KASPERSKY lab

CYBERSECURITY AWARENESS

www.kaspersky.com

Cybersecurity Awareness

WHO WILL BENEFIT

These courses will be of particular benefit to:

- Business Managers,
- Regional IT Security officers,
- All those working online with sensitive data and/or with external contact.

Online interactive training modules and on-site CyberSafety Games training programs are designed for all employees who use computers or mobile devices at work, and for those who manage them.

APPROACH TO LEARNING

Around 80% of all cyber incidents are caused by human error. Companies are spending millions on cybersecurity awareness programs, but few CISOs are really satisfied with the results. What's wrong?

Most cybersecurity awareness training is too long, too technical and essentially negative. This does not play to people's core strengths - their decision-making principles and learning abilities - and as a result can render training ineffective.

So organizations are seeking more sophisticated behavioral support approaches (such as corporate culture development) that deliver a quantifiable and worthwhile return on their investment in security awareness.

Kaspersky Lab Cybersecurity Awareness courses work by:

- Changing behavior – stimulating the individual's commitment to working securely, building a corporate environment where "Everybody else cares about cyber safety, so I do, too".
- Combining a motivational approach, gamification learning techniques, simulated attacks and in-depth interactive cybersecurity skills training.

Comprehensive but simple and straightforward	Training covers a wide range of security issues – from how data leaks occur to internet based malware attacks and safe social networking, through a series of simple exercises, in a language suitable for non-IT people. We use learning techniques – group dynamics, interactive modules, cartoons and gamification - to make the learning process engaging.
Continuous motivation	We create teachable moments - by gamification and competition, and then re-inforce these moments throughout the year via online simulated attacks, assessment and training campaigns.
Changing beliefs	We teach people that it is human beings, not machines, who are the primary targets of cybercriminals. We show how, through working in a more safety-conscious manner, individuals can avoid becoming victims and exposing themselves and their workplace to attack.
Building a corporate cybersafety culture	We train management to become security advocates; a culture where cybersecurity becomes second nature is best achieved through management commitment and example, and cannot simply be imposed by IT.
Positive and collaborative	We demonstrate how security practices make a positive contribution to business efficiency, and promote more effective cooperation with other internal departments, including the IT Security team.
Measurable	We provide tools to measure employee skills, along with corporate-level assessments analyzing staff attitudes to cybersecurity in their daily work.

PROGRAM BENEFITS

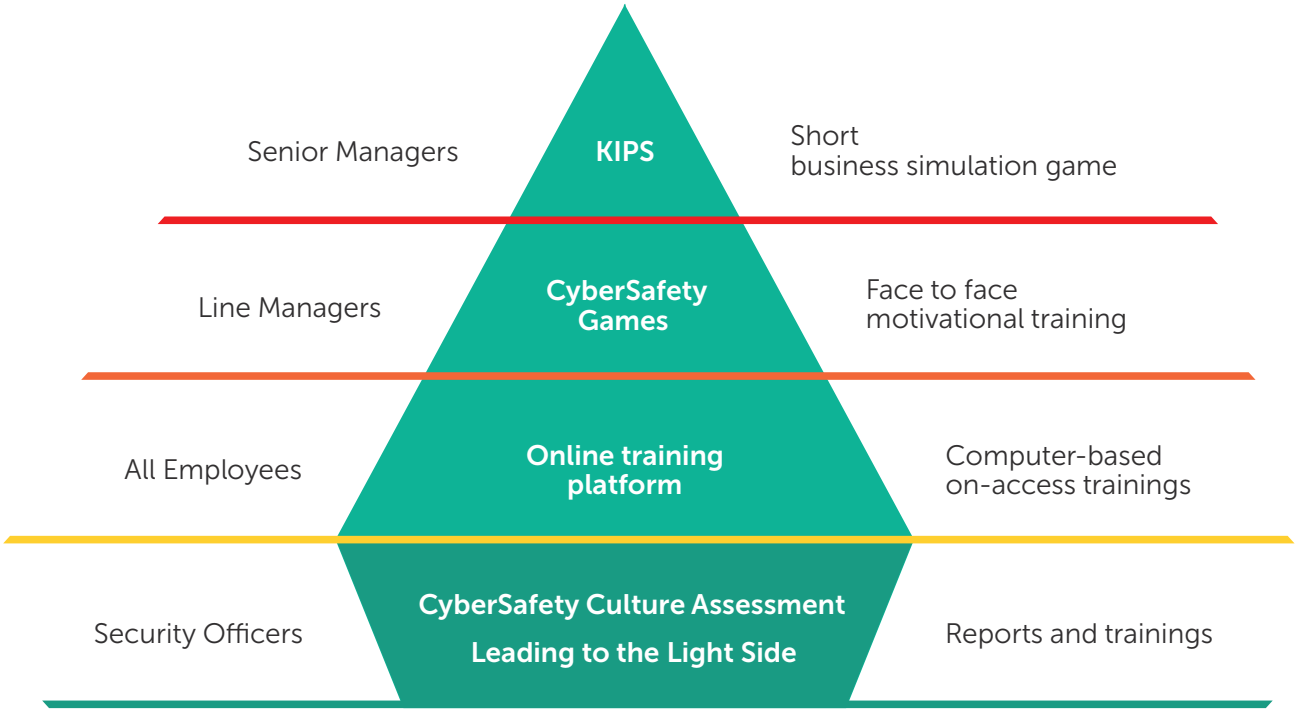
Kaspersky Cybersecurity Awareness Training changes minds, promoting security-minded behavior in real-world situations and reinforcing the principles of cybersecurity best practice in the workplace.

A recent study[1] concluded that:

- Companies with security awareness programs spend 76% less on security incidents than their non-training counterparts (average annual financial losses of just $162,000 versus $683,000).
- Organizations with a security awareness program were 50% less likely to have staff-related security breaches. The value of an effective Cybersecurity Awareness Program can:
  - Decrease the number of incidents by up to 90%.
  - Reduce the cyber risk in monetary terms by 50-60%.
  - Translate cybersecurity from IT-jargon to business language, and generate get business management 'buy-in'.
  - Generate measurable results in terms of cybersecurity awareness.

COURSE COMPONENTS

Cybersecurity Awareness Training from Kaspersky Lab comprises elements which intermesh, but which are also fully effective if used separately:



Kaspersky CyberSafety Awareness Trainings structure

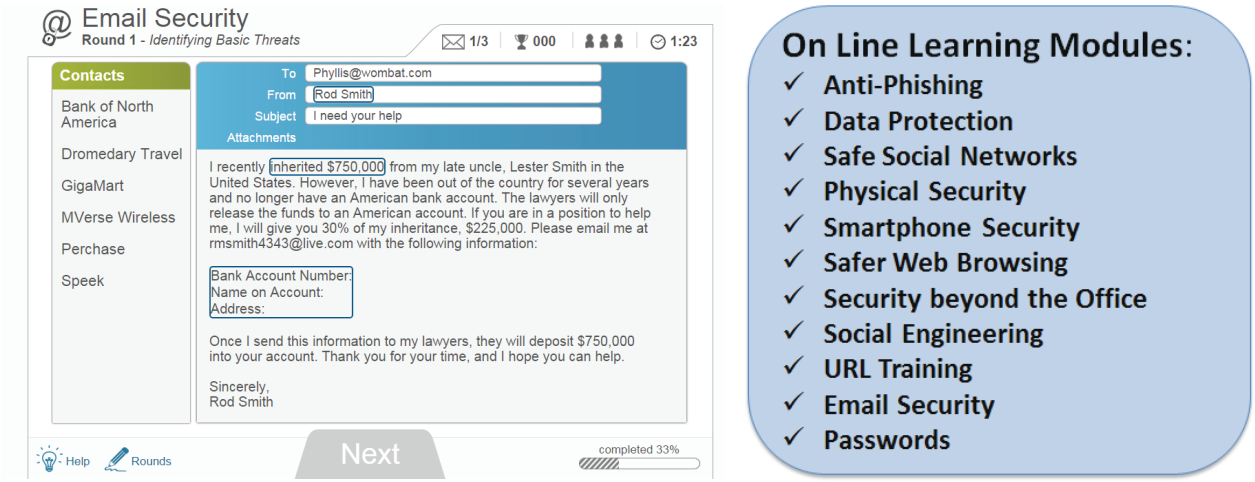
[1] ABERDEEN GROUP. The Last Mile in IT Security: Changing User Behaviors, ABERDEEN GROUP, October 2014

ONLINE SKILLS TRAINING PLATFORM

It is important to build on skills and knowledge, so access to an online skills platform is essential, allowing the student to work through typical scenarios and situations, gaining greater knowledge and understanding of potential threats and how to deal with them. Key aspects of the Online element of Kaspersky Cybersecurity Awareness Training are:

- **Skills Assessment:** To determine the in-depth skills and training needs of the user. Covers various security domains, includes predefined or random assessments, customer-defined questions, and customizable length.
- **Training Modules:** Anti-Phishing, Data Protection and Destruction, Safe Social Networks, Physical Security, Smartphone Security, Safer Web Browsing, Security Beyond the Office, Social Engineering, URL Training, Email Security, Passwords.
- **Simulated attacks:** Ready-to-go customizable templates of phishing emails presenting various levels of challenge. If the employee receiving the email clicks on the dangerous phishing link, he or she experiences a teachable moment, and can be auto-assigned to the relevant training module.
- **Analytics & Reporting:** Results by Campaign, Group, Device Type, Repeat Offender, Location. Plus supporting security posters, email templates, screensaver images.

Online learning allows candidates to practice and learn through an interactive learning portal.



On Line Learning Modules:

- ✓ Anti-Phishing
- ✓ Data Protection
- ✓ Safe Social Networks
- ✓ Physical Security
- ✓ Smartphone Security
- ✓ Safer Web Browsing
- ✓ Security beyond the Office
- ✓ Social Engineering
- ✓ URL Training
- ✓ Email Security
- ✓ Passwords

By using this portal, in conjunction with the Kaspersky Best Practice Guide, the Training Manager can establish an implement a powerful, continuous and measurable cybersecurity education plan, taking employees right through from simple to complicated concepts, varying the training elements according to the threat landscape and individual skillsets.

CYBERSAFETY GAMES TRAINING

This highly interactive workshop is instructor led by one of Kaspersky Lab's qualified instructors and provides the candidates with a foundation level of knowledge around actual cyber threats within a scenario based approach.

The delivery allows candidates to explore every day events through an interactive hands-on experience into the latest attacks and malware that no other provider can offer. The program has been specifically developed for enterprises that view security as a strategic requirement to raise employee awareness of the cyber threats during every day business activities.

BY THE TRAINING LINE MANAGERS ARE MOTIVATED:

- to understand "why they should care about security";
- to distinguish between safe and unsafe behaviour (technical and vigilance skills);
- The program provides positive examples "How to do", not only "Don'ts";

And allows candidates to understand how they look from the perspective of the Cyber Criminals.

Value: 93% - the likelihood of applying the knowledge gained in the training in the daily job[1].

Delivery form:

- Training by Kaspersky trainer
- Train-the-trainer (license plus teaching to run the trainings internally in the enterprise)

Formats available:

- Series of 2-hours sessions
- Full-day session

Changing beliefs

We teach people that it is human beings, not machines, who are the primary targets of cybercriminals. We show how, through working in a more safety-conscious manner, individuals can avoid becoming victims and exposing themselves and their workplace to attack.

Change misbeliefs	Into adequate perception	And positive role model
Smart hacker will send the virus and it will break my PC	Beware bad people, not broken computers	I understand which criminals can get value from my digital assets, so I am motivate to protect them
I am too small target	Small targets are easier and often more attractive to criminals	I want to be a harder target than the others
I don't have time for security	Security is a part of long-term efficiency	I will choose the safest way to achieve the business goal and cooperate with security team

[1]Data from case studies and evaluation of Kaspersky Lab customers running CyberSafety Games trainings.

CYBERSAFETY CULTURE ASSESSMENT

CybersSafety Culture Assessment analyzes actual everyday behavior and attitudes at all levels of the enterprise, revealing how employees in your organization perceive different aspects of cybersecurity.

The resulting report can be used to understand imbalances and areas for greater focus, helping to justify and align priorities in the internal and external activities of the Security Department, including awareness and training, internal PR and information sharing, and other collaboration principles while working in the business.

LEADING TO THE LIGHT SIDE TRAINING

Skills gained and instruments learned:

- How to influence users with security awareness messages;
- How to overcome resistance and ignorance;
- How to achieve up to 90% policy acceptance and compliance.

The training helps you find the way to the users' hearts and minds. The shift to safer behavior becomes their conscious choice.

The training uses group work to give you an opportunity to see typical "unsafe" situations from different perspectives. You are then able to structure your message in such a way that stimulates correct choices and shifts the user attitudes.

The training is a part of Kaspersky Security Awareness portfolio, based on CyberSafety Culture methodology.

Delivery form:

- Training by Kaspersky trainer, 4 hours

KASPERSKY INTERACTIVE PROTECTION SIMULATION (KIPS)

One of the biggest security challenges 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":

- Business, Managers may see security measures as a complication/contradiction to their business goals (cheaper/faster/more/better);
- IT Security Managers may feel that cybersecurity as an infrastructure and investment issue moves 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 3 are crucial to successful cybersecurity. However, traditional awareness formats, like lectures and red/blue exercises, are flawed: - lengthy, over-technical, and unsuited to busy managers, and they fail to build "common language" at the "common sense" level.

KIPS AS THE SOLUTION

The aim of KIPS is to bring these senior professionals from different areas of decision-making together, understanding one another's remits, objectives and concerns as they work towards the greater good of the organization as a whole.

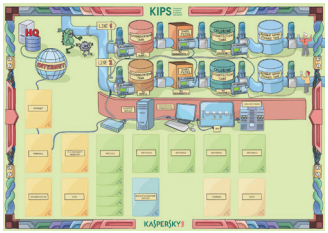
For IT, Business and Security – strategy simulation for cybersecurity decision-makers.

- Fun, engaging and fast (2 hours)
- Team-work builds cross-divisional co-operation
- Competition fosters initiative & analysis skills
- Gameplay develops an understanding of cybersecurity measures and strategy

Teams compete at running a simulated enterprise and earning money.

As the enterprise experiences a cyberattack, the players experience the impact on production and revenues, and learn to adopt different business and IT strategies and solutions in order to minimize the impact of the attack and to earn more money. Scenarios available include:

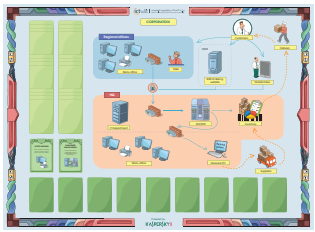
Industrial: Water Plant



Financial

Government

Corporate



Having played the KIPS Game, players should have come to important, actionable conclusions regarding their everyday business activities:

- Cyber-attacks damage revenues, and need to be addressed from top-management level,
- Cooperation between IT Security and Business Divisions is essential to successful cybersecurity,
- The costs of security need not run into millions, and are much less than the revenue you risk losing,
- Security tools are not difficult to use, and their use is important.

Attendees not only realize the cost of cyber-attacks, but more significantly, the importance of investing wisely in cybersecurity.

KASPERSKY lab