

EMPLOYEE SKILLS TRAINING PLATFORM

On-access skills training and measurement – for all employees

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.

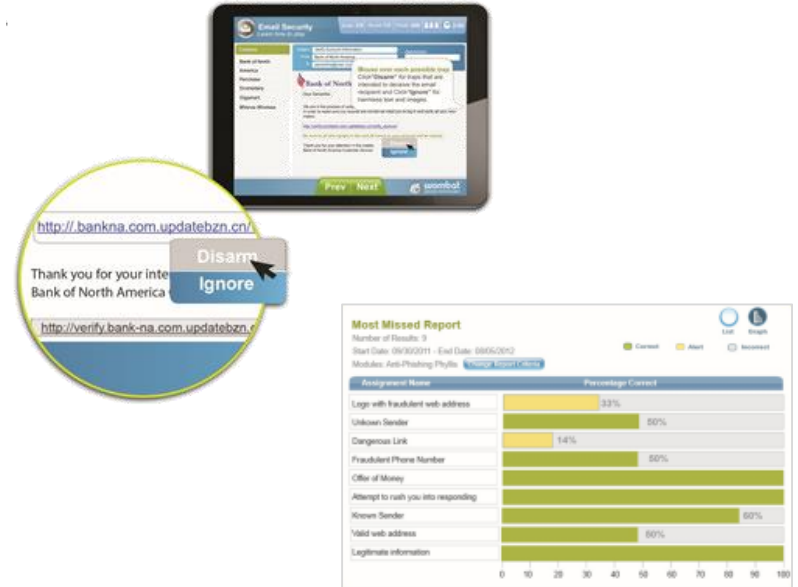
*** Calculations based on Ponemon Institute, "Cost of Phishing and Value of Employee Training", August 2015.

WHAT IS EMPLOYEE SKILLS TRAINING PLATFORM



For all employees

- SaaS platform to deliver online training modules to employees
- One integrated platform for assessments, training and reporting:
 - Easy to spot trends
 - Easy to show vulnerabilities and risks
 - Easy to show improvements
 - Easy to manage from one place
- Developed in partnership with Wombat Security Technologies and built on its award-winning training software



EMPLOYEE SKILLS TRAINING PLATFORM



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

EMPLOYEE SKILLS TRAINING PLATFORM FOR GLOBAL ENTERPRISE



For all employees

 العَرَبِيَّة	 עִבְרִית	 português
 čeština	 Magyar	 русский
 Deutsch	 Íslenska	 Slovák
 English(UK)	 italiano	 svenska
 English(US)	 日本語	 ภาษาไทย
 español	 한국어	 Türkçe
 Español	 Nederlands	 tiếng Việt
 français	 Norsk	 简体中文
 français	 polski	繁體中文

Employee Skills Training Platform is available in 27 languages, and this count is growing.

SECURITY DOMAINS COVERED (LIST OF INTERACTIVE MODULES)

Data Protection and Destruction

Use portable storage safely and properly discard sensitive data

Email Security

Learn to identify phishing emails, dangerous attachments, and other email scams

Mobile App Security

Learn how to judge the safety of mobile apps

Mobile Device Security

Use important physical and technical safeguards to protect your devices and your data

PII

Protect confidential information about yourself, your employer and your customers

Passwords

Learn how to create and manage strong passwords

Physical Security

Learn how to protect people and property

Protected Health Information (PHI)

Learn why and how you should safeguard Protected Health Information

Protecting Against Ransomware

Learn to recognize and prevent ransomware attacks

PCI DSS

Recognize warning signs and improve security of credit card data

Safe Social Networks

Learn how to use social networks safely and responsibly

Safer Web Browsing

Stay safe on the Internet by avoiding risky behavior and common traps

Security Essentials

Recognize security issues commonly encountered in daily job

Security Essentials – Executives

Recognize and avoid threats met by senior managers at work and at home

Security Beyond the Office

Avoid common security mistakes while working at home or on the road

Social Engineering

Recognize and avoid social engineering scams

URL Training

Learn how to spot fraudulent URLs

USB Device Safety

Protect yourself, data, and systems when using USB devices

Anti-Phishing Phil

Learn how to spot phishing attacks by identifying fraudulent URLs

Anti-Phishing Phyllis

Learn how to recognize phishing emails by identifying red flags

FLEXIBLE ONLINE PLATFORM: ASSIGNING TASKS TO EMPLOYEES

Create New Assignment

Step 2: Add Modules

<input type="checkbox"/>	Module Name
<input type="checkbox"/>	URL Training
<input type="checkbox"/>	Social Engineering
<input type="checkbox"/>	Smartphone Security
<input type="checkbox"/>	Security Beyond the Office
<input type="checkbox"/>	Safer Web Browsing
<input type="checkbox"/>	Safe Social Networks
<input type="checkbox"/>	Protected Health Information
<input type="checkbox"/>	Physical Security

Page 1 of 1

Cancel

On-site training manager can assign specific training modules to employees, based on their profile, department, results of previous assessments or time passed since other training.



SHORT MODULES TO ENSURE SMOOTH INTEGRATION INTO WORKING PROCESS

URL Training
Round 3 - Spot Advanced Tricks

How to **verify** a web address

www.searcher.com/search?q=bonaonline.com

Searcher
bonaonline.com
About 373,000 results (0.20 seconds)

[Sign in to Online Banking](#)
Sign in to your Online Banking account by entering your username and password.
[www.bona.com/account](#)

Look carefully at the first result.
Notice that the first result's address doesn't have the same domain as you searched for - it's **bona.com** instead of **bonaonline.com**. When you search for a fraudulent domain, the top results won't match the domain you entered.

Rounds completed 59%

Back Next

In short ~15 minutes sessions

Every training module integrates teaching with exercises and learning-by-doing

URL Training
Round 2 - Watch Out For Tricks

0 | 1:54

https://amazon.co.uk/s?q=mobile+phones

Visit
Avoid

Rounds completed 47%

Next

© 2008-2014 Wombat Security Technologies, Inc. All rights reserved. [v4.0]

LEARNING PRINCIPLES

Combining explanations, tests and “do-it-yourself” with hints and feedback...

Social Engineering
Lesson 1 - Social Engineering Basics

True or False 2/3

Good job! Filters and firewalls can protect you from some attacks, but they never catch everything.

True False

Review Next

completed 44%

Email Security
Round 1 - Identifying Basic Threats

To: Phyllis
From: purchase4568@live.com
Subject: Cash for your opinion

Attachments

We would like your opinion on our new survey. The survey has only five short questions and will give you a \$10.00 credit on the purchase of any product. To fill out the survey, click the following link: <http://perchasesurvey.survey4568.com/06556jdfisk/survey>

Oops! This link uses the organization name in the URL to make you think it is legitimate. Examine the link carefully.

The survey link is only valid for two days, so please hurry!

Thank you,
Purchase Survey Department

Next

completed 33%

... to ensure people learn effectively with exercises and learning-by-doing

BUILDING SAFE BEHAVIOR STEP BY STEP

Password Security
Lesson 2 - Password creation

Insertion password creation

3. Click two or more letters to change their case

oCto475Pus
strong

Next step

Create two strong passwords to move on!

completed 56%

Password Security
Lesson 2 - Password creation

Great job!
Congratulations! Click "Next" to continue...

Phrase-based passwords

1. Read the provided phrase
2. Use the phrase method to create a strong password
3. Use the "next" button if you get stuck

apples to oranges

apP13s>0rang3s
strong

Next

Create two strong passwords to move on!

completed 69%

Password Security
Lesson 3 - Password families

Great job!
Congratulations! Now click "Next" to create the second family

Create a password family

Use the supplied base password to create a password family

Foot#36bAll

Foot#36bAlgm ✓

Foot#36bArb ✓

Foot#36bAlly ✓

Foot#36bAlas ✓

Next

Create two families to move on!

completed 94%

Training module guides students through the topic from basics to advanced knowledge

SECURITY POLICY SIGN-OFF

Edit Training Jacket Template

Review and make any necessary changes training jacket.

English (US) French ✕ +

Company Policy on the passwords is:
- follow the minimum password complexity enforced by the Company
- never use the same or similar password for any other personal resource outside of the company
- change the password very 3 months (for Financial department - every 2 months)

Please read the full security policy here: intranet.customer.com/security

In case you beleive your password may be compromised, report it to the Security team immediatly by:
- Dialing #1911 extension
- Email security@customer.com

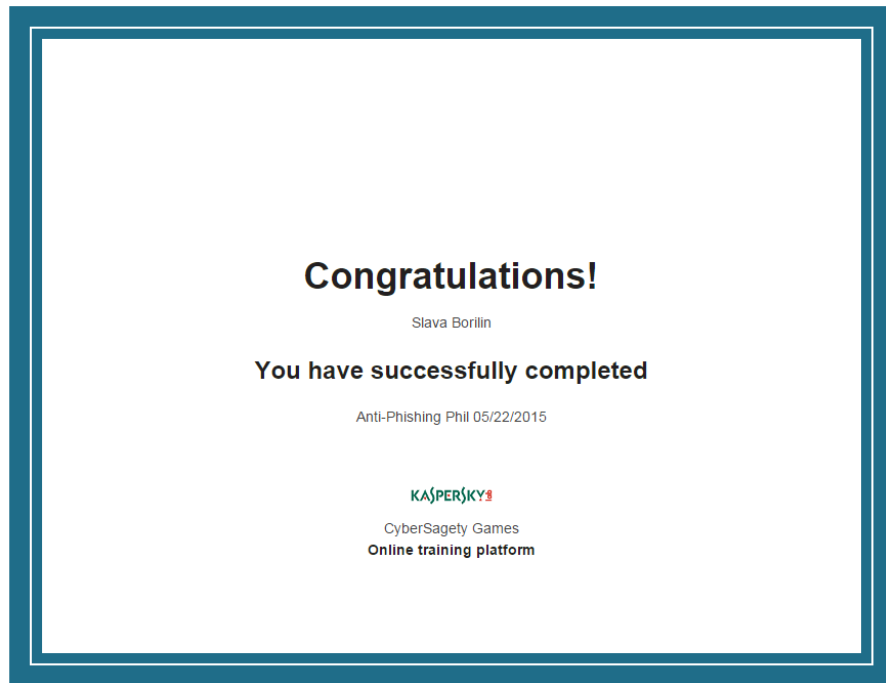
I acknowledge that I have completed and understand the material in this Training Module, including the Password security policy of my company.

Accept
 Decline

Exit

On-site training manager can add security policy details, links, IT Security team contacts to the end of training modules.

CERTIFICATES TO AWARD EFFORTS



User can get customer certificate after the training is completed

Print Exit

CERTIFICATES TO AWARD EFFORTS

Create a CyberStrength Assessment

Select Subject Areas

Assessment Name: Slava

Subjects

3 selected of 9		<input type="checkbox"/>
Phishing (13 questions) Identify Phishing Threats	<input checked="" type="checkbox"/>	
Data Protection (10 questions) Protect and dispose of data securely	<input checked="" type="checkbox"/>	
Mobility (19 questions) Work safely outside the office	<input checked="" type="checkbox"/>	
Internet Browsing (17 questions) Use the Internet Safely	<input type="checkbox"/>	

Cancel

Define length and domains to assess employees and organization's cybersafety as a whole



INTERACTIVE QUESTIONS TO CHECK LEVEL OF COMPETENCE



CyberStrength

On the Road: Safe or Unsafe?

2/20

Is the displayed activity safe?



Amy picks up her order at the counter.



Safe

Unsafe

INTERACTIVE QUESTIONS TO CHECK LEVEL OF COMPETENCE



CyberStrength

Data Protection and Destruction

6/20

Choose the best answer:

! Which of these is the best way to share sensitive data with colleagues?

- A** Via a cloud-based file sharing app like Dropbox
- B** Via a CD that can be shredded
- C** Via a secure corporate server
- D** Via an encrypted company email

SIMULATED PHISHING ATTACKS: READY-TO-GO TEMPLATES



Security Education Platform

Select Attack Category

Select the category below which most closely matches the type of

1 OF 1

Category	Description
Personal	Scams about your personal accounts
Social Network	Scams About Social Networks
Work Related	Scams involving work related accounts or information
Attachments	Scams asking a user to open an attachment
New Templates	Recently added phishing attacks
Logistics	Scams focusing on package delivery
Seasonal	Scams focusing on seasonal events
Financial	Scams About Your Bank
Custom	Create your own email from scratch



SIMULATED PHISHING ATTACKS: RELEVANCE AND VARIETY

Select Attack : Work Related

Select a phishing attack from the list below:

Language:

1 OF 1

Name	Description	Failure Rate
Corporate e-Faxx message	The user receives a 5 page e-Faxx message containing a PDF link.	25.53 %
Email Improvements	Tells the user that there is a more secure email system and they must click to not lose access.	7.88 %
Email Password Change	Warns the user that their password is about to expire and if they don't change it they will lose access to email.	20.93 %
Email Quota Alert	Warns users their email has run out of space and they may not receive email unless they click a link.	19.24 %
NetworkMeet account suspended	Claims that the user's NetworkMeet account is disabled, they must click to reactivate.	8.94 %
Voicemail Alert	Tries to get the user to click on a link by looking like an automated voicemail alert.	30.03 %

Based on the real-life phishing
Various difficulty

SIMULATED PHISHING ATTACKS: EASILY CUSTOMIZABLE BY YOU

Edit Email Template

Review and make any necessary changes to the phishing email for your campaign.

From Name:

From Address:

Subject:

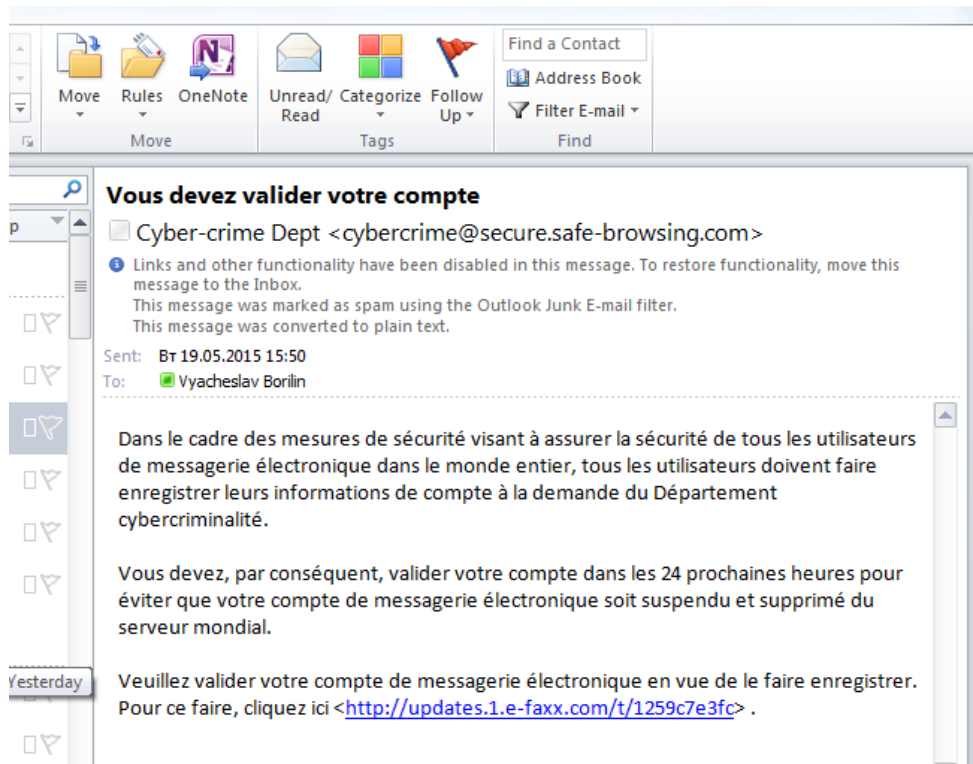
Edit ▾ Insert ▾ Table ▾ Format ▾

B *I* U ▾ ▾ Add Contact Property ▾

Font Family ▾ Font Sizes ▾

Postal notification,
Courier service couldn't make the delivery of your parcel.
Status:An error at the delivery address.
LOCATION OF YOUR ITEM:Cincinnati
STATUS: sorting
SERVICE: Standard Shipping
NUMBER OF YOUR ITEM:U358210589NU
INSURANCE: No
Label is enclosed to the letter.

SIMULATED PHISHING ATTACKS: EMPLOYEE RECEIVES PHISHING AND CLICKS...



Learning experience obtained by shocking (while actually safe) aftermaths of clicking to artificial phishing email

SIMULATED PHISHING ATTACKS: EMPLOYEE RECEIVES PHISHING AND CLICKS...

Oups ! Le courriel auquel vous venez de répondre était un courriel d'hameçonnage factice. Pas la peine de s'inquiéter ! Il vous a été envoyé pour vous aider à apprendre à éviter les attaques réelles. Veuillez ne pas partager votre expérience avec vos collègues, pour qu'ils puissent également apprendre.

John reçoit un courriel urgent...

Ce courriel paraît important. Je ferais mieux d'agir au plus vite.

ARRÊTEZ-VOUS !

Vous auriez pu vous faire avoir par cet hameçonnage par courriel. Les pirates utilisent les courriels pour voler des informations confidentielles.

Voici comment les escrocs essaient de vous tromper...

Dans le cadre des mesures de sécurité visant à assurer la sécurité de tous les utilisateurs de messagerie électronique dans le monde entier, tous les utilisateurs doivent faire enregistrer leurs informations de compte à la demande du Département cybercriminalité.

Vous devez, par conséquent, valider votre compte dans les 24 prochaines heures pour éviter que votre compte de messagerie électronique soit suspendu et supprimé du serveur mondial.

Je vous envoie ce qui paraît être un message important ou intéressant pour vous persuader de répondre immédiatement.

Le courriel paraîtra légitime, mais c'est une ruse. Dès que vous répondez avec des informations ou que vous cliquez sur des liens, j'ai facilement accès à vos données ou à vos comptes en ligne !

Comment vous protéger...

1 Ne révélez jamais des informations personnelles, commerciales ou financières en réponse à un courriel non sollicité.

2 Ne cliquez pas, ne répondez pas ou ne remplissez pas les formulaires envoyés dans des courriels suspects.

Nom : **John Smith** Numéro de sécurité sociale : **111-11-111**

3 Pointez sur les liens pour afficher leurs véritables sources.

<http://updates.1.e-faxx.com/t/1259c7e3fc>

Ne craquez pas d'une de logos et de marques familières. Plutôt

Hmmm... je ne suis plus si sûr de ce courriel maintenant. Je vais y regarder de plus près avant de répondre.

J'aurais pu avoir accès à de précieuses informations ! Il aurait suffi d'un clic !

- Landing page = Teachable moment
- Auto-assignment of training (employee is redirected to the relevant training module after he/she reacted to the simulated attack)
- Statistics

ONLINE TRAINING PLATFORM: ANALYTICS AND REPORTS

Assignment Details

Most Missed Report

Module Performance

Module Completion Summary

Policy Acknowledgement

User Report Cards

User Record Export

CyberStrength Risk

For Simulated phishing attacks:

Archived Campaigns

Campaigns Report

Contact Groups

Device Type

Repeat Offenders

Twelve Month Trend

ONLINE TRAINING PLATFORM: ANALYTICS AND REPORTS

XYZ Company (DC)

CyberStrength Assessment Report

Assignment: Baseline Knowledge Assessment - CYB

[Change Report Criteria](#)

General Information

Overall Score: 85%

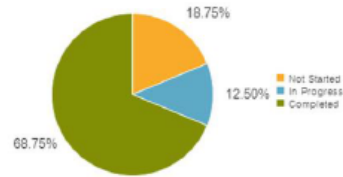
Number of Users: 18

Total Number of Questions: 10

Question Generation Type: Administrator Defined

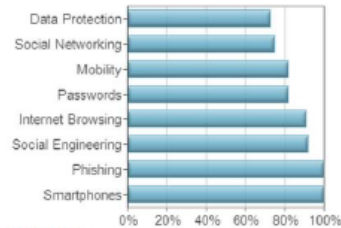
Subject	Number of Times Asked
Data Protection	22
Internet Browsing	11
Mobility	11
Passwords	22
Phishing	12
Smartphones	12
Social Engineering	12
Social Networking	12

Assessment Status



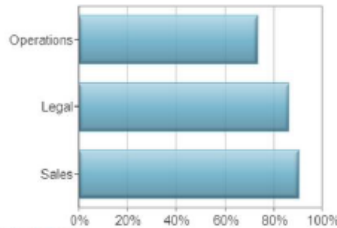
Know security skills strength in particular domains from summary down to individual level

Score By Category



[Click for Details](#)

Score By Group



[Click for Details](#)



DELIVERY AND SET-UP

KASPERSKY LAB WILL PROVIDE

- User Account for the Online Platform
- Training for Administrators
- Technical support

CUSTOMER IS RESPONSIBLE FOR

- Loading the employee emails into the platform
- Creating:
 - Simulated attacks
 - Assessments
 - Training Programs
- Groups assignments
- Analyzing the results

TRY OUT THE INTERACTIVE DEMO AND ASK US FOR DETAILS!

[www.kaspersky.com /demo-sa](http://www.kaspersky.com/demo-sa) – free interactive demo of training modules and simulated phishing attacks

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

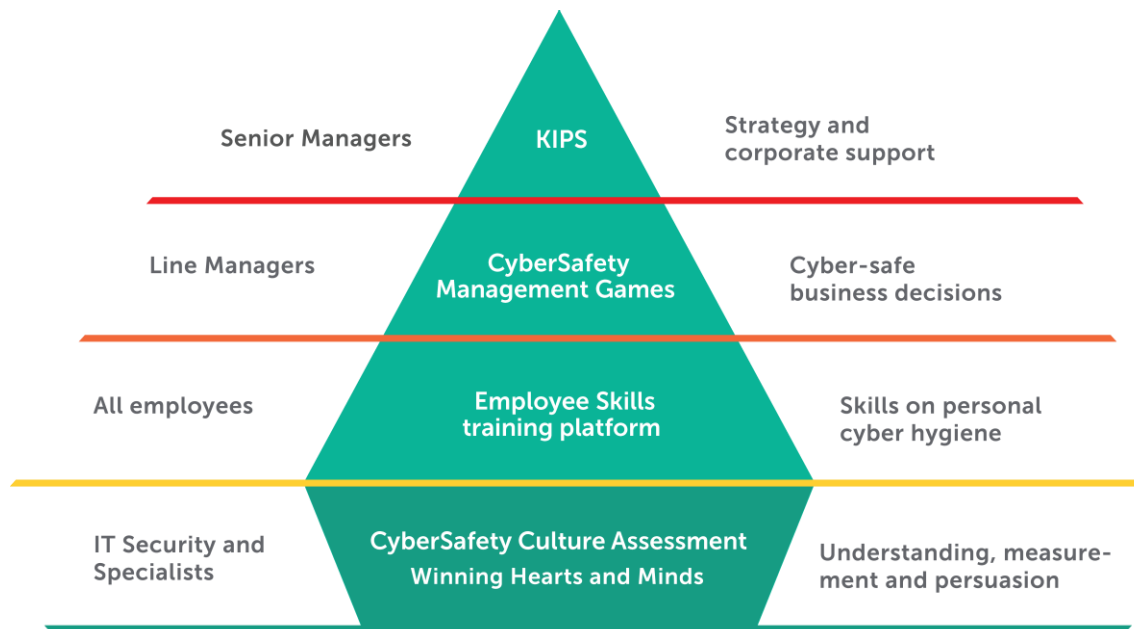
INTERACTIVE TRAINING MODULES

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

ALL KASPERSKY SECURITY AWARENESS TRAINING PRODUCTS

- 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.

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 more buildings and a highway. The overall scene is a mix of urban architecture and natural light.

WE PROTECT WHAT MATTERS MOST

KASPERSKY LAB

www.kaspersky.com/awareness