
KNOWBE4: SECURITY AWARENESS

PROGRAM INFORMATION FOR STAFF

Thank you for participating in security awareness training provided by the State of Maine's State and Local Cybersecurity Grant Program (SLCGP)!

Counties, towns, and schools have become frequent targets for cyberattacks because these organizations hold valuable data (like payroll or student information) and often rely on smaller IT teams. The uncomfortable truth is that most breaches don't start with a broken firewall; they start with a person. Someone clicks a fake invoice, replies to a spoofed vendor email, or types a password into a convincing fake login page. It happens to smart, careful people every day, simply because the tricks are designed to feel routine.

That's why this program exists. We use the KnowBe4 platform to provide you with security awareness training and phishing activities. Our goal is to equip staff with the knowledge and confidence to help prevent, recognize, and report cybersecurity threats. The purpose of this guide is to explain what you can expect from the program and how to interact with some crucial KnowBe4 features.

Need Help?

Your organization's Program Contact and Technical Support individual/s are defined in the email you received which provided this guide. Please familiarize yourself with these individuals and reach out to them respectively with any questions.

Program Activities

Your Program Contact determines which of the following activities its staff will receive and how frequently the activities are run. You may only receive some of the activities described below, and the activities you receive may change over time. For any questions regarding the program and what you need to do that are not addressed below, please reach out to your Program Contact.

By participating in program activities, you are helping yourself and your organization by becoming more cyber-safe. **Thank you for doing your part to protect yourself and your organization from cybersecurity threats!**

Below is a breakdown of the program activities that you may be receiving. The activities you will be receiving should be identified in the email, however you can always confirm with your Program Contact.

Security Awareness Program Newsletters

What is this?

Security Newsletters are brief one-pager resources with practical security tips to help everyone stay cyber-safe. Each issue focuses on a new topic and highlights what to look out for and what you can do to protect yourself, your organization, and sensitive information.

How will I receive it?

Newsletters are published quarterly to the SLCGP Website for anyone to view. Your organization's point of contact will receive an email from securitytraining@nuharborsecurity.com that provides a link to the newly published Newsletter, which they may forward to you or provide the link separately. You can also directly access each new Newsletter on the SLCGP Website under the [KnowBe4: Security Awareness](#) subpage.

What should I do with it?

Take a few minutes to read the Newsletter and learn about the topic. Review the main tips and find ways to incorporate smart cybersecurity practices into your daily life. Maybe you read the Newsletter and are curious to learn more; do your own research or make use of the "Additional Resources" section. A great way of raising security awareness is to have a conversation with your colleagues and discuss what you learned and what you already knew. There may be topics that you or someone you know has personally experienced.

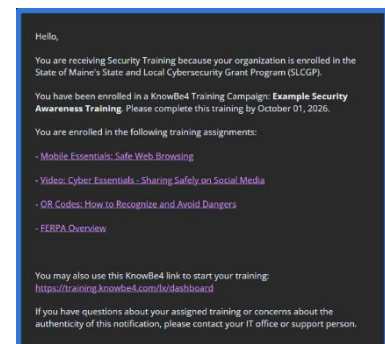
Security Awareness Training

What is this?

Security Awareness Training consists of training modules that will help you learn how to recognize common cyber risks. Training modules are essential for raising security awareness and can cover essential topics like spotting a phishing email or how to safely browse the web.

How will I receive it?

When new training is assigned, you will receive an automated email from the KnowBe4 platform notifying you that new training is assigned. A notification email may resemble the image to the right.



What should I do with it?

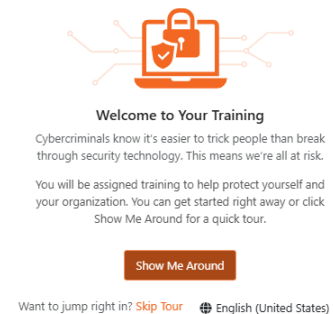
If this is the first time you are assigned training, you will first need to activate your account. For more information about activating your account, refer to the following KnowBe4 article: [Learner Support: Quickstart Guide – KnowBe4 Knowledge Base](#)

Once you activate your account, you can now start your training! Once you log in, you will be greeted by your **Dashboard** where you can see your assigned training.

When you navigate to the **Training** tab, you will see a popup (see the image to the right) encouraging you to take a tour of the platform. If this is the first time logging in, we recommend you take a tour to familiarize yourself with the platform.

What if I need help?

If you have any questions about assigned training, reach out to your Program Contact. For more information on navigating the Learner Platform, refer to the following KnowBe4 article: [Learner Support: Navigating the Learner Experience \(LX\) – KnowBe4 Knowledge Base](#).



If you receive Simulated Phishing Tests

What is this?

Phishing is a common cyberattack where an attacker tries to trick you into things like clicking a malicious link, downloading an infected attachment, or handing over sensitive information like passwords and other sign-in information. The *Simulated* Phishing Tests sent through this program are realistic but entirely harmless, fake scam emails designed to look like a real phishing attempt but are sent through the KnowBe4 platform. The goal is to give you a safe way to practice spotting and reporting these attempts before a real attacker sends you one.

How will I receive it?

Simulating phishing emails arrive in your normal email inbox without warning, just like a real attempt would. You likely will not know ahead of time when a test is coming.

What should I do with it?

If you spot a suspicious email, report it using KnowBe4's Phish Alert Button (PAB). The PAB can look like the image to the right but may change depending on your email platform. Reporting a suspicious email is always the right move, whether it turns out to be real threat or simulated.



If you end up accidentally falling for a simulated test, don't worry! The KnowBe4 simulated phishing emails will lead you to a safe landing page. If your organization chooses to participate in Remedial Training and Remedial Testing, you may also receive one more short training module and/or a second phishing test.

If you are set to receive Remedial Training & Tests

After clicking on a fake phishing link, you may receive another round of training and testing. The purpose of remedial activities is not to punish you for making a mistake and clicking on a malicious link. The goal is to further improve recognizability around what real phishing attacks could look like and get realistic practice in.

If you have questions about a phishing test or aren't sure whether an email is simulated or real, contact your organization's Technical Support individual.