sosafe

How Gamification is Revolutionizing E-Learning

6 Tips for Your Security Awareness Training

Table of Contents

For a Strong Information Security Culture

Why companies should use gamification in awareness training

From corporations to medium-sized companies, healthcare facilities to administrative authorities, **no organization is safe from cyber attacks**. Numerous new malware variants are discovered every day; at the same time, the number and quality of cybercriminal extortion methods are increasing significantly with each passing year.

The damage is enormous and, according to the Cybercrime Magazine it will cost the world 10.5 trillion dollars by 2025. The "human factor" plays an increasingly important role here—after all, **9 out of 10 cyberattacks start with humans**. When spam filters and antivirus programs are tough to break through, cybercriminals look for new loopholes: They use increasingly sophisticated methods for their attacks and manipulate their victim's emotions with psychological tactics. They arouse curiosity, entice users with offers, or announce supposedly important news. Then all it takes is one careless click to cause immense damage to organizations. After all, a single link in an email or the playing of a fake video is enough for attackers to install malware and acquire sensitive data.

Challenge for organizations: Activating the "human firewall"

A good security culture therefore no longer relies solely on technical precautions. This increases the pressure on organizations and their cyber security managers.

Not only do they have to continuously educate themselves and keep their knowledge up to date, but above all they have to sensitize all their employees to the issue and turn them into a protective barrier, or a "human firewall". This is a major challenge that can be overcome with the right training concept.

Gamification as a central element in security awareness training

Current security awareness training courses no longer rely on long, on-site training sessions. Since the start of the COVID-19 pandemic at the latest, online training courses—such as e-learnings – have become increasingly important.

Some training courses also rely on **gamification, meaning the transfer of elements typically found in games to non-game contexts**. This works so well because the training courses appeal to people's natural play instincts, which remain with us even beyond childhood. Typical elements from computer games are integrated into the learning process, increasing the fun factor and motivating continuous learning. Complex facts are conveyed in a playful way and, above all, internalized. The success of this method has been proven: **The activation rate increases by more than 40 percent when gamification is used**. This means that significantly more employees complete the training, which has a positive effect on the overall safety culture in organizations.

6 Reasons Why Gamification in Security Awareness Training is so Successful

People who like to learn do so more often, more effectively, and more sustainably—this also applies to awareness training. The use of gamification elements creates real added value for companies in building the “human firewall”. The following six psychological mechanisms show why this is so:

01 People like to be rewarded.

The human brain works with a reward system that decisively influences our motivation. As soon as we perceive pleasant stimuli, the happiness hormone dopamine is released. This positive feeling drives us and ensures that we voluntarily repeat certain actions because we again expect a reward.

Gamification Tip

Learners are more motivated when they receive points and praise for a successfully completed lesson. Focus on awareness training that uses a point system and regular positive feedback.

02 People are curious and want to be entertained.

Curiosity and the urge to discover are important drivers that remain with us through our childhood development and into adulthood. Not only are they the stuff of any exciting story, but they drive people to seek out new experiences.

Gamification Tip

Choose trainings that uses storytelling. A continuous storyline and interesting characters ensure that learners are excited about the content and want to know what happens next.

03 People are social creatures and want to help others.

Altruism refers to selfless behavior that helps others—and is part of being human. We are social beings and have a strong need to help others. It's not entirely altruistic, because at the same time we feel better about ourselves and needed by others.

Gamification Tip

Gamification elements allow learners to show their willingness to help. Typically, they solve tasks and help the protagonists of a story to prevent a negative event (e.g., phishing scam). Combined with rewards and good storytelling, motivation is further enhanced.

04 People want to evolve.

There is a natural ambition in everyone that drives them. We strive to get ahead in life, to become better and to develop ourselves further. Once we have achieved an important goal, we feel pride and want to continue.

Gamification Tip

Even a simple progress bar can make a big impact: Visualizing one's own progress spurs us on to achieve 100 percent. When the bar is finally filled, learners receive points and advance to the next level. In this way, they go through a development process that makes them proud and motivates them to continue.

05 People seek recognition.

The desire for recognition is a basic human need. Not only children are happy to receive praise; adults also want to be recognized for their achievements. If we are proud of our successes, we want to celebrate them and share them with those around us.

Gamification Tip

In effective e-learning, learners receive badges that they can use to present their success to the outside world. This awakens in them the desire to collect as many such rewards as possible—and to compare themselves with others. Once the will to win is awakened, learners spur each other on.

06 People want to actively participate.

People like to feel they belong and are committed to a cause. Interactive learning methods make content tangible. This helps to deeply anchor learned material into our memory.

Gamification Tip

Small games or tasks add variety to e-learning and make learners feel included. Animations, quizzes, or drag-and-drop elements make training more interactive.

Fun, pride, team spirit, and sustainable behavior change in awareness training: Based on psychological mechanisms, gamification helps employees develop a positive learning experience. This makes them want to do more training—and ultimately significantly reduces cyber security risks.

EXCURSUS

How Human-Centered Design Increases Learning Success

Interview with Dr. Gundula Zerbes
Psychologist and Instructional Designer at SoSafe

The term human-centered design originates in the field of product and software development and is also frequently used in management concepts. The focus rests on the users as well as their needs and expectations. The goal is to make products, systems, and other offers as user-friendly as possible.

What role does human-centered design play in the conception of e-learning content?

E-learning is about adapting learning modules to the people who are going to consume them. So we always try to keep our focus on the learner. The content and information should be made available as simply and intuitively as possible so that the learners remember it for a long time.

What can organizations do to integrate the topic of cyber security into their culture while getting their workforce excited about it?

Organizations need to take a step toward their employees and provide them with the information in the most accessible format possible. E-learning needs to get down to the individual learner level and show that the topic is not only important, but also fun. Employees should know exactly how they can recognize phishing emails, for example, and how to behave in dicey situations.

What are the special features of security awareness training?

Many people perceive the topic of cyber security as dry, boring, and complex. Therefore, they have no intrinsic motivation to approach it or learn more about it. And in stressful, everyday work environments, there is usually little time for these topics.

What is the best and most sustainable way for employees to learn?

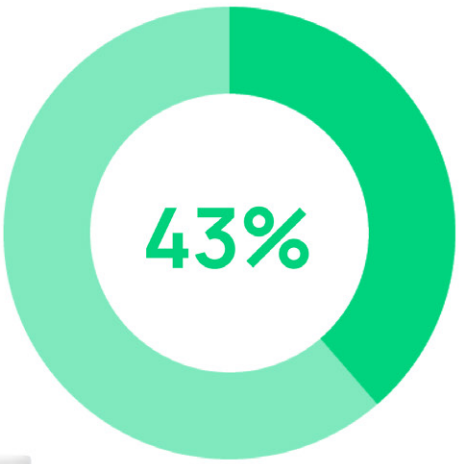
The most important thing is not to do everything at once. It's much more useful to break information into small "bites" and consume it over a longer period of time. Then it's more likely to be remembered in the long term. It is also important that learners always experience the content in the context in which they will use it. They learn much better in an everyday situation at work than in a theoretical seminar in a classroom. In addition, it's all about efficiency: Training measures should be easy to integrate into everyday life despite busy schedules.

Focus on People

This combination reveals gamification's full potential

People strive for rewards and recognition. They are curious, love entertainment, and want to develop themselves. And people are social beings who want to help others but also want to be involved. All these insights are deliberately used in modern security awareness training to put a stop to cybercriminals and strengthen the security culture in organizations.

Gamification elements put the focus on the person learning. Organizations benefit from this because the training starts exactly where the greatest potential lies: with the people themselves. When it comes to the complex topic of cyber security in particular, this can be a decisive factor. If employees feel "picked up" and enjoy learning, they will be happy to complete the training and will retain the content in their memory in the long term.



Gamification whets the appetite for security awareness training: The use of gamification elements increases the activation rate **by 43 percent**.

In addition to gamification, there are other factors that have a positive impact on the learning effect, such as:

Applicability

The content must be adapted to the prior knowledge and competencies of the learners. This prevents learners from struggling through the training in frustration.

Time efficiency

Short, concise micro-modules shorter than ten minutes conserve resources and can be easily integrated into the daily work routine.

Continuity

Distributed learning over a longer period of time promises sustainable learning success, for example in the form of regular attack simulations. If, on the other hand, employees are only trained selectively, the risks quickly increase again.

What all these factors have in common is that they are **based on findings from behavioral research and the psychology of learning**—and thus focus on the needs of the learners. Effective awareness training therefore relies on a holistic methodology that includes other user-centric elements in addition to gamification.

Only if organizations succeed in educating all employees can they ensure cyber security in the long term. **Using gamification in awareness training can make all the difference.**

ABOUT SOSAFE

sosafe

With its agile awareness platform, SoSafe empowers organizations to scale a security culture. Our dynamic upskilling programs fuse behavioral science, smart algorithms, and a human-centered approach to empower every employee to be part of their organization's human firewall. Beyond building secure habits among employees, you can understand exactly where vulnerabilities lie with contextual data, proactively respond, and measure the ROI of your awareness programs.

Employees receive smart attack simulations and personalized micro-learning experiences within their daily work environment. Curated content delivered with a level of gamification makes the trainings engaging, informative, and effective. Our self-learning systems react to personal risk scores, continuously delivering tailored trainings to each employee. This continuous process drives secure behavior at scale.

The SoSafe difference is how easy it is to deploy, manage, and scale our GDPR-compliant solution, saving you time and resources. Organizations can leverage our simple self-serve model or opt for done-for-you implementation and service from our team of experts.

SoSafe GmbH
Ehrenfeldguertel 76
50823 Cologne, Germany

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800