kaspersky

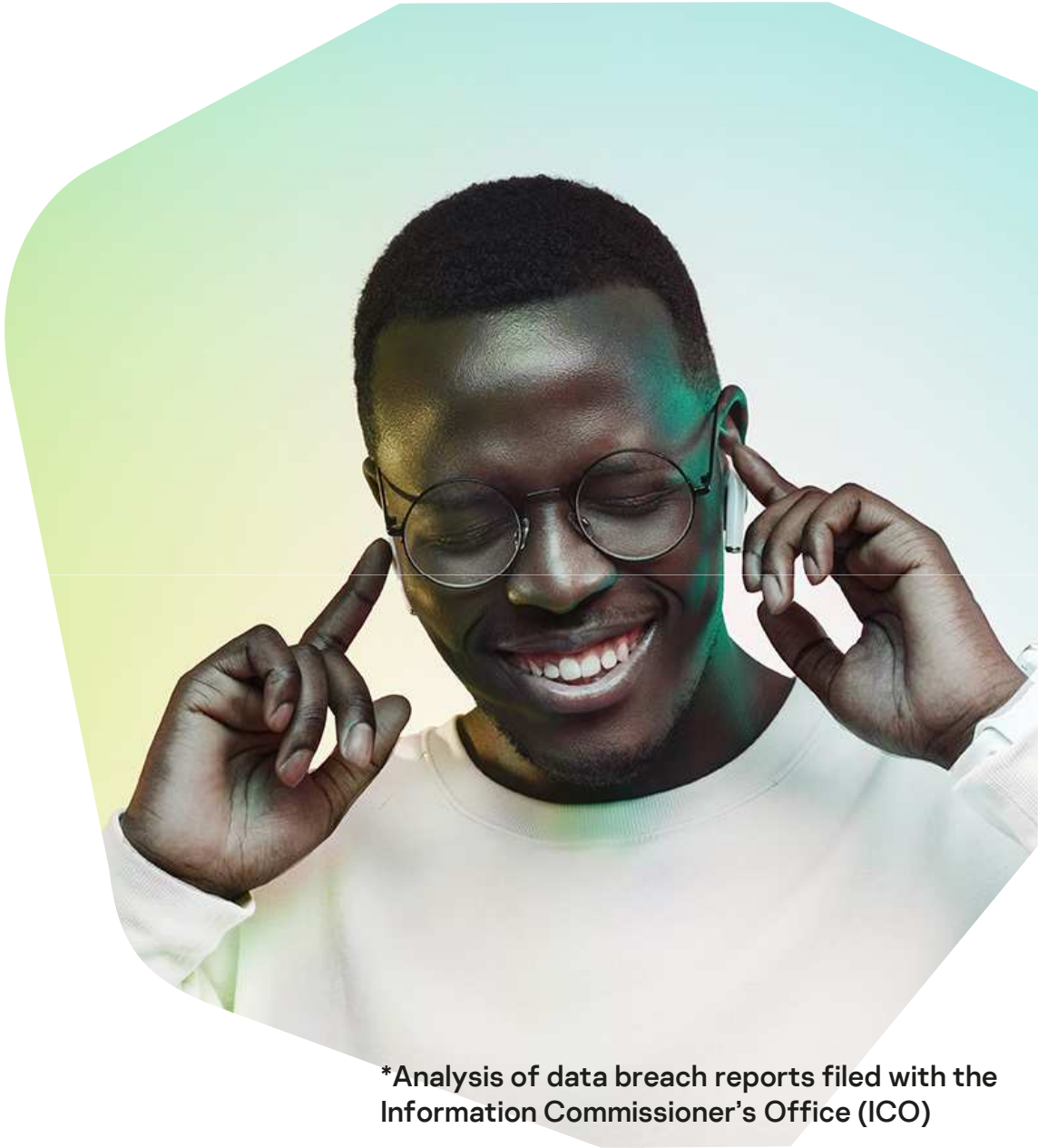
How to train the HOS

Bogdan Albu – Territory Channel Manager
Romania, Bulgaria and Moldova

Human error – the main source of cyber-incidents

90%* of all **cyber-incidents** can be attributed to human error

Exploiting human weaknesses like inattention, ignorance or negligence is so much easier and cheaper than trying to fool sophisticated protection software



*Analysis of data breach reports filed with the Information Commissioner's Office (ICO)

People are the weakest link in corporate cybersecurity

52% of companies regard employees as the biggest threat to corporate cybersecurity *

60% of employees have confidential data on their corporate device (financial data, email database, etc.) **

30% of employees admit that they share their work PC's login and password details with colleagues **

23% of organizations do not have any cybersecurity rules or policies in place for corporate data storage **

* *Research: "The cost of a data breach", Kaspersky, Spring 2018.*
** *"Sorting out a Digital Clutter". Kaspersky, 2019.*

Employees make mistakes. Organizations lose money...

Employee behavior is a major IT security risk, despite traditional awareness programs being in place:

$1,195,000

per enterprise organization

The average financial impact of a data breach caused by inappropriate IT resource use by employees*

$116,000

per SMB

The average financial impact of a data breach caused by inappropriate IT resource use by employees*

52%

of enterprise organizations

Experienced cybersecurity incident as a result of inappropriate IT recourse use by employees

(50% of SMB)**

more than

$1,7Bln

global financial losses

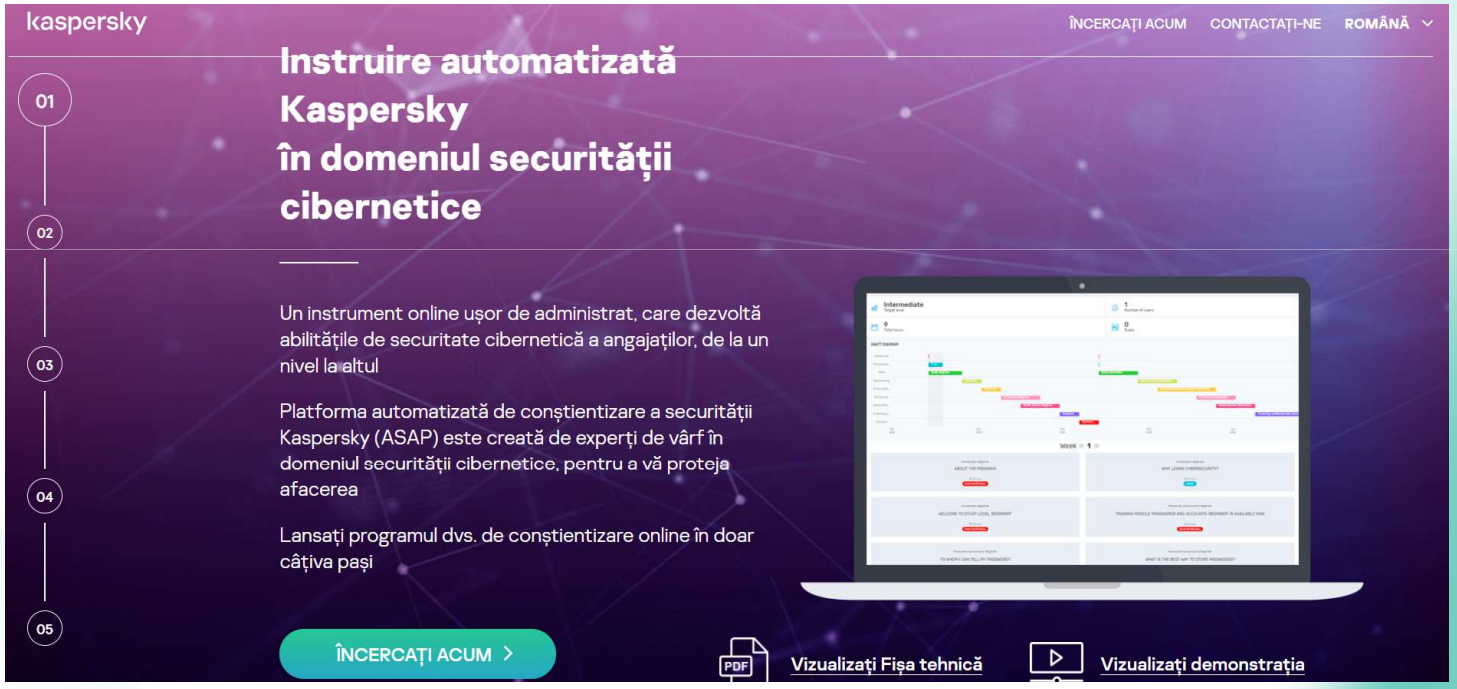
Resulted from business email compromise complaints***

* Report: "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives . Kaspersky Lab, 2019
** Report: "IT security economics in 2019', Kaspersky
*** FBI "2019 Internet Crime Report"

Engaging security education for organizations of any size

Learning made easy for SMB/ENT:

Kaspersky Automated Security Awareness Platform



Learn

online or on mobile

- Pre-determined learning efficiency for **employees**
- Time-saving program administration for **companies**
- **Romanian**

Instant free trial at: www.asap.kaspersky.com/ro

Company
Kaspersky Ro

English | Bogdan Albu

Dashboard | Users | Training groups | Content New | Phishing simulator | Company settings

My actions

- Add new users
- Import and syno
- Start Group Training
- Add to training
- Pause Training
- Resume Training
- Download report

Users and training slots

Training in progress	3
Completed	0
Unassigned	0
Paused	0
Total users	6

6 Total number of available training slots

10 Total number of training slots

Recommendations

1. Check out the features of the platform:
   - the training program for each level can be found in the Content section
   - the schedule of each group is created automatically depending on the selected training program
2. Prepare training
   - add users, put them into groups manually or by applying rules.
3. Start training and supervise those who needs attention

FAQ

Demo videos

New

Graphic materials

Posters, screensavers, and comics to increase your employees' knowledge of cybersecurity basics

Who needs my attention?

Main course

Won't finish on time	0
Significantly behind schedule	0

Who needs my attention?

Express course

Employees in training

3

February 06 — March 06

Skills learned on average

0

Notifications about phishing by month

After installing the Report Phishing plugin, you can see how often your employees send in suspicious emails for verification.

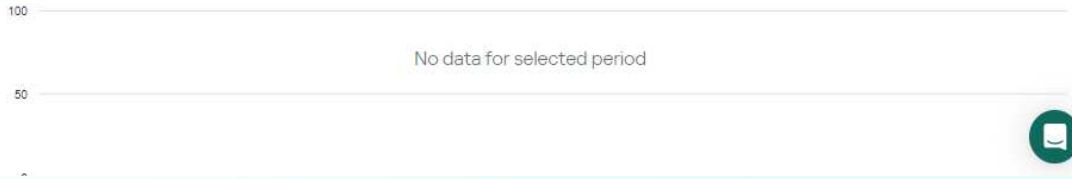
Plugin not installed or employees don't use it

Configure plugin

Phishing emails

3 months | Add filter

Take into account phishing from the Main Course



Contents

Main course | Express course

Level
Beginner

Email | Passwords and accounts | Websites and the internet | Social Media & Messengers | PC Security | Mobile Devices | Confidential Data | Personal data | GDPR | Physical data security | Industrial Cybersecurity | Bank card security and PCI DSS

Table of Contents

Lesson plan

Available languages

Lesson

- Email account danger
- What you should do if your email is hacked
- What to look out for when asked to enter your email password
- What kinds of data shouldn't be sent via email
- Dangerous emails and how to spot them

Email Reinforcement

Email: Beginner

Email is a crucial tool, and everyone uses it. But even with a corporate email account, people still use their personal email to send and receive work files, discuss work-related issues, and even access corporate resources (especially if employees work from home).

But your email account is also the key to most other online resources, and cybercriminals know this. They use all sorts of methods to gain access to email accounts, such as stealing passwords using malware, or tricking the account owner into giving their password away. As an example of how widespread these practices are, just check out the 2015 hack of CIA Director John Brennan's email account.

What does your company gain when employees study this topic?

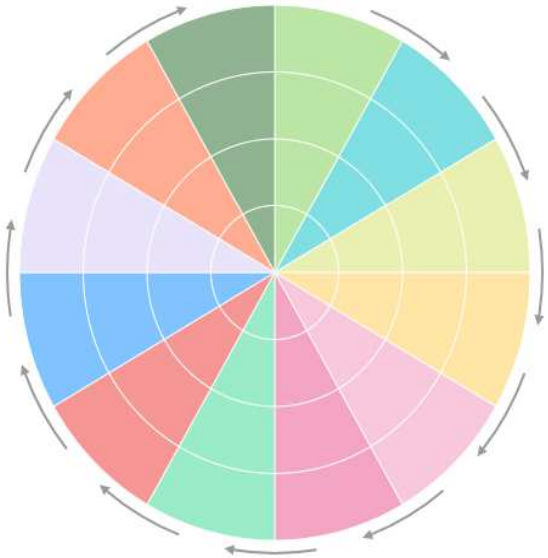
- Reduced risk of corporate email hacks
- Reduced potential loss of confidential data by employees
- Decreased risk of corporate network malware infections

The lesson also teaches about
#Passwords #Phishing #Dangerous messages #Bank cards

Contents

Main course | Express course

Security Awareness Training Plan



Email | Passwords and accounts | Websites and the internet | Social Media & Messengers | PC Security
Mobile Devices | Confidential Data | Personal data | GDPR | Physical data security | Industrial Cybersecurity
Bank card security and PCI DSS

About the program | About levels

The platform's library is conveniently divided into units, or different study topics and difficulty levels.

During training, users acquire real-world knowledge and skills. The complete course includes the mastering and application of more than 450 basic skills.

Training is carried out one unit at a time. Each unit covers a specific topic at a certain difficulty level of the program. Each unit has several lessons that last between 5 and 15 minutes each. These lessons are further reinforced by study guides, tests and simulated phishing attacks (when applicable).

Here you can see which practical skills are developed in each unit and take a look at sample lessons and tests.

Hashtags

#Passwords #Phishing #Corporate accounts #Dangerous messages #Bank cards #Ransomware #Social Engineering #Dangerous Files #Working with browsers #Corporate ethics

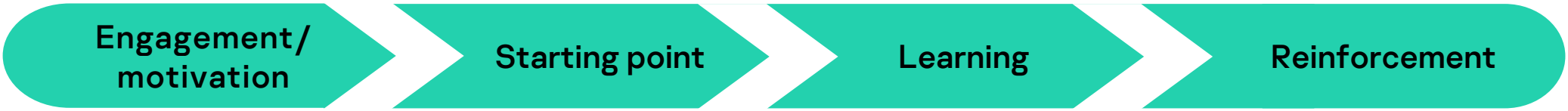
#Antivirus #Malicious software #Applications #Browser #Confidential information #Storing information #Sending information #Personal data #Internet and the law #European legislation

#Business #Dangerous Links #Fake websites #Ransomware sites #Backup #Mobile data #Encryption #Cloud services #Industrial espionage #PCI DSS

#Two-factor authentication #Digital footprint #Torrents #Catfishing #Targeted attack #Hashing #Tokens #Pattern locks #Mining #Parental control

Our approach is to build a continuous learning cycle – as sustainable change in behavior is only possible over time and including multiple components

Continuous learning cycle



- Why do I need this?
- Cognition

- Am I aware?
- What do I know and where are the gaps?

- Micro learning
- Continuous learning
- Adaptivity

- Did I get it right?
- Do I remember this?
- Do I act accordingly?

Try
challenge yourself

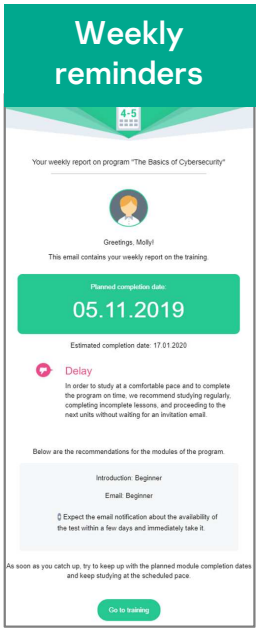
Learn
online or on mobile

Live
your life with new skills

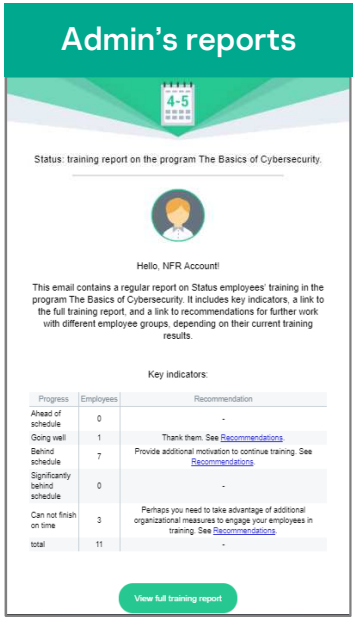
Notifications are part of internal communications

ASAP saves hours of administrative work

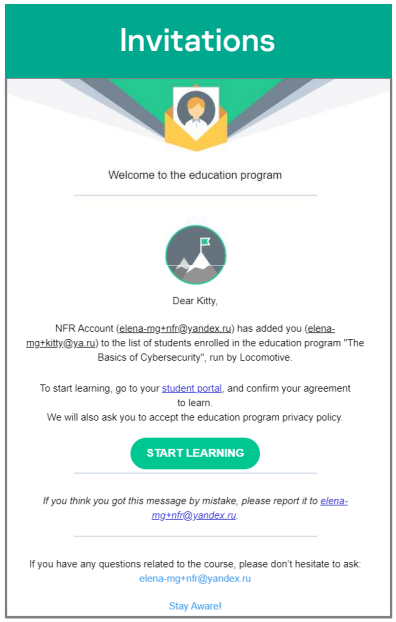
Weekly reminders



Admin's reports

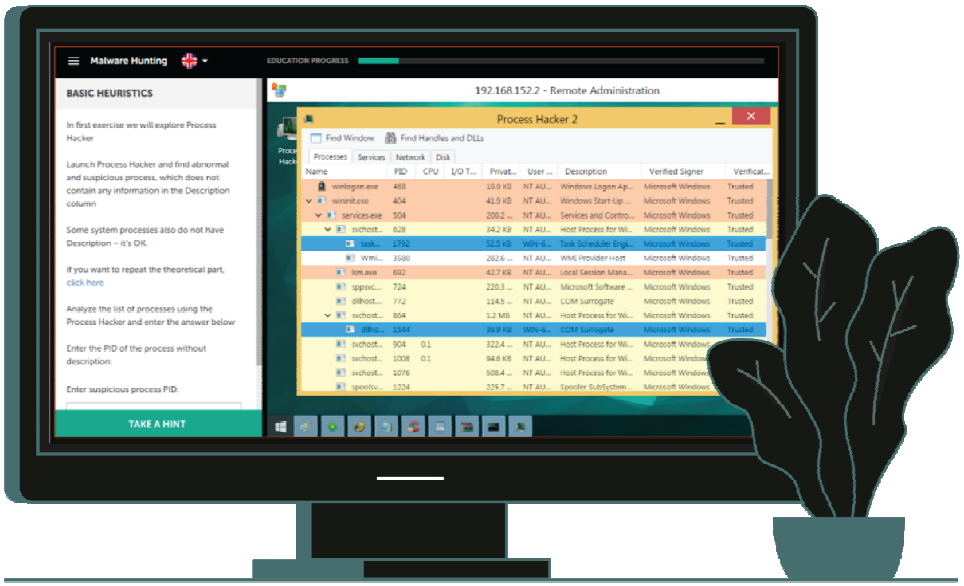


Invitations



Certificates

Learning made insightful for IT teams:
Cybersecurity for IT Online (CITO)



Security Awareness Online Training
for IT generalists (IT support, service desks, etc.)

Learn

online or on mobile

Empower “first line of defense” in the cyber incident response

Decrease the number of incidents caused by misconfiguration mistakes

Develop the critical thinking for IT teams on cybersecurity

Cybersecurity for IT Online: 4 modules, ~ 30 practical exercises; Cloud or On-premise

Malicious Software

Verification of the existence or absence of an incident related to malware.

#Processhacker, #Autoruns, #Fiddler, #GMER

Potentially Unwanted Programs

Working with system event monitors and sandboxes. Using statistical engines (virustotal). Removing PuPs.

#ProcessMonitor, #Cuckoo, #Virustotal

Phishing Incident Response

Phishing emails lookup. Verification of an incident related to phishing. OSINT

#ExchangeComplianceSearch , #Robtex, #Whois, #GoogleDorks

Investigation Basics

Incident localization, data collection, collecting digital evidence, log and timeline analysis.

#EventLogExplorer, #Autopsy, #FTK-Imager

NIS2 Directive (Network and Information Security) is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.

In 2016, the EU adopted the NIS Directive.
On 27.12.2022, the EU is deepening this framework, represented by the new Cybersecurity Directive, the so-called NIS2

The transposition deadline (i.e. the deadline for Member States to transpose the current Directive into national law) is set to 16 October 2024

Article 20, mandatory training of senior management and greater management responsibility for ensuring cyber security in the organization;
It applies to all members of the governing bodies of obliged persons and must receive training to provide them with sufficient knowledge and skills to identify risks and assess cyber security risk management practices and their impact on the services provided.

kaspersky

Stay aware. Stay safe.

Bogdan.Albu@kaspersky.com

www.kaspersky.com/awareness
www.k-asap.com/ro