AN ESSENTIAL GUIDE FOR NATIONAL CYBER SECURITY AWARENESS MONTH

CyberTalk.org

Cyber Security Awareness Month reflects a collaborative effort between governments and private entities to raise awareness regarding digital security. Objectives include empowering employees and individuals to take an active role in the prevention of cyber threats and the continuous safeguarding of information.

Research indicates that the majority of enterprises are behind when it comes to implementing strong cyber security practices. To fight against malicious intent, it's critical fororganizations to educate, inspire and lead people to make cyber security best practices part of everyday routines.

Informing employees about their role in mitigating cyber risk shifts the burden of risk management from IT alone to everyone; together. It also drives positive behavioral changes that shape an organization's overall cyber security posture.

68% of business leaders believe that their cyber security risks are increasing, but only **46%** of IT departments feel ready to handle advanced cyber attacks.

Your organization can leverage Cyber Security Awareness Month in order to create a culture of cyber security that will make your organization more resilient, anti-fragile and ready for whatever comes next. Here's exactly how to accomplish that.

Get buy-in for organization-wide awareness initiatives. There's nothing worse than planning educational awareness activities, only to have them swept aside because high-level leadership doesn't see their value. Provide your leadership with compelling reasons to support you and your team as you work to increase cyber security awareness across your organization.

1 Develop a Cyber Security Awareness Month campaign.

Outside of IT or technology roles, employees often don't know about or have no particular reason to care about cyber security. The launch of a cyber security awareness campaign can help align employees with larger organizational goals when it comes to cyber security.

As you develop a Cyber Security Awareness Month campaign that's directed at internal employees, be sure to consider company objectives, behaviors that the security team wants to transform, and this year's cyber security awareness month theme. Also, consider creating a different focus for each week of the campaign.

Ensure that you also have means of measuring the campaign's impact. Report on campaign results, which should show that security is taken seriously by your organization's employees.

2 Tackle the biggest business risks.

Cyber Security Awareness Month offers an opportunity for IT administrators to consider how employee actions impact the organization's cyber security, and what behavioral changes would be most helpful preventing threats.

For example, phishing threats often trick employees into sharing login credentials, clicking on malicious links or downloading malicious files. The vast majority of organizations will benefit from embedding phishing recognition activities into a larger cyber security awareness campaign. Inadequate employee awareness around phishing techniques is a major business risk.

3 Calendar a range of cyber security awareness programs.

Whether your employees are working-from-home or in-person at the office, there are an endless number of ways to organize fun, engaging and educational cyber security events.

For example, create mini cyber security training sessions. Training sessions can take place across a series of days or weeks – each with its own theme. You can offer them as asynchronous or synchronous courses or modules.

Each type of training session can include the same type of activity (ex. phishing training is always gamified) or you can plan for different types of activities within different types of learning blocks.

4 Make cyber security awareness fun.

While it might not be Disney World-level fun, cyber security doesn't have to feel like watching paint dry. Among those in non-technology roles, cyber security tends to be branded as snooze-worthy, so try to break the stereotype, if possible.

For example, immersive, online and game-based learning can help employees gradually advance their skills through fun, visually engaging means. Gamification tools often include digital rewards, helping employees feel a sense of accomplishment around their learning and a desire to keep going.

Consider inviting a fun and engaging guest speaker to converse with your audience. Find someone who can clearly communicate cyber security messaging through storytelling. Help everyone plan for a Q&A session at the end.

No matter which educational awareness paths you pursue, be sure to identify a nice way to recognize your employees for their cyber security achievements. Find a tangible means of showing your employees how much their training has truly assisted the organization.

5 Run a social media campaign.

#Cybersecurityawarenessmonth. In planning your Cyber Security Awareness Month strategy, develop a social media campaign that highlights key cyber security messages. Make sure that you set the right tone.

In your campaign, use photos, infographics, video elements or a combination of all three. Include relevant hashtags in posts and be sure to link to helpful, informative and engaging content.

Publish a new set of Cyber Security Awareness Month posts every day, every other day, or share cyber security tips once per week. Measure reactions and shares to determine what kind of messaging is most relevant and effective.

FURTHER THOUGHTS

Employee education is key. Cyber Security Awareness Month helps organizations show employees how they can participate as empowered advocates for cyber security and the security of the organization as a whole.

For more information about how to create a security awareness program that employees will enjoy, please see this CyberTalk article.

Lastly, to receive cutting-edge cyber security news, exclusive interviews, expert analyses and security resources, please sign up for the CyberTalk.org newsletter.