

Kaspersky ASAP is an effective and easy-to-use online tool that shapes employees' cybersafety skills and motivates them to behave in the right way.

Although the training fulfils the security awareness needs for all companies, the automated management will appeal especially to those without dedicated training management resources.

### 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. The platform itself builds an education schedule for each group of employees, providing interval learning offered automatically through a blend of training formats.
- **Ease of use for administrators……:** Automated platform management, synchronization with AD (Active Directory), SSO (Single Sign-On), Open API (the ability to interact with third-party solutions), a user-friendly dashboard, online onboarding during the first visit, a FAQ section and tips – all make platform management convenient and efficient.
- **……and learners:** Clear lesson structure, bite-sized lessons, real-life examples, a user-friendly interface, email reminders, the ability to return and repeat lessons if necessary, PC or mobile friendly interface – all make the learning process enjoyable, interesting and effective.

**Kaspersky ASAP: easy-to-manage online tool which builds employees' cybersecurity skills level by level**

Topics covered in ASAP:

- Passwords & Accounts
- Email
- Websites and the Internet
- Social media & Messengers
- PC Security
- Mobile Devices
- Protecting confidential data
- GDPR
- Industrial Cybersecurity
- Personal data
- Bank card security & PCI DSS
- Doxing
- Cryptocurrency security
- Information security when working remotely
- Russian Federal law 152-FZ

**ASAP Express course**

A short version of the training in audio-visual format.

- Interactive theory
- Videos
- Tests

Kaspersky ASAP is a multi-language solution.

**ASAP is ideal for MSPs and xSPs** – training services for multiple businesses can be managed through a single account, and monthly license subscriptions are available.

Try 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!

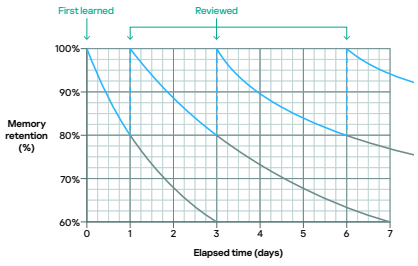
**Consolidation**

Reinforcement is an essential part of the learning program, and is necessary for cementing the knowledge and skills gained during learning.

The best way to turn learned skills into habits is to put them into practice. At the same time, people sometimes make mistakes and learn from personal experience. But when it comes to cybersecurity, learning from your own mistakes can be massively expensive.

Using gamified training, you can 'live' a situation and experience its consequences without causing any harm to yourself or your company.

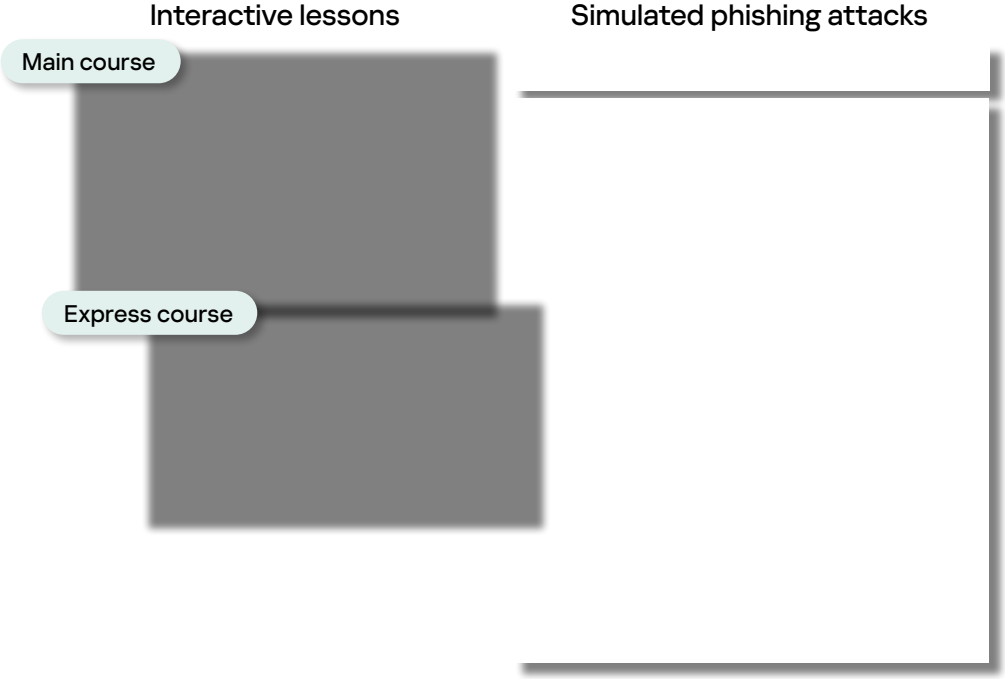
**70%**
**of what is learned**
is forgotten within one day in traditional forms of training




- **Predefined learning efficiency:** The 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.
- **Customization:** It's easy to change the appearance of the training program – replace the Kaspersky logo with your company's logo in the admin and learner portal and platform emails, customize certificates and add personal content to any lesson.
- **Flexible learning:** Choose the employee training option that's right for you – assign employees a basic Express course that will help you quickly meet regulatory requirements for cybersecurity training or update their knowledge, or choose the Main course broken down into complexity levels for more detailed and in-depth cybersecurity skills development.
- **Flexible licensing** (for Managed Service Providers): the per-user licensing model can start from as few as 5 licenses, and multiple companies can be managed from a single account.

## Simulated phishing campaigns

Simulated phishing attacks can be used before, during and after training, to test employees' ability to resist cyberattacks and help them, and company management, to see the benefits of training.




## Tracking results

You can follow employees' progression from the dashboard and assess the progress of the entire company, and all groups, at a glance. You can also dig down for more detail on an individual level.

**Specialized learning**

General IT specialists: helpdesks, and other technically savvy personnel are often left out of training because standard awareness programs are not enough for them, but companies also don't need to turn them into cybersecurity experts: it's too expensive, time consuming and unnecessary.

We are pleased to announce training that fills this gap – not as in-depth as expert training, but more advanced than training for ordinary employees.

**CITO training modules:**

- Malicious software
- Potentially unwanted programs and files
- Investigation basics
- Phishing incident response
- Server security
- Active Directory Security

**CITO delivery method:**

Cloud or SCORM format

# **Cybersecurity for IT Online**: the first line of incident defense

Cybersecurity for IT Online is interactive training for anyone involved in IT. It builds strong cybersecurity and first-level incident response skills.

The program equips IT professionals with practical skills to recognize a possible attack scenario in an ostensibly benign PC incident. It also fosters an appetite for hunting out malicious symptoms, cementing the role of all IT team members as the first line of security defense.

CITO also teaches investigation basics and how to use IT security tools and software, to equip your IT professionals with theoretical, practical and exercise-based skills, enabling them to collect incident data for handover to IT security.

This training is recommended for all IT specialists within your organization, but primarily service desks and system administrators. Most non-expert IT security team members will benefit from this course too.

**Getting executives on board**

Top managers are among the most desirable targets for cybercriminals, yet they're often a real challenge for educators. However, without their involvement and support for various cybersecurity initiatives and advocacy, it's impossible to create a cybersafety culture in the organization.

Cybersecurity is an important aspect of revenue generation along with project management, financial instruments, and business operational efficiency. This is the focus of our course for executives.

# **Executive training**:

In our executive training program, business leaders and top managers learn the basics of cybersecurity through a tutor-led interactive workshop or online course which gives them a better understanding of cyberthreats and how to protect against them.

Special attention is given to the financial aspects of cybersecurity and the feasibility of investing in it, giving C-level executives a better understanding of the connection between cybersecurity and business efficiency. They'll find out what the current threat landscape means for your business, what actions to take in the event of a cyberattack, plus a host of other interesting, relevant and useful information.

To get even more out of this course, it's ideal to combine it with KIPS training. Executive training can be taken before or after KIPS, depending on your Security Awareness approach.

* Current list of modules is available at cito-training.com

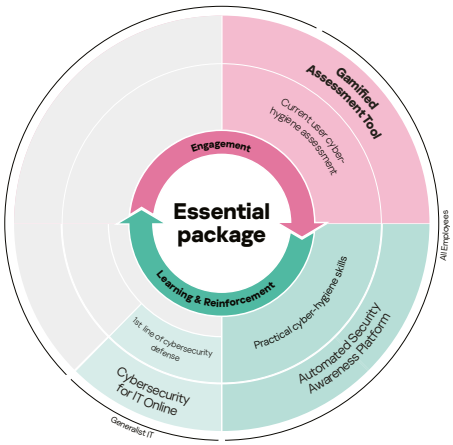
# **Kaspersky Security Awareness**: Flexible ways to train

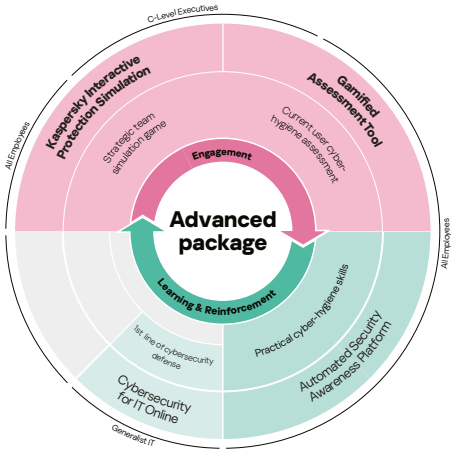
Kaspersky training solutions cover every level of your company and can be used on their own or collectively. We also make it easy to get started using packages tailored to your needs.

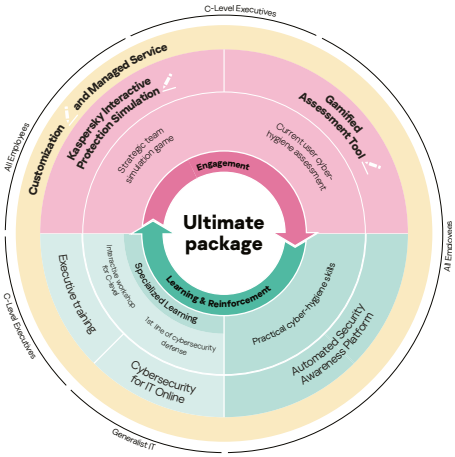
The hassle-free option to raise employees' cybersecurity awareness – simple to set up, easy to manage.
Provides a basic level of security training to help you operate successfully and meet regulatory or third-party requirements for general cybersecurity training.

Helps larger organizations maintain business continuity using a simple 'turnkey' training solution. Supports every organizational level and changes behavior by covering every stage of the learning cycle.

Ensures maximum cybersecurity awareness, featuring customization and managed services, so that executives are well-versed in threat scenarios, employees have automatic cybersafe skills, and generalist IT staff support you as the first line of defense.




Kaspersky Security Awareness training uses the latest training methods and advanced techniques to ensure success. Flexible new packaged solutions can be tailored to your needs, so there's a solution for everyone. Find out more at kaspersky.com/awareness

Kaspersky Security Awareness: kaspersky.com/awareness
IT Security News: business.kaspersky.com/

kaspersky.com



kaspersky