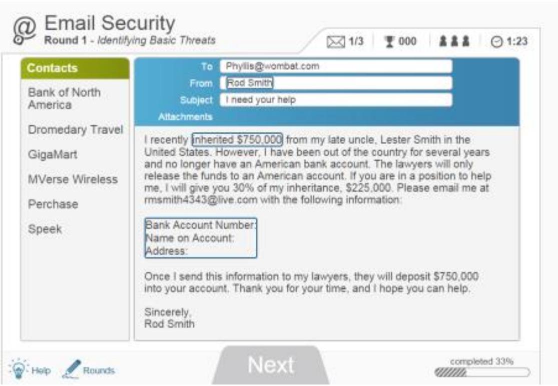
ACTIONABLE SECURITY AWARENESS: CONVERT THE WEAKEST LINK INTO THE SAFETY FORCE

Cyber security awareness by gamification:
Kaspersky Lab CyberSafety Trainings

KASPERSKY lab

APPROACHES TOWARDS SECURITY EDUCATION

“Old fashion”



To: Phyllis@wombat.com

From: Rod Smith

Subject: I need your help

Attachments

I recently inherited $750,000 from my late uncle, Lester Smith in the United States. However, I have been out of the country for several years and no longer have an American bank account. The lawyers will only release the funds to an American account. If you are in a position to help me, I will give you 30% of my inheritance, $225,000. Please email me at rmsmith4343@live.com with the following information:

Bank Account Number:
Name on Account:
Address:

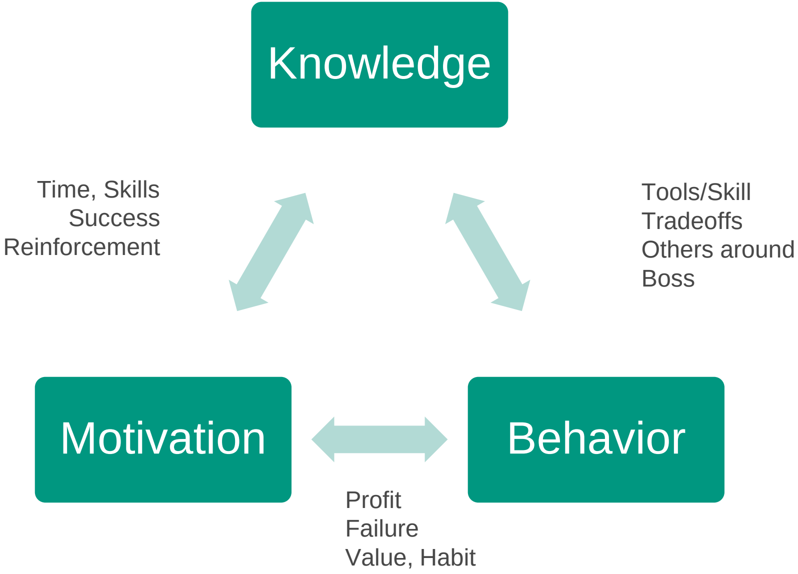
Once I send this information to my lawyers, they will deposit $750,000 into your account. Thank you for your time, and I hope you can help.

Sincerely,
Rod Smith

- 93% likelihood to apply knowledge in the daily work
- 90% decrease in mistakes
- 50-60% lower risk $ volume
- 30x ROI

Low efficiency
Not measurable

CYBER SAFETY 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

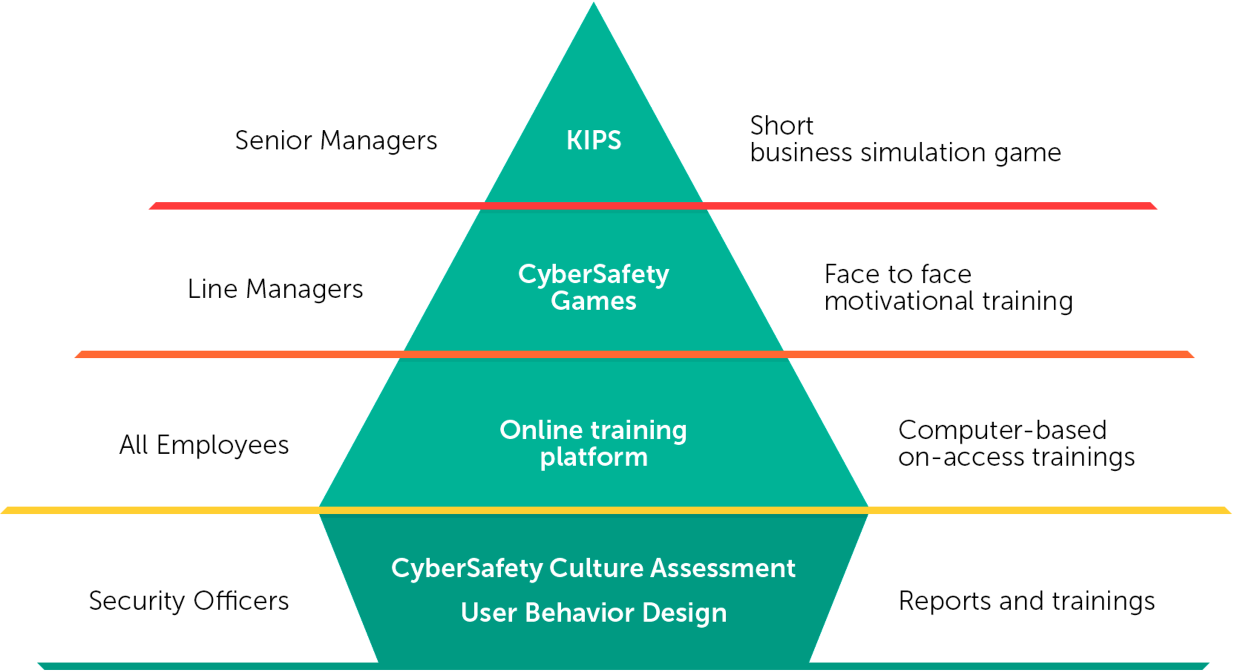
The approach we propose (Cyber Safety Culture) is Influential and measurable. At 3 levels – Knowledge, Behavior, Motivation.

AWARENESS WORKS = PEOPLE BEHAVE

	WHAT WE EXPECT FROM PEOPLE AFTER THE “AWARENESS PROGRAM”
BUSINESS MANAGERS	Team-work with IT Security Take some responsibility for cyber safety
LINE MANAGERS	Create cyber-safe environment Enforce cyber-safe behavior of employees
EMPLOYEES	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.

SECURITY AWARENESS TRAININGS FROM KASPERSKY LAB



Senior Managers

KIPS

Short
business simulation game

Line Managers

CyberSafety Games

Face to face
motivational training

All Employees

Online training platform

Computer-based
on-access trainings

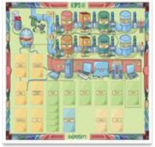
Security Officers

CyberSafety Culture Assessment

User Behavior Design

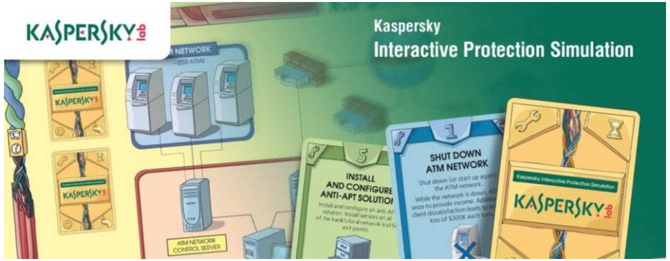
Reports and trainings

Kaspersky CyberSafety Awareness Trainings structure



1. INTERACTIVE PROTECTION SIMULATION

For decision makers in Business, IT and Security


KASPERSKY lab
Kaspersky
Interactive Protection Simulation
NETWORK
SHUT DOWN ATM NETWORK
INSTALL AND CONFIGURE ANTI-APT SOLUTION
ATM NETWORK CONTROL SERVER
KASPERSKY lab

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

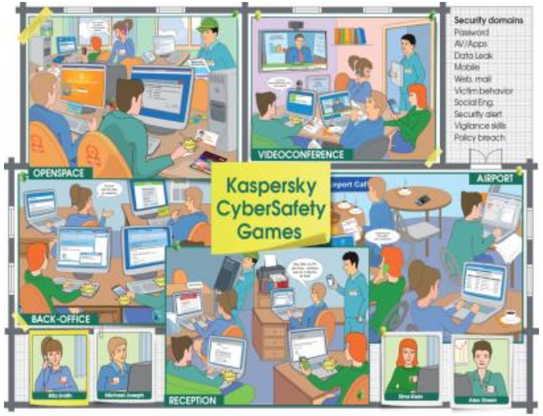
SCENARIOS	
Corporate	Protecting the enterprise from ransomware, APTs, automation security flaws
Financial	Protecting the financial institutions from high-level emerging APTs
E-Government	Protecting the public web servers from attacks and exploits
Industrial	Protecting Industrial Control systems

2. CYBERSAFETY GAMES TRAINING

For line managers

Gamification

To engage people to compete,
and learn by doing



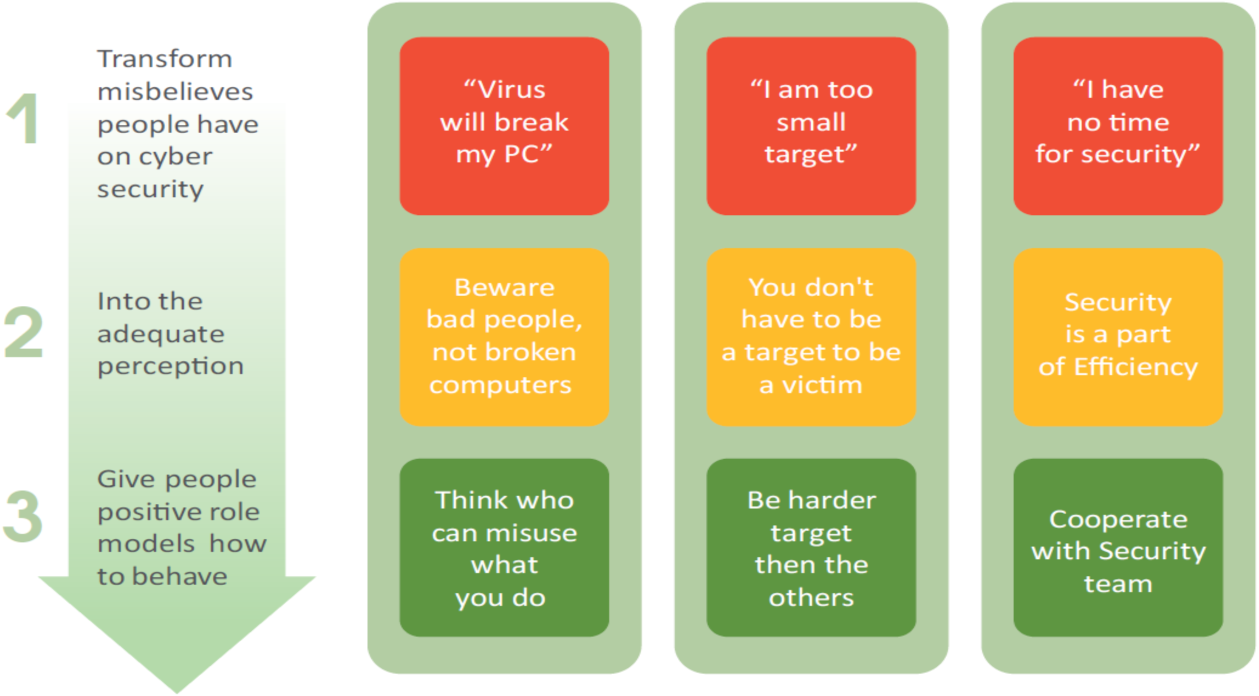
10 security domains in typical workplaces

1-day on-site by Kaspersky trainer,
20-50 people

or

Train-the-Trainer model –
for enterprise T&D

BUILDING BEHAVIOR BY FIGHTING MISBELIEFS



1 Transform misbelieves people have on cyber security	“Virus will break my PC”	“I am too small target”	“I have no time for security”
2 Into the adequate perception	Beware bad people, not broken computers	You don't have to be a target to be a victim	Security is a part of Efficiency
3 Give people positive role models how to behave	Think who can misuse what you do	Be harder target then the others	Cooperate with Security team

3. ONLINE TRAINING PLATFORM

For all employees

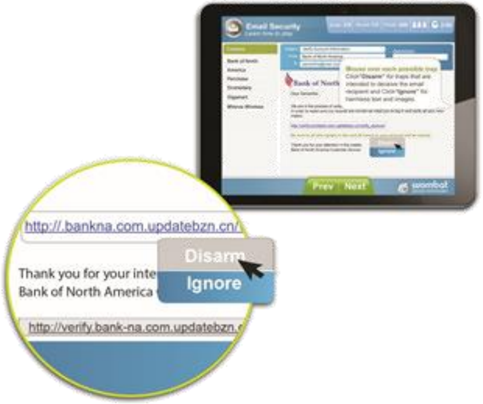
Skills training modules

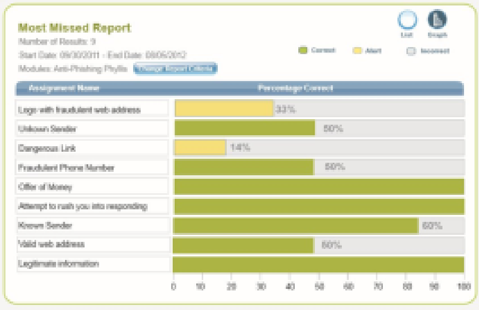
+

Simulated phishing attacks

Knowledge Assessment

Analytics and Reporting





čeština

Deutsch

español

Español

français

italiano

日本語

한국어

Nederlands

Norsk

polski

português

русский

svenska

ภาษาไทย

tiếng Việt

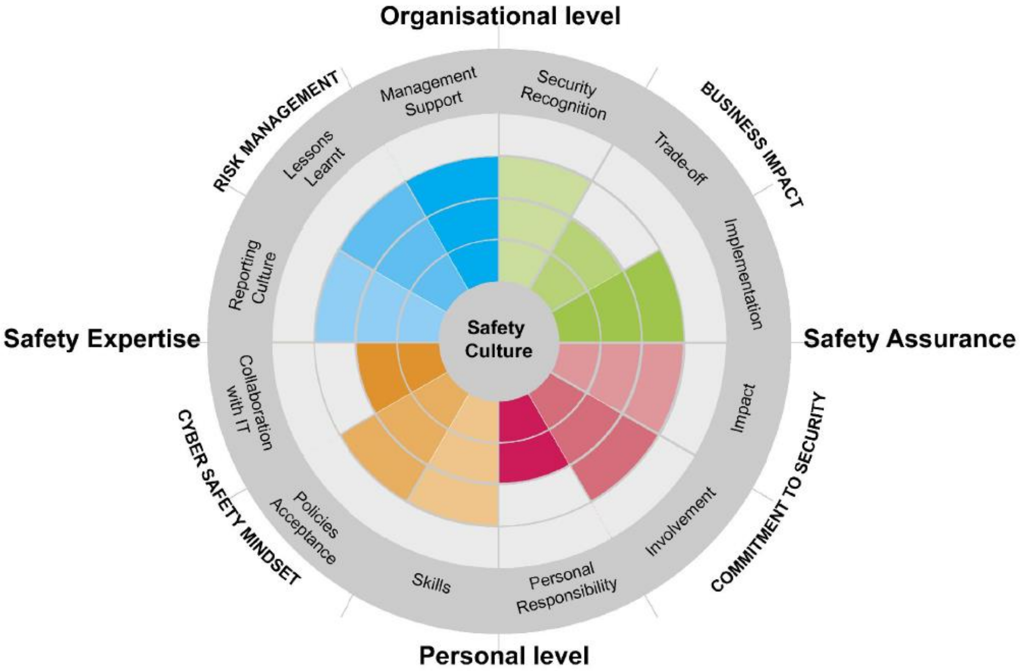
简体中文

繁體中文

Cloud-based Platform with multiple administrative roles

4. CYBERSAFETY CULTURE ASSESSMENT

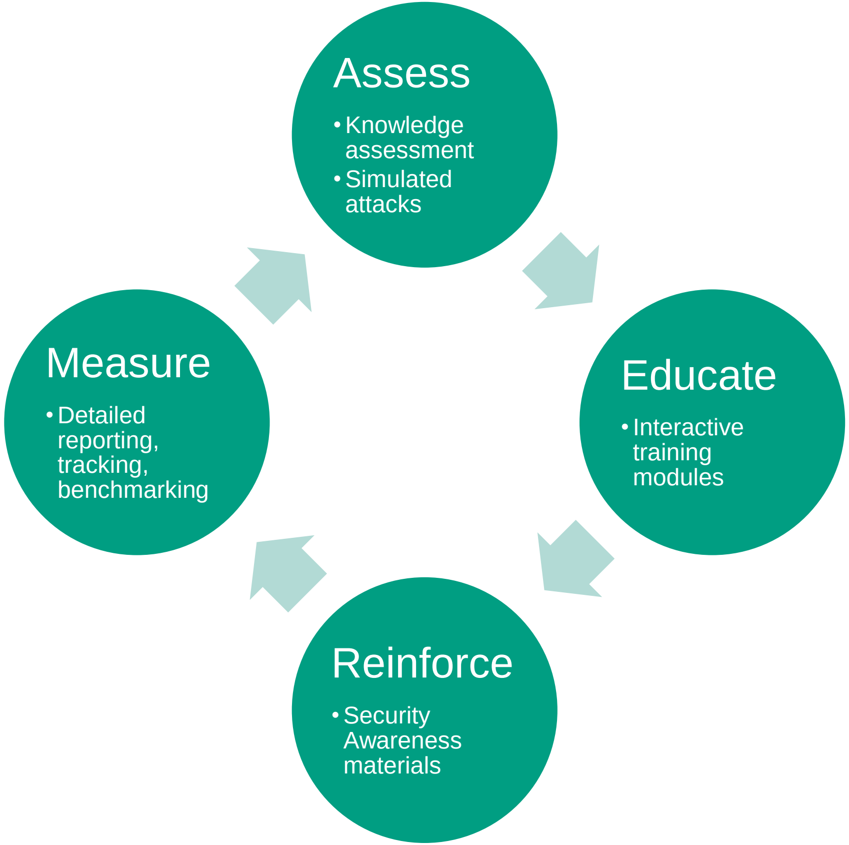
For Chief Information Security Officers



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

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

CONTINUOUS TRAINING METHODOLOGY



Assess

- Knowledge assessment
- Simulated attacks

Educate

- Interactive training modules

Reinforce

- Security Awareness materials

Measure

- Detailed reporting, tracking, benchmarking

Continue during the year, cycle by cycle.

We provide Best Practice Guide and technical support.

CYBERSAFETY CULTURE – CASE STUDIES

BASF We create chemistry

CERN

du add life to life

TOSHIBA

Licensed CyberSafety games Training providers

SANS

wombat security technologies

SLTN inter access

إنجازات Injazat DATA SYSTEMS لنظم البيانات

MITSUBISHI HITACHI POWER SYSTEMS

ISA

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

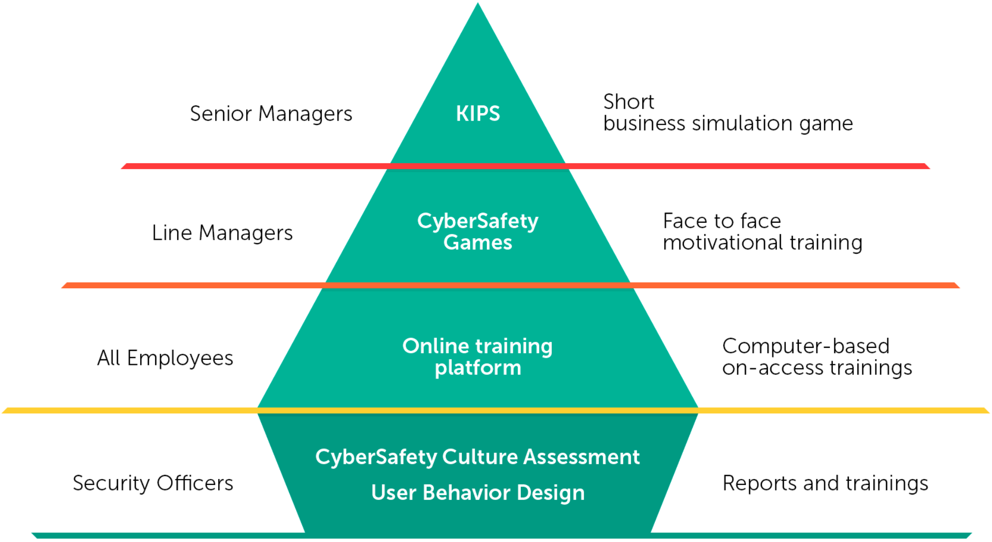
National Cyber Drill was based on Kaspersky Interactive Protection Simulation

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



Kaspersky CyberSafety Awareness Trainings structure

* Aberdeen Group. Research as of 2014

WE PROTECT WHAT MATTERS MOST

KASPERSKY lab