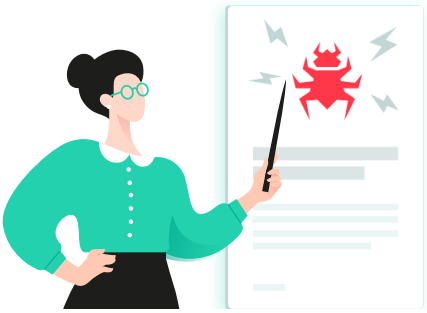
Kaspersky Adaptive Online Training

Cybersecurity skills from
a leading IT security vendor,
supported by adaptive learning

kaspersky BRING ON THE FUTURE

KAOT: Kaspersky Adaptive Online Training

More than 80% of all cyber-incidents are caused by human error*, and enterprises lose millions recovering from these incidents. Employees are the main gateway into the organization for attackers – but properly trained, cyber-aware staff who practice cyber-hygiene can also become a very effective first line of defense. There are various training programs on the market, but a very traditional approach often fails to achieve the desired motivation and behavioral changes to be effective.



"Ignorance more frequently begets confidence than does knowledge."

Charles Darwin,
The Descent of Man

Why is traditional awareness training often ineffective?

Many awareness solutions help companies to adhere to compliance standards for security awareness, but in fact they don't change employees' behavior and don't ensure long-lasting use of acquired skills. Among the main reasons why training fail with their mission are:

- **Doesn't ensure the progress of each individual**
  A 'one-size-fits-none' approach, whether online or classroom-based, fall short. The more employees in the program, the more difficult it is to create a curriculum that takes into account their individual abilities and characteristics.

- **Training takes too much time**
  If an employee has already mastered a skill, there's no option to skip those lessons, making the training long and tedious to get through.

- **Employees aren't motivated to learn**
  People don't always recognize their knowledge needs, and think they know something when they don't. This results in unconscious incompetence where employees aren't motivated to learn something because they think they already have those skills and learning them is a waste of time, even when it's not.

- **Content isn't engaging**
  Training is often generalized rather than personalized and interactive, so it's not engaging and struggles to achieve skills retention. Videos, games, and online course-style training have their place, but they don't restructure individual learning paths according to personal knowledge levels and contribute to true mastery of the materials.

Why should enterprises consider Kaspersky when looking for a security awareness training provider?

Kaspersky has expanded its portfolio with a product specifically tailored for enterprises – Kaspersky Adaptive Online Training (KAOT). KAOT is the result of collaboration between Kaspersky and Area9 Lyceum, a leader in adaptive learning systems.

KAOT training is unique solution combining content based on Kaspersky's 20+ years' experience in cybersecurity and an advanced learning & development methodology.

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. The individual learning path fosters retention and automatic skills use that changes employee attitudes and habits sustainably, protecting enterprise cybersecurity from human error.

* CybSafe analysis, ICO

What distinguishes KAOT from other offerings?

- **Kaspersky Cybersecurity skillset:** based on our vast experience in cybersecurity, we have identified a set of skills that every employee should possess in order to operate IT safely at work. This skillset forms the content of the training.
- **Adaptive learning system:** by adjusting a learner's current level of knowledge and creating a customized learning path for each person, the adaptive learning algorithm makes sure that the learner masters the skills until they become automatic.

"Each problem that I solved became a rule, which served afterwards to solve other problems."

Rene Descartes,
Discourse on Method

What makes the KAOT solution so effective?

- **One-on-one personal tutor approach**
  One of the main components of this efficiency is a personal tutor-like approach that's achieved as a result of using key elements of learning science: problem-based learning, keeping the learner at just the right difficulty of study throughout, using different approaches to the same topic and constantly assessing the learner's progress.
- **Saves employees' time**
  The training suggests a personalized approach for each employee, depending on their current level of skills, confidence in these skills/ knowledge and their ability to absorb information, so they can learn without wasting time on what they have already mastered[1].
- **Boosts internal motivation**
  Adaptive learning can identify areas in which people are unconsciously incompetent – i.e. they think they know something, but in fact they don't! By identifying how familiar a learner is with a topic, they are provided with explanations and help only when they need it. Eliminating tiresome repetition helps improve internal motivation.
- **Immersive learning process**
  The platform uses formative assessment teaching by asking questions that ensure that the learner has learnt everything and that the knowledge it not only acquired, but anchored. No overtraining or excessively long and tiring learning modules. Reinforcement and knowledge refreshment of those topics that an employee found most difficult contribute to making use of the skills automatic.

1 Training time cut by up to 50% compared to traditional online or classroom training

How does adaptive learning work?

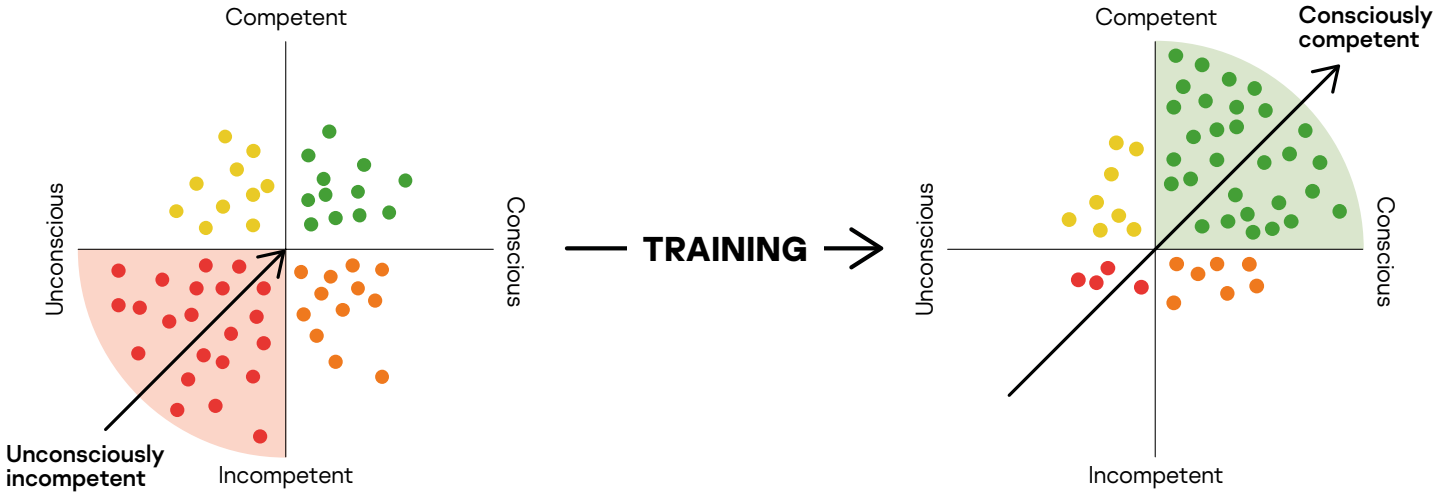
An innovative cognitive approach lies at the heart of the adaptive learning. It's grounded in research on human factors and adaptive algorithms and contributes to a personalized, tutor-like teaching experience at scale that take into consideration the abilities and needs of each learner. It allows learners to move forward according to their competences, using different approaches to the same topic when needed and constantly assessing whether the learner is progressing. By building an individual learning path, training fosters greater competency in cybersecurity essentials, contributing to a safe corporate cyber environment.

The KAOT platform uses algorithms to evaluate the learner constantly and adjust the learning path accordingly. It moves steadily from unconscious incompetence to conscious competence, which gives learners more awareness and greater confidence in what they know, resulting in better application of cybersafe behavior in their everyday work, leading to better business outcomes.

Automaticity is the ability to do things without occupying the mind, allowing it to become an automatic response pattern or habit

KAOT adapts to the learner, presenting content only when necessary; students receive follow-up in areas in which they struggle, filling skill gaps and building greater competency quickly and effectively. At a high level of competency, certain knowledge becomes second nature, allowing actions to become automatic and habitual. This level of knowledge mastery is known as "automaticity." KAOT builds automatic cybersafe behavior that is constantly reinforced by "refresh" activities when a learner might be at risk of forgetting the content. The result is an optimized path to learner proficiency.

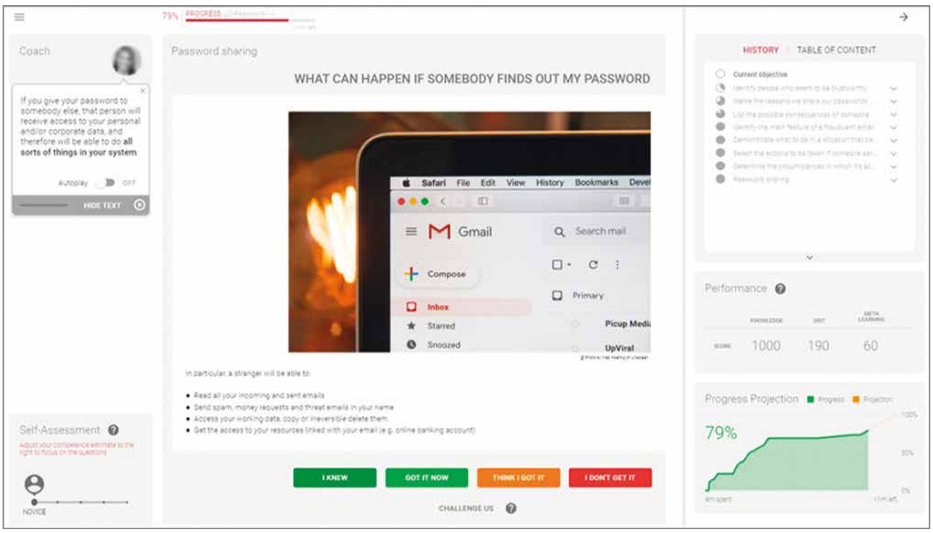
Training efficiency ensured by methodology



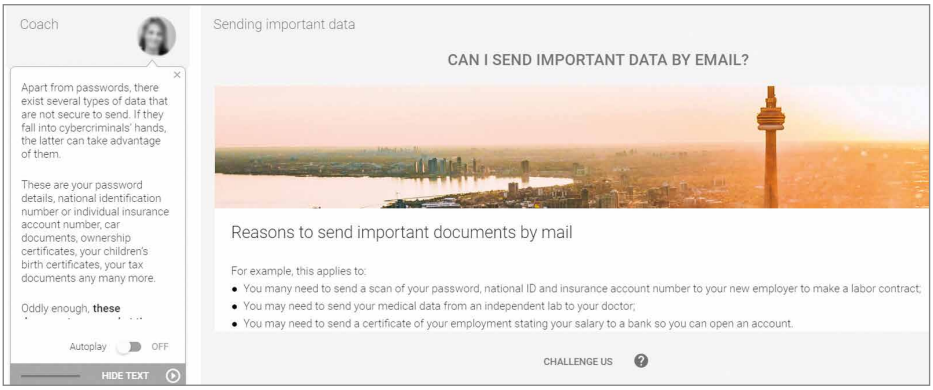
How is the training structured?

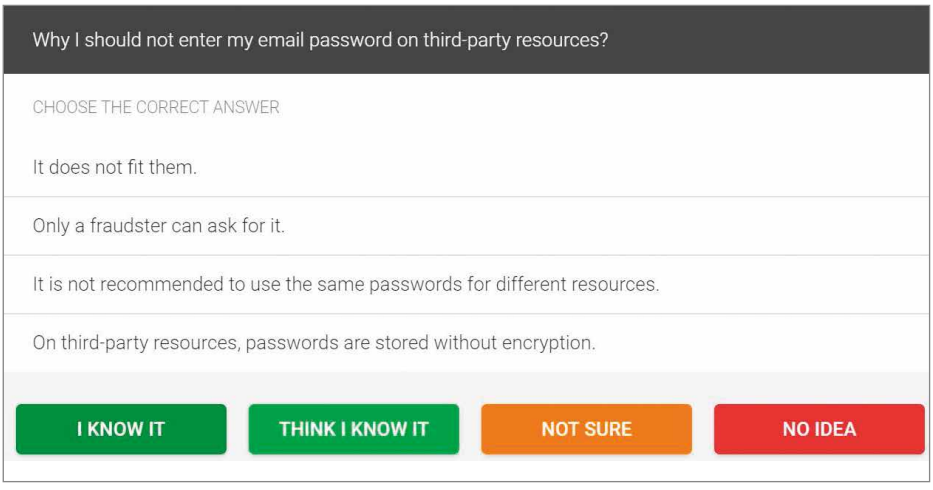
The platform's content is based on a competency model consisting of practical and essential cybersecurity skills that all employees should have. Without these skills, whether through ignorance or negligence, employees can damage your business.

- Passwords
- Email Security
- Web browsing
- Social networks and messengers
- PC security
- Mobile devices
- GDPR



Every lesson begins with a question, and based on the user's understanding of the topic, the platform then either follows up with a theoretical lesson or moves to another topic (if the answers were correct). The platform will also ask to identify the level of certainty about each statement to offer the learner a relevant scenario according to their actual unconscious competency level.





As of June 2020, KAOT will be available in the following languages: English, German, Spanish, Arabic, French, Italian, Russian.

Each lesson consists of

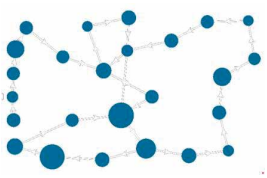
Questions where it's important to rate the level of confidence in the answer. Be honest, it's not an exam!

Short text explanations when a learner needs it

The administrator needs to choose which modules to assign to each group of users. Once registered, each employee can run the lessons in their preferred order. The content of every lesson is built according to the user's progress and confidence, ensuring that they learn only those skills that they don't know and skip those they do (and already use). Every lesson must be refreshed within a certain time period, automatically depicted in the user's interface.

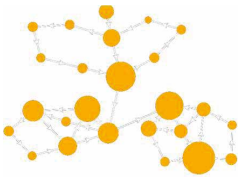
The picture below shows the learning paths of three different learners who took the same course. At the end, each learner achieved 100% proficiency, but they learnt at different speeds and in a different manner. Every circle on the scheme is a topic - the bigger the circle the longer it took for the learner to master it. People learn at different rates, taking into account many factors, including their ability to absorb information and existing knowledge levels, but they all ultimately mastered the skill.

Individual learning paths based on an employee's answers and their level of confidence



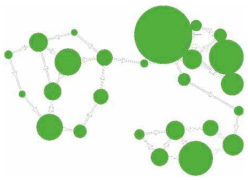
Learner 1
100% proficient at 8m 25s

Takes an almost linear path through the course as most of the answers were correct and he/she was confident about them.



Learner 2
100% proficient at 19m 39s

Requires much more support and explanations as 52% of the initial answers were correct.



Learner 2
100% proficient at 33m 40s

47% correct. Has as much to learn as Learner 2, especially struggled with one learning objective.

Is there a mechanism to prevent cheating?

The training program is 100% personalized – KAOT checks the unconscious competency level of each employee and builds the program accordingly, so employees receive different questions according to their level of knowledge, making cheating impossible.

How do you track results?

Extensive statistics allow you to follow up employee progression – performance summary, reports and diagrams for groups and individuals. Admin can identify high performers as well as those who need additional coaching. Reports on user progress, progress of classes, assignment details with indepth analysis of employee competence and metacognition as well as an 'at risk' diagram showing employees' unconscious incompetence analytics all help to track results.

Comprehensive analytics

- The way for educators to manage students – all learning in personalized ways.
- Handle assignments and/or learning paths.
- Advanced analytics.
- Early warning technology to highlight at-risk students.

What are the training outcomes?

- Uncovers and fixes unconscious incompetence, providing motivation for learning and ensuring sustainable cybersafe behavior
- Eliminates boredom and frustration through a personalized approach to each learner which boosts engagement and involvement in cybersecurity
- Ensures automatic, habitual use of skills, as a result of:
  - Training materials adapted to individual learners' characteristics
  - How the content is presented, taking into account the specifics of adult learning
  - Constant assessments that make learners constantly solve problems and answer questions that help them to better absorb information
  - Ongoing "refreshment" – returning to those topics and issues that caused difficulties early on.
- Cuts training time by 50% thanks to the adaptive learning methodology, so less time is spent on training and more time applying it on the job.

Technical features:

- Supports Single Sign On (SSO) via OpenID Connect
- AD synchronization is available through integration with ADFS
- Can be integrated with LMS via the SCORM or LTI e-learning formats (SCORM 1.2 and LTI 1.0, LTI 1.1 and LTI 1.1.1)

www.kaspersky.com
www.kaspersky.com/awareness

kaspersky BRING ON THE FUTURE

 GBD-6382 Q2/2020 V2