STATE & LOCAL CYBERSECURITY GRANT PROGRAM (SLGCP)

ADMINISTRATOR'S GUIDE TO KNOWBE4

Publication Date: 09/09/2026
Version: 1.0

Last Updated: 09/08/2026

Table of Contents

Getting Started

Welcome to the State of Maine's State and Local Cybersecurity Grant Program! We're excited you're helping strengthen the State's cybersecurity awareness across counties, towns, and K-12 schools. This program provides security awareness training through the KnowBe4 platform. Additional activities such as phishing testing, remedial training, and remedial testing are also offered.

This guide is meant to assist administrators with navigating the KnowBe4 platform, setting up campaigns, and implementing a security awareness program for their organization.

If you run into technical issues or questions about using the platform, please reach out to the nuHarbor support team at securitytraining@nuharbor.com. If you have questions or concerns about program eligibility, licenses, or participation in the program, please reach out to SLCyberSecurity.Grant@maine.gov.

Before You Begin

By now you should have:

1. Filled out the Onboarding Form, where you set your preferred management model (Self- or nuHarbor-Managed content) and content preferences (which of the testing, training, and remedial activities your organization wishes to participate in).
2. Signed into your KnowBe4 console and added your list of staff to be trained.
3. Set up any whitelisting and/or the Phish Alert Button, if desired (highly recommended). Please refer to the Configuration Guide on the SLCGP website for instructional guidance on setting these up.

If you have not already signed into your console and added your staff, you have not finished the onboarding portion of the program. Please reach out to the nuHarbor support team.

Self-Managed Administrator Responsibilities

Your onboarding form shows that your organization has elected to self-manage its security awareness training program. This means that your organization administrator is responsible for the following actions:

- Maintaining a list of users (staff) to be trained in the KnowBe4 platform
- Selecting, scheduling, and distributing **at least one** security training campaign annually. This is a program requirement.
- Selecting, scheduling, and distributing phishing testing through KnowBe4
- Selecting, scheduling, and distributing remedial training and testing in KnowBe4
- Forwarding new newsletter notifications to users (staff), as desired
- Educating your users (staff) on how to report phishing emails
- Monitoring and analyzing training and testing results

If you wish to switch to a nuHarbor-Managed model instead, please reach out to the nuHarbor support team.

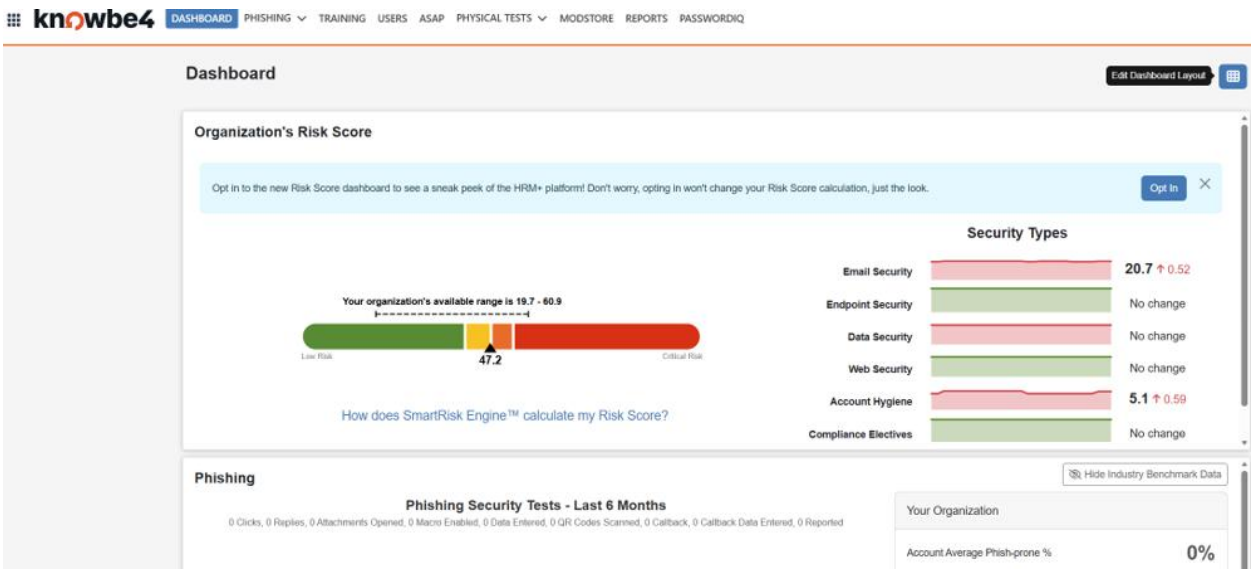
Navigating KnowBe4

This section provides a high-level overview of the KnowBe4 platform. It is not an exhaustive guide on all features offered by the KnowBe4 platform. Links to additional KnowBe4 resources are provided for detailed information on platform features.

At the top of your screen, to the right of the KnowBe4 logo, is a set of tabs labeled: Training, Users, ASAP, Physical Tests, etc. Clicking on these tabs will navigate you to different functions of your console. Continue reading to understand what each tab/function does.

Dashboard

After logging into the platform, you will be greeted with the Dashboard page. This is a snapshot of how your program is doing overall. It is only visible to you, users with administrative rights, and the nuHarbor team.



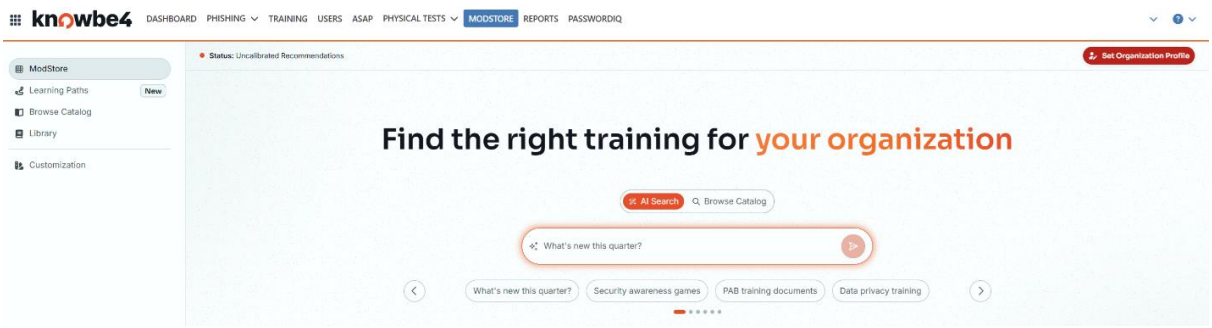
The following information (and more) is displayed:

Risk Score	A single number estimating your organization's overall security risk based on staff behavior, tracked over the last six months.
Security Awareness Proficiency Assessment (SAPA)	A score estimating how prepared your organization is to recognize security threats, compared to similar organizations.
Security Culture Survey (SCS)	An optional survey comparing your staff's attitudes toward security to similar organizations.
Phish Alert Button (PAB) Activity	Shows how many staff installed the button and how many suspicious emails were reported (and if they were real or fake).

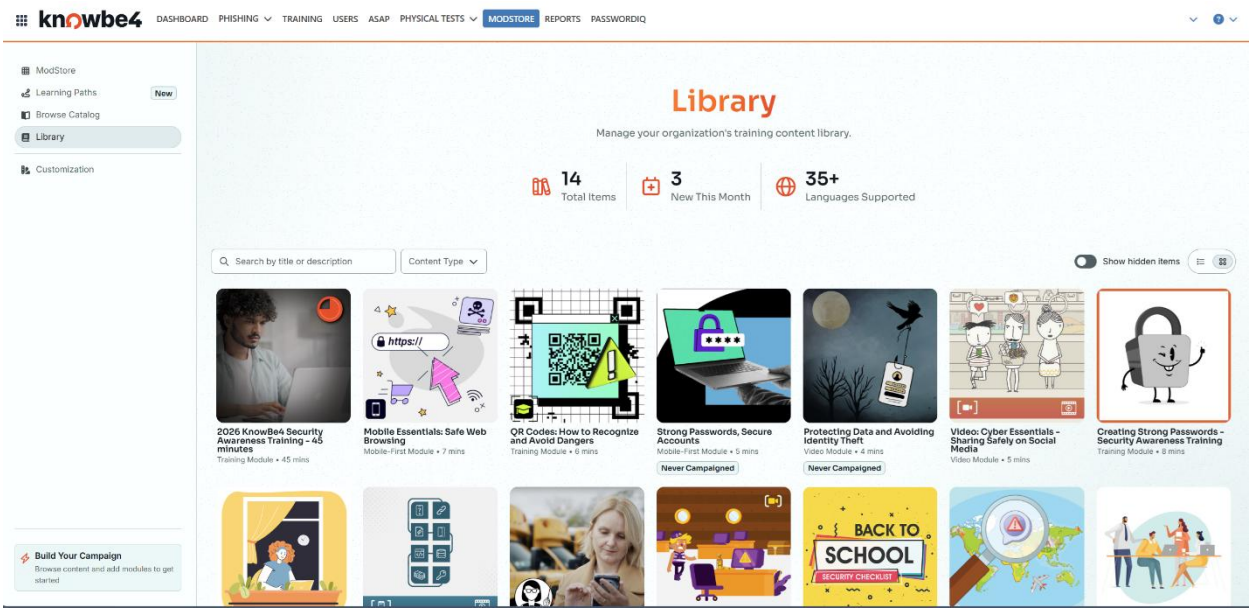
Additional Resource: Dashboard Overview – KnowBe4 Knowledge Base

Modstore

The Modstore or module store is where you can view all of KnowBe4's available training content. You can search for content by either using the AI search or by browsing the catalog. When you find a module you want, click the + Add to Library button on its card (or on its details page) to add it.



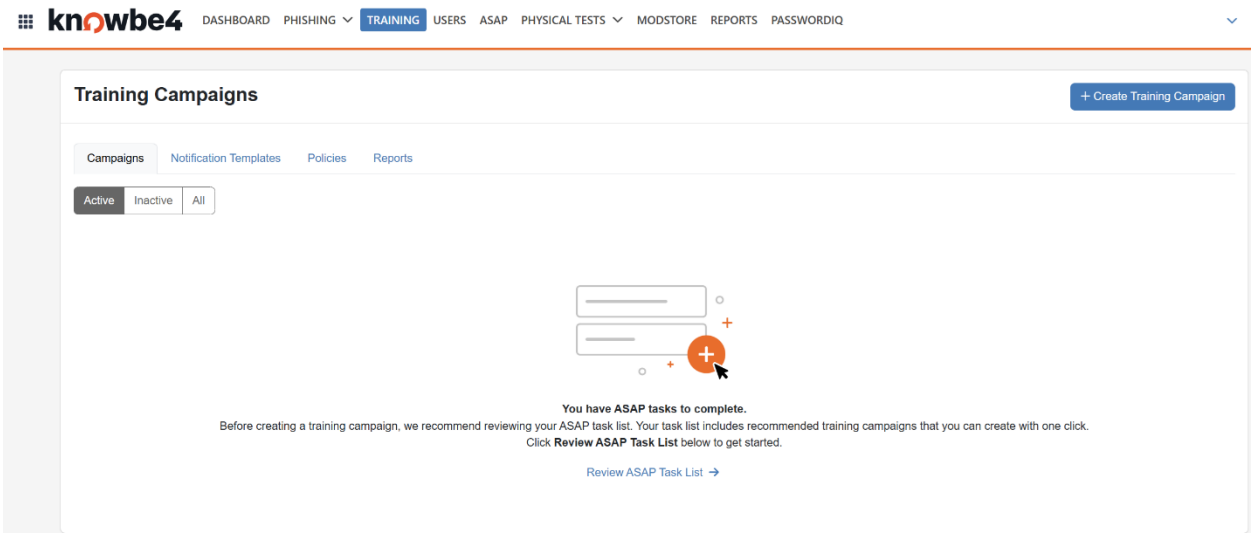
You will also see some additional subsections to the Modstore. Click Library to view all the training modules you have added from the Modstore. **Please note that modules need to be added to the library before they can be used in a training campaign.**



Additional Resource: ModStore and Library Guide – KnowBe4 Knowledge Base

Security Awareness Training

The “Training” tab is where you manage all activities related to security awareness training.



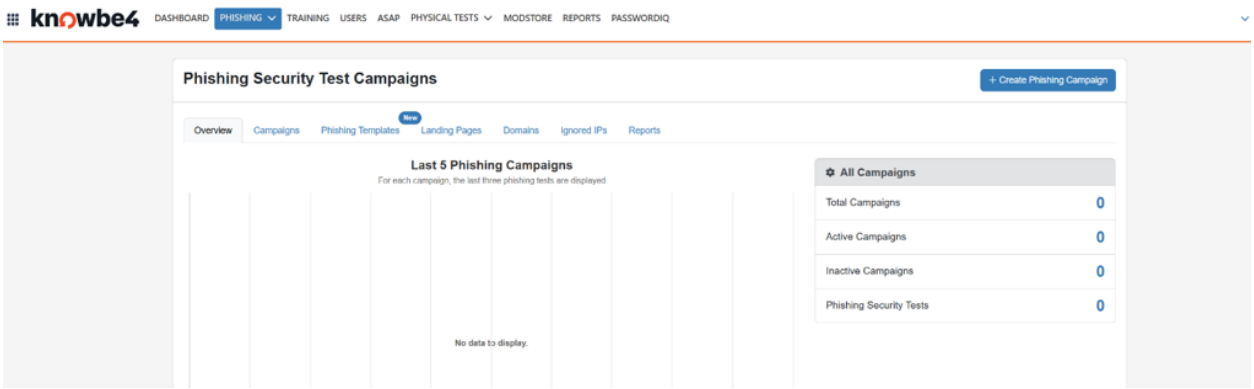
You will see a handful of subsections (the exact sections shown will depend on your console):

Campaigns	Create new training campaigns, manage active campaigns, and view inactive campaigns that have concluded.
Notification Templates	These notifications are emails that staff, managers, and administrators receive throughout a training campaign (like a welcome message when they're enrolled, a reminder before something's due, and a confirmation once it's complete). KnowBe4 provides built-in templates you can use.
Policies	If your organization uses policy acknowledgment, this is where policies are prepared and attached so they can be included as part of a training campaign.
Reports	Training-specific reports showing who has and hasn't completed the training you've assigned. This overlaps with the Reports section described later, but it's also accessible directly from the Training tab.

Simulated Phishing Testing

The “Phishing” tab is where you manage simulated phishing campaigns. Phishing campaigns are emails designed to look like real phishing attempts, sent to your staff to test and build their ability to recognize them.

When you click the Phishing tab, you land on the Overview subtab by default. This tab provides high-level information on the last 5 phishing campaigns, other stats on phishing campaigns for your organization, and a button to quickly create a new phishing campaign.

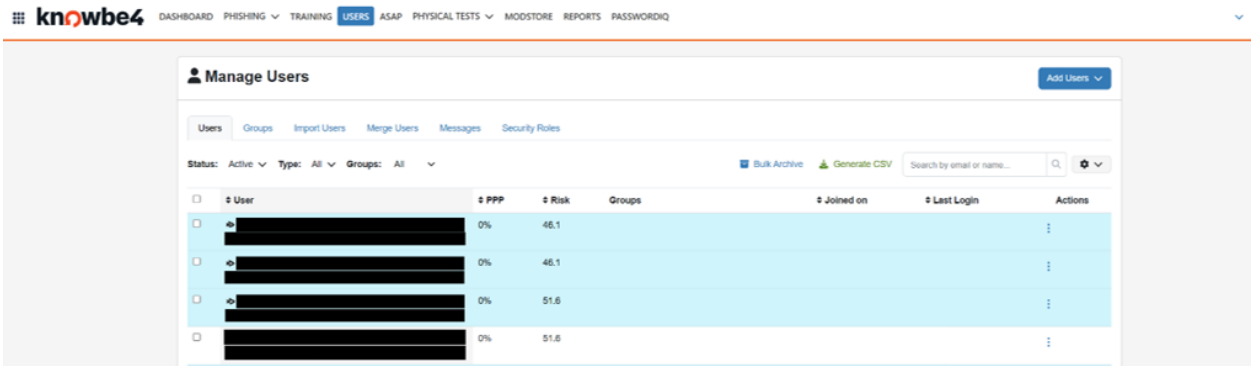


These are some of the other most frequently used subsections within the Phishing section:

Campaigns	The campaigns tab shows information relating to all phishing campaigns such as active campaigns, who was included in test, results from the test, and a button to create new phishing campaigns.
Phishing Templates	A phishing template is the email staff will see as part of simulated phishing campaigns. The phishing template tab provides all the available emails available to use for phishing campaigns.
Landing Pages	A landing page is the page that staff see after they fail a particular phishing campaign. The phishing landing pages tab provides all the available pages available to use for phishing campaigns.

User Management

The “Users” tab is where you manage everything related to your user list (staff). This is where KnowBe4 keeps track of who your training and phishing campaigns are sent to. You’ll want to keep this updated as staff in your organization changes over time.

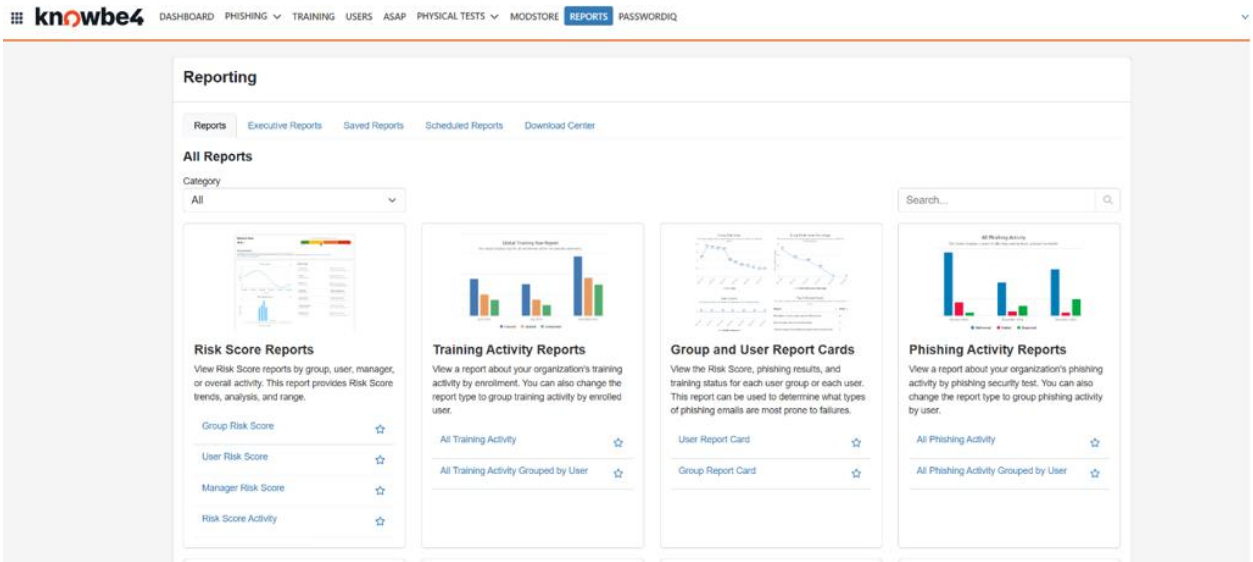


These are the other subsections within the Users tab:

Users	The Users tab allows you to see a list of everyone currently in your console along with their Phish-Prone Percentage (PPP) which represents how often they've failed phishing tests and Risk score.
Groups	The Groups tab allows you to see all the groups created within your console. This is where you create new groups.
Import Users	If you are manually uploading staff and not leveraging Active Directory (AD) or Google User Provisioning (GUP), you will use the Import Users tab to add new staff to the platform.
Merge Users	For combining two user profiles into one if someone accidentally ended up with duplicate accounts (for example, after an email change). This preserves their training and phishing history rather than losing it.
Messages	For sending messages directly to staff through the platform, such as a custom announcement. This is optional and separate from training or phishing campaign notifications.
Security Roles	For assigning different levels of console access to other staff (for example, a second administrator).

Reporting

The “Reports” tab is where you can gather metrics from training and phishing campaigns to create detailed reports. You don't need to review every report type every time – the Training Activity and Phishing Activity Reports will cover most of what you need.



These are the other subsections within the Reports tab:

Reports	The Reports tab is where metrics from phishing and training campaigns are collected. KnowBe4 has several report templates to choose from.
Scheduled Reports	If you want to set up a report to be generated and sent automatically on a recurring basis, such as every quarter, instead of running it manually each time.
Saved Reports	If you edit any of the Reports from the Reports tab you have the ability to save them for later. You can find them within the Saved Reports tab.
Download Center	All reports created within KnowBe4 can be downloaded, within the Download Center tab you can view all the reports generated within the last 90 days

Additional Resource: Reporting Guide – KnowBe4 Knowledge Base

Setting Up Campaigns & Reporting

This section walks you through how to set up training, testing, and remedial activities that you can distribute to your users (staff). Links to additional KnowBe4 resources are provided for detailed information on platform guidance.

Preparation

User Groups

A User Group is a collection of users which can be managed together for the purposes of training and testing.

Before any training or phishing is launched, we recommend reviewing the current groups, creating new groups, and verifying existing groups. You can manually create new groups, import groups from Active Directory (AD) or Google User Provisioning (GUP), and even leverage KnowBe4's smart groups for dynamically adding and removing staff to groups based on set criteria. Leveraging groups is especially useful for assigning a group of people training or phishing.

Refer to the following step-by-step instructions on how to configure users and groups as well as assign or remove administrative functions to users:

- Users and Groups Management Guide – KnowBe4 Knowledge Base
- Assign and Remove Admin Functions from a User – KnowBe4 Knowledge Base

Training Campaigns

Refer to the following step-by-step instructions on how to configure your training campaign:

- Video: Setting Up a Training Campaign | KnowBe4 Knowledge Base
- Training Campaigns Guide – KnowBe4 Knowledge Base

When selecting content to include in your training campaigns, the length of training and number of modules assigned is important to consider.

- If you are assigning training annually, we recommend assigning about **30** - **90** minutes' worth of security awareness training.
- If you are assigning training quarterly, we recommend assigning about **10** - **30** minutes' worth of security awareness training.

After you configure the campaign, you can leverage the campaign's cloning features to copy the configuration to a new campaign. This is especially helpful if you are creating quarterly training campaigns, or if you are creating a training campaign from a template. For instructions on how to clone a campaign refer to the following KnowBe4 guide: Clone a Phishing or Training Campaign – KnowBe4 Knowledge Base

Phishing Campaigns

Refer to the following step-by-step instructions on how to configure your phishing campaign and guides on the phishing templates and landing pages:

- Video: Creating Phishing Campaigns | KnowBe4 Knowledge Base
- Create and Manage Phishing Campaigns – KnowBe4 Knowledge Base
- Phishing Templates Advanced Features Guide – KnowBe4 Knowledge Base
- Create and Edit Email Templates and Landing Pages – KnowBe4 Knowledge Base

Phish Alert Button (PAB)

Before any phishing campaigns are launched, it is highly recommended to verify that KnowBe4's Phish Alert Button (PAB) is installed. Staff should be notified and educated about how to use the PAB. If staff don't use the PAB, you will not be able to collect accurate reporting metrics within the KnowBe4 platform.

For step-by-step instructions on sample emails to use for notifying staff, training campaign, and testing campaign refer to the following KnowBe4 article: Best Practices: Phish Alert Button (PAB) Implementation – KnowBe4 Knowledge Base

Selecting Phishing Emails and Landing Pages

One of the most important parts of the phishing campaigns is the phishing template and landing page. The phishing template is the simulated phishing email that staff will see. The landing page is what they will see after clicking links, entering credentials, downloading attachments, or otherwise failing the campaign. KnowBe4 offers hundreds of phishing email templates you can choose from.

For the phishing template, you have many options such as defining which types of email templates you want to use, the difficulty of said emails, and if you want each user to receive the same email, or if everyone should receive different emails. All these settings can have an impact on the overall difficulty of a campaign.

If you are just starting out, we recommend starting with 1- or 2-star difficulty phishing templates before moving onto higher difficulty templates. This way the phishing simulates scale in difficulty with your organization's security awareness. To learn more about KnowBe4's template difficulty rating, reference the following: Template Difficulty Ratings Overview – KnowBe4 Knowledge Base

Remedial Training and Testing Campaigns

Refer to the following step-by-step instructions on how to configure a smart group for automatic enrollment as well as a step-by-step guide on configuring a remedial training campaign:

- Smart Groups Training Automation Guide – KnowBe4 Knowledge Base
- Create a Remedial Training Campaign – KnowBe4 Knowledge Base
- Video: Remedial Training Campaigns | KnowBe4 Knowledge Base

Remedial activities include providing additional security awareness activities for staff members who fail simulated phishing tests. Remedial training means assigning additional training modules to staff who fail a phishing campaign. Remedial testing means enrolling staff who fail in another phishing campaign. The goal of remedial testing is to provide staff with more opportunities to spot and report phishing attempts. Based on your organization, you may decide if you want staff to receive additional training and/or testing.

If decide to conduct remedial training or testing, you will want to ensure you track staff who failed the previous phishing campaign. This can be done by making a separate smart group automatically populate based when staff fail a phishing campaign. Or this can be done when you configure the phishing campaign, make sure to leverage the option to “Add Clickers to” a group.

Once the groups have been prepared, you can configure the remedial activities. If you are conducting remedial testing, it is highly recommended to conduct remedial training before testing. This way staff are provided with more training opportunities on safe habits before being tested again.

When creating remedial training and testing campaigns we recommend the following:

- Assign remedial training immediately following a failure, or shortly after a phishing campaign ends. This way staff are provided with information on security best practices within a timely manner.
- Assign remedial testing within roughly two weeks following remedial training activities. This way staff have time to absorb material from training and reflect before receiving the next test.

Reporting

The table below provides KnowBe4 resources and guidance for you to leverage when choosing and creating your own reports. We recommend creating a report after running a campaign to gain insight into your security awareness program's health and progress.

Below we have identified the most valuable KnowBe4 resources for guidance and setup on Reports, recommending you leverage **Executive Reports**, **Training Activity Reports**, and **Phishing Activity Reports**.

General Reporting Guidance	Reporting Guide – KnowBe4 Knowledge Base Save and Send Reports – KnowBe4 Knowledge Base
Executive Reports	Video: Executive Reports Overview – KnowBe4 Knowledge Base
Training Activity Reports	Customize and View Training Activity Reports – KnowBe4 Knowledge Base
Phishing Activity Reports	Customize and View Phishing Activity Reports – KnowBe4 Knowledge Base

To access guidance on all reports, please reference the Using Reports – KnowBe4 Knowledge Base.

Running a Security Awareness Program

This section covers general best practices for running an effective security awareness program, drawn from established cybersecurity guidance (NIST Special Publication 800-50) and KnowBe4's own recommendations. These aren't strict rules but following them will help your program change behavior over time, rather than just checking a box.

***Participation in this program requires conducting at least one security awareness training campaign annually!**

Determine Your Goals

When thinking about running a security awareness program, you will want to think about what your end goals are so you can be better prepared when engaging stakeholders and your staff. Below are some questions you may want to think about when planning your organization's security awareness program.

- Are there any compliance requirements my organization is required to follow?
- What is the best way to engage staff in a new initiative?
- What does a successful security awareness program look like for my organization?

You will also want to consider what type of activities you want to include as part of your Security Awareness program. While we recommend incorporating all activities defined below, you should consider which activities will be the most beneficial to your organization.

***Security Awareness Training**	Staff receive assigned KnowBe4 training modules covering security best practices, current threats, and emerging technology. Training is distributed through the KnowBe4 platform.
Simulated Phishing Testing	Staff are sent emails that look malicious from the KnowBe4 platform. The goal of these tests is to test effectiveness of training and staff's ability to report phishing attempts within a safe environment.
Remedial Training and Testing	Only staff who fail phishing campaigns receive remedial testing and training. The goal is to ensure that staff who may be more vulnerable to phishing attacks are provided with more training and opportunities to reinforce safe cyber habits.
Security Newsletters	Quarterly cybersecurity newsletters are published to the SLCGP website. Your organization's administrator will receive notification of newly published newsletters and is responsible for relaying that notification to their staff.

Set a Schedule

Security awareness isn't something you set up once and finish. It works best as a repeating cycle: deliver training and testing, see how staff respond, adjust based on what you learn (reports), and repeating. We recommend building a regular rhythm into your calendar rather than treating a single round of training as the finish line. Below are the three most common times to implement security awareness training. We recommend running activities both upon hire and quarterly/semi-annually. If this is not feasible, an annual schedule is sufficient for minimum program requirements.

Upon Hire (**recommended**):

1. Security Awareness Training
2. Security Policy Review (if your organization has security policies, we recommend utilizing the Policy feature in KnowBe4's Training tab to have new employees review and acknowledge them)

Quarterly or Semi-Annually (**recommended**):

1. Security Awareness Training
2. Simulated Phishing Test
3. Remedial Training
4. Remedial Testing

*Annually (**at a minimum**):

1. Security Awareness Training
2. Simulated Phishing Test
3. Remedial Training
4. Remedial Testing

As you plan, keep in mind that you must provide phishing tests in order to conduct remedial testing and remedial training! This is because remedial activities are triggered by a user (staff member) failing the original phishing test. The intent of remedial activities is to provide additional learning opportunities and reinforce safe behavior.

Engage Your Users (Staff)

You and your staff are the most important part of the program! Training and testing can only be effective if the people receiving it are aware and engaged. Below are some recommendations on what to communicate with your staff, especially if security awareness is new(er) to your organization. A separate guide for staff explaining the program and its offerings is currently in development and will be uploaded to the SLCGP website upon completion. Configuration Guide

- Let staff know that security training is a regular part of your organization's security program. You can tell them when training occurs.

- If you are participating in phishing, let staff and IT know that phishing testing is a regular part of your organization's security program without revealing when a specific test will happen.
- Phishing tests should never be used to penalize or call out individual staff members. Results are there to show where more training is needed, not to punish anyone who clicks. Assuring your staff of this ahead of time is often beneficial.
- Staff should understand the Phish Alert Button and know that reporting a suspicious email, whether it turns out to be real or a simulated test, is always the right move. If staff do not use the Phish Alert Button, KnowBe4 cannot know if the user actually reported the simulated phishing email.
- Let staff know who your organization's administrator is (or whoever they can reach out to if they have issues with training or testing activities).
- **Please do not direct staff to nuHarbor's support team**. The support team is available to administrators.

Notifying IT

Before running a phishing campaign, you may want to notify additional personnel of the upcoming phishing test. If you are planning organization-wide campaigns, you may want to notify IT staff in case concerned staff reach out to IT. You should notify the minimum number of staff prior to a test to preserve the integrity of the phishing test.

For any IT personnel who are notified prior you may consider providing the following details:

- **Scheduled test date**: Provide information on when the test is launched and how long the test campaign will be open.
- **Responding to questions or inquiries**: Provide instructions on how IT staff should respond. Should IT tell users that the email is just a test? If you are sending a test to a large group or everyone, we recommend the following:
    - Thank the individual for reaching out to IT.
    - Disclose that the email was a test and not a real attack.
    - Encourage and promote usage of the PAB.
    - Asking the individual not to share the email is a simulated test to others.

Select Content

Choose training content based on what's actually relevant to your organization's risk exposure and staff roles, rather than trying to cover everything in KnowBe4's library at once. A smaller, focused set of modules that staff can genuinely absorb is more effective than a long list that dilutes attention. If certain staff have elevated access or responsibilities (finance, IT, HR), consider whether they need additional or more targeted content beyond what the general staff population receives.

KnowBe4 updates its Modstore regularly. We recommend reviewing the content at least annually to ensure the training provided is still relevant and up to date. Incorporating new content with each campaign helps mature your security awareness program by training your staff on a wider variety of cybersecurity topics.

Here are some topics highly relevant to schools and municipalities that we recommend providing training on:

Artificial Intelligence (AI) scams	This is a fast-growing category. AI tools make scams more convincing, more personalized, and harder to spot (realistic voice cloning, AI-generated emails that mimic a real coworker's writing style, or deepfake video/audio used in a scam call).
Business email compromise	Municipalities and school districts regularly process vendor payments, payroll, and reimbursements, which makes finance and administrative staff a common target for scams asking someone to urgently change a bank account or approve an unusual payment.
Handling sensitive data	Schools handle protected student data (subject to FERPA) and municipalities handle resident records, tax information, and sometimes law enforcement or court-related data. Staff should understand what counts as sensitive information and how it should (and shouldn't) be shared.
Passwords and multi-factor authentication (MFA)	Weak or reused passwords are one of the easiest ways an attacker gets into an account, and MFA acts as a second lock on the door even if a password is stolen. This matters especially in smaller organizations without dedicated IT oversight, where staff are more likely to reuse the same password across personal and work accounts.
Safe web browsing	Fake websites are a common way attackers steal login credentials or install malware, often reached through a malicious link in an email or in a search engine result. Staff should know how to spot the signs of an unsafe site before entering any information or downloading a file.

Run a Practice Campaign

Before you run your first phishing and training campaigns, it is recommended to do a quick test run with yourself and other trusted personnel. For training campaigns, it is most important to verify that all emails from KnowBe4 are being received. For phishing campaigns, it is important to verify that the platform is capturing "failures" accurately, ensure that the PAB is functioning, and confirm that KnowBe4 is properly pulling metrics. Once everything has been verified, you can confidently start sending training and phishing to your staff.

To ensure any practice phishing tests don't negatively impact any metrics, make sure to hide campaigns from Reports. Refer to this guide on how to hide results: Hide a Phishing Campaign from Reports – KnowBe4 Knowledge Base

Train Before You Test

Deliver training on a topic before you test staff on it, not the other way around. Running a phishing simulation before staff have been taught what to look for tells you where they're starting from, but it doesn't teach them anything. Lead with training, then reinforce it with testing.

Reporting Best Practices

Regular reporting is essential to measuring the effectiveness of your security awareness program and identifying opportunities for continuous improvement. We recommend creating and analyzing a report after running each campaign. When running Training and Phishing Campaigns, the three KnowBe4 reports you will typically get the most insight into your program's effectiveness from are Executive Reports, Training Activity Reports, and Phishing Activity Reports. Regularly creating and reviewing these reports will help you understand user engagement, measure program performance, identify areas of elevated risk, and demonstrate the value of the security awareness program to leadership.

Regularly running reports provide valuable insight into how users interact with training and phishing campaigns, helping administrators identify trends, measure effectiveness, and better understand areas of user risk. Regularly reviewing report data can help determine which topics resonate with users, where additional awareness is needed, and how the program is performing over time.

We recommend using these insights to make informed adjustments to your security awareness program rather than taking a one-size-fits-all approach. Training results, phishing outcomes, and user engagement metrics can help guide future campaign planning, training assignments, and awareness communications, further aligning your security awareness program with your organization's needs and expectations.

Recommended Reports

Executive Reports: We recommend leveraging these for high-level insight into your console, user engagement, and program development. These reports give insight into important areas such as Training completion rates and overdue assignments, phishing campaign participation, phish-prone percentage trends, user engagement, and security awareness maturity over time.

Training Activity Reports: These are critical for evaluating the effectiveness of your training campaigns and monitoring user engagement and performance over time. From these reports, you can identify security awareness program enhancement opportunities by seeing what works best for your users. When reviewing training reports, pay particular attention to training completion rates, overdue or incomplete training assignments, training content with high completion rates and positive engagement, and training content struggling for engagement.

Phishing Activity Reports: Running these are recommended to evaluate phishing campaign effectiveness, monitor user susceptibility to phishing attacks, and identify gaps in security awareness from testing results and user behavior over time. These reports can help you determine which security topics or individual users require more training, allowing you to tailor future training or phishing to target those areas. When reviewing phishing reports, key areas to monitor include repeat clickers or repeat phishing failures, users who consistently report simulated phishing emails, user or user group performance trends, and performance against phishing campaigns covering specific security topics.

Appendix A: Training Campaign Checklist

This encompasses the major steps necessary to create either a standard training or remedial training campaign:

☐ Confirm the training content you want is already in your Library (Modstore)
☐ Name the campaign
☐ Set a start date
☐ Set an end date
☐ Select the content to include
☐ Choose who's enrolled (all staff, or a specific group)
☐ Decide whether staff can complete it after the due date
☐ Set up at least a welcome notification and a reminder before the due date
☐ Launch the campaign

Appendix B: Phishing Campaign Checklist

This encompasses the major steps necessary to create a standard simulated phishing or remedial phishing campaign:

☐ Name the campaign
☐ Choose who receives it (all staff, or a specific group)
☐ Choose a difficulty level
☐ Choose a template or templates
☐ Set when the test should go out (set date, weekly, bi-weekly, monthly, etc.)
☐ Set when the emails are delivered (all at once, or over several days)
☐ (if conducting remedial activities after) verify Smart Group has been configured to add users who fail campaign OR leverage “add Clickers to group” option within the phishing campaign wizard.
☐ Launch the campaign

Change Control

Version No.	Date	Description of Changes	Owner
1.0	09/08/2026	Document Created	nuHarbor