5 innovative cybersecurity training methods to try in 2021

Engaging methods raise workers' awareness up to 13 times

As much as 88% of data breaches are caused by human error, but only 43% of workers admit having made mistakes that compromised cybersecurity. In the past year a third of the breaches incorporated social engineering techniques and the cost of a breach caused by a human error averaged to $3.33 million.

To mitigate the risk, enterprises develop complex cybersecurity strategies and action plans, yet they are insufficient unless acknowledged by every member of their organization. Half of the Chief Information Security Officers (CISOs) plan to extend cybersecurity and privacy into all business decisions and that makes it every employee's concern.

"With the ever-changing and evolving digital threats, maintaining cyber resistance is no longer limited to IT and security officers and depends on every member of the organization. Constant training is a way to build the team's resilience against threats, yet it is not uncommon for them to turn into dull PowerPoint sessions, after which few remember the safety measures they should take. The problem is amplified by the workforce operating from home and not subscribing to security policies of the company", says Juta Gurinaviciute, Chief Technology Officer at NordLayer.

CISOs and other stakeholders can grab employees' attention by changing the methods of the regular cybersecurity training. Those who found training to be very interesting were 13 times more likely to change the way they think about cyber threats and protection against them. Therefore, organizations should seek memorable, entertaining and accessible ways to talk about complicated security matters.

5 ways to make cybersecurity training more attractive

Gamify it. Dull figures slide after slide, myriads of 'dos and don'ts' along with knotty safety procedures make the process lethargic. Quizzes, games, prizes and quality time with colleagues will enhance enjoyment and learning. Interactive activities boost engagement and thus yield better results when it comes to teaching staff about cybersecurity.

Engage in friendly competition. The key element of the gamification is competition. However, putting a prompt question within the video lesson or offering 'innovative' content is not enough. People are engaged when they have an incentive, be it a prize or pride. Companies should organize monthly, quarterly or yearly competitions to keep a workforce constantly aware of new threats and how to tackle them.

Make it rewarding. Turn the right answer into a badge, a discovered vulnerability into a star, and a year without an incident into a holiday bonus. People expect feedback while participating in a competition, and the reward system is the optimal way to do it. Instead of giving an opinion to everybody in private, security and IT professionals can award the achievements. They also help to track the progress of each employee and take the precautions if necessary.

Turn it into a team effort. Staying protected from breaches and attacks is everyone's interest. Thus employees should be encouraged to work in teams and solve riddles with their colleagues. In a cybersecurity workshop, for instance, employees can be asked to craft a phishing email. This encourages them to find out more about this criminal technique, to look at the examples of it and thus recognize them at the first glance next time.

Be understood. For information security professionals, IT and cybersecurity jargon is a native language. Yet for accountants, marketers and many others it's just a meaningless jabber. Make sure to speak clearly and to explain every term in plain language so the relative layman understands and remembers.

These tips also apply when teaching the staff how to use various cybersecurity tools, such as cloud services or VPNs. With people working remotely, many of them face the need to use two-factor authentication or secure connection for the first time as it was readily available by default at their usual workstations. Now they have to care for their and their company's protection themselves.

"Cybersecurity is no longer a thing only information security and IT departments care about. As many workplaces rely solely on digital solutions which are used by the entire workforce, staying protected against cyberattacks requires everyone's joint effort. The main notions of data security must be conveyed in an appealing manner" summarizes NordLayer expert.