Training programs to help you build a cybersafe organization

Kaspersky Security Awareness

kaspersky BRING ON THE FUTURE

Learn more on kaspersky.com

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 employs 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.

52% of companies regard employees as the biggest threat to corporate cybersecurity*

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 – a new approach to mastering IT security skills

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 that includes multiple components.

Continuous learning cycle

Engagement/ motivation	Starting point	Learning	Reinforcement
– Why do I need this? – Cognition	– Am I aware? – What do I know and where are the gaps?	– Micro learning – Continuous learning – Adaptivity	– Did I get it right? – Do I remember this? – Do I act accordingly?

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.

* Research: "The cost of a data breach", Kaspersky Lab, Spring 2018.

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

Employees make mistakes. Organizations lose money...

$1,195,000
per enterprise organization
The average financial impact of a data breach caused by inappropriate IT resource use by employees*

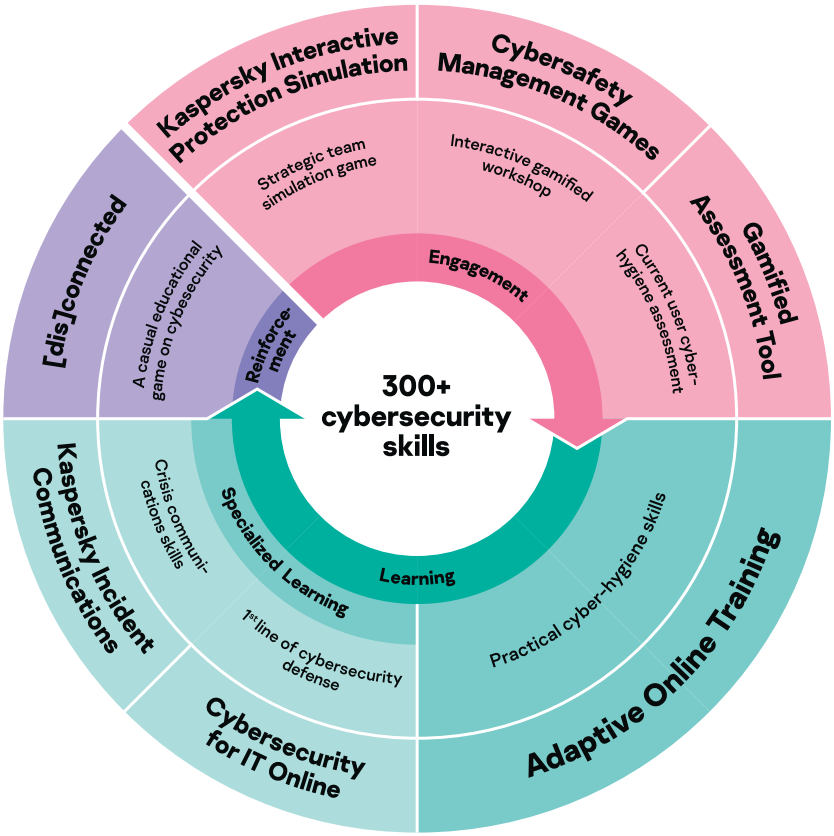
52%
of enterprise organizations
experienced cybersecurity incidents as a result of inappropriate IT resource use by employees **

More than $1,7Bln
global financial losses
resulted from business email compromise complaints***

Fueling motivation for effective security awareness

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



* Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives . Kaspersky Lab, 2019

** Report: "IT security economics in 2019', Kaspersky

*** FBI "2019 Internet Crime Report"

Kaspersky Security Awareness products

Engagement/ motivation

Starting point

Learning

Reinforcement

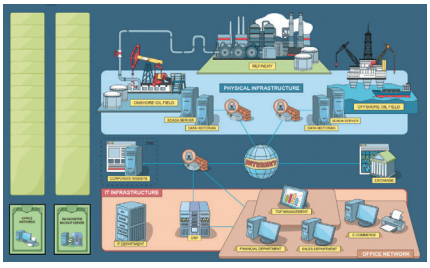
Motivation

Employees aren't always keen on more compulsory training, and when it comes to cybersecurity, many consider it 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**

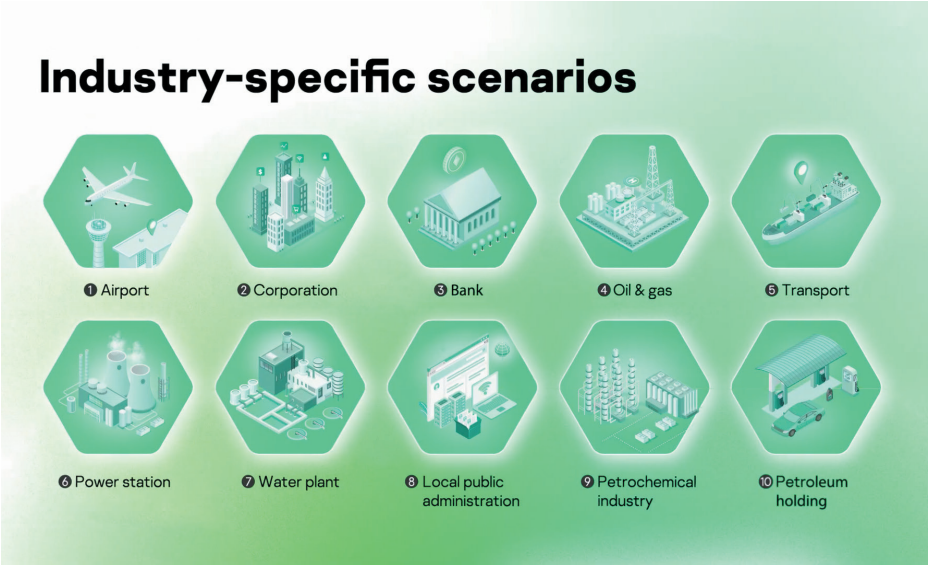
KIPS training is targeted at senior managers, business systems experts and IT professionals, to increase their awareness of the risks and challenges associated with using all kinds of IT systems and processes.



Kaspersky Interactive Protection Simulation (KIPS) strategic game: 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.

10 industry-related scenarios (with more being added constantly)



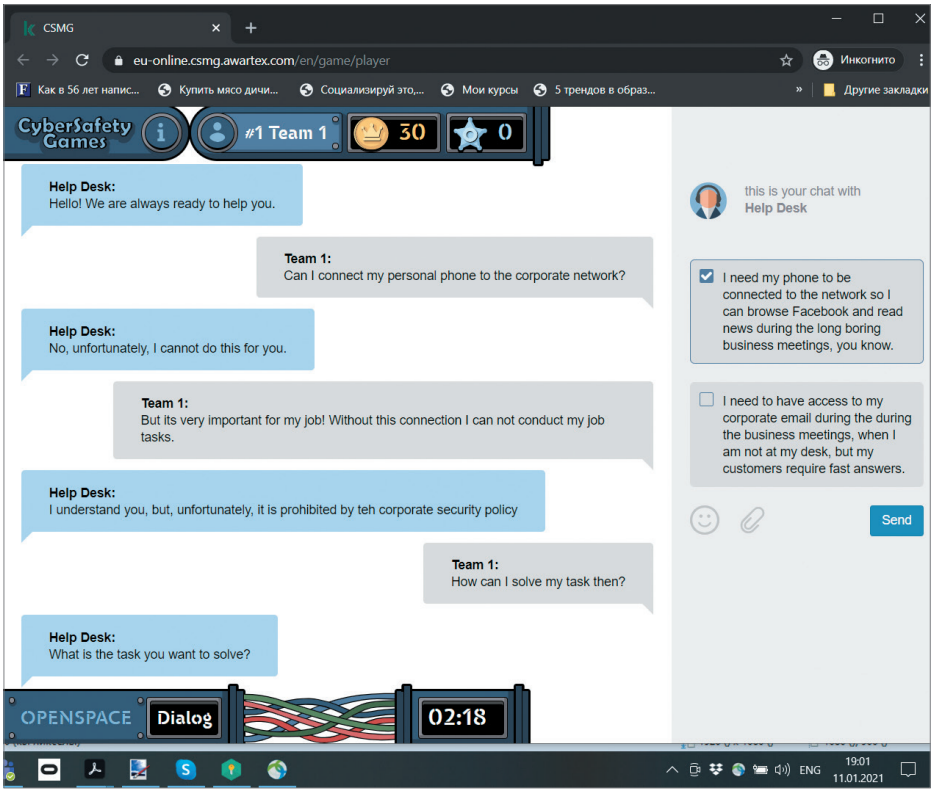
Each scenario demonstrates the true role of cybersecurity in terms of business continuity and profitability, highlighting emerging challenges and threats and the typical mistakes that organizations make when building their cybersecurity. It also promotes cooperation between commercial and security teams,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

Cybersafety Management Games: turning business leaders and line managers into proactive cybersecurity advocates

Cybersafety Management Games in an interactive workshop (combination of computer-based and instructor-led or fully online) that give line managers the competence, knowledge and attitudes essential to maintaining a secure working environment in their divisions, without sacrificing efficiency. The training turns line/ middle managers into cybersecurity supporters and advocates, making cybersafety a key ingredient of everyday decision-making.

* Ebbinghaus "Forgetting Curve"
** Capgemini "The digital talent gap"

During training, we identify the basic misconceptions that people usually have, and help managers to understand why employees tend to ignore cybersecurity rules and principles. Through specially designed exercises, we then demonstrate how to transform these misconceptions into positive, cybersafe behavior.



Engagement/ motivation

Starting point

Learning

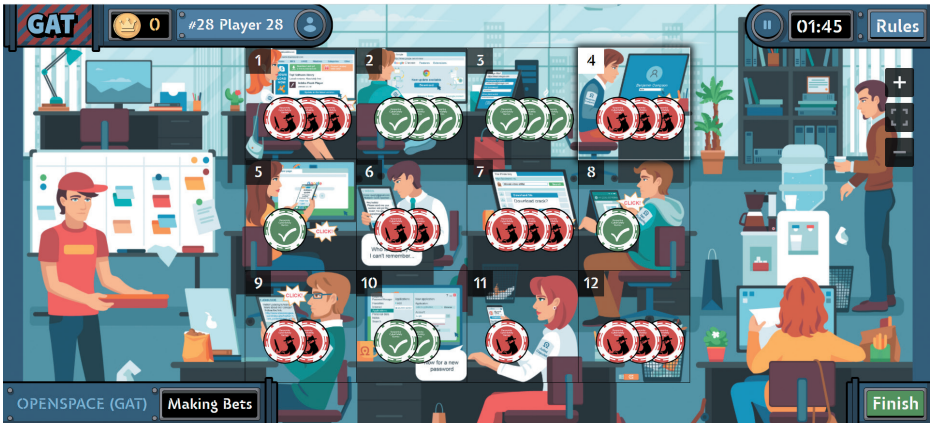
Reinforcement

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. Taking 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.



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.

Engagement/ motivation

Starting point

Learning

Reinforcement

Learning

Our online learning platforms are the core of the awareness program. They contain **more than 300 cybersecurity skills** covering all the major IT security topics, including Passwords & Accounts, Email security, Social networks & messengers, PC security, GDPR, etc.

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.

To maximize efficiency, we use adaptive technologies and build automated learning paths for every student, taking into consideration their initial level of knowledge and target level (the target level depends on the role each learner has in the company). This is hard graft, with many practical examples, a lot of explanations about WHY this is important, and numerous assessments that give immediate feedback on user actions.

"Ignorance more frequently begets confidence than does knowledge."
Charles Darwin, The Descent of Man

Topics covered in KAOT:
Passwords
- Email security
- Web browsing
- Social networks and messengers
- PC security
- Mobile devices
- GDPR

KAOT is currently available in: English, German, Italian, French, Spanish, Arabic, Russian.

Learn more: kaspersky.com/kaot

Kaspersky Adaptive Online Training: cybersecurity skills from a leading IT security vendor, supported by adaptive learning

Kaspersky Adaptive Online Training (KAOT) is unique solution combining content based on Kaspersky's 20+ years' experience in cybersecurity and an advanced learning & development methodology. KAOT is the result of a collaboration between Kaspersky and Area9 Lyceum, a leader in adaptive learning systems.

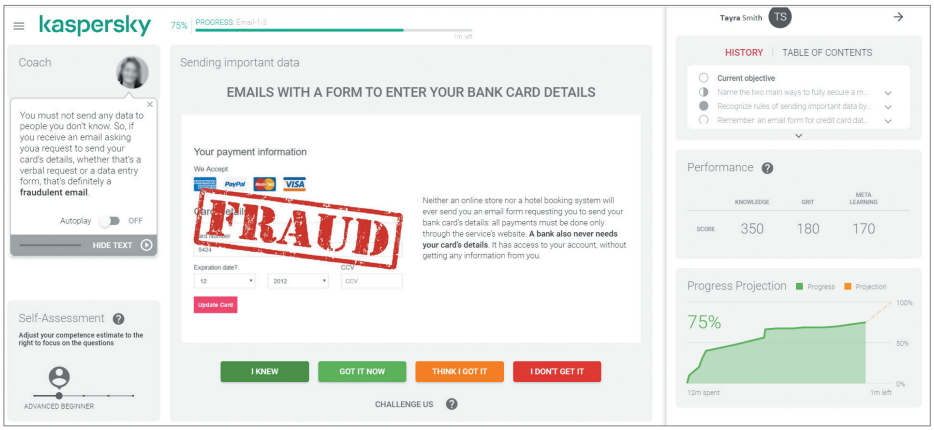
Grounded in innovative adaptive learning methodology, the cognitive-driven approach contributes to a personalized learning experience that takes into account the abilities and needs of each and every learner.

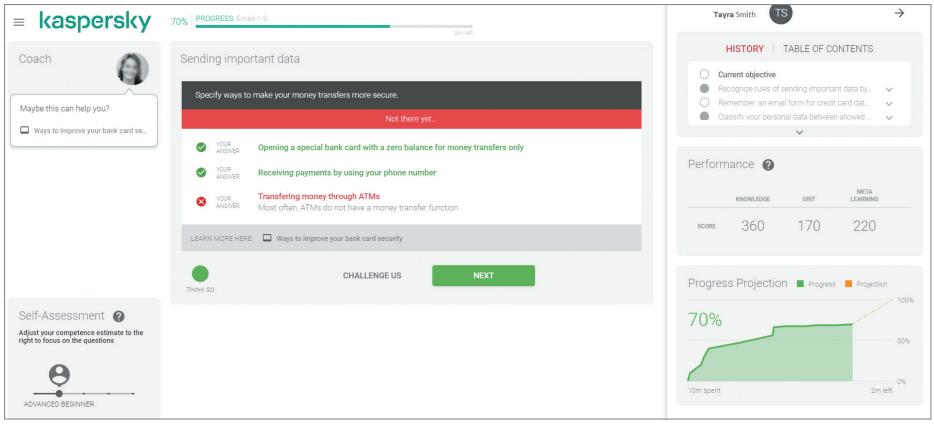
Key benefits

- **The one-on-one personal tutor approach** achieved as a result of using adaptive learning methodology
- **It uncovers and fixes unconscious incompetence** providing motivation for learning and ensuring sustainable cybersafe behavior. Being aware of what you don't know and what you need to improve on leads to mastery more quickly and more efficiently.
- **It eliminates boredom and frustration** through a personalized approach to each learner. Every lesson begins with a question followed by a theoretical lesson only when it's needed. Problem-based education boosts engagement and involvement in cybersecurity.
- **It ensures automatic, habitual use of skills** thanks to the adaptive algorithms that allows learners to move forward according to their competencies, using different approaches to the same topic when needed and constantly assessing whether the learner is progressing. The training fills skill gaps and builds greater competency quickly and effectively. At a high level of competency, certain knowledge becomes second nature, so actions become automatic and habitual, constantly reinforced by "refresh" activities when a learner may be at risk of forgetting the content.

Tracking results

Extensive statistics allow you to follow employee progression – performance summaries, reports and diagrams for groups and individuals. Admin can identify high performers as well as those who need additional coaching. Also see reports on user progress, progress of classes, and assignment details with indepth analysis of employee competence and metacognition.





Engagement/ motivation

Starting point

Learning

Specialized learning

Reinforcement

Specialized learning

Most enterprises provide cybersecurity education and training on two levels – expert training for IT security teams and security awareness for non-IT employees (Kaspersky has a comprehensive set of products for both). But what's missing? IT teams, service desks, and other technically advanced staff. Standard awareness programs are not enough for them, but companies still don't need to turn these employees into cybersecurity experts: it's not necessary, and is too expensive and time-consuming.

CITO training is conducted 100% online – participants just need an internet connection/ access to their corporate LMS and the Chrome browser.

Each of the 4 modules comprises of a short theoretical overview, practical tips and between 4 and 10 exercises – each practicing a specific skill and demonstrating how to use IT security tools and software in everyday work.

KIC training ensures that your crisis team:

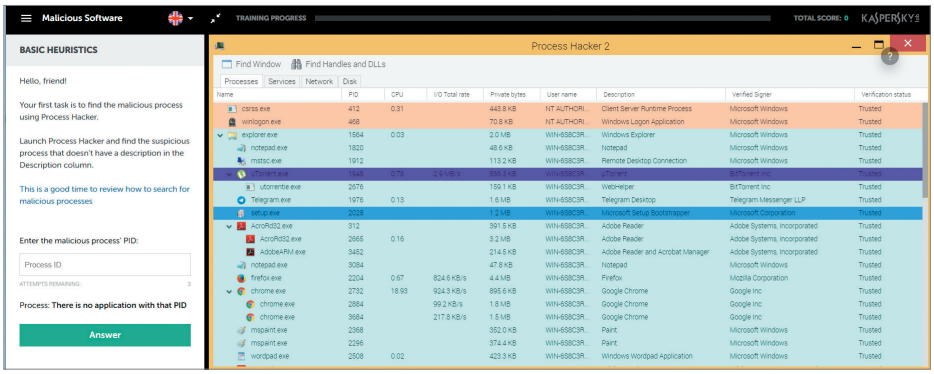
- Understands the cyberthreats heading your way
- Recognizes potential outcomes
- Can coordinate effectively with your IT security team
- Gains experience through cyber-incident simulation
- Knows what is essential, and safe, to say in internal and external communications in the wake of a cyberattack
- Updates and implements your cybercrisis communications plan

Cybersecurity for IT Online: the first line of incident defense

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

The program equips IT professionals with practical skills on how to recognize a possible attack scenario in an ostensibly benign PC incident, and how to collect incident data for handover to IT security. 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.
It consists of four modules: Malicious software, potentially unwanted programs and files, investigation basics, and phishing incident response.

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.



Kaspersky Incident Communications: empowering your corporate comms team to respond to a cyberattack

From the instant a cyber-incident is discovered, every action counts. How your communications are managed – externally and internally – is critical, particularly when dealing with unknown attack vectors and advanced persistent threats (APTs).

Kaspersky Incident Communications educates top management, information security and corporate communications professionals on how to handle crisis communications, including developing and applying appropriate assets. It helps build strong links between members of a crisis team and looks at how to prepare a crisis communications plan, providing practical recommendations, operation security procedures and tools for encrypting communication during a cyber-incident to support business continuity.

Engagement/ motivation

Starting point

Learning

Reinforcement

Reinforcement

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

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.

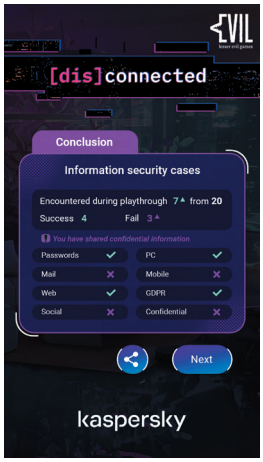
[Dis]connected: a casual educational game

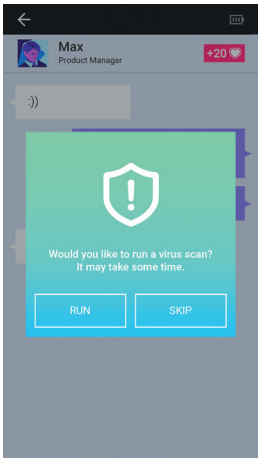
[Dis]Connected is a highly immersive story-rich visual novel cybersecurity game where users are challenged with a quest to maintain a healthy work-life balance and be successful both personally and professionally.

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 – the goals. There are 18 cases to solve, including topics on passwords and accounts, email, web browsing, social networks and messengers, computer security and mobile devices.

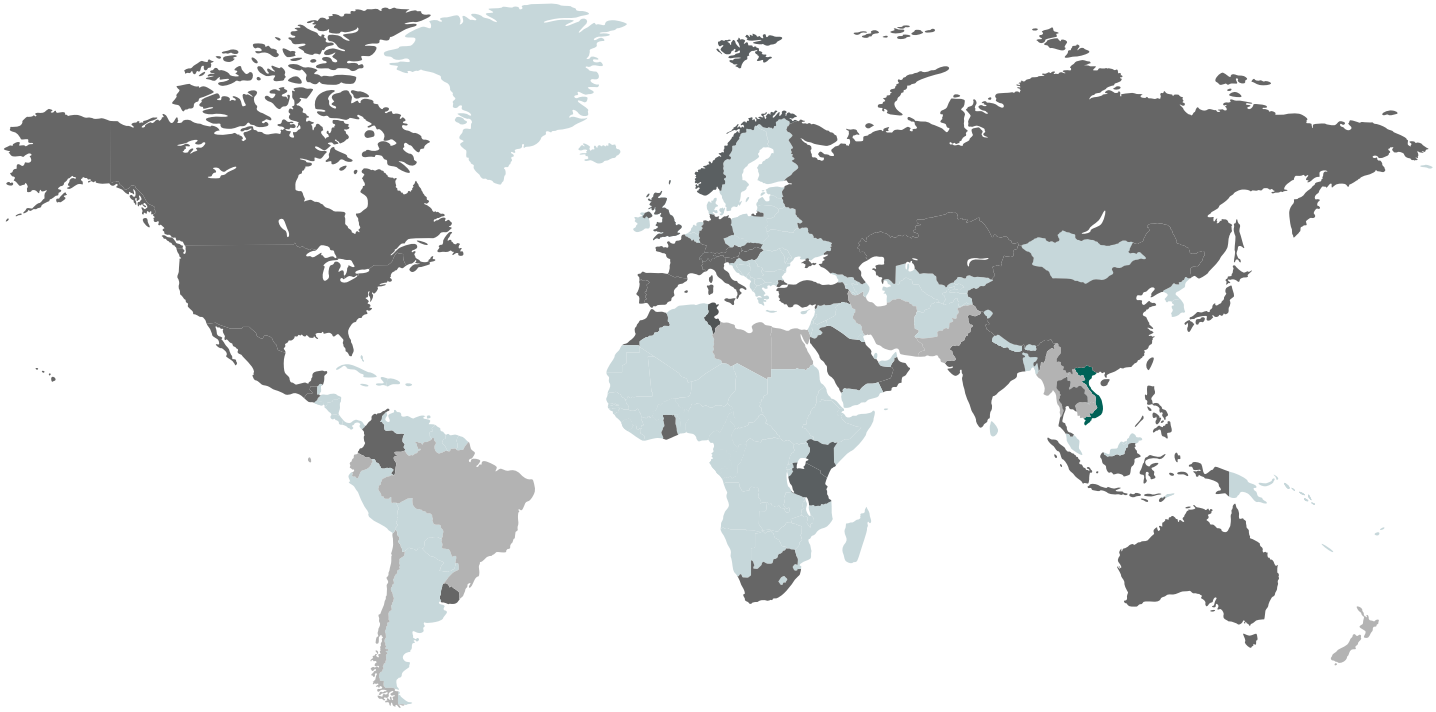
Built-in emulated applications – messengers, banking apps, etc. – ensure an even more complete immersive experience.

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.





Kaspersky Security Awareness worldwide



75
countries

>500,000
trained employees

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

kaspersky.com

kaspersky BRING ON THE FUTURE