

State of Maine: State and Local Cybersecurity Grant Program (SLCGP)

Building a Secure Future

Getting Started with Cybersecurity Training

August 11, 2026

Overview

1. SLCGP Overview
2. Implementation Strategies
3. Services: KnowBe4
4. NuHarbor Security Overview
5. Questions



Presenters

Jesse Blier

Deputy Chief Information Security Officer
State of Maine

Emily Kaster

Statewide Cybersecurity Coordinator
State of Maine

Tiffany Campo

Project Manager
Michael Baker Intl.

Kristin Lothar

Project Manager
KnowBe4

Amy McLellan

Project Manager
NuHarbor Security

Emily Crawford

Project Support
NuHarbor Security

State and Local Cybersecurity Grant Program (SLCGP)

National Programmatic Goal

Improve cybersecurity posture of state, local, and territorial (SLT) government organizations.

Key Objectives

- Develop and implement cybersecurity plans.
- Enhance cybersecurity resilience through assessments and training.
- Encourage the adoption of best practices, such as multifactor authentication and data encryption.



Administered by the U.S.
Department of Homeland
Security (DHS)



Funded by the
Infrastructure Investment
and Jobs Act (IIJA)

SLCGP Implementation Strategies



Build and leverage partnerships

Building relationships with partners across Maine and maintaining open lines of communication with critical infrastructure sector leads to ensure a coordinated approach.



Reduce barriers

Strive to understand what barriers organizations face in implementing cybersecurity best practices and identify collective approaches to overcome them.



Increase resiliency

Build capability and capacity at the organizational level to ensure the impact of these cybersecurity initiatives is enduring and sustainable.



KnowBe4

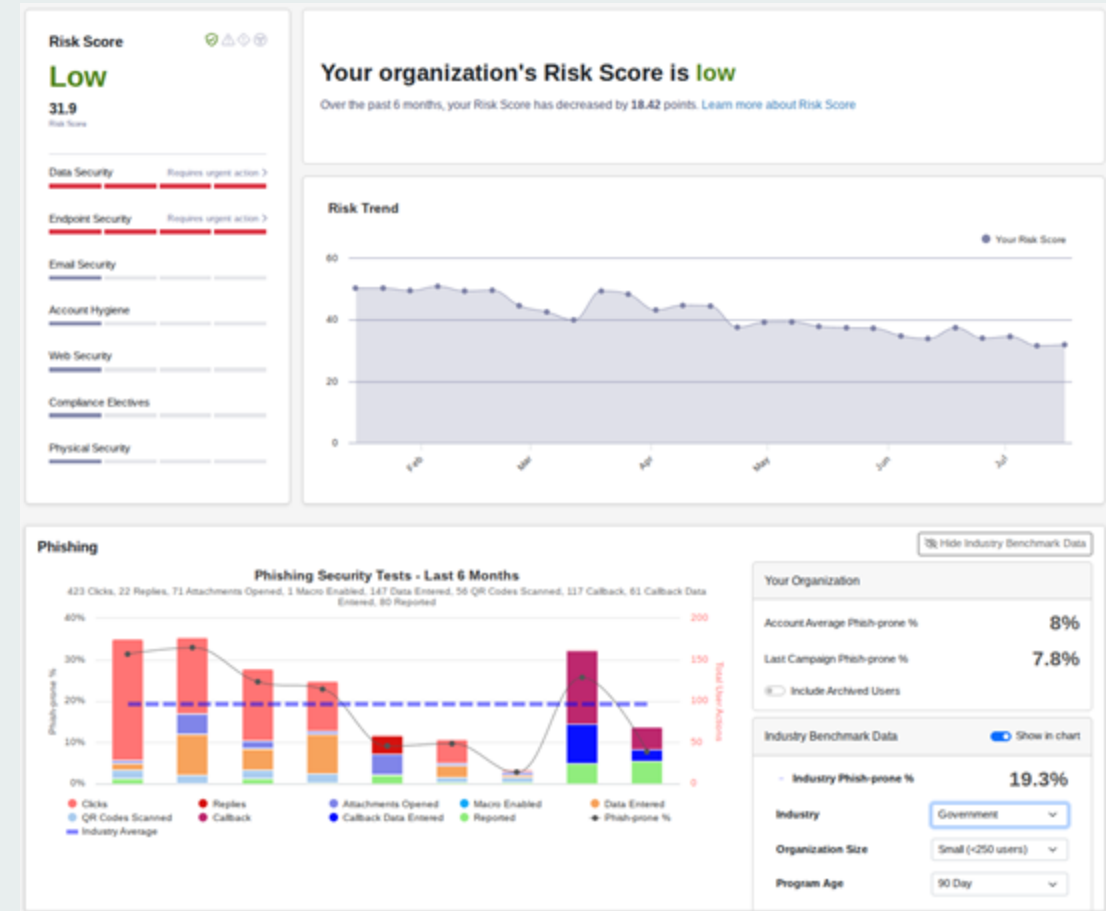
Security Awareness Training

KnowBe4 Security Awareness Training

KnowBe4 transforms your workforce from a vulnerability into your strongest security asset

Personalized, relevant, and responsive AI-native attack simulation and training, covering topics like:

- Phishing and email security
- Social engineering attacks
- Ransomware threats
- Data protection & privacy
- Mobile device security
- Password management



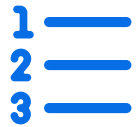
KnowBe4 Managed Services

Program Overview

Getting Started



A structured onboarding process guides administrators through the steps needed to launch their program.



Onboarding Form

You complete and submit the provided Onboarding Form for your organization.



Console Creation

We work with KnowBe4 to create your organization's console.



Account Setup

You add the staff you want to be trained.

You modify settings to allow KnowBe4 to send you emails.



Ready for Training!

Your organization is ready to receive training and testing.



Building Security Awareness



Security Newsletters

- Share simple, practical security tips and tricks to help everyone stay cyber-safe.



Security Training

- Teach staff how to recognize common cyber risks and how to protect themselves.



Simulated Phishing

- Send realistic but fake phishing emails to help teach staff how to spot scams in real-time.



Remedial Testing & Training

- Provide an extra layer of training to staff who are tricked by the simulated phishing test.

• Did You Know?

- Phishing was the initial attack vector for 15% of breaches analyzed in Verizon's 2024 Data Breach Investigations Report.

“Security is a process, not a product.” - *Bruce Shneier*



Phishing Email Example

From: Chase Bank < alerts@security-chasebank.com>

Reply-To: Chase Bank <alerts@security-chasebank.com>

Subject: Suspicious transactions

652340



Shocking content to entice you to click link or open attachment.

 Suspicious transactions have been taking place with your account.

 To halt them, please immediately log in from this link.

 <https://www.onlinebanks-chase.com/av98/sesh5q2wlkws>

Support When You Need It



Documented Guidance

Step-by-step guides provide instructions and resources to support each phase of the program.



Individual Issue Resolution

1:1 support to help administrators address specific needs, challenges, and program goals.



Open Office Hours

Convenient drop-in sessions provide timely support to common questions or challenges.



Dedicated Support Email: securitytraining@nuharborsecurity.com

The primary support channel to directly ask questions, share feedback, or request changes.



Questions?

Resources:

www.maine.gov/mema/grants/state-and-local-cybersecurity-grant-program

Email:

SLCyberSecurity.Grant@maine.gov