DON’T GET HACKED!

DEVELOP BETTER CYBER SECURITY TRAINING

Adam Filler, Kaspersky Security Awareness

www.kaspersky.com/awareness

KASPERSKY lab

Who we are

Essentials

Founded in 1997 and led by Eugene Kaspersky

Present on 5 continents in 200 countries and territories

Provides innovative IT security solutions and services for business and consumers

Numbers

>20 million product activations per year

> 3,900 highly qualified specialists

USD 698 million — global unaudited revenue in 2017*

Achievements and Industry Recognition

One of the four biggest endpoint security vendors**

Kaspersky Lab received the Platinum Award as part of the 2017 Gartner Peer Insights Customer Choice Awards for Endpoint Protection Platforms***

Our solutions are the most tested and most awarded in independent tests and reviews****

> 400,000,000

users worldwide are protected by our technologies

* According to International Financial Reporting Standards (IFRS)
** IDC - Worldwide Endpoint Security Market Shares, 2015 - Nov 2016 US41867116
*** The Gartner Peer Insights Customers' Choice Logo is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers' Choice distinctions are determined by the subjective opinions of individual end-user customers based on their own experiences, the number of published reviews on Gartner Peer Insights and overall ratings for a given vendor in the market, as further described here and are not intended in any way to represent the views of Gartner or its affiliates.
****kaspersky.com/top3

KASPERSKY lab

Customer Reach

Our Next Generation solutions and services are available for a wide range of clients: from individual home users to large and small organizations, including big enterprises, critical infrastructure networks and governments

INDUSTRIAL FACILITIES

ENTERPRISES

SMALL AND MEDIUM BUSINESSES

VERY SMALL BUSINESSES

CONSUMERS

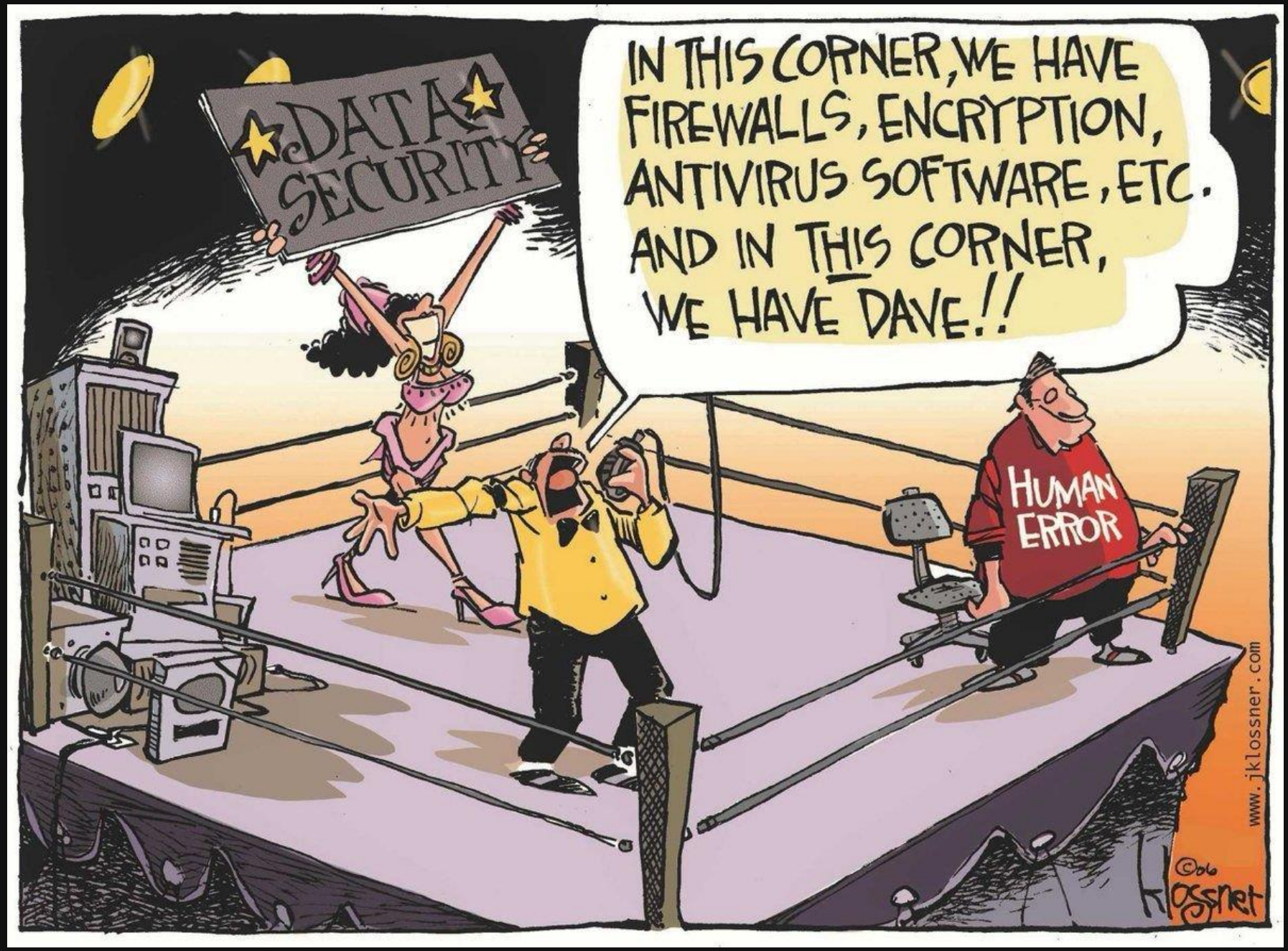
>270,000

Corporate clients worldwide

>400,000,000

Users worldwide are protected by our technologies

KASPERSKY lab



THIS IS ABOUT MONEY…

Despite traditional awareness programs being in place:

$1,155,000

per enterprise organization

The average financial impact of attacks caused by careless/ uninformed employees*

$83,000

per SMB

The average financial impact of attacks caused by careless/ uninformed employees*

$101,000

per SMB

The financial impact of attacks caused by phishing/social engineering*

($1,3M per enterprise)

up to $400

per employee per year

The average cost of phishing attacks alone**

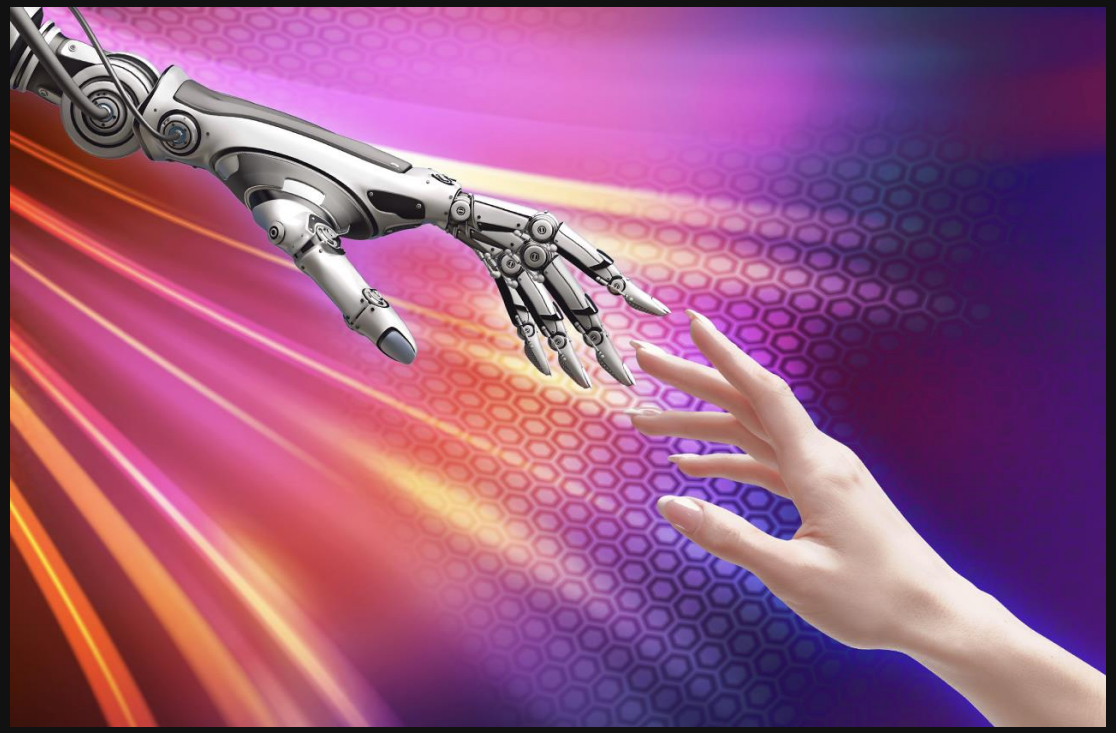
* *Report: "Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", Kaspersky Lab and B2B International, June 2017.*

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

BUT THERE IS MORE AT STAKE…

Digital Capability- key challenge of our age

- Security Awareness is a primary building block of Digital Capability
- It is a foundational security layer, designed to bridge ‘real’ and virtual worlds
- Spread of digital literacy is the starting point
- Everyone on the planet needs to do this



WHAT COMES TO MIND WHEN CYBERSECURITY AWARENESS IS MENTIONED?

PLEASE WRITE IN CHAT – 2 minutes

KASPERSKY lab

DANGER

BORING

DON’T DO THIS! MORE RULES?

LIMITING FREEDOM

IMPORTANT

DON’T BOTHER ME WITH THIS…

I ALREADY KNOW ENOUGH

NOT MY JOB

CHALLENGES WITH EXISTING AWARENESS PRODUCTS

No clue how to set goals and plan education

Training takes too much time to manage

Reporting does not help in goal tracking

Employees don’t appreciate program → don’t get skills

MOTIVATING THE LEARNERS

KASPERSKY lab

DEMOTIVATION BY MISCONCEPTIONS

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

"Smart hackers will send me a virus and break my PC"

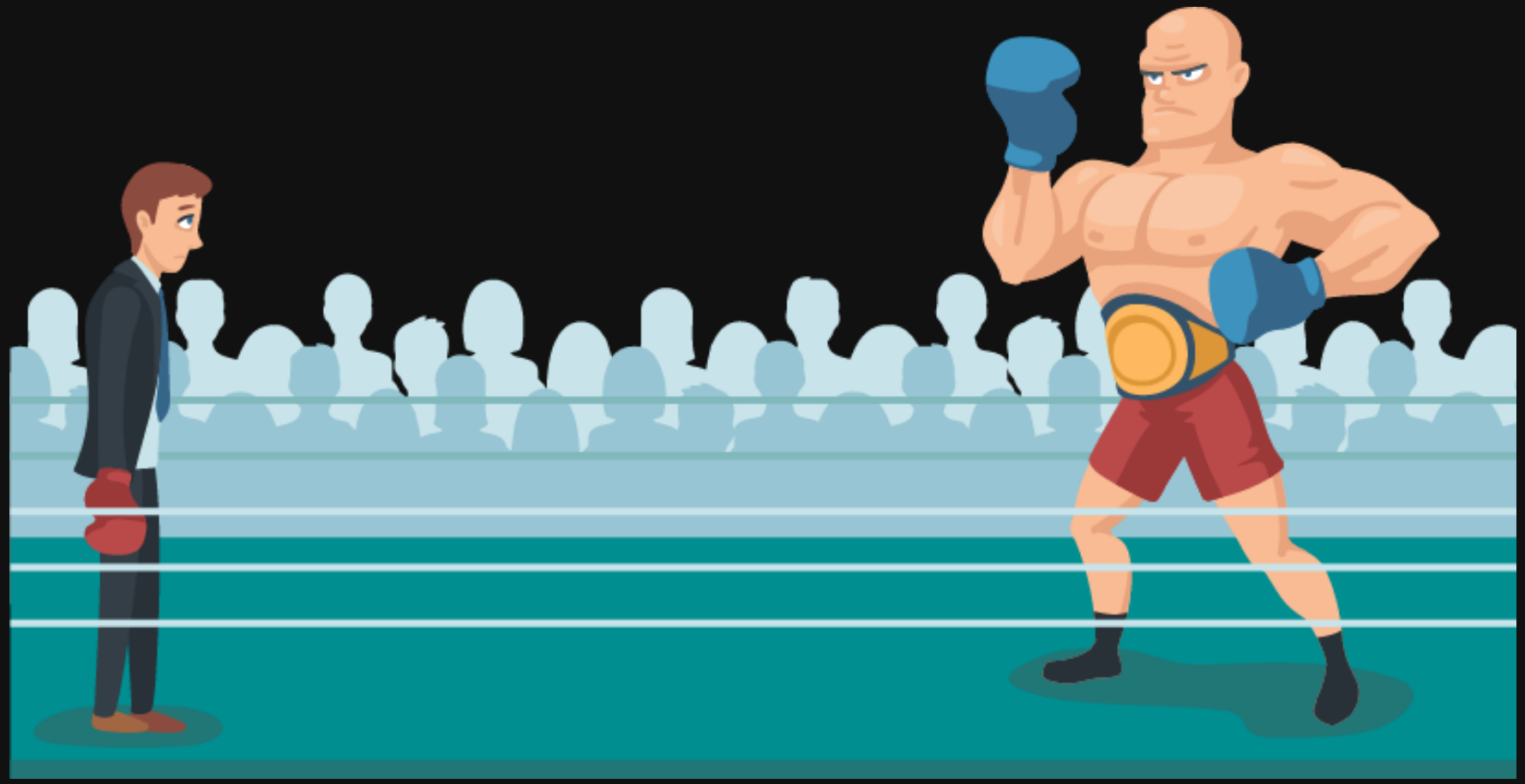
Beware bad people, not broken computers

I understand which criminals can get value from my digital assets and motivated to protect them

"I am too small a target"

"I have no time for security"

DEMOTIVATION



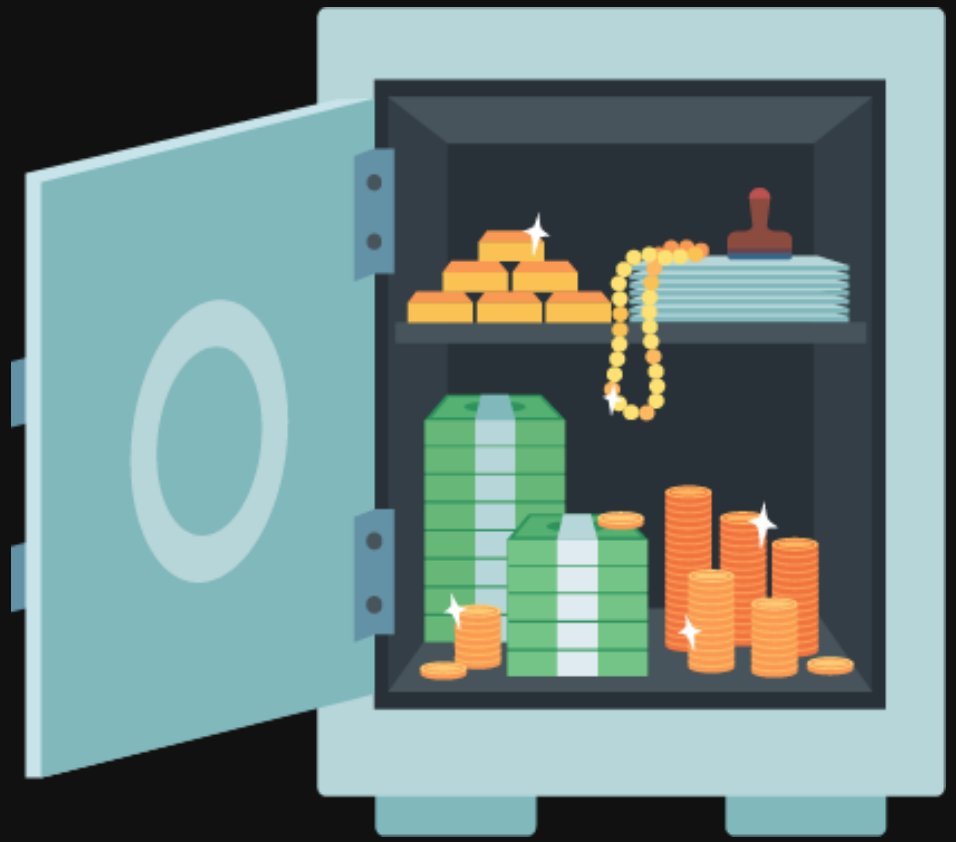
KASPERSKY lab

REALITY

Cybercriminals are neither superheroes nor computer ninjas

OUR VALUABLES

What kind of valuables do we have in the cyber world?



KASPERSKY lab

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

“Hackers will break my PC”	“I am too small a target”	“I have no time for security”
Beware bad people, not broken computers	Small targets are easier and more attractive to cyber criminals	
Think who can misuse what you do	I want to be a harder target than the others	

EVERYONE IS A TARGET

1 x $1000000 = 1000000 x $1

KASPERSKY lab

NO NEED TO OUTRUN THE TIGER

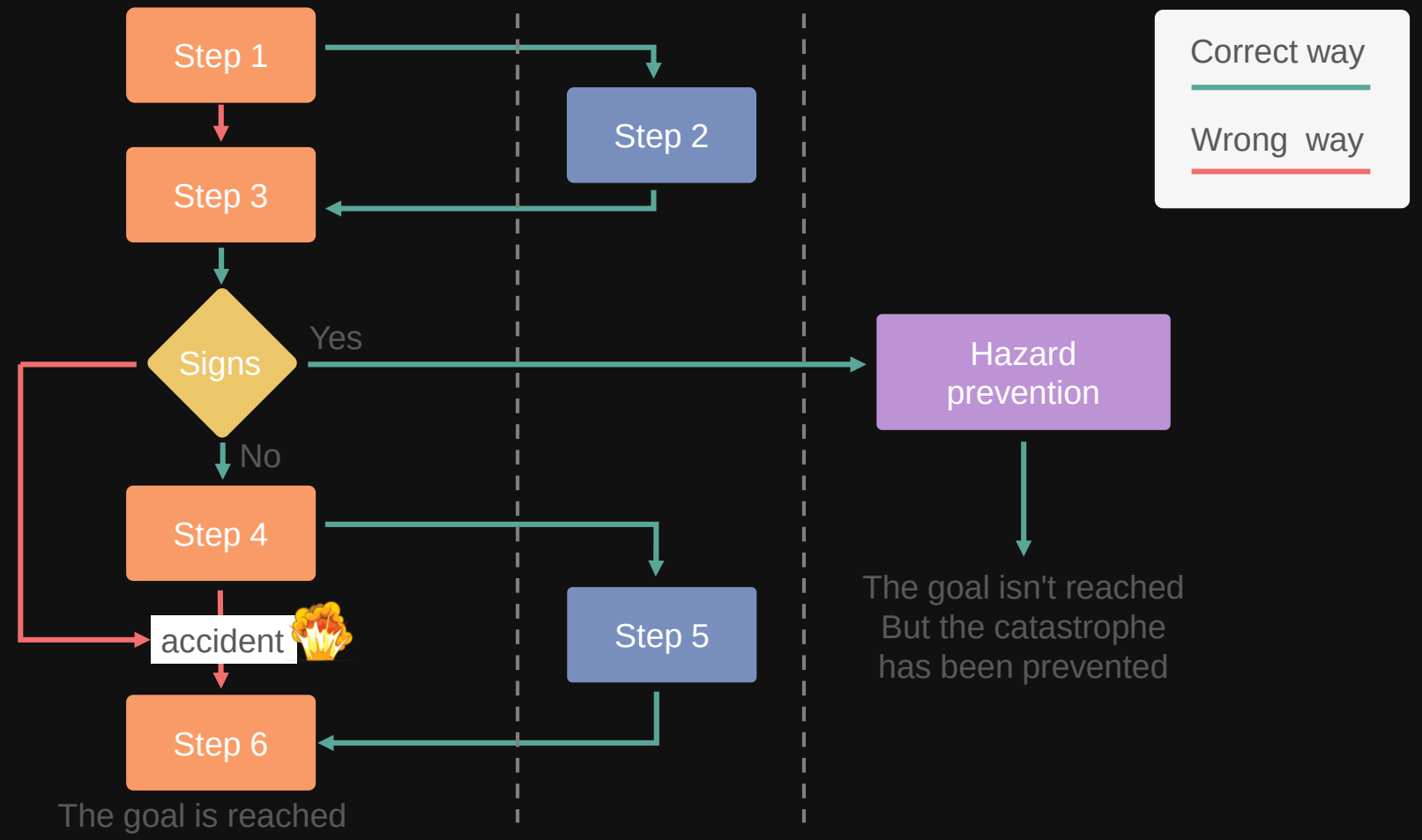
KASPERSKY lab

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

“Hackers will break my PC”	“I am too small a target”	“I have no time for security”
Beware bad people, not broken computers	You don’t have to be a target to be a victim	Security is part of long-term efficiency
Think who can misuse what you do	Be a harder target than the others	I will choose the safest way to achieve the business goal and cooperate with security team

TURNING MISCONCEPTIONS INTO POSITIVE USER ACTIONS

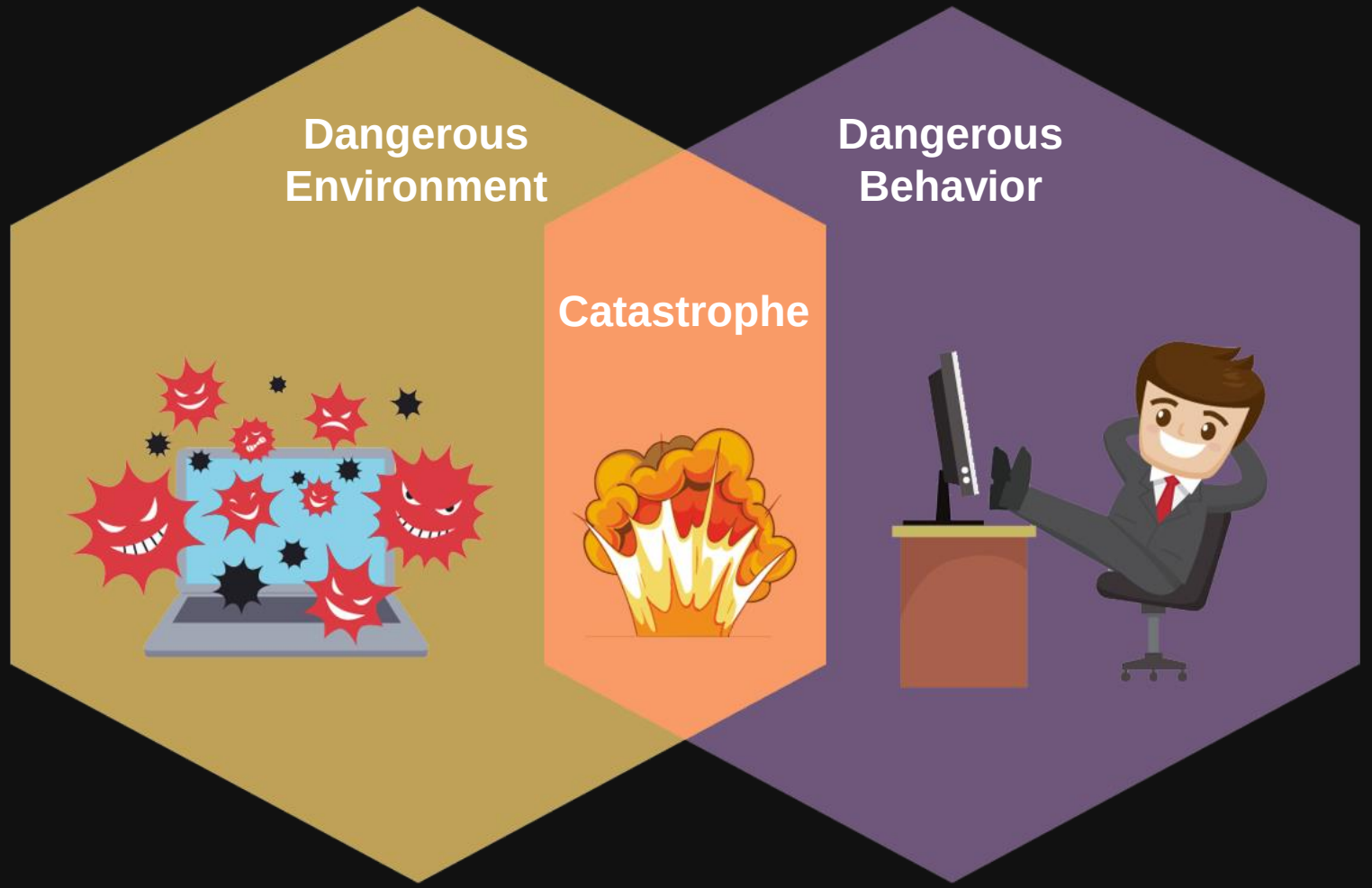
The car analogy – getting from A to B



WHY MOST SECURITY AWARENESS TRAININGS ARE INEFFECTIVE?

1. Transform misconceptions people have on cybersecurity	“Hackers will break my PC”	“I am too small a 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 a harder target than the others	Cooperate with Security team

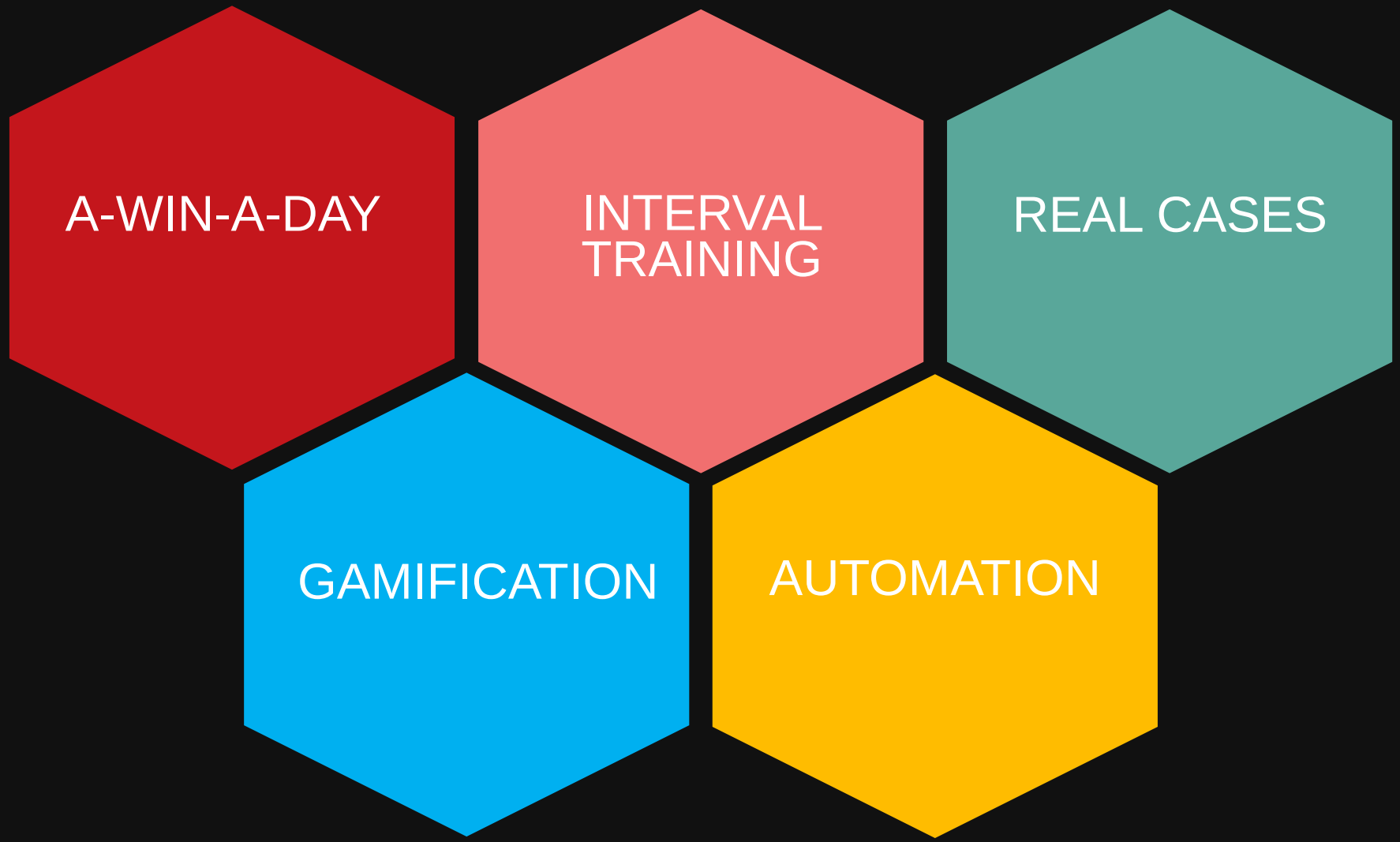
WHY IS THIS IMPORTANT?



HOW DO WE GET TO POSITIVE CYBERSECURITY?

KASPERSKY lab

THE LEARNING FUNDAMENTALS



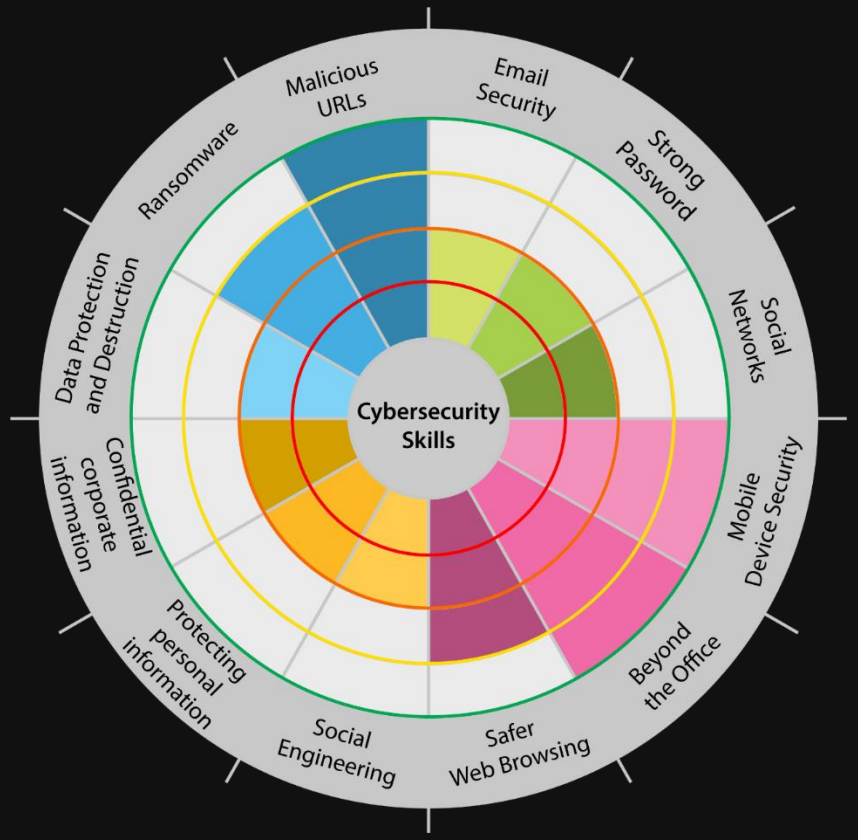
KASPERSKY AWARENESS: LEARNING PRINCIPLES

Key goal of education	**Motivate** -> Raise awareness -> Develop skills -> **Create capability** to identify and resist new threats
Efficiency achieved through	Carefully balanced AI-enabled learning path, featuring **constant reinforcement;** **Different risk levels** for groups of trainees
Content variety	**Interval learning** Lessons + tests + reinforcement emails + simulated phishing attacks = REAL skill acquisition and pattern recognition

- ❑ Learn something new every day
- ❑ 1 lesson 1 skill
- ❑ Use immediately
- ❑ Tell others

Well-defined secure behaviour

Universal multi-level curriculum



Cybersafe behavior comprised of 350 specific skills – examples: email security

- What endangers my email?
- Whom can you tell your email password?
- What should I do if my email is hacked?
- What kinds of passwords should I use for my email accounts?
- Why is it important to use different passwords for your personal and work email accounts?
- What kinds of information should not be sent over email?
- What should you look out for if you're asked to enter your email password?
- Can I open any link from email?
- Are all attachments good to open?
- What should I do about my email accounts today?

Chapter One

EPIC NOVELS

These are works of fiction longer than *110,000 words*, although many of the most popular epics surpass this word limit by a great deal.

A Suitable Boy
Vikram Seth
593,674

Ulysses
James Joyce
265,222

Bleak House
Charles Dickens
360,947

War and Peace
Leo Tolstoy
561,304

Everything I know, I know because of love.
LEO TOLSTOY • WAR AND PEACE

Gone With the Wind
Margaret Mitchell
418,053

Les Miserables
Victor Hugo
530,982

Infinite Jest
David Foster Wallace
483,994

My dear, I don't give a damn.
MARGARET MITCHELL
GONE WITH THE WIND

Chapter Two

FAMOUS SERIES

Fictional series have grown in popularity over recent years and now dominate lists of most-read novels around the world. Some of these are classed as *epic novels*, due to their immense word count, whereas those between *50,000 and 110,000* are classed as *novels*.

A SONG OF ICE AND FIRE
GEORGE R.R.MARTIN

A Game of Thrones
298,000

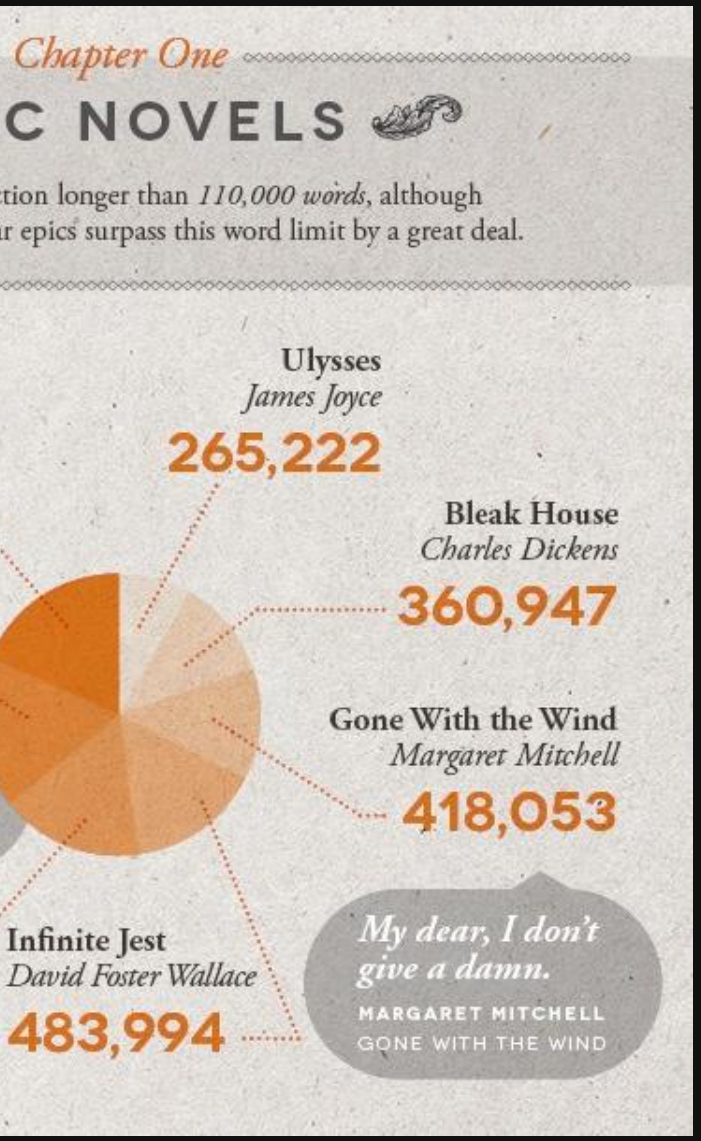
A mind needs books as a sword needs a whetstone, if it is to keep its edge.
GEROGE R.R.MARTIN • A GAME OF THRONES

A Clash of Kings
326,000

A Feast for Crows
300,000

A Storm of Swords
424,000

A Dance with Dragons
422,000



6 SECURITY AWARENESS TOPICS

146 LESSONS

220 LEARNING OBJECTS

264 RECOMMENDED BEHAVIORS

279 CASE ILLUSTRATIONS

272500 WORDS

X

7 LANGUAGES (ACTUAL) +
5 LANGUAGES (IN WORK)

KASPERSKY lab

- INFORMATION AND PRACTICE IN DIGESTIBLE DOSES
- SPORT AND LANGUAGE TRAINING IDEAS

What do you choose to learn English?

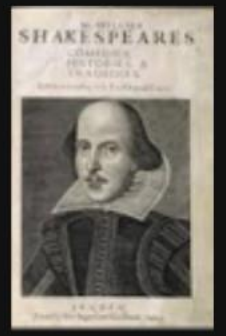
IELTS™

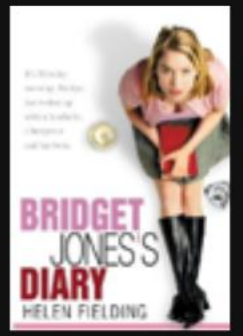
Cambridge Assessment English

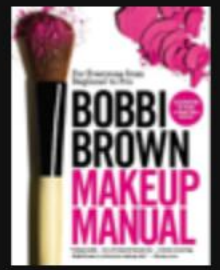
Authorised Exam Centre

ETS TOEFL

GMAT™







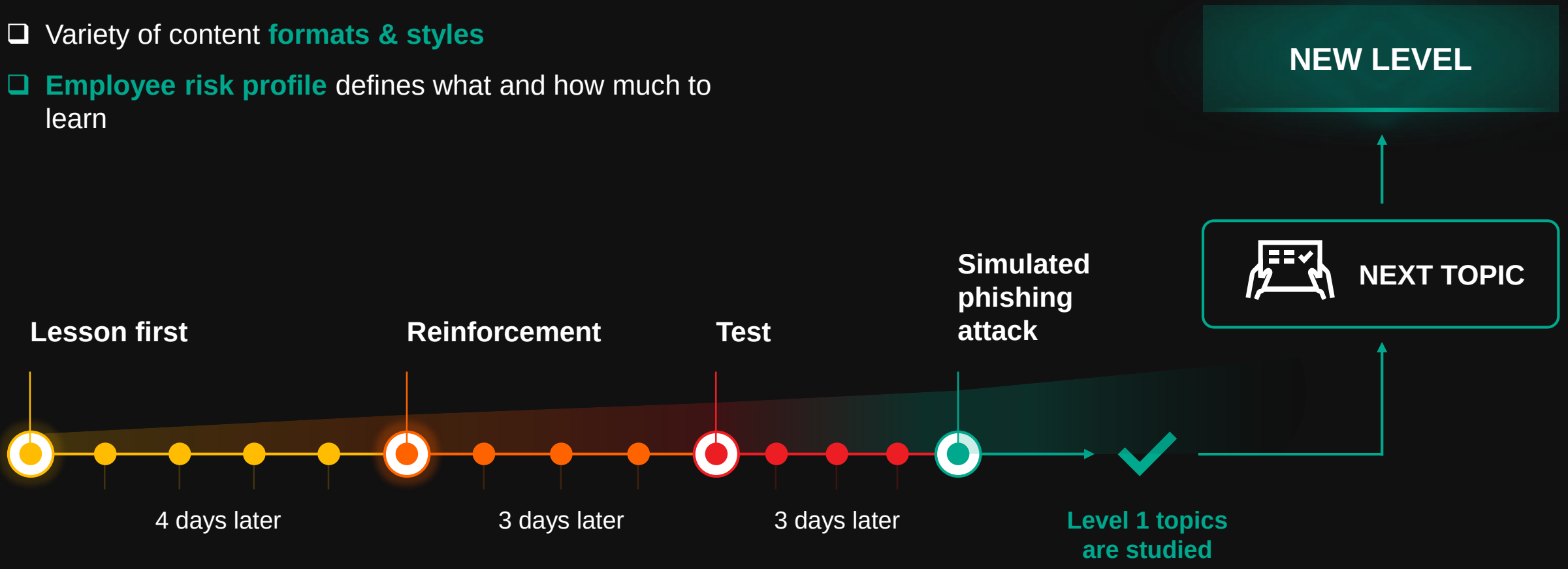
Structured, standardized and measurable training

or

Random library

Learning Management

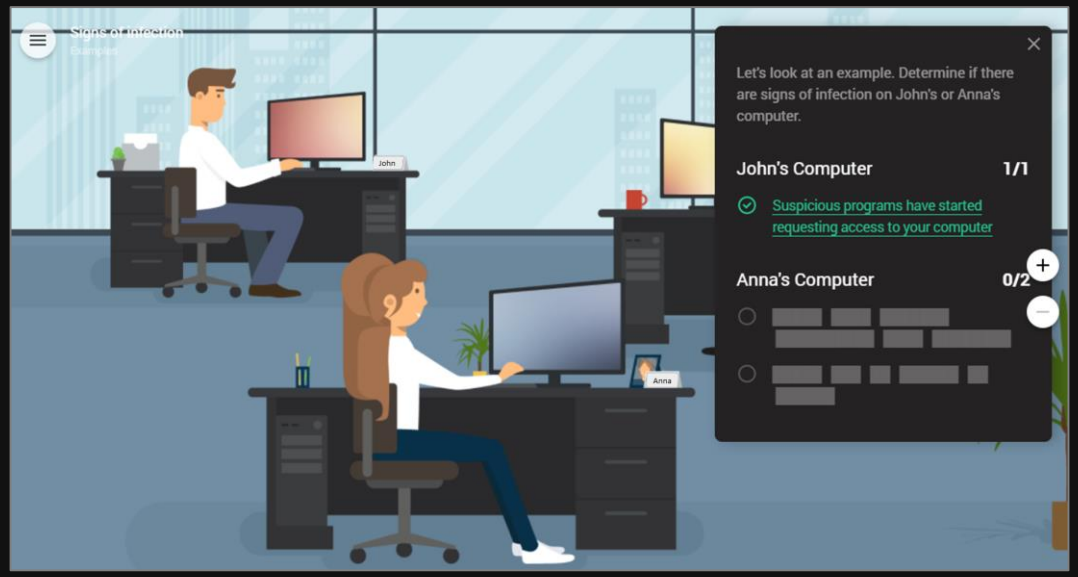
- **Interval learning** at own pace to ensure content retention
- Variety of content **formats & styles**
- **Employee risk profile** defines what and how much to learn



REAL CASES

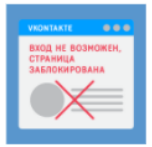
- FRESH RELEVANT INFORMATION
- IMMEDIATELY USEFUL

MOTIVATION + SKILLS + REINFORCEMENT +TEST



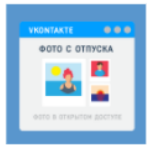
QUESTION 3

What is the danger of giving your social media password to someone else?


My account may be stolen


Money may be removed from my bank account.


Purchases may be made in online stores, and I could lose money.

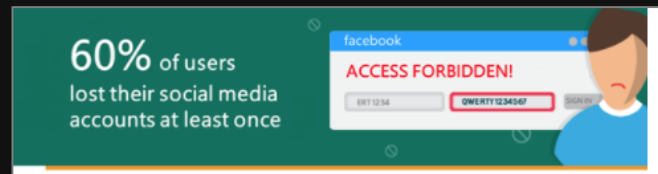

Photos from current or previous significant others may become public.


Spam may be sent in my name.


I may lose important information.


I may lose my achievements in an online game I care about.


Nothing really bad can happen.



Hello, Edward!

You are surely agree that loosing access to your social media account is a big pain.

How to protect yourself and your account:

Use strong and unique passwords to enter your account and never tell it to anyone. Social media is your personal space, and password is a key. Handle it with care.

If you think someone has gained access to your email account, change the password right away and contact helpdesk. For example, if you get a confirmation text message when you haven't done anything to require one.

Do not post scans of your documents (e.g. passport, ID, or airline tickets) – criminals can use it and do damage.

SPAM *People tend to help criminals to rob themselves*

According to Mail.Ru survey, users suffer from criminals in social media more often then during email exchange or online payment.

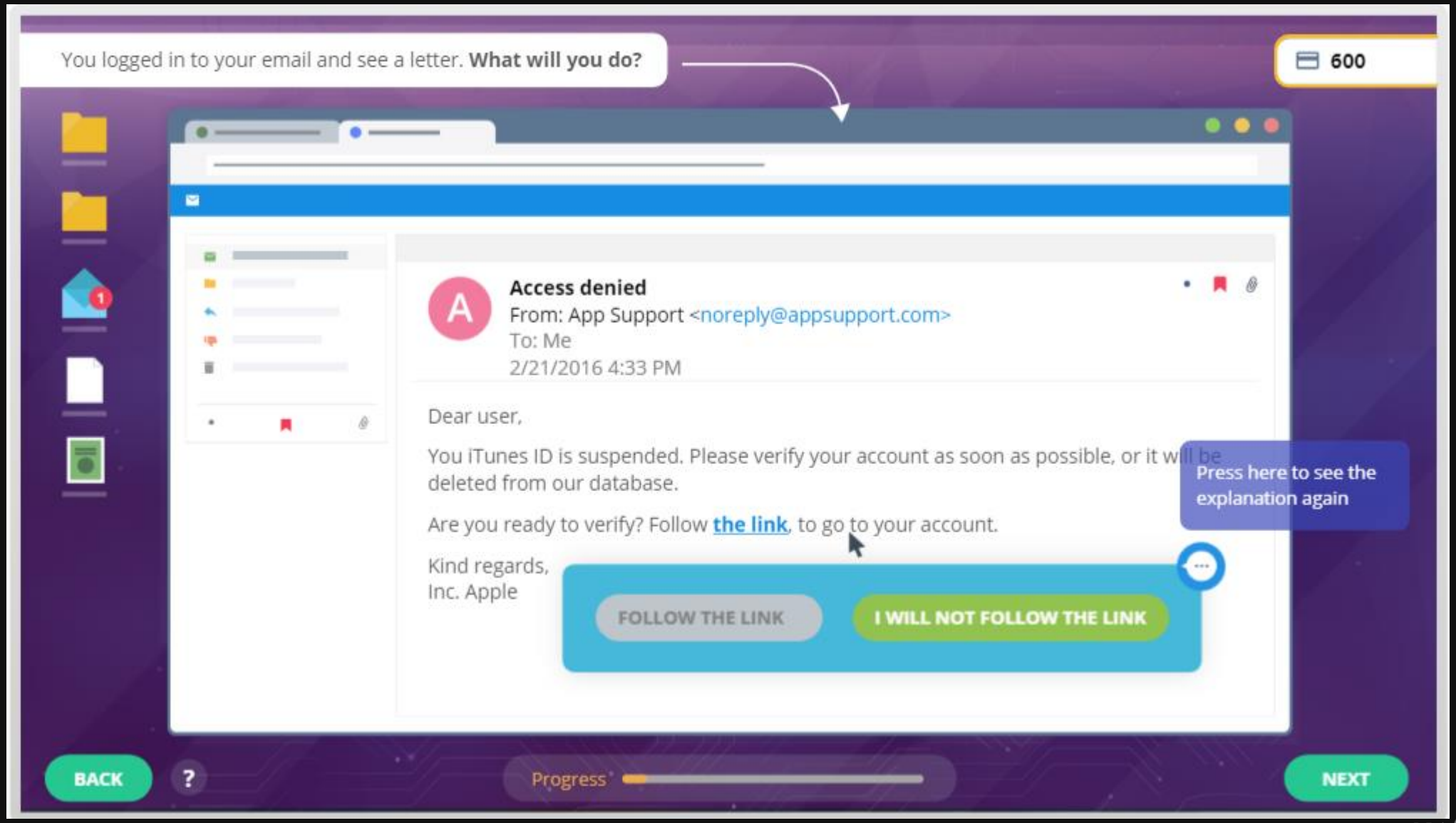
ever found their social media password stolen **48%**

ever received fraudulent messages **58%**

found out that spam is being sent on their behalf **50%**

People frequently (unintentionally or because they're too lazy) help cybercriminals.

CASE-BASED CONTENT



- NOT JUST PRETTY PICTURES
- VARIETY
- BUILD INTEREST

Kaspersky 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
LPA (Local Public Administrations) New!	Web servers, public services issues and GDPR procedures
Oil & Gas	Exploring influence of variety of threats – from website deface to a highly actual ransomware and a sophisticated APT.
Power station / Water Plant	Protecting Industrial control systems
Transportation	Protecting passenger-and-freight carriage against Heartbleed, ransomware and APT

KASPERSKY lab

Two forms of KIPS training

KIPS Live

- up to 80 trainees in the same room
- the same language for all participants
- a trainer and an assistant on site
- printed materials are essential

More limitations, but stronger engagement due to on-site presence and face-to-face competition. Plays as a team-building event as well.

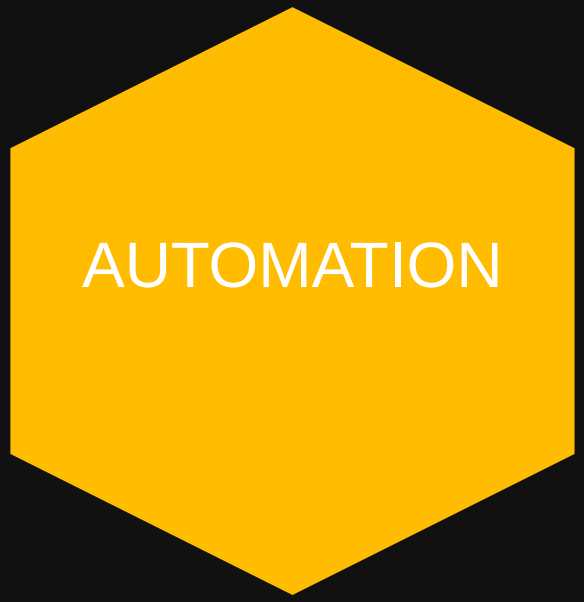
KIPS Online

- up to 300 teams (= 1000 trainees) simultaneously, from any location
- different teams can choose a game interface in different languages
- a trainer leads a session via WebEX

Perfect for global organizations or public activities. Can be combined with KIPS Live to add some remote teams to the on-site

Cybersafety Management Games

- 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 2 to 4 hours.



- LESS WORK FOR THE ADMINISTRATORS
- RELEVANT REPORTING

CHALLENGES WITH EXISTING AWARENESS PRODUCTS

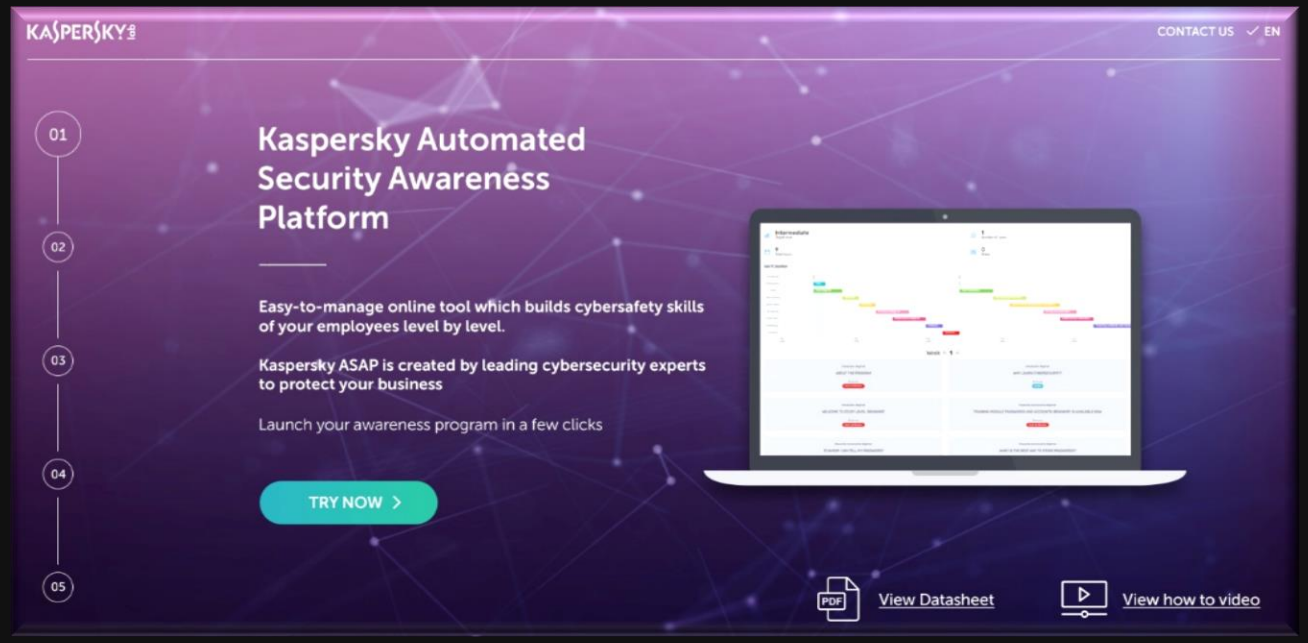
No clue how to set goals and plan education

Training takes too much time to manage

Reporting does not help in goal tracking

Employees don’t appreciate program → don’t get skills

Cornerstone of Kaspersky Lab offering: Automated Security Awareness Platform (ASAP)



- **Pre-determined efficiency**

  Quick win every day + interval training + constant reinforcement + measurement in #skills

- **Close to zero time spend for manager**

  Automated learning path requires few minutes to set up and manage. SMB and VSB as the biggest ASAP markets. MSP helps expansion.

- **Freemium**

  Free training for up to 5 employees or a family

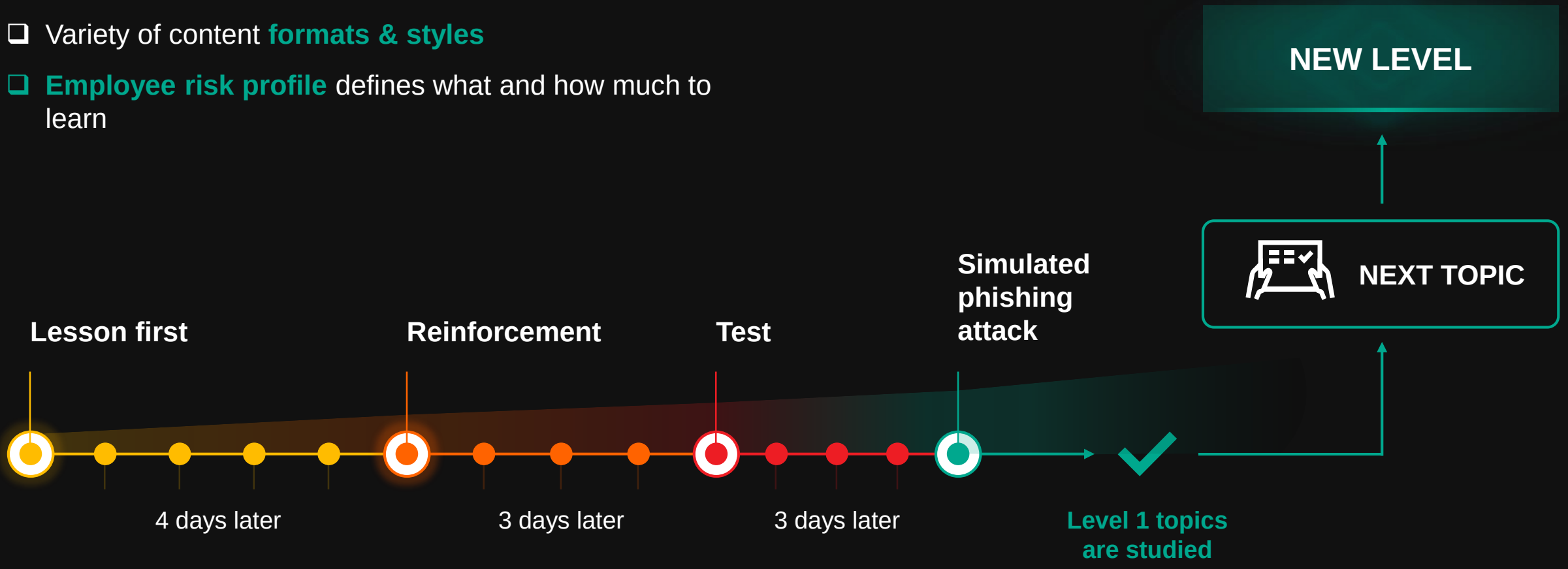
Register for free trial:

www.k-asap.com

KASPERSKY lab

LEARNING MANAGEMENT

- **Interval learning** at own pace to ensure content retention
- Variety of content **formats & styles**
- **Employee risk profile** defines what and how much to learn

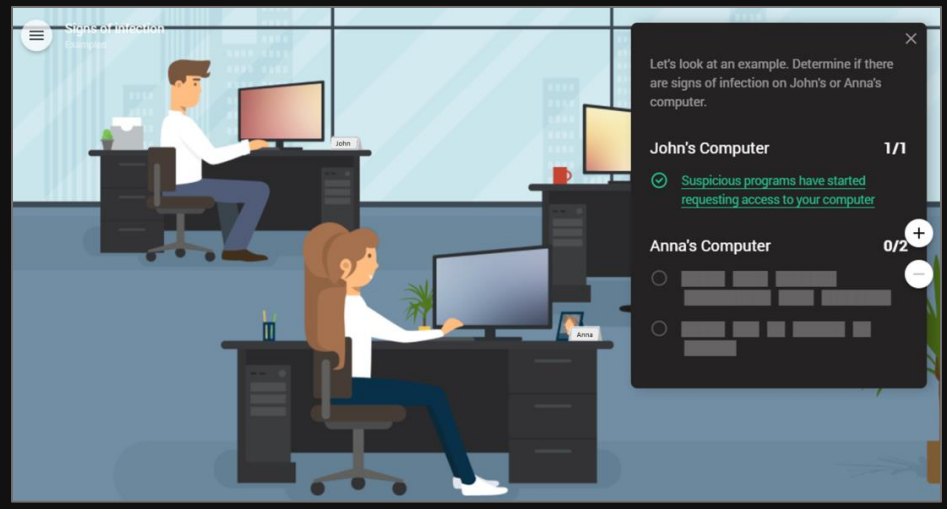


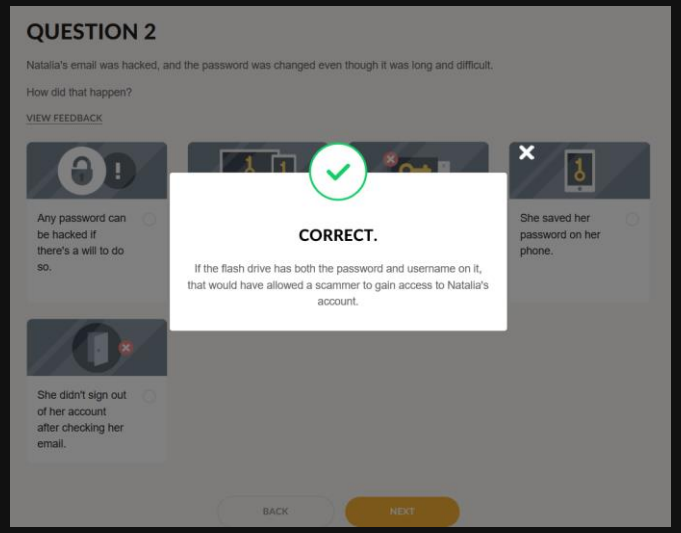
SETTING OBJECTIVES & CHOOSING A PROGRAM

- Recommended **learning paths** form basic to advanced
- Learning **targets based on risk levels, benchmarked** against world/industry data
- Easy **ongoing assessment** to align and focus
- **Time efficient** – learn only what you need
- **Tangible** and measurable training **results**

PROGRAM EFFICIENCY AND APPRECIATION

- **Comprehensive coverage** – Competency Model of 350 skills to be acquired for complete SC of any employee
- **Relevant** to participants' everyday life
- **Incremental interval learning**– to ensure the content retention. One lesson = one skill, a win a day





KEY PROGRAM DIFFERENTIATORS

Setting objectives & choosing a program

- Setting goals based on global data
- Benchmarking against world/ industry averages

Learning management

- Learning automation
- Self-adjusting learning path
- Calculation of time spent

Reporting & analytics

- Actionable reports anytime
- On-the-fly analysis of potential for improvement

Program efficiency & appreciation

- Practical exercises based on real-life scenarios
- Competition & challenge
- Overload prevention
- Subsequent skills application

An Approach that Delivers Proven Results

up to

90%

Reduction in the total number of incidents

not less than

50%

Reduction in the financial impact of incidents

up to

93%

Probability that knowledge will be applied in everyday work

more than

30x

ROI from investment in security awareness

an amazing

86%

Of participants willing to recommend the experience

Forrester's "Now Tech: Security Awareness and Training Solutions, Q1 2019"

FOR SECURITY & RISK PROFESSIONALS

Now Tech: Security Awareness And Training Solutions, Q1 2019

Forrester's Overview Of 20 Security Awareness And Training Solution Providers

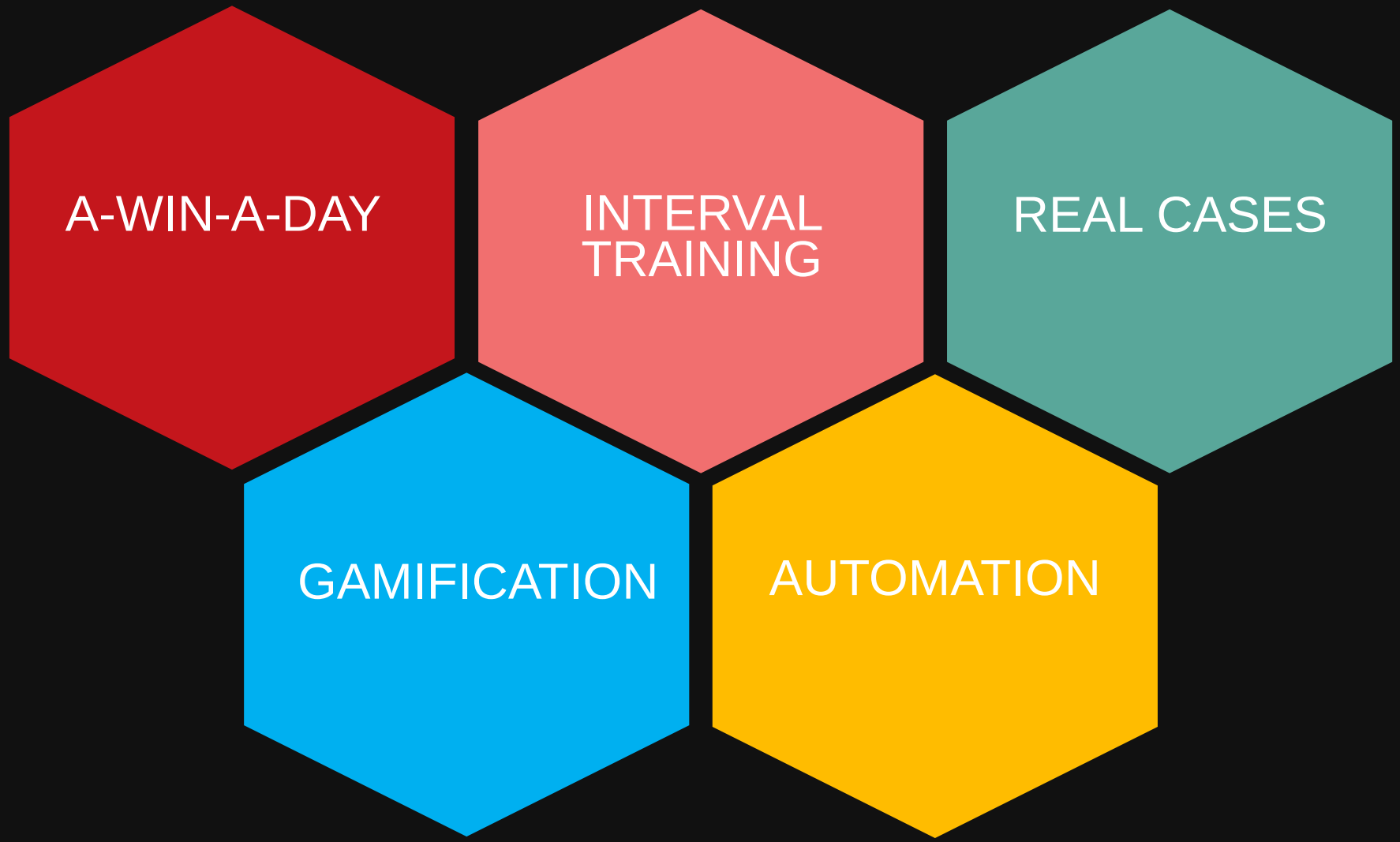
January 23, 2019

By Jinan Budge, **Claire O'Malley** with Stephanie Balaouras , Seles Sebastin , Peggy Dostie

Kaspersky Lab	Niche	NA 3%; LATAM 10%; EMEA 75% (Europe — 55%, Middle East, Turkey & Africa — 17%, Russia & CIS — 3%); AP 12%	Financial services; critical infrastructure/ energy; manufacturing	Donau Chemie Group, Austria

"Niche vendors are gamifying cybersecurity learning. These solutions take a **learning-by-doing approach**. Many have in-person workshops that can educate the entire workforce or are catered for just executives or developers. They also offer cyberattack simulations that allow employees to learn by acting as the hacker, or other micro learning gamification techniques that **are more advanced than the suite solutions."**

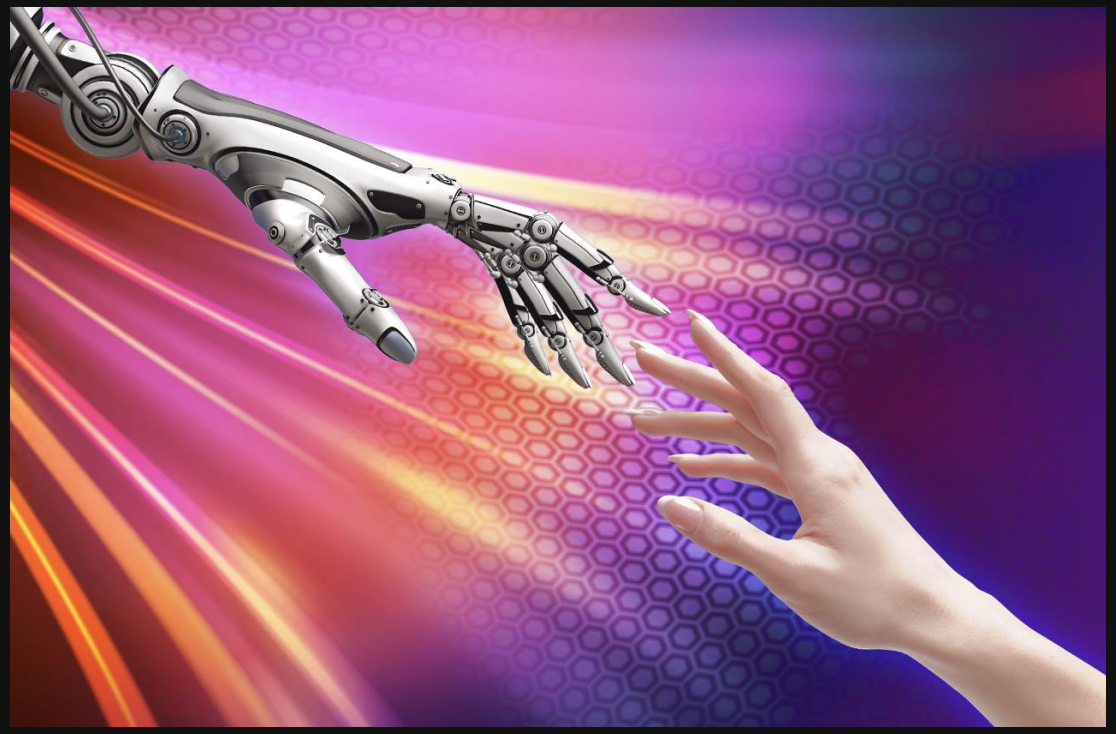
THE LEARNING FUNDAMENTALS



REMEMBER THE BIG PICTURE…

Digital Capability- key challenge of our age

- Security Awareness is a primary building block of Digital Capability
- It is a foundational security layer, designed to bridge ‘real’ and virtual worlds
- Spread of digital literacy is the starting point
- Everyone on the planet needs to do this




WE PROTECT WHAT MATTERS MOST
KASPERSKY lab
www.kaspersky.com/awareness