



---

Computer-  
based training  
programs for all  
organizational  
levels

# Kaspersky Security Awareness

# Kaspersky Security Awareness

## The effective way to build cybersafety throughout your organization

More than 80% of all cyber-incidents are caused by human error. A culture of cybersafe behavior together with fundamental cybersecurity skills and awareness throughout your organization are key to reducing the attack surface and the number of incidents you have to deal with. Organizations often struggle to find the right tools and methods for effective employee training that changes behavior for the better. The key to achieving this is to deploy training that uses the latest techniques and technologies in adult education and delivers the most relevant and up-to-date content.

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

### 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.

**52% of C-level executives** say employees are the biggest threat to operational security\*

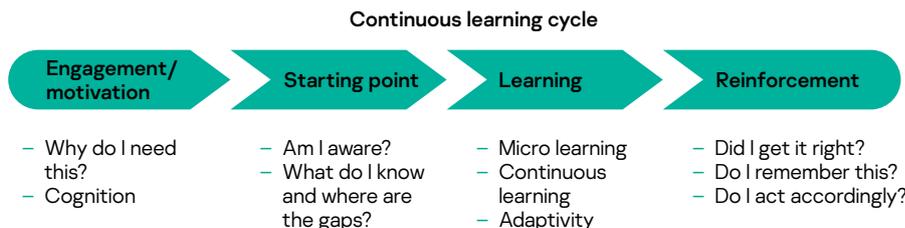
**43% of small businesses** suffered a security incident due to violation of IT security policies by employees\*\*

**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\*\*\*

Kaspersky Security Awareness offers a range of highly engaging and effective training solutions that 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.



### Key program differentiators



#### Substantial cybersecurity expertise

20+ 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.

\* "Weathering the Perfect Storm: Securing the Cyber-Physical Systems of Critical Infrastructure" report, 2020

\*\* 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...**



**\$1,315,000**

**per enterprise organization**

The average financial impact of a data breach caused by inappropriate IT resource use by employees\*

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



**50%**

**of businesses**

reported experiencing threats directly caused by inappropriate staff behavior, making this the most common threat to IT security\*



**86%**

**of companies**

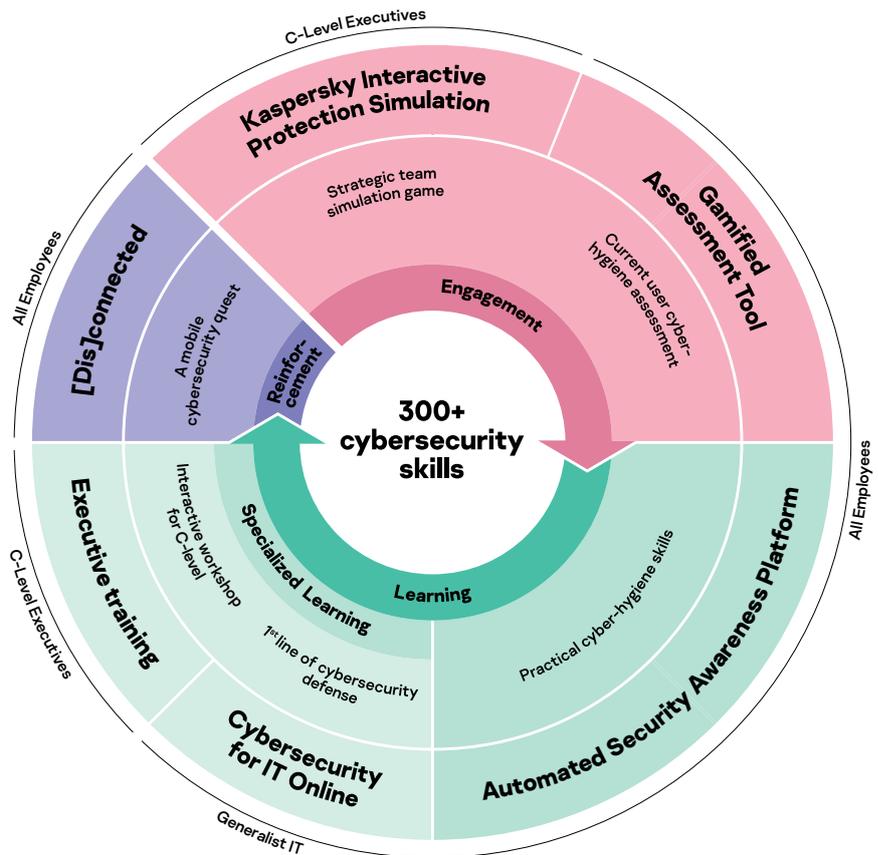
claimed that at least one person clicked a phishing link\*\*



**\$5,01 mil**

**the average cost per breach**

from BEC attacks (BEC - Business Email Compromise - is a type of phishing where attackers hijack or spoof legitimate corporate email accounts)



\* Report "IT Security Economics 2021", Kaspersky

\*\* Cybersecurity threats trends 2021, CISCO

\*\*\* Cost of a Data Breach, 2021. IBM

# Kaspersky Security Awareness solutions



## 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.

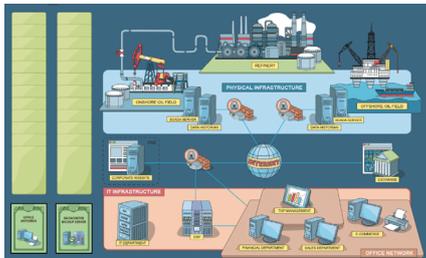
### 70% of what is learned

is forgotten within one day in traditional forms of training

### 42% of respondents working in companies with more than 1000 employees

said that the majority of training programs they attended were useless and uninteresting\*\*

**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)



Airport



Corporation



Bank



Oil & gas



Transport



Power station



Water plant



Local public administration



Petrochemical industry



Petroleum holding



Small & Medium Business



Telecom



Technical attribution

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.

## Customization of scenarios

From Q3 2022, for selected industrial scenarios, companies will be able to create their own game scenarios with different attacks. By using different attack combinations, companies with a KIPS enterprise license can play the same industrial scenario multiple times.

## KIPS Virtual Reality

**KIPS Power Station VR** is a new immersive experience in a realistic environment as close as possible to the real operations of a power plant. The technology allows managers to "work" as information security specialists, demonstrating the role of cybersecurity and its business impact visually, so they can see the consequences of their IT decisions in highly realistic 3D graphics rather than just have an abstract idea of them.



### 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 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

### ASAP Express course

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

- Interactive theory
- Videos
- Tests

Kaspersky ASAP is a multi-language solution.

## 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 builds an education schedule for each group of employees, providing interval learning offered automatically through a blend of training formats, including learning modules, email reinforcement, tests and simulated phishing attacks.
- **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.
- **Flexible learning:** choose the employee training option that's right for you: whether to assign employees a basic Express course that will help you quickly meet regulatory requirements for cybersecurity training or update their knowledge, or choose a 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.

**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](https://asap.kaspersky.com) – see for yourself just how easy it is to set up and manage your own corporate security awareness training program!

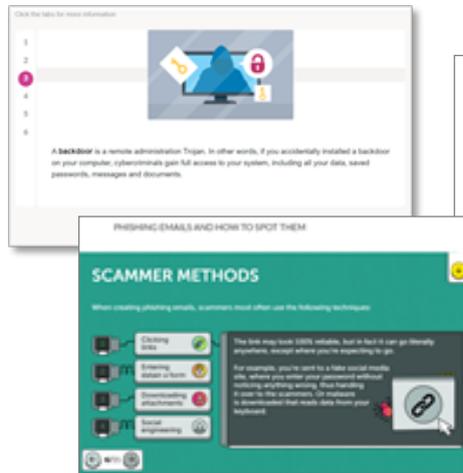
Main course

Express course

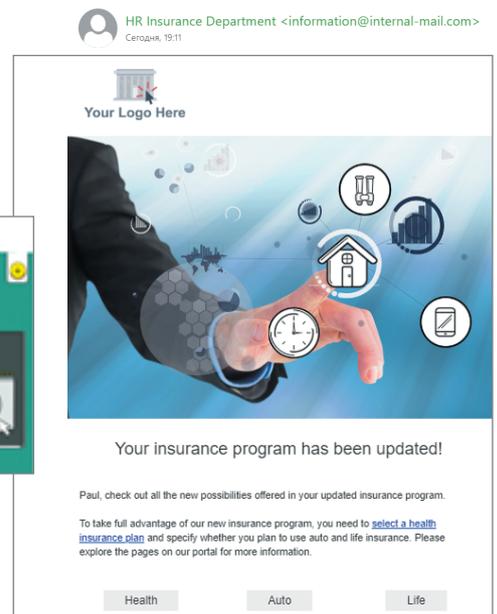
## Simulated phishing campaigns

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.

### Interactive lessons



### Simulated phishing attacks



## Track results

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



### Reinforcement

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.

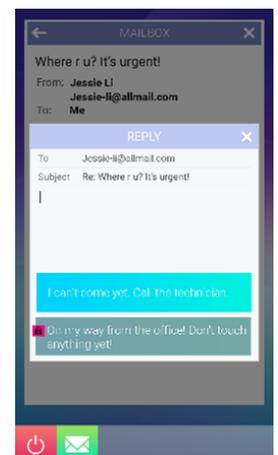
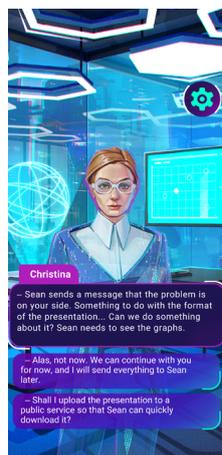
Using gamified training, you can 'live' a situation and experience its consequences without causing any harm to yourself or your company.

## [Dis]connected: a mobile cybersecurity quest

[Dis]connected is a highly immersive story-rich visual novel mobile cybersecurity game that challenges users with a quest to maintain a healthy work-life balance and be successful both personally and professionally.

Elements of cybersecurity are woven into the game's plot, and the game reveals how our decisions around cybersecurity can help to achieve – or spoil – these goals. There are 24 cases to solve, including topics on passwords and accounts, email, web browsing, social networks and messengers, computer security and mobile devices. Built-in emulated applications – messengers, banking apps, etc. – ensure a completely immersive experience.

At the close of the game, players receive a summary of how successfully they coped with the project and find out if their security skills are sufficient for today – and tomorrow.



The game runs on mobile phones. A **free demo** is available in Google Play and the AppStore: <https://kas.pr/mobilestores>



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

## Advanced 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

## Try one of the CITO modules for free:

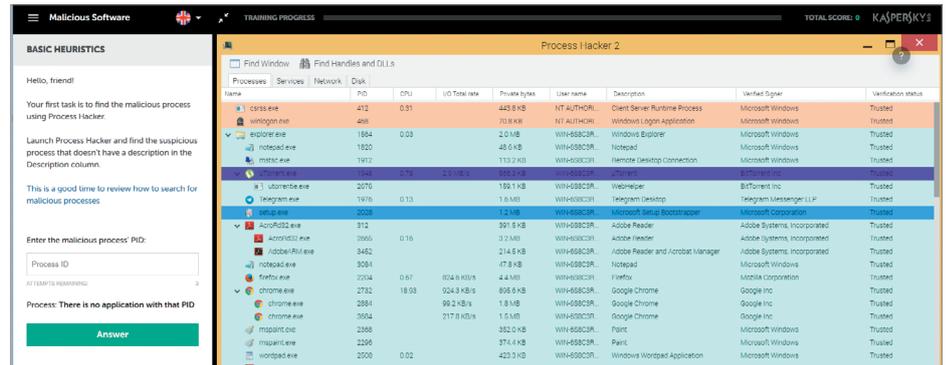
[cito-training.com](http://cito-training.com)

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.



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 cybersecurity 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: increasing business resilience for digital transformation

Business leaders and top managers learn the basics of cybersecurity through a tutor-led course which gives them a better understanding of cyberthreats and how to protect against them.

Research shows that there is a direct link between the speed and efficiency of incident response and the degree of damage an incident can cause. The course pays particular attention to the financial aspects of cybersecurity and the feasibility of investing in it, giving your C-level executives a better understanding of the connection between cybersecurity and business efficiency.

Kaspersky Interactive Protection simulation (KIPS) can be used in addition to this training to further consolidate the material through practical exercise.

## Course objectives

- Share the latest information on modern cyberthreats and their risks to business
- Bring learners up to date with the modern cyberthreat landscape
- Provide an opportunity to practice the basic rules of corporate and personal cybersecurity culture
- Ensure that the impact for business of the main regulatory issues in the field of information security is understood
- Clarify the basic concepts of cybersecurity, and the methods of protection against targeted attacks
- Give practical recommendations for corporate policy
- Advise on communications for responding to and investigating incidents

# Kaspersky Security Awareness: Flexible ways to train

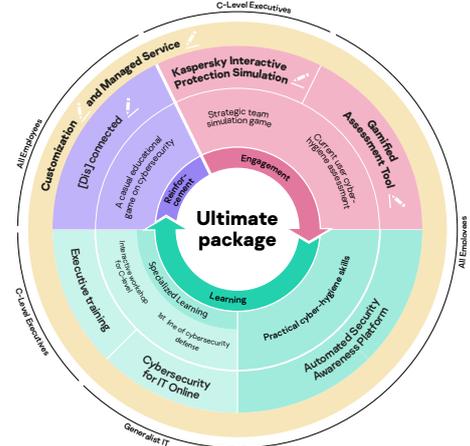
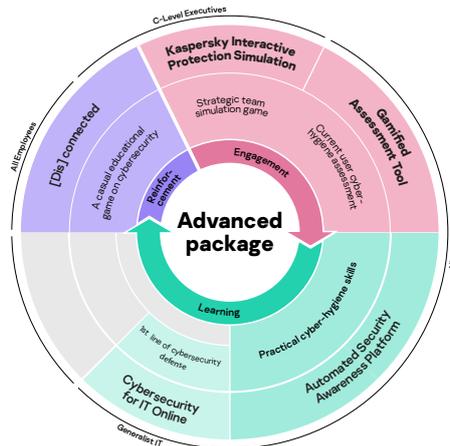
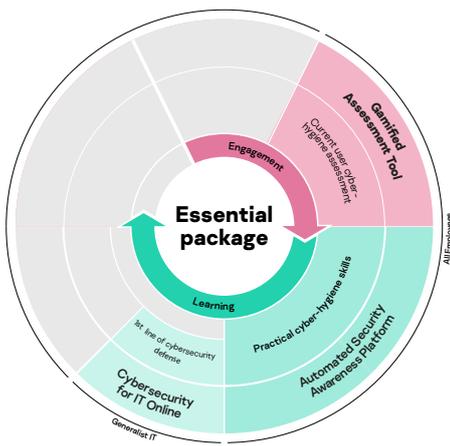
Kaspersky training solutions cover every level of your company and can be used on their own or collectively. We also make it easy to get started using packages tailored to your needs.

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](https://kaspersky.com/awareness)

---

Kaspersky Security Awareness: [kaspersky.com/awareness](https://kaspersky.com/awareness)  
IT Security News: [business.kaspersky.com/](https://business.kaspersky.com/)

**kaspersky.com**

© 2022 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owners.

**kaspersky** BRING ON  
THE FUTURE