SecurityAdvisor

Six Steps for a Cyber Immune Culture

Employees are the first line of cybersecurity defense for organizations. Focusing on the human element of an organization's cybersecurity strategy is the best way to effectively combat phishing techniques. People are often deceived by cybercriminals to trick them into performing risky online behaviors. Real-time personalized microlearning moments directly correlate with an individual's actions. Organizations can better educate and equip people to promote positive behavior, resulting in a cyber-immune culture.

Educate the entire organization on cybersecurity basics and roles.

Nurturing a strong cybersecurity culture requires clear guidelines and processes. Without this fundamental piece, security training will fall short, leaving employees confused and unsure of proper procedures.

Provide frequent and just-in-time training.

Humans retain information best when its continuously delivered, and having directly relate to an action taken. People listen more when they know the information is relevant and specific to them.

Customize training to specific role requirements.

Data on how cybercriminals target employees in various departments and jobs should be used to help organizations shape their security awareness training efforts. Real-life examples of cyberthreats give important context for employees, which helps them retain knowledge and interact with the coaching content.

Do not overdo phishing simulations.

In order to motivate workers to avoid hazardous internet activities, a positive approach is required. When a phishing assault happens, using an encouraging tone helps to develop employee trust, which makes people feel secure and encouraged to come forward. Organizations that overdo phishing simulations risk antagonizing the workforce and diminishing their influence.

Using AI and data analysis for a targeted approach to educate high-risk users.

Training and education should match an individual's real-life behaviors. Cybercriminals target individuals with extremely specific information, therefore cybersecurity teaching must have the same degree of customized connection. AI assists with the ability to message an individual instantly after risky behavior is carried out and uses contextual nudges over time to ensure a change in behavior.

Measure and report the results.

The ability to effectively measure security training results enables executives to continue developing and improving their organization's cyberculture over time.