5 MISTAKES TO AVOID WITH A NEW USER AWARENESS PROGRAM

All the security tools in the world are incomplete without trained users. User awareness training programs exist to educate users and equip them with the skills to be the last line of defense against cyberattacks. Even with the best intentions, user awareness training programs can fall flat. To make the most out of your investment and truly increase security, here are five mistakes to avoid when launching a program.

1. LACK OF ORGANIZATIONAL BUY-IN

Developing a true, company-wide program means that multiple departments need to have involvement: IT will be responsible for deployment and management, HR for ensuring all employees are involved and executive leadership to manage adaptation. Therefore, it is important that as a first step there is inter-departmental buy-in with key players. The major players must be on board and understand the value of a program. This support is critical for a trickle-down effect of getting company buy-in and participation.

2. INCONSISTENT PROGRAM

Three billion phishing emails are sent every day. Is one, 30-minute training a year enough to keep employees vigilant and educated on such attacks? A truly effective program is consistent and year-round to keep it top of mind for all users.

3. ONLY CHECKING A REQUIREMENT BOX

Cybersecurity insurance companies are now requiring user awareness training programs as a prerequisite to coverage. State regulations and mandates also require security protections and training. Regardless of your reason for implementing a program, simply checking the requirement is not enough. To be frank, it is a waste of money and resources. User awareness programs are empowering and reap years of defense while deploying a single simulated phishing attack does little.

4. UTILIZING GENERIC TACTICS

Attackers are sneaky. When the payday is big enough, attackers will do their research and due diligence into crafting appropriate messages for an individual and organization. If obvious, generic templates are used during simulated training attacks, users are not getting the most beneficial experience or developing a keen eye.

5. LACK OF A DEDICATED RESOURCE

Not having a dedicated resource to implement, track and customize your program puts the organization at a disadvantage. User awareness programs require a fairly heavy lift to implement and a variety of upkeep tasks. We'll be honest, the initial setup is not incredibly long. However, the value is not in a single running, but rather how organizations create custom, ongoing trainings.

At the end of the day remember: people, users, employees are the targets of cyberattacks – not security tools and machines. If you're spending the money on a user awareness training program, then move the needle and properly educate users by avoiding common mistakes.

ABOUT BRITEPROTECT

BriteProtect is an advanced managed security service that solves the problem of tedious alert management leading to missed critical alerts and employee fatigue. We leverage decades of cybersecurity experience to provide our customers with unprecedented visibility, swift response and expert insights delivered via people, process and technology. Now, organizations can leverage existing security tools by partnering with Brite's team utilizing new, next-generation technology to elevate its security posture and better utilize internal resources.