KnowBe4

Winning User Hearts and Minds With An Engaging Learner Experience

Your users have lots to do on any given day. Pressures on their time and attention come from everywhere, no matter the industry you're in.

As someone responsible for managing employee risk through security awareness training (SAT), the competition for user focus is stiff. An effective approach to training needs to be able to stand up to bustling inboxes, growing to-do lists and even the siren song of their personal mobile devices.

Vying for user hearts and minds against these attention grabbers means deploying training that's engaging and effective in changing behavior.

When it comes to SAT, how training is presented is just as important as what is taught. Your approach to learner experience can mean the difference between a lesson taken to heart and a phishing email clicked.

Read on to explore ways to provide a relevant, intentional learner experience that contributes to greater learner engagement and ultimately a strong security culture.

Learner Assessments

Assessments, also called quizzes, can provide a positive user experience in two ways. One, when given before a training module, they prime the learner to help prepare them for the topics they'll be engaging with. Even this little bit of "this sounds familiar" as the user works through the training can improve the experience and help engagement.

Two, assessments help the learner recall and reinforce lessons they've learned throughout the primary training content experience. This can help with a sense of accomplishment once completed. Everybody likes to feel they did well!

Frequent low-stakes questions integrated throughout the training better reinforce the material compared to an all-or-nothing final exam. Employees are more likely to stay engaged when faced with bite-sized comprehension checks rather than the looming pressure of a high-stakes test at the end.

Tailored Training

A one-size-fits-all training approach often provides too much or too little information for individual employees. Tailoring the content to their existing knowledge level and risk exposure results in a more personalized and relevant experience.

Use learner assessments to establish baselines of what employees already know and what threats they face in their particular roles. Use these assessments to customize learning paths and deliver training focused on the most pertinent gaps and risks for each user.

Additionally, a tailored training approach improves the learner experience by providing users more of what they need to know and less of what they don't. For example, those handling sensitive data may require more in-depth instruction on safeguarding procedures, while general staff may just need broader awareness basics. Avoiding excessive redundancy for knowledgeable users and overwhelming beginners with too much advanced material increases engagement.

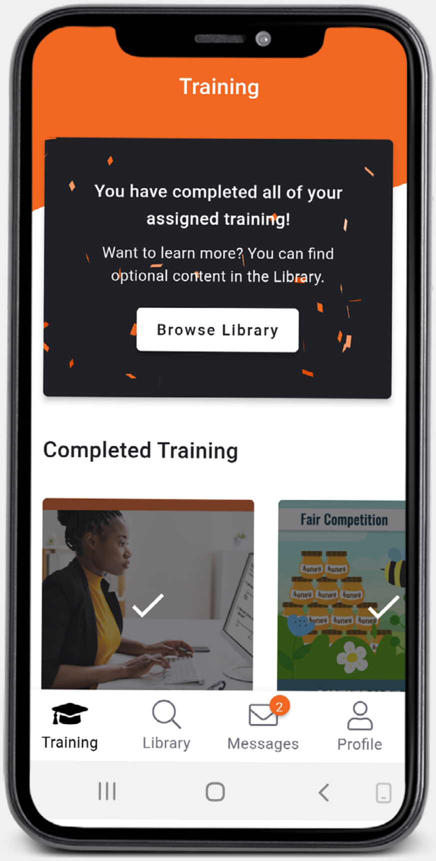
Fun and Games

The broader concept of "games" in security awareness training is typically considered in two ways.

First and hopefully the most obvious: games built into a training curriculum. There's nothing wrong with trying to work some fun into content that can typically be dry and boring. Training about how to spot phishing emails or testing knowledge on sensitive information practically beg to be worked into a game format. Fortunately, the better SAT vendors out there are jumping on this bandwagon, so you won't have to go this approach alone.

Second is the concept of "gamification." A properly equipped training platform will allow administrators to roll out mechanics like scoring, leveling up, earning badges and leaderboards to introduce an element of fun and satisfaction in mastering the content. Even just awarding points for completing training modules or getting quiz answers correct provides a gentle "nudge" that encourages focus.

Tapping into psychological motivators like achievement, competition and reward systems keeps learners invested in a way that an old-school PowerPoint presentation or a 45-minute training video cannot. This enables changes in behavior as well through positive reinforcement. Gamified elements like badges and leaderboards activate the brain's reward pathways, improving knowledge retention. Simply put, people love to be rewarded for stuff, especially if they get to show off in front of colleagues!



You have completed all of your assigned training!

Want to learn more? You can find optional content in the Library.

Outside the "Classroom"

A big part of effective learner experience is meeting learners where they are, and increasingly this means on their mobile devices. An effective security awareness program needs to make training accessible anytime, anywhere.

By delivering content optimized for mobile delivery, you allow learners to easily fit microlearning nuggets into their daily routines and workflows. Mobile-friendly training should be accessible during commutes, breaks or any other idle moments.

In this way, bite-sized modules and learning activities designed for mobile enable seamlessly integrating education into the typical ebbs and flows of the workday. Employees can squeeze in a 5-minute refresher or assessment when they have a free moment, reinforcing knowledge in the moment of need.

The flexibility and convenience of mobile-ready training removes barriers to access, driving higher engagement by meeting modern learners where they are rather than requiring them to be in a dedicated "classroom" setting. Your learners are going to be scrolling anyway. You might as well teach them something that benefits them and your organization.

The Upshot

An intentional, well-designed learner experience is key to driving engagement and change behavior with your security awareness program. Incorporating elements like tailored content, gamification and mobile accessibility helps you capture attention, and ensure lessons truly resonate. Training that feels personalized, interactive, and integrated into the modern workflow empowers employees and helps strengthen your security culture.

Learn More About KnowBe4's Approach to Security Awareness Training

Learn More