Human Factor in Corporate Cybersecurity

Kaspersky
Security
Awareness

kaspersky

BRING ON
THE FUTURE

Learn more on
kaspersky.com/awareness

Accounting for the Human Factor is Central to Corporate Cybersecurity

Now that organizations have installed advanced phishing filters and firewalls, and deploy specialized tools to mitigate cyberthreats, cybercriminals have shifted their focus to employees as their initial point of entry into IT systems. Exploiting common gaps in user knowledge is the easiest way to penetrate corporate IT infrastructure.

According to the Kaspersky and B2B International survey, **52% of businesses** admit that employees are their biggest IT security weakness, with careless actions or lack of knowledge compromising corporate IT security strategy.

According to Wombat's 2018 User Risk Report, **55% of working adults** allow friends and family members to access their employer-issued devices at home, and **66% of respondents** who don't use a password manager tool admit to reusing 60% of their passwords across online accounts.

60% of employees have confidential data on their corporate device (financial data, email database, etc.) and **30% of employees** admit that they share their work PC's login and password details with colleagues.[1]

According to the 2018 Verizon Data Breach Report, **4% of people** still believe that clicking on a suspicious attachment is not a big deal.

No organization is too small, or too large, to avoid becoming the goal of cybercriminals:

- In 2018, **43%** of cyberattacks targeted small businesses.[3]
- In 2017, the Equifax data breach that exposed the personal information of more than **146 million** people resulted from human error, when employees failed to follow security warnings and code reviews while implementing software fixes.

The average financial impact of inappropriate actions by careless/uninformed employees[4]

For SMBs

- The average annual financial impact of data breaches caused by inappropriate IT resource usage by employees – **$98K**
- Physical loss of company owned devices or media - **$105K**

For Enterprises

- The average annual financial impact of data breaches caused by inappropriate IT resource usage by employees - **$1,057K**
- Physical loss of company-owned devices or media - **$1,416K**

Human Error – the Main Source of Cyber-incidents

Employees have become a primary target for cybercrime – exploiting human weaknesses like inattention, ignorance or negligence is so much easier and cheaper than trying to fool sophisticated protection software.

Last year, **67% of credentials** thefts succeeded thanks to careless employees falling for phishing scams[2]. Errors or casual events are currently responsible for **21% of all security breaches**.[3]

Nearly half of all **C-Suites (47%)** and one in three **small business owners (31%**) record human error or accidental loss by an employee/insider had as being the cause of a data breach, according to a Shred-it survey conducted by Ipsos.

The UK's Information Commissioner's Office (ICO) reports that **88% of data breaches** in the UK over the past two years were caused by human error, rather than by hacker attacks.

Taking into account all these statistics, many organizations naturally put issues relating to the strengthening and improvement of cybersecurity awareness as among their top priorities, as they work towards building a safer corporate environment.

"Increase staff training to prevent careless behavior" is among the top **3 governance priorities** during 2019 for **53% of survey respondents**, says the Ponemon Institute's report "Measuring & Managing the Cyber Risks to Business Operations".

Effective Security Awareness

Training is essential in raising awareness among employees - motivating them to pay attention to cyberthreats and countermeasures even if this is not initially perceived by them as part of their job responsibilities.

Unfortunately, however, many security awareness training programs are less than effective. What's going wrong?

Security Awareness training is often perceived as a difficult, boring, irrelevant drudge. Employees tend to:

- consider such training too complicated and technical to be worth devoting time to,
- fail to see the connection between their actions and possible consequences,
- reason that it's the work of IT specialists to take care of corporate cybersecurity – not theirs.

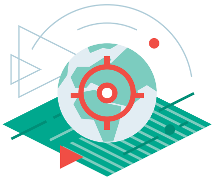
Whatever the reason for employee indifference to the training on offer, the end result's the same – they continue to act as just before.

It's also a fact that training programs are often too short, so that the knowledge acquired just doesn't have time to sink in and get retained, or too long and tedious to complete, being full of peripheral or irrelevant information.

Training can also prove ineffective if employees feel so overwhelmed with instructions about what they should and shouldn't do, that they can't digest it all and turn defeatist – cybersecurity issues becoming perceived as a series of continuous restrictions and hindrances to getting on with the job.

[1] "Sorting out a Digital Clutter", Kaspersky, 2019.
[2] "Measuring & Managing the Cyber Risks to Business Operations", Ponemon Institute LLC, Dec 2018
[3] "2019 Data Breach Investigations Report" Verizon
[4] "On the Money: Growing IT Security Budgets to Protect Digital Transformation Initiatives", Kaspersky, 2018

An effective security awareness training program needs to incorporate 4 key elements:

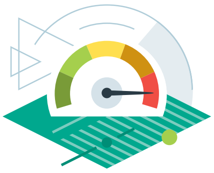


Role-based, targeted training

- Learn what you need to know, based on your role and risk profile
- Real-life examples and skills that can be put to immediate use
- Learning by doing

Human-centric

- Training that's structured in line with the way people naturally think
- Putting a positive, proactive spin on safe behavior
- Information and skills that are easy to digest and retain, thanks to methodologies based on the specifics of human memory



Continuous incremental learning

- From the simple to the more complex
- Expanding and applying previously acquired knowledge in new contexts

Easy to manage and control

- Online
- Automated learning management
- Invitations and motivational emails sent automatically with individual recommendations for every student

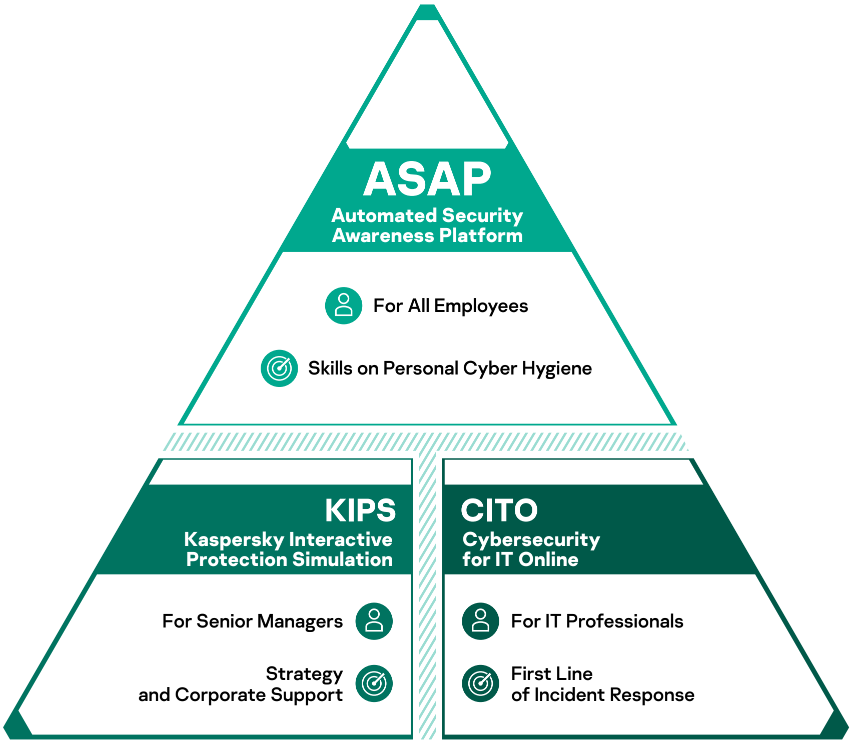
Understanding what lies behind any learning and teaching process helps build an effective educational program. Our programs not only deliver knowledge, but – more importantly – change habits and form the new behavior patterns that are the real goal of awareness training.

At Kaspersky, we offer computer-based training products that combine expertise in cybersecurity with best-practice educational techniques and technologies. This approach changes users' behavior and helps create a cybersafe environment throughout the organization.

Kaspersky Security Awareness worldwide

- **75** countries
- **580** organizations
- **550,000** people trained so far

Kaspersky Security Awareness Training



ASAP
Automated Security Awareness Platform
For All Employees
Skills on Personal Cyber Hygiene
KIPS
Kaspersky Interactive Protection Simulation
For Senior Managers
Strategy and Corporate Support
CITO
Cybersecurity for IT Online
For IT Professionals
First Line of Incident Response

Enterprise Cybersecurity: www.kaspersky.com/enterprise
Kaspersky Security Awareness: www.kaspersky.com/awareness
ASAP free trial: k-asap.com

www.kaspersky.com

kaspersky