

2025 SECURITY AWARENESS TRAINING SCHEDULE

Keeping Employees Informed About Cyber Threats.

Q1

Q2

Q3

Q4

Internet Security and
Phishing Alerts
(24 min)

Security Culture and
AI Scams
(22 min)

Common Threats
and Social
Engineering (14 min)

Holiday
Cybersecurity
Essentials (23 min)

QUARTERLY TRAINING

Q1 Feb	Your Role	18 min	<u>2025 Your Role: Internet Security and You</u> Tactics constantly evolve. This training teaches participants to recognize threats like phishing emails and malicious links, equipping them to protect themselves, their devices and their organization from data breaches, ransomware and other cyber risks.
	Phishing Alert Button	3 min	<u>Make it a Habit ... PAB it!</u> This introductory module will explain how the Phish Alert Button (PAB) protects your organization from phishing attacks and why it is so important to make reporting suspicious emails a security habit.
	2FA Fatigue	3 min	<u>Push It to the Limit: Push Notification Abuse</u> Don't fall victim! This module will cover what push notification abuse is, how these attacks work and provide tips on how to respond to a push notification attack.
Q2 May	Culture of Security	10 min	<u>2025 Security Culture Survey (SCS)</u> The Security Culture Survey provides an accurate and reliable assessment of the current state of security culture across your organization.
	AI Scams	10 min	<u>New Tools: Artificial Intelligence Scams</u> AI technologies enable more realistic phishing attacks and entirely new scams like voice cloning and deepfakes. This module uses videos and scenarios to teach detection and prevention strategies, ending with a short quiz to reinforce learning.
	AI Chatbots	2 min	<u>Captain Awareness: AI Chatbots and Sharing Sensitive Information</u> Nick learns the dangers of using unapproved AI tools.
Q3 Aug	Common Threats	14 min	<u>2025 Common Threats</u> This interactive module demonstrates a phishing attack leading to ransomware, teaching users to spot email red flags and understand cloud security's role. Participants will learn to report incidents and build a proactive cybersecurity culture, equipping them to better safeguard their organization.

continued >>>

2025 SECURITY AWARENESS TRAINING SCHEDULE

Keeping Employees Informed About Cyber Threats.

Q4 Nov	Safe Holidays!	7 min	<u>The Gift of Awareness: Holiday Cybersecurity Essentials</u> Stay cautious and safe, even during the busy holiday season, with simple tips for work and home. This module teaches how to spot scams, identify unsafe links, recognize deepfake videos and address privacy concerns with smart devices.
	Think Before You Click	16 min	<u>2025 Social Engineering Red Flags:</u> This module highlights top threats like business email compromise, authentication fraud and AI-driven impersonation. Learn to recognize warning signs and respond effectively to protect yourself and your organization.

INITIAL & NEW EMPLOYEE TRAINING			
Basic Training		15 min	<u>2025 KnowBe4 Security Awareness Training</u> Learn to spot cyberattack warning signs, understand common threats and take proactive steps to protect your organization. This interactive course covers the latest cyberthreats, including simulated phishing attacks, and teaches users to identify red flags in emails. It emphasizes the role of cloud security, reporting incidents using tools like the Phish Alert Button (PAB) and fostering a culture of vigilance.
What Do You Know?		10 min	<u>2025 Security Awareness Proficiency Assessment (SAPA)</u> Assess your organization's proficiency in seven key security awareness training topics. Each user will be presented with 21 questions (pulled randomly from larger question pools) of varying difficulty. The results can be used to create more effective security awareness and behavior training programs.
Phishing Alert Button		3 min	<u>Make it a Habit ... PAB it!</u> This introductory module will explain how the Phish Alert Button (PAB) protects your organization from phishing attacks and why it is so important to make reporting suspicious emails a security habit.
2FA Fatigue		3 min	<u>Push It to the Limit: Push Notification Abuse</u> Don't fall victim! This module will cover what push notification abuse is, how these attacks work and provide tips on how to respond to a push notification attack.
You Clicked?		5 min	<u>Phishing Reinforcement: So You Clicked, Now What?</u> What happens when someone falls for a phishing attack? How do you know if a device is infected with malware? What steps can you take to remove malicious infections? This module answers those questions by demonstrating the dangers of phishing and how to avoid them.

REMEDIAL TRAINING			
If You Fail Email Test	Basic Training	15 min	<u>2025 KnowBe4 Security Awareness Training</u> Gain insights into the tools and tactics cybercriminals use, learn to recognize the warning signs of cyberattacks and understand the best actions to take when faced with such situations.
You Clicked?	Remedial	5 min	<u>Phishing Reinforcement: So You Clicked, Now What?</u> What happens when someone falls for a phishing attack? How do you know if a device is infected with malware? What steps can you take to remove malicious infections? This module answers those questions by demonstrating the dangers of phishing and how to avoid them.