One for all

Cyber threats come in many forms.
So should your company-wide training.

kaspersky BRING ON THE FUTURE

Kaspersky Security Awareness Training

Reduce the 90%[1] human error threat across your organization

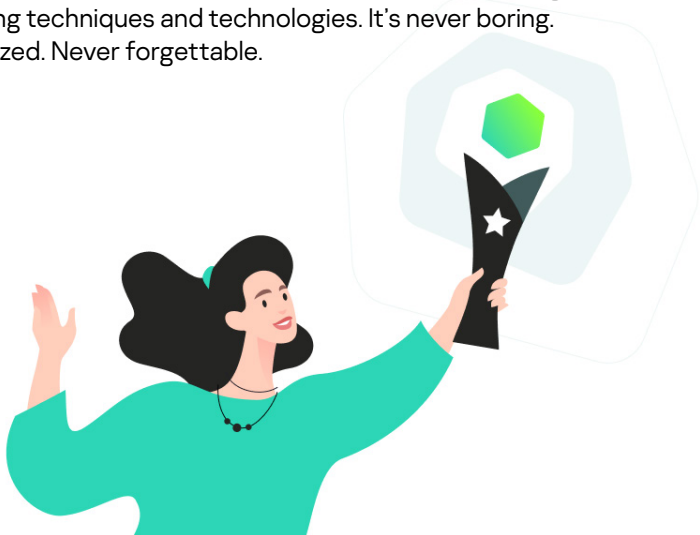
Everyone works differently and has different skills – but when it comes to security, anyone in your organization can be a cybersecurity risk.

Even with just basic cybersecurity skills, employees can protect their companies from cyber attacks. Cyber criminals are more likely to exploit employees who have low levels of security awareness than write complicated code to hack complex cybersecurity systems. Google has registered 2,145,013[2] phishing sites as of January 17, 2021, which are designed to exploit 'the human factor'. And with the average financial impact of data breaches at $1,195,000[3] per enterprise organization, the value of security awareness training is unmistakable.

Despite this, only about 60%[4] of organizations provide employees with formal security awareness training that is mandatory for all employees. And in 10%[4] of organizations where security training programs are available, they are only optional.

Kaspersky believes the problem is a lack of appropriate security learning technology. Changing employees' behavior is a big challenge for many companies – yet the vast majority of classroom and online training solutions are one dimensional, and don't permanently change security behavior for the better.

Kaspersky Security Awareness training changes that. Its diverse range of solutions cover all the security-specific needs of enterprises and teaches the skills everyone should possess, using the latest learning techniques and technologies. It's never boring. Never standardized. Never forgettable.



[1] 'Sorting out a Digital Clutter', Kaspersky Lab, 2019
[2] Blog: Tessian 'Phishing Stastics', 2020
[3] Kaspersky Lab, 2019
[4] Mimecast Security Awareness Training Statistics, 2018

One flexible training solution for all

52%[5] of companies
regard employees as the biggest threat to corporate cybersecurity

60%[6] of employees
have confidential data on their corporate device (financial data, email database, etc.)

Our Security Awareness training builds a safer working environment throughout your organization.

We have training that's right for every tier of your organization, from C-Level and IT professionals to employees of all levels. Learning is tailored to different requirements for having cybersecurity training and uses a mix of engaging techniques, from a tutor-like learning approach to gamification, which leverages our natural desire for learning, mastery and competition – the perfect way to motivate employees to think about the value of security awareness.

And since this is Kaspersky Security Awareness training, you can be confident you're training the right skills, thanks to our deep understanding of employee security needs. We'll help you change employees' behavior – giving your people freedom to work safely without constraints.

[5] Research: 'The cost of a data breach', Kaspersky Lab, Spring 2018
[6] 'Sorting out a Digital Clutter', Kaspersky Lab, 2019

Good for C-Level executives

58%[8] of C-Level executives

claim that IT security is too complex

42%[9] claimed

IT security is a low priority for them

60%[10] of IT leaders

say C-Suite executives are the most likely to be targeted by a malicious cyberattack

76%[11] of CEOs

admit to bypassing security protocols to get something done faster, sacrificing security for speed

28%[12] of C-Level executives

have requested to bypass security protocols in their organizations

Challenging cybersecurity perceptions through teamwork and simulation

There's little point in training hundreds of employees to be security aware, yet neglecting senior managers, business systems experts and IT professionals.

Organizations need to drive understanding of the corporate and financial damage caused by security breaches, such as the dangers of sharing passwords or the threat of phishing, from the top.

C-Level executives will also be responsible in investing in training that keeps their organization safe. The percentage of employees protected by organizations' cybersecurity programs ranges from 85% to just 56%.[7]

Motivating and effective

Kaspersky will give your C-Level executives a better understanding of the connection between cybersecurity and business efficiency. For example, with **Executive Training**, business leaders and top-managers learn the basics of cybersecurity through a tutor-led course which empowers them with a better understanding of cyber threats and ways to protect against them.

In addition to **Executive Training**, or taken entirely separately, we have interactive team games like **Kaspersky Interactive Protection Simulation (KIPS)** which put learnings into action. Designed specifically for decision-makers, KIPS is an interactive team game that challenges perceptions of cybersecurity and leads to better cooperation between different levels of your organization.

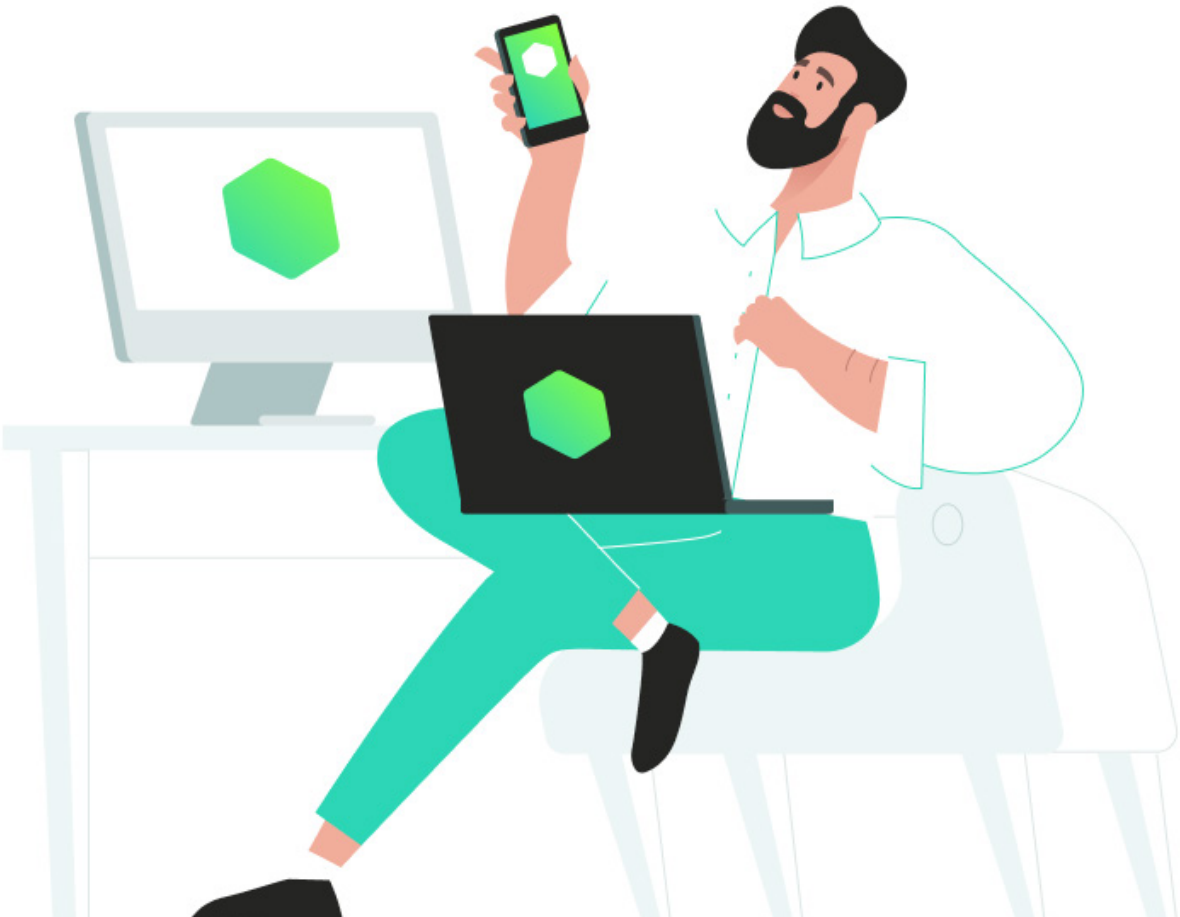
[7] Accenture Cybersecurity Report 2020
[8] Study: MobileIron 'Trouble at the Top'
[9, 10, 11] Forbes 'Cyberscurity's Greatest Insider Threat Is In The C-Suite', 2020
[12] Study: MobileIron 'Trouble at the Top'

In this training session, your executives will anticipate the consequences of an attack, respond within time and money constraints, and adapt to the industry-specific scenarios Kaspersky has created – from security challenges in banking and corporations to transport and utilities.

KIPS is also supported by a **Cybersafety Management Game** for your line managers and middle management – to train them as cybersecurity supporters and advocates and make cybersafety a key ingredient of everyday decision-making.

Immerse your senior executives in training as they've never experienced it before.

KIPS training screenshot: Power Station Virtual Reality



Good for all employees

42%[13] **of respondents**

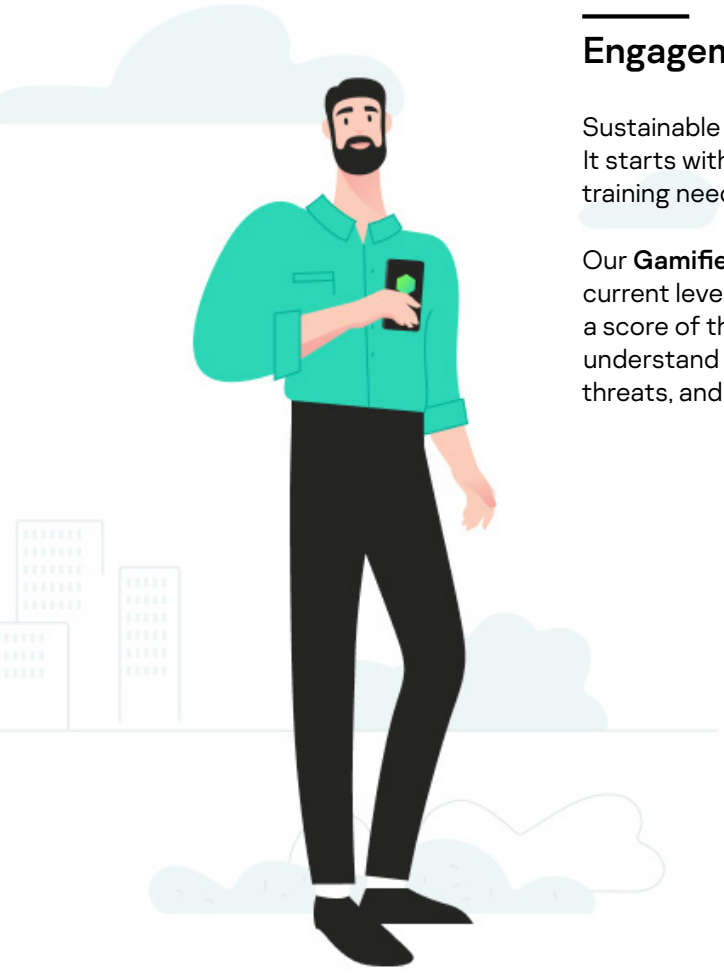
working in companies with more than 1,000 employees said that the majority of training programs they attended were useless and uninteresting

75 countries

have adopted our training solutions

500,000+
trained employees

keep their organizations safer using Kaspersky Security Awareness training



Personalized training that builds lasting skills

For the majority of the workforce, organizations need to build lasting security awareness skills that are used 'automatically' whenever and wherever a potential security issue arises.

That's a challenge for two reasons: people are generally not motivated to change their habits; and most training doesn't do a good job of engaging and developing skills.

Kaspersky has applied its 20 years' experience in cybersecurity and understanding of advanced learning to help you overcome these issues – and deliver training that is more effective, engaging and easy for your company to manage.

Engagement from the start

Sustainable changes in employees' behavior takes time. It starts with engagement and defining what your employee training needs are.

Our **Gamified Assessment Tool (GAT)** quickly measures the current level of employees' cybersecurity skills and provides a score of their security awareness level. You can then understand your company's readiness to face and resist cyber threats, and implement appropriate Kaspersky training.

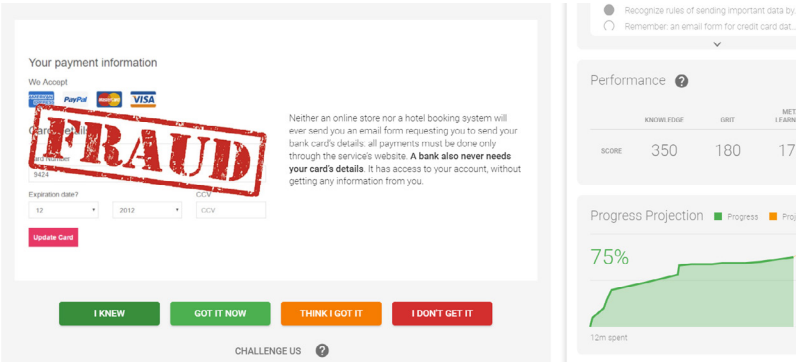
[13] Capgemini 'The digital talent gap'

Gain skills with adaptive learning

Kaspersky Adaptive Online Training (KAOT) delivers the content of every lesson using adaptive learning and an advanced learning algorithm to guide learners through topics.

KAOT is unique in teaching 300+ cybersecurity skills using a scientific approach, which ensures the safe actions of employees become automatic and habitual in the workplace.

KAOT monitors progress and adjusts training according to correct answers and how confident you are as training progresses.



KAOT training screenshot

Employees needn't miss out on rich gamification either. **Kaspersky [Dis]connected** – educational casual video game – is an additional training solution that will cement knowledge and skills gained during training with KAOT.

Good for Generalist IT

100% online:
participants just need an internet connection

4 modules
including a short theoretical overview and practical tips

4 to 10 exercises
in specific skills and use of IT security tools and software

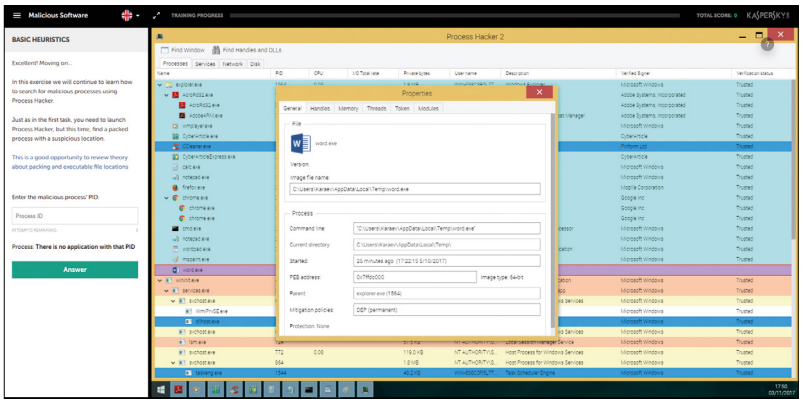
Build first-level incident response skills

IT teams, service desk staff and other non-expert security staff often fall through the skills gap for security training. They may be too knowledgeable for general security awareness training, yet they still require specialized training since they are your first line of incident defense.

Kaspersky created **Cybersecurity for IT Online (CITO)** to fill this important gap. Our training teaches your generalist IT staff how to recognize a possible attack scenario manifesting as a benign PC incident.

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

This is a great way to further protect the organization at a crucial incident defense level, without the expense of training your staff to expert levels.



CITO training screenshot

CITO fosters an appetite for hunting out malicious symptoms, cementing the role of your IT team members as the first line of security defense.

Good for Information Security and Corporate Communications

Improve handling of crisis communications

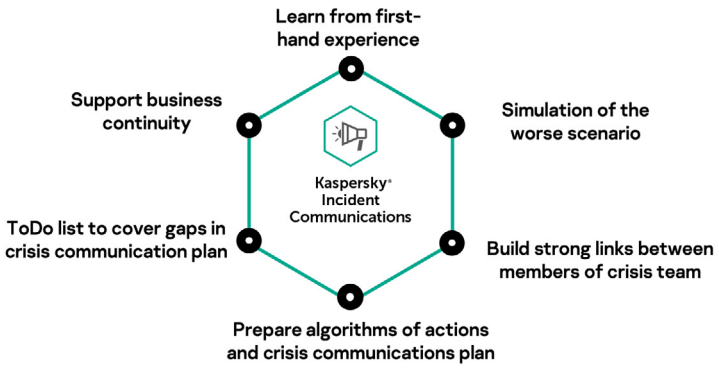
Does your corporate communication team know how to respond to a cyberattack? It's not a commonly trained skill, yet it's essential when an external or internal cyber-incident or advanced persistent threat (APT) is discovered.

Your people need to know how to react internally and externally to the cyber-incident, and that requires management and crisis communications skills.

Kaspersky Incident Communications (KIC) will upskill your corporate communications team to operate optimally by using simulations to help them understand how to behave while under attack. It also shows how to coordinate effectively with your IT security team during a cyber-incident – including how to develop and apply assets which will minimize reputational damage and financial losses.

All of this valuable knowledge can be included in a crisis communications manual: so you build better PR crisis communication skills that will support business continuity.

What is the value?



KIC training screenshot

KIC ensures that your crisis team understands the cyber threats heading their way through cyber-incident simulation.

Good for Information Security and Corporate Communications

Real-life

Training materials based on a real-life targeted attack, which was mitigated and successfully made public.

Professional

Created by world famous security experts and top PR professionals.

Prepared

Your organization creates or updates a cyber crisis communications plan which your incident response team can follow.

Conclusion

Cyber threats come in many forms and they are now deliberately targeted at your people as the weakest link in your cybersecurity chain.

One size doesn't fit all, so you need training that creates a safe working environment at every level of your organization – in both management and non-management roles.

With a wide range of solutions designed for the needs of enterprises, learning tailored to different roles, and engaging training methods that build skills fast, Kaspersky Security Awareness is the one flexible training solution that changes cybersecurity behavior quickly and effectively.

Talk to one of our experts or Find a Partner to discover how Kaspersky Security Awareness solutions can improve your corporate security strategy

Get in touch.