CYBERSAFETY MANAGEMENT GAMES

Immersive learning and motivational experience to promote cyber-secure decision making by line managers
Do line managers encourage subordinates to use cybersafety skills in their daily work?

Do they regard cybersecurity as an essential part of business efficiency?

Can they motivate employees to care more about security – or they’re not motivated themselves?
Kaspersky CyberSafety Management Games provide 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.
TRAINING OUTCOME

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
Transform misconceptions people have on cybersecurity

Into the adequate perception

Give people positive role models how to behave

1. "Hackers will break my PC"
   Beware bad people, not broken computers
   Think who can misuse what you do

2. "I am too small target"
   You don’t have to be a target to be a victim
   Be harder target than the others

3. "I have no time for security"
   Security is a part of Efficiency
   Cooperate with Security team
Cybersafety Management Games Format

- Combines gamification with comprehensive coverage of security topics, examples, explanations and exercises,
- Powered by purpose-build CyberSafety Management Games software to support easy-to-manage training delivery process,
- Divided into short modules and runs in 4 hours.
TRAINING SETUP

- 20-50 people in a room, split in competing groups, using training materials – game fields, chips, iPads with CyberSafety Games app,

- Teams are walking through the virtual enterprise, examining every gaming area, encountering all possible sources of cyberthreats,

- Once they discover the particular threat, they are trained to mitigate it.
TYPICAL WORKPLACES AS A LEARNING TOOL

Each workplace contains 12 marked zones
 Zones on the map contain potential cyber threats.

10 security domains - AV/Apps, Data Leak, Mobile, Web, Mail, Victim behavior, Social Engineering, Security alerts, Vigilance skills, Policy breach, Social networking
Participants put “casino-style” bets on all the potential cyberthreat zones – which means that they put their knowledge and reputation at stake and win or lose the highest score in the competition.

Alternative mechanics with eliminated gambling environment available.
VARIETY OF STUDENTS’ ACTIVITY

Some Zones do contain threats, some don’t. Sometimes there are paired good/bad Zones from the same domain.
EXERCISES TO SHAPE SAFE BEHAVIOR

For a threat identified, teams propose a set of actions, which they can do at their workplace to lower or mitigate a risk and earn mitigation experience points.

After the exercise is completed, a trainer explains the best practice employees should follow at their desks.
EXERCISES TO SHAPE SAFE BEHAVIOR

People make exercises which help them to make responsible risk-taking decisions.

Trainees learn to judge everyday situations from the view of both business efficiency and security.
EXERCISES TO SHAPE SAFE BEHAVIOR

Software platform offers:
- step-by-step exercises to master technical skills (f.i., spotting the malicious emails – where to look, what to think, etc.)
- integrating cartoons,
- live interaction,
- tests,
- theoretical guidance.
EXERCISES TO SHAPE SAFE BEHAVIOR

Software platform covers major technical skills and domains.

It presents people with real-life situations, asks for their opinion and returns a professional advice on the real security status and recommended actions ➔ “learning-by-doing” concept.
EXERCISES TO SHAPE SAFE BEHAVIOR

Students roleplay typical discussions with IT Security. Why do they always prohibit things employees want to do? Or maybe we’d better reconsider our manner when talking to IT Security – to tell our real needs, to explore options together, etc.

This approach brings to mutually beneficial resolutions, which are both effective and secure.
# DELIVERY OPTIONS

<table>
<thead>
<tr>
<th>Kaspersky Lab trainer</th>
<th>Train-the-trainer</th>
<th>Custom scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our certified trainer</td>
<td>License to use the training inside the enterprise by internal trainers</td>
<td>Based on the customer cybersecurity environment</td>
</tr>
</tbody>
</table>

**Group:** 20-50 people, split into teams comprised of 4 people

**Room:** ~ 3m²/person, no columns, regular form

**Equipment:** Projector (6-8 lumens), Screen, 1 iPad per team + Wi-Fi, Sound system (speakers, microphones (2-3), Flipchart (2) and markers (4 colors each)

**Furniture:** Tables of participants for 4 people (rectangular size not less than 75x180 cm, or round with no more than 1.5 m diameter), Participants should sit in groups of 4 at the tables. Table and chair for the trainer. Chairs on the number of participants.
KASPERSKY SECURITY AWARENESS TRAINING PRODUCTS

Technical training programs for IT Security professionals are also available.
CUMULATIVE EFFECT – EACH TRAINING SUPPORTS THE OTHERS

MONTH 1
- KIPS
- UNDERSTANDING
  Senior managers understand how cybersecurity affects business results
- BUILDING THE BASICS
  Line managers equipped with personal cyber hygiene skills to form a basis for a dedicated training on management skills
- INITIAL STATE OF SECURITY
  Baseline state of security skills and attitudes is identified to customize a program and measure future results

MONTH 2
- SUPPORT
  Executive level ensures corporate-wide support for the entire program
- MANAGEMENT SKILLS
  Vigilance and cyber safe decision making. Ability to communicate security to employees
- SKILLS
  Employees cybersecurity hygiene skills are constantly growing

MONTH 3
- MOTIVATION
  Motivation to maintain cyber safe working environment
- ADMINISTRATION
  Individual training plans automatically adjusted depending on ongoing results
- CONTROL
  Employees activity monitored, progress and ROI measured
- EFFICIENCY
  Number and volume of real incidents reduces

ALL EMPLOYEES
- CYBERSAFETY CULTURE ASSESSMENT
- INITIAL SKILLS ASSESSMENT
- SKILLS ASSESSMENT
- AUTO-ENROLLED TRAINING MODULE
- SECURITY ESSENTIALS
- ANTI-PHISHING PHYLIS
- SKILLS ASSESSMENT
- AUTO-ENROLLED TRAINING MODULE
- SAFE WEB BROWSING
- MOBILE DEVICE SECURITY
- REGULAR ASSESSMENTS AND SIMULATED ATTACKS
- 20 MODULES OF EMPLOYEE SKILLS TRAINING PLATFORM

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

Recommended Kaspersky Security Awareness training products:
- KIPS
- Employee Skills Training Platform modules and features
- CyberSafety Management Games
- CyberSafety Culture Assessment

Kaspersky Interactive Protection Simulation (KIPS)
<table>
<thead>
<tr>
<th>Efficiency</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A decrease in a total number of incidents</td>
<td>up to 90%</td>
</tr>
<tr>
<td>A decrease in a monetary volume of incidents</td>
<td>not less than 50%</td>
</tr>
<tr>
<td>Probability of using the knowledge in the daily work</td>
<td>up to 93%</td>
</tr>
<tr>
<td>ROI from spending to the security awareness products</td>
<td>more than 30x</td>
</tr>
<tr>
<td>Willingness to recommend the program</td>
<td>amazing 86%</td>
</tr>
</tbody>
</table>
WE PROTECT WHAT MATTERS MOST

www.kaspersky.com/awareness