Show don’t tell

How automated cybersecurity training helps employees perform without limits

Kaspersky
Automated Security
Awareness Platform

kaspersky BRING ON THE FUTURE

Start your free trial today:
k-asap.com

Introduction

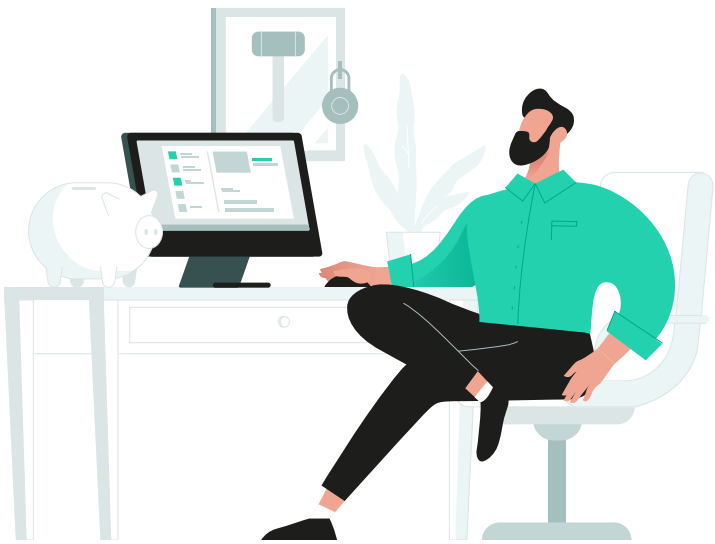
90%[1]
of all **cyber-incidents** can be attributed to human error

If, like so many companies, you have suffered from an internal cybersecurity incident, you may already be aware of cybersecurity's weakest link: the well-meaning, but untrained employee. As phishing filters and firewalls have become more sophisticated, so the focus of cybercriminals has turned to your personnel as a potential entry point into IT systems. As a result, over 90%[1] of all cyber-incidents can be attributed to human error.

Issues such as confidential data loss, downtime and hardware failure have serious financial consequences. The average cost of a data breach for SMBs caused by inappropriate IT use internally is $116K[2], while the average global cost of one security breach is $3.92M[3]. It is estimated that in the first half of 2019, nearly 4,000 data breaches put more than four billion users' data at risk[4].

This clearly points to a **lack of awareness around cybersecurity best practice amongst employees,** and potentially a lack of appropriate learning technology to ensure that training is delivered effectively.

This document examines the benefits of training as a means to ensure employees can use an organization's technology confidently. Specifically, training which is continuous, interactive and engaging – which *shows* rather than tells – to ensure employees have the freedom to perform.



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

2 Kaspersky report – IT security economics in 2019

3 IBM – Cost of a Data Breach report, 2019

4 Kaspersky report – IT security economics in 2019

A desktop, remote and mobile challenge

The evolving complexity of our IT landscape means that cyberattacks are increasing in scale and severity. New security technologies help to reduce exposure to malicious threats, but our behaviors both as consumers of technology and employees in the workforce now have the most impact on the security of the organization.

We are all more connected, more mobile, carrying more personal devices, and using more free and popular services in our daily lives. Mobile devices now form an integral part of the business processes of 75% of companies, yet only 17% of employers prefer to supply their entire staff with corporate phones[1]. The others allow the use of personal devices at work to some extent, which carries greater risk.

The continued rise in remote working also changes the dynamic. While companies may be able to thoroughly protect networks and devices in the workplace, **the same corporate standards cannot be provided at home.** In recent research on working from home[2], 47% of people researched said they spent more time watching videos, with around one-in-two (48%) doing so on devices they use for work. More unexpectedly, half (51%) of workers who watch adult content admit to watching it on work devices, with the associated threat of malware from those sites. It doesn't help that 73% of workers have not received any IT security awareness training from their employer since they transitioned to working from home.

Cybercriminals are shifting focus to target remote workers with new cyberthreats and new forms of manipulation, so strengthening awareness around basic secure behavior has never been more important. Training must also evolve to be more memorable and effective, ensuring that employees can spot different threats, from easy mass attacks to more sophisticated attacks.

"Cybercriminals are shifting focus to target remote workers with new cyberthreats and new forms of manipulation"

1 Study by Oxford Economics for Samsung, 2018

2 Kaspersky – "How Covid-19 changed the way people work", 2020

Why so much training is currently forgotten

Cybersecurity incidents can be significantly reduced through effective computer-based interactive training

To make a radical shift in how employees become more cybersecurity aware, training must be more engaging in order to ingrain new knowledge. Learning which is heavily paper-based or reliant on watching videos is not an effective way to nurture learning, since **many employees will find the medium boring, and the content forgettable.**

To be memorable, training must combat the Ebbinghaus 'forgetting curve' where memory retention declines over time. Learning methodologies must be based on human memory and behavioral psychology and recognize the huge importance of empathy in education and training. Here are two examples where traditional learning fails in that respect. Firstly, teaching content that is not related to the real-life situations which people face at work. Secondly, rigid coursework which lacks visual appeal and interaction for participants, and therefore lowers participation rates and does not significantly change cybersecurity behavior.

Training courses which fail to engage employees are as quickly forgotten as the skills they were supposed to teach. For example, in one business, the average click rate on phishing emails was around 40% amongst staff. Immediately after training that percentage dropped, only to rise back to 40% in a few months[1].

By contrast, repeated reinforcement with online interactive training such as Kaspersky Automated Security Awareness Platform (ASAP) includes knowledge tests and high levels of interaction – making learning memorable, and helping to build strong, long-lasting cybersecurity skills. It is effective because it provides knowledge as well as cultivating better patterns and habits of cybersafe behavior.

1 Kaspersky – "IT security economics in 2019", respondent feedback

Show don't tell: the role of interaction and cybersecurity scenarios

"We had struggled to deliver training that really worked in a classroom scenario. We've seen much greater success by automating training with Kaspersky, and after 6 months of use we're reporting far fewer cyber-incidents"

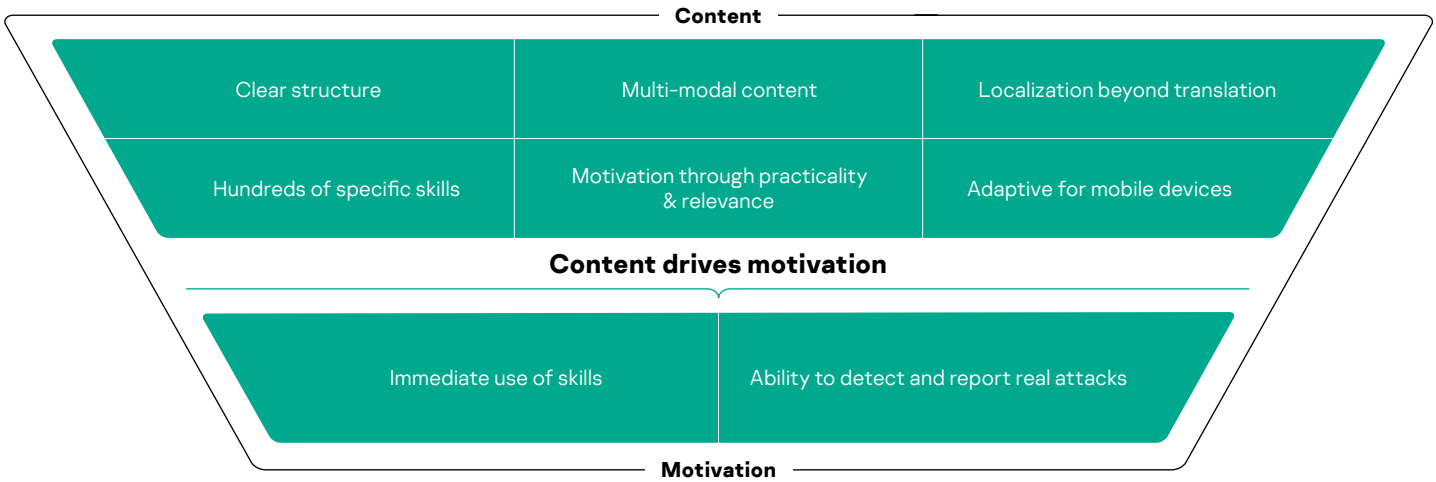
HR Director in Manufacturing

Instead of cybersecurity theory, reading or listening, training can be made more exciting and engaging through multi-modal content, where different training elements complement each other to develop a skill – for example, interactive lessons, tests, reinforcement and simulated attacks.

Realistic cybersecurity scenarios and simulated attacks are an important element in a 'show don't tell' approach. They help employees to think on their feet and take actions based on their understanding. **This reinforces cybersecurity behavior when decisions have to be made during an actual attack.**

When multi-modal content is supported by a clear program structure, training will be easy to understand, logical and balanced. An element of challenge should be present during the program to provide motivation and the training should never be 'one track'. Continuous and incremental learning – with reminders of past topics and reinforcement of habits – is the most effective way to ensure employees are engaged and information is retained.

It also helps that the training content is created by an organization focused on cybersecurity with a specialist skillset in security, rather than training per se. In the case of Kaspersky, the company has over 20 years of experience in cybersecurity, and so knows which skills employees should develop in order to behave safely and safeguard the company; these skills are built directly into training content, divided by topics and levels.



Simplicity delivered through automation

As discussed, to reinforce new patterns of behavior, security awareness training should be continuous, with **regular refresher sessions to emphasize what was learnt in previous lessons.** Manually assigning all of this material would be a challenge for many administrators – particularly in smaller businesses with limited resources – whereas automation does this effortlessly to save time.

Automation can also remove program complexity and allow training to be fine-tuned, managed, and delivered to a wide range of employees with different levels of cybersecurity learning requirements. Training is divided into smaller step-by-step lessons that allow easier tracking of progress towards specified training goals. This overcomes the limitations of traditional classroom training, which cannot reach large numbers, and often provides little evidence that requirements have been met.

While online interactive training cuts administration time, it does not sacrifice training depth. With Kaspersky ASAP over 300 practical skills can be taught, with automatic training plans for every group of employees.

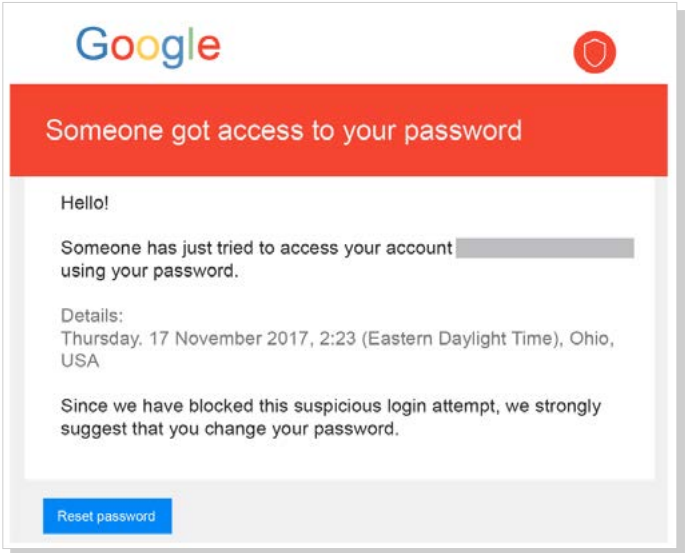
Showing the way: one cyberthreat training example

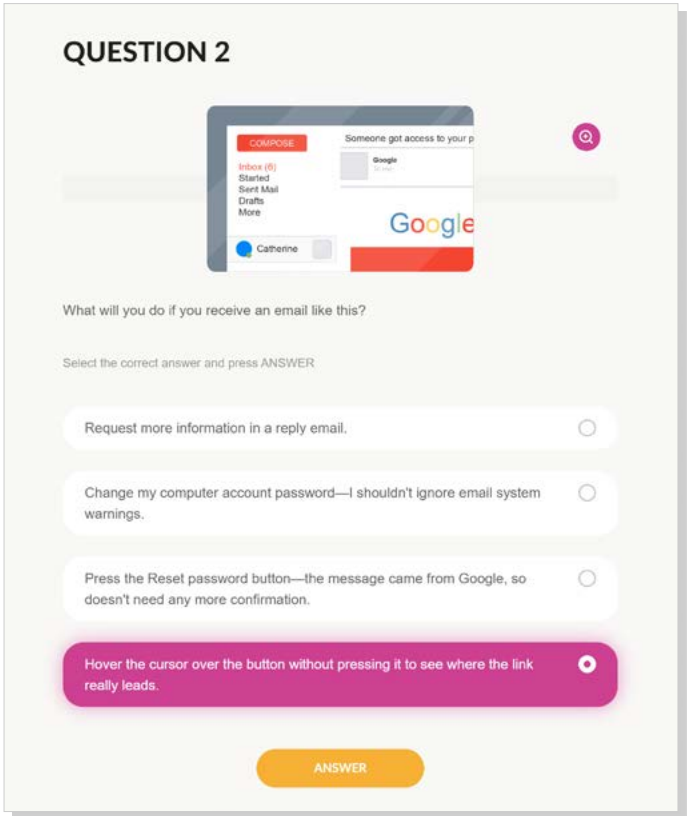
Simulated phishing attack

So many people believe that a phishing attack could not happen to them. So with Kaspersky ASAP, after interactive lessons, tests and learning reinforcement, a real-life scenario unfolds – and the employee is at the center of the process.

This training example challenges the employee to see if they're savvy enough to spot the signs of a faked email. What are the signs of danger? How do they check the sender's name and address for authenticity? What should they do if they suspect phishing?

The content is purposefully **short, interesting, challenging and memorable.** By solving the problem, the employee gains a sense of achievement – 'a win a day' – and the skills that have been learnt can be put to immediate use after just one lesson, to safeguard the company.





Conclusion

IT and security decision-makers are beginning to realize the importance of security training for their employees. Now they need to choose a provider and a training solution that delivers long term results. Training must use better learning principles, and interactive content which promotes security-minded behavior in real-life situations – ingraining new knowledge and beating the 'forgetting curve'.

The right training will have benefits beyond the financial, including improved employee morale and confidence, and a better work culture. **By using training to *show not tell*, employees can truly have the freedom to perform without limits.**

Kaspersky ASAP free trial: k-asap.com
IT Security News: business.kaspersky.com
Kaspersky Security Awareness: kaspersky.com/awareness