KnowBe4

How Real-Time Security Coaching Mitigates Spear Phishing, Malware and Ransomware

Of all the cyber threats your organization faces, spear phishing, malware and ransomware are the most pervasive, costly and common.

Traditional security tools, such as endpoint protection, email security and intrusion management products, are absolutely essential to mitigate these threats, but they don't fully address the dynamic nature of these attacks. A new, more innovative, proactive approach is required to truly secure your organization from these threats.

Real-time security coaching has emerged as a powerful tool in this context. By providing guidance to users as they interact with a potential threat, real-time security coaching becomes an essential two-pronged mitigation strategy: it provides real-time guidance to mitigate an attack before it succeeds while also providing feedback and training at the moment of risky behavior.

This whitepaper examines how real-time security coaching can significantly reduce the risks of spear phishing, malware and ransomware attacks.

A TRIPLE THREAT LANDSCAPE

Spear phishing, ransomware and malware comprised approximately 70% of all cyber attacks in 2023, according to industry reports by Verizon, Sophos and Check Point. Here is a brief overview of all three.

Spear-Phishing Campaigns

Spear phishing is a targeted attempt to steal sensitive information such as login credentials or financial information by masquerading as a trustworthy entity. Unlike generic phishing, spear phishing is targeted at a specific individual or department within an organization that appears to be from a trusted source. Cybercriminals gather details about their targets through social media, corporate websites and other online sources to craft emails that appear legitimate.

- Spear-phishing attacks have increased by 667% since 2020, according to Barracuda Networks
- The average cost of a spear-phishing attack for an organization is $1.6 million USD, according to Ponemon Institute

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or data until a ransom is paid. Attackers use various vectors, such as phishing emails or exploit kits, to infiltrate systems. Once inside, the ransomware encrypts critical files, rendering them inaccessible. The victim is then extorted to pay a ransom, often in cryptocurrency, to regain access. Ransomware attacks cause downtime, data loss and intellectual property theft.

- Ransomware attacks have increased by 105% year-over-year, according to the 2023 SonicWall Cyber Threat Report
- The average cost of a ransomware attack for an organization is $1.85 million USD, according to Sophos research

Malware

Malware, or malicious software, encompasses a broad range of harmful programs including viruses, worms, trojans and spyware. These programs can disrupt operations, steal sensitive data, or provide unauthorized access to an organization's systems. Malware is often spread through email attachments, infected websites and software downloads.

- Malware attacks have increased by 87% since 2023, according to Check Point research.
- The average cost of a malware attack for an organization is $3.5 million USD, according to IBM's Cost of a Data Breach Report, 2023

REAL-TIME SECURITY COACHING: A GOLDEN OPPORTUNITY

Real-time security coaching is a new cybersecurity tool focused on the human layer of security. Instead of viewing users as a liability, real-time security coaching recognizes that users can become your organization's greatest security asset through targeted behavior change.

Real-time security coaching correlates, identifies and responds to user-related security events detected by other security tools and delivers immediate feedback to the user using real-time coaching. Alongside security awareness training, real-time security coaching is a critical component for strengthening the security culture of an organization.

This is critical within the context of spear phishing, ransomware and malware, because it offers the ability to mitigate the threat at the moment the security event is detected while also turning it into a coachable moment to increase future awareness. By delivering timely alerts, behavioral analysis, and in-the-moment training, organizations take a proactive approach that both addresses the immediate threat and also reinforces long-term security practices to reduce cyber risk.

SPEAR-PHISHING MITIGATION AND AWARENESS WITH REAL-TIME SECURITY COACHING

Real-time security coaching can provide immediate, contextual guidance to your users as they encounter potential phishing threats, improving their ability to recognize and respond appropriately. Here are some examples of how real-time security coaching can be used to mitigate phishing and drive awareness:

Email Filtering and Alerts

Advanced email security products play a crucial role in combating spear phishing. These products analyze incoming emails for characteristics indicative of phishing, such as suspicious links, unusual sender addresses or urgent language. When a malicious email is detected, users can receive a real-time alert to be on the lookout and to report any suspicious emails using their Phish Alert Button.

Immediate Feedback on Risky Behavior

If an employee clicks on a potentially dangerous link or opens an unverified attachment, real-time security coaching can provide immediate instructions to report the email and/or contact your IT department. Additionally, it can explain why the action was unsafe and how to avoid such risks in the future.

Pop-Up Warning for Unverified Website

If a user does fall for a phishing email and visits a potentially harmful website or enters credentials on a suspicious login page, real-time pop-up warnings can alert them to the dangers. These warnings can suggest safer alternatives and provide brief educational messages explaining the risks.

Reinforce Simulated Phishing

Simulated phishing is an effective way to train users on identifying and responding to spear phishing attempts. If a user interacts with a simulation, they receive immediate feedback explaining what they missed and how to spot similar attacks in the future. Additionally, they can be prompted to complete a short training module. This hands-on approach helps users build practical skills in a controlled environment.

RANSOMWARE/MALWARE MITIGATION AND AWARENESS WITH REAL-TIME SECURITY COACHING

Real-time security coaching can also play a crucial role in mitigating ransomware and malware threats by providing immediate guidance to users. Here are some examples of how real-time security coaching can be used to address these threats:

Real-Time Scanning and Alerting

Firewalls, emails security gateways and endpoint protection tools continuously scan for malware in emails, downloads and files. When a threat is detected, real-time security coaching can leverage that alert data to provide a user with an alert explaining why a file is suspicious and instructions on how to handle it.

Behavioral Analysis

Security tools can also analyze user behavior that could lead to a ransomware or malware download, such as downloading a file from an untrusted source, visiting a suspicious website or engaging with an attachment in an email. Real-time security coaching can provide a real-time notification of why this is dangerous and potential actions to immediately take, such as contacting your IT department.

Automated Incident Response

When malware is detected on a user's system, real-time security coaching can direct users towards instructions for isolating the system, running an antivirus scan and contacting the IT department. These automated responses help users take immediate action to contain and mitigate the threat.

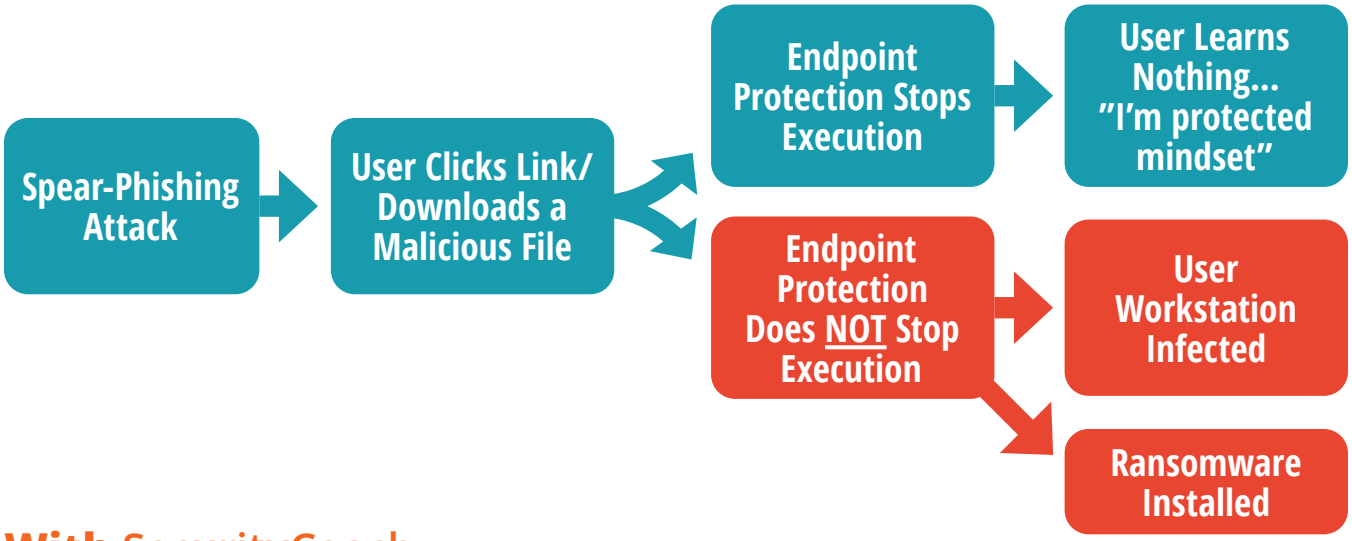
KNOWBE4'S SECURITYCOACH

KnowBe4's SecurityCoach is the industry's first real-time security coaching product that provides coaching to users at the moment of risky behavior. It takes alerts generated by your security stack, analyzes them, identifies events related to risky behavior, and sends a SecurityTip to the appropriate user about the activity and how to avoid it in the future.

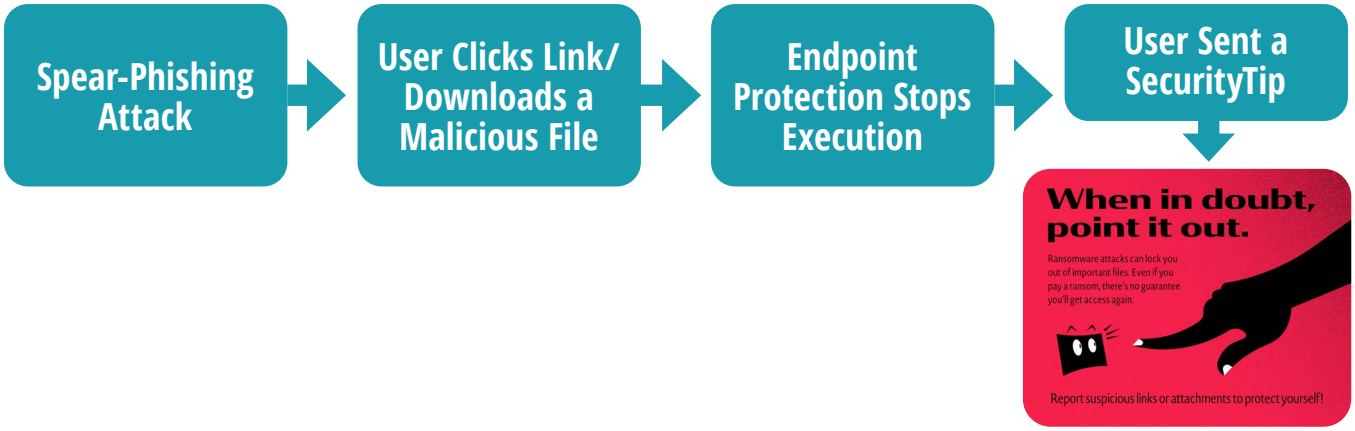
There are four key components that allow SecurityCoach to help mitigate an attack before it succeeds and reinforce your organization's security awareness to reduce risk moving forward.

Integrations	Detection	Real-Time Coaching	Reporting
Integrates directly into your existing security stack to access alerts generated by risky user behavior.	Sift through all the alert "noise" and identify actionable events that present an opportunity to coach the user.	At the moment risky behavior is detected, SecurityCoach sends a real-time SecurityTip directly to that user via Microsoft Teams, Slack, Google Chat or email.	Detailed reporting of coaching campaigns, detection rules and detected security events, in addition to the ability to measure a user's risk to the organization based on their behaviors.

Without SecurityCoach



With SecurityCoach



Conclusion

Real-time security coaching represents a new approach to mitigating spear phishing, ransomware and malware. By providing users with immediate, contextual feedback and training, organizations can affect real behavior change through enhanced security awareness and reduce the likelihood of successful attacks. It presents a unique opportunity to address immediate threats while fostering a stronger security culture that reduces cyber risk.

Learn the Top 10 Risky Behaviors SecurityCoach Has Detected →

Learn More About KnowBe4's SecurityCoach →

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, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4

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

01E08K01