

# **ACTIONABLE SECURITY AWARENESS: CONVERT THE WEAKEST LINK INTO THE SAFETY FORCE**

Cybersecurity Awareness by gamification:  
Kaspersky CyberSafety Training

# HUMAN MISTAKES AS THE BIGGEST CYBERRISK FOR ENTERPRISES TODAY



**\$861,000**

per enterprise

average financial impact of a single data breach and attack vector\*



**\$86,500**

per SMB company

average financial impact of a single data breach and attack vector\*



**\$865,000**

per breach

average financial impact of an incident involving careless actions of employees\*\*



up to **\$400**

per employee per year

average cost of phishing attacks alone\*\*\*

\* Report: "Measuring the Financial Impact of IT Security on Businesses", Kaspersky Lab, 2016.

\*\* "Business Perception of IT Security: In The Face of an Inevitable Compromise", Kaspersky Lab, 2016.

\*\*\* Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.

# ALL THIS DESPITE OF SECURITY AWARENESS PROGRAMS THAT ARE IN PLACE IN MOST ENTERPRISES...

80%

of CISOs are not happy  
with the efficiency of their  
awareness program

# DIMENSIONS OF TRAINING EFFICIENCY

## BUILD BEHAVIOR, NOT JUST GIVE KNOWLEDGE

A learning approach should involve gamification, learning-by-doing, group dynamics, simulated attacks, learning paths, etc. It results in strong behavioral patterns and produces a long-lasting cybersecurity effect.

And don't let your training be boring.

## MEET BUSINESS NEEDS AND FORMAT PREFERENCES OF EVERY ORGANIZATIONAL LEVEL

Having different training for different organizational levels and functions creates a collaborative CyberSafety culture, shared by everyone and driven from the top.

Senior managers, line managers and regular employees need different skills.

## MANAGE PAINLESSLY, MEASURE REAL TIME

Computer-based training programs ensure consistence in training quality as well as flexibility, real-time skills assessment and efficient reinforcement. Automated training assignments, repeated attacks, auto-enrollment in training modules build a long-term efficiency.

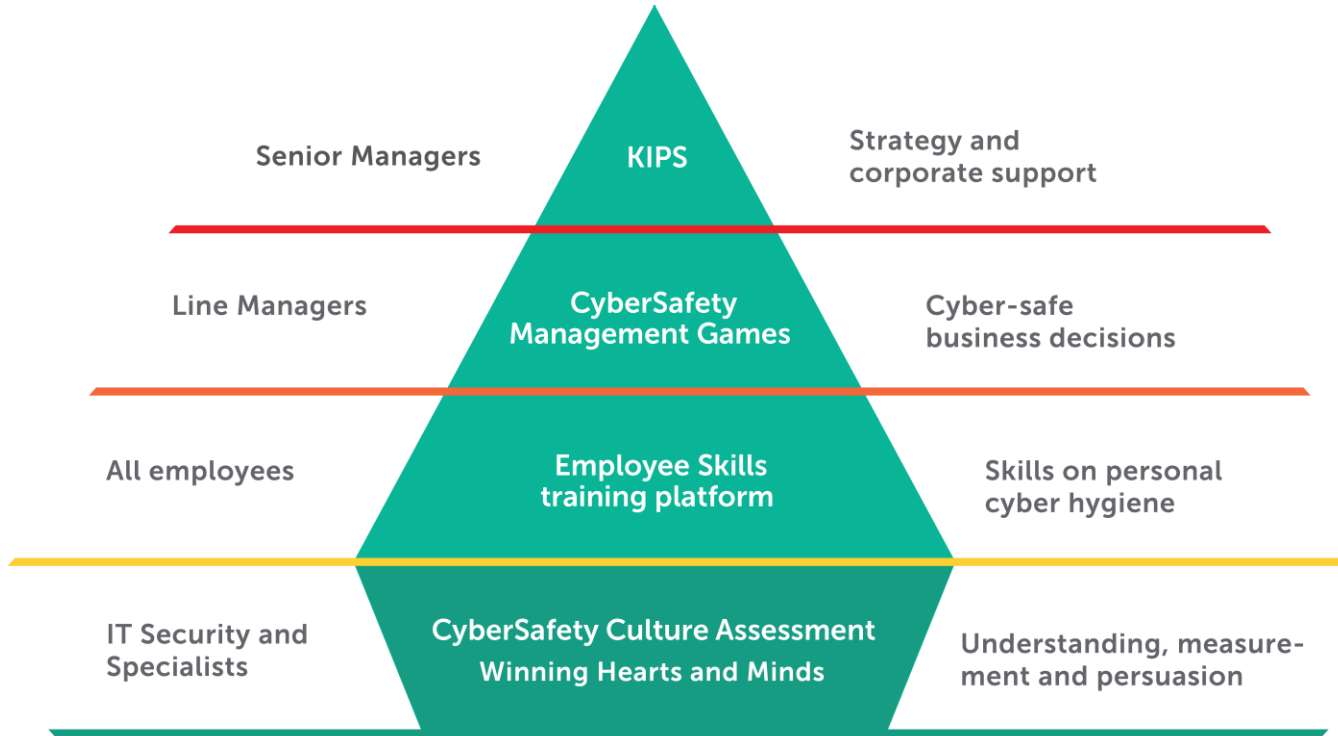
Easily managed by Security team or HR/ T&D.

## BASE EVERY TRAINING ON A STRONG CYBERSECURITY GROUNDS

Don't think that 'non-IT' training does not need a deep cybersecurity expertise. Every training should be based on a strong security model – and be up-to-date towards most recent threats.

That's how we add to building a safe cyber environment – which is strong, shared and self-sustained.

# KASPERSKY SECURITY AWARENESS PRODUCTS



# PROGRAM OUTCOME

up to

90%

A decrease in a total number of incidents

not less than

50%

A decrease in a monetary volume of incidents

up to

93%

Probability of using the knowledge in the daily work

more than

30x

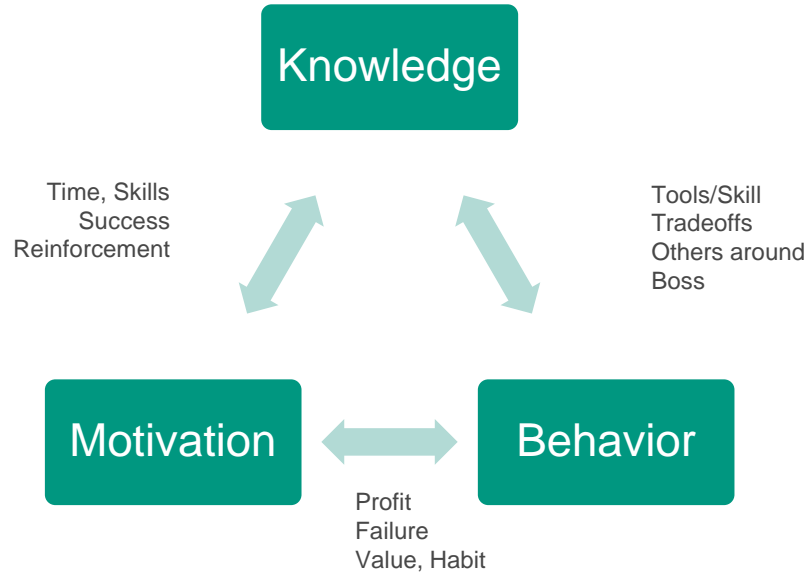
ROI from spending to the security awareness products

amazing

86%

Willingness to recommend the program

# CYBERSAFETY CULTURE: PSYCHOLOGY



Most awareness programs address just Knowledge, while this is not the way people live their lives

Behavior is the actual target of awareness, and it is tightly linked with both knowledge and motivation

The approach we propose (CyberSafety Culture) is Influential and measurable. At 3 levels – Knowledge, Behavior, Motivation.

# AWARENESS WORKS = PEOPLE BEHAVE

	WHAT WE EXPECT FROM PEOPLE AFTER THE AWARENESS PROGRAM
<b>BUSINESS MANAGERS</b>	Team-work with IT Security Take some responsibility for cyber safety
<b>LINE MANAGERS</b>	Create cyber-safe environment Enforce cyber-safe behavior of employees
<b>EMPLOYEES</b>	Share cyber safety values Act cyber safely Report Near Misses Cooperate with IT Security team

Kaspersky CyberSafety Culture methodology is based on Industrial Safety Programs used by DuPont, BP, Shell, Siemens, and millions of enterprises.



# 1. INTERACTIVE PROTECTION SIMULATION

## => STRATEGIC SUPPORT



For decision makers in  
Business, IT and Security



- Strategy simulation for decision makers on the cybersecurity
- Team-work
- Competition
- Strategy & mistakes

### SCENARIOS

#### Corporation

Protecting the enterprise from ransomware, APTs, automation security flaws

#### Bank

Protecting financial institutions from high-level emerging APTs

#### E-Government

Protecting the public web servers from attacks and exploits

#### Power station / Water Plant

Protecting Industrial control systems

## 2. CYBERSAFETY MANAGEMENT GAMES

### => DECISION-MAKING SKILLS



For line managers



### Understanding

Inner adoption of cybersecurity measures as an important yet uncomplicated time-consuming set of actions



### Monitoring

Seeing everyday working process through the cybersafety lens



### Cyber-safe decision making

Cybersecurity considerations as an integral part of business processes



### Reinforcement and inspiration

Influential leadership and helpful advice to employees

4-6 hours long gamified training providing managers with competence, knowledge and attitudes essential to maintain secure working environment in their divisions.

Covers all major security domains and typical situations at workplaces.  
Available at a Train-the-Trainer model.

# BUILDING BEHAVIOR BY FIGHTING MISBELIEFS



# 3. EMPLOYEES ONLINE TRAINING PLATFORM

=> CYBER HYGIENE SKILLS



For all employees

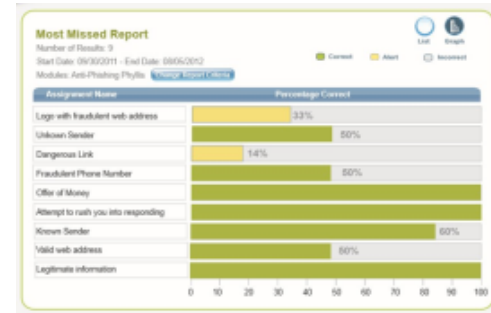
Skills training modules

+

Simulated phishing attacks

Knowledge Assessment

Analytics and Reporting



العربية

čeština

Deutsch

English(UK)

English(US)

español

Español

français

français

עברית

Magyar

Íslenska

italiano

日本語

한국어

Nederlands

Norsk

polski

português

русский

Slovák

svenska

தமிழ்

Türkçe

tiếng Việt

简体中文

繁體中文

Check demo at [www.kaspersky.com/demo-sa](http://www.kaspersky.com/demo-sa)



# 3. EMPLOYEES ONLINE TRAINING PLATFORM

## => CYBER HYGIENE SKILLS



For all employees

### Interactive training modules

- Fun and short
- Based on exercises with a knock-on effect
- Auto-enrollment reinforces skills
- 20+ modules covering all security domains

### Simulated phishing attacks

- 3 types of phishing attacks of various difficulty, all based on real-life cases
- Teachable moments appear every time employees open phishing emails
- Customizable templates
- Auto-assignment in training modules for those who failed the simulated attack

### Knowledge assessment

- Includes predefined or random assessments, customer-defined questions, and customizable length
- Covers various security domains
- Vast questions library and randomization exclude cheating

### Reporting & analytics

- Provides statistics for the organization as a whole or by department, location, position, as well as on individual level
- Monitors employees' level of skills and its dynamics
- Supports data export to a number of formats or to customer's LMS

# 4. CYBERSAFETY CULTURE ASSESSMENT



For Chief Information Security Officers



Analyses actual everyday behavior and attitude toward cybersecurity of the all management levels of the enterprise.

Cloud-based survey.  
Takes ~15 minutes to complete for an employee.  
Consolidated report

## 5. “WINNING HEARTS AND MINDS” TRAINING



For IT/ IT Security Specialists

### TARGET AUDIENCE:

- Cybersecurity awareness program managers
- Security officers

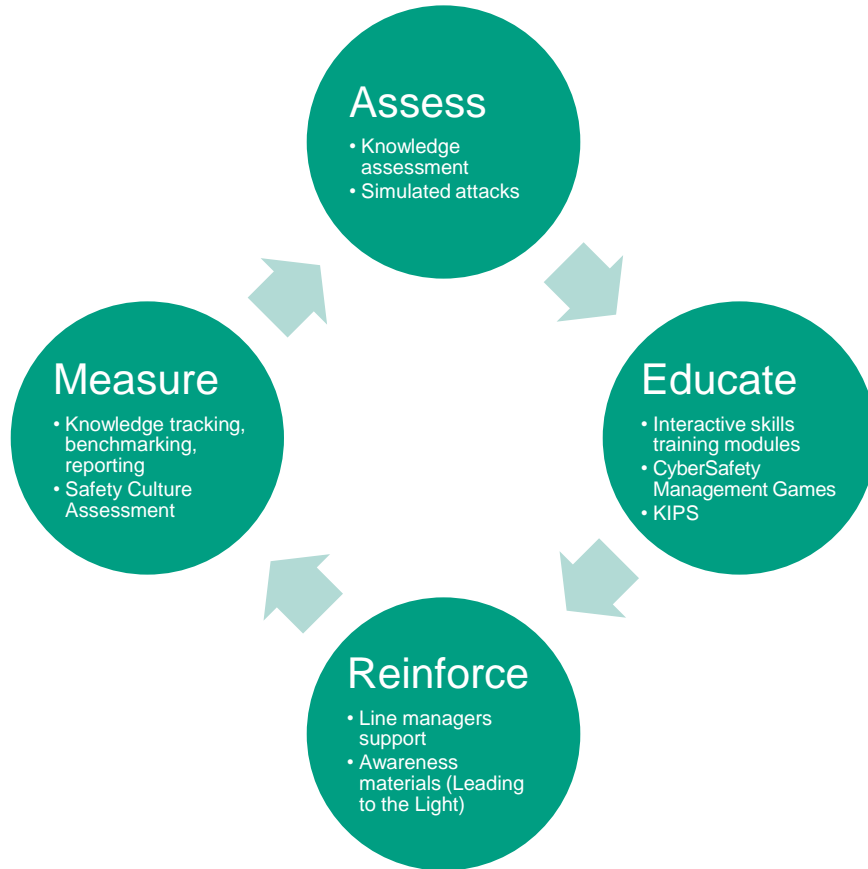
Security specialists often feel that their business colleagues do not hear their message, or even actively resist. Kaspersky “Leading to the Light” helps those who’s struggling to be heard.

### 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

4-hours training with real-life examples, workable tips and lifehacks and exercises which help reframe mutual understanding and co-operation.

# CONTINUOUS TRAINING METHODOLOGY

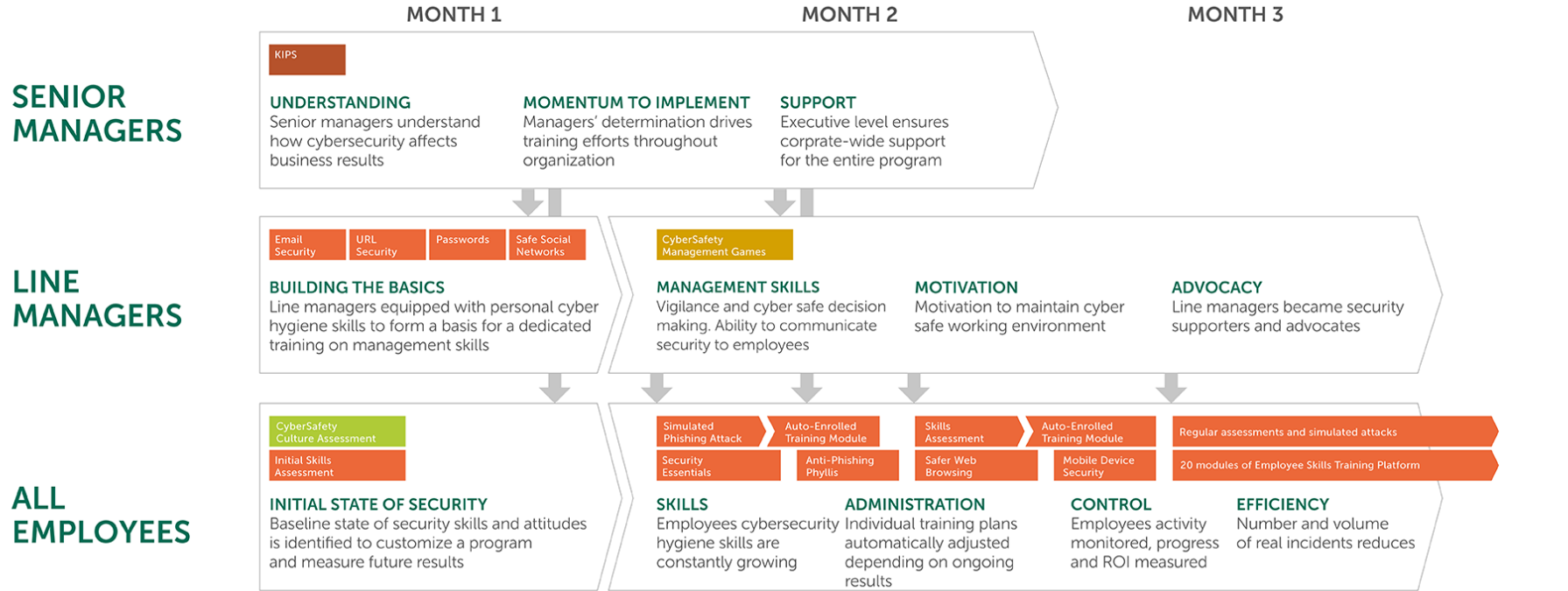


Continue during the year, cycle by cycle.

We provide Best Practice Guide and technical support.




# CUMULATIVE EFFECT – EACH TRAINING SUPPORTS THE OTHERS



Ongoing online skills training for 12 months and after...

Recommended Kaspersky Security Awareness training products:

 Kaspersky Interactive Protection Simulation (KIPS)

 Employee Skills Training Platform modules and features

 CyberSafety Management Games

 CyberSafety Culture Assessment

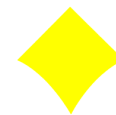
# KASPERSKY SECURITY AWARENESS – SELECTED CLIENTS



**TOSHIBA**



**RusHydro**



**YOKOGAWA**



Senato  
della Repubblica

## Licensed Training providers



# CASE STUDY. STAR-3 – NATIONAL CYBER DRILL OF QATAR. 2015



National Cyber Drill was based on Kaspersky Interactive Protection Simulation

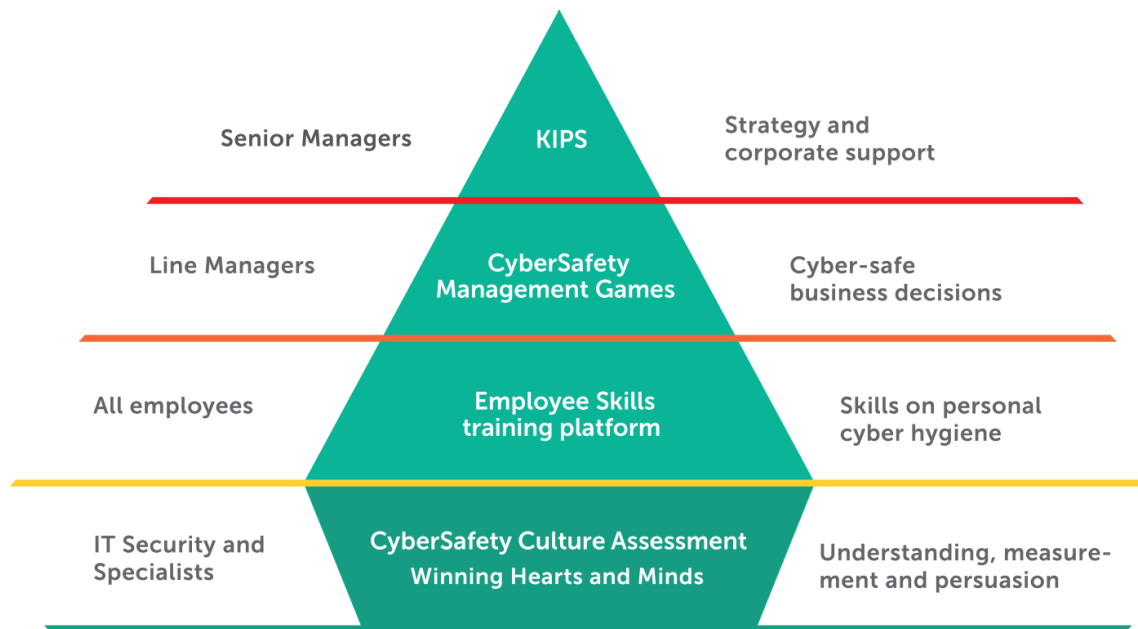
Games were held for 4 different economy sectors:

- Financial
- Industrial
- Corporate
- Government

# THE VALUE

- 93% likelihood to apply knowledge
- 90% decrease in the number of incidents
- 50-60% reduction\* of the cyber risk monetary volume
- 30x ROI
- Measurable security awareness program results

\* Aberdeen Group. Research as of 2014



Technical training programs for IT Security professionals are also available.

# TRY OUT THE INTERACTIVE DEMO AND ASK US FOR DETAILS!

[www.kaspersky.com/demo-sa](http://www.kaspersky.com/demo-sa) – a free interactive demo of Kaspersky Employee Skills Training Platform

[www.kaspersky.com/awareness](http://www.kaspersky.com/awareness) – more on our Security Awareness products

Contact your local Kaspersky Lab office or our partners for more information (including administrative features' demo, pricing, etc.)

Solutions for: Home Products Small Business 1-99 employees Medium Business 51-999 employees Enterprise 1000+ employees

KASPERSKY

Employee Skills Training Platform Interactive Training Modules Simulated Phishing Attacks Contact sales

## EMPLOYEE SKILLS TRAINING PLATFORM

Try out the interactive demo

Back to Solution Overview

Kaspersky Employee Skills Training Platform is designed to teach and reinforce technical cybersecurity hygiene skills. Offered as a modular on-access interactive tool, it is recommended for effective security education of all non-IT employees.

See how the Platform works by trying the free interactive demos below. Please note that these demos are not a complete version of our training course. The full Platform consists of 20 training modules of 15 minutes each, as well as assessment tools, auto-enrollment in training modules, advanced analytics and reporting functionality.

Interactive Training Modules Simulated Phishing Attacks

### INTERACTIVE TRAINING MODULES

1. Email Security
2. URL Training
3. Security Essentials
4. Data Protection and Destruction
5. Mobile App Security
6. Mobile Device Security
7. Password Security
8. PCI DSS
9. Protected Health Information
10. Physical Security
11. PII
12. Safe Social Networks
13. Safer Web Browsing
14. Security Beyond the Office
15. Social Engineering
16. Security Essentials for Executives
17. Anti-Phishing Phil
18. Anti-Phishing Phyllis

An aerial photograph of a city skyline at sunset. The sun is low on the horizon, casting a warm orange glow over the city. The skyline is filled with various skyscrapers and buildings. In the foreground, there are several large, modern buildings and a highway interchange. The overall scene is a mix of urban architecture and natural light.

**WE PROTECT WHAT MATTERS MOST**

**KASPERSKY** LAB

[www.kaspersky.com/awareness](http://www.kaspersky.com/awareness)