Kaspersky Security Awareness

Building a culture of cybersafety that keeps your business secure

kaspersky cybersecurity true to business

Human error

is a top threat: on average, 64-86% of breaches involve non-malicious human actions[1]

$ 4.4 million

is the average cost of a data breach per organization[2]

Regulations require security awareness

as part of compliance: PCI DSS, ISO / IEC 27001, GDPR, NIS 2 and others require or strongly recommend security awareness programs to protect sensitive data

Building a security-conscious culture pays off

Kaspersky research shows that over 85% of employees who complete awareness training report improved vigilance and caution — a behavioral shift that helps prevent incidents.

92%

of user would recommend Kaspersky Security Awareness to others

3 million

employees have successfully completed our training programs

160+

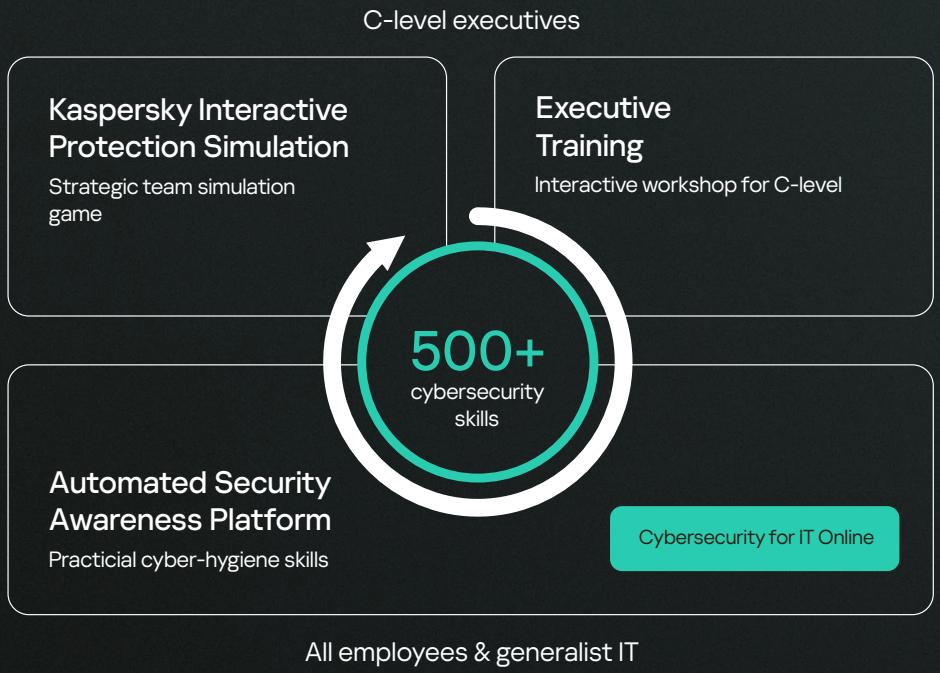
countries where organizations protect their employees with our training solutions

An effective approach to reducing human cyber risk

Build a culture of cybersafe behavior across your organization, supported by strong cybersecurity awareness and practical skills. This helps reduce the number of incidents caused by human error. The best way to address the human factor is through a structured training program that combines relevant, up-to-date content with the latest learning methods and technologies.

Kaspersky Security Awareness solutions

Kaspersky Security Awareness empowers businesses of all sizes across the world to increase cyber literacy among employees and foster a culture where security is everyone's responsibility. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with various tools and reinforcement materials: Kaspersky Interactive Protection Simulation, Executive Training, Automated Security Awareness Platform, and Cybersecurity for IT Online.



Why customers choose Kaspersky Security Awareness

Skills and confidence to spot and respond to real-world threats

Drawing on nearly 30 years of Kaspersky's cybersecurity expertise and live threat intelligence, we create highly relevant cybersecurity training content. As new threats emerge, our content evolves, helping ensure your employees are always prepared.

Accessible, interactive learning

Our training deploys interactive learning with a clear, logical structure that helps employees connect lessons to their daily tasks, improving understanding, retention and real-world application.

Lasting behavioral change

Our methodology reinforces new skills, provides continuous motivation, and helps embed learning into organizational routines. The result is a sustained shift in behavior, where secure practices become second nature.

Engagement across the board

From executives needing high-level, actionable insights to frontline staff requiring hands-on guidance, we deliver the right material, in the right format for every audience.

1 Kaspersky Human Factor 360 Report, Cybersecurity Ventures, Verizon Data Breach Reports
2 Cost of a Data Breach Report 2025, IBM

Kaspersky Automated Security Awareness Platform: Building a human firewall

Kaspersky Automated Security Awareness Platform (ASAP) is an online tool that delivers continuous training, equipping employees with skills and knowledge to recognize and stop real-world attack vectors.

Built by world-class experts, Kaspersky ASAP empowers your people and strengthens your business:

Reduces the number of human-related incidents and the resulting financial and reputational damage

Minimizes the risk of non-compliance fines by supporting regulatory requirements

Reduces the time and effort needed to manage awareness training and eases the burden on IT teams

Kaspersky ASAP is more than just an anti-phishing tool. The training maps to MITRE ATT&CK techniques, showing which human-driven attack vectors employees can help prevent. Examples include:

MITRE technique	Threat	Skills and behavioral outcomes
T1566 — Phishing	Malicious emails	Recognize and report phishing attempts
T1585 — Establish Accounts	Fake accounts/profiles	Verify authenticity before sharing info
T1199 — Trusted Relationship	Exploiting partner trust	Learn to question unusual requests
T1091 — Replication Through Removable Media	Removable media	Understand danger of malware on USBs
T1078 — Valid Accounts	Credential theft	Avoid giving access via social engineering

95%

of trained employees can now spot phishing attacks

20x

fewer data breaches when employees are consistently trained [1]

Key topics covered in ASAP include, but are not limited to:

- Email
- Passwords and accounts
- Websites and the internet
- PC security
- Confidential data
- Personal data
- Physical data security
- GDPR
- Artificial intelligence and neural networks
- Attacks on top managers
- Mobile devices
- Social media & messengers
- Supply chain attacks
- Industrial cybersecurity
- Bank card security and PCI DSS
- How to respond to incidents
- Vishing

Empower your employees to become an extra layer of protection alongside technical tools.

Start trial

1 2025 Kaspersky Automated Security Awareness Platform Research

Content and methodology that sticks, to retain knowledge and apply skills

Expert driven

Content built on almost 30 years of cybersecurity expertise and a competency model covering practical, essential cybersecurity skills across multiple topics.

Varied content

Supports knowledge retention through interactive modules and exercises, real-world cases, tests, videos and multi-scenario phishing simulations.

Wide range of customization options

Add your logo, brand certificates, enrich lessons with internal slides, documents or policies, add custom SCORM/PDF modules and adjust test structures.

Human centric

Designed around how people absorb, retain and apply information

How it works

Everyone in your organization needs cybersecurity awareness, but the depth of that knowledge varies by role and risk profile. This is where one-size-fits-all training fails. Our platform helps your team build more than 500 practical skills, group staff effortlessly, and assign the right training for each participant in just a few clicks using the components below.

Main course

Gain in-depth knowledge through micro lessons organized by complexity level.

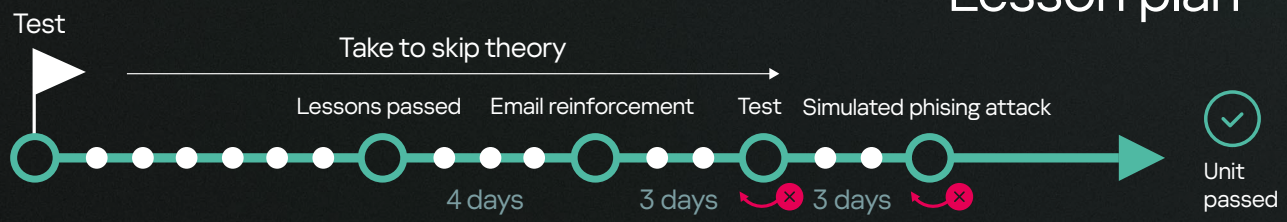
Express course

Meet cybersecurity training compliance requirements quickly or refresh knowledge with short, highly engaging audio-video training.

Phishing simulator

Run simulated phishing attacks before, during and after training, to test employees' ability to resist cyberattacks.

Lesson plan



Blocks with different types of activities to maximize memorization

Easy-to-manage solution for organizations of any size

Simple onboarding

Register online and get demo access for up to five users for two months. Includes a "how to start" guide and online support

Full automation

Training modules, tests and phishing simulations are assigned automatically, aligned with training group settings

Proactive human risk management

Seamless integration with Kaspersky SIEM and XDR, and APIs for integration with third-party applications provides the full picture of employee behavior and assign training based on real security events directly from the console

Multi-tenant support and flexible admin roles

Ideal for organizations with subsidiaries and distributed teams, enabling centralized oversight while delegating management to local admins.

Automated user grouping based on custom predefined rules

Organize by role, department or risk profile

Clear reporting

Dashboards provide essential data with drill-down views of each employee's progress, delays or underperformance, with a ready-to-send PDF report for management in one click

Flexible deployment

Available as a SaaS platform or on-premises installation

Seamless enrollment

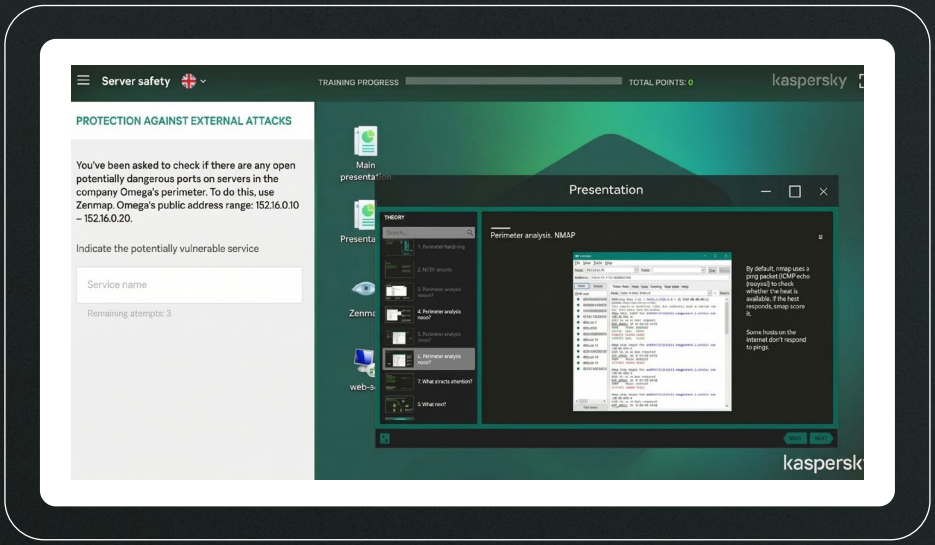
Integrates with Active Directory and SSO

Cybersecurity for IT Online

Cybersecurity for IT Online (CITO) is an interactive training program that empowers service desk specialists, system administrators and non-specialist IT security team members with practical skills to detect hidden cyberattacks in everyday PC incidents, collect relevant data and act as the first line of cybersecurity defense.

Practical skills for first-level incident response:

- Learn to detect, analyze and respond to malware, potentially unwanted programs, exploits and phishing attacks
- Apply real-world tools and techniques to strengthen IT infrastructure security and investigate incidents effectively
- Develop skills in log analysis, digital evidence collection and threat investigation
- Learn to secure servers and Active Directory through hardening, policy configuration and monitoring



Participants progress through six modules combining concise theory, practical tips, and 4–13 exercises per module focused on real-world IT security tools and everyday tasks.

Malicious software	Potentially unwanted programs and exploits	Server security
Investigation basics	Phishing and open-source intelligence	Active Directory security

Kaspersky Executive Training

Drive a top-down security culture by showing how executive decisions directly influence risk posture, regulatory compliance, and long-term organizational resilience.

Kaspersky Executive Training is a live workshop for business leaders and top managers that explains what the current threat landscape means for your business, what actions are needed in the event of a cyberattack, and much more. Beyond core cybersecurity principals, participants gain critical insight into the financial viability of security investments, empowering C-level leaders to connect protection with business performance. It is ideal to combine this training with KIPS.

Critical business-related aspects of cybersecurity explained in clear, accessible, non-technical language:

- Gain an understanding of cybersecurity as part of an overall system
- Learn how cyber risks affect business operations and how they can be managed
- Understand the role of senior management in cybersecurity governance

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

KIPS increases awareness of the risks and challenges associated with using all kinds of IT systems and business processes. It is a two-hour interactive team game targeted at senior managers, business systems experts and IT professionals. The industry-specific scenarios expose participants to modern attack techniques observed by Kaspersky experts in active campaigns, including supply chain attack, exploitation of third-party access, social engineering, or malware. Working under time and budget constraints, teams must strategize, anticipate the impact of security incidents, and respond effectively to protect business performance and revenue.

- Establishes an understanding between decision-makers
- Helps visualize cybersecurity risks and map them directly to revenue and operations
- Engages teams with cybersecurity issues and fosters a security-first culture

14 industry-specific 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
- IT

KIPS Live

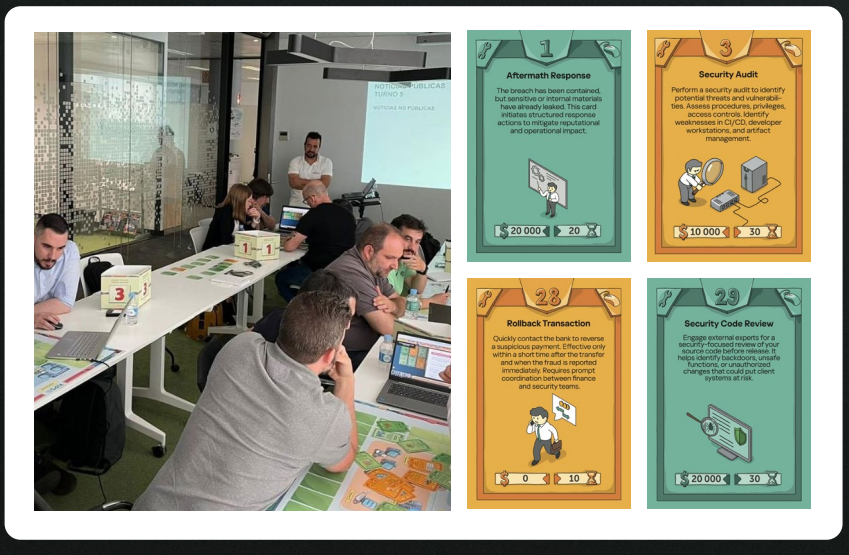
An entertaining activity that can be played as a standalone event or as a session within an existing conference, seminar or corporate event.

- Up to 100 participants, 4–5 people in each team
- On-site facilitator and training assistant

KIPS Online

An online version is perfect for global organizations or public activities. It can also be combined with KIPS Live to include remote teams to an on-site event.

- Up to 300 teams (1000 participants) from any location



KIPS customization options

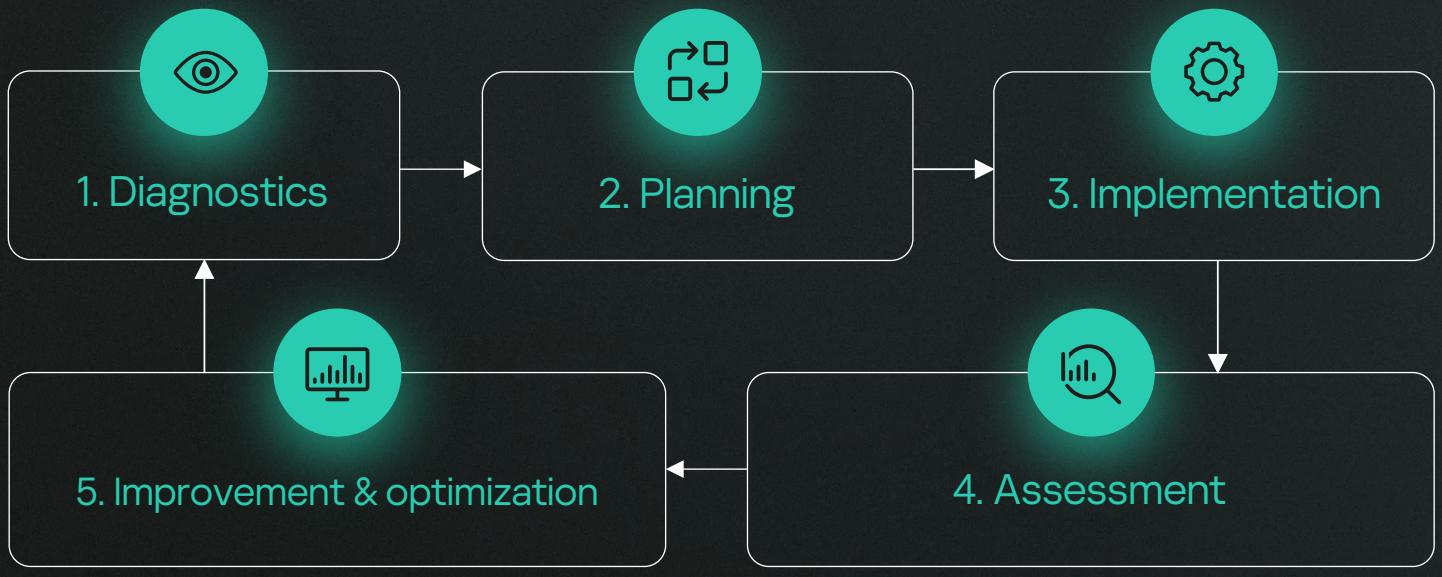
- Co-branded or customer-branded boards, cards, and table numbers
- A unique scenario, built in partnership with Kaspersky, that can mirror your network, past incidents or your specific industry's threats

Building a culture of cybersafety

True cyber resilience isn't just about policies and technologies — it's about culture. And culture is shaped by how people act, how leaders lead, how processes are designed, and how technology enables it all:

- People & behavior
- Leadership & cooperation
- Operational integration
- Security enablement & readiness

A sustainable cybersafe culture is achieved through ongoing commitment. That's why we've developed a systematic approach built on five essential steps where you can use Kaspersky Security Awareness solutions.



What is the current cybersafety culture maturity level in your organization?

0 Fragmented
Risk: The absence of basic practices and structures creates a high level of vulnerability. Even a minor incident can lead to serious consequences.

1 Aware & reactive
Risk: Only explicitly prescribed rules are followed. In non-standard situations, employees act according to their own judgment.

2 Managed
Risk: The number of incidents is decreasing, but the system remains vulnerable to more complex scenarios.

3 Integrated
Risk: Processes seem fine, but if cyber culture does not function as a self-regulating system, a "lag risk" remains.

4 Resilient
Result: The number and severity of incidents continue to decline. The organization can adapt quickly to the evolving threat landscape.

When security stops being a campaign and becomes culture, risk decreases — and results follow.

CISO

Customer Engagement Services

Start building a cyber-resilient culture by aligning people, processes and technologies with Kaspersky ASAP.

Try now

Kaspersky Security Awareness

Be aware. Stay safe.

www.kaspersky.com

#kaspersky
#cybersecuritytruetobusiness