

Viruses, games and adaptive learning

The online training that
changes users' behavior

Eric Payne
Presales manager
Kaspersky NA

kaspersky

Who we are



Essentials

Founded in **1997** and led by Eugene Kaspersky

Operations in almost **200** countries and territories worldwide

Provides **innovative** IT security solutions and services for business and consumers

>**440,000,000**

>**250,000**

> **30000**



Numbers

> **20 million** product activations per year

> More than **4,200 professionals** and IT security specialists in **34** representative offices across **31** countries

users worldwide are protected by our technologies

companies use Kaspersky products

threats neutralized threats every 24 hours



Recognition

In 2019, the company's products featured in **86** independent tests and reviews.

Kaspersky products were awarded **64** first places and achieved **70** top-three finishes*

Customers

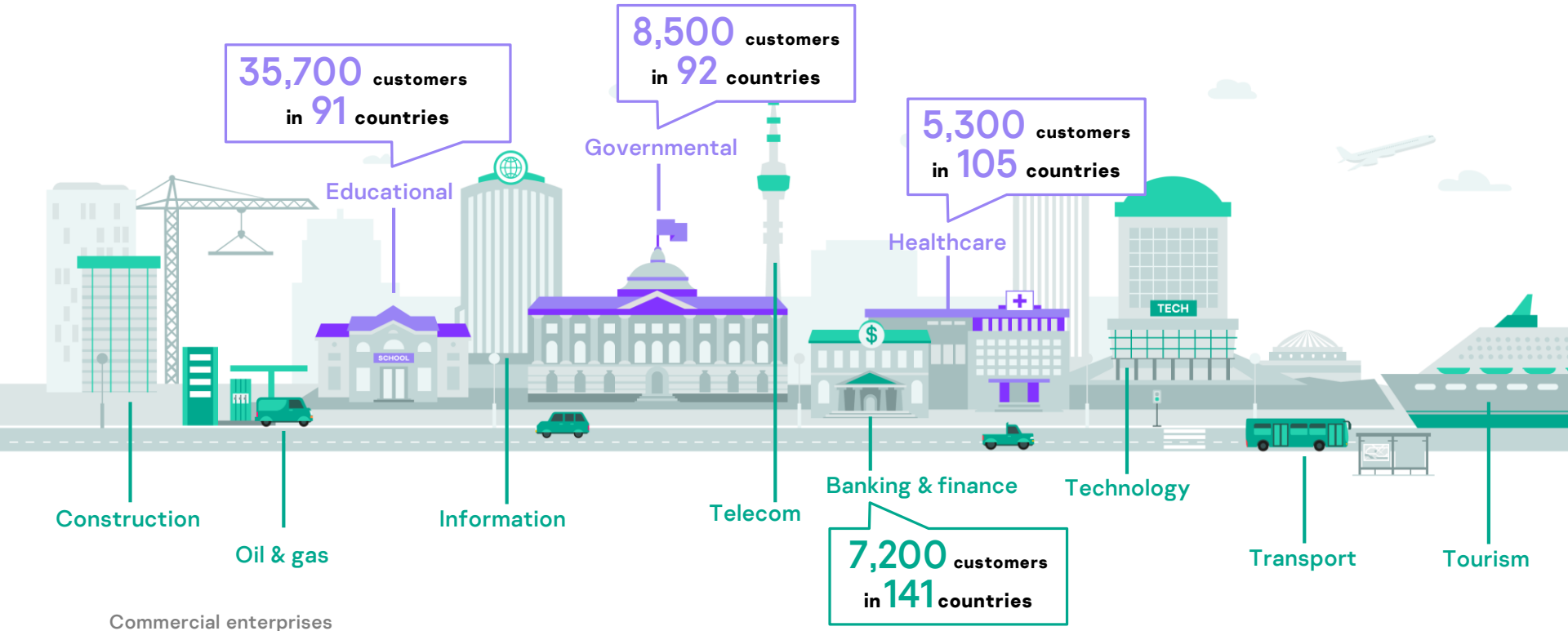
● Public
organizations

● Private
companies

We work in a wide range of industry sectors.

Our solutions and services successfully protect around **270,000** businesses around the world, regardless of size or complexity

3



Kaspersky's expertise in cybersecurity

- 20+ years in cybersecurity
- 1400 professionals in RnD
- 40+ experts in our Global Research & Analysis Team



Expertise in education

- 10 years of working in security education field
- Involved specialists in group facilitation, educational design and pedagogy / andragogy
- Partnership with one of leaders in adaptive learning - Area9 Lyceum



Kaspersky Security Awareness was recognized as a 'Contender' in "The Forrester Wave™: Security Awareness And Training Solutions, Q1 2020. The 12 Providers That Matter Most And How They Stack Up"

Kaspersky is rated 5.0/5.0 in the Security Awareness Computer-Based Training market on Gartner Peer Insights, based on 29 ratings as of 9 Sept, 2020 in the last 12 months

Get a complimentary copy of the report here:
<https://go.kaspersky.com/SA-forresterwave.html>

"KCAT - Significantly Enhances Cybersecurity Within The Company"

Customer review by
Firm size: 250M – 500M USD

Industry: Finance
Role: Security and Risk Management
Submitted: July 15, 2020

**Why security
awareness
is important?**



Computers has been intervened
to every sphere of human life



91%

of organizations are currently
involved in some sort of digital
initiative

70%

of companies either have a digital
transformation strategy in place
or are working on one

Cybercrime as a major threat

8



\$3.5 billion

Total losses from officially
reported cybercrime in
2019*



\$500K and more

Cost companies **53%**
of cyberattacks**

* [FBI "2019 Internet Crime Report."](#)

** Cisco 2018 Security Capability Benchmark Study

Paradox of cybersecurity:
everybody
understand its
importance and only
few do something.

Like wearing a seat belt....

**Somehow, way too many Americans
still aren't wearing seat belts**



People are the weakest link in corporate cybersecurity

10

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...

11

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"

How do you get your employees to learn something which isn't naturally interesting to them?

How do you transform knowledge into action?



What are the results we would like to achieve?

13

We want user to be:

Careful and aware of potential
threats

Proactive

Interested in further learning
and willing to constantly
improve their skills

We want user to transfer
behavior and get new safe
habits

Challenges enterprises face in employees' Learning & Development (all topics)

14

70%

of what is learned is forgotten within one day
in a traditional form of training

90%

is forgotten within 2 weeks

only 8%

of leadership sees the business impact of learning

Significant time

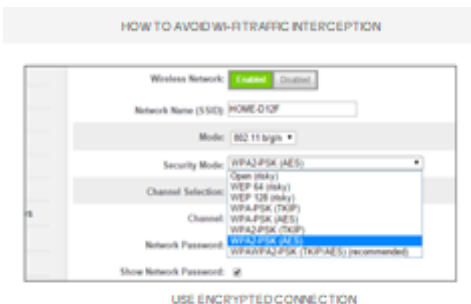
are spent by employees and training managers in
order to get optimal results

1. Got what to teach

Protecting your home wi-fi network

- Use networks encrypted by WPA2 standard
- Set a strong, at least 12-character password on your router
- Use 2-factor authentication for important resources

2. Prepare the course



missmarple → m6Ssm@Rp18\$)

3. Reported!

- 570 of employees passed the course
- Average test results – 70%

...and eventually it all comes down to...

In real life:

- Information is often lost
- Information tends to be forgotten
- Knowing something does not mean that people behaving accordingly



-
- A stylized illustration of a person with dark hair, wearing a teal sweater and black pants, jumping joyfully on a light blue office chair. They are positioned behind a white desk. On the desk, there is a computer monitor displaying a green hexagon, a small potted plant, and a mouse. Floating around the person are various icons: a musical note, a document with a green bar, a folder with a refresh arrow, a picture icon, and a line graph. The background is a soft, light blue circular glow.

What is the reality?

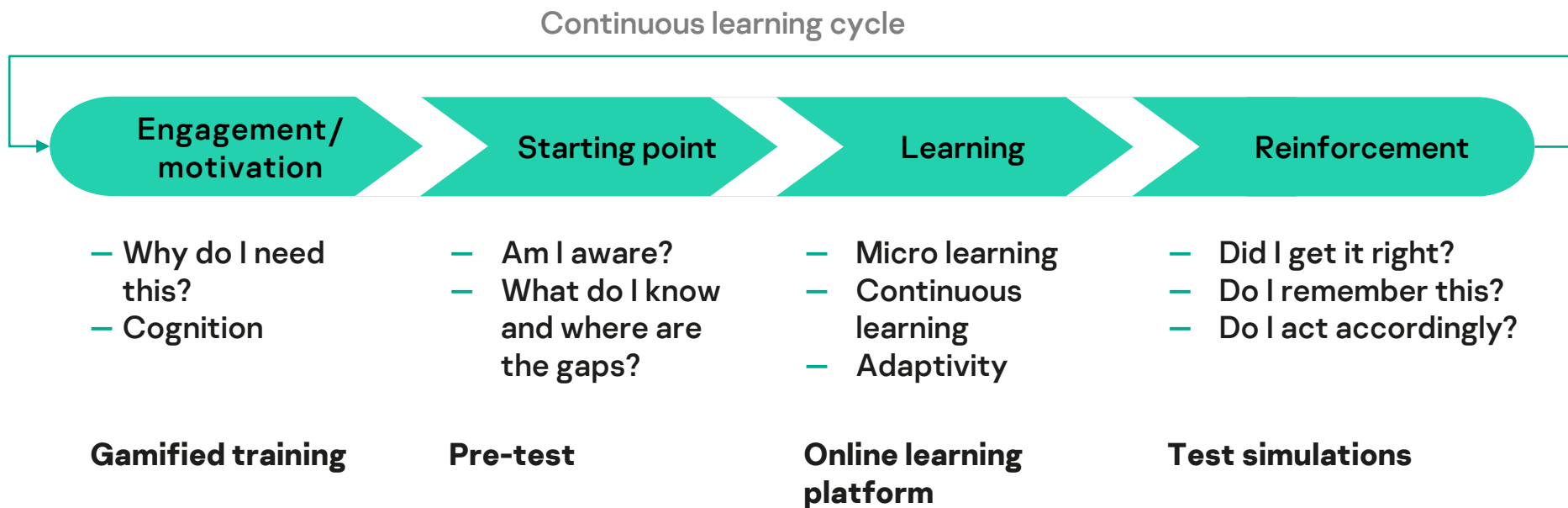
18

Changing behavior involves many small habits that need to be changed progressively, step by step, over time

Behavior change involves pushing people forward, steadily and persistently... often through boring unpleasant procedures



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



Motivation



Work with users misconceptions in cybersecurity perceptions

21

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

No need to outrun the bear....

26



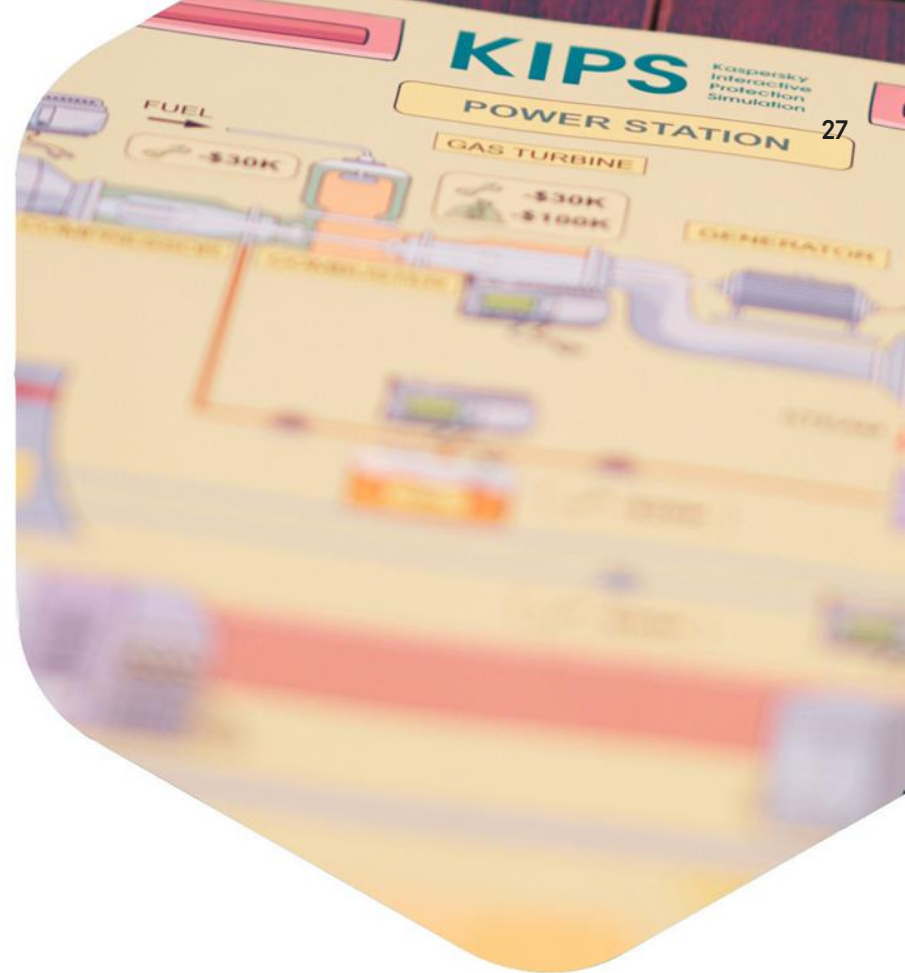
Engagement: Kaspersky Interactive Protection Simulation (KIPS)

A strategic team simulation game that demonstrates the connection between business efficiency and cybersecurity

Increase awareness among decision makers

Improve cooperation between different departments.

Teaches to interact more effectively in critical situations



**Define the
starting point**



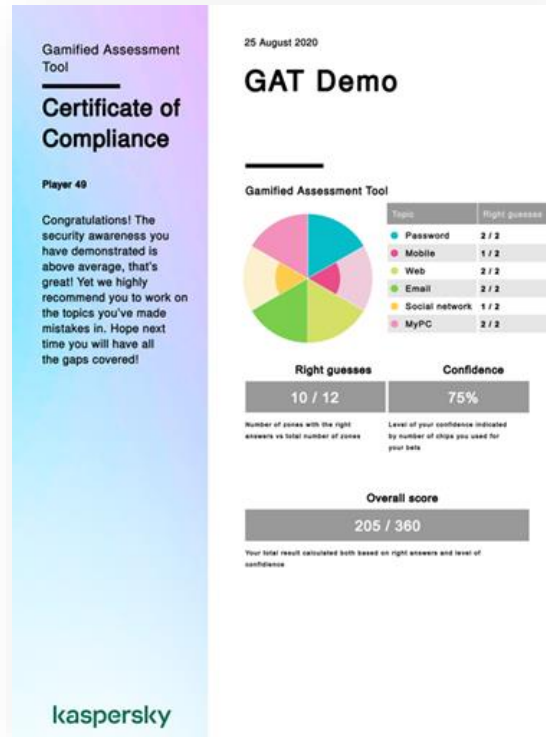
Gamified Assessment

- Online single play
- 3 maps involving different cybersecurity skills: Working in open space, travelling, and the home office
- The user has to decide whether each situation is risky or not
- Bets for demonstrate the level of confidence in the answer
- Clear feedback and recommendations for improvement



Gamified Assessment

30



- Changes the way cybersecurity is perceived in everyday workflows
- Increases motivation to study further

Learning



It's cybersecurity experts who can tell safe from risky

32

Cybersecurity experts know what cybersafe user behavior looks like

We just add learning techniques to make our customers' employees immune from attacks



Cybersecurity Skillset

Methods

Formats

Level of
difficulty

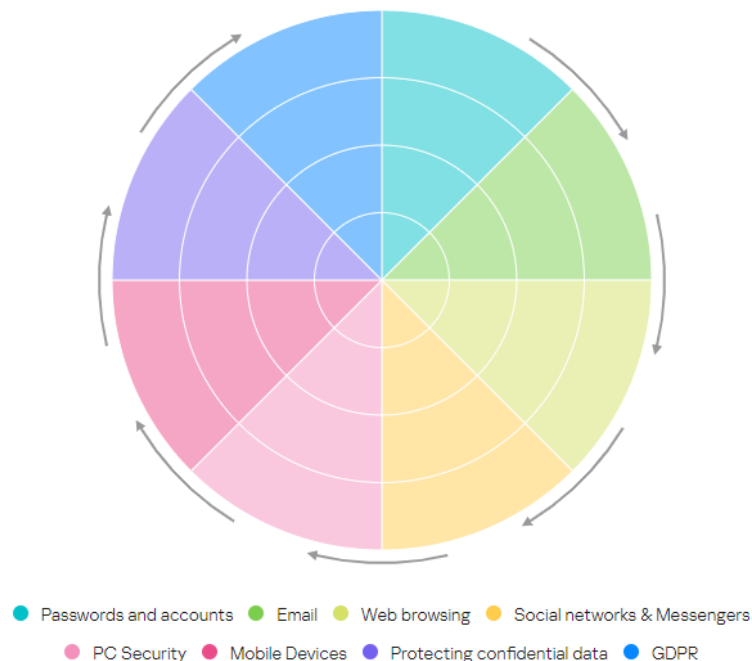
Delivery

Licensing
model

Client admin's
engagement

200+ specific skills

Universal multi-level curriculum



1 lesson = 1 (or more) new skills

- Why don't we worry about the security of our passwords and what kinds of mistakes do we make?
 - Can you tell your passwords to others?
 - How do I safely store passwords?
 - What do I do if someone found out my password?
 - Why do I need strong passwords and how do I make one?
 - Why can't I use the same password for my work and personal accounts?
-
- Why are people afraid to forget their passwords?
 - How do I create a strong password that is easy to remember?
 - How often do I need to change the password?
 - Can I use one password for all my Internet resources?
-
- Is it possible to get authorized without a password?
 - Can I store passwords in a browser?
 - Is it okay to store passwords in a password manager?
 - What is two-factor authentication and where should I use it?

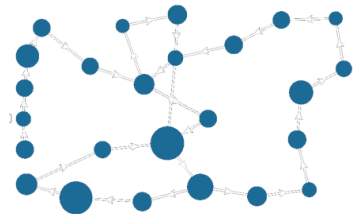
Main principles of online awareness program

Carefully balanced learning path based on full automation or adaptive learning algorithms

Micro-lessons, reinforcements, constant assessments and simulated phishing attacks to ensure knowledge retention and build new safe habits

Interactivity, test & examples based on the situations that employees face in their daily work



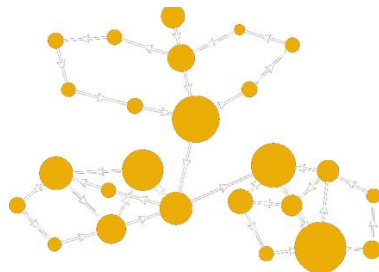


Learner 1

100% proficient at

8m 25s

Takes an almost linear path through the course as most of the answers were correct and he/she was confident about them.

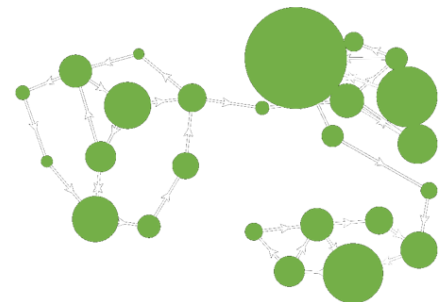


Learner 2

100% proficient at

19m 39s

Requires much more support and explanations as 52% of the initial answers were correct.



Learner 3

100% proficient at

33m 40s

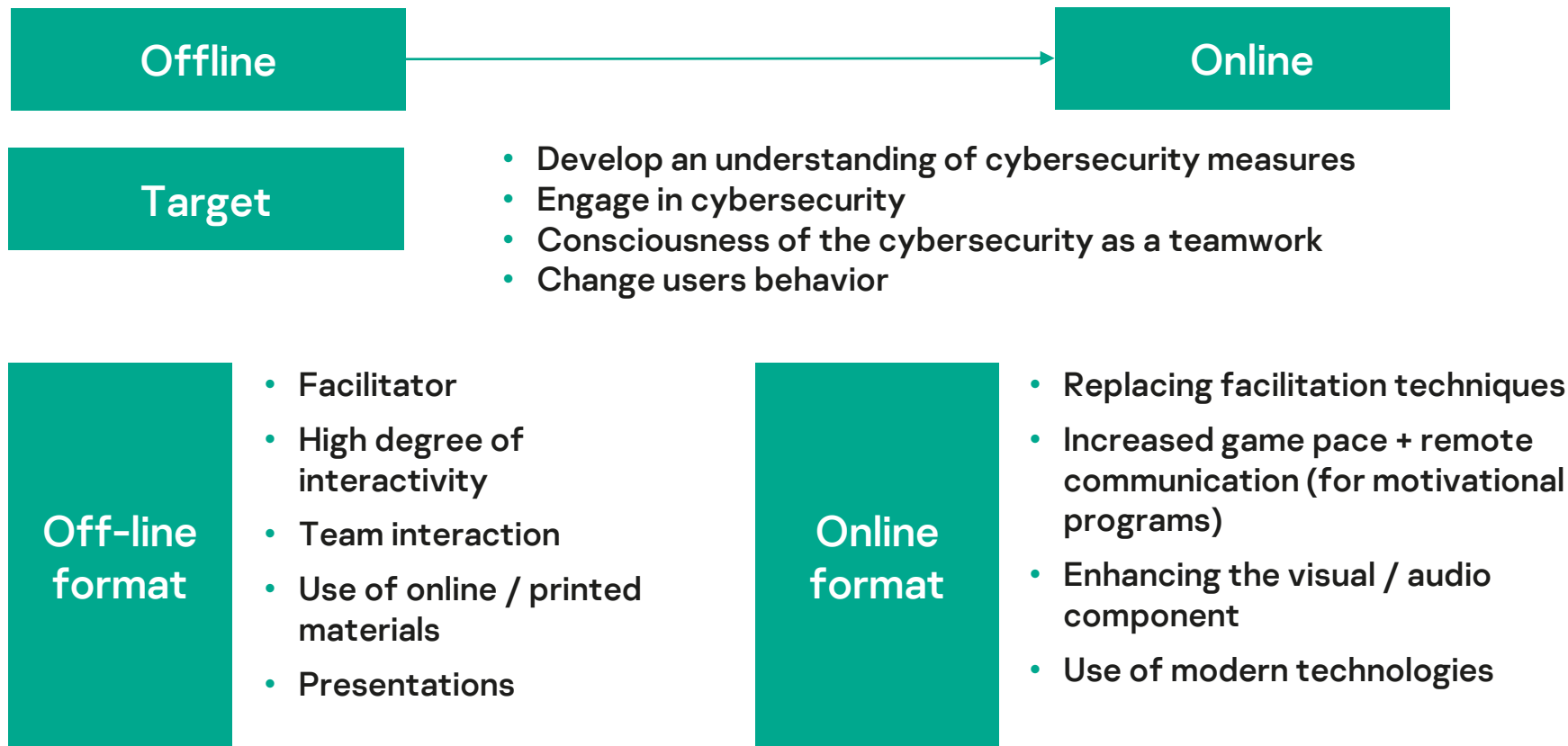
47% correct. Has as much to learn as Learner 2, especially struggled with one learning objective.

Whatever learning path the Platform builds, the result is always the same:

100% proficiency

Challenges of online training







Use of modern technologies

For engagement:

- Singleplay games
- The transition to virtual reality
- Visual novel: a story-rich game with cybersafety decisions driving the game forward

For learning and reinforcement:

- Adaptive learning algorithms

Learning points

1. Changing behavior can't be done just by waving a magic wand – it's a long, gradual, sometimes 'painful' for the user process.
2. One learning platform is rarely the answer to all the questions - only a range of products can change behavior (1 product per 1 stage of the learning cycle).
3. Starting paradigm change and motivation works better in gamified formats.
4. The effectiveness of online learning is increased by its "mass" individualization through the use of latest techniques and technologies.



Stay aware.

Kaspersky Security Awareness

www.kaspersky.com/awareness

www.kaspersky.com/kaot

kaspersky