Kaspersky Interactive Protection Simulation

Build cybersecurity awareness among top managers and decision-makers

kaspersky bring on the future

Learn more at
kaspersky.com/awareness

Kaspersky Interactive Protection Simulation

The "people problem"

One of the biggest security challenges faced by businesses today is that different senior management roles view cybersecurity from different perspectives, and have different priorities. This can result in a sort of decision-making "Security Bermuda Triangle":

- Businesses see security measures
- as being contrary to their business goals (cheaper/faster/better).
- IT Security Managers may feel that cybersecurity as an infrastructure and investment issue is outside their remit.
- Managers tasked with cost control may not see how cybersecurity spending relates to revenues and saves rather than generates cost.

Mutual understanding and partnership between these three are crucial for effective cybersecurity. However, traditional awareness formats, like lectures and red/blue exercises, are flawed: lengthy, overtechnical, and unsuited to busy managers, and they fail to build a "common language".

A company's cyber-immunity starts with the C-suites

For many companies today, looking after the sustainability of their IT infrastructure is a priority. However, dealing with cybersecurity issues is usually the responsibility of IT and IT security staff, which can create a fragmented culture of cybersecurity behavior within the business. Business leaders focus primarily on sales, customer experience, risks and costs, and often overlook cybersecurity as they work to achieve their goals. But without the support of the board, leading by example, creating a unified culture of cybersecurity can be unattainable.

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**.

51% of Information Security workers find talking about increasing budget for IT security most difficult.... but they're on the same page when it comes to workable communication strategies.

The majority of C-level **(56%) and IT (48%)** workers agree that providing real-life examples is the most efficient method to ease communication on IT security related issues**.

How Kaspersky Security Awareness helps

Kaspersky Security Awareness is a proven, efficient and effective solution with a long-standing 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 experience in cybersecurity with the Kaspersky Academy's extensive experience in adult education.

The portfolio is made up of engaging training products that **increase the cybersecurity awareness** of your employees at every level, empowering them to play their part in the overall cybersecurity of your organization.

Each product in the portfolio plays a specific role in the overall learning cycle – and is also available independently.

A strategic cybersecurity business game for executives

Kaspersky Interactive Protection Simulation (KIPS) is a strategic business simulation, a team game that demonstrates the connection between business efficiency and cybersecurity.

Participants are placed in a simulated business environment as members of the IT security team, where they're faced with a series of unexpected cyberthreats while having to keep the company running smoothly and earning revenue.

They must build a cyber-defense strategy by choosing from the best proactive and reactive controls available to them. Every choice they make changes the way the scenario plays out, and ultimately affects how much revenue the company does – or doesn't – make.

Balancing engineering, business, and security priorities against the cost of a realistic cyberattack, the teams analyze data and make strategic decisions based on uncertain information and limited resources. If this sounds realistic, it's because all the scenarios are based on real-life events.

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

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

KIPS is a dynamic awareness game with a "learning by doing" approach:

- Fun, engaging and fast (2 hours).
- Teamwork builds cooperation.
- Competition fosters initiative & analysis skills.
- Gameplay develops an understanding of cybersecurity measures.
- All scenarios and attacks are based on real-life cases

Why KIPS works

KIPS training is aimed at business system experts, IT people and line managers, to increase their awareness of the risks and security problems involved in running modern computerized systems.

Each team of 4-6 people is tasked with running a business that involves production facilities and computers controlling them. During the game, the production facilities generate revenue, public awareness, and business results. At the same time, the teams must deal with the cyberattacks threatening to impact the business's performance.

At the end of the game, players will have gained important and actionable insights that they can apply in their work.

- Cyberattacks hurt revenue, and must be addressed by top management
- Cooperation between IT and non-IT decision-makers is essential for effective cybersecurity within every business
- An appropriate security budget won't break the bank, but lost revenue as a result of a successful cyberattack can…
- People quickly become comfortable with security controls and their importance (audit training, anti-virus, etc.).

KIPS is available in two flavors:

The very popular **KIPS Live** option creates an atmosphere of excitement and enthusiasm, and is 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 wherever is convenient for them.

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.
- 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.
- 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 shows:

- The role cybersecurity plays in business continuity and profitability.
- The emerging challenges and threats faced by businesses.
- The typical mistakes companies make when building their cybersecurity.
- How cooperation between business and security teams helps to maintain stable operations and sustained protection against cyberthreats.

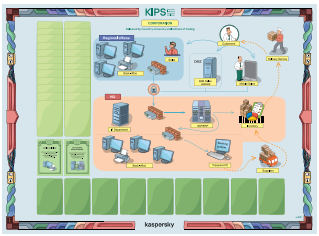
Depending on the scenario, the teams are responsible for the IT security of the company in that industry. Their task is to ensure the normal, uninterrupted functioning of the company, maintain relationships with customers and suppliers, and find and neutralize cyberthreats.

As the enterprise comes under cyberattack, the players experience the impact on production and revenues, and learn to adopt different business and IT strategies and solutions to minimize the impact of the attack without losing revenue.

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!**

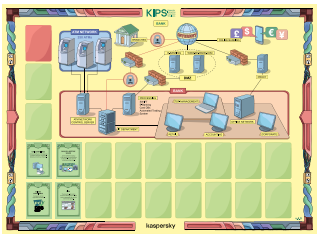
Enterprise KIPS scenarios for all vertical sectors

Corporation



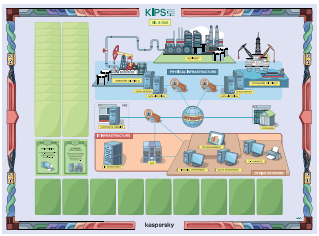
Protect the enterprise from **ransomware, APTs, automation security flaws.**

Bank



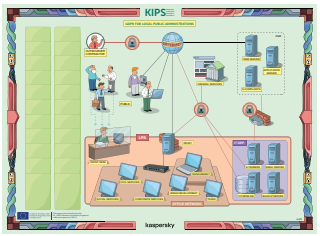
Protect financial institutions from **high-level emerging APTs, like Tyukpin, Carbanak.**

Oil & gas



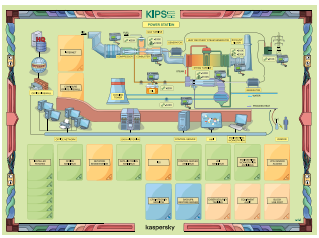
Explore the impact of a variety of threats – from **website defacement to a real ransomware and a sophisticated APT.**

Local public administrations



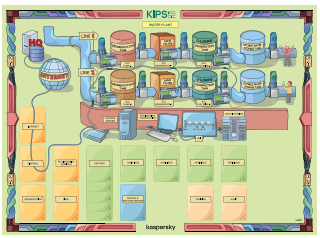
Protect public web servers from attacks and exploits.

Power station



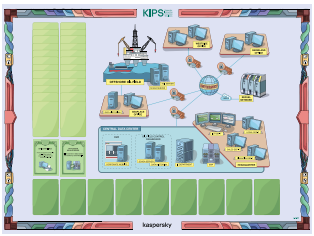
Protect industrial control systems and critical infrastructure from Stuxnet-style cyberattacks.

Water plant



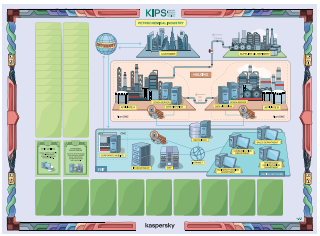
Protect the IT infrastructure of a water purification plant, ensuring the stability of two production lines.

Petroleum holding



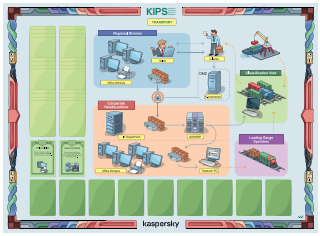
Preserve cybersecurity to protect the revenue of a global Oil&Energy company with offices across the world.

Petrochemical industry



Ensure the normal functioning of the new branch of a large petrochemical holding that focuses on ethylene production.

Transportation



Protect logistic companies from **Heartbleed, APT, B2B Ransomware, Insider.**

Airport

Ensure the safety of passengers and timely delivery of goods at the airport, protecting its assets from numerous cyberattacks and threats.

Technical attribution

Investigate and conduct a technical attribution of a complex APT attack on UN servers.

Small & Medium Business

Help SMBs protect their businesses from cybersecurity threats related to DDoS, Ransomware, Mobile App hack and Identity theft.

Telecom

Protect the assets of a large telecommunications holding consisting of a telecoms provider, a cloud service provider, a game developer and the HQ.

Want to get even more out of KIPS?

Why not round-out your KIPS experience with **Executive Training**, part of Kaspersky's Security Awareness portfolio? This training for managers can be taken before or after you've played KIPS, depending on your Security Awareness approach. Boost your KIPS experience by discovering 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. (Executive Training comes in two formats: an interactive offline workshop or via online course)

What KIPS users and customers say about the game

The Kaspersky Industrial Protection Simulation was a real eye-opener and should be made mandatory for all security professionals.

Warwick Ashford,
Computer Weekly

We at CERN have a huge number of IT and engineering systems, with thousands of people working on them. Thus, from a cybersecurity perspective, increasing awareness and engaging people to take care about cybersecurity is as crucial as the technical controls. Kaspersky training proved to be engaging, bright and efficient.

Stefan Luders,
CERN CISO

It was truly eye-opening and a number of the participants asked about using this game at their companies.

Joe Weiss PE,
CISM, CRISC, ISA Fellow

We have to build a network of people based on affiliation and cooperation and the KIPS is a perfect way how to kick it off.

Daniel P. Bagge,
Národní centrum kybernetické bezpeč nosti, Chezh Republic

How to prepare for a KIPS session

Schedule: Plan KIPS as a separate event or session within an existing event/ conference/ seminar (in this case, the optimum time for KIPS is on the evening of the first day).

Group: 20–100 people, split into teams of 3–4 people, ideally each team is a mix of people from Management, Engineers, CISO/ IT Security:

- it's best to have at least 1 member from each role/function,
- teams may consist of people from different or the same company/ department,
- it doesn't matter whether or not participants know one another.

Setup: The game takes 1,5 – 2 hours, but the room must be available to Kaspersky's facilitator team for 2 hours prior to the game for preparation and setup.

Room: Plan ~3m2/person, no columns, standard AV Equipment: Projector (6–8 lumens), Screen, Sound system (speakers, remote control, microphones).

Wi-Fi with internet access (for access to KIPS game server), from 4Mbps iPad per each team (4 persons) with Wi-Fi support or other tablet.

Furniture: Tables of participants for 4 people (rectangular size not less than 75x180 cm, or round with no more than 1.5 m diameter), Participants should sit in groups of 4 at the tables. Tables for co-host, chairs for all participants.

References and case studies

KIPS Game was played by industrial security professionals from 50+ countries.

- KIPS has been translated into English, Russian, German, French, Japanese, Spanish EU, Spanish LA, Portuguese, Turkish, Italian, Chinese, Dutch, Arabic;
- KIPS is used by numerous government agencies, including CyberSecurity Malaysia, the Czech Republic 's NSA, and Cyber Security Centrum in the Netherlands, boosting critical infrastructure awareness for hundreds of experts within national critical infrastructure organizations
- KIPS is licensed by leading education authorities such as the SANS Institute, where it is used in training for SANS students worldwide
- KIPS is licensed by security service providers and vendors, including Mitsubishi-Hitachi Power Systems where it's used in training for critical infrastructure customers
- KIPS is a part of the European Commission's Geiger project to train and protect small and micro enterprises from cyberthreats and improve their privacy management

Train-the-trainer available

If a customer wants to use KIPS to train a broader audience – a large number of employees, managers and experts from multiple departments or sites – it may be useful to purchase a license for KIPS training, to educate internal trainers and run KIPS sessions at the customer's own pace and convenience.

This type of license includes:

- The rights to use the KIPS training program internally.
- A set of training materials and the rights to use/reproduce it.
- Login/password for the KIPS software server for the duration of the license .
- Trainer's guide, education and training for program leaders on how to run and conduct KIPS training.
- Maintenance and support (updates and support for KIPS software and training content).
- Optional customization of KIPS Scenarios (an extra fee applies).

KIPS for partners and training centers

KIPS is a great opportunity for partners to benefit from Awareness solutions in a variety of ways. Not only can they sell it as a product – they can also sell it to their training center customers, or even conduct the sessions themselves. (Kaspersky's training specialists can upskill the partners for training if they choose that option.)

Kaspersky Security Awareness

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.

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

Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle that incorporates 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.

Continuous learning cycle

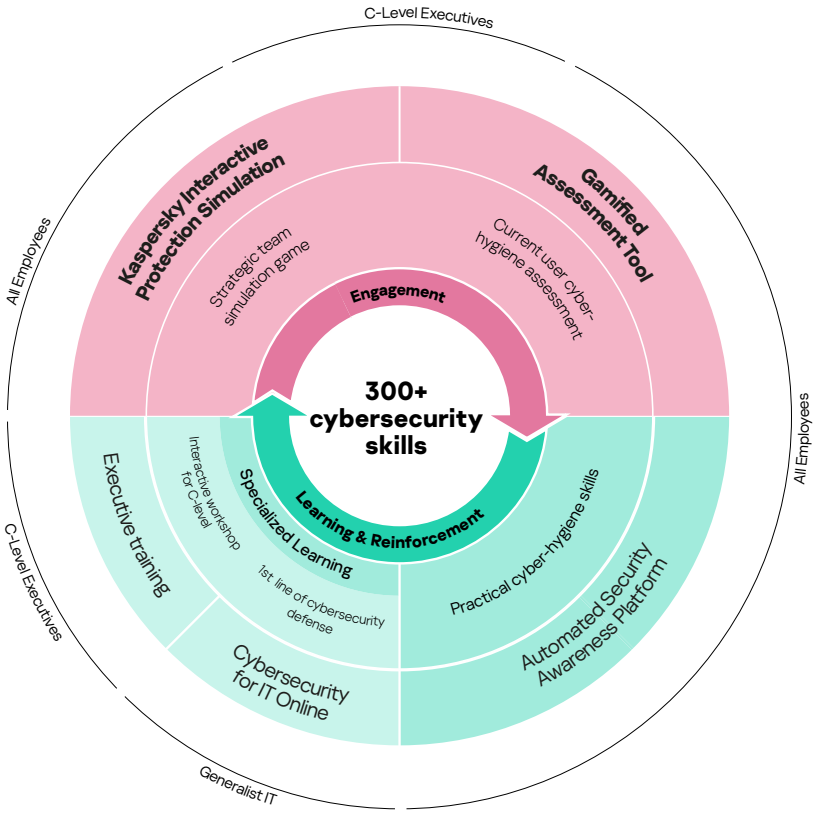
Engagement/ motivation
- Why do I need this?
- Cognition

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

Learning
- Micro learning
- Continuous learning
- Adaptivity

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

Different training formats for different organizational levels



Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness

www.kaspersky.com

kaspersky