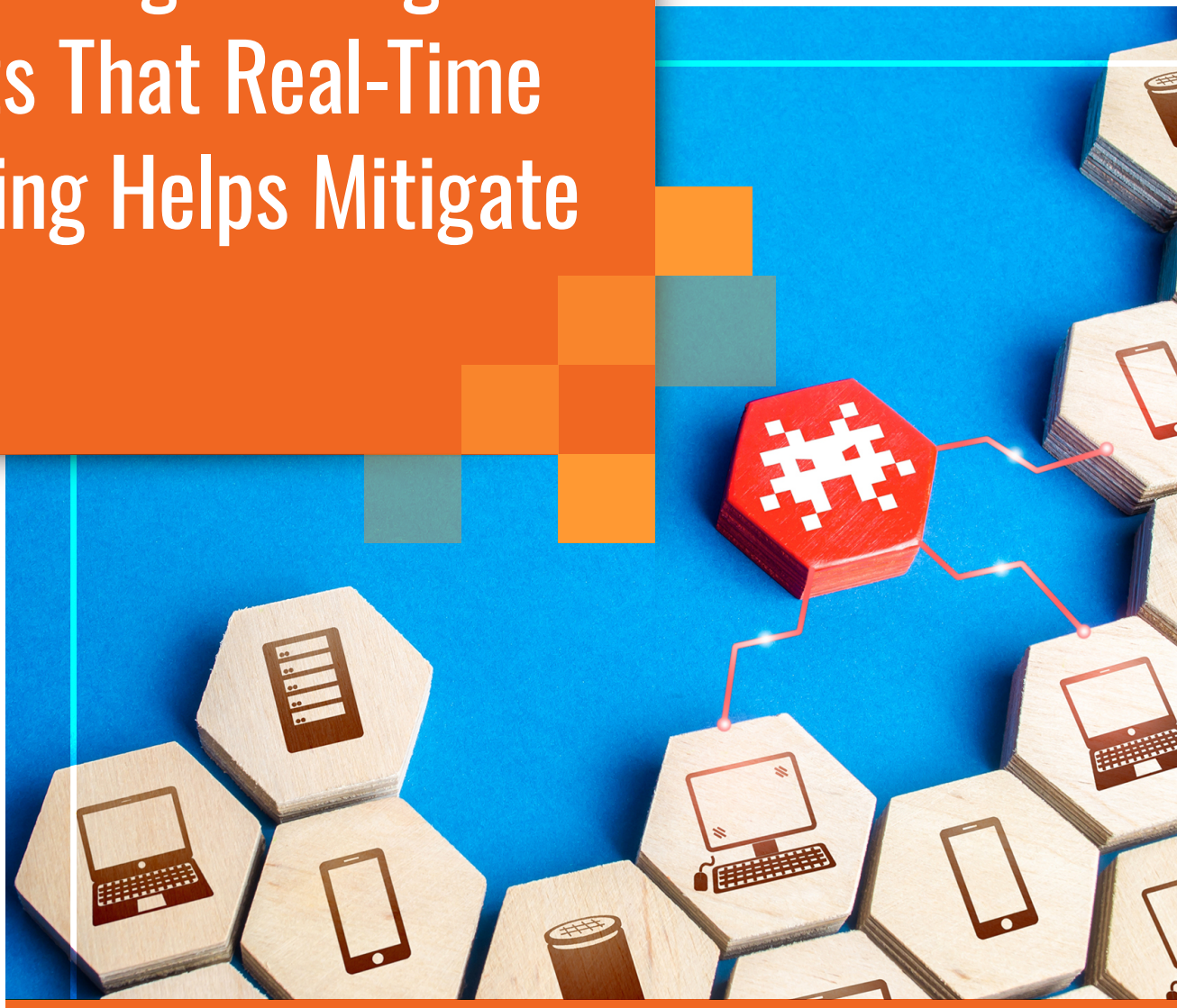
KnowBe4
Human error. Conquered.

7 Social Engineering Threats That Real-Time Coaching Helps Mitigate



INTRODUCTION

Fortifying your organization's human firewall represents the last line of defense against cyber attacks and data breaches. New-school security awareness training is one of the best ways to accomplish this.

Another is real-time coaching of users in response to risky security behaviors by sending the right education at the moment of risky action. To accomplish this, a real-time coaching platform like KnowBe4's SecurityCoach consolidates alert data from your organization's security stack (endpoint management, email/web, identity access, SIEM/SOAR, etc.), analyzes it and determines which threats provide the best opportunities to coach your users. Real-time coaching presents the chance for organizations to fortify their human firewall against an array of social engineering threats.

7 SOCIAL ENGINEERING THREATS

Here are seven of the most common social engineering threats and how real-time coaching can help mitigate them leveraging alert data from your existing security stack.

Downloading Potentially Dangerous File Attachments
Many social engineering attempts revolve around getting a potential victim to download and/or open a dangerous file attachment, such as an EXE, DOC or HTML file. Many of the aforementioned security tools will block the majority of high-risk file downloads. However, when integrated with real-time coaching, these actions can be used as an opportunity to train users not to download potentially malicious files.

Clicking on High-Risk Links
Many social engineering attempts contain malicious URLs masquerading as a trusted link from a particular vendor or trusted source. Again, many of the aforementioned security tools will block these rogue links. But when integrated with real-time coaching, this alert data can be used to remind users to hover over URL links to inspect it for legitimacy before clicking on it.

Content Filtering
Many security tools block objectionable content as defined by an organization's content policies. For example, a user might try to watch a violent video or get tricked into reading questionable/inappropriate content. Access to this content is blocked, and the user can be presented with a warning message to avoid similar content because it is against an organization's policies.

Executing or Installing Unauthorized Software
Users often try to install software not approved by the organization. A security application control program would block the install or execution, while real-time coaching could be used to remind users not to install unauthorized applications or services in addition to other relevant information.

Initiating Rogue Outbound Connections
Certain network traffic analysis and monitoring tools identify rogue outbound connections to known malicious locations. When paired with a real-time coaching platform, the user could be reminded not to install or use any unauthorized communication software or services.

Trying to Login Into Unauthorized Computers
Within most organizations, computer-to-computer logins are rare. A primary sign of malicious activity is unexpected logins coming from one computer to another without there being a legitimate reason. Many of the aforementioned security tools will block these rogue connections, and a real-time coaching platform could remind users not to attempt to log into computers they are not authorized to use.

Trying to Bypass Multi-Factor Authentication Requirements
Many organizations require users to use multi-factor authentication (MFA) to login to the organization's networks or computers. Users who attempt to bypass MFA or use an unauthorized form of MFA will typically invoke a detection and blocking mechanism. A real-time coaching platform could be used to remind users they must use a company-approved MFA login.

REDUCE RISK AND IMPROVE YOUR SECURITY CULTURE

Ultimately, people are more likely to accept correction when their mistakes are immediately identified and security best practices are provided in real time.

Real-time coaching accomplishes this, allowing your organization to:

- Reinforce existing security awareness training
- Gain insight into security risks by tracking trends in your users' risky activity over time
- Reduce human risk and improve your organization's overall security culture
- Extend the value of your existing security stack by integrating with common security tools you already leverage

Turn the table on threat actors and their mischievous tactics by adding real-time security coaching to your security awareness toolset.

LEARN MORE [How SecurityCoach Can Strengthen Your Human Firewall]

Additional Resources

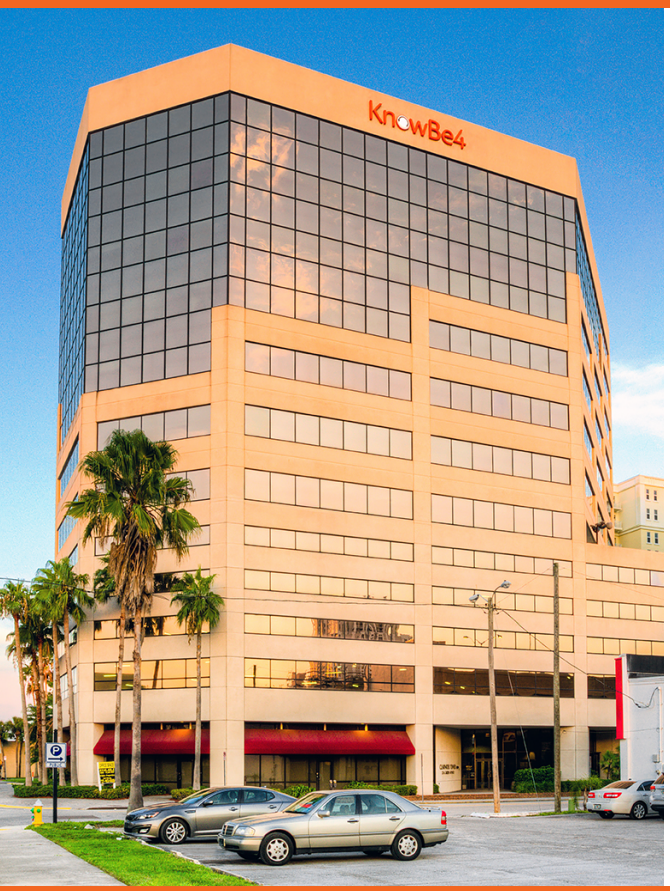
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01D03K01