WEBROOT®

by opentext™

Security Awareness Training

Admin Guide

Table of Contents

Chapter 1: Security Awareness Training Admin Guide **1**

Security Awareness Training Overview 2
Enabling Sites for Security Awareness Training 3
Enabling for Existing Sites 4
Enabling for New Sites 5

Chapter 2: Creating and Launching Phishing Simulations **6**

Creating And Launching Phishing Simulations Overview 7
Creating Phishing Simulations 8
Designing Phishing Emails 22
Designing Phishing Sites 29
Designing Education Pages 36
Creating Training Modules 37
Creating Templates and Infographics 43
Designing Lure Pages 53
Designing Broken Link Pages 57
Reviewing and Sending Phishing Simulations 60
Selecting Sites in the Dashboard 64

Chapter 3: Creating Training Sessions **66**

Creating Training Campaigns Overview 67
Selecting Trainees 68
Designing Invitation Emails 75
Designing Education Pages 78

Chapter 4: Working With Programs and Campaign Scheduling **84**

Programs And Campaign Scheduling Overview 85
Sending Welcome Emails 86
Scheduling Phishing Campaigns 98
Creating Training Campaigns 105
Sending Campaign Summary Reports 111
Understanding Email Types 112

Chapter 5: Working With Reports **113**

Accessing Delivery Reports 114
Accessing Training Reports 126

Understanding Report Results 134
Accessing Security Awareness Training Reports 138
Accessing Breach Reports 143
About Phishing Simulation Reports 149
Sample Phishing Report Campaign Summary 149
Understanding Email Events 150
Sample PDF Summary Report 153
Chapter 6: Managing Spam Filters 156
Allowing Emails In Proofpoint Essentials 157
Allowing Email In Microsoft Exchange and Microsoft 365 158
Allowing Emails In Google Workspace 172
Allowing Webroot Training Email Servers 173
Chapter 7: Working With Settings 174
Verifying Domains 175
Importing Targets 179
Integrating with Microsoft Azure Active Directory 188
Microsoft Azure Active Directory Frequently Asked Questions 197
Chapter 8: Security Awareness Training Technical Support 198
Accessing Technical Support 199
Leaving Feedback 201
Index i

Notices

Security Awareness Training Admin Guide revision Monday, July 29, 2024.

Information in this document is for the following product:

- Security Awareness Training

One or more patents may cover this product. For more information, please visit https://www.opentext.com/patents.

Chapter 1: Security Awareness Training Admin Guide

To use the Security Awareness Training Admin Guide, see the following topic:

Security Awareness Training Overview **2**
Enabling Sites for Security Awareness Training **3**
Enabling for Existing Sites **4**
Enabling for New Sites **5**

Security Awareness Training Overview

This admin guide is intended to help administrators understand how to manage the Webroot Security Awareness Training (SAT) platform, along with the features and functionality available within the platform.

Webroot Security Awareness Training (SAT) is a hosted platform integrated with Webroot Global Site Manager (GSM) that includes a fully featured phishing simulator along with training courses pre-loaded onto our integrated Learning Management System (LMS). Both the phishing simulator and training courses are managed through campaigns.

A campaign is a single phishing simulation or training course sent to a select group of users that provides the basis for reporting and managing Security Awareness Training.

As our client, you will be able to build phishing simulations through our easy to use Simulation Wizard. Using the wizard, you will be able to:

- Import your company’s email target list.
- Add your bait email and lure page by choosing from our pre-canned templates, or writing your own content.
- Send test emails to test the simulation.
- Schedule and launch your simulation against your targets.
- See reports in real-time:
  - Email processing and delivery.
  - Email opens and clicks.
  - Data post attempts to the lure page.

Enabling Sites for Security Awareness Training

To enable Webroot Security Awareness Training within the web console, you can do either of the following:

- Enabling for Existing Sites on page 4
- Enabling for New Sites on page 5

Enabling for Existing Sites

The process for enabling Security Awareness Training is different depending on your console view.

Business view:

1. Go to the **Security Awareness Training** tab and then the **Settings** tab..
2. Enable the setting **Enable Security Awareness Training**.
3. Select your keycode type.

   Full—This option is the full product with no limitations. You will be billed for this service.

   Trial—This option is the full product, however, it is limited to a free, 30-day trial.

4. Click **Save Changes**.

Service provider view:

1. Click **Sites List**.
2. For the site that you want to enable Security Awareness Training, click one of the following buttons in the **Security Awareness Training** column.

   Start Trial—This button starts a free, 30-day trial.

   Upgrade—This button converts a trial to a full version. You will be billed for this service.

3. Select your keycode type.

   Full—This option is the full product with no limitations. You will be billed for this service.

   Trial—This option is the full product, however, it is limited to a free, 30-day trial.

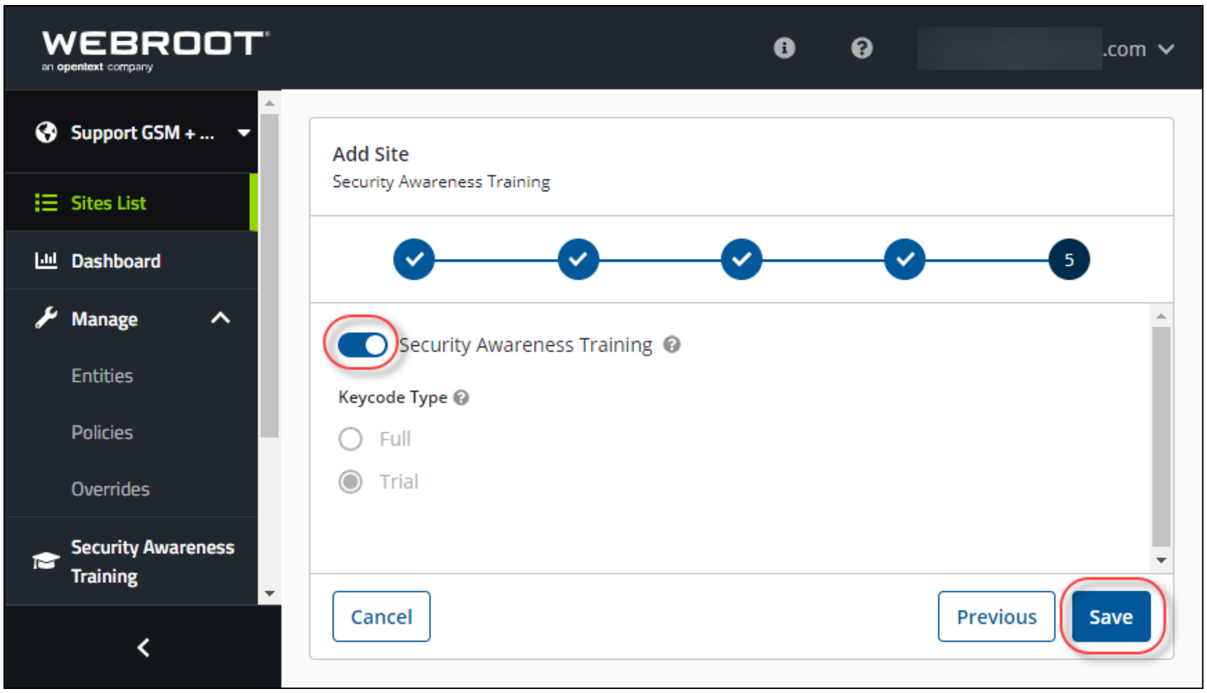
4. Click **Save Changes**.

Enabling for New Sites

Use the following procedure to enable Security Awareness Training for a new site.

To enable for a new site:

1. Select the toggle to enable **Security Awareness Training** on the final step of new site creation.



For more information on creating Sites, see the [Business Products Administration Guide]().

2. Click **Save**.

Chapter 2: Creating and Launching Phishing Simulations

To create and launch phishing simulations, see the following topics:

Creating And Launching Phishing Simulations Overview **7**
Creating Phishing Simulations **8**
Designing Phishing Emails **22**
Designing Phishing Sites **29**
Designing Education Pages **36**
Creating Training Modules **37**
Creating Templates and Infographics **43**
Designing Lure Pages **53**
Designing Broken Link Pages **57**
Reviewing and Sending Phishing Simulations **60**
Selecting Sites in the Dashboard **64**

Creating And Launching Phishing Simulations Overview

By default, phishing simulations are only available to launch against your authorized domains. You will not be able to target email addresses outside of your authorized domains list. These types of tests are generally ran by your company IT or security team. More information on managing domains and importing users is found below and a step-by-step available within the Security Awareness Training Getting Started Guide.

Before running any simulations against your organization, you should consult with your company's IT and/or security team to alert them of the tests, and maximize the success of your simulation. If you are a security consultant, you can contact us to become a verified security consultant to launch campaigns for your clients.

> **Note:** Email addresses on ISP or public domains (for example @gmail.com, @yahoo.com, etc.) are restricted and cannot be used within the Securecast service. Target email addresses must be valid company or organization addresses.

There are three steps to creating and launching a phishing simulation:

- Creating Phishing Simulations on page 8
- Designing Phishing Emails on page 22
- Designing Phishing Sites on page 29

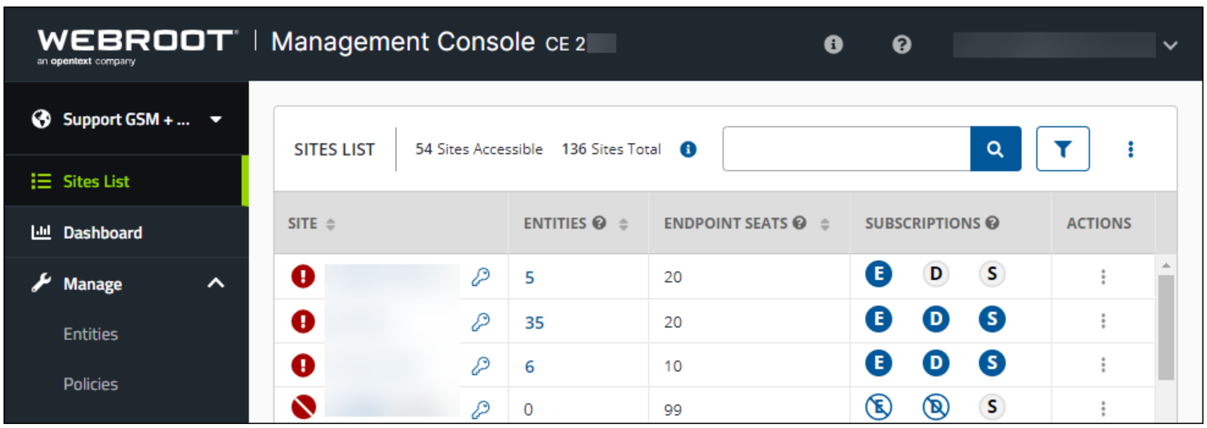
Creating Phishing Simulations

Follow this procedure to create a phishing simulation.

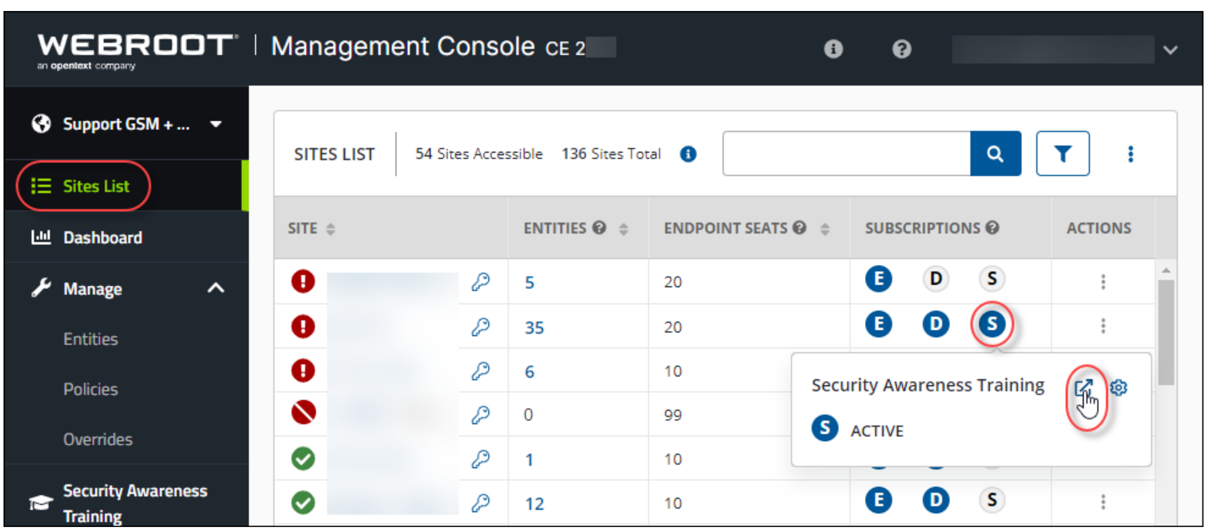
To create a phishing simulation:

1. Log in to the Management Console.

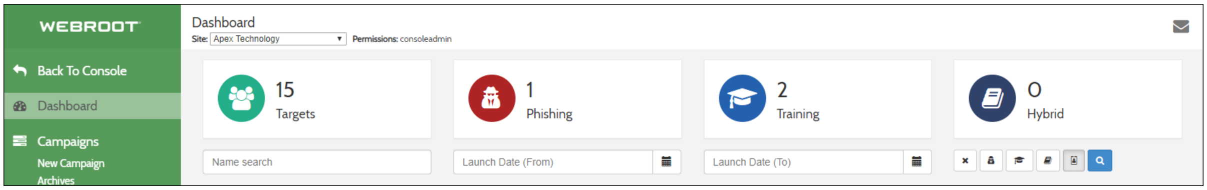
   The Management Console displays.



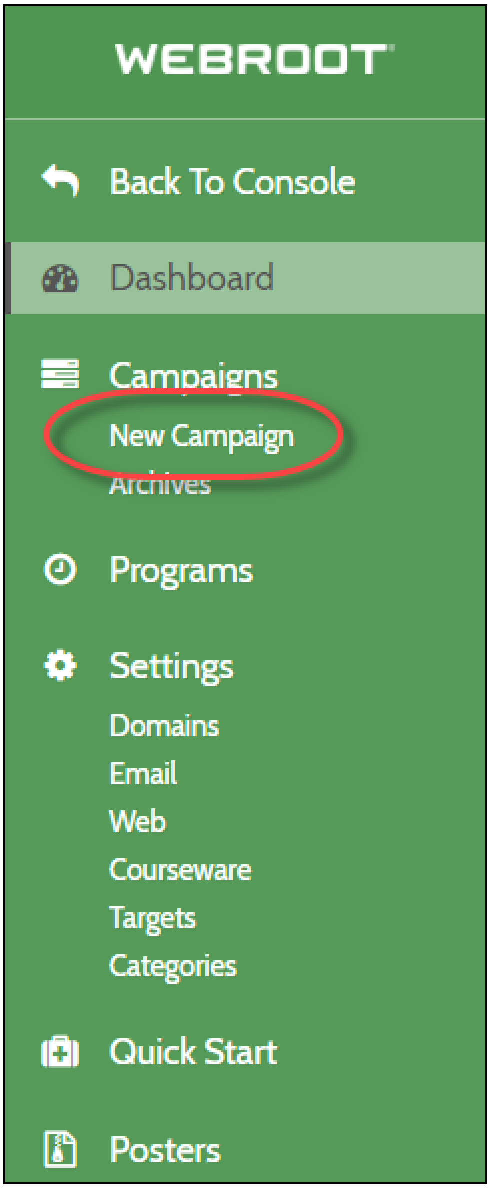
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



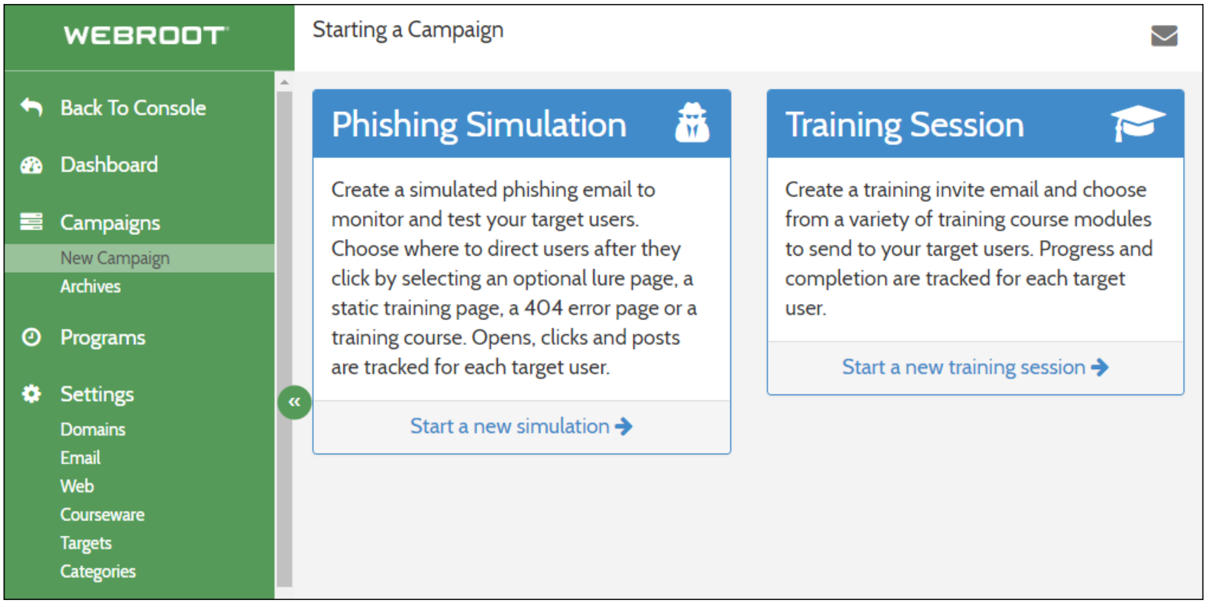
The Security Awareness Training console displays.



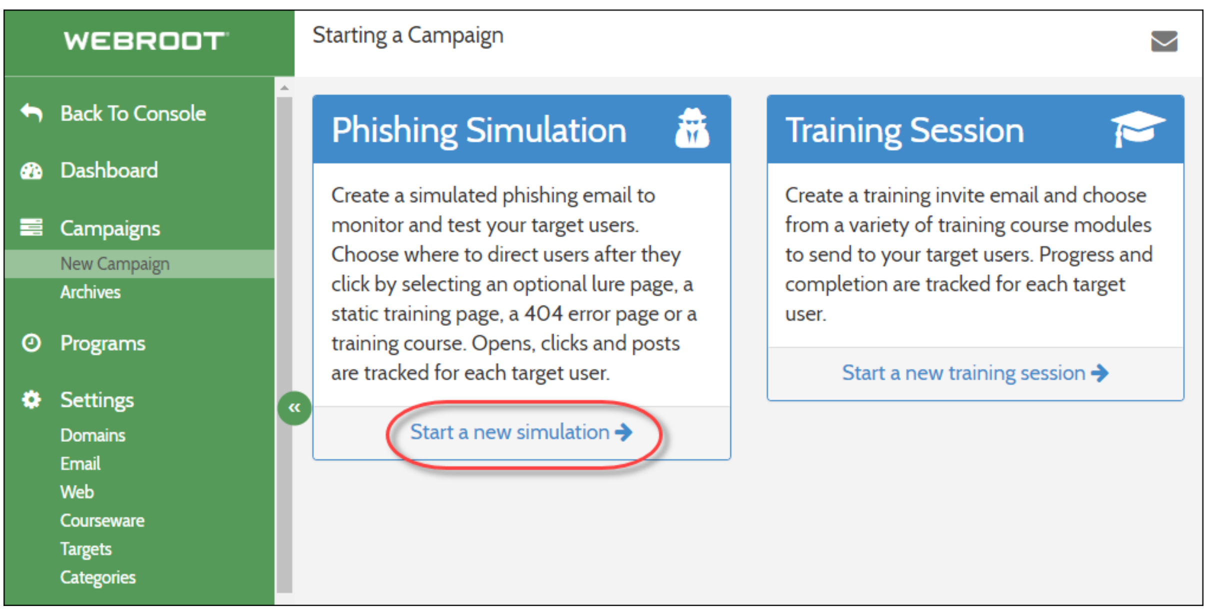
3. In the Nav bar, click the **New Campaign** icon.



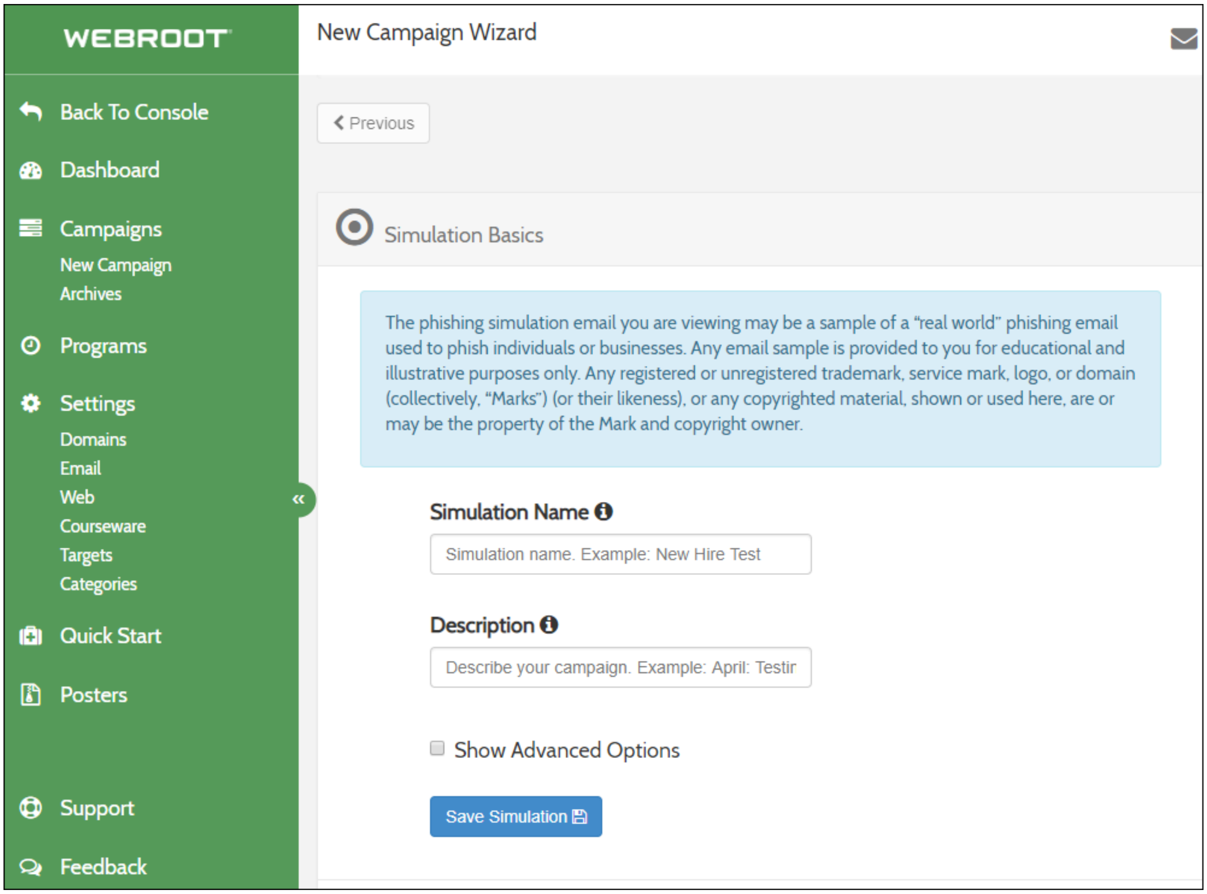
The Starting a Campaign panel displays.



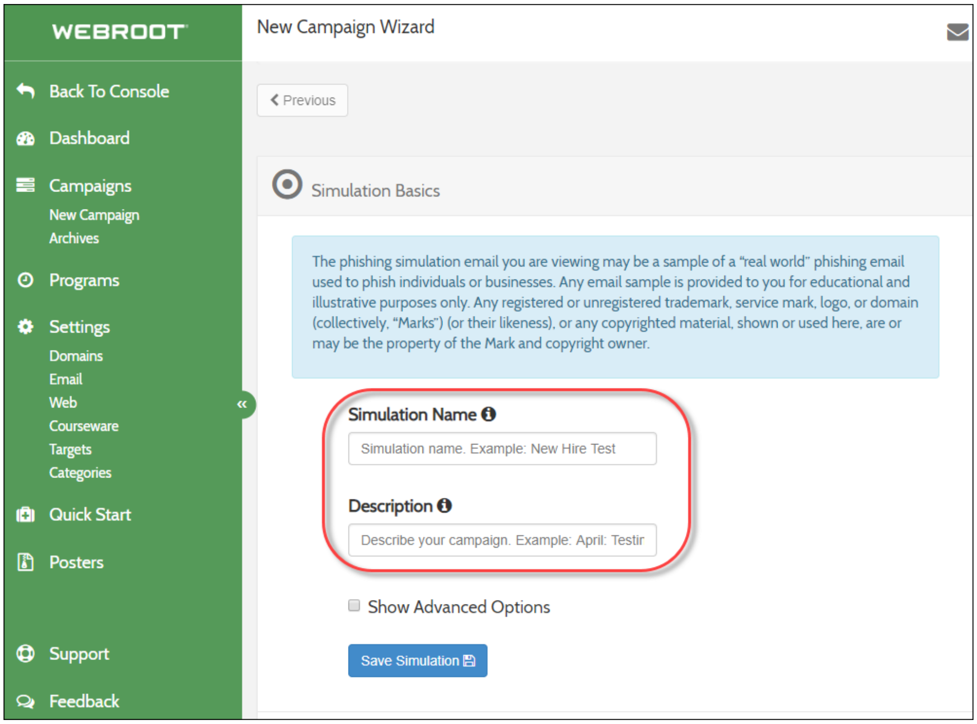
4. Click the **Start a new simulation** link.



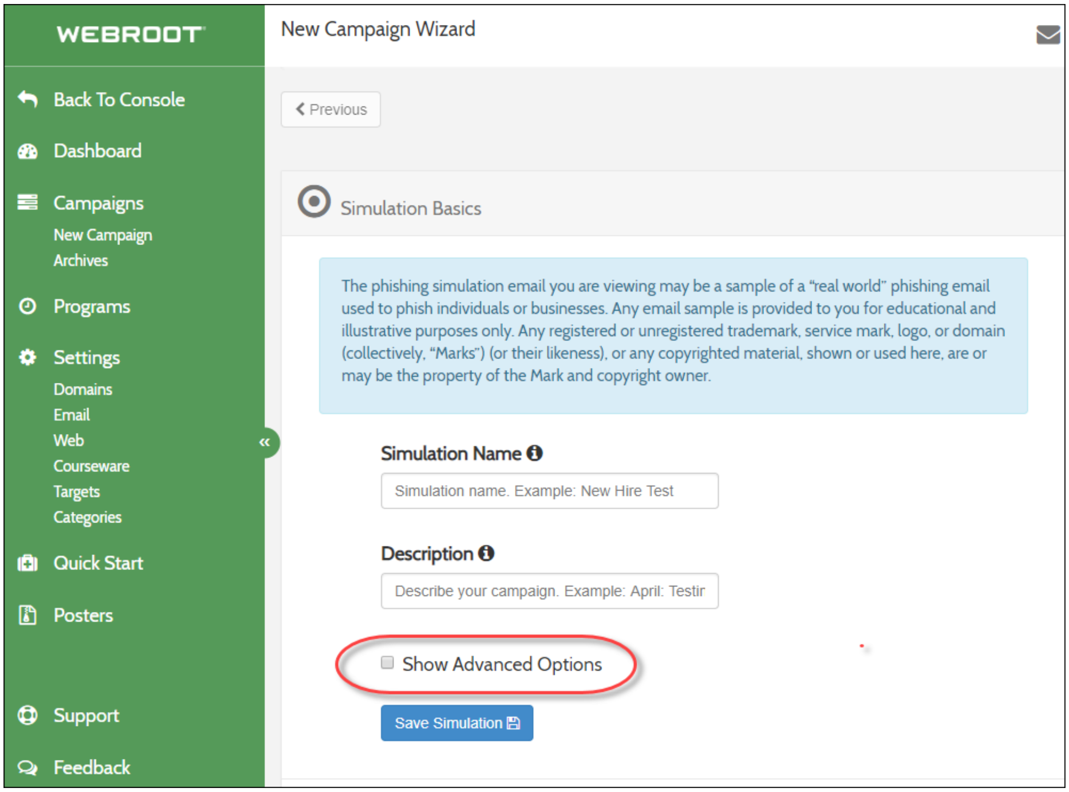
The New Campaign Wizard panel displays.


WEBROOT
New Campaign Wizard
Back To Console
Dashboard
Campaigns
New Campaign
Archives
Programs
Settings
Domains
Email
Web
Courseware
Targets
Categories
Quick Start
Posters
Support
Feedback
Previous
Simulation Basics
The phishing simulation email you are viewing may be a sample of a "real world" phishing email used to phish individuals or businesses. Any email sample is provided to you for educational and illustrative purposes only. Any registered or unregistered trademark, service mark, logo, or domain (collectively, "Marks") (or their likeness), or any copyrighted material, shown or used here, are or may be the property of the Mark and copyright owner.
Simulation Name
Simulation name. Example: New Hire Test
Description
Describe your campaign. Example: April: Testir
Show Advanced Options
Save Simulation

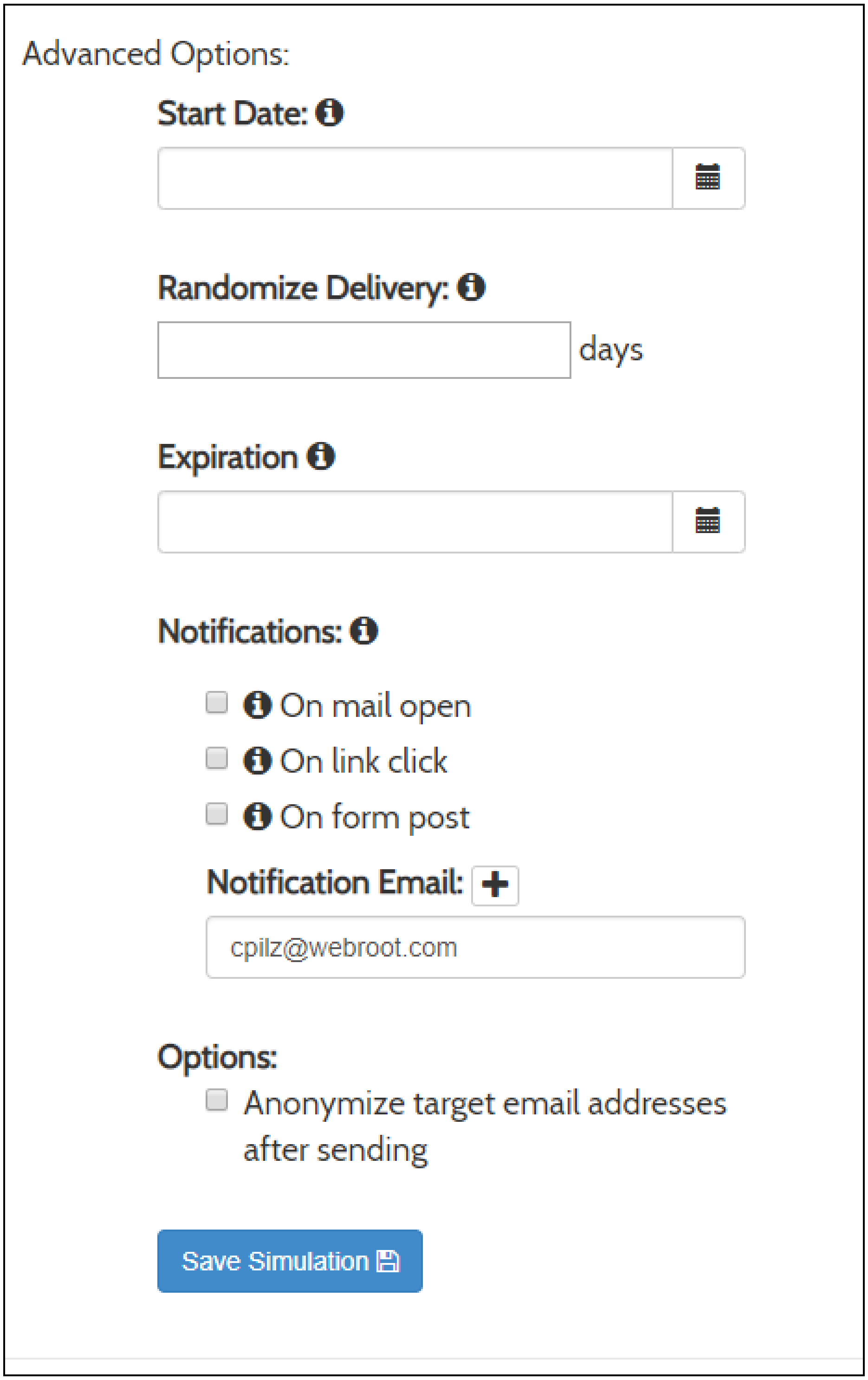
5. In the Simulation Basics area, populate the following fields:
   - **Simulation Name** — Enter a name for your simulation.
   - **Description** — Enter a description for your simulation. This is an optional step.



6. As needed, select the **Show Advanced Options** checkbox to display the advanced options area.



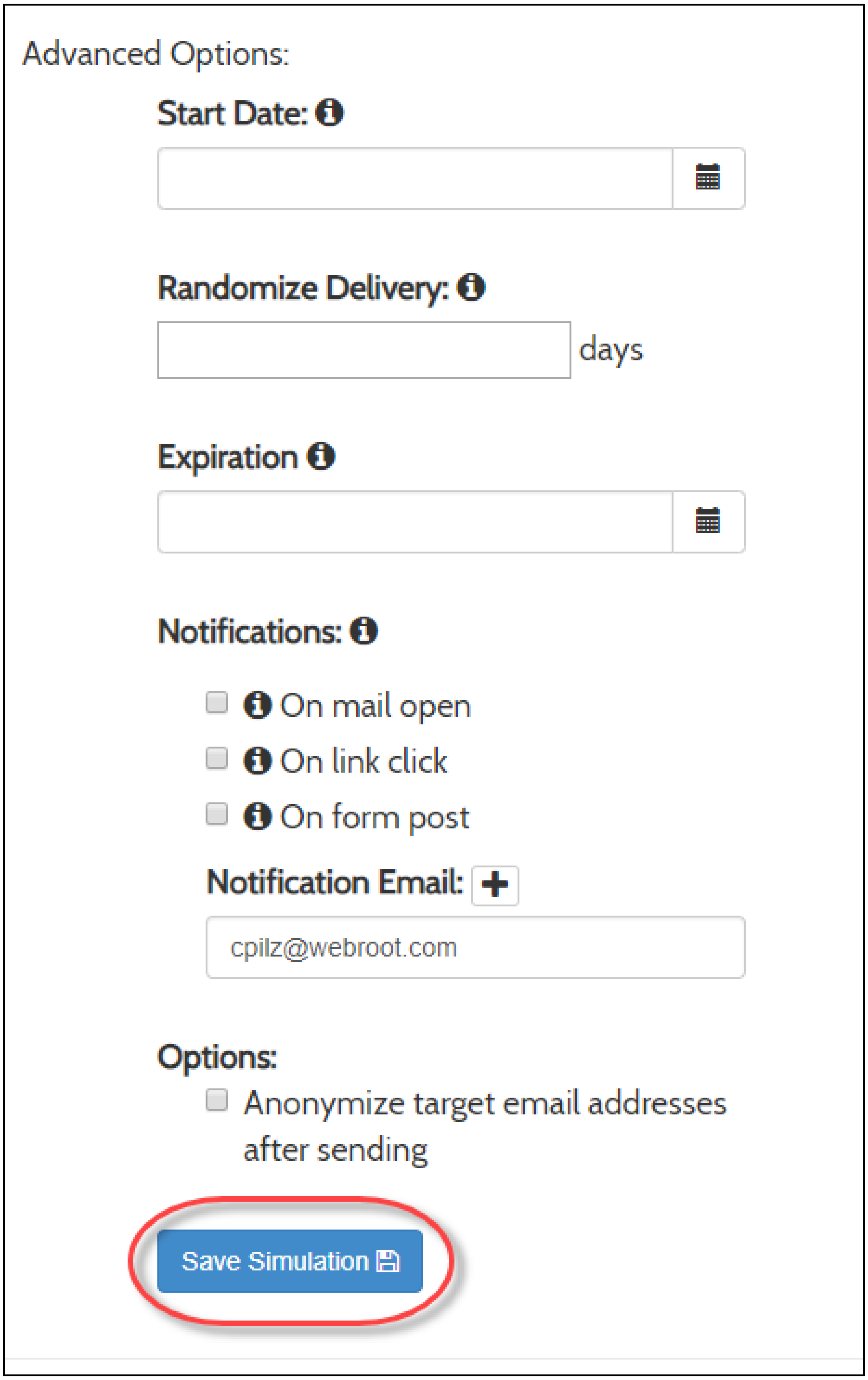
The Advanced Options area displays.


Advanced Options:
Start Date:
Randomize Delivery:
days
Expiration
Notifications:
On mail open
On link click
On form post
Notification Email:
cpilz@webroot.com
Options:
Anonymize target email addresses after sending
Save Simulation

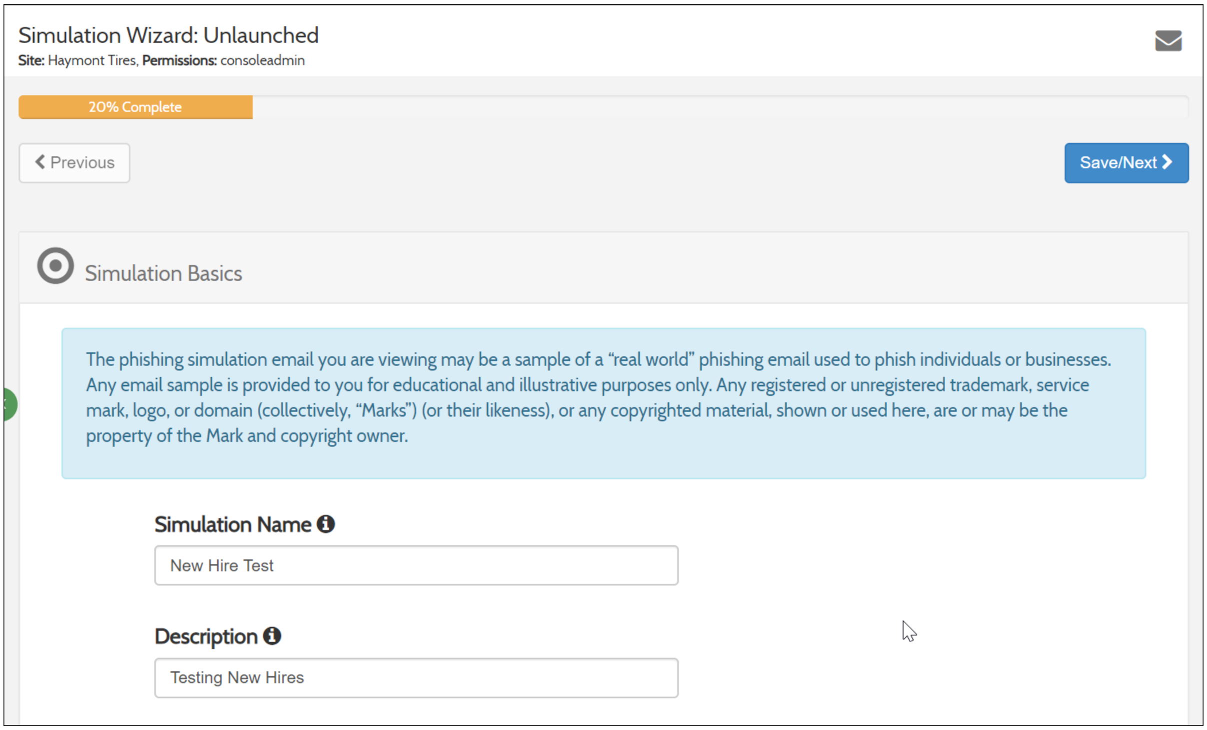
7. In the Advanced Options area, populate the following fields:
   - **Start Date** — Enter a start date to schedule the launch of the campaign for a future date. If this is left blank, the campaign will start when you click the **Launch** button at the end of the wizard.
   - **Randomize Delivery** — Enter the number of days to randomize the delivery of phishing emails over a period of time.
     - Use the **Up** and **Down** arrows to set your number of days.
     - Workday span will configure the randomization over the working hours you set.
     - The time zone is automatically configured using your computer's time zone.
   - **Expiration** — Enter the last date of the campaign, and wrap up reporting for the campaign.
   - **Notifications** — Select one of the following to determine when notification emails will be sent:
     - On mail open
     - On link clink
     - On form post

     Note: These notification emails are sent for every action chosen and may become quite frequent for larger campaigns.
   - **Notification Email** — Enter the email to which notifications should be sent.
   - **Anonymize target email addresses after sending** — Select this checkbox to anonymize the reporting data and not identify the person who opened or clicked it. This is useful for organizations that are concerned about sharing who performed which actions.

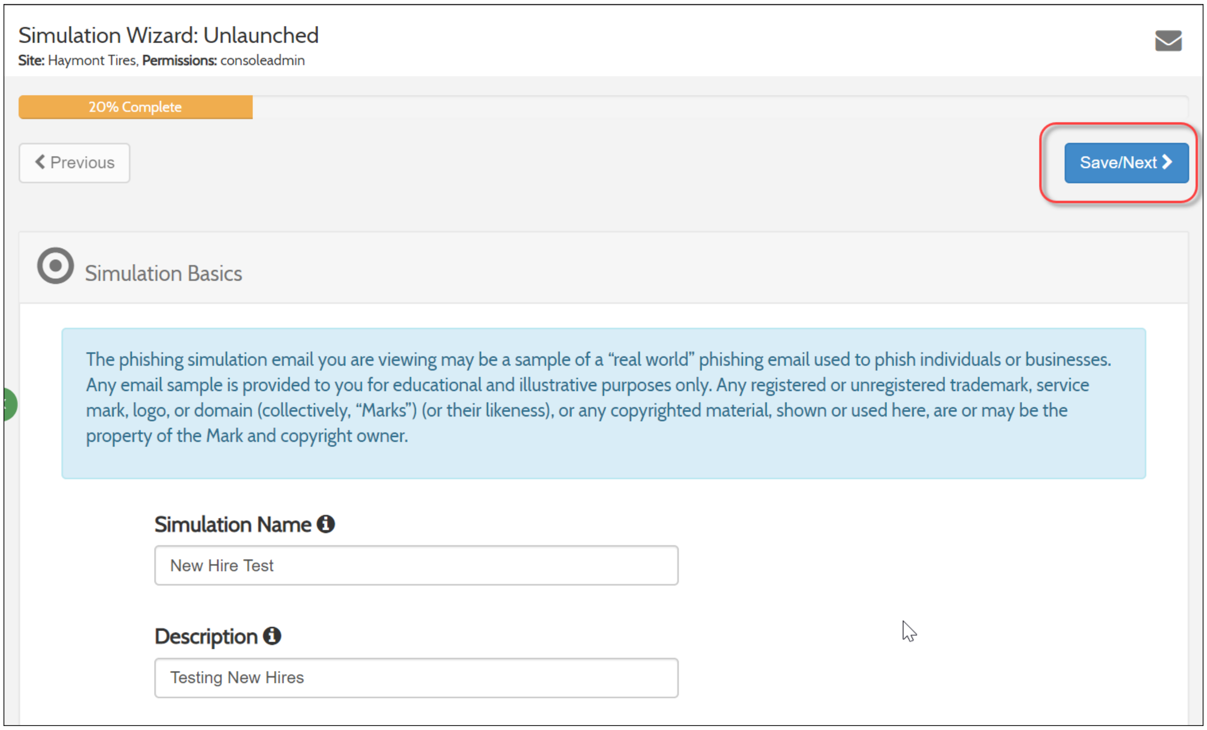
8. Click the **Save Simulation** button.


Advanced Options:
Start Date:
Randomize Delivery:
days
Expiration
Notifications:
On mail open
On link click
On form post
Notification Email:
cpilz@webroot.com
Options:
Anonymize target email addresses after sending
Save Simulation

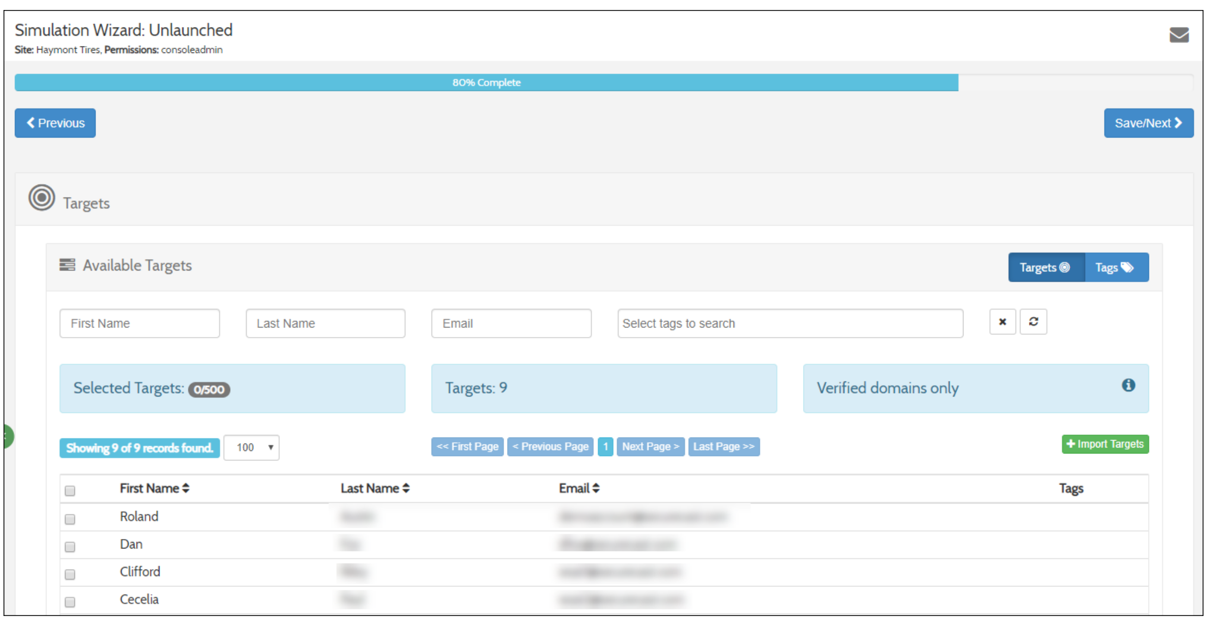
The Simulation Wizard: Unlaunched panel displays, with all of the fields populated.



9. When you're ready, click the **Save/Next** button.

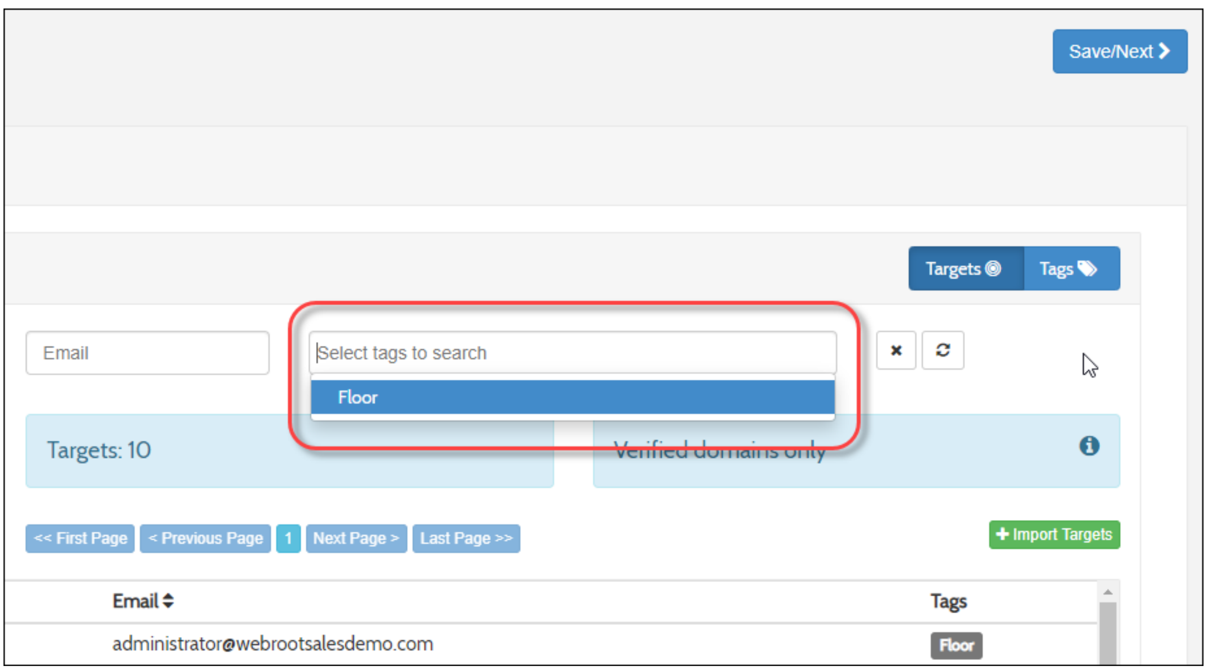


The Targets pane displays, with the Target tab active.



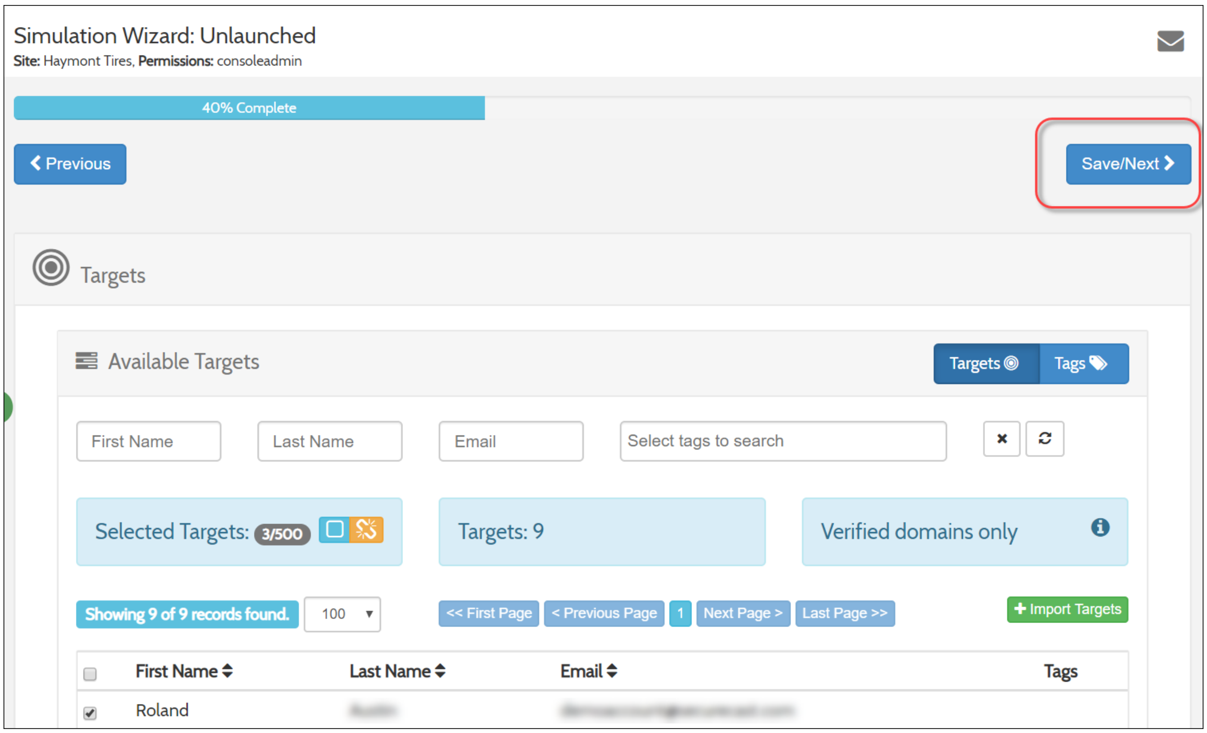
10. Do one of the following to determine the targets you would like to send the phishing simulation to:
    - Select one or more users by selecting the checkbox next to their name.

    - Click the **Tags** button and select users based on their tag. To do this, from the Select tags to search drop-down menu, select the tag of the users you want to send the email to. You can select multiple tags, as needed.



Note: For information on how to create tags so that they display in the drop-down menu, see Importing Targets on page 179.

11. When you're ready, click the **Save/Next** button.



You've now created a phishing simulation and can move on with the next step, Designing Phishing Emails on page 22.

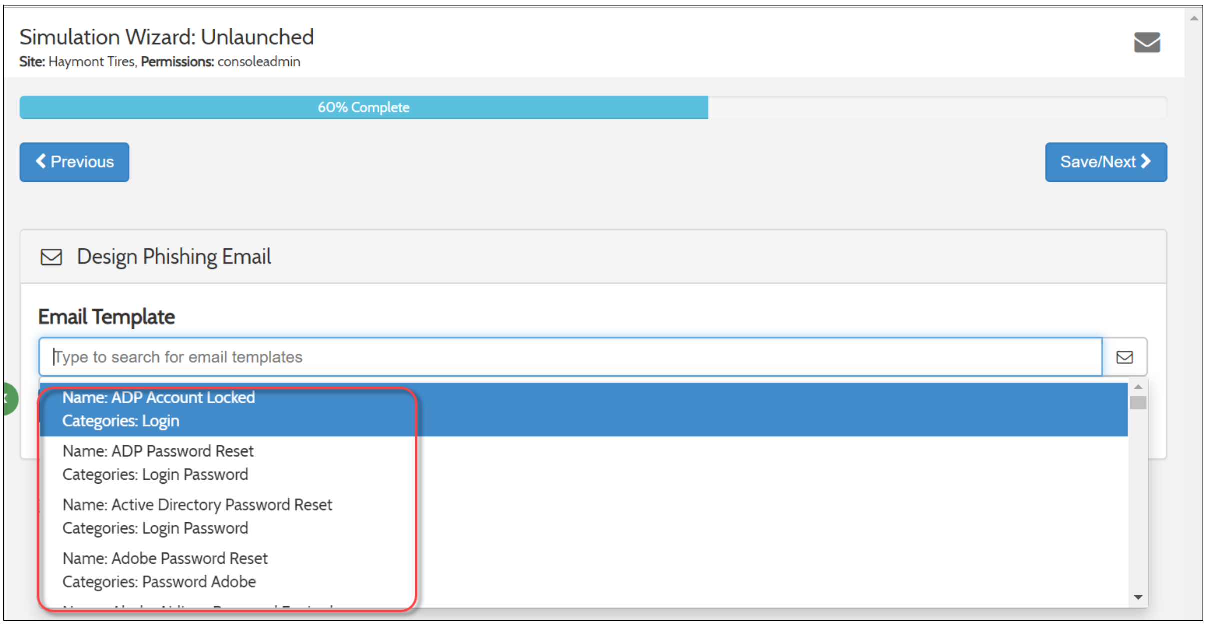
Designing Phishing Emails

Follow this procedure to design phishing emails.

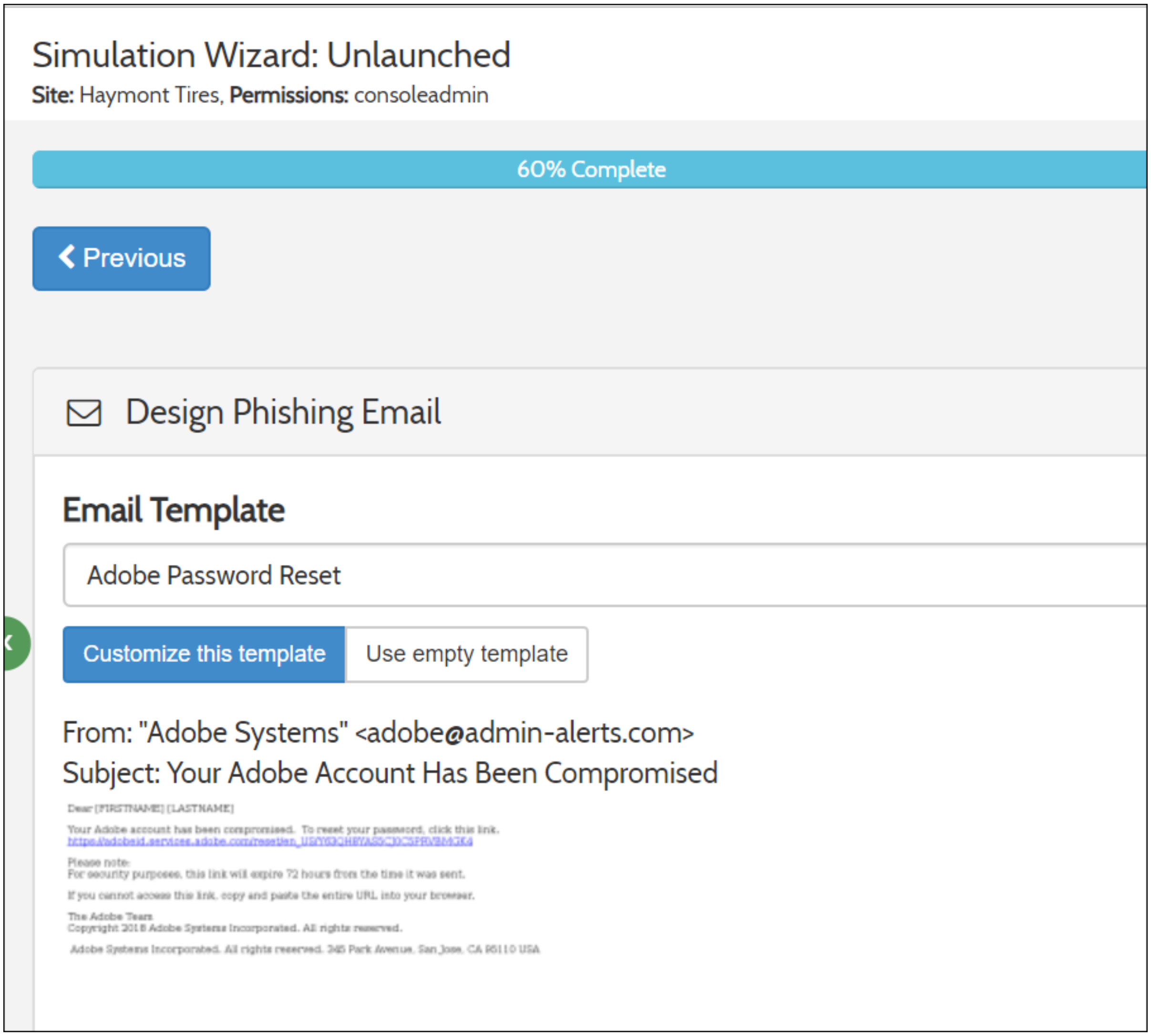
Note: Before beginning this procedure, you must first create a phishing simulation.

To design a phishing email:

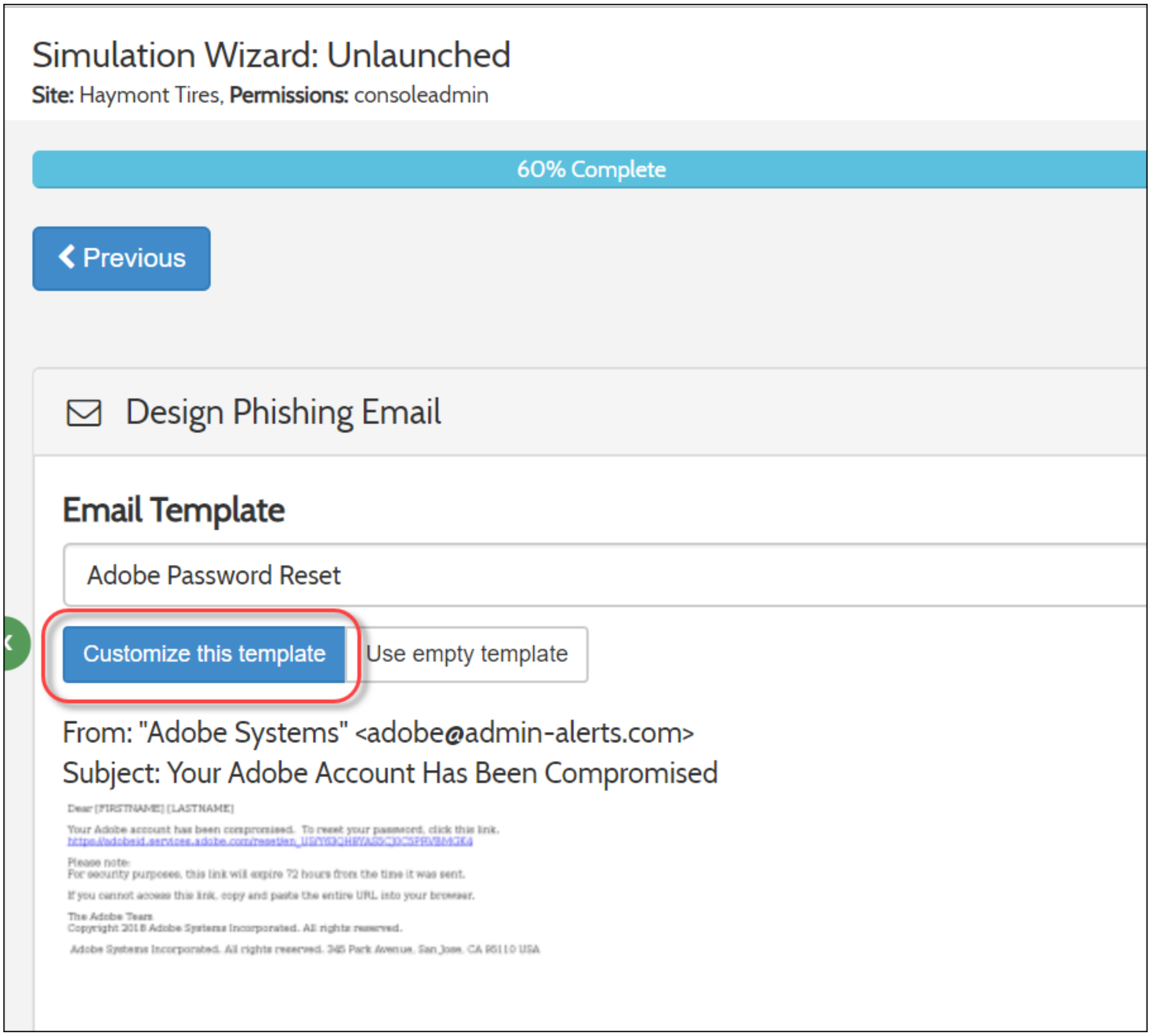
1. Once you've created a phishing simulation, from the Email Template drop-down menu, select a phishing email from one of our default templates.



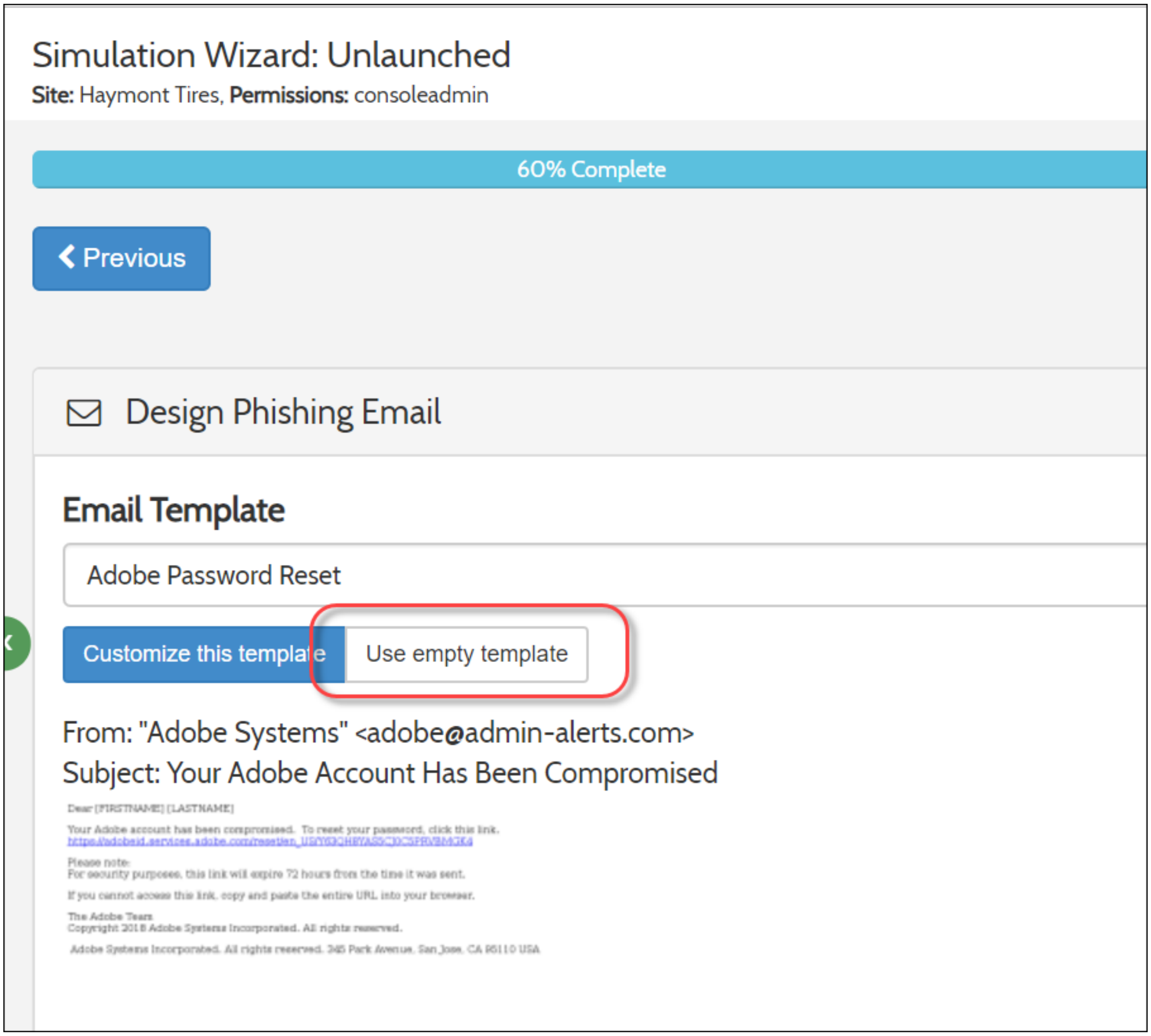
The template you have selected displays.



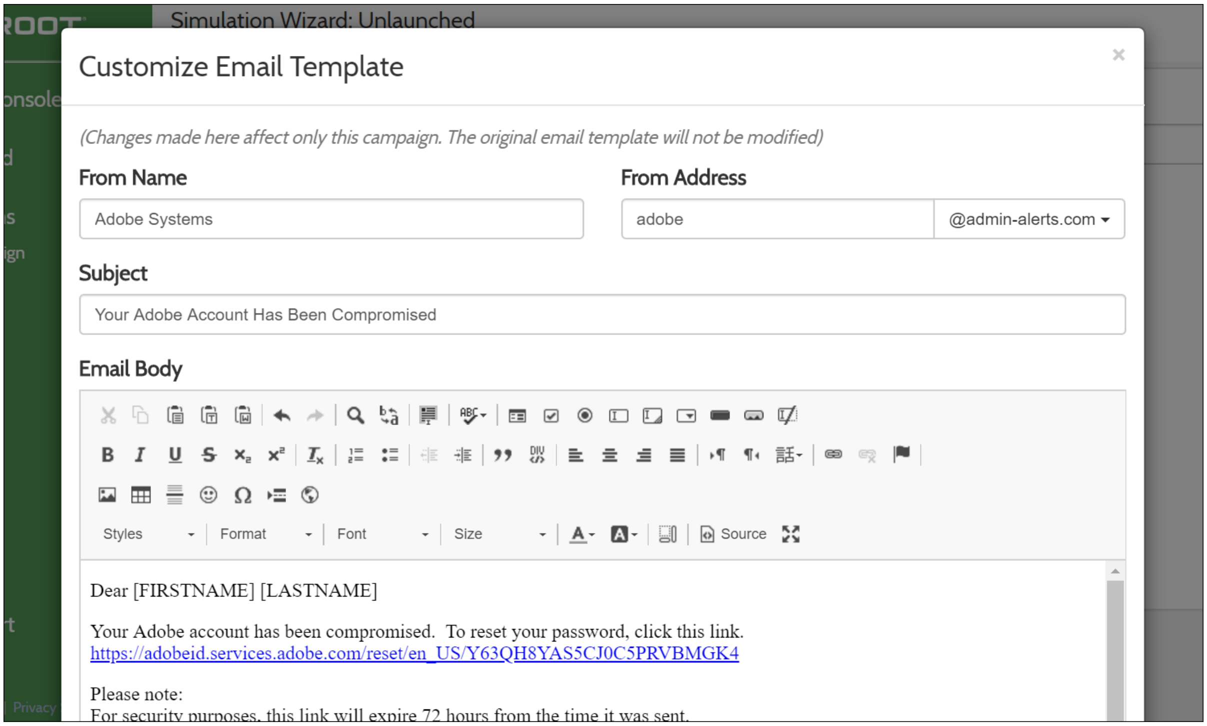
2. Do any of the following:
   - Use the email template as is.
   - Click the **Customize this template** button to use the WYSIWYG editor to modify the template for your phishing email.



- Click the **Use empty template** button to use the WYSIWYG editor to create a phishing email from scratch.



3. If you clicked the Customize this template button or the Use empty template button, the email WYSIWYG editor displays.

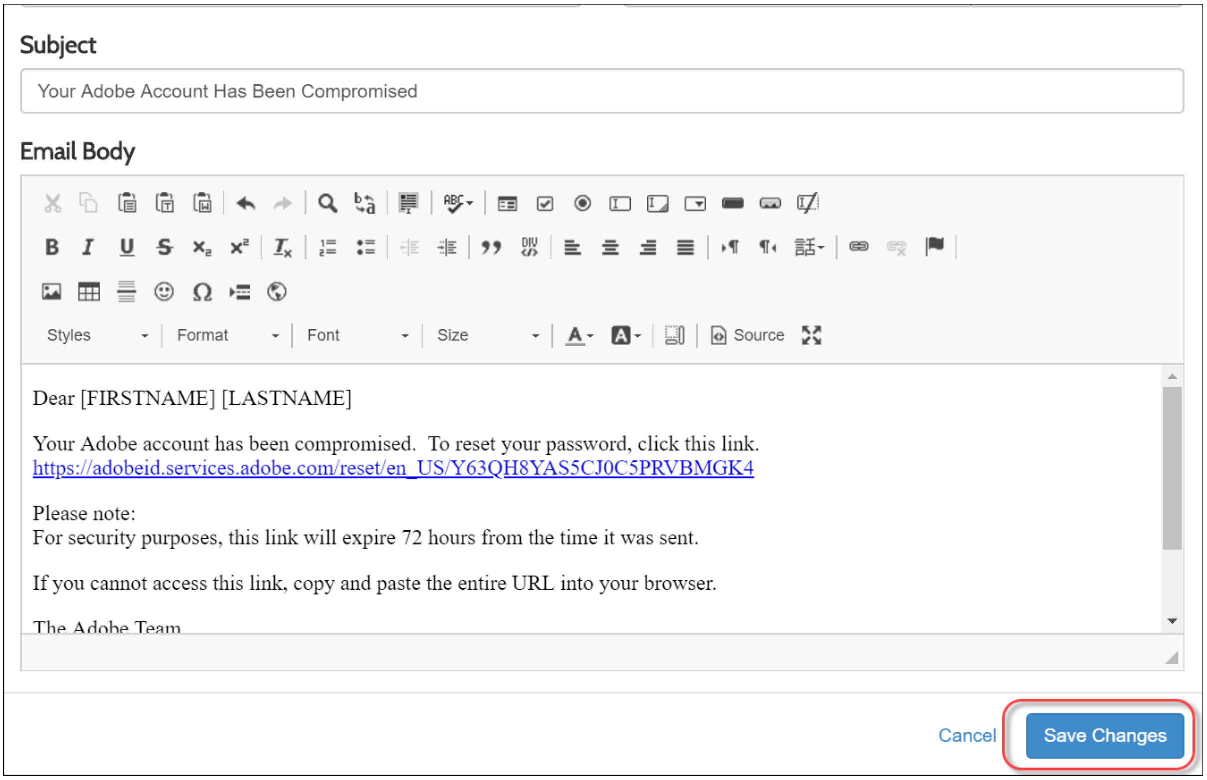


4. As needed, either update or populate the following fields:
   - From Name
   - From Address
   - Subject
5. In the Email Body area, enter information or instructions to complete the phishing scenario.
6. Use the WYSIWYG editor to configure and customize your text.

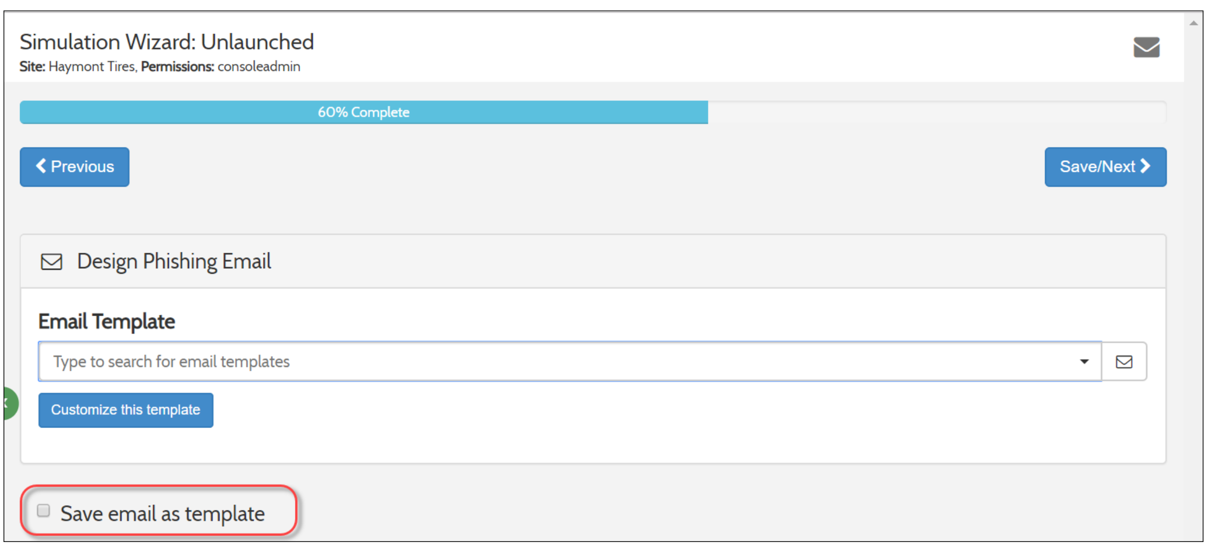
> **Note:** Hover over each icon to see its function.

7. Enter variables as needed. Variables include:
   - **[FIRSTNAME]** — Replaces the variable with the recipient's first name.
   - **[LASTNAME]** — Replaces the variable with the recipient's last name.
   - **[EMAIL]** — Replaces the variable with the recipient's email.

8. When you're ready, click the **Save Changes** button to return to the Wizard.



9. If you would like to use the template you have just created again in the future, select the **Save email as template** checkbox.



10. You’ve now created a phishing simulation and can move on with the next step, Designing Phishing Sites on page 29.

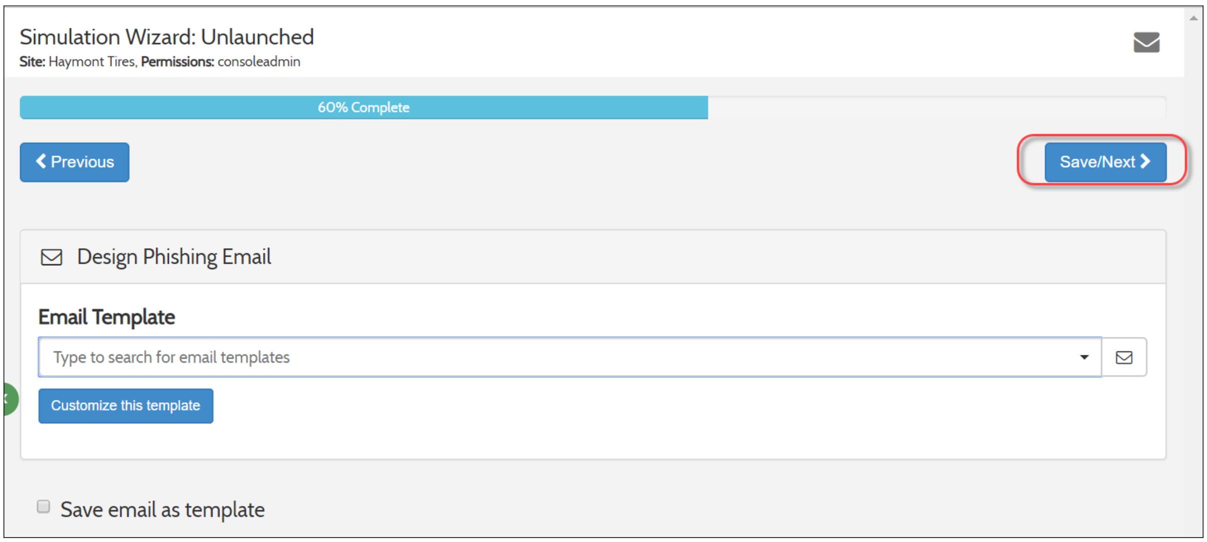
Designing Phishing Sites

Follow this procedure to design fishing sites.

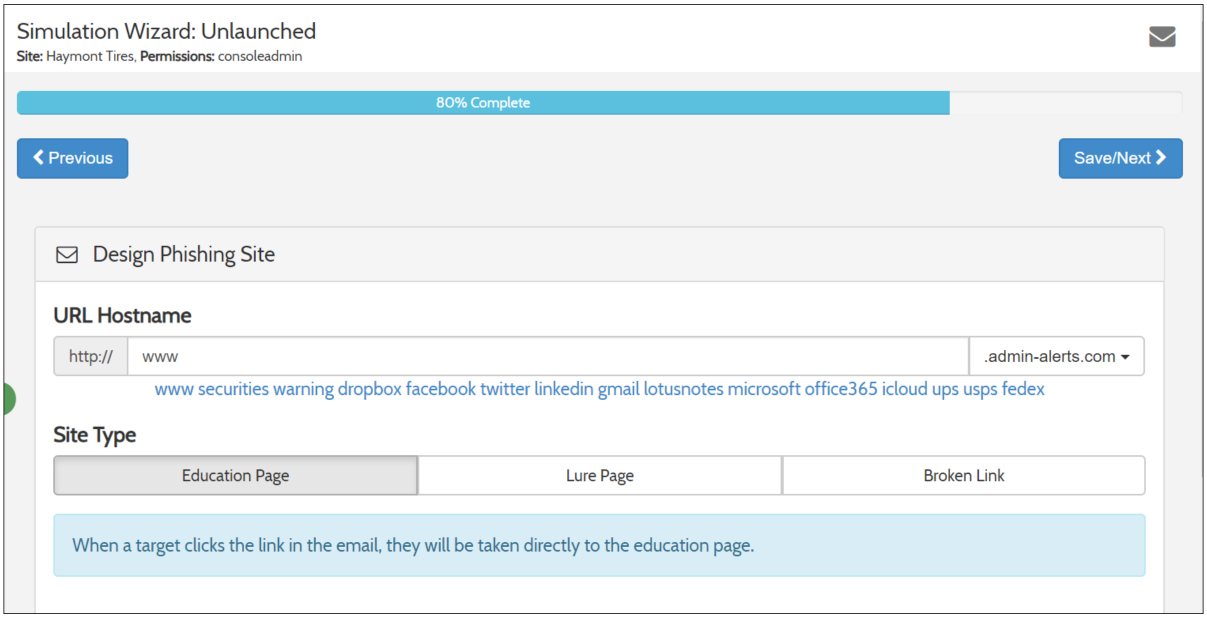
Note: Before beginning this procedure, you must first design a phishing email.

To design a phishing site:

1. Once you've created your phishing email, click the **Save/Next** button.

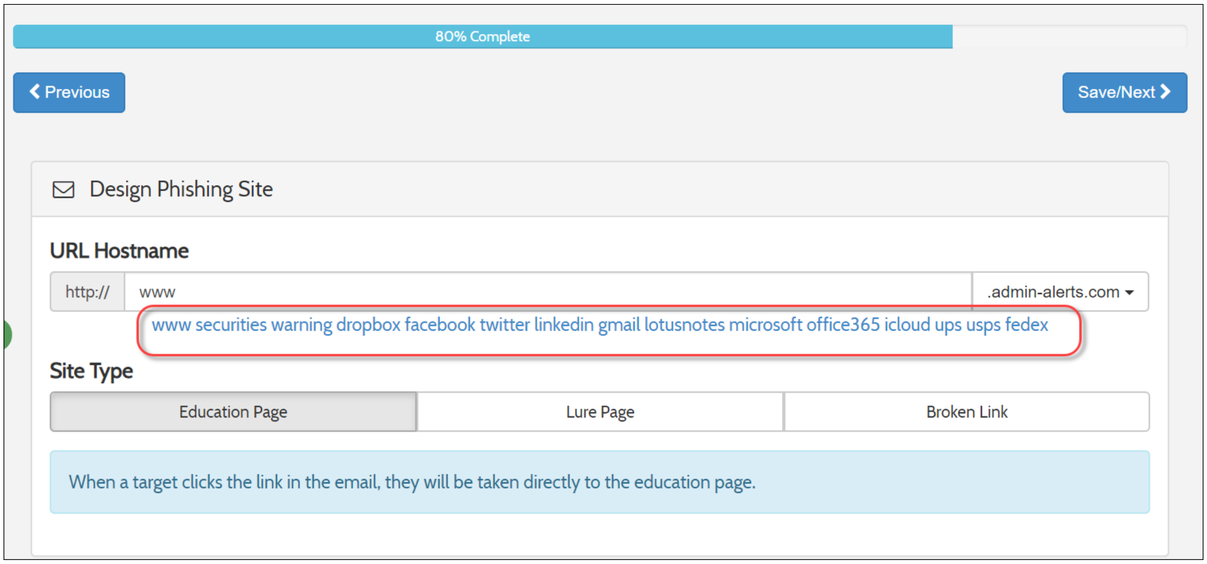


The Design Phishing Site panel displays.



Note: Also on this page is the area where you would design an Education Page for a training program. For more information, see Designing Education Pages on page 78.

2. In the URL Hostname field, do either of the following:
   - Enter a fake URL name.
   - Click one of the suggested URL types.



3. In the Site Type area, click one of the following buttons to determine what type of site you want to design that your user will be sent when they click on a link:

> **Note:** Depending on button you click, the area below displays the fields that you will need to populate to create that type of phishing page or link.

To Create This...	Click This...
An Education Page	The **Education Page** button. When you click this button, scroll down the page and create an education page. When a target clicks the link in the email, they will be taken directly to that education page, which will either provide a training module or an informational graphic. For more information, see Designing Education Pages on page 36.
A Lure Page	The **Lure Page** button. When you click this button, scroll down the page and create a lure page. When a target clicks the link in the email, they will be taken to the lure page, which will then provide either a training module or an informational graphic. For more information, see Designing Lure Pages on page 53. These templates are customizable, or you can create your own. Lure pages are optional and used to an add extra web landing page after a user clicks an email lure and before you take the user to education or a 404 broken link page.

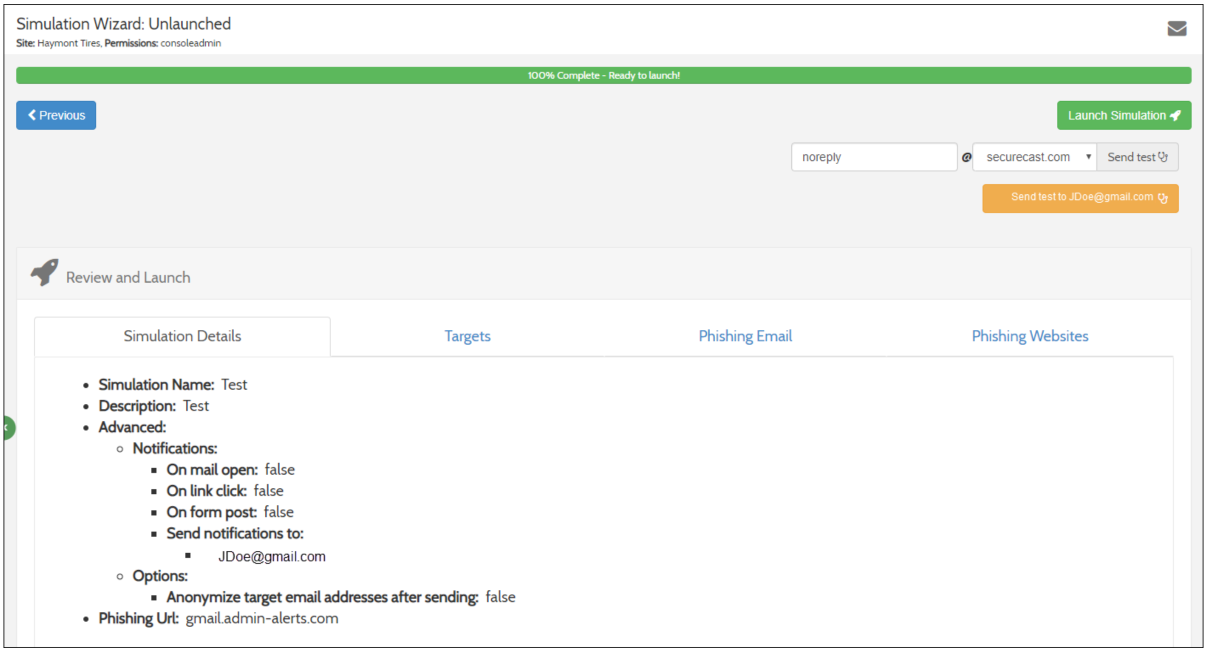
To Create This...	Click This...
A Broken Link Page	The **Broken Link** button. When you click this button, scroll down the page and create a Broken Link page. When a target clicks the link in the email, they will be taken to the 404 page. For more information, see Designing Broken Link Pages on page 57. **Note:** An Education page cannot be used with a Broken Link page.

4. When you've selected the type of site to send your users to, select one of the following:

To Send A User To...	Do This...
A Training Module	Click the **Training Module** button, then select the module you want to send the user to. You can customize the landing page for the training module using the custom branding and log, background image, title, and intro settings available.
A Template or Infographic	Click the **Template** or **Infographic** button, and select one of our pre-built education templates. Similar to the phishing email templates, these can be customized and saved in the WYSIWYG editor.

5. Click the **Save/Next** button.

   The final review panel displays.



6. Continue with Reviewing and Sending Phishing Simulations on page 60.

Designing Education Pages

Follow this procedure to create an education page where targets will be taken when they click on a link in a phishing email.

Keep in mind that you are still working on the process of creating and launching a phishing simulation. This is the part of the process where you create the final step of sending targets to education pages that will lead them to a training campaign or an informational graphic.

To create an education page:

1. Once you have completed Designing Phishing Emails on page 22 and selected the name of your URL, click the **Education Page** button.
2. Scroll down and click one of the following buttons:

To Send A User To...	Do This...
A Training Module	Click the **Training Module** button, then select the module you want to send the user to. For more information, see Creating Training Modules on page 37.
A Template or Infographic	Click the **Template or Infographic** button, and select one of our pre-built education templates. Similar to the phishing email templates outlined in Designing Phishing Emails on page 22, these can be customized and saved in the WYSIWYG editor. For more information, see Creating Templates and Infographics on page 43.

Creating Training Modules

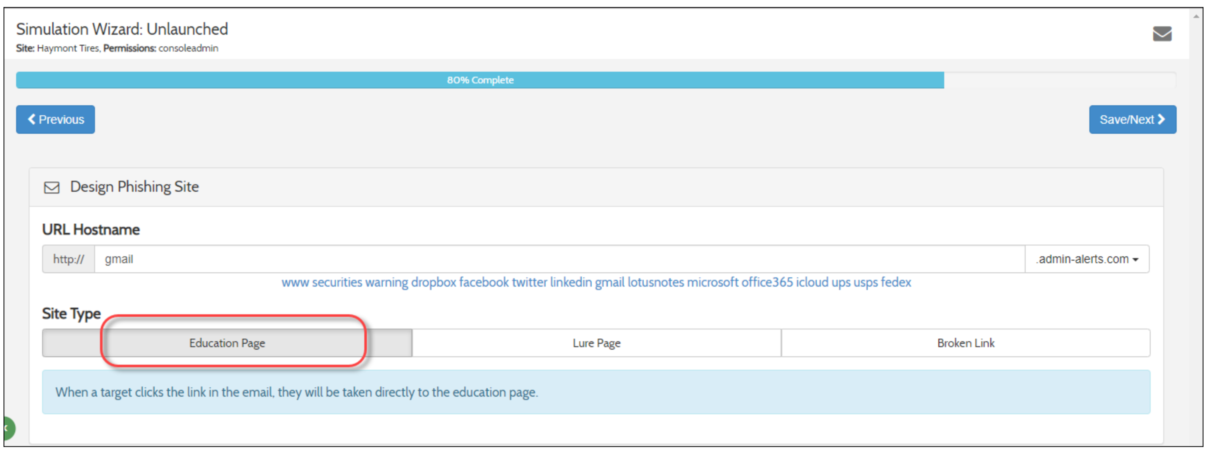
Follow this procedure to create a training module that your targets will be directed to when they click on a link in a phishing email.

A training module takes your targets through basic training to teach them about phishing scams.

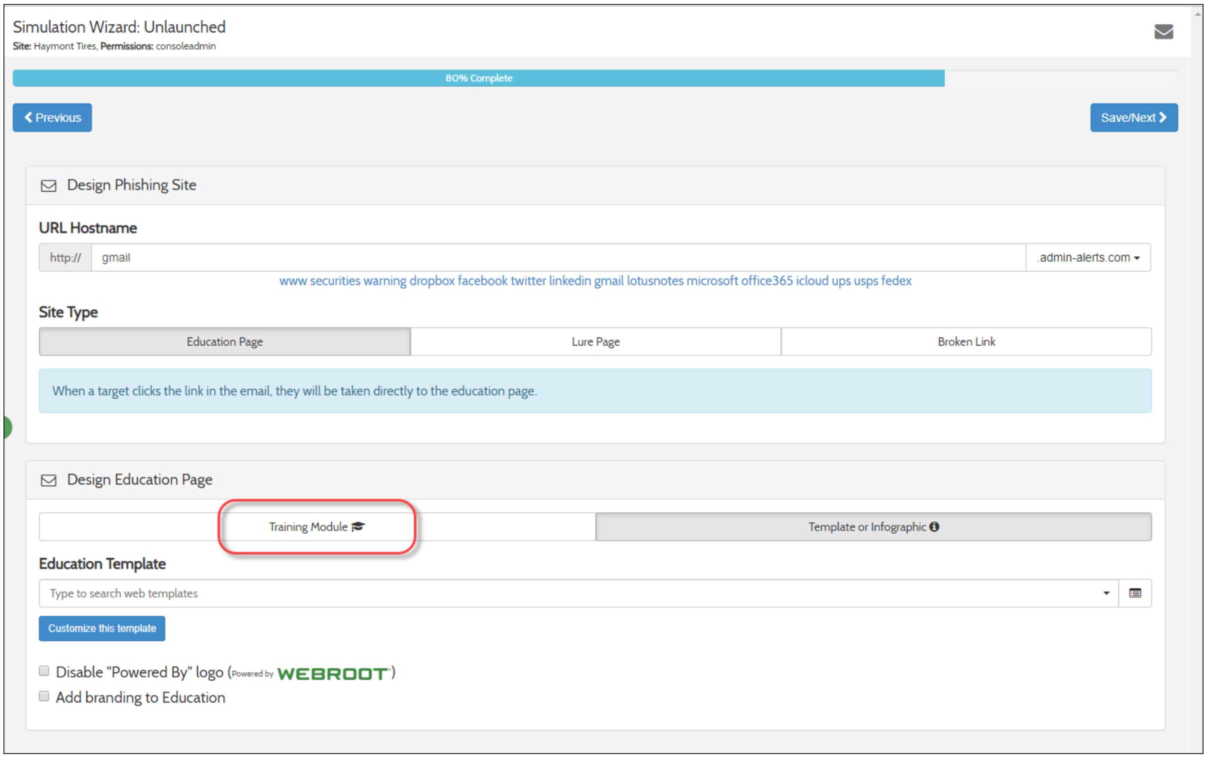
Fore more information, see Designing Phishing Sites on page 29.

To create a training module:

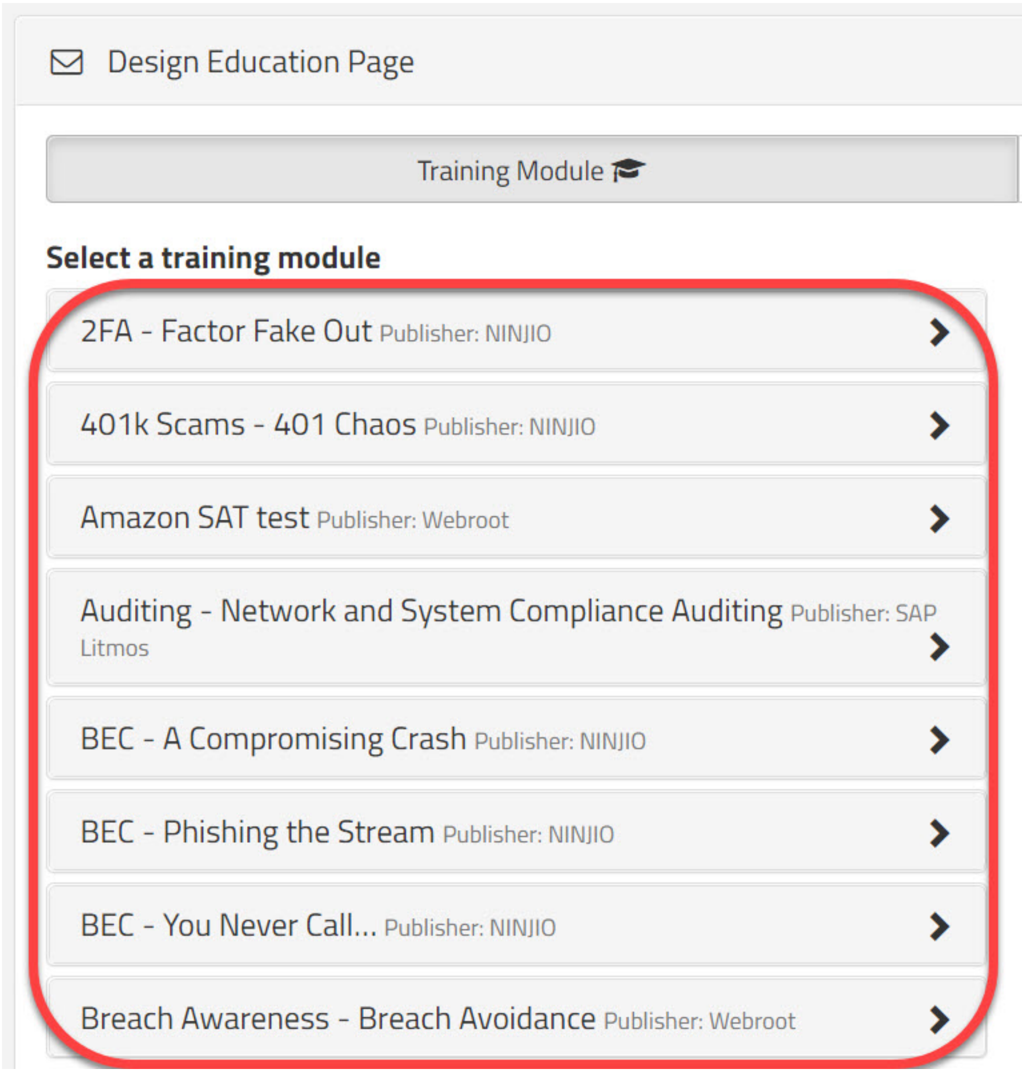
1. From the Design Phishing Site Page, click the **Education Page** button.



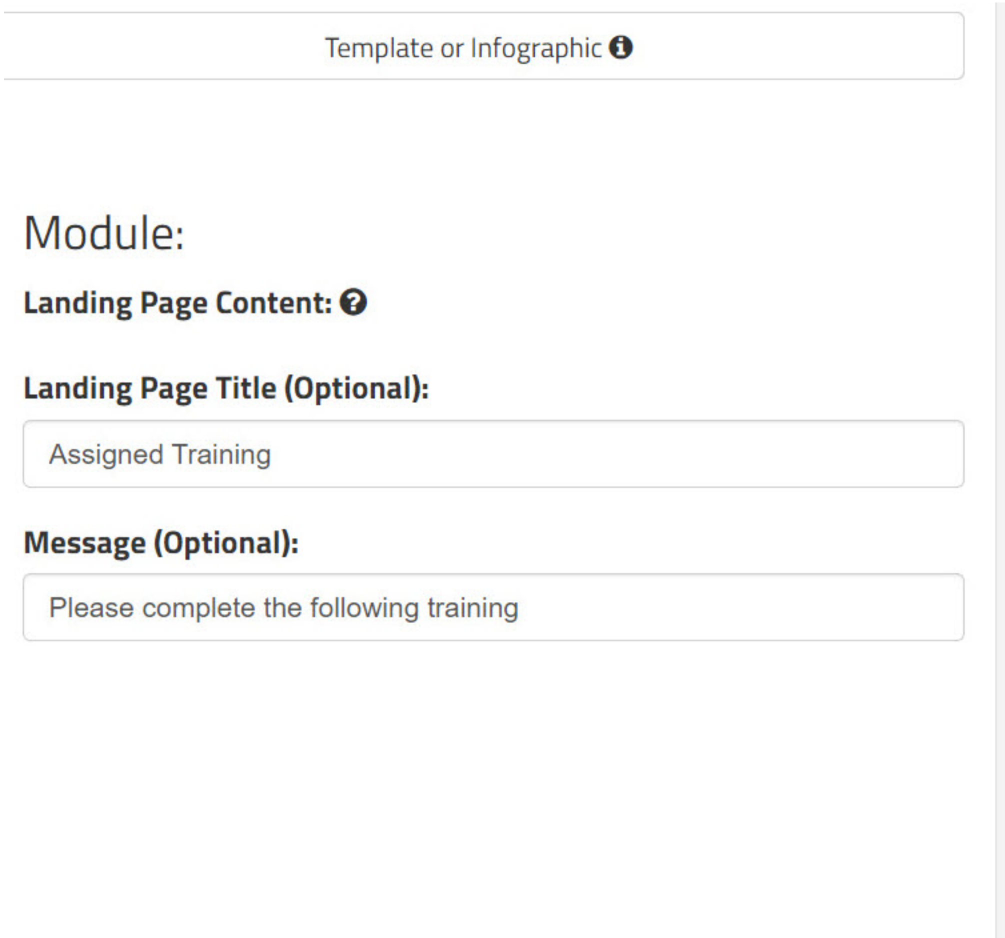
2. Click the **Training Module** button.



3. In the Select a training module column, select a pre-designed training module. For example, you might select a short video that discusses phishing scams.



To the right is where you will add an optional title and message to include in the training landing page.



4. As needed, click the **Preview** button to preview what the training looks like before sending.

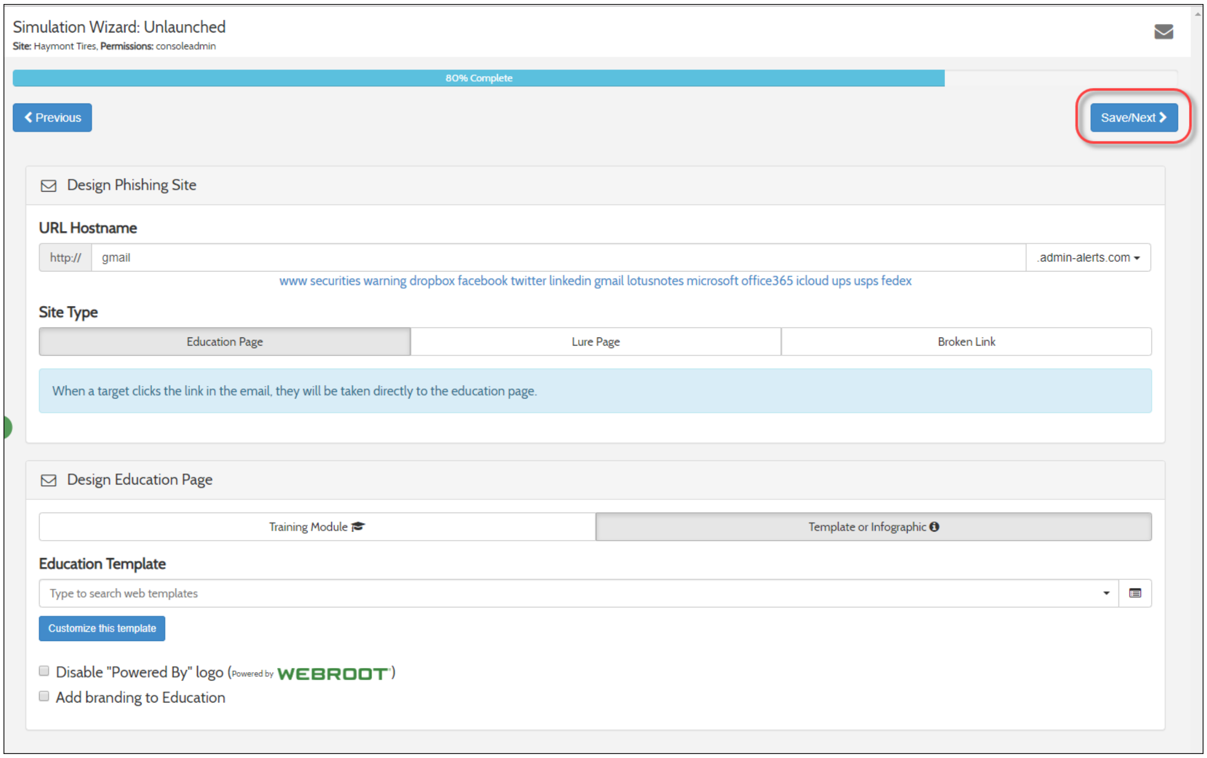
Training Module

Select a training module

2FA - Factor Fake Out Publisher: NINJIO

- Description: 2-Factor Authentication using your mobile phone (SMS) is a great security measure, and countless end-users have it in place – but that's bad news for Nico as he tries to use some stolen credentials. Nico and his hacking buddy think of a scheme to get around 2FA via SMS, opening the potential for business email compromise and all sorts of mischief. Watch to see how a hacker might try to get around 2FA via SMS, and how you can avoid becoming a victim of this plot.
- Preview

5. When you're ready, click **Save/Next** to proceed to the next step.



Creating Templates and Infographics

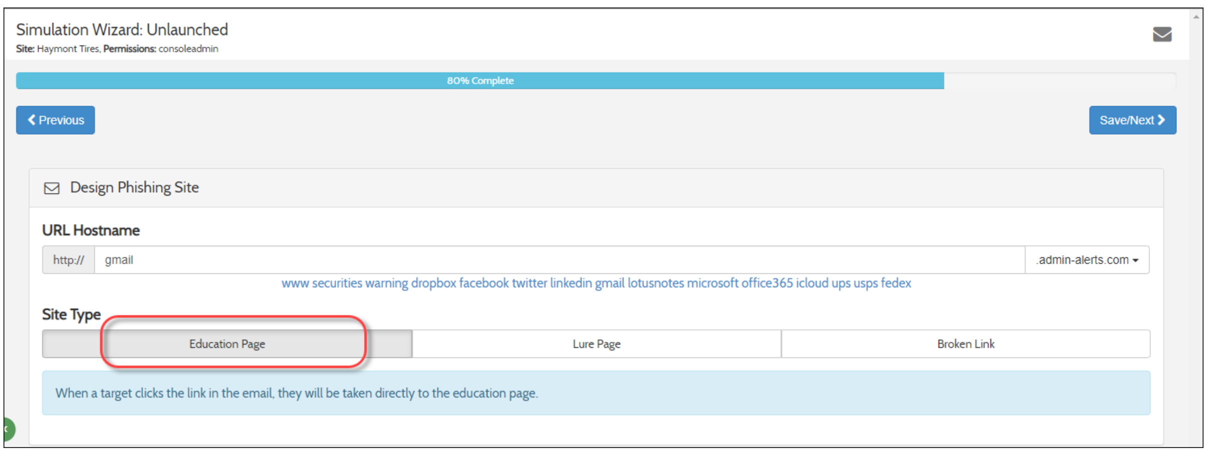
Follow this procedure when you've decided to create an Infographic Page where your targets will be taken when they click on a link in a phishing email.

An infographic is a page that displays a message to tell your target that they took the bait, or that they fell for a phishing scam. It's an easy way to demonstrate how easy it is to fall for a phishing attack.

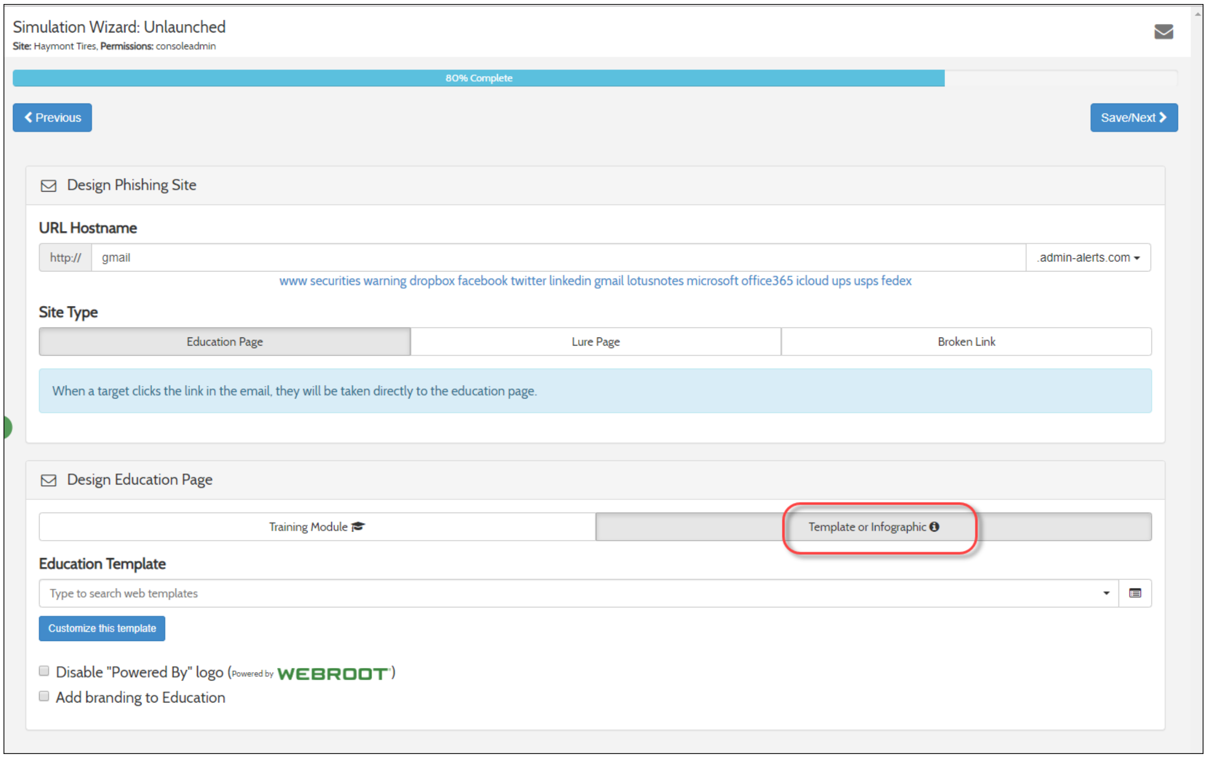
Fore more information, see Designing Phishing Sites on page 29.

To create an infographic:

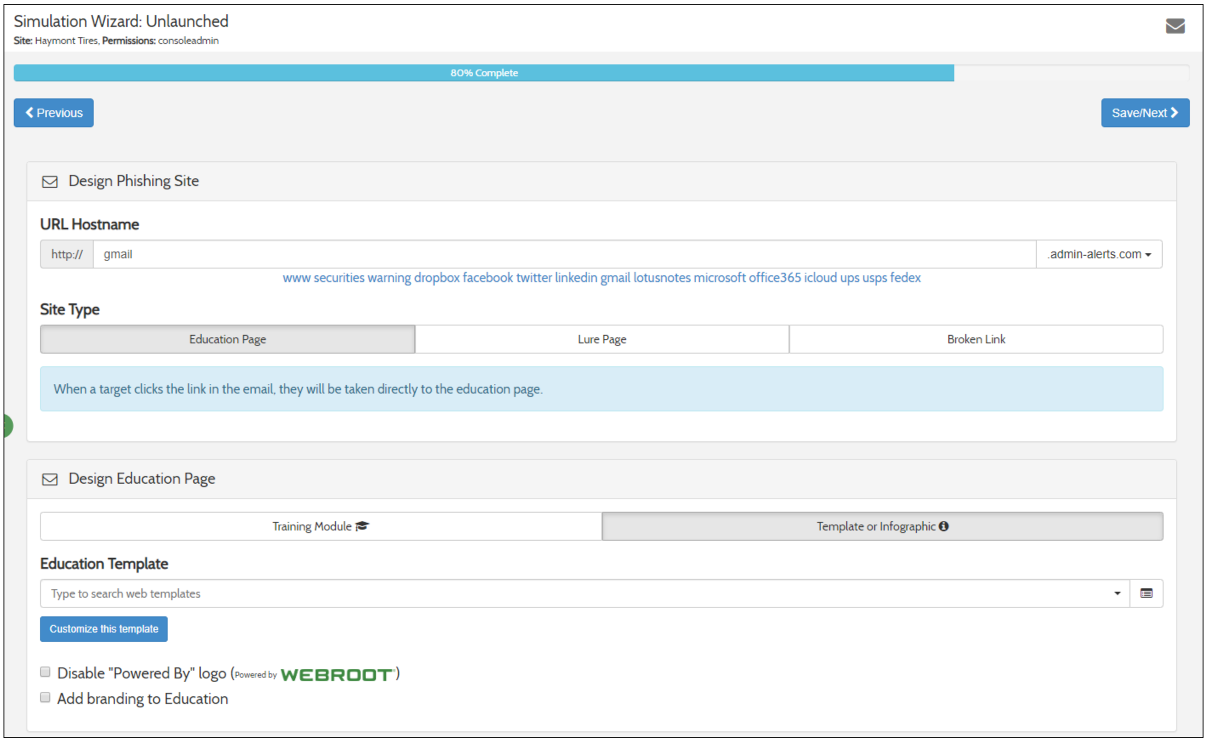
1. From the Design Phishing Site page, click **Education Page** button.



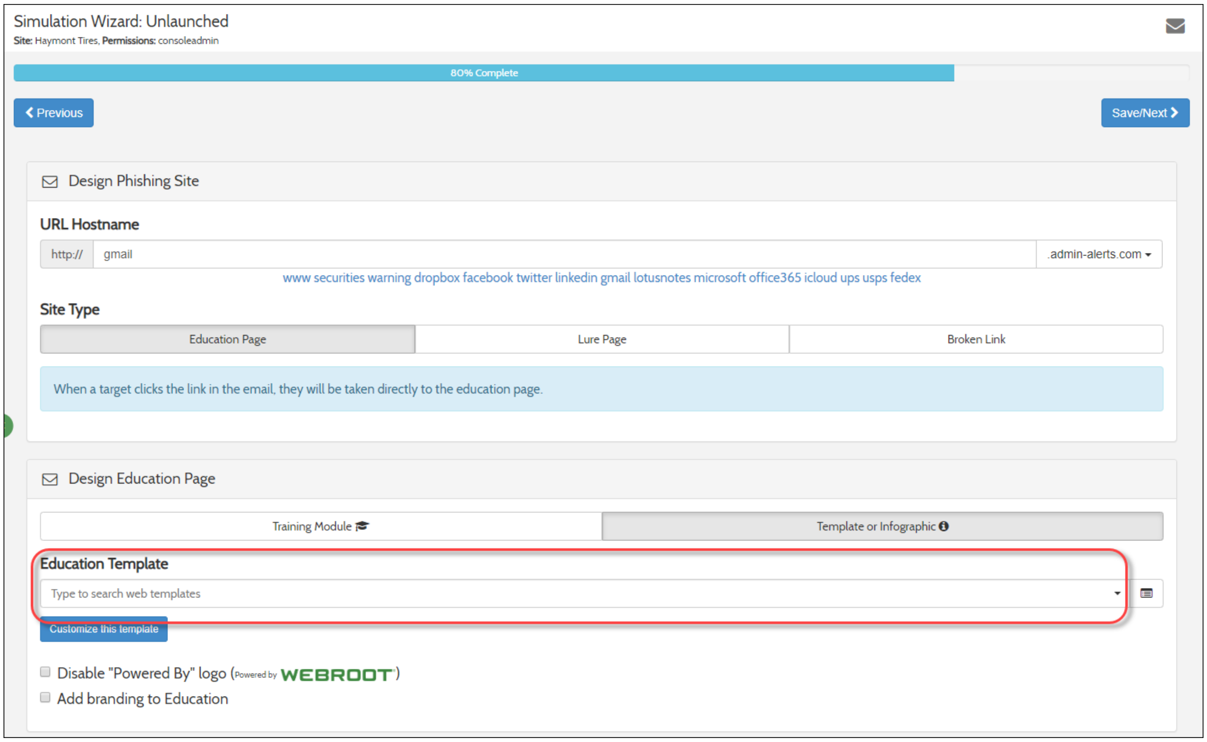
2. Click the **Template or Infographic** button.



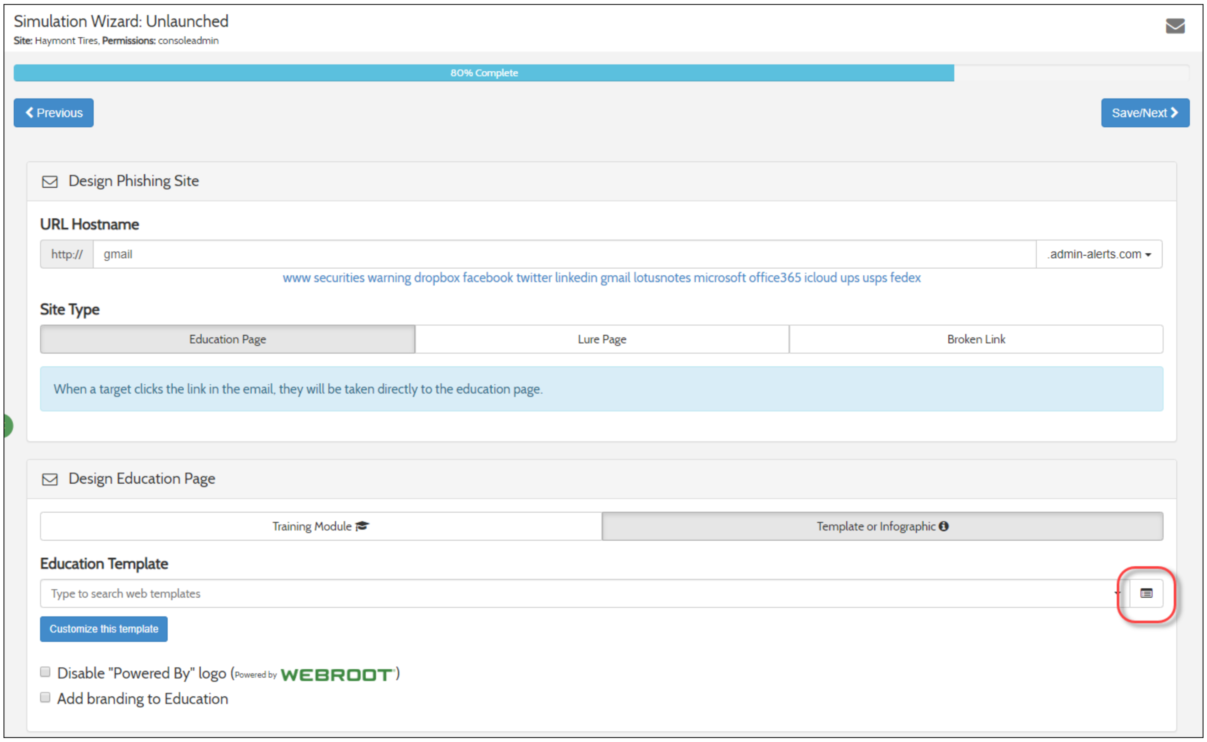
The Education Template displays.


Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin
80% Complete
Previous
Save/Next
Design Phishing Site
URL Hostname
http://
gmail
.admin-alerts.com
www securities warning dropbox facebook twitter linkedin gmail lotusnotes microsoft office365 icloud ups usps fedex
Site Type
Education Page
Lure Page
Broken Link
When a target clicks the link in the email, they will be taken directly to the education page.
Design Education Page
Training Module
Template or Infographic
Education Template
Type to search web templates
Customize this template
Disable "Powered By" logo (Powered by WEBROOT)
Add branding to Education

3. From the Education Template drop-down menu, select an infographic template.

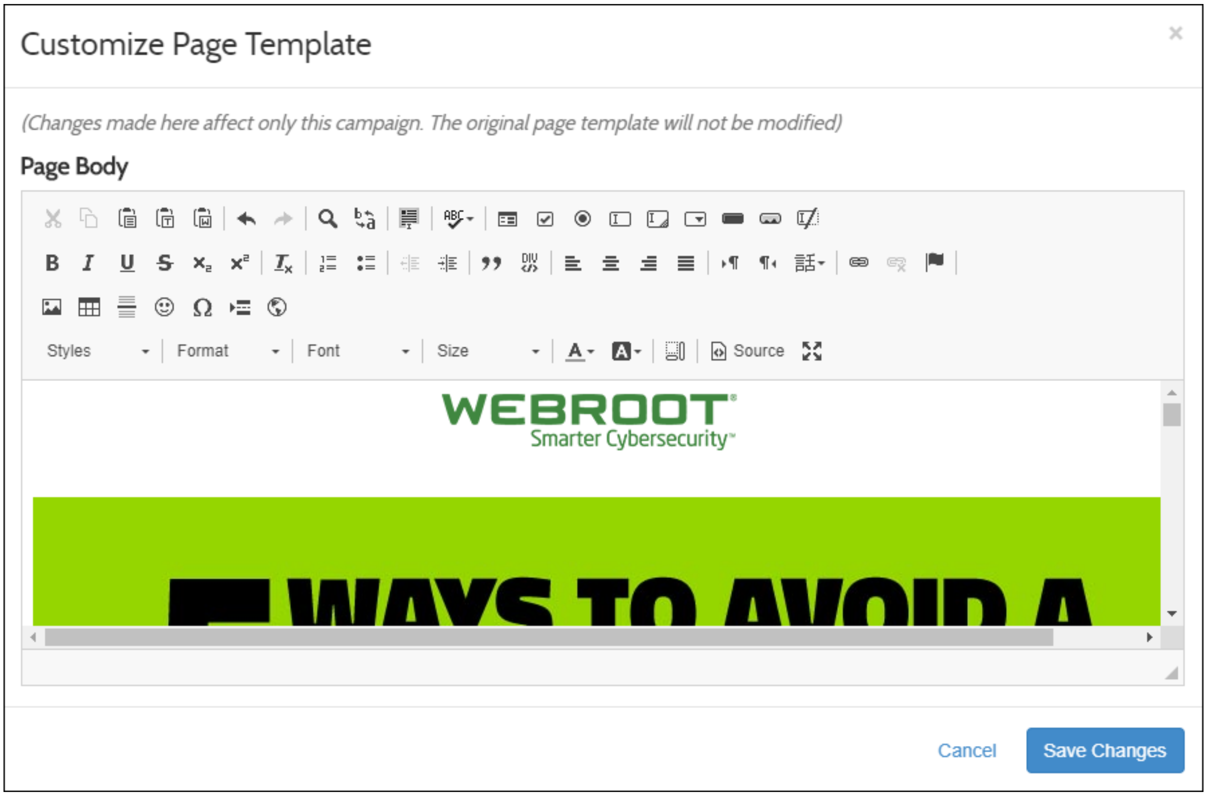


Alternately, you can click the **Browse** icon, and select your Education Template visually.

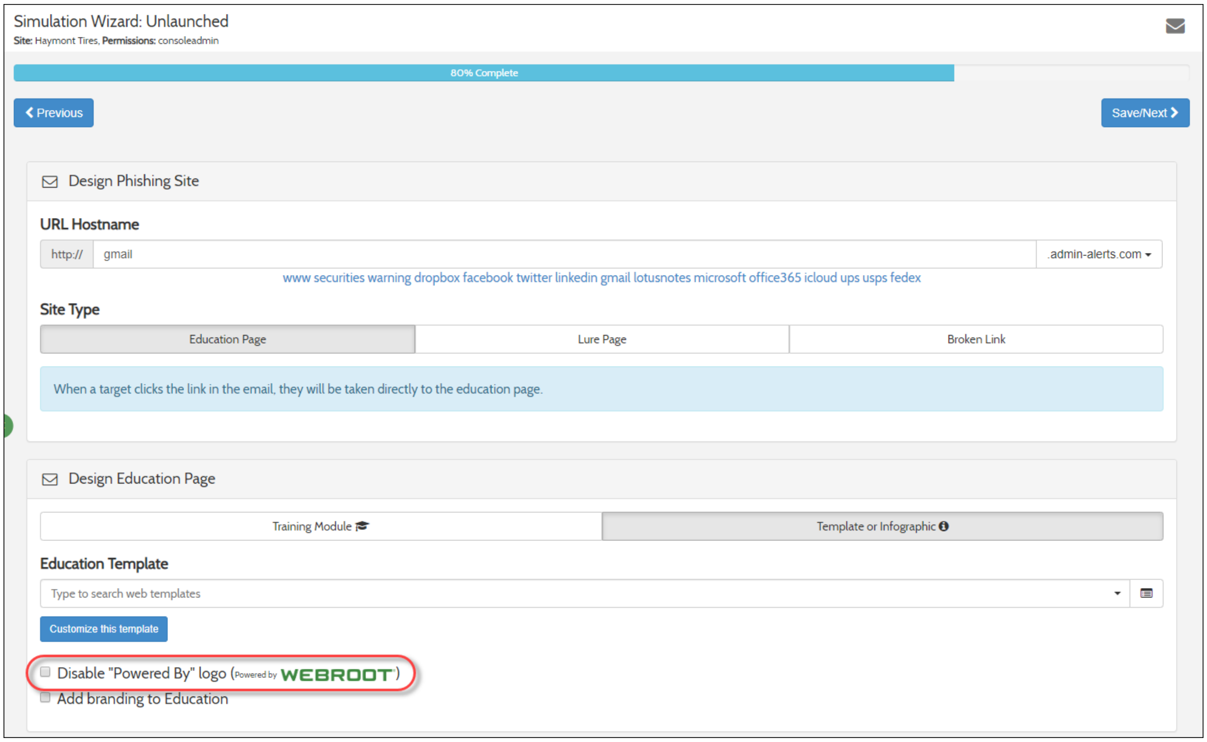


4. Do any of the following:
   - Use the infographic template as is.
   - Click the **Customize this template** button to use the WYSIWYG editor to modify the template for your phishing email.
   - Click the **Use empty template** button to use the WYSIWYG editor to create a phishing email from scratch.

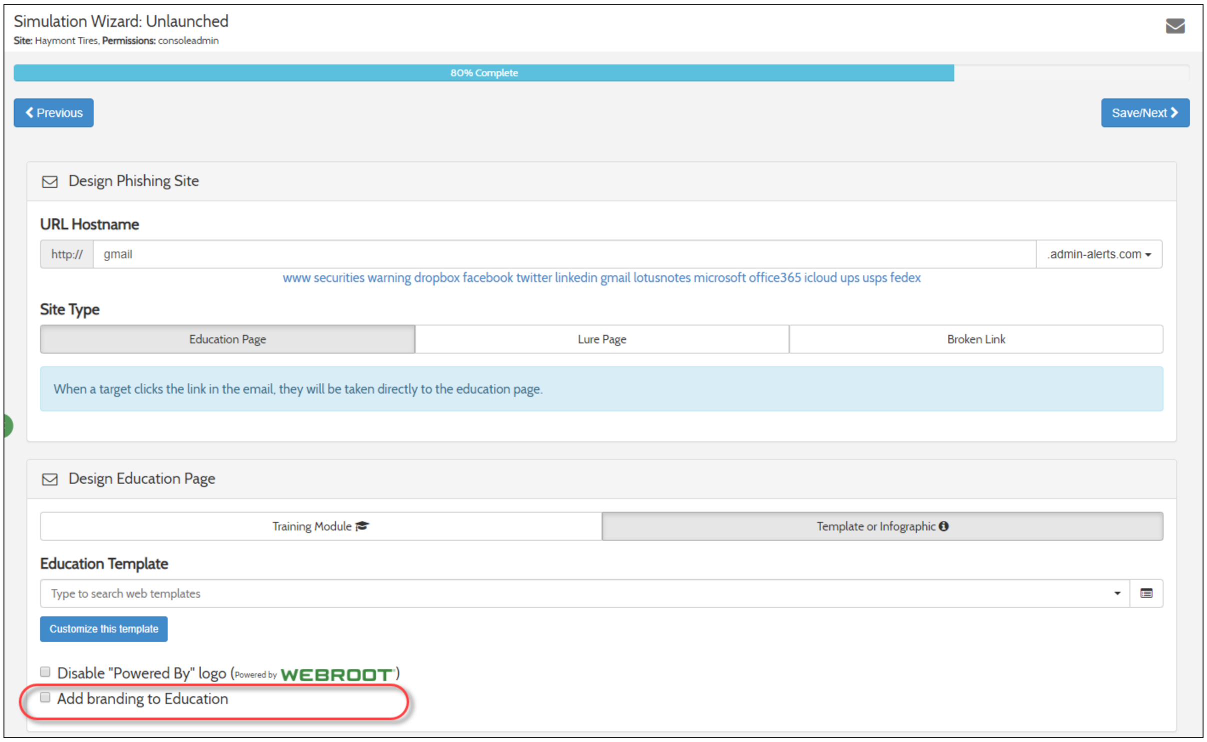
If you clicked the **Customize this template** button or the **Use empty template** button, the email WYSIWYG editor displays.



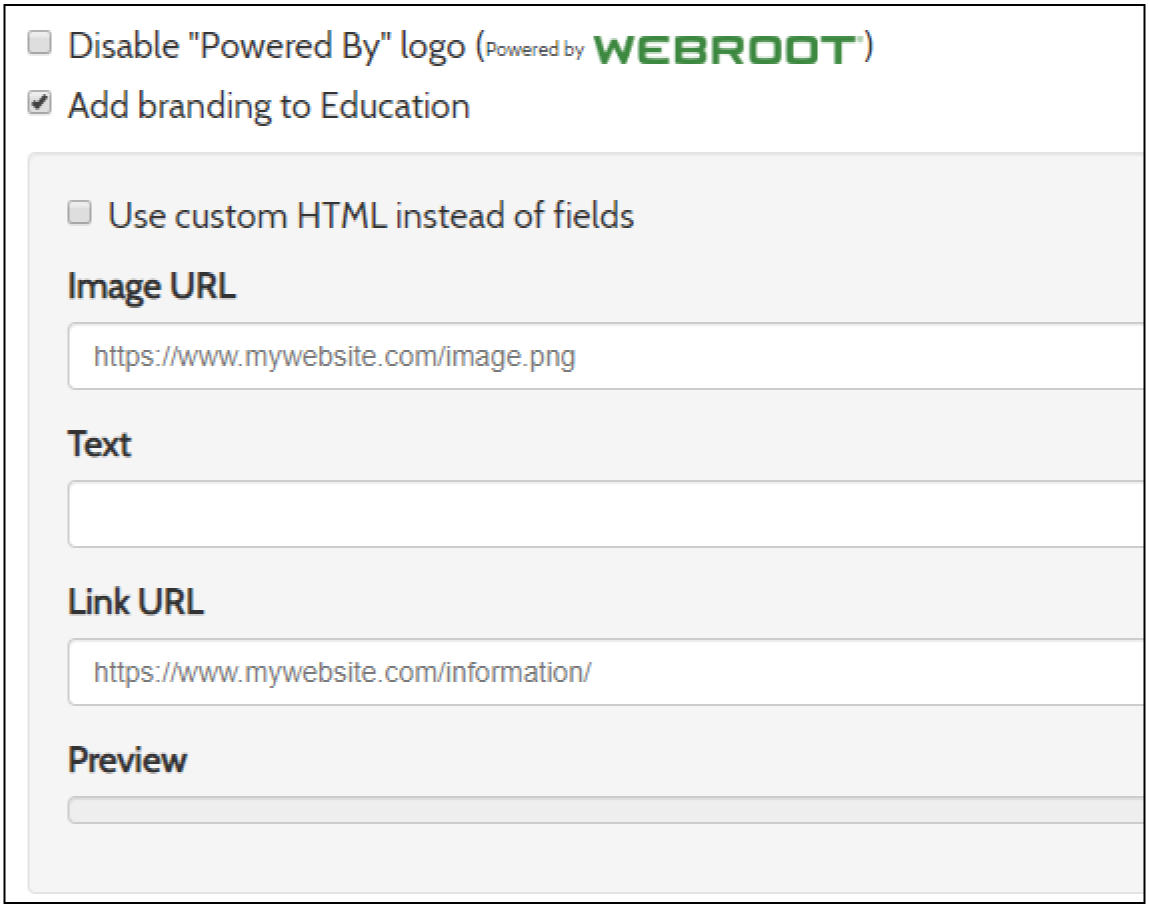
5. Use the editor to add or delete images, or to change and format the text.
6. To hide that the training comes from Webroot, select the **Disable Powered By Logo** checkbox.



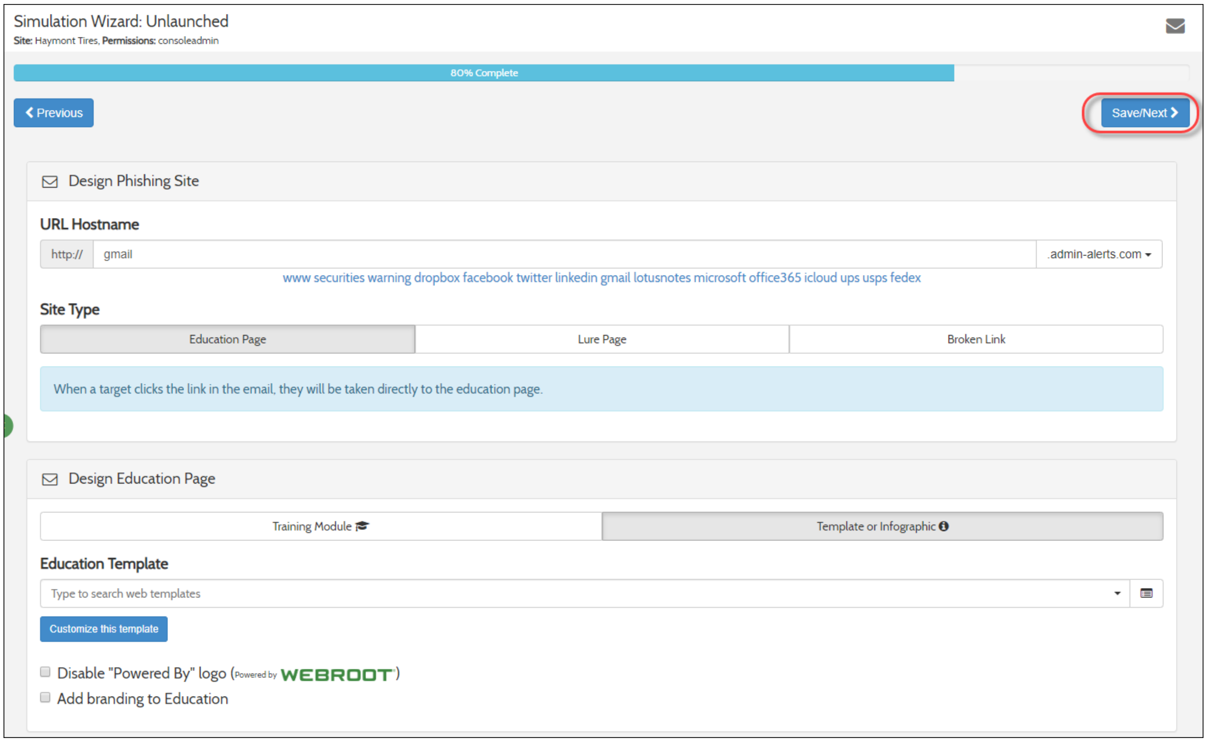
7. To add your own company's branding, select the **Add branding to Education** checkbox.



8. If you selected the Add branding to Education checkbox, populate the following fields:
   - Select the **Use custom HTML** checkbox to display a WYSIWYG editor.
   - In the Image URL field, enter the URL for an image that you store online, for example, a company logo.
   - In the Text field, enter the text that you want to display with your infographic.
   - In the Link URL field, enter the URL for your link.
   - In the Preview field, you can preview what your infographic page looks like.


Disable "Powered By" logo (Powered by WEBROOT)
Add branding to Education
Use custom HTML instead of fields
Image URL
https://www.mywebsite.com/image.png
Text
Link URL
https://www.mywebsite.com/information/
Preview

9. When you're ready, click the **Save/Next** button in the upper right corner.



Designing Lure Pages

A Lure Page is a page that acts as a continuation of the phishing test and presents an imitation login page. It's a way to demonstrate how easy it is to fall for a phishing attack.

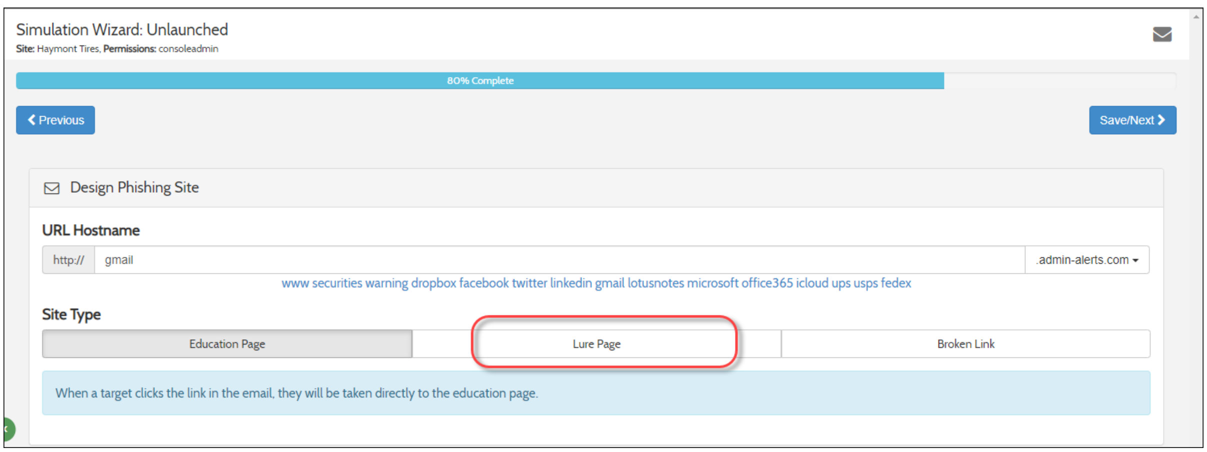
Lure Page templates are customizable, or you can create your own. Lure pages are optional and used to an add extra web landing page after a user clicks an email lure and before you take the user to education or a broken link page.

Follow this procedure when you've decided to design a Lure Page where your targets will be taken when they click on a link in a phishing email.

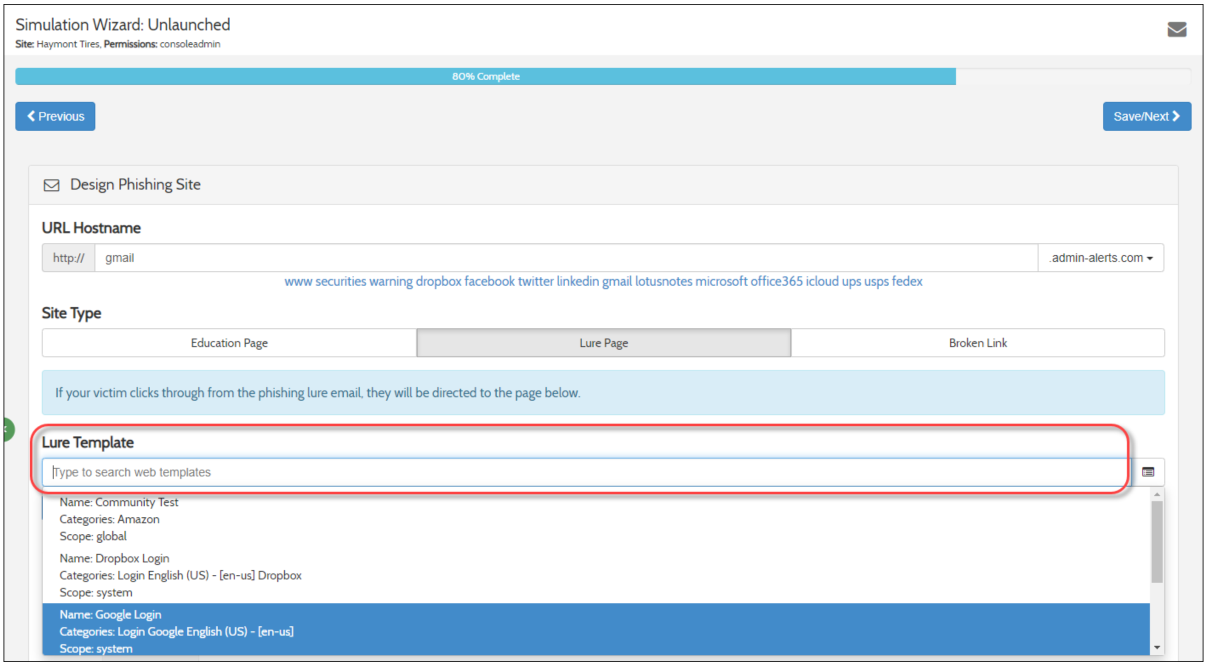
Fore more information, see Designing Phishing Sites on page 29.

To create a lure page:

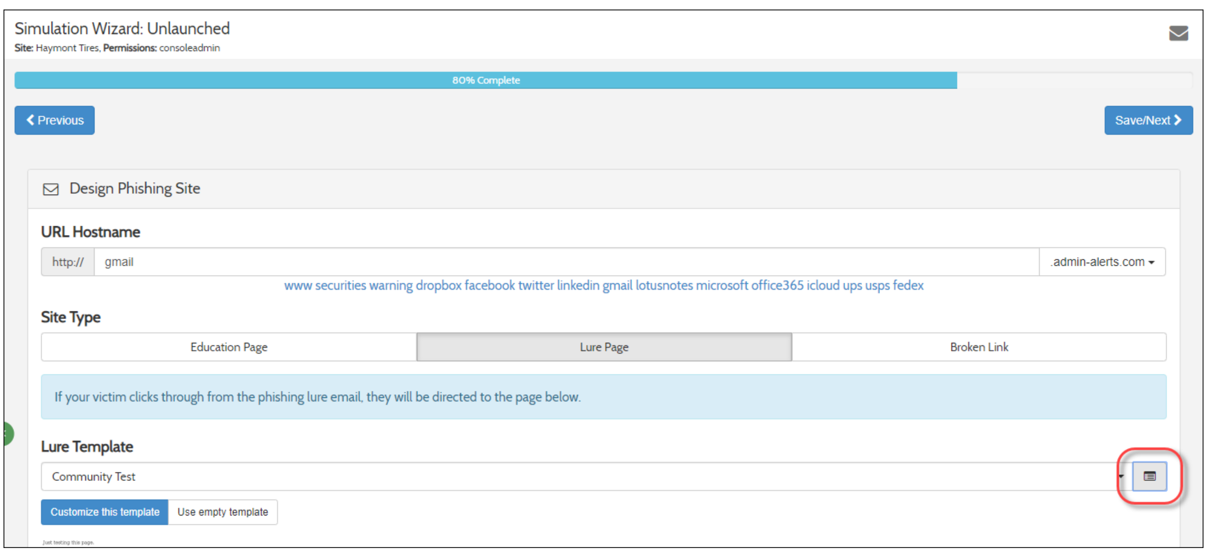
1. From the Design Phishing Site page, click the Lure **Page** button.



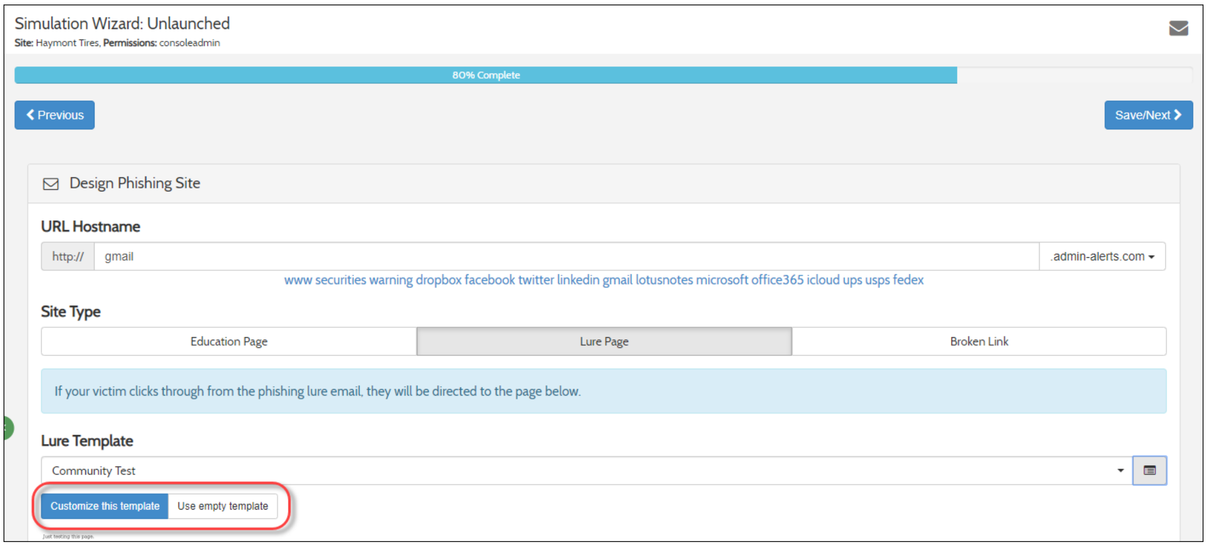
2. From the Lure Page drop-down menu, select a pre-formatted lure page.



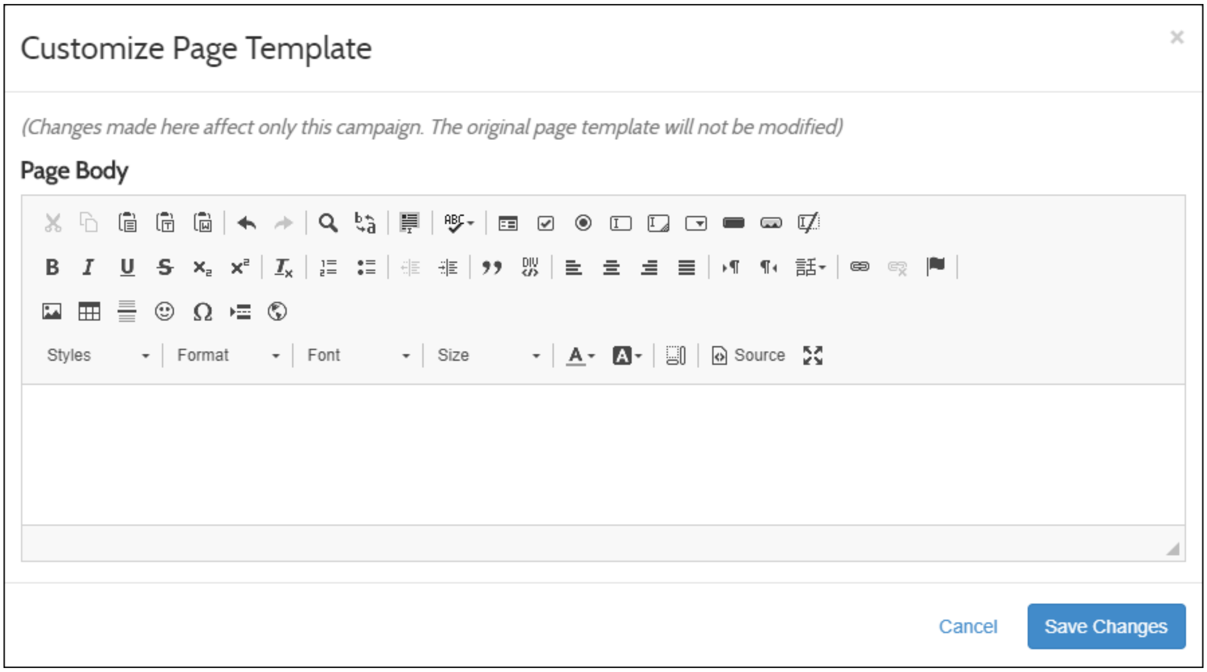
Alternately, you can click the **Browse** icon, and select your Lure page visually.



3. Do any of the following:
   - Use the lure template as is.
   - Click the **Customize this template** button to use the WYSIWYG editor to modify the template for your phishing email.
   - Click the **Use empty template** button to use the WYSIWYG editor to create a phishing email from scratch.



If you clicked the **Customize this template** button or the **Use empty template** button, the email WYSIWYG editor displays.



4. Use the editor to add or delete images, or to change and format the text.
5. When you're done, click the **Save Changes** button.

Designing Broken Link Pages

Follow this procedure when you've decided to design a Broken Links page where your targets will be taken when they click on a link in a phishing email.

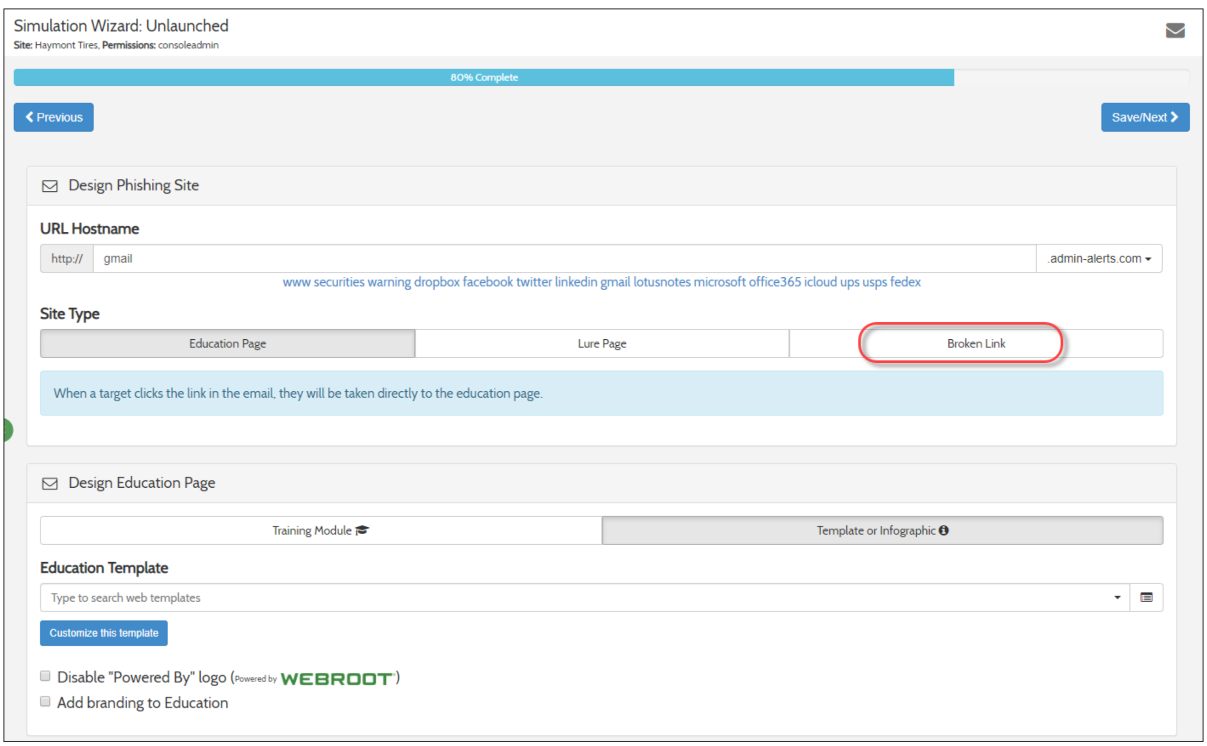
An Broken Links page is a page that displays what looks like a webpage that is a dead end, similar to a 404 page.

Fore more information, see Designing Phishing Sites on page 29.

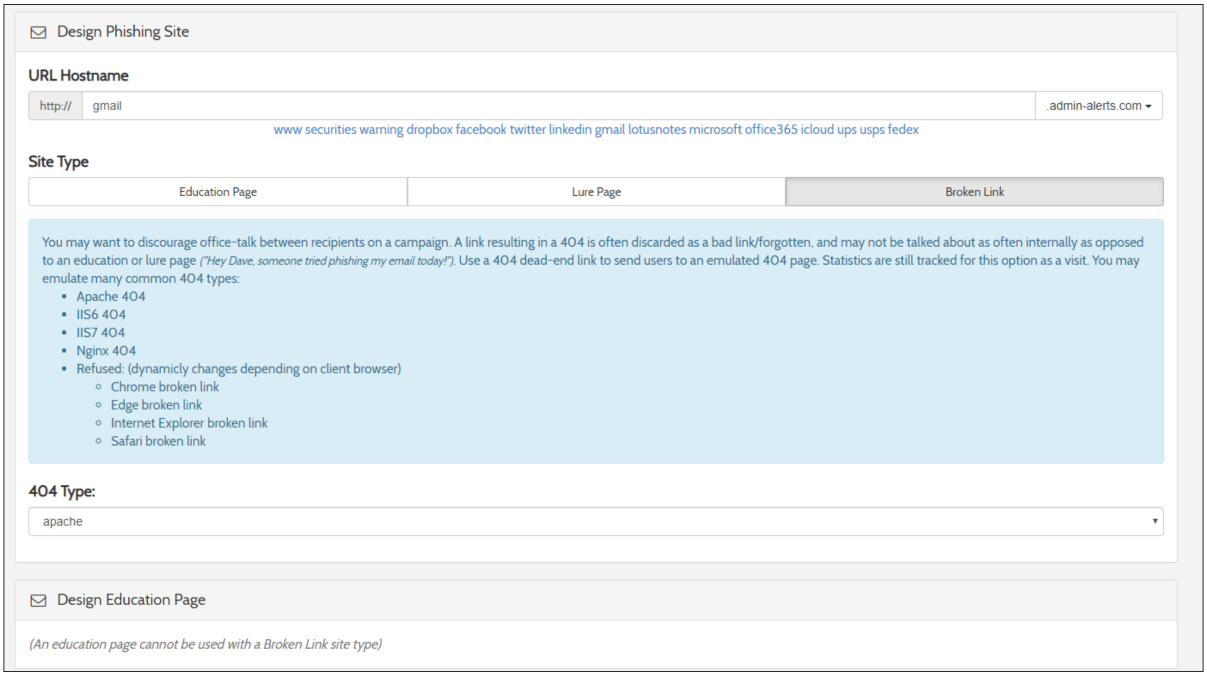
Note: An Education page cannot be used with a Broken Link page.

To create a broken link page:

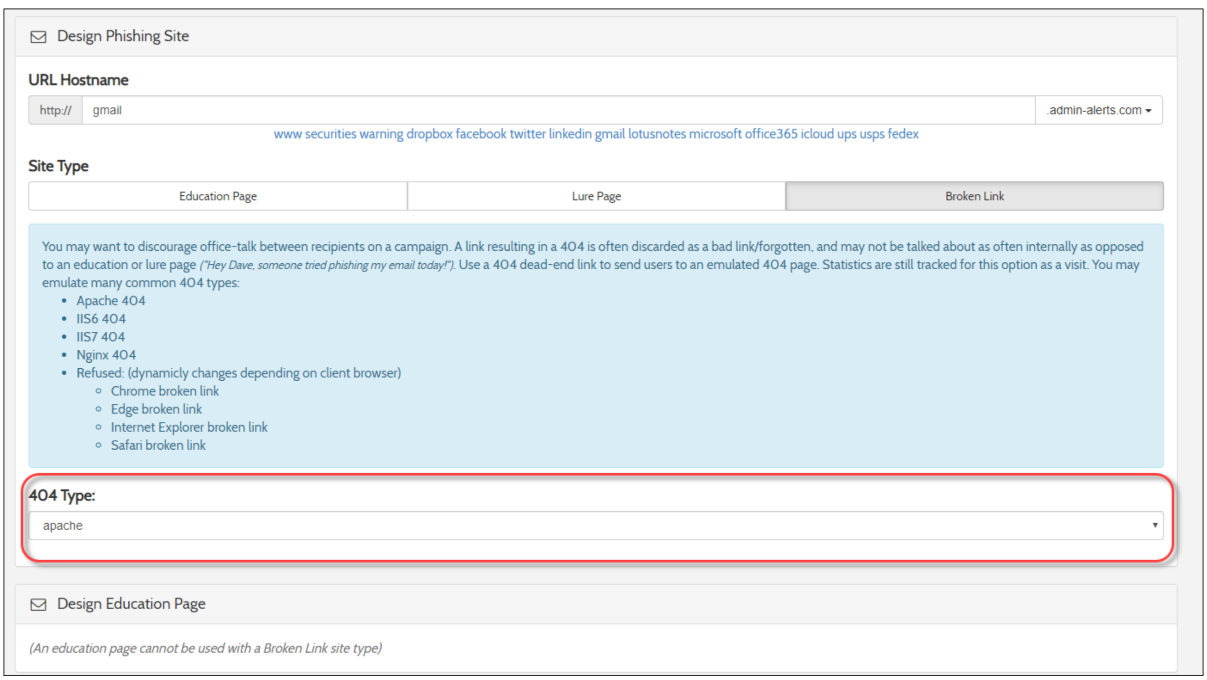
1. From the Design Phishing Site page, click the **Broken Link** button.



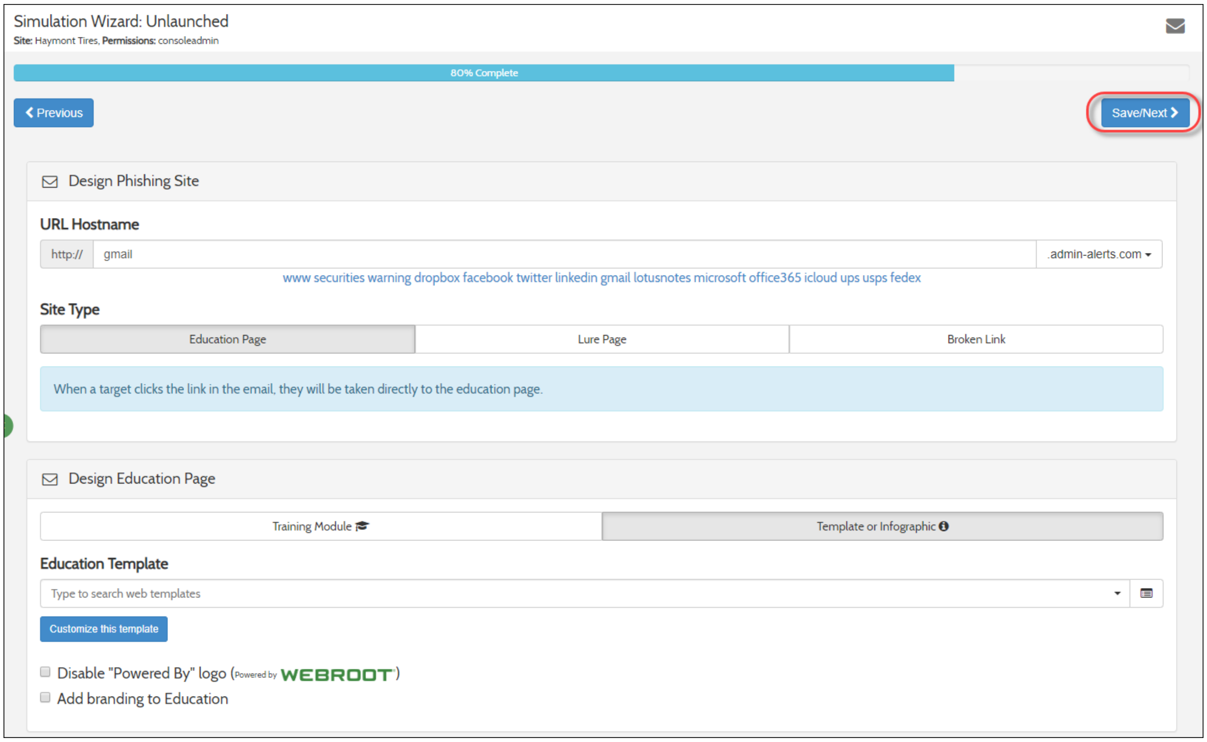
A list of broken link types displays.



2. From the 404 Type drop-down menu, select a broken link page type.



3. When you're ready, click the **Save/Next** button in the upper right corner.



4. Continue with Reviewing and Sending Phishing Simulations on page 60.

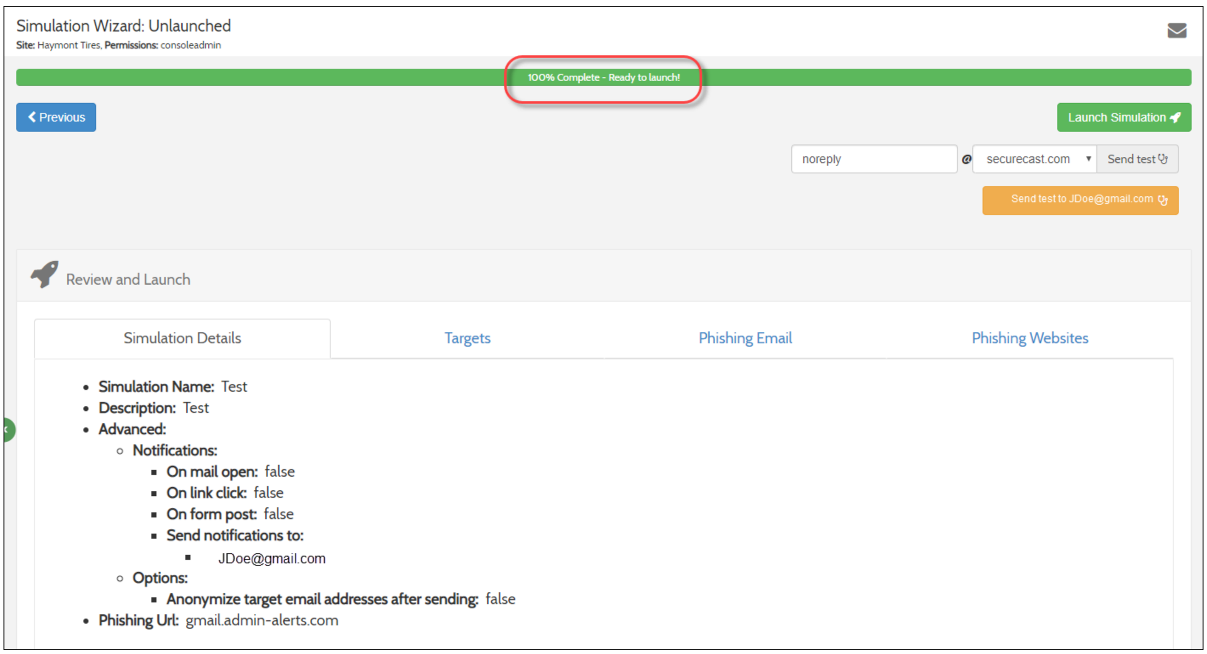
Reviewing and Sending Phishing Simulations

Once you've created and designed the parts of your phishing simulations, you are given a chance to review the simulation before you send it. Follow this procedure to review your phishing simulation.

For more information, see Creating Phishing Simulations on page 8.

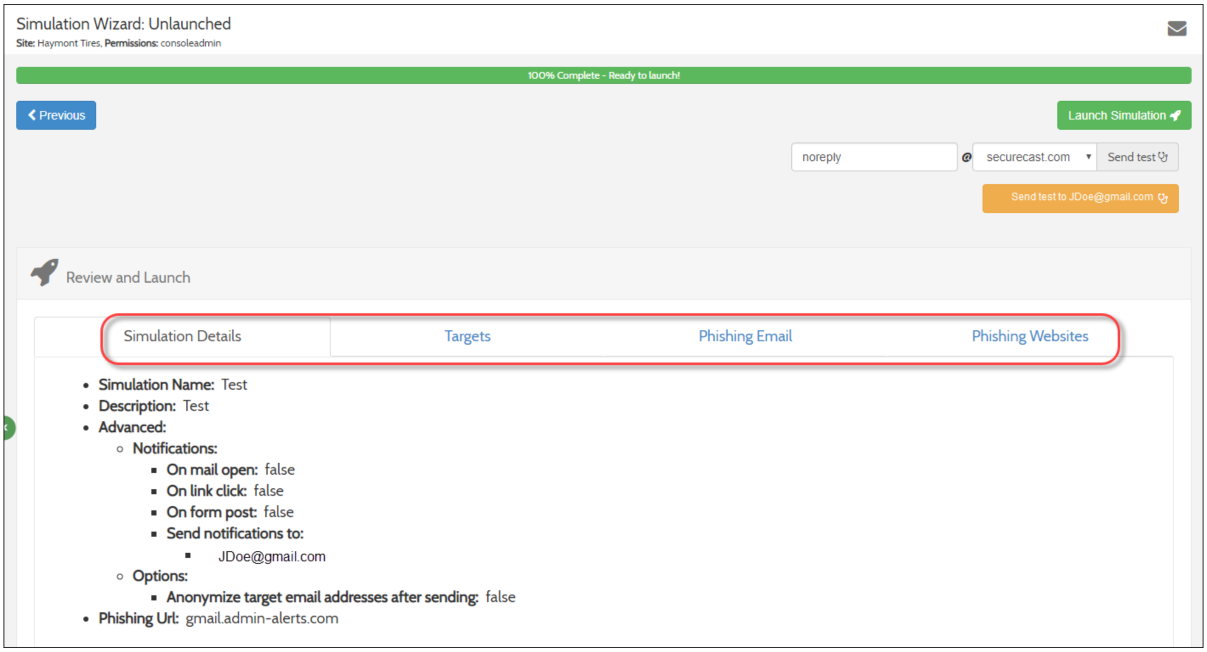
To review a phishing simulation:

1. Notice that at the top of the page, it indicates that you've completed 100% of the tasks needed to create a phishing simulation.

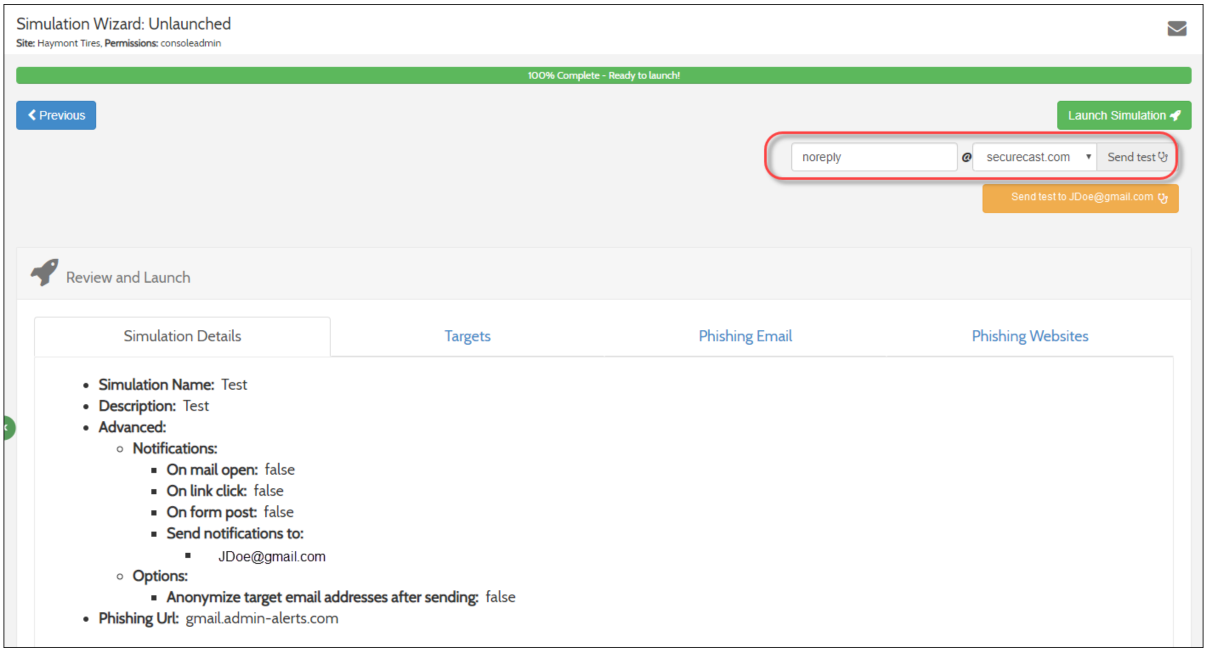


2. Select any of the following tabs to review your campaign settings before sending:
   - **Simulation Details** — Reflects the information you entered when you first created your phishing simulation. For more information, see Creating Phishing Simulations on page 8.
   - **Targets** — Reflects the targets you selected to send the phishing simulation to. For more information, see step 10 in Creating Phishing Simulations on page 8.
   - **Phishing Email** — Reflects the information you entered when you designed your phishing email. For more information, see Designing Phishing Emails on page 22.

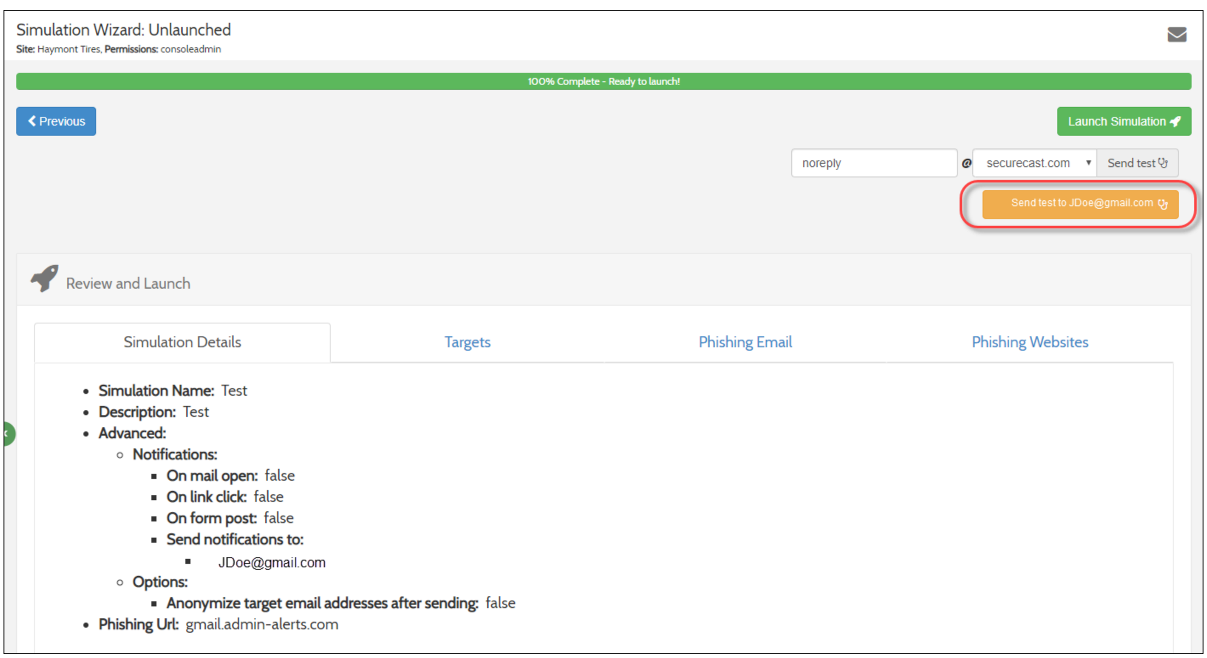
- **Phishing Websites** — Reflects the information you entered when you designed your phishing site. For more information, see Designing Phishing Sites on page 29.



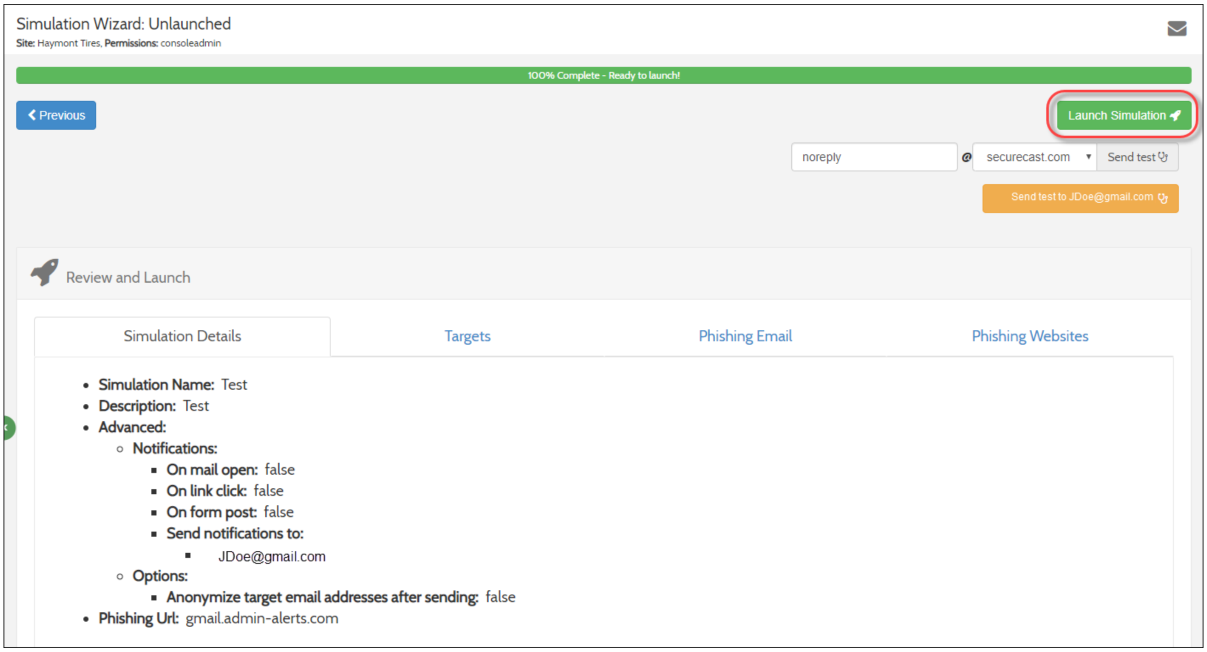
3. Optionally, you can enter the email address of another individual you would like to have review the simulation.



4. We recommend that you click the **Send test** button to send yourself a sample of your phishing email before launching your campaign.



5. When you're done, click the **Schedule Launch Simulation** button to launch your campaign.



6. To find out how your simulation went, see Accessing Training Reports on page 126.

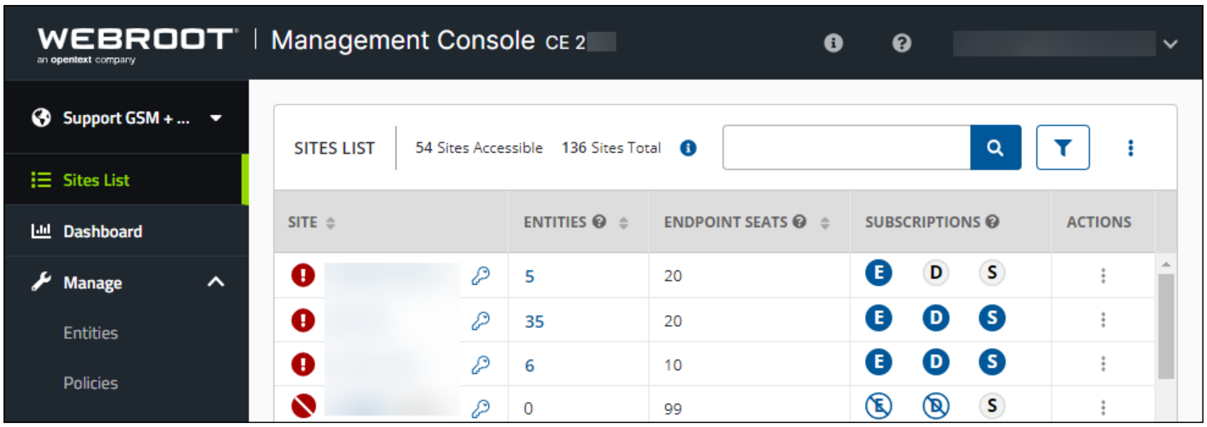
Selecting Sites in the Dashboard

Follow this procedure to select a specific site to work on while you are in the Security Awareness Training dashboard.

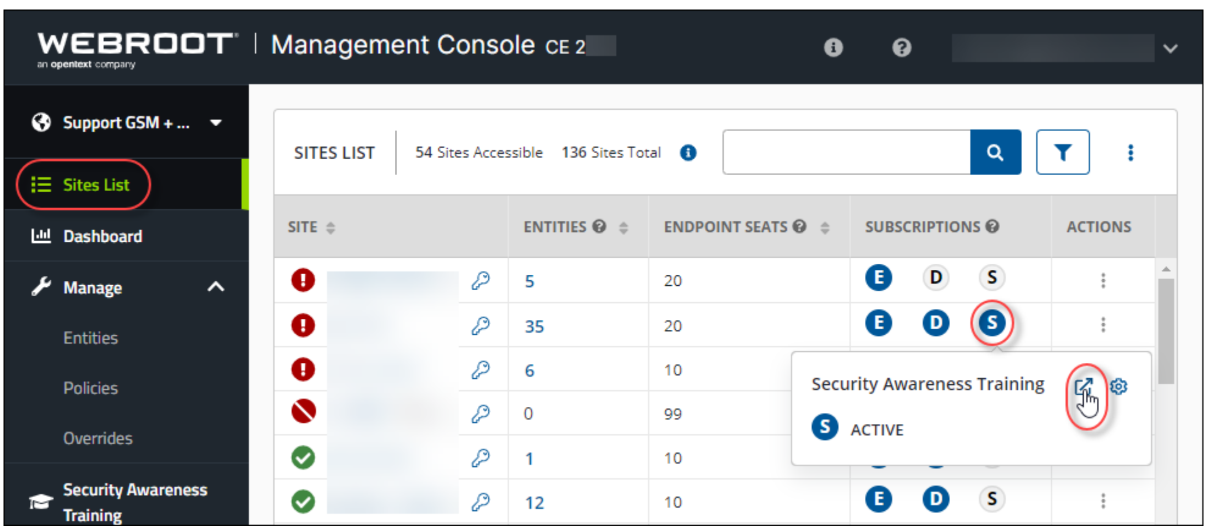
To select a site:

1. [Log in to the Management Console](#).

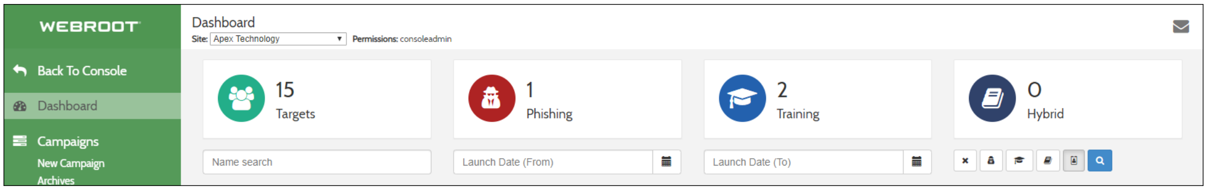
   The Management Console displays.



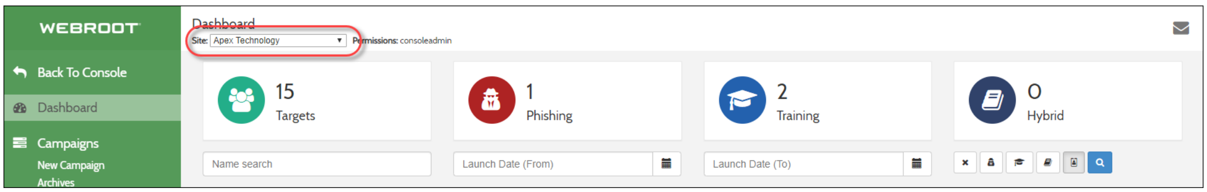
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



The Security Awareness Training console displays.



3. In the Site drop-down menu, select the site you want to work with.



The site you want to work with displays.

Chapter 3: Creating Training Sessions

To create training sessions, see the following topics:

Creating Training Campaigns Overview **67**
Selecting Trainees **68**
Designing Invitation Emails **75**
Designing Education Pages **78**

Creating Training Campaigns Overview

Training campaigns are used to invite trainees to take one of Webroot Security Awareness' pre-loaded training courses. Creating and launching a training campaigns includes the following steps:

- Selecting Trainees on page 68
- Designing Invitation Emails on page 75
- Designing Education Pages on page 78

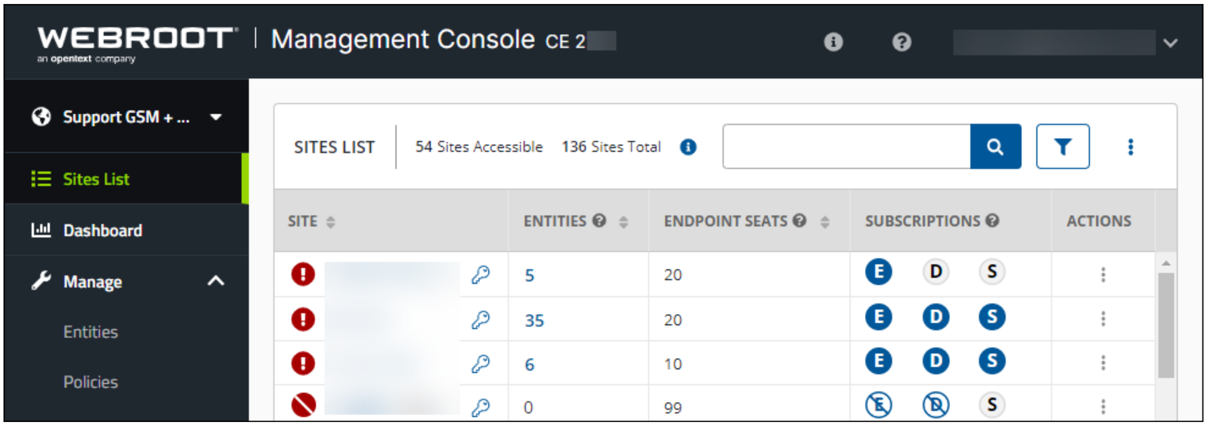
Note: You can send employees to a training campaign, even without sending them a phishing campaign.

Selecting Trainees

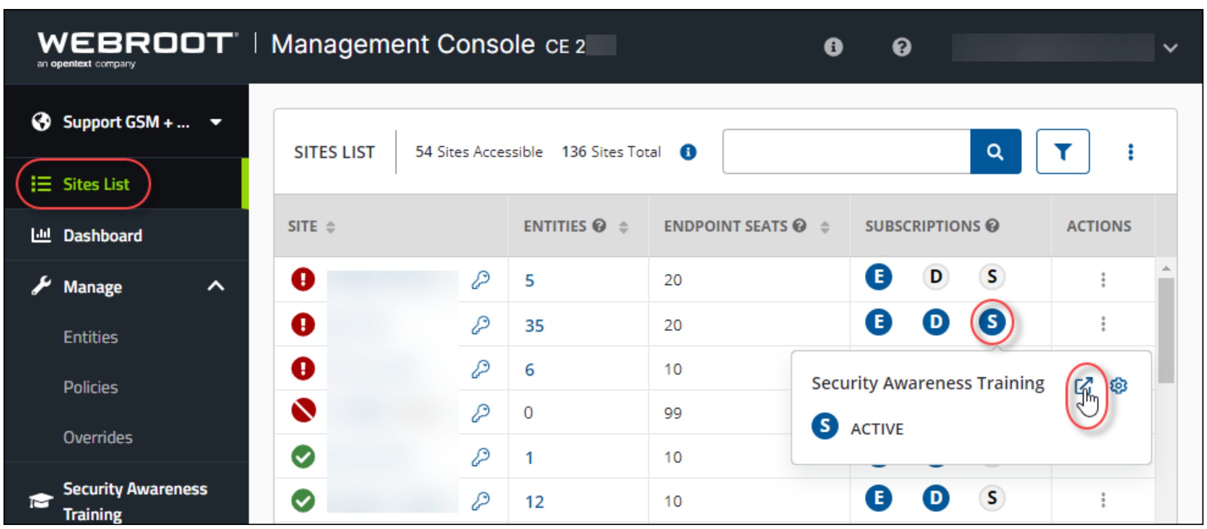
Use the following procedure to select trainees for training sessions.

To select a trainee:

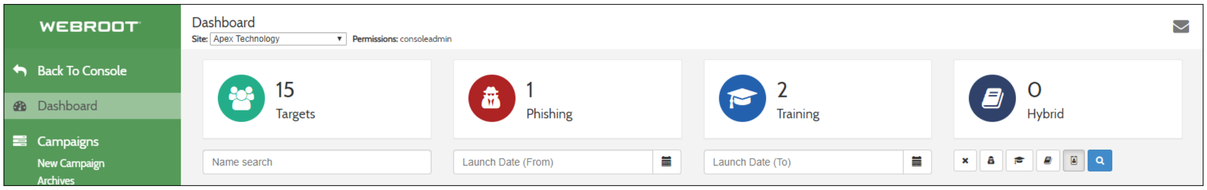
1. [Log in to the Management Console](#).



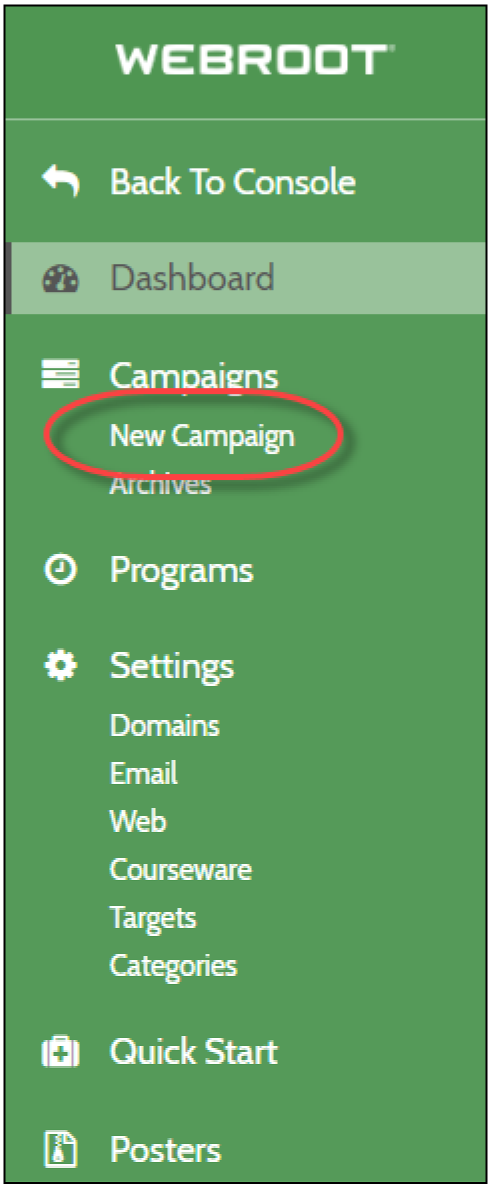
2. In the **Sites List** tab, choose a Site and click the **Go to Security Awareness Training** icon in the **Actions** column.



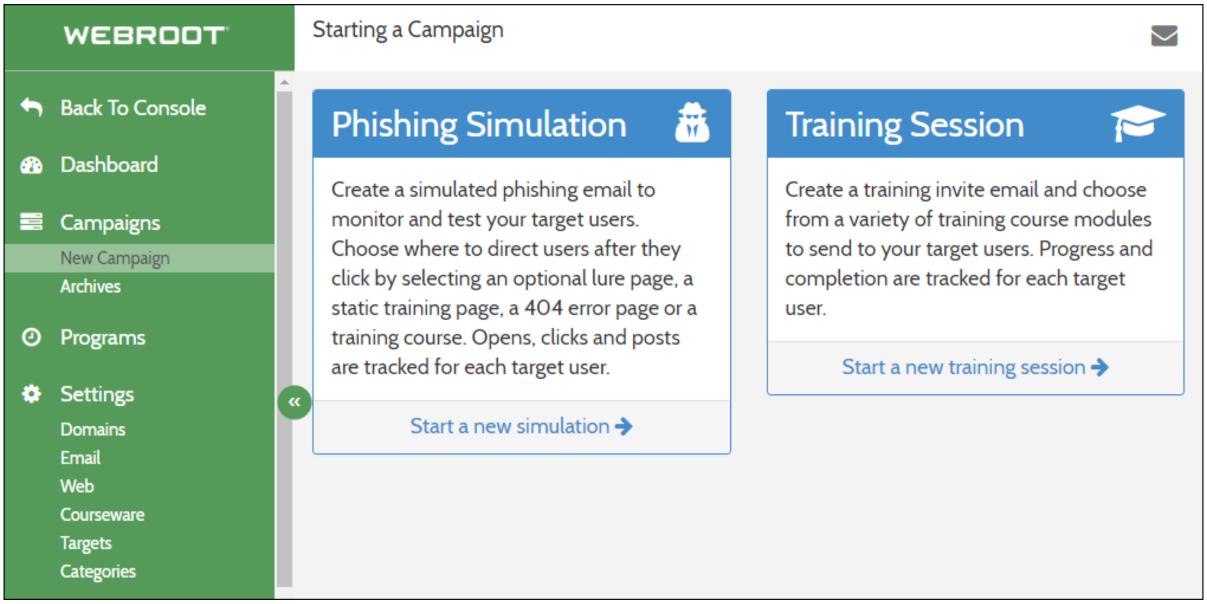
The Security Awareness Training console displays.



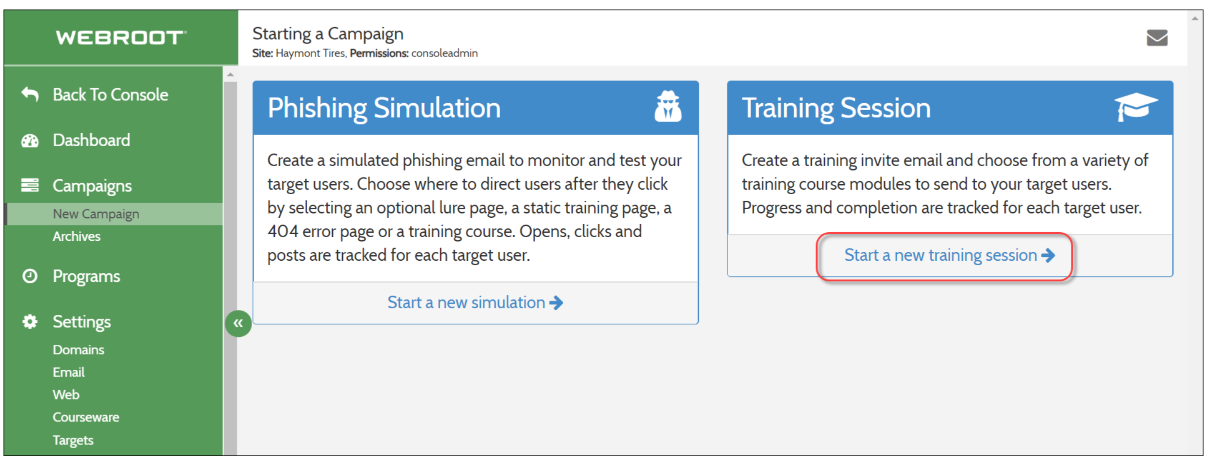
3. In the navigation pane, click **New Campaign**.



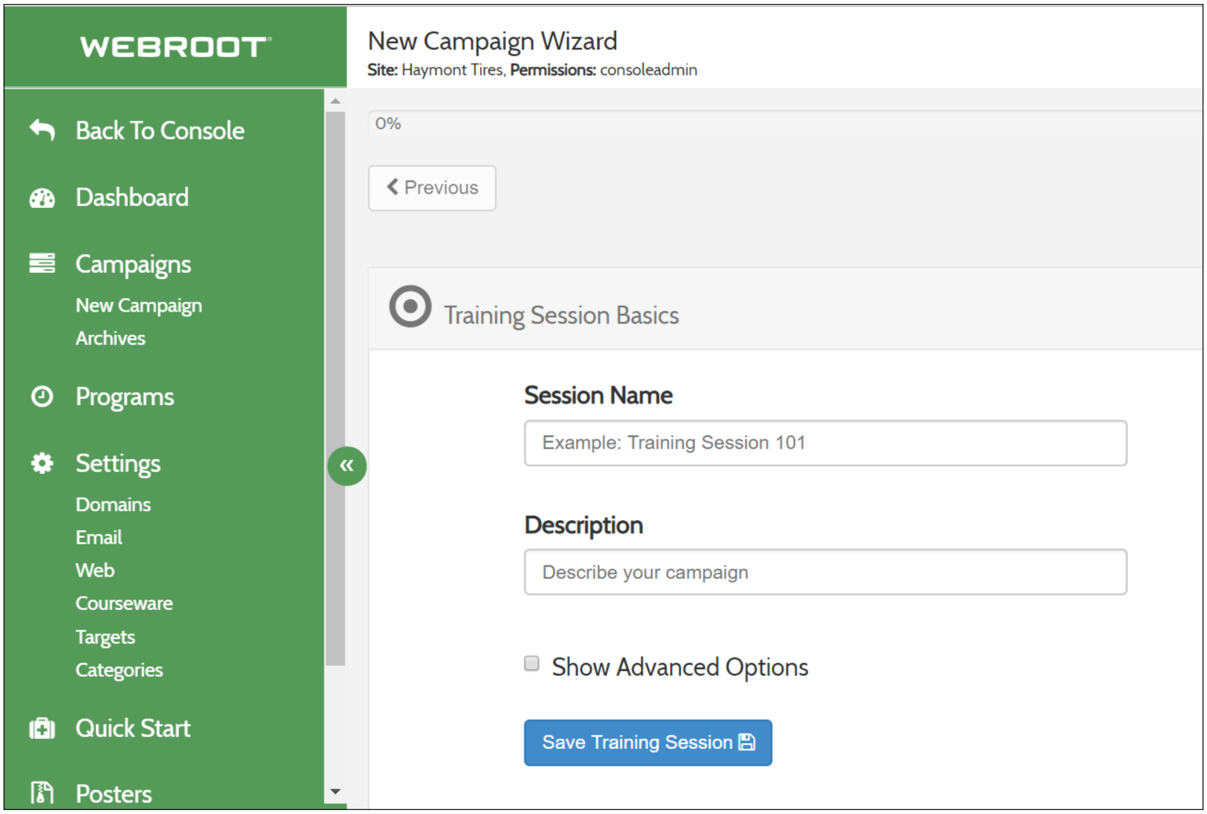
The **Starting a Campaign** panel displays.



4. Click **Start a new training session**.



The **New Campaign Wizard** displays.

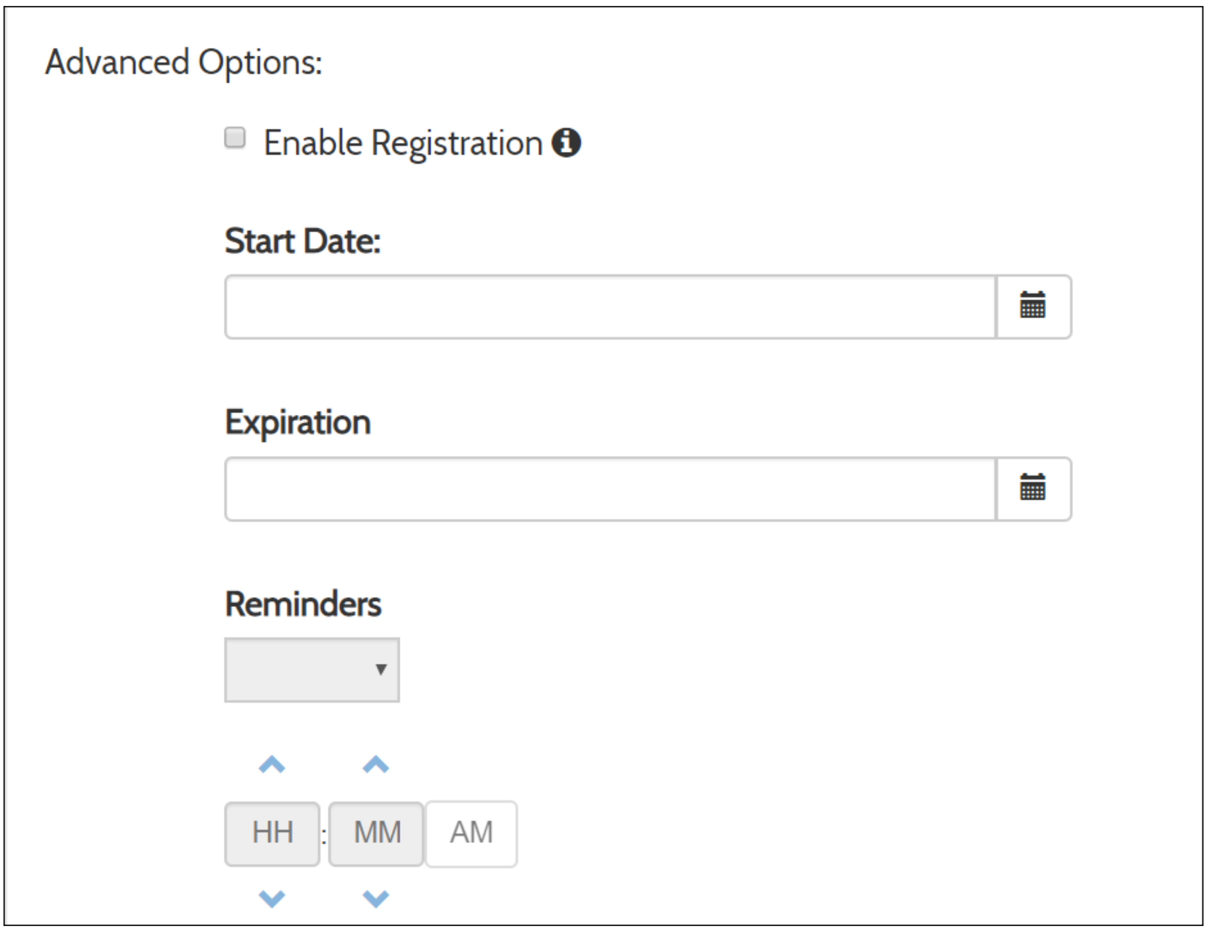


5. In the Training Session Basics area, populate the following fields:
   - **Simulation Name** — Enter a name for your simulation.
   - **Description** — Enter a description for your simulation. This is an optional step.
6. As needed, select the **Show Advanced Options** checkbox to display the advanced options area.

   The Advanced Options area displays.
7. In the Advanced Options area, populate the following fields:
   - **Enable Registration** —Provides a registration URL once you complete the setup of your course.
     - The URL link is unique to this course and can be used to register new users to the SAT service and to this course.
     - The URL can be posted to an internal website or sent out in a welcome email to new employees or those you wish to invite to the course.

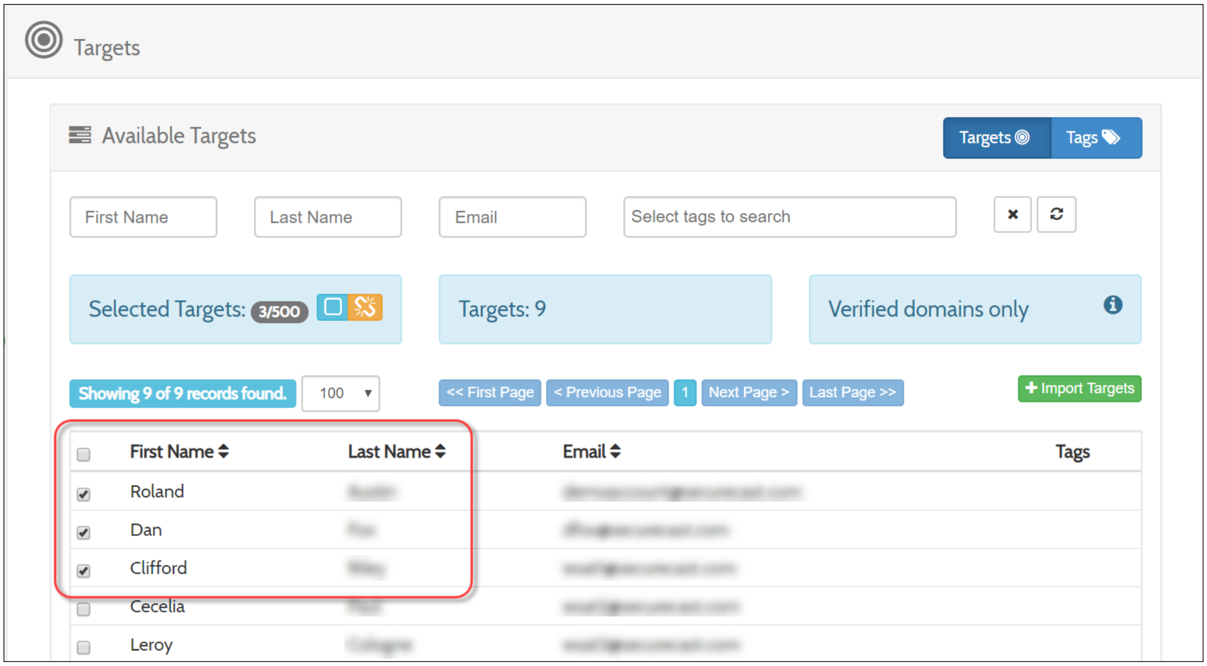
- Users who click the URL will be presented with a form prompting them to enter their email address to register for the course, which will then send an email invite to the user to take the course.

- **Start Date** — Enter a start date to schedule the launch of the campaign for a future date. If this is left blank, the campaign will start when you click the Launch button at the end of the wizard.
- **Expiration** — Enter the date when the campaign should be completed for reporting and reminder purposes. This date is optional and can be left open-ended.
- **Reminders** — Set to daily or weekly and are activated from the Expiration Date. Reminders are sent daily or weekly until the Expiration date is reached.

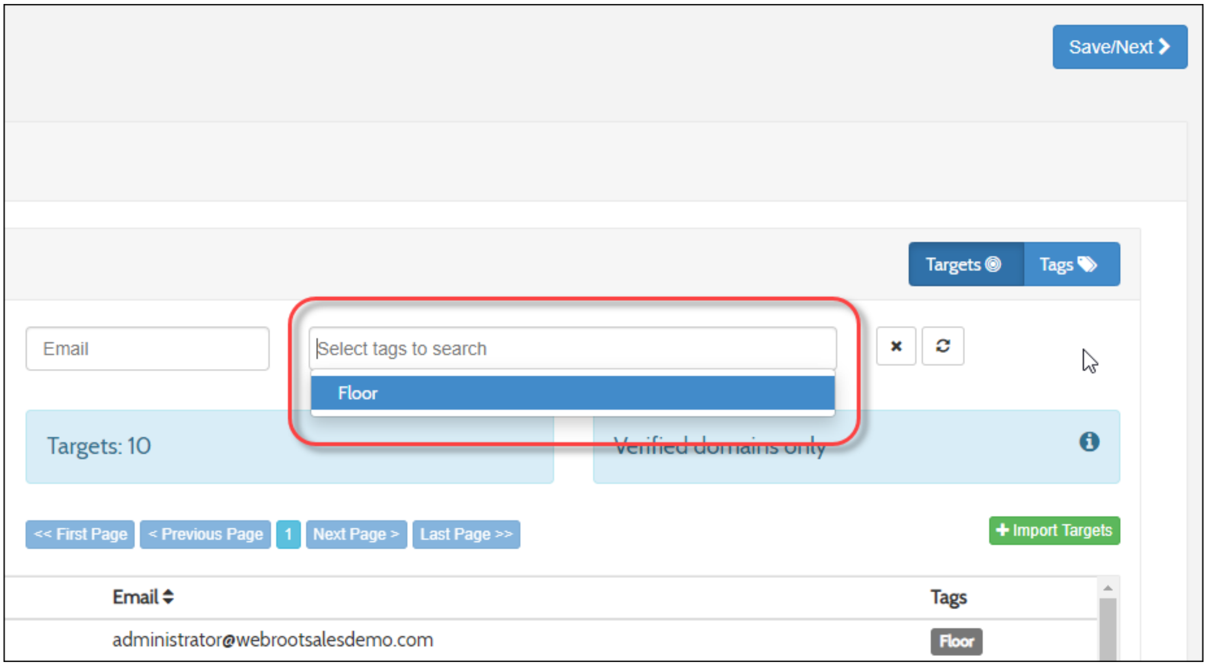


8. Click **Save Training Session**.
9. Click **Save/Next**.

10. On the next pane, do one of the following to determine the targets you would like to send the phishing simulation to:
    - Select one or more users by selecting the checkbox next to their name.



    - Click the **Tags** button and select users based on their tag. To do this, from the Select tags to search drop-down menu, select the tag of the users you want to send the email to. You can select multiple tags, as needed.



Note: For information on how to create tags so that they display in the drop-down menu, see Importing Targets on page 179.

11. When you are finished, click **Save/Next**.

    Next, see topic Designing Invitation Emails on page 75.

Designing Invitation Emails

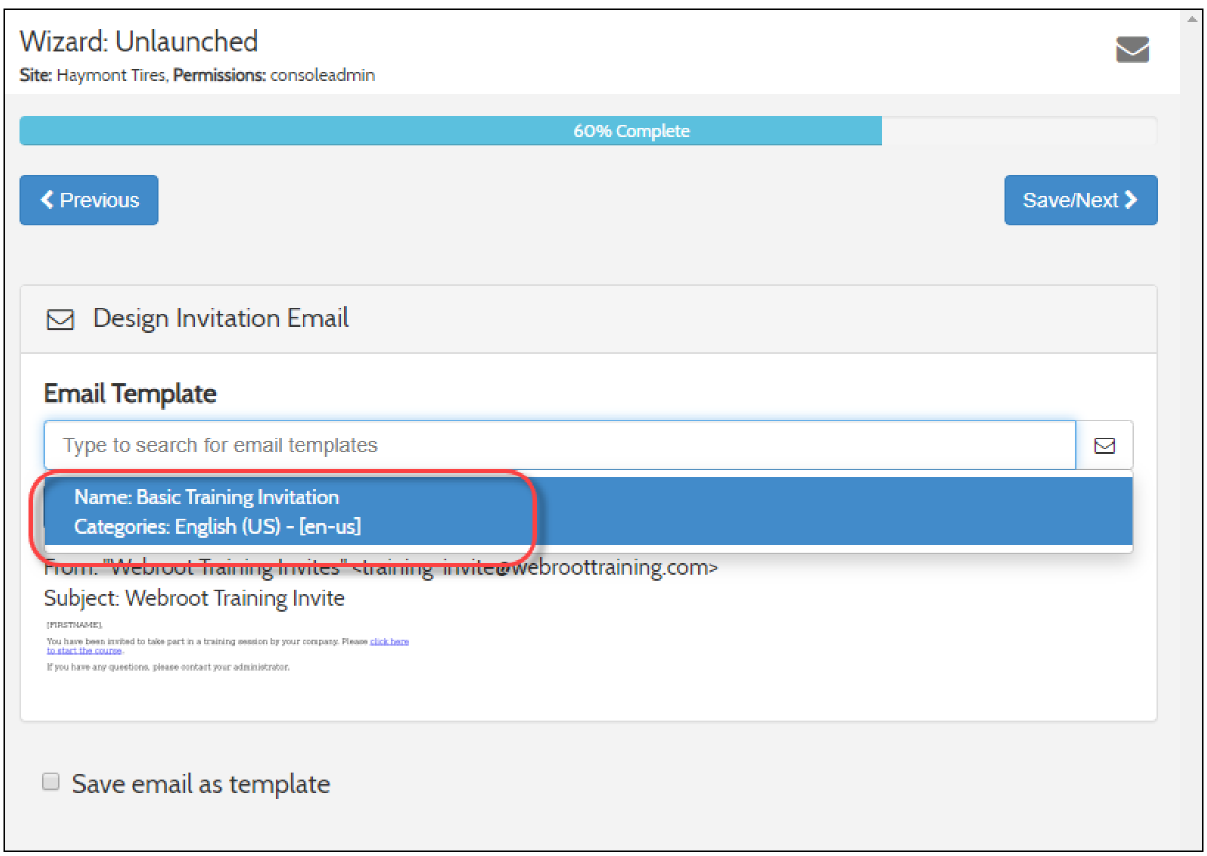
Note: You need to have invited trainees before you design your invitation emails. For more information, see Selecting Trainees on page 68.

Once you select trainees for your training program and are ready to create a training invitation email, you can either:

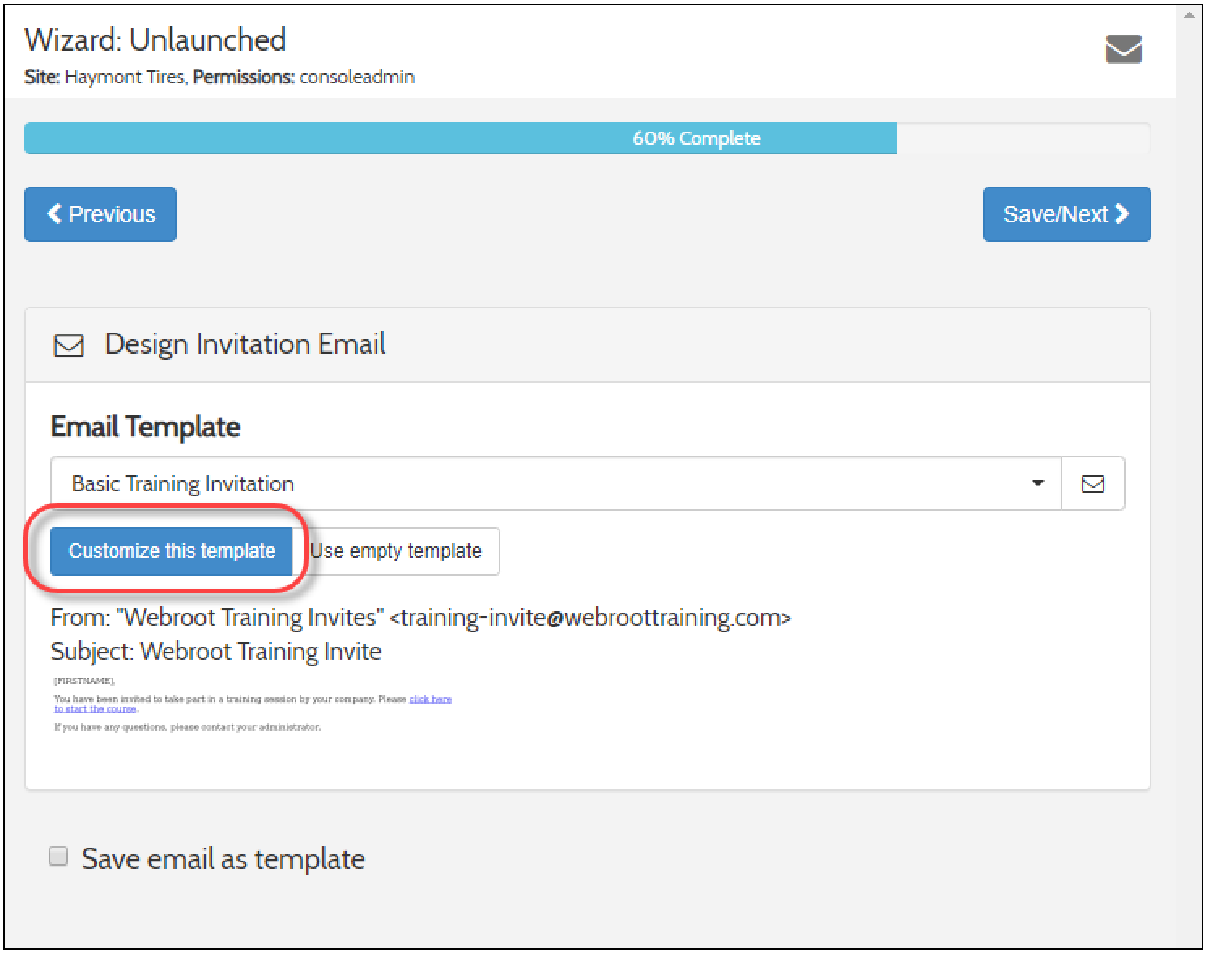
- Use a pre-built Basic Training Invitation template, as is.
- Use a WYSIWYG editor to customize the Basic Training Invitation email.

To create an invitation email:

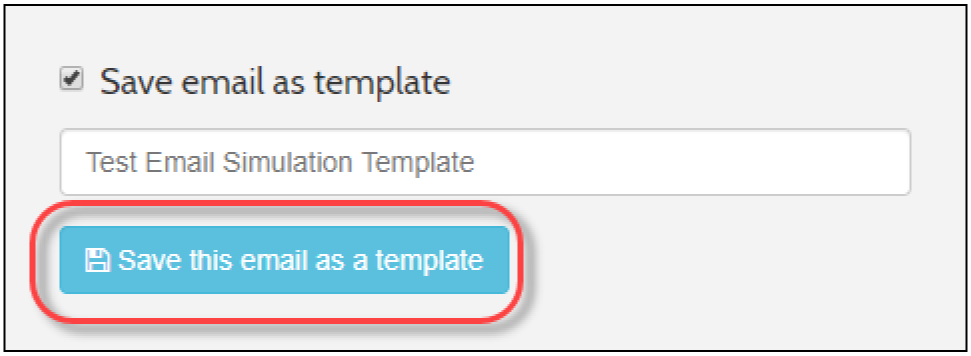
1. From the Email Template drop-down menu, select a phishing email from one of the default templates.



2. Click **Customize this template** to use the WYSIWYG editor to modify your training email, as needed.



> **Note:** You can save your customized templates for future use by selecting the **Save email as template** checkbox, naming the custom template, then clicking the Save this email as a template button.



The **Customize Email Template** window displays.

3. Fill out the following fields:
   - From Name
   - From Address
   - Subject
4. In the Email Body area, enter information or instructions to complete the phishing scenario.
5. Use the WYSIWYG editor to configure and customize your text.
6. Enter variables as needed. Variables include:
   - **[FIRSTNAME]** — Replaces the variable with the recipient's first name.
   - **[LASTNAME]** — Replaces the variable with the recipient's last name.
   - **[EMAIL]** — Replaces the variable with the recipient's email.
7. Click the **Save Changes** button.
8. When you are finished, click **Save/Next**.

   For the next step, see topic Designing Education Pages on page 78.

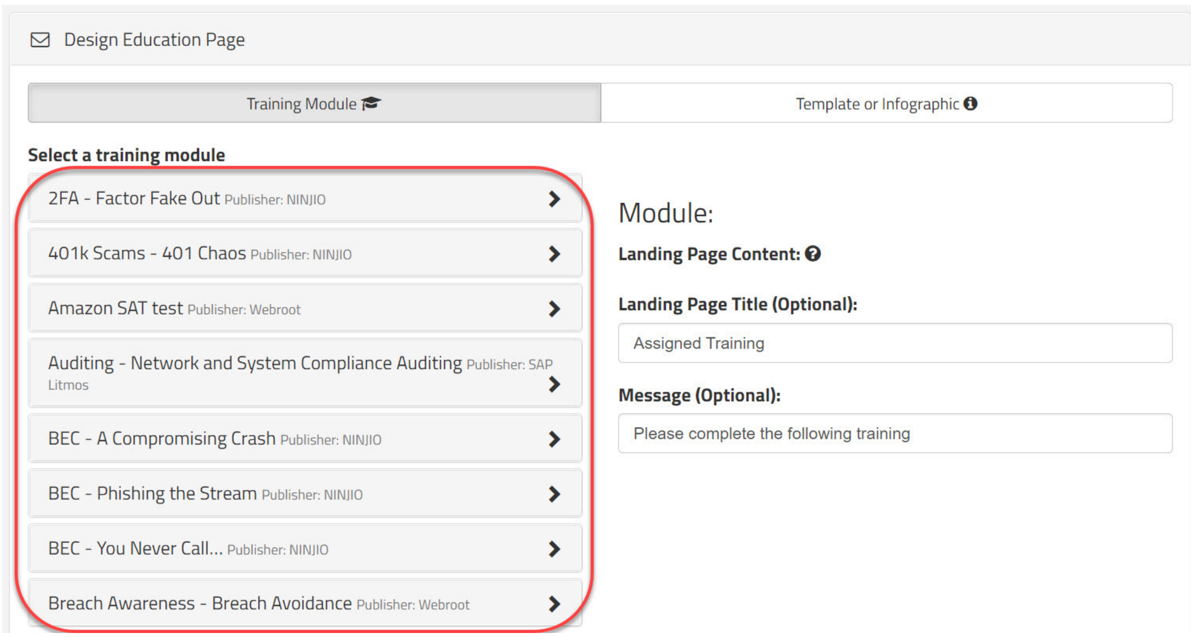
Designing Education Pages

Follow this procedure to design an education page.

Note: You must first have completed the task of Designing Invitation Emails on page 75.

To design an education page:

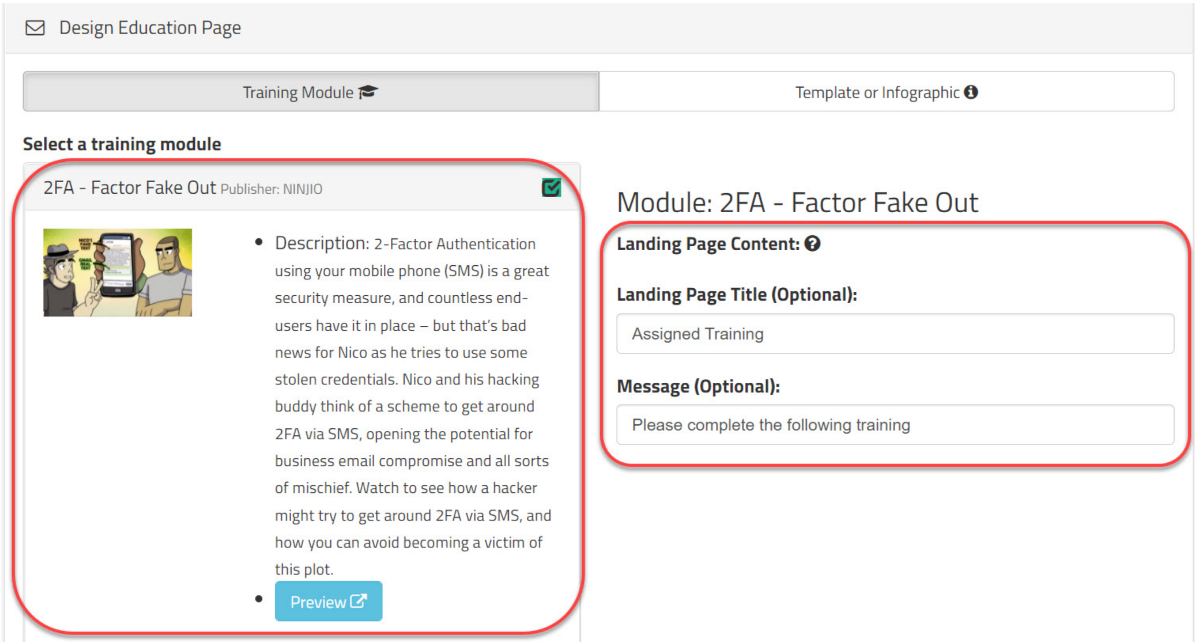
1. From the list, select a training module.



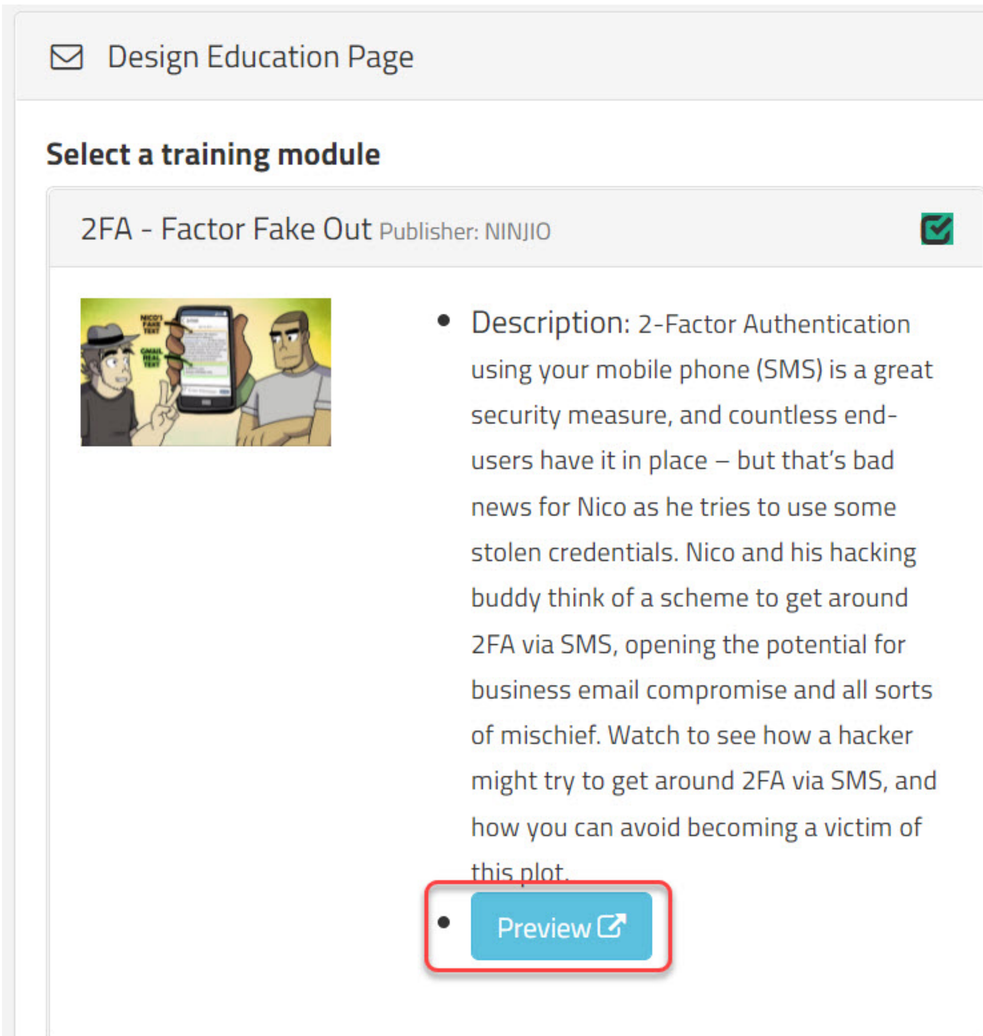
When you select a module; the following occurs:

- The training module panel expands to display information about the module.
- The **Landing Page Content** page displays, which allows you to add an optional

title and message that will be shown on the training landing page.

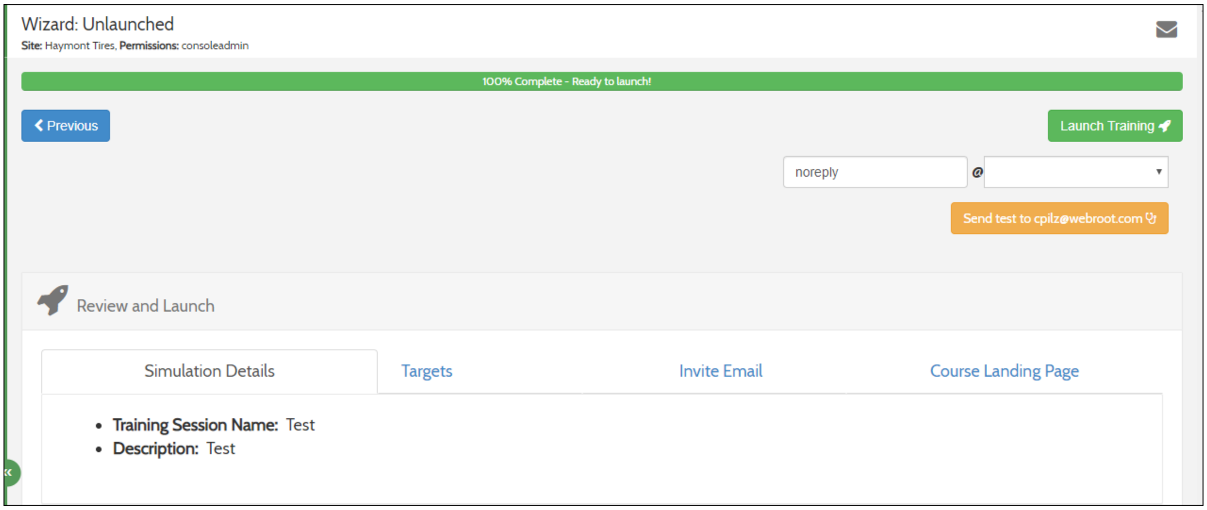


2. To view the training module, click the **Preview** button.

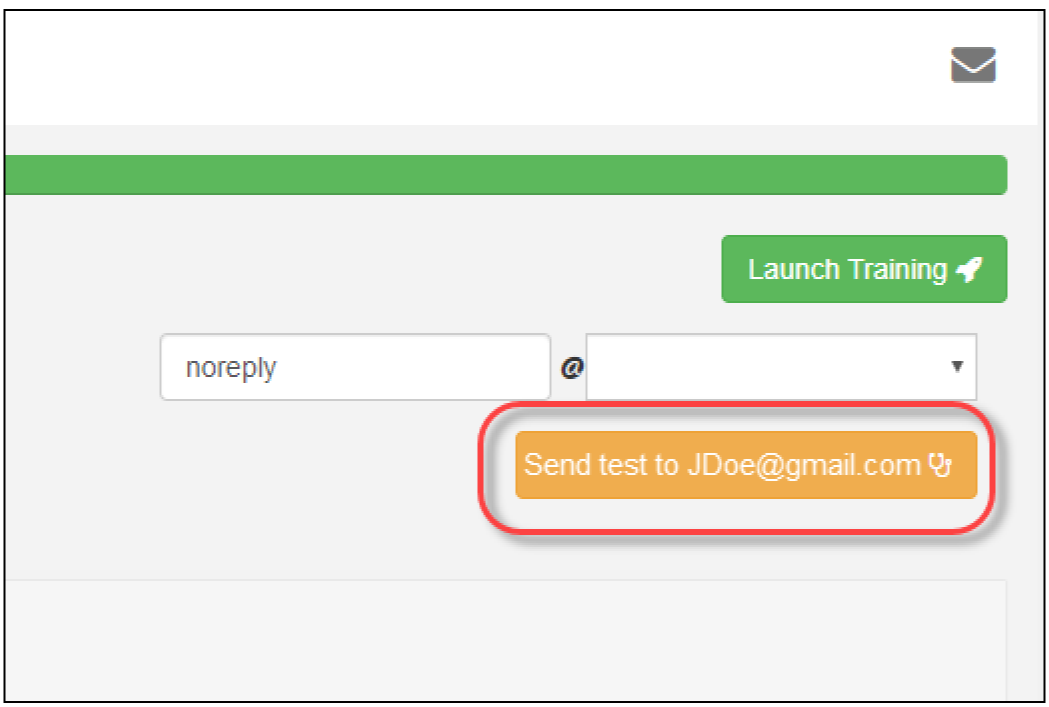


3. When you are finished, click **Save/Next**.

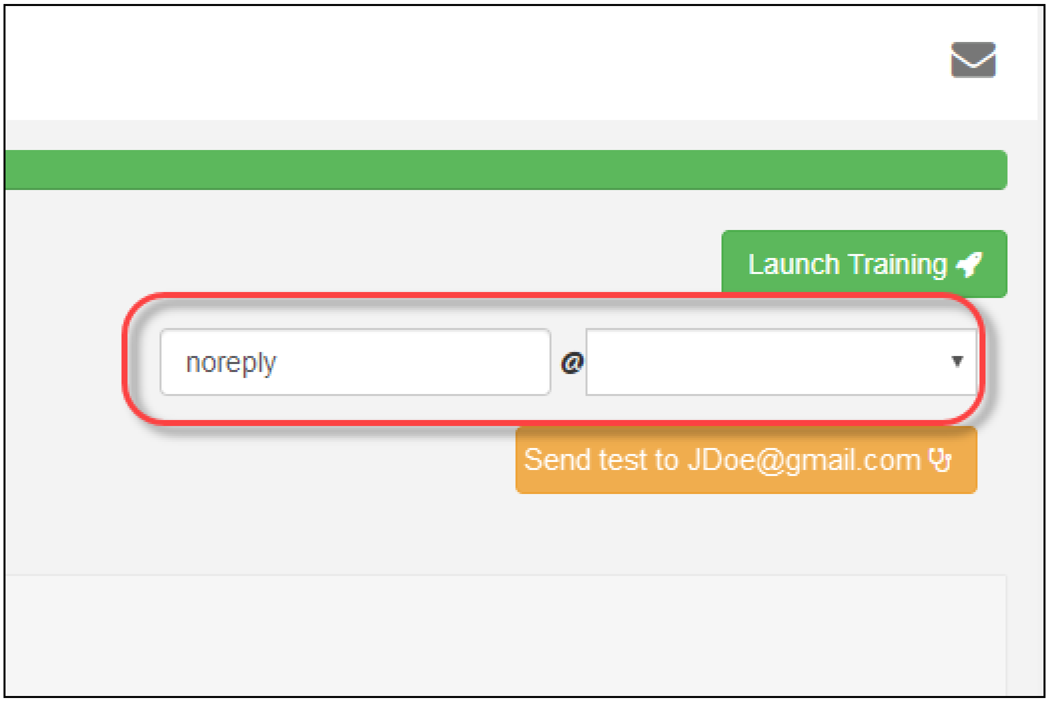
   The Review and Launch panel displays.



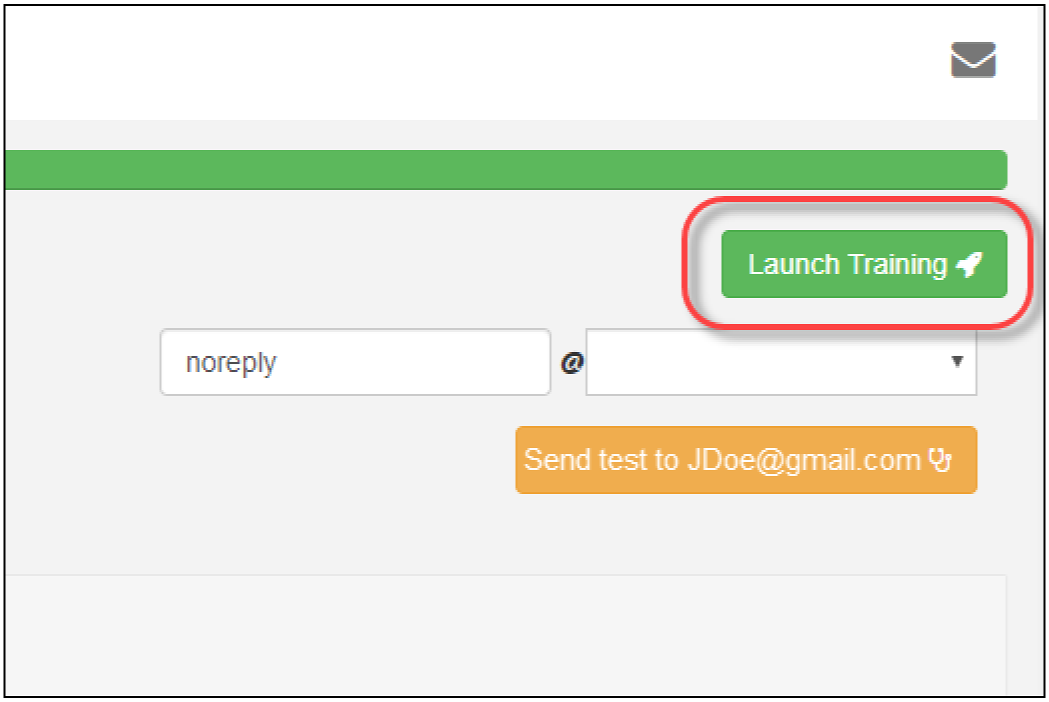
4. Before you launch the training, we recommend that you do the following:
   - Review your settings.
   - Send a test invitation to yourself ensure you are satisfied with the look and feel of the training invitation and training landing page.



- Send out a test invitation to another individual for review.



5. When you are ready to send out your invitations to your targets, click the **Launch Training** button.


Launch Training
noreply
@
Send test to JDoe@gmail.com

Chapter 4: Working With Programs and Campaign Scheduling

To start working with programs and campaign scheduling, see the following topics:

Programs And Campaign Scheduling Overview **85**
Sending Welcome Emails **86**
Scheduling Phishing Campaigns **98**
Creating Training Campaigns **105**
Sending Campaign Summary Reports **111**
Understanding Email Types **112**

Programs And Campaign Scheduling Overview

Programs is a feature that allows you to schedule multiple campaign tasks with the goal of helping automate your training program. Tasks available for scheduling include:

- Sending Welcome Emails on page 86
- Scheduling Phishing Campaigns on page 98
- Creating Training Campaigns on page 105
- Sending Campaign Summary Reports on page 111
- Sending Welcome Emails on page 86

Sending Welcome Emails

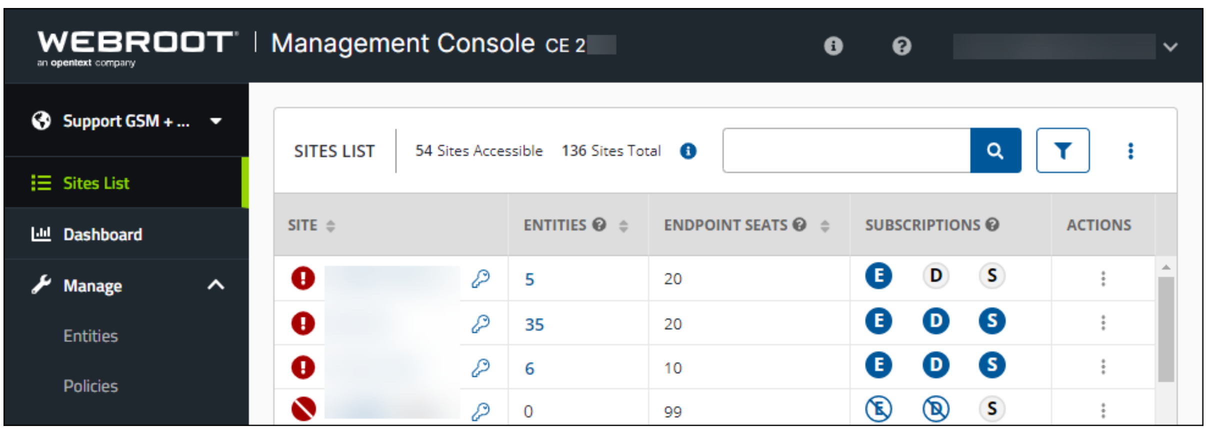
Welcome Emails are generally used for sending out an introduction to your new Security Awareness program to end users, management, IT staff, etc.

- You can use the Welcome Email task as the first introductory email to your users or consider scheduling it after your first Phishing Campaign to introduce Security Awareness after a baseline phishing simulation has been run.
- Welcome Email is a template type and can be created, edited and managed under the Settings tab in the Menu bar.
- This email task can be scheduled at a date and time you specify.

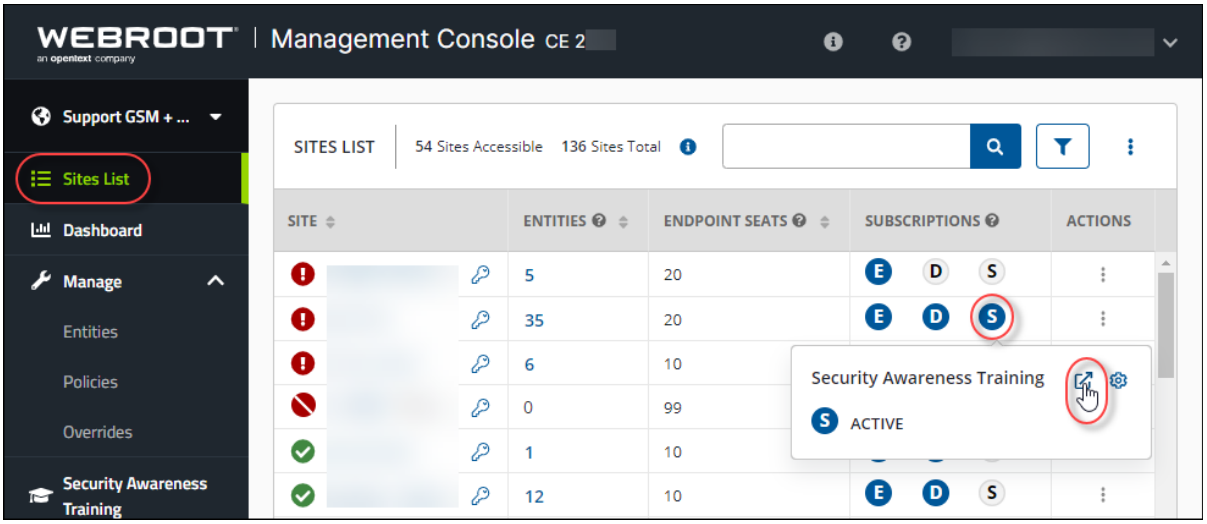
To send a Welcome Email:

1. [Log in to the Management Console](#).

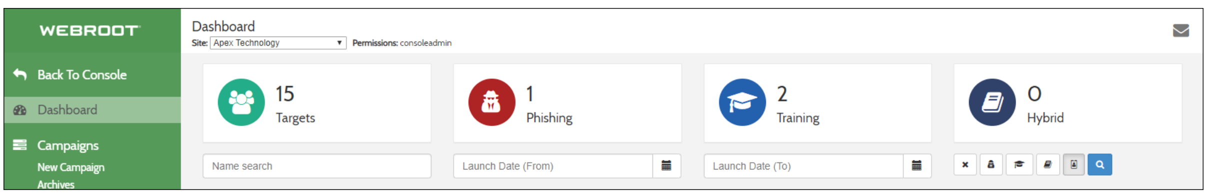
   The Management Console displays.



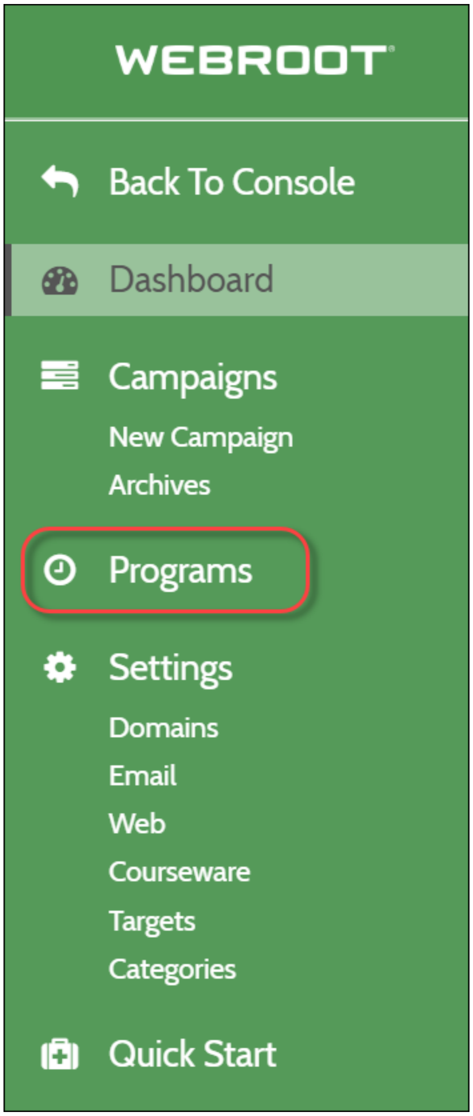
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



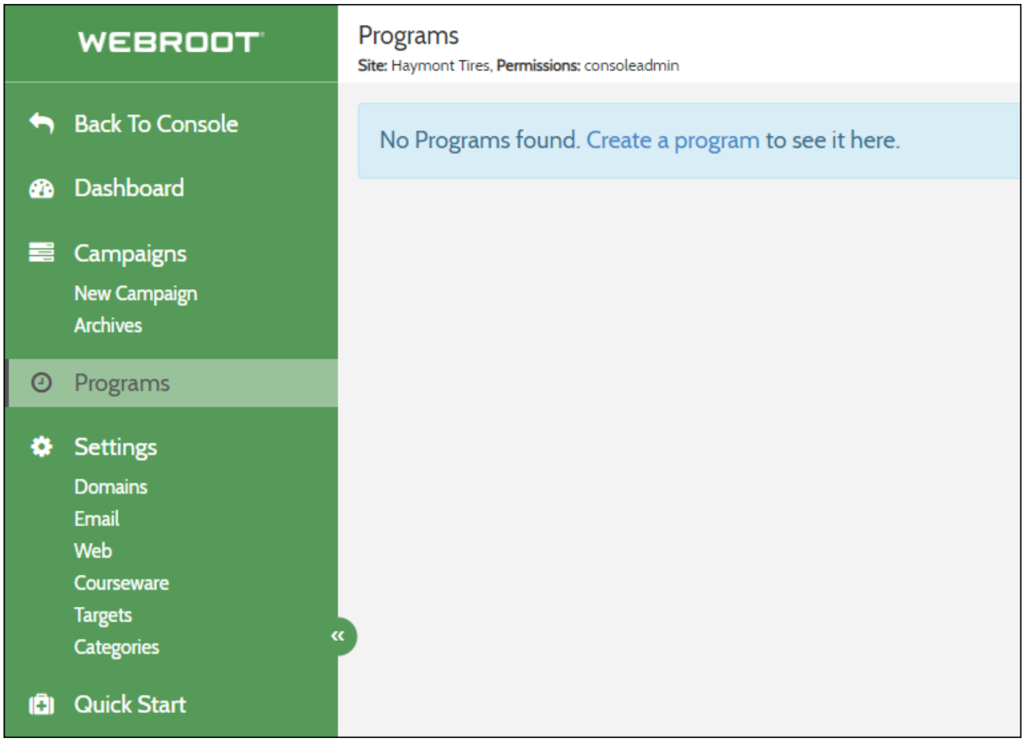
The Security Awareness Training dashboard displays.



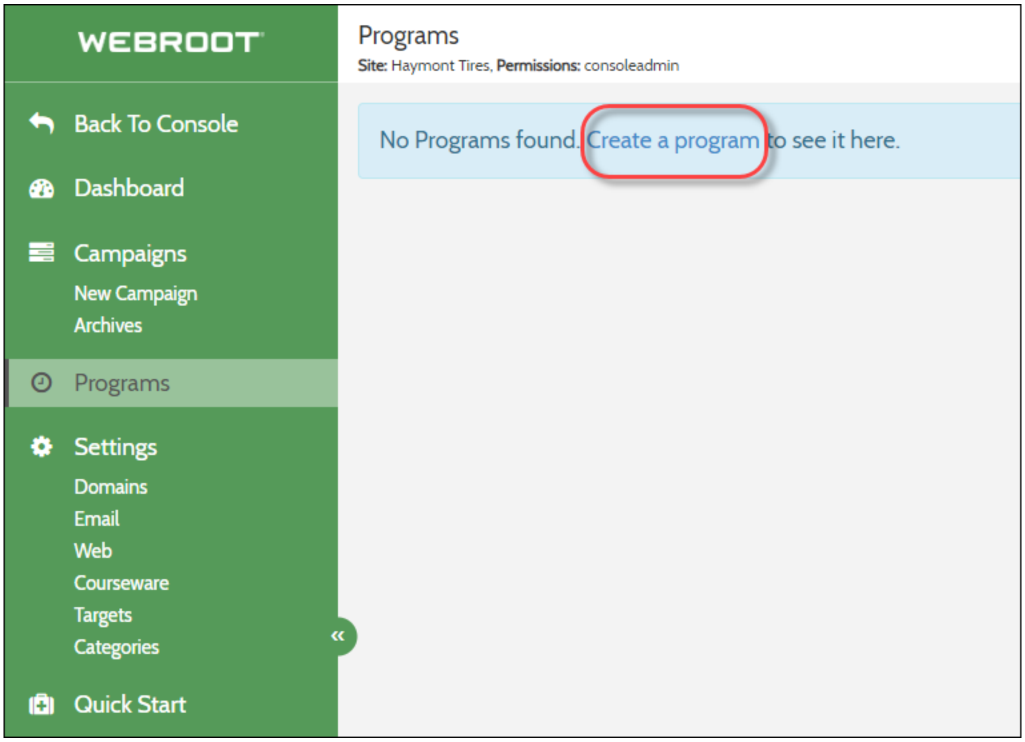
3. In the Nav bar, click the **Programs** tab.



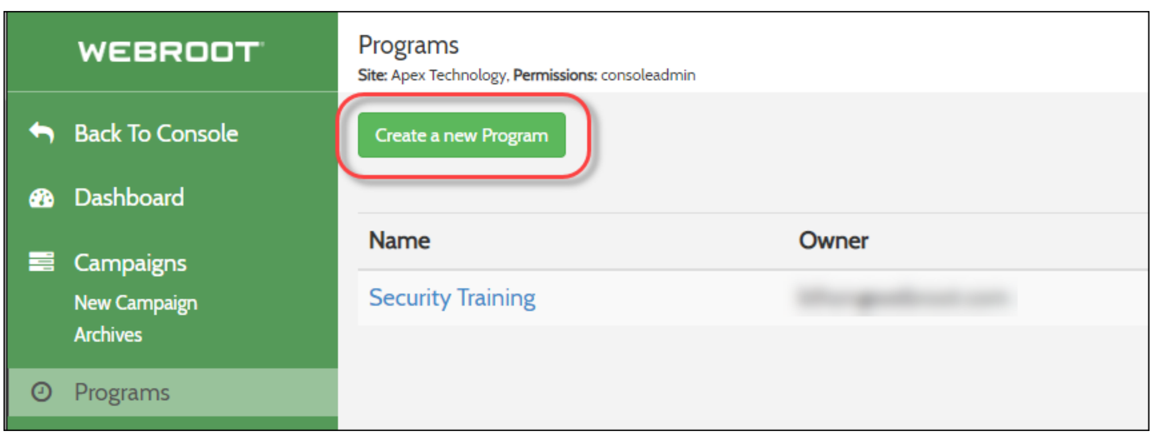
The Programs panel displays.


WEBROOT
Programs
Site: Haymont Tires, Permissions: consoleadmin
Back To Console
Dashboard
Campaigns
New Campaign
Archives
Programs
Settings
Domains
Email
Web
Courseware
Targets
Categories
Quick Start
No Programs found. Create a program to see it here.

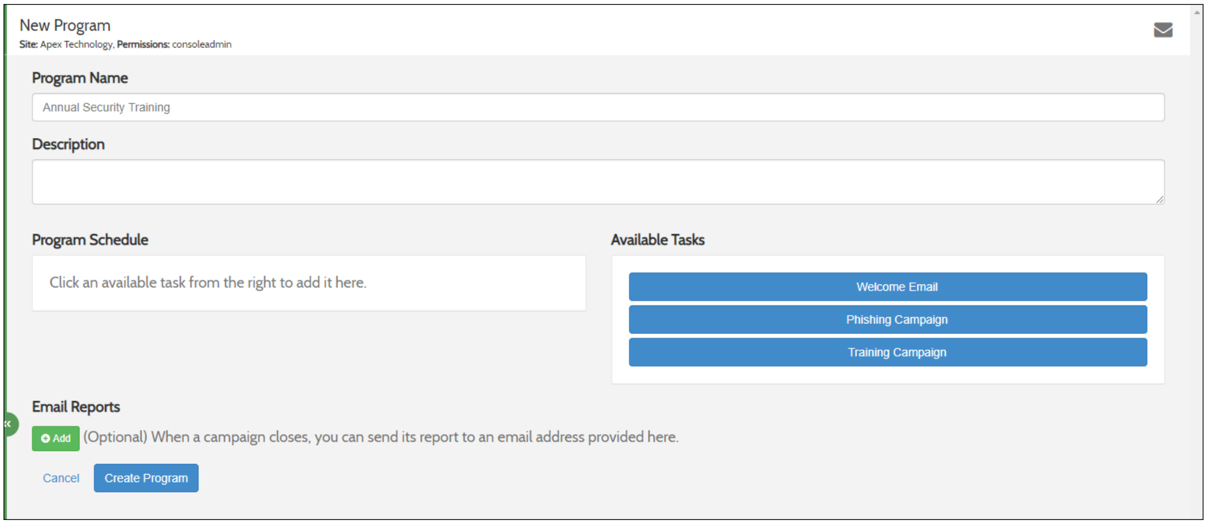
4. Do one of the following:
   - If this is the first program you're creating, click the **Create a program** link.



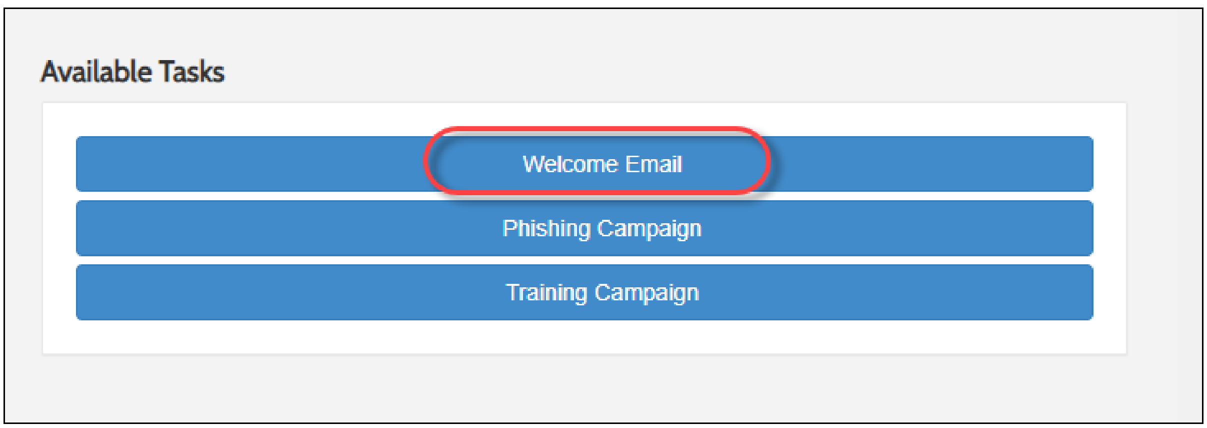
   - If this is not the first program you're creating, click the **Create a new Program** button.



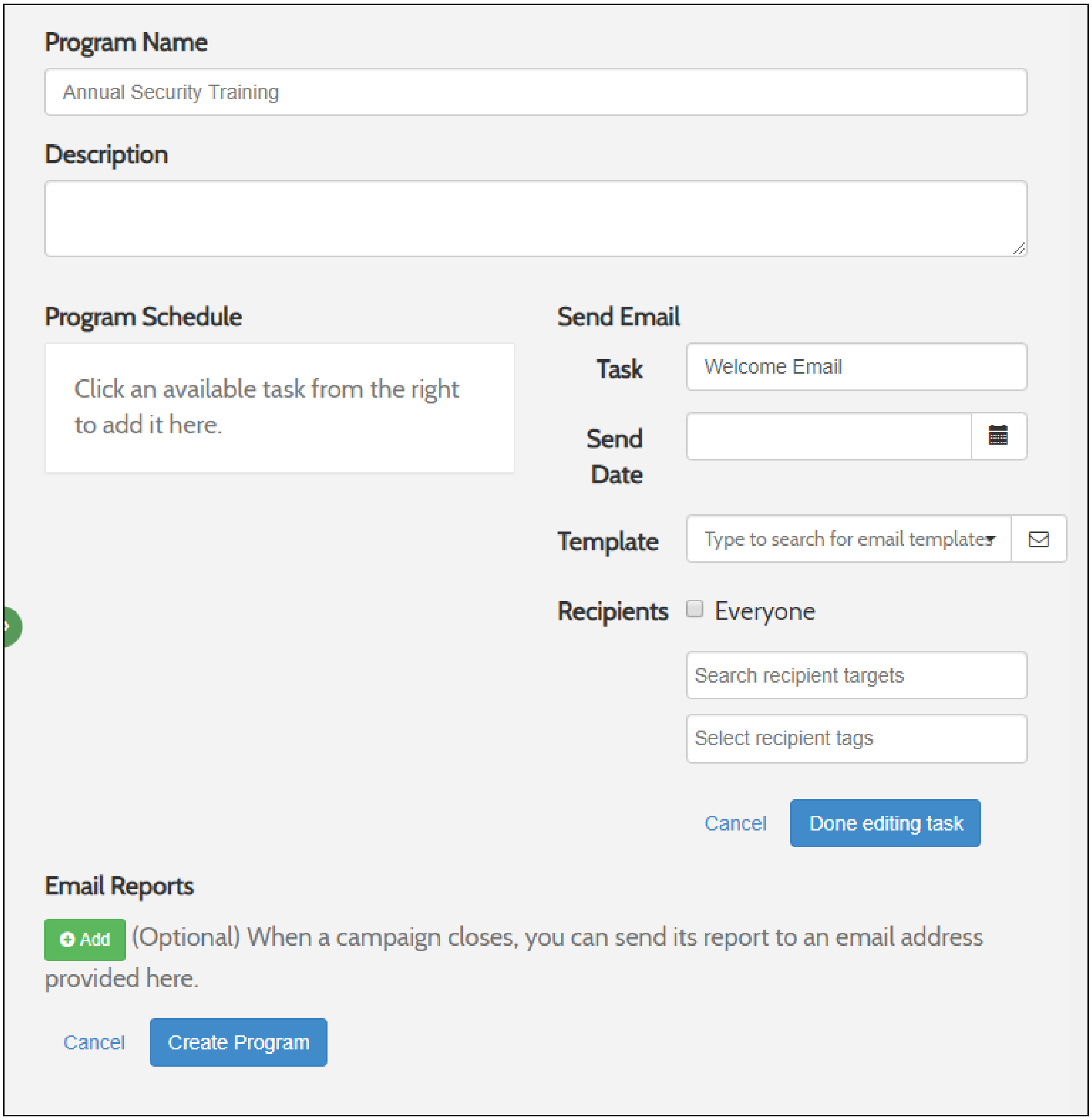
In either case, the New Program panel displays.



5. Click the **Welcome Email** button.



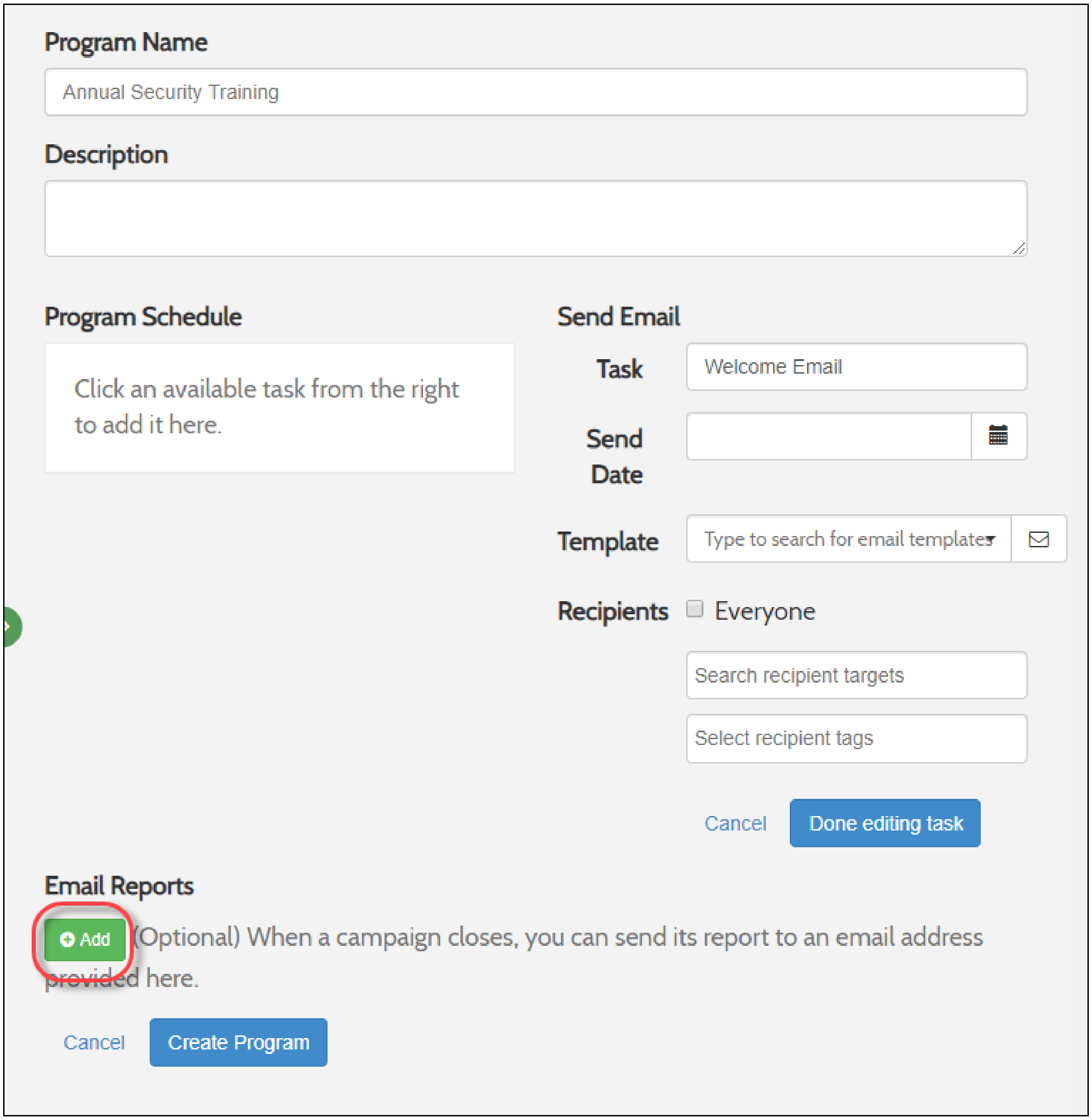
The Welcome Email edit panel displays.



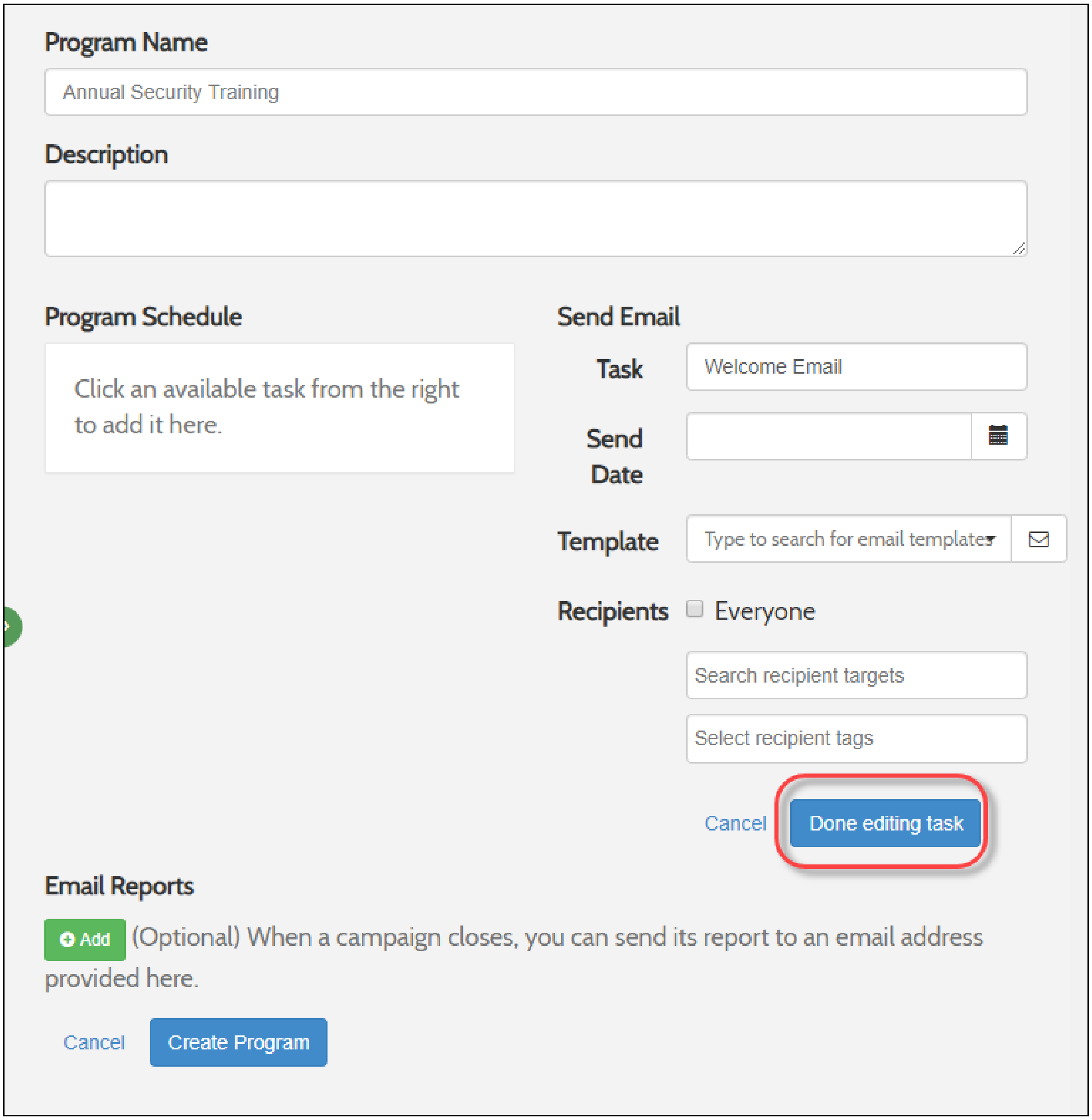
6. Populate the following fields:
   - **Program Name** — By default, the field is populated with the name of the program, but you can edit this as needed.
   - **Description** — Enter a description of the welcome email. This is an optional field.
   - **Program Schedule** — Click an available task from the right to add it here.

- **Task** — By default, the field is populated with the name of the task, in this case, Welcome Email, but you can edit this as needed.
- **Send Date** — Click the **Calendar** icon to select a date to send the welcome email.
- **Time** — When you select a date, the time fields display. As needed, select a time either in the morning or the afternoon to send the welcome email.
- **Template** — From the drop-down menu, select a welcome email template.
- **Recipients** — Do both of the following:
  - Click the Search recipient targets field to display a list of targets to select from.
  - Click the Select recipient tags field to display a list of tags to select from.

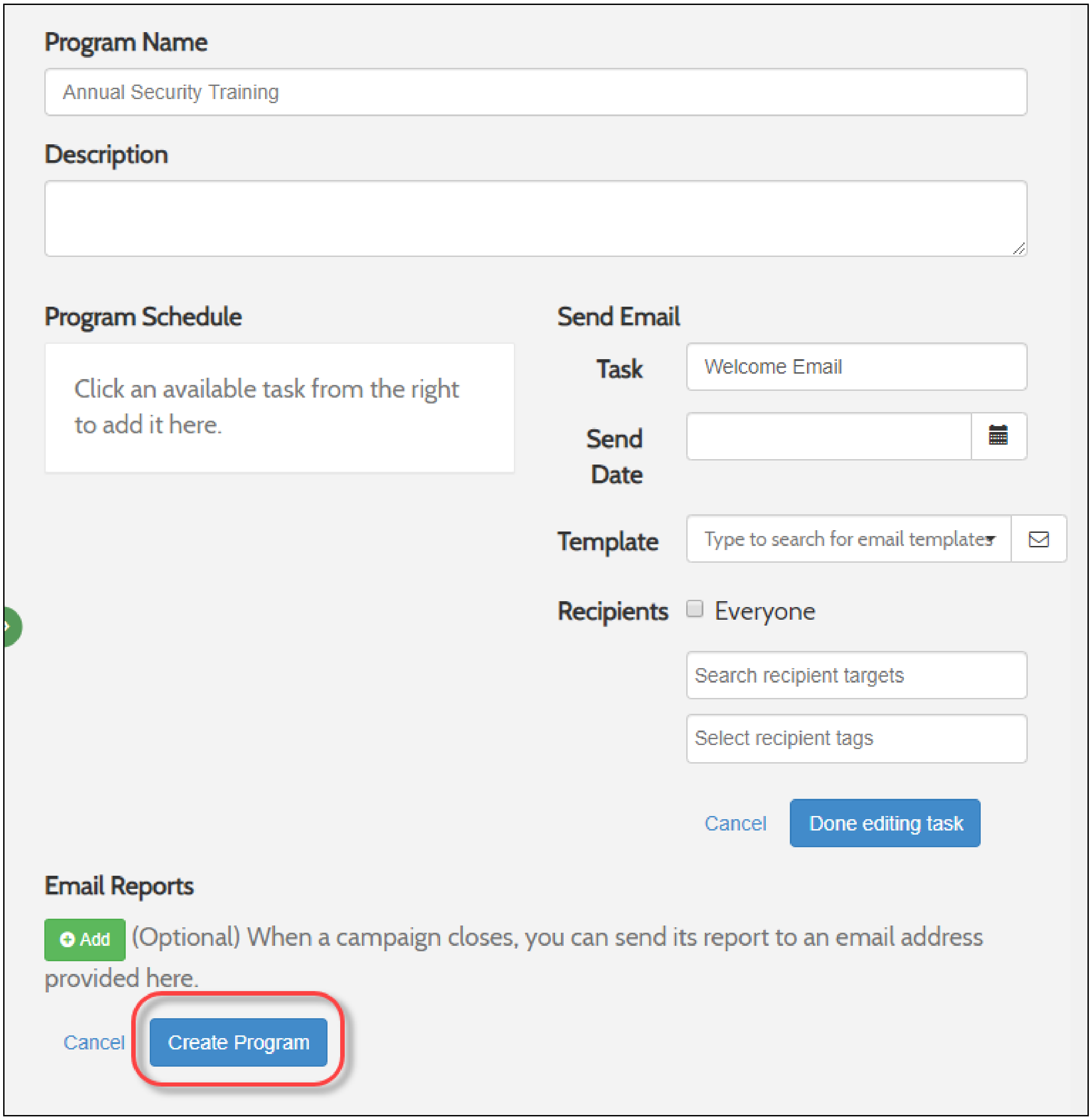
7. Click the **Add** button to add email addresses of individuals who will receive a report about the campaign after it closes. This is an optional step.


Program Name
Annual Security Training
Description
Program Schedule
Click an available task from the right to add it here.
Send Email
Task
Welcome Email
Send Date
Template
Type to search for email templates
Recipients
Everyone
Search recipient targets
Select recipient tags
Cancel
Done editing task
Email Reports
Add
(Optional) When a campaign closes, you can send its report to an email address provided here.
Cancel
Create Program

8. When you're done modifying the welcome email, click the **Done editing task** button.



9. When you're done, click the **Create Program** button.



The Welcome Email is now listed in the Programs panel.


Programs
Site: Haymont Tires, Permissions: consoleadmin
Create a new Program
Showing the only record found
Name
Owner
Status
Created
Test Training
JaneDoe@gmail.com
active
3/25/2019

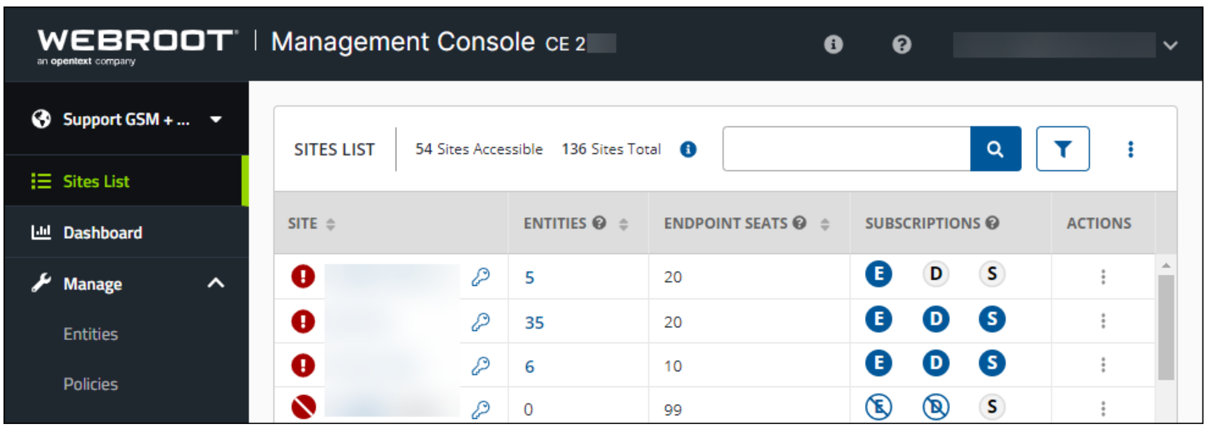
Scheduling Phishing Campaigns

After you create a phishing campaign, you can schedule it to run at a date and time you specify. You can schedule multiple phishing campaign tasks to help automate your security awareness program.

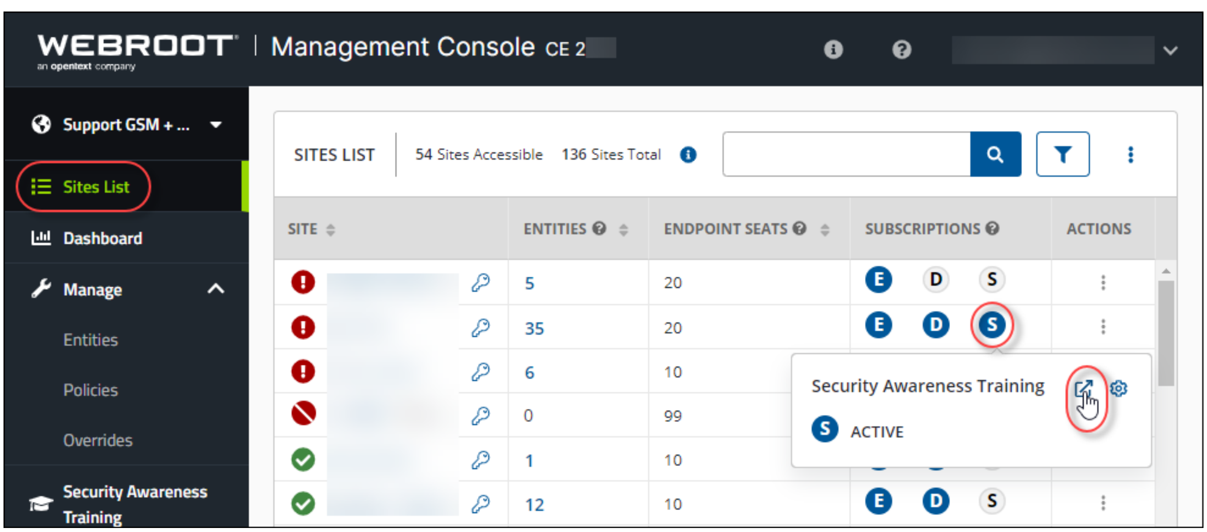
To schedule a phishing campaign:

1. [Log in to the Management Console](#).

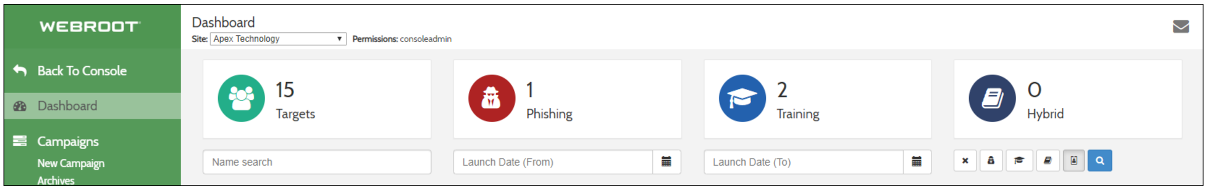
   The Management Console displays.



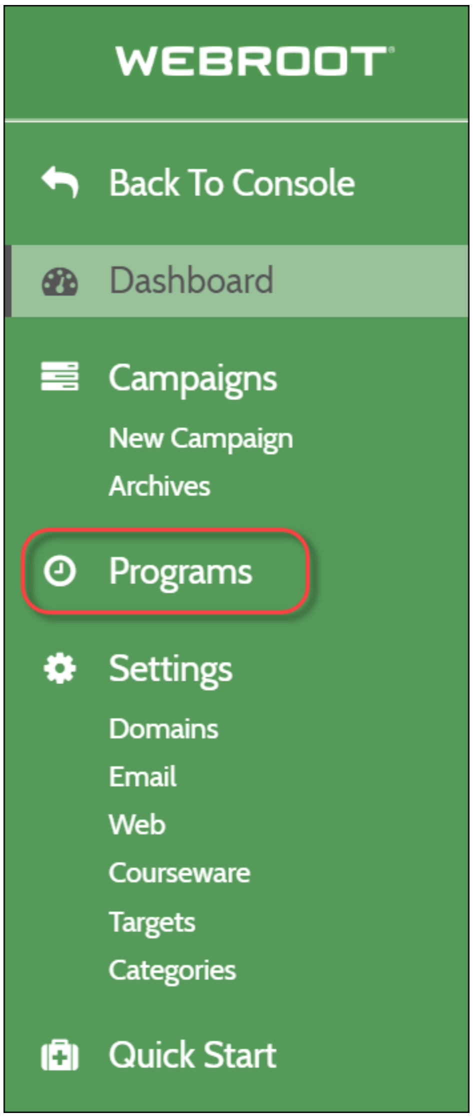
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



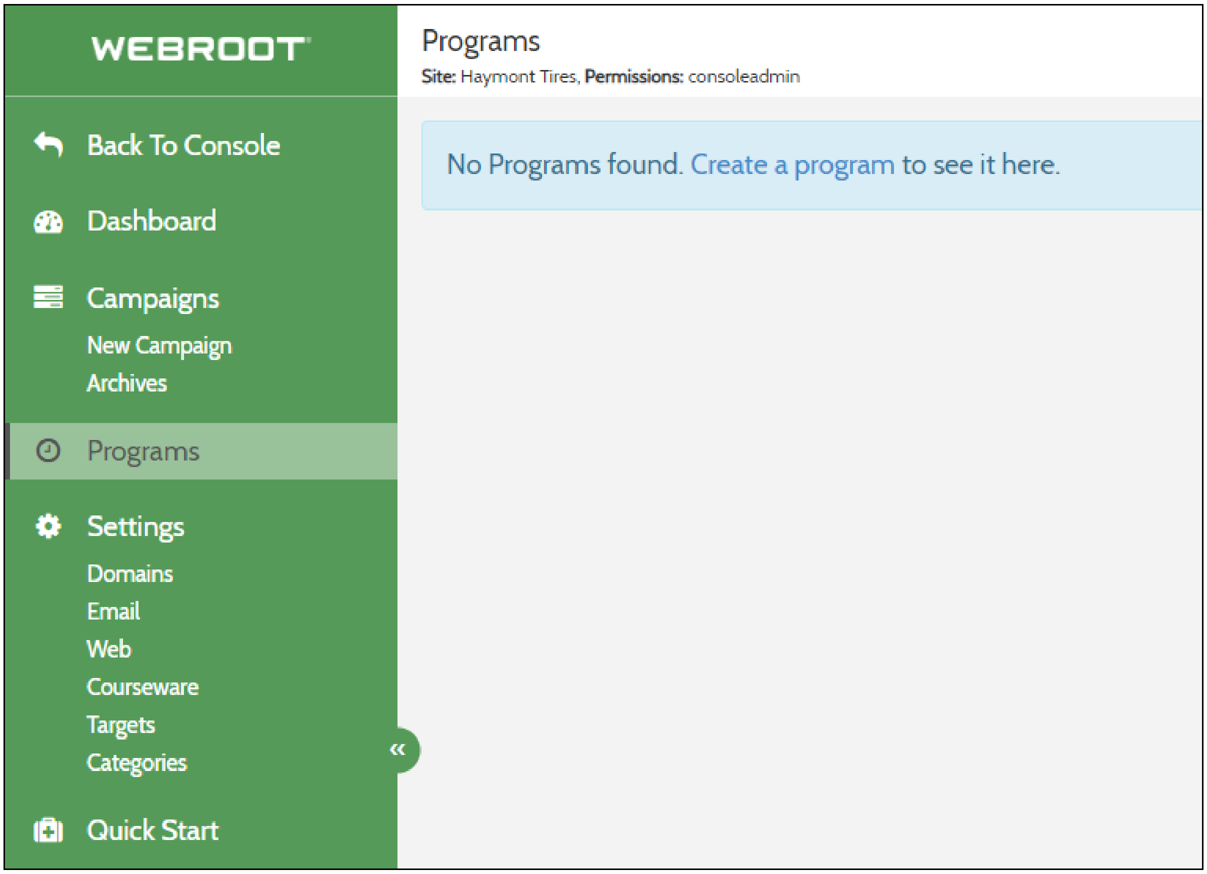
The Security Awareness Training dashboard displays.



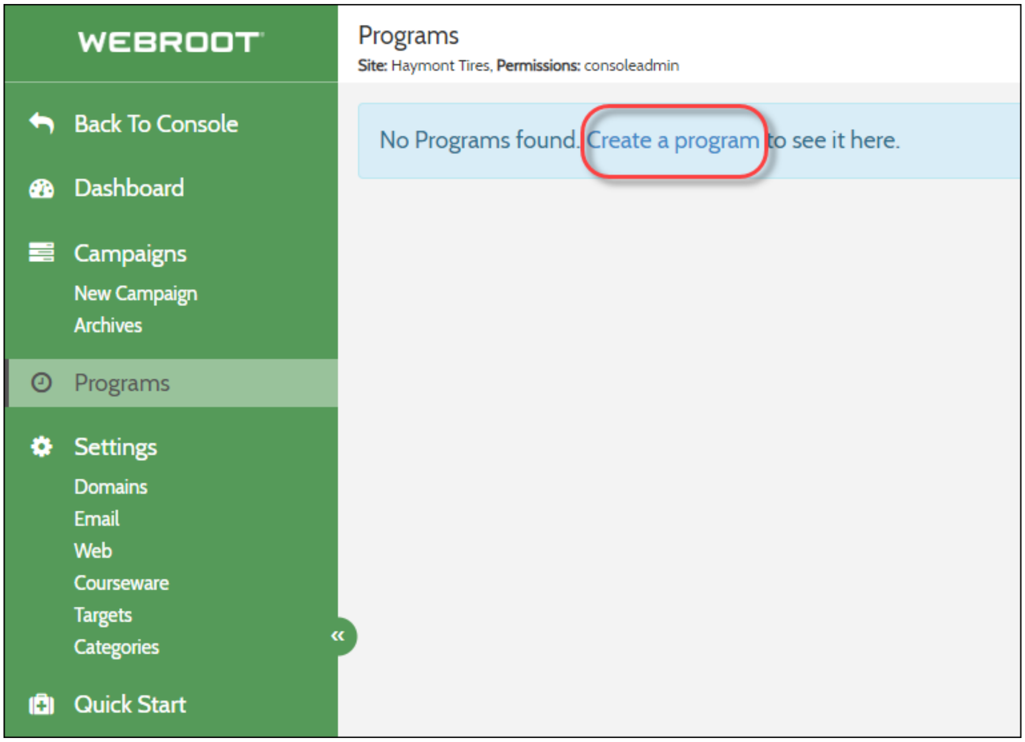
3. In the Nav bar, click the **Programs** tab.



The Programs panel displays.

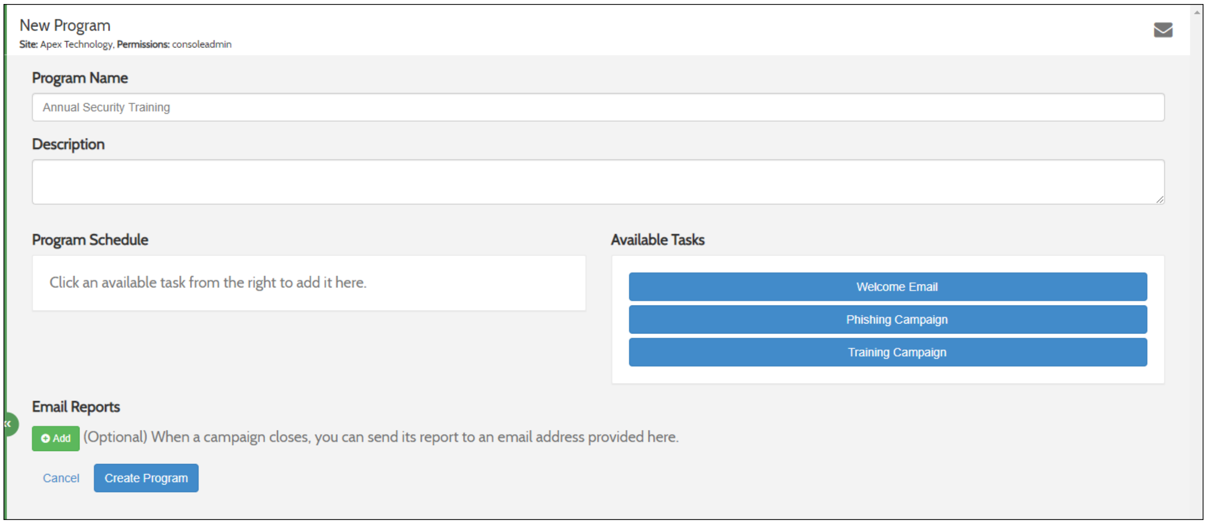


4. Do one of the following:
   - If this is the first program you're creating, click the**Create a program** link.

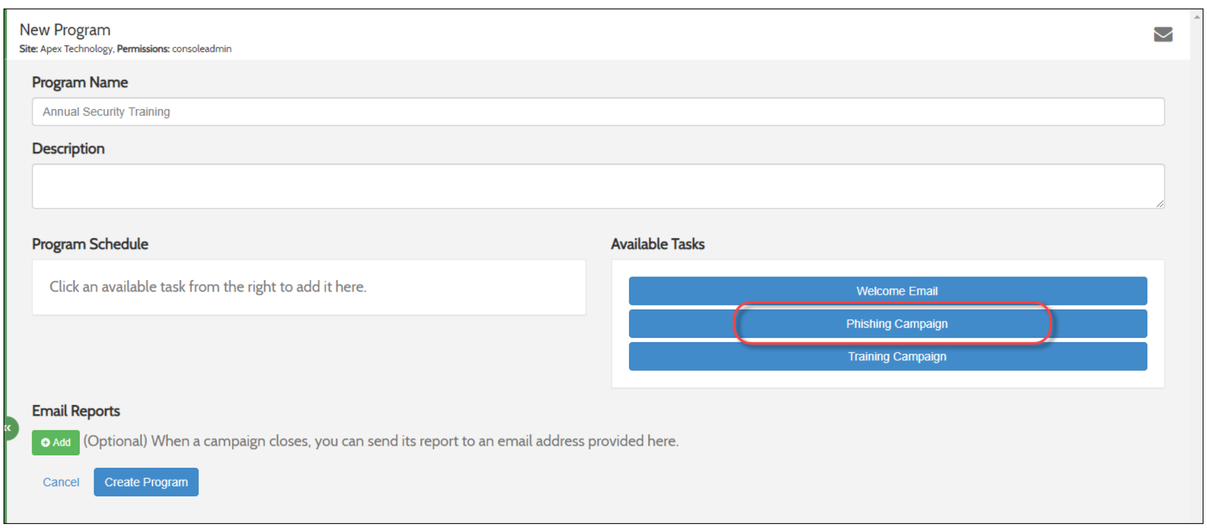


   - If this is not the first program you're creating, click the **Create a new Program** button.

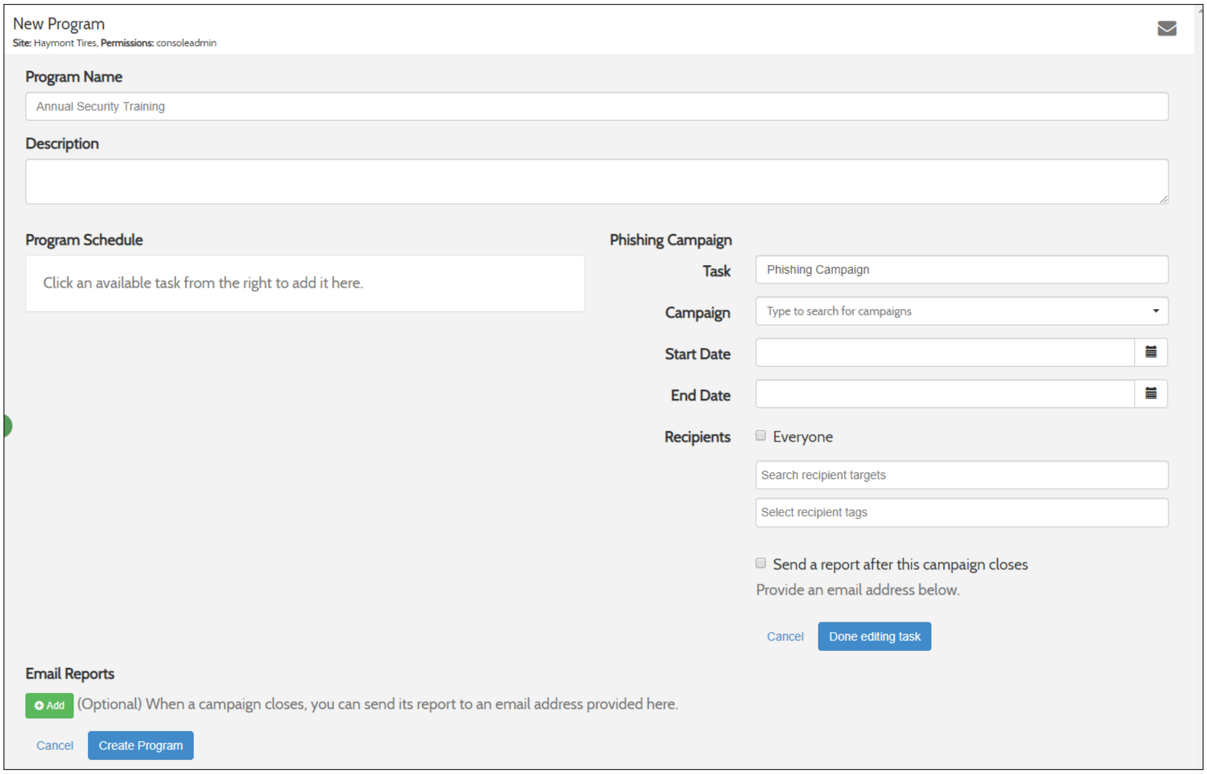
In either case, the New Program panel displays.



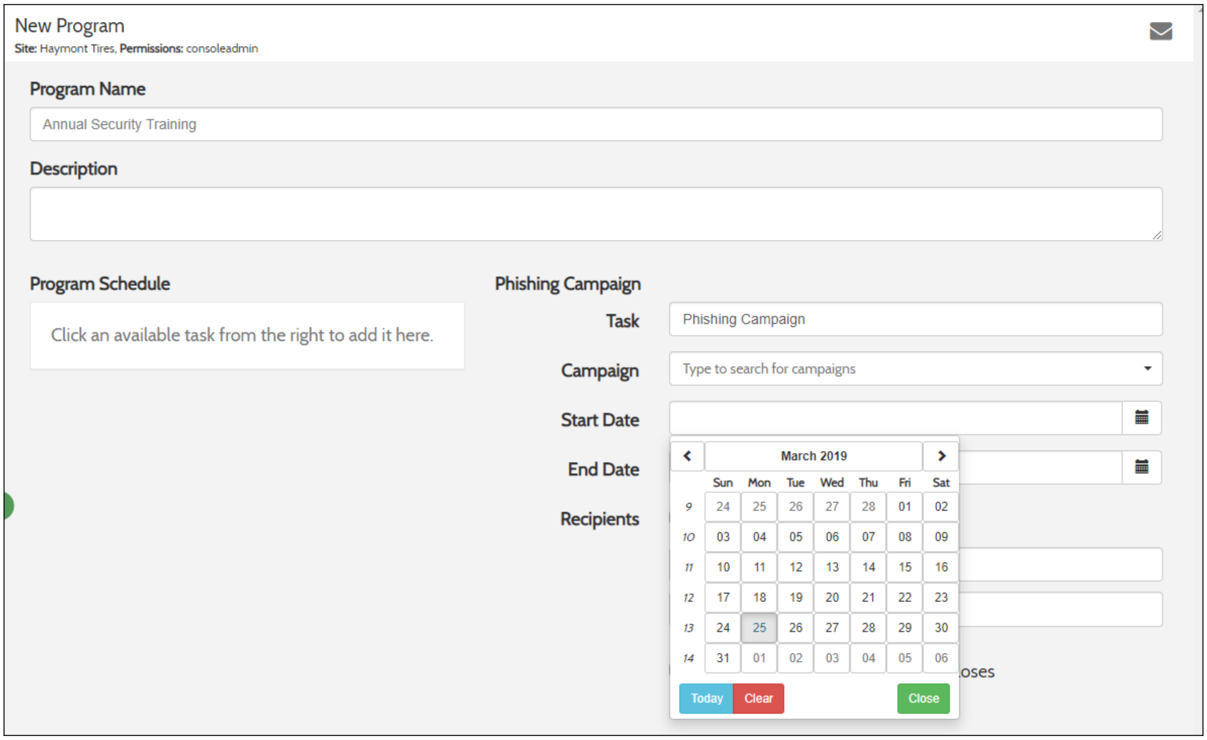
5. Click the **Phishing Campaign** button.



The edit area displays.



6. Do one of the following:
   - In the Task field, enter a unique name for the campaign.
   - From the Campaign drop-down menu, select the phishing campaign you want to schedule.
7. Populate the Start Date field to set the date and time you want to send your Phishing Campaign.
8. Populate the End Date field to determine when to complete the campaign and finalize reporting.



9. Select recipient targets can be selected from the picker individually or by entering tags.
10. Select the **Send report after this campaign closes** checkbox to schedule a campaign summary report to be sent to email addresses you enter

Note: Phishing campaigns are scheduled using Programs, and can be created and configured using Campaigns or Create New Campaign options in the menu.

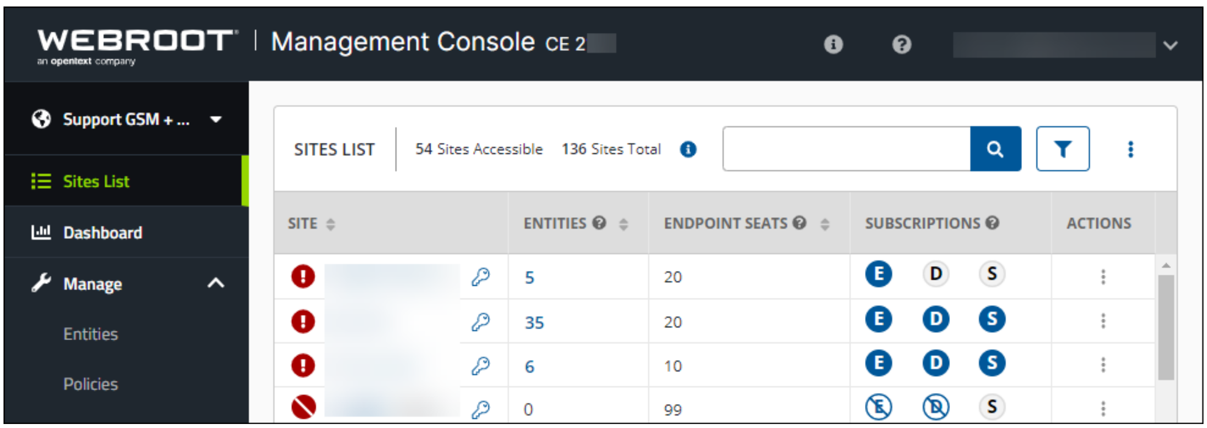
Creating Training Campaigns

This task will schedule a training campaign to be run at a date and time you specify very similar to a phishing campaign. You can schedule multiple training campaign tasks to help automate your security awareness program.

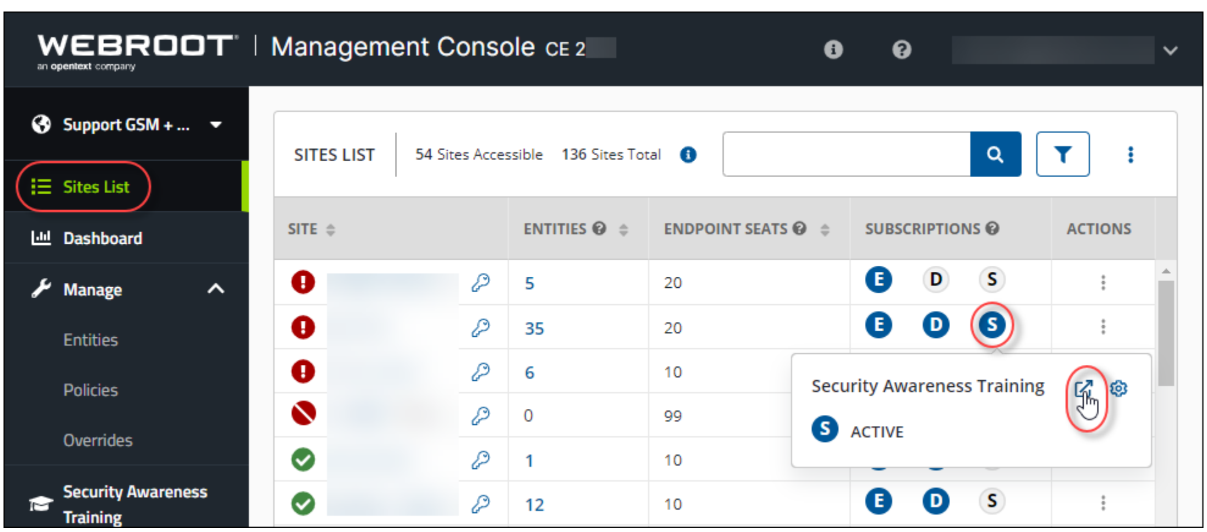
To create a training campaign:

1. Log in to the Management Console.

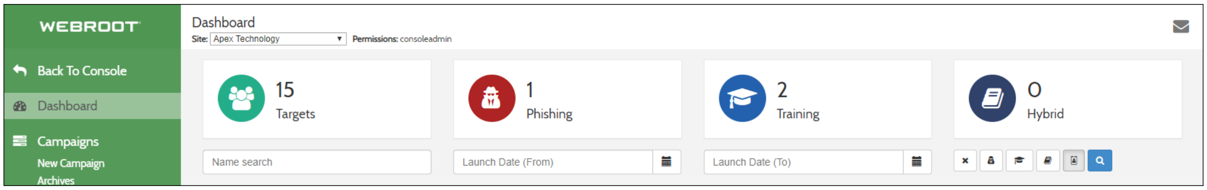
   The Management Console displays.



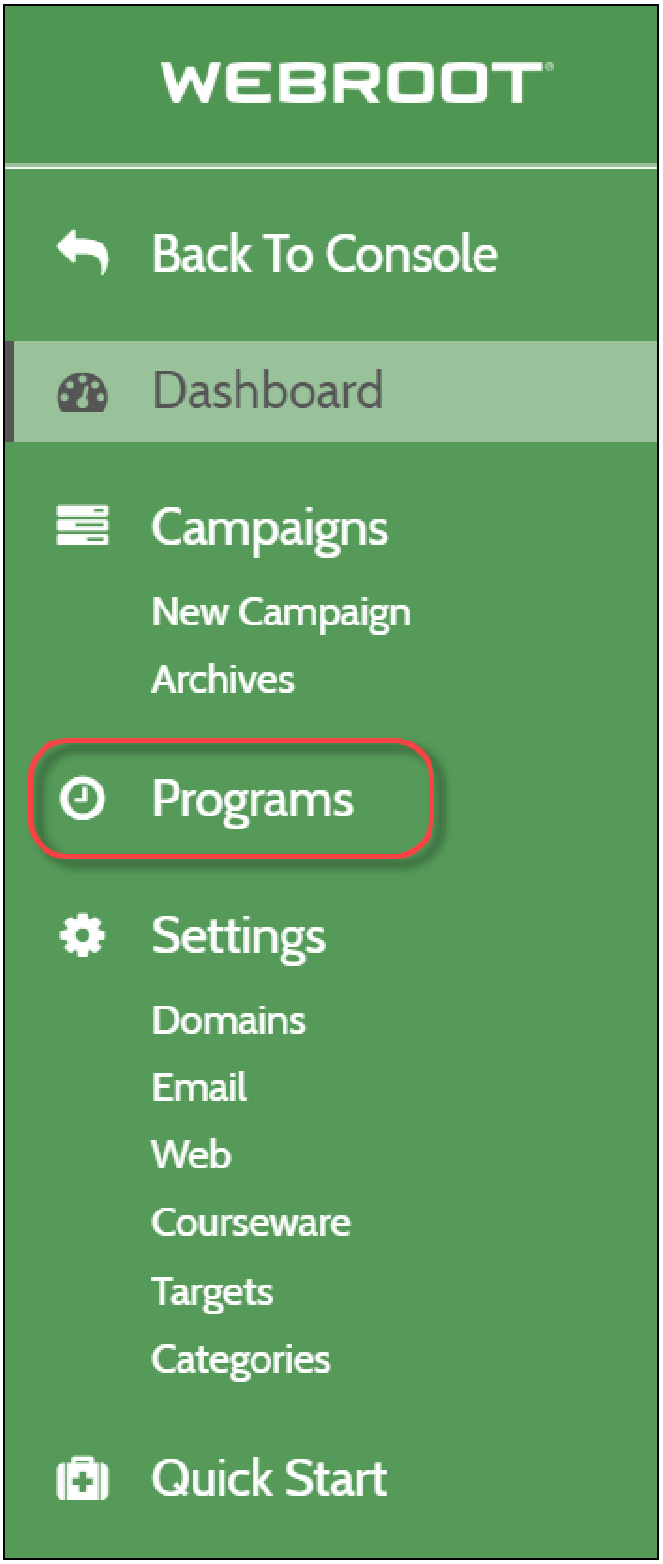
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



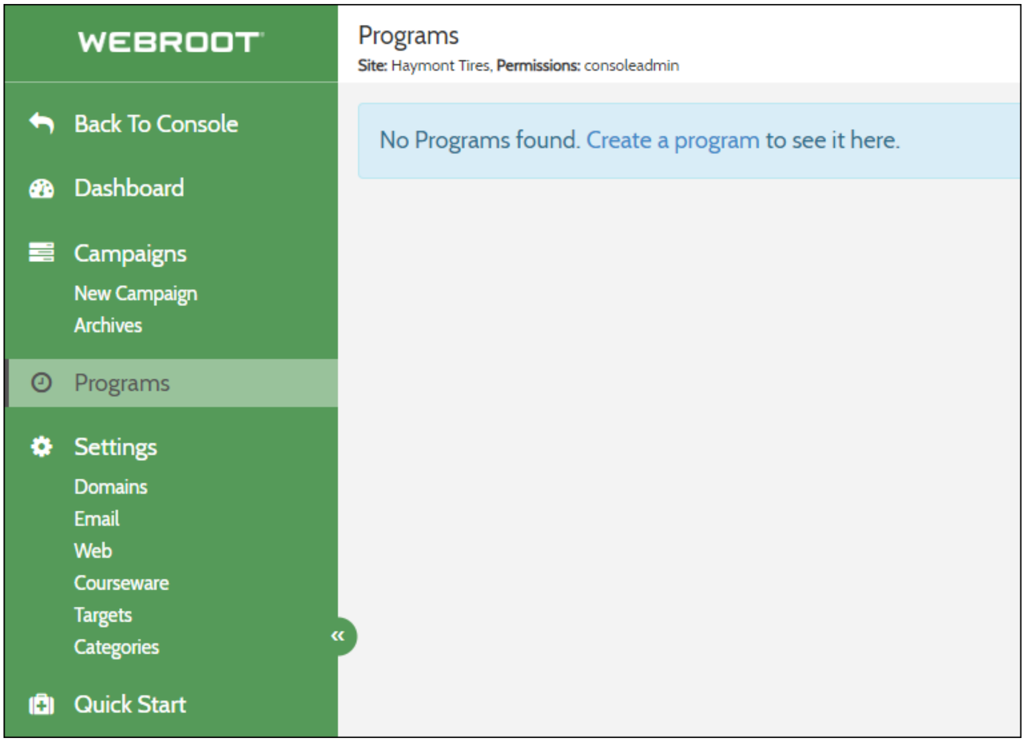
The Security Awareness Training dashboard displays.



3. In the Nav bar, click the **Programs** tab. The Programs panel displays.


WEBROOT
Back To Console
Dashboard
Campaigns
New Campaign
Archives
Programs
Settings
Domains
Email
Web
Courseware
Targets
Categories
Quick Start

The Programs panel displays.



4. Do one of the following:
   - If this is the first program you're creating, click the Create a program link.
   - If this is not the first program you're creating, click the Create a new Program button.

   In either case, the New Program panel displays.

5. Do either of the following:
   - When creating a new training campaign, enter a unique name.
   - From the Campaign drop-down menu, select the existing training campaign you want to schedule.
6. Populate the Start Date field to set the date and time you want to send your Training Campaign.
7. Populate the End Date field to determine when to complete the campaign and finalize reporting.

8. Select recipient targets can be selected from the picker individually or by entering tags.
9. Select the **Send report after this campaign closes** checkbox to schedule a campaign summary report to be sent to email addresses you enter.

> **Note:** Training campaigns are scheduled using Programs and can be created and configured using the Campaigns or Create New Campaign options in the menu.

Sending Campaign Summary Reports

The campaign summary report is a report in PDF format that contains a summary of important details about the campaign run including the following:

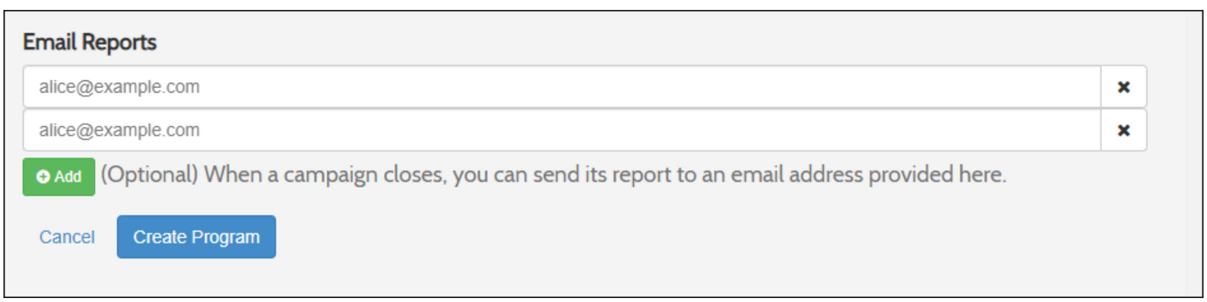
- Name of campaign
- Date of campaign
- Key statistics, along with a summary of the campaign templates used

Follow this procedure to send a campaign summary report at the conclusion of a phishing or training campaign.

To send a campaign:

1. Select the **Send a report after this campaign closes** checkbox.
2. Click the **Add** button to determine who will receive the report.
3. To add multiple recipients, clicking the **Add** button again to expand additional recipient settings boxes. This is an optional step.

> **Note:** Reports can be sent to any valid email address including distribution lists.



Understanding Email Types

There are two types of email addresses that you can enter:

- **Authorized Domain Address (Admin)** — This is your own address on your company's or organization's domain. When you add an Authorized Domain address, you will be sent a validation link to your inbox. Click that link to verify that you are the owner of the email box, and have an account on your company's/organization's domain. This will allow you to import target email addresses on that domain.
- **Target Email Addresses (End-Users)** — These are your company's or organization's employee's or member's email addresses that you will target your simulation toward. These are needed by the simulation in order to deliver the bait email.

Chapter 5: Working With Reports

To start working with reports, see the following topics:

Accessing Delivery Reports **114**
Accessing Training Reports **126**
Understanding Report Results **134**
Accessing Security Awareness Training Reports **138**
Accessing Breach Reports **143**
About Phishing Simulation Reports **149**
Sample Phishing Report Campaign Summary 149
Understanding Email Events 150
Sample PDF Summary Report 153

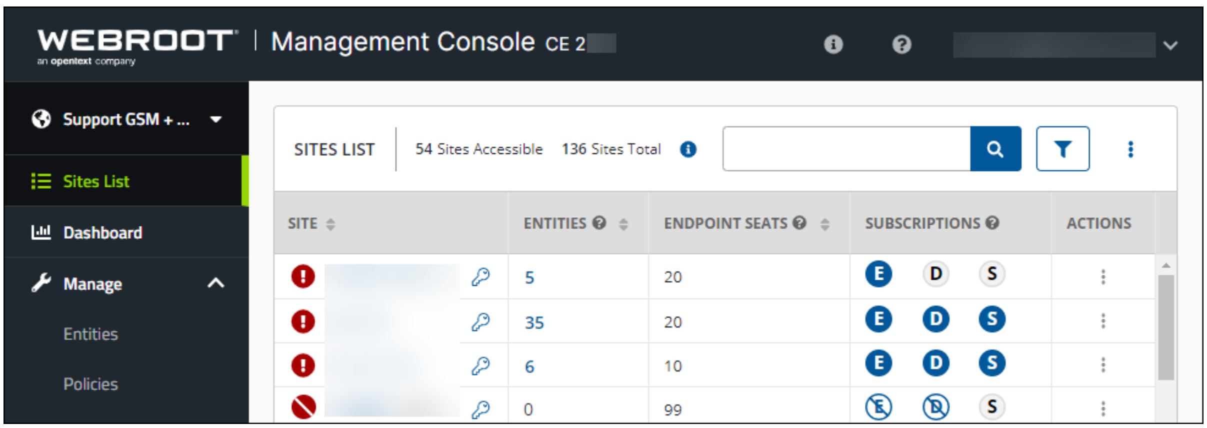
Accessing Delivery Reports

Delivery Reports display information about the report such as when the report was created and delivered, as well as statistics reflecting what happened to the campaign or training after it was delivered.

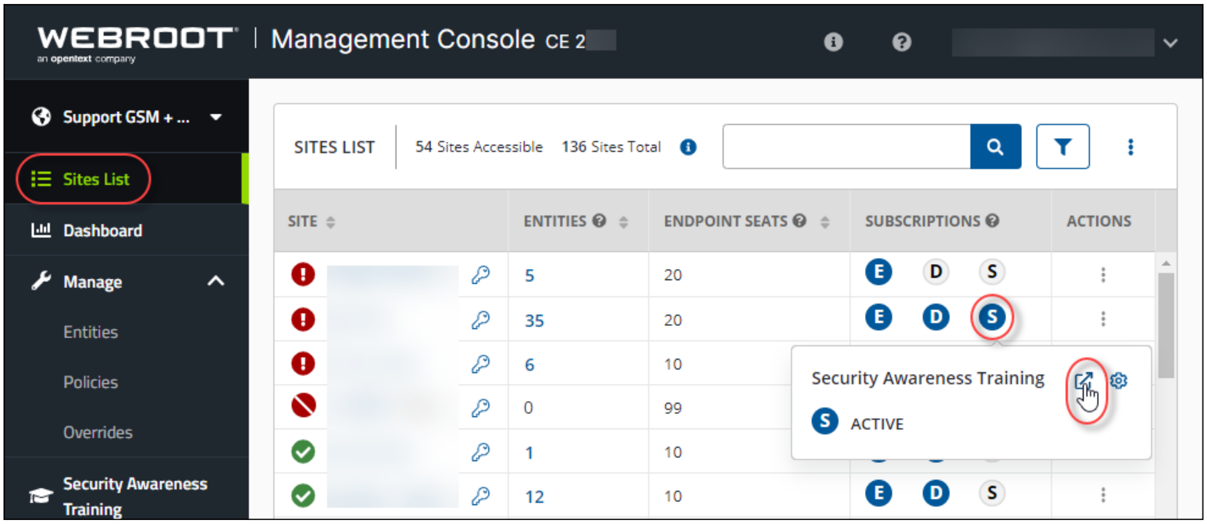
To access a Delivery Report:

1. [Log in to the Management Console](#).

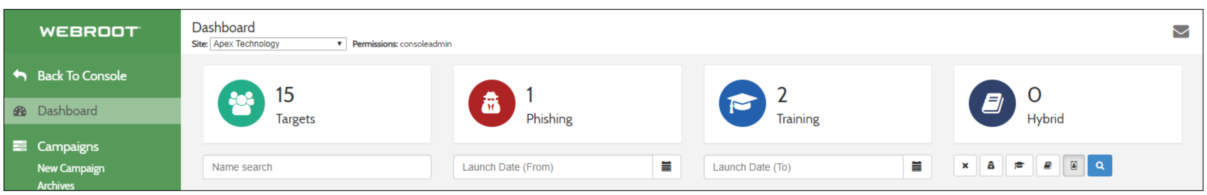
   The Management Console displays.



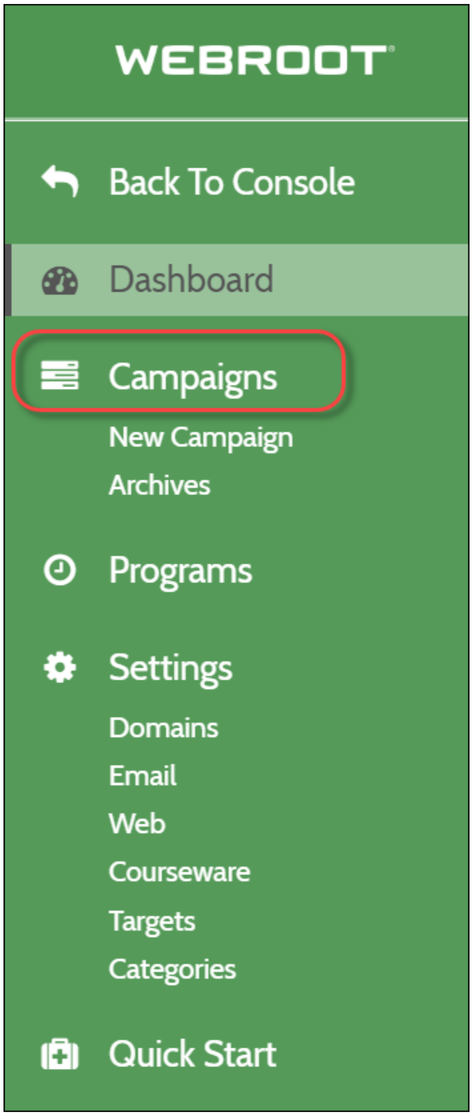
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



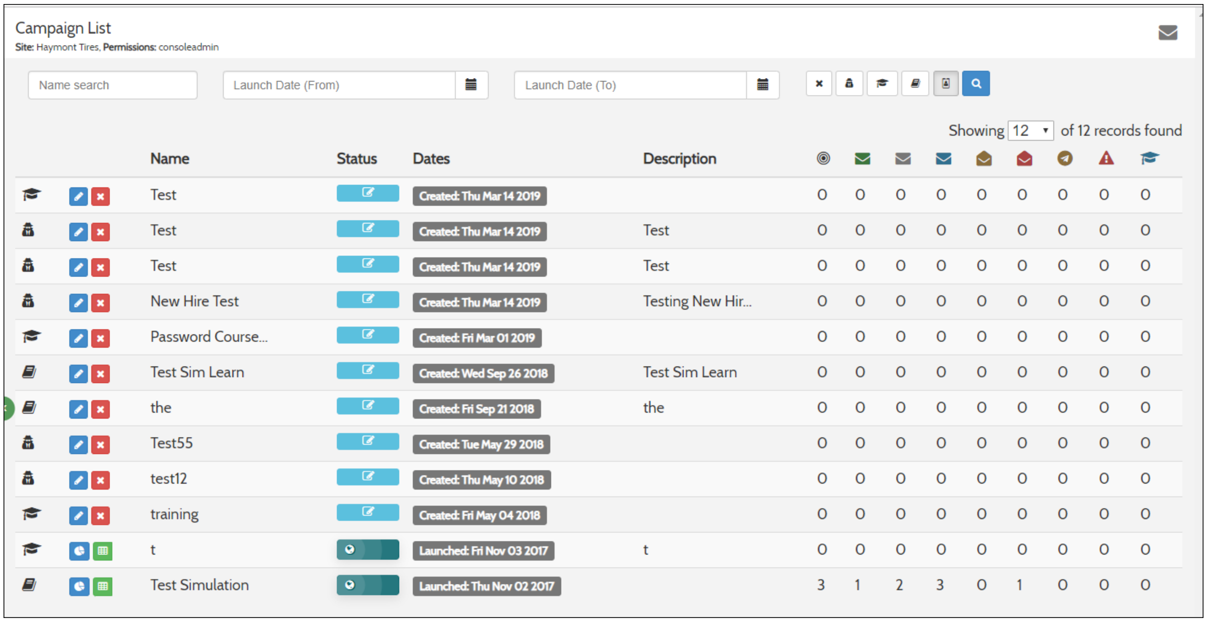
The Security Awareness Training console displays.



3. In the Nav bar, click **Campaigns** to display all programs, campaigns, and simulations regardless of their status.

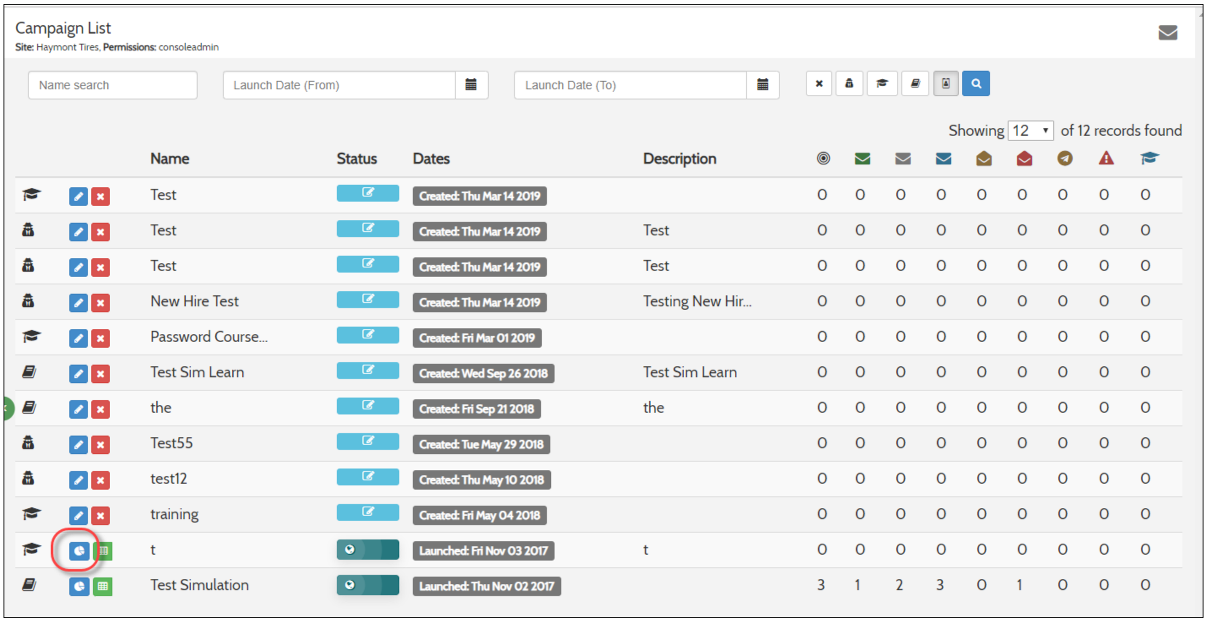


The Campaign List panel displays.

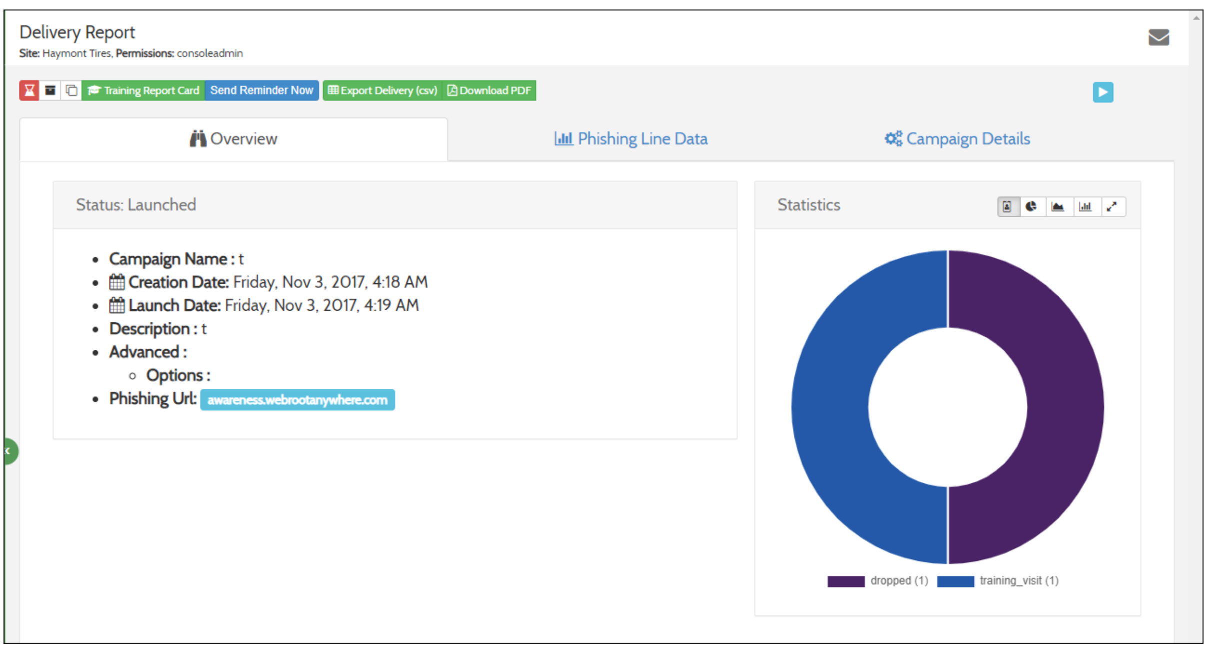


Note: You can also click Archives to display only those programs, campaigns, and simulations that have been launched. The Campaign List displays.

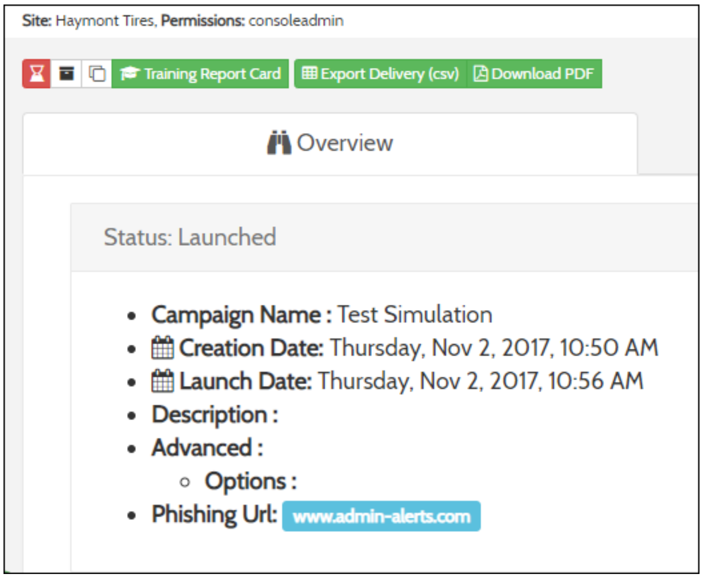
4. For the Delivery Report for the campaign you want to view, click the **Simulation Stats** icon.



The Delivery Report panel displays, with the Overview tab active.



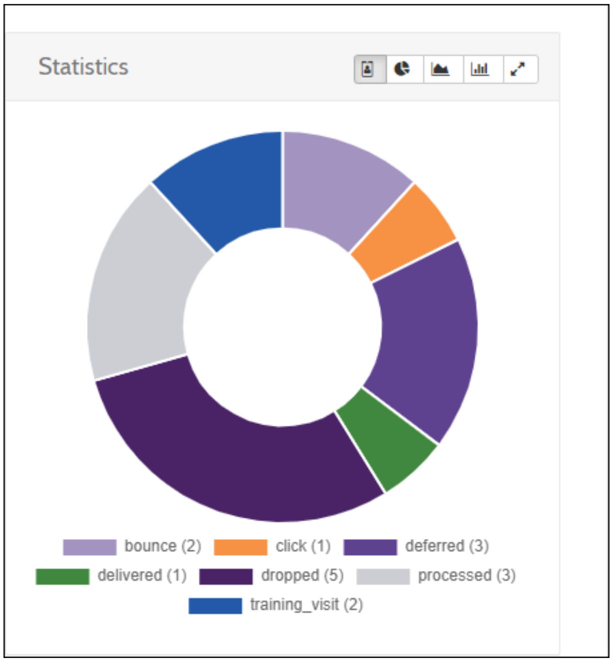
5. The Status area displays the following information:
   - Campaign Name
   - Creation Date
   - Launch Date
   - Description
   - Advanced/Options
   - Phishing URL



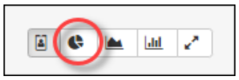
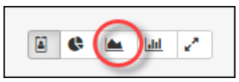
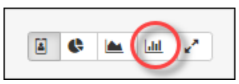
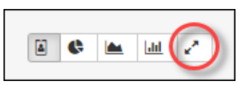
6. The Statistics area displays the following information in a graph format. Hover over the various sections of the graph to display specific information:
   - **Processed** — Requests from your website, application, or mail client via SMTP Relay or the API that the emailer processed.
   - **Clicks** — When a recipient clicks one of the Click Tracked links in your email.
   - **Delivered** — An email that was delivered to a recipient.
   - **Opens** — When an email is opened by a recipient.
   - **Deferred** — The recipient mail server asked the emailer to stop sending emails so quickly.
   - **Drops** — The emailer drops an email when one of the following occurs:The contact on that email is in one of your suppression groups.

- The recipient email previously bounced.
- The recipient has marked your email as spam.

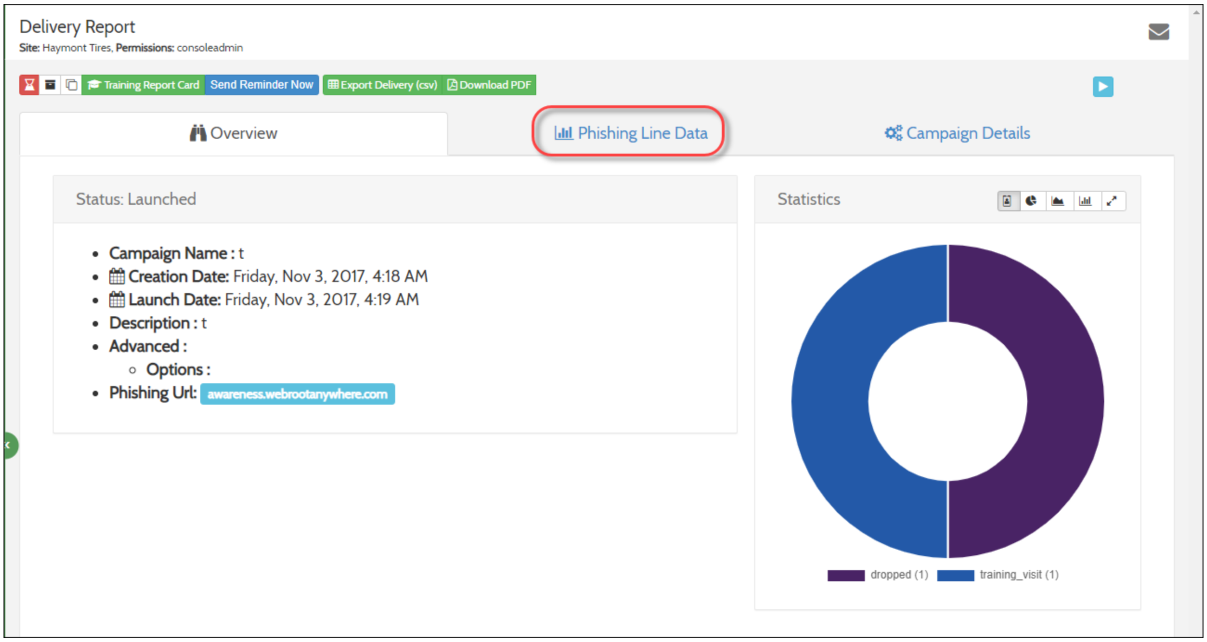
- **Bounces** — When an attempt is made to deliver an email, but the recipient mail server rejects it.
- **Spam Reports** — When a recipient marks your email as spam and their mail server tells us about it.



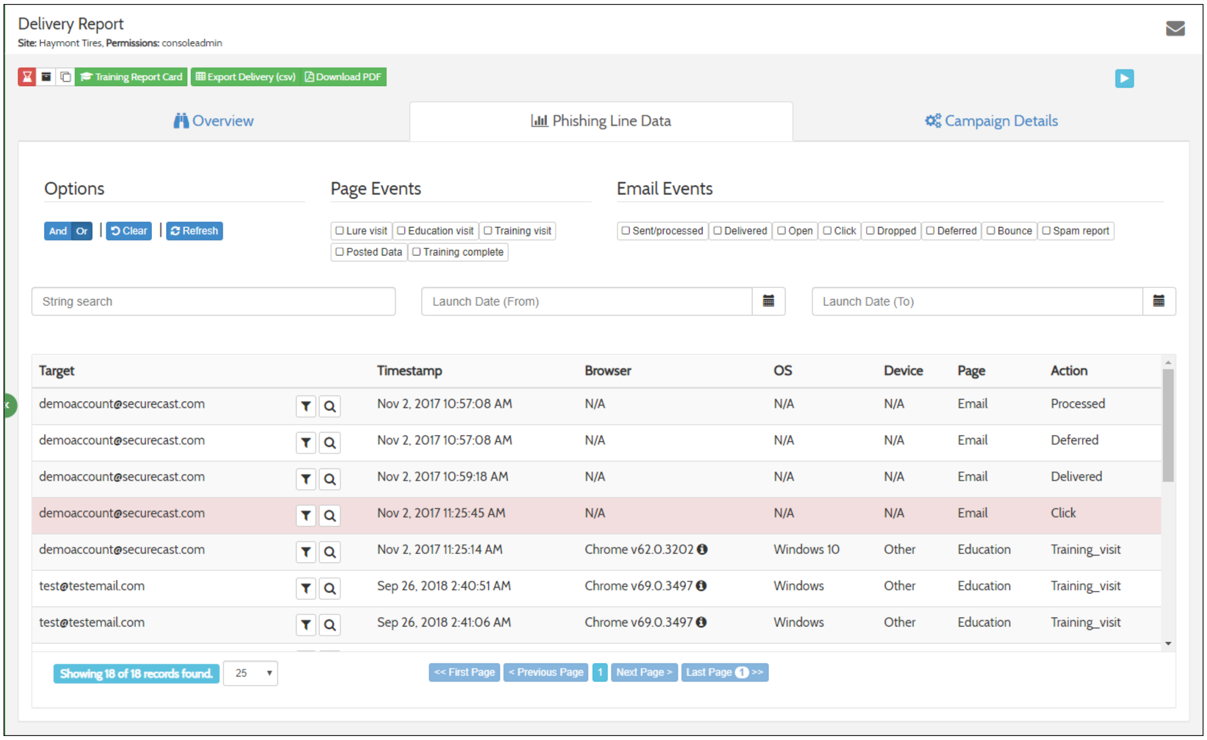
7. Additionally, in the Statistics area, you can click any of the following icons to display information differently:

ICON	DESCRIPTION
	Displays the information as a circular bar chart.
	Displays the information as a circular bar chart.
	Displays the information as a circular graph.
	Displays the information as a bar chart.
	Expands the display to fill the panel, or shrinks it back to its original size.

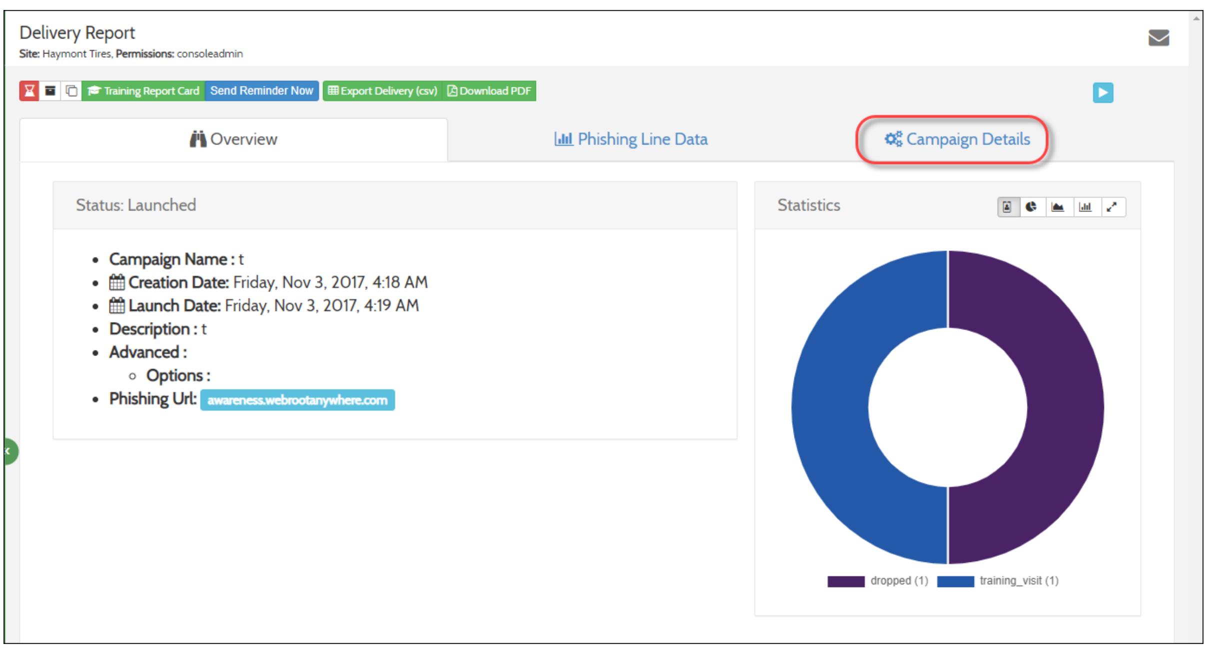
8. Click the **Phishing Line Data** tab.



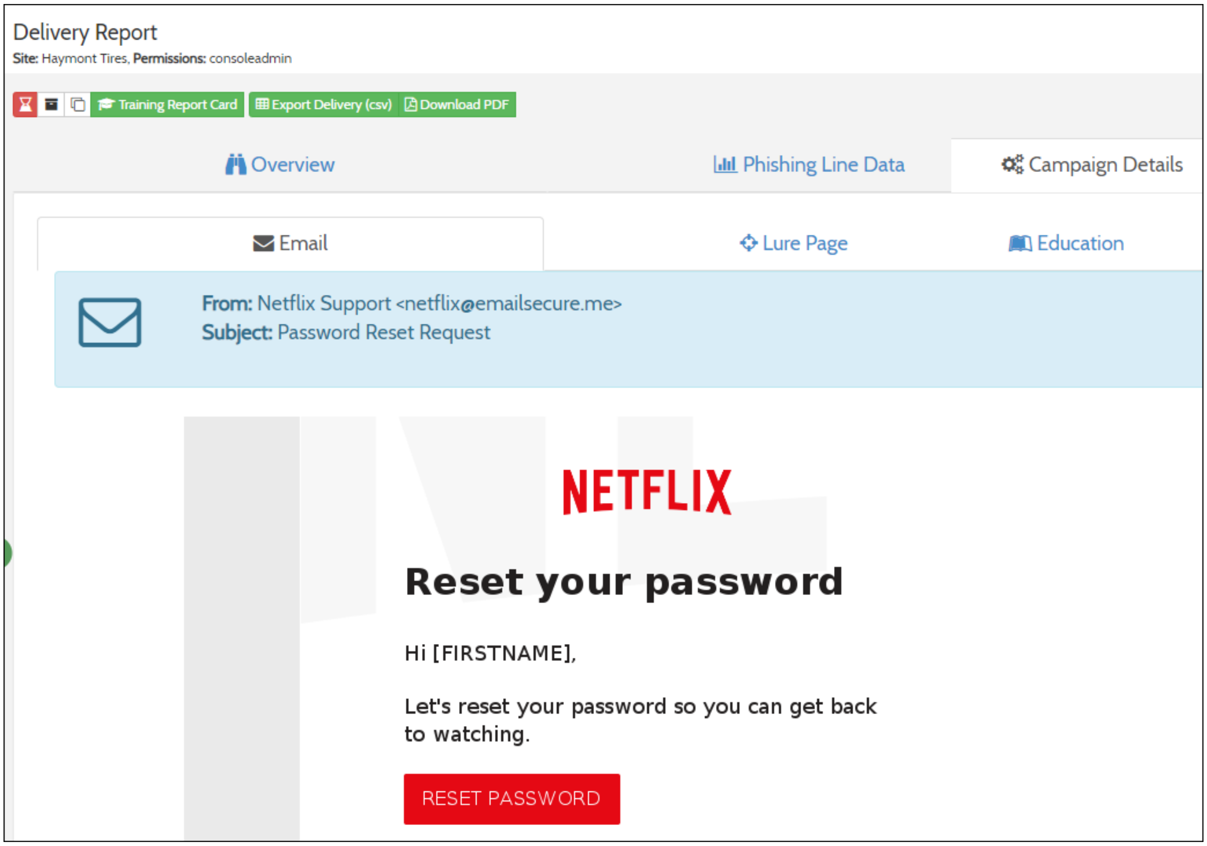
The Phishing Line Data tab displays. There you can selection actions and filters in real time.



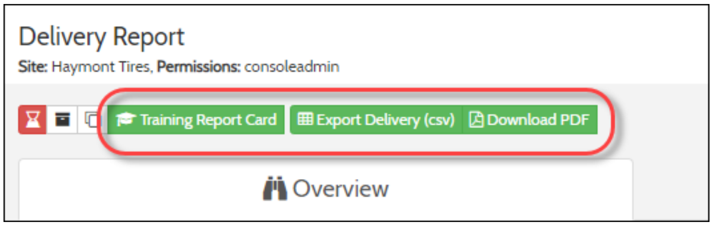
9. Click the **Campaign Details** tab.



The Campaign Details tab displays with information about the phishing campaign that was sent.



10. When you’re done reviewing the information, you can do any of the following
    - Export the report into a CSV file — Click the **Training Report Card** button.
    - Send a reminder to yourself about the training — Click the **Send Reminder Now** button.
    - Export delivery information into a CSV file — Click the **Export Delivery (csv)** button.
    - Download a PDF containing report information — Click the **Download PDF** button.


Delivery Report
Site: Haymont Tires, Permissions: consoleadmin
Training Report Card
Export Delivery (csv)
Download PDF
Overview

Accessing Training Reports

Training campaigns include a training invite that is sent to a select number of recipients. Those invited to take a training course would click on a link to launch their training. The Webroot SAT platform tracks the delivery of training invites along with the progress of trainee users as they complete a course.

Training courses can be stopped and re-started picking up where the trainee user left off. Trainee users receive a certificate of completion when a course is complete.

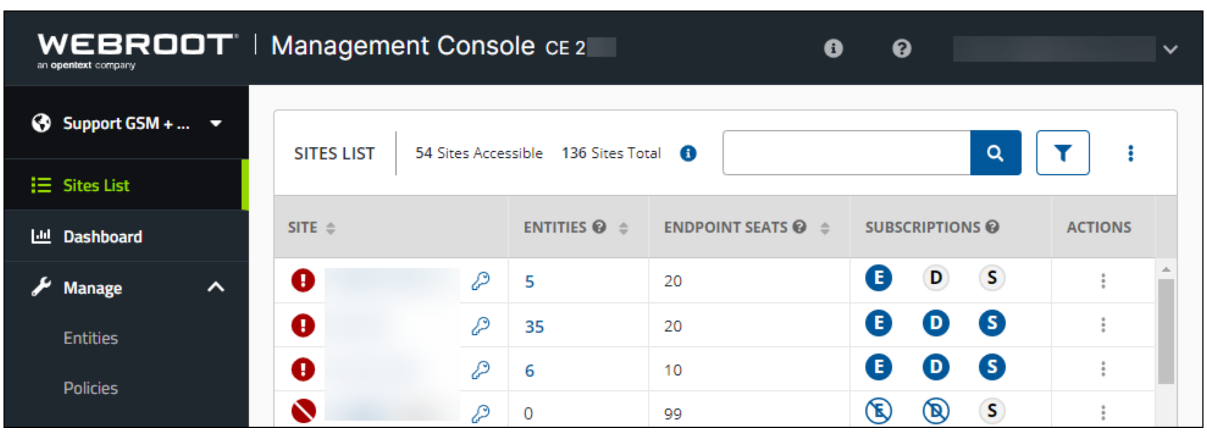
All actions and progress of a trainee user are tracked and logged in Webroot SAT reporting including user invite delivery, trainee user progress and completion. Reporting is available to both summarize training activity and provide detail on a per trainee user level.

Note: You can only access a Training Report for a simulation or campaign that has been launched.

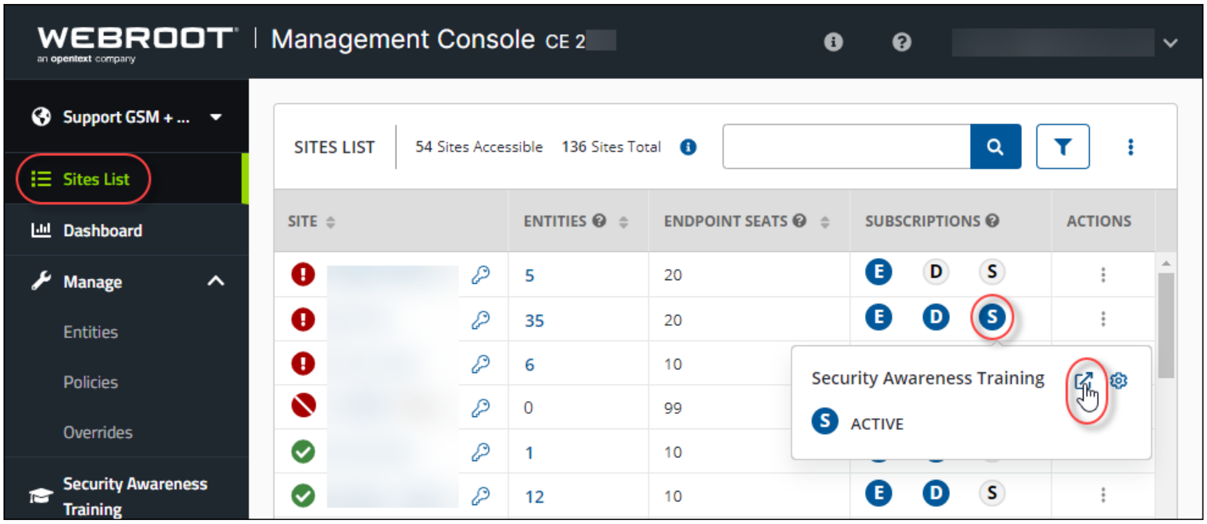
To access a Training Report:

1. Log in to the Management Console.

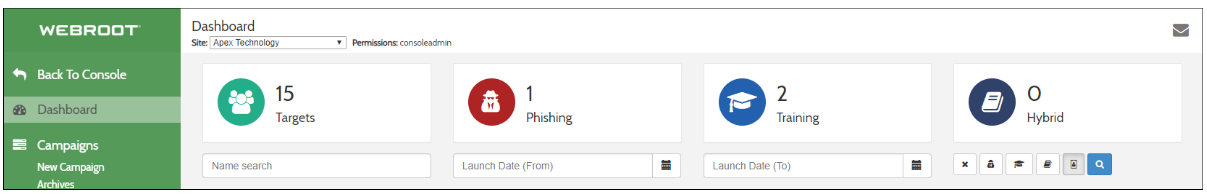
   The Management Console displays.



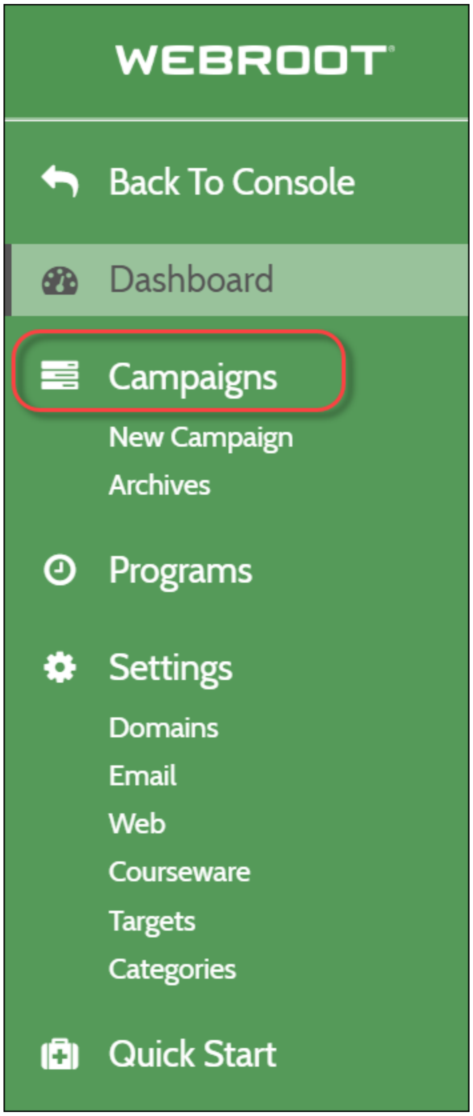
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



The Security Awareness Training console displays.

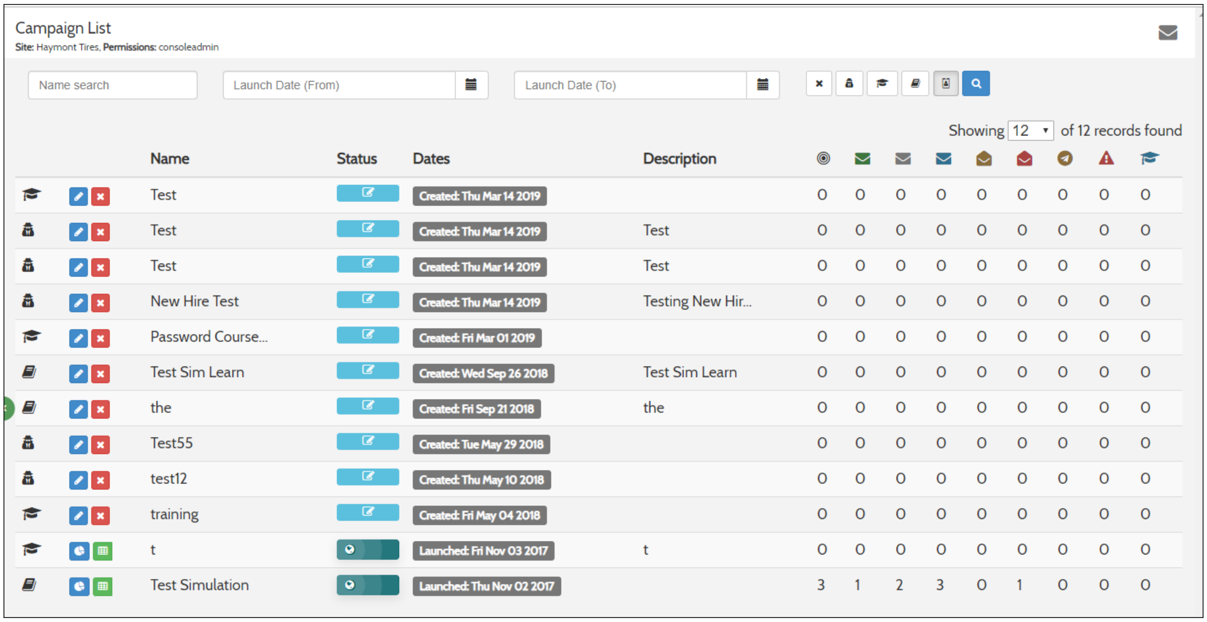


3. In the Nav menu, click the **Campaigns** tab.

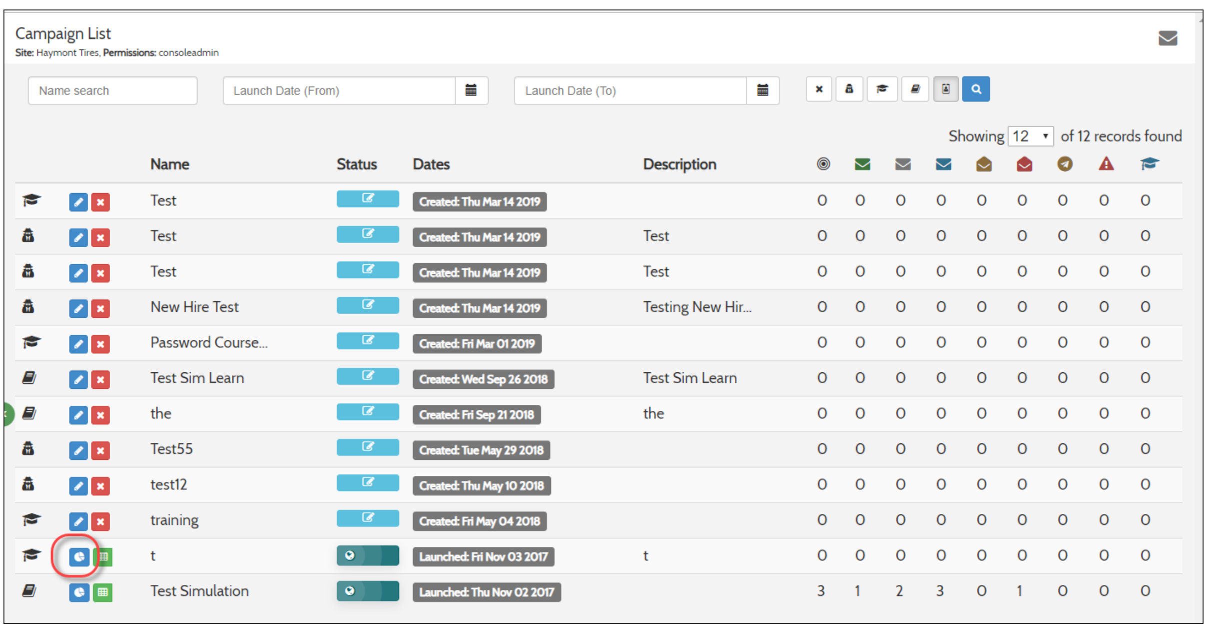


Note: As needed, you can access archived campaigns by clicking the **Archives** tab.

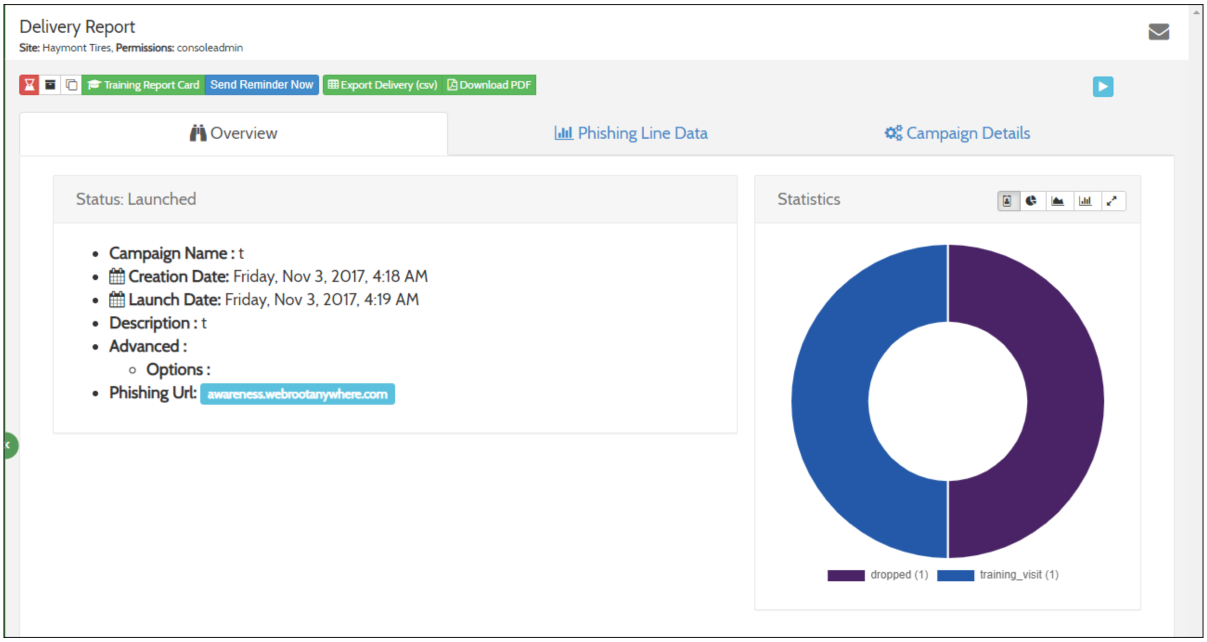
The Campaign List panel displays.



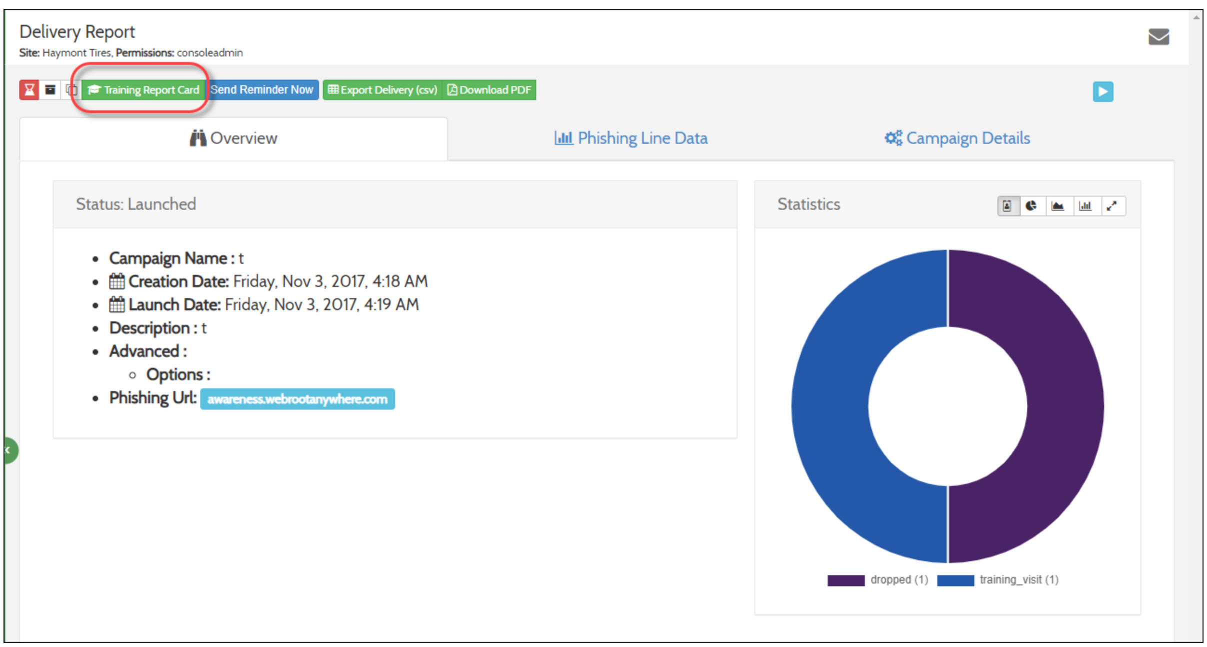
4. For the Training Report for the campaign you want to view, click the **Simulation Stats** icon.



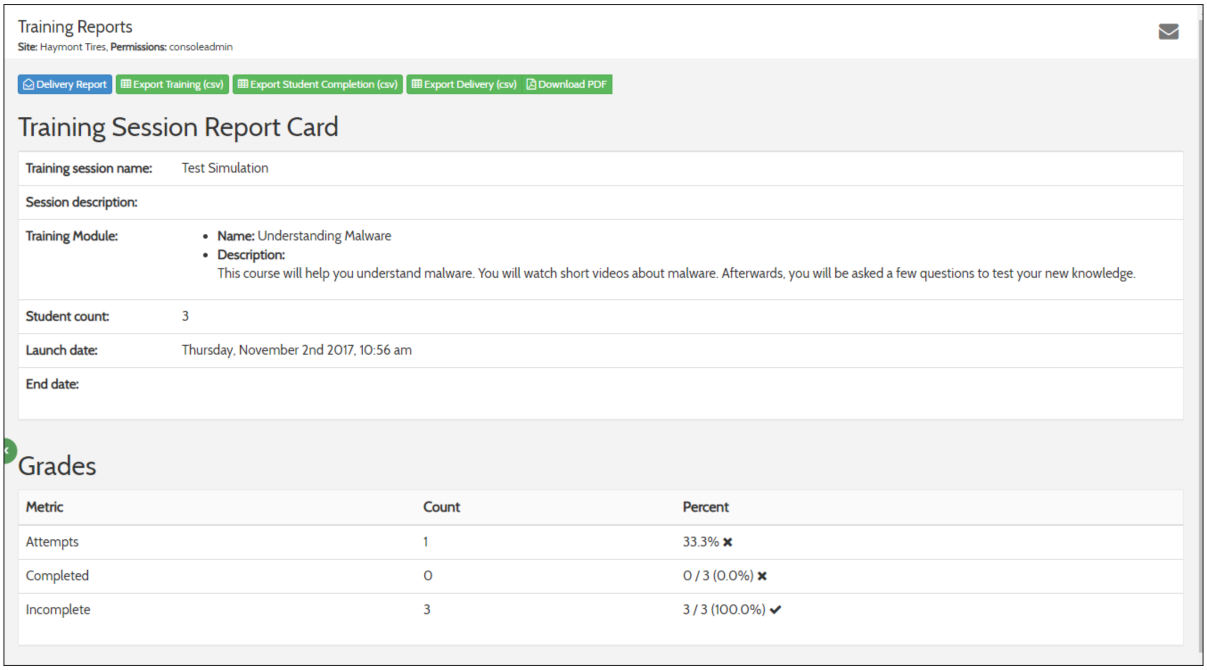
The Delivery Report panel displays.



5. In the upper left, click the **Training Report Card** icon



The Training Reports panel displays.

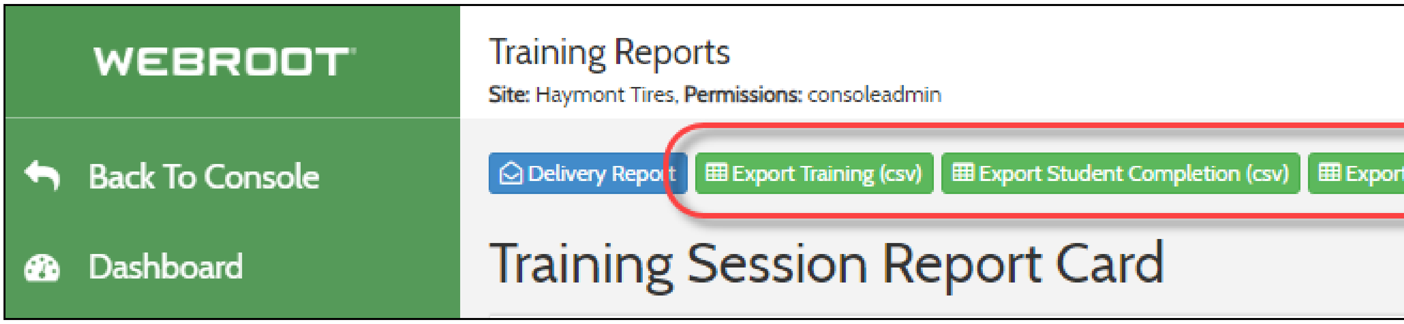


There are three sections available for your review.

SECTION	DESCRIPTION
Training Session Report Card	Displays the following information: • Training session name • Session description • Training Module • Student count • Launch date • End date
Grades	Displays the following information: • Attempts - Number of attempts made and the percent of all attempts. • Completed - Number of attempts completed and the percent of all attempts. • Incomplete - Number of incomplete attempts and the percent of all attempts.

SECTION	DESCRIPTION
Individual User Logs	Displays the following information: • Timestamp • Target • Type • Name • Action • Result • Score

6. When you're done reviewing the information, you can do any of the following:
   - Export the report into a CSV file – Click the **Export Training (csv)** button.
   - Export the report about student completion into a CSV file – Click the **Export Student Completion (csv)** button
   - Export delivery information into a CSV file – Click the **Export Delivery (csv)** button.
   - Download a PDF containing report information – Click the **Download PDF** button.



Understanding Report Results

Webroot Security Awareness Training tracks nearly every event, click, open, score etc. on a user by user basis within each phishing or training campaign. Below are examples of some of the pre-built reports that currently exist within the Webroot Security Awareness Training platform. More reports are being added regularly and custom reports can be requested.

Below is a data legend to help define each item that Webroot SAT tracks within its reports.

DATA	DESCRIPTION
Campaign Count	Total number of campaigns a client launched.
Phishing (Campaign)	Total number of phishing campaigns a client launched. Phishing campaigns consist of: • Simulated phishing lure to entice the user to open/click through to a lure page. For example, a phishing message could be the following: *Please log in to your bank verify your credentials*. • A simulated phishing lure page that entices a user to enter data (credentials/bank info/etc.), or click on a link. For example a simulated phishing lure page would state: Log in to your bank account. • An education page, for example: “What to look for to identify phishing attacks…”), training module (hybrid(*1) campaign; example: “Understanding Malware” course) or faux error page (example: “404 not found” to try and get users to think this is a benign/broken link and discard) • All actions are logged throughout all these steps.
Training (Campaign)	Total number of training campaigns the client launched. A training campaign consists of: • Welcome email for the trainee to access the training material. • Course material/interactive training course. (see Courses Available below).

DATA	DESCRIPTION
Hybrid (Campaign)	Total number of hybrid (*1: phishing campaign that ends with a training course session) campaigns the client launched.
Processed (Emails)	Total number of emails sent to targeted user across all campaigns.
Delivered (Emails)	Total number of emails delivered to targeted users across all campaigns.
Deferred (Emails)	Total number of emails deferred by the recipient email systems. Deferrals may end in a dropped, delivered or bounced email message.
Bounce (Emails)	Total number of emails bounced by the recipient email systems. Bounced messages are generally reported by one of the following: • Incorrect email address. • Email account/server has blocked the message.
Dropped (Emails)	Total number of email dropped by the recipient email systems. Dropped messages are generally reported on email accounts that received a bounce, and our transactional email system drops the message so that we’re not re-sending to an invalid email address.
Click (Emails)	Total number of users that clicked on email messages sent across all campaigns.

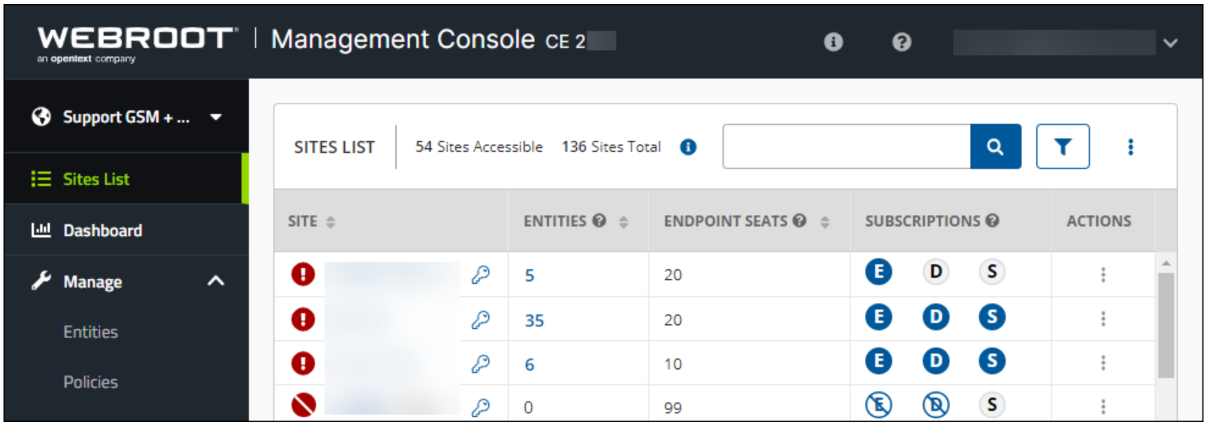
DATA	DESCRIPTION
Open (Emails)	Total number of users that clicked on email messages sent across all campaigns.
Lure_visit	Total number of visits by users to simulated phishing lure pages.
Post	Total number of attempts to post data to a simulated phishing lure page form (login creds, bank info, etc.).
Education_visit	Total number of visits by users to education pages (infographics/static education page).
Training_visit	Total number of visits by users to a training course launch page.

Accessing Security Awareness Training Reports

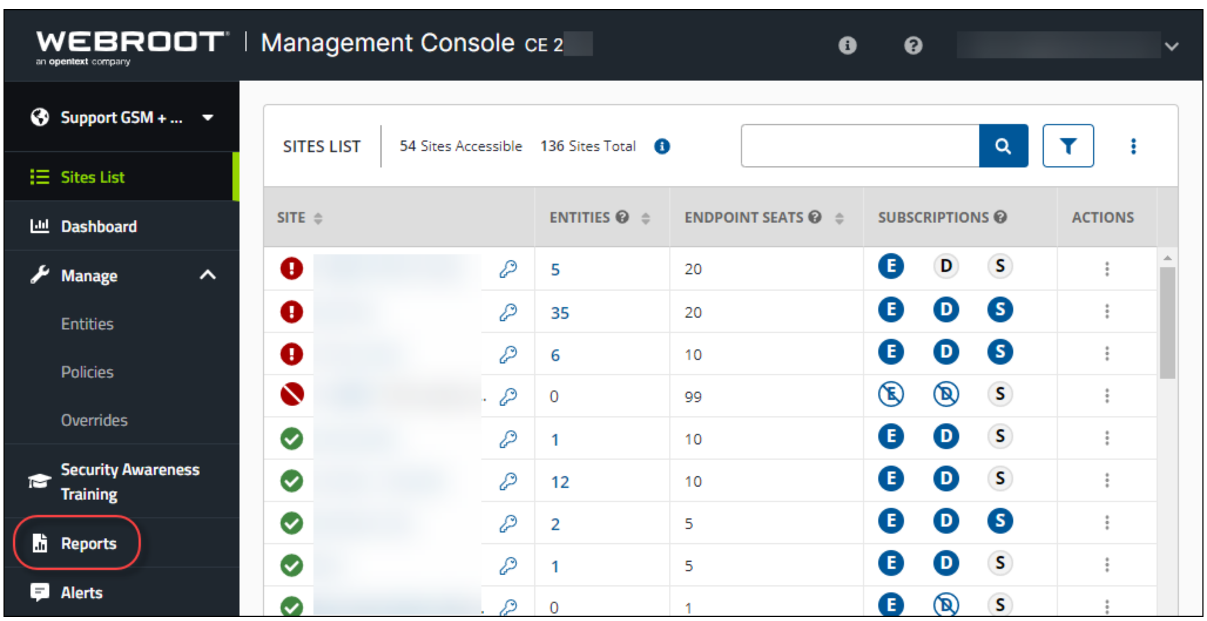
Follow this procedure to access Security Awareness Training reports.

To access a Security Awareness Training report:

1. Log in to the Management Console.

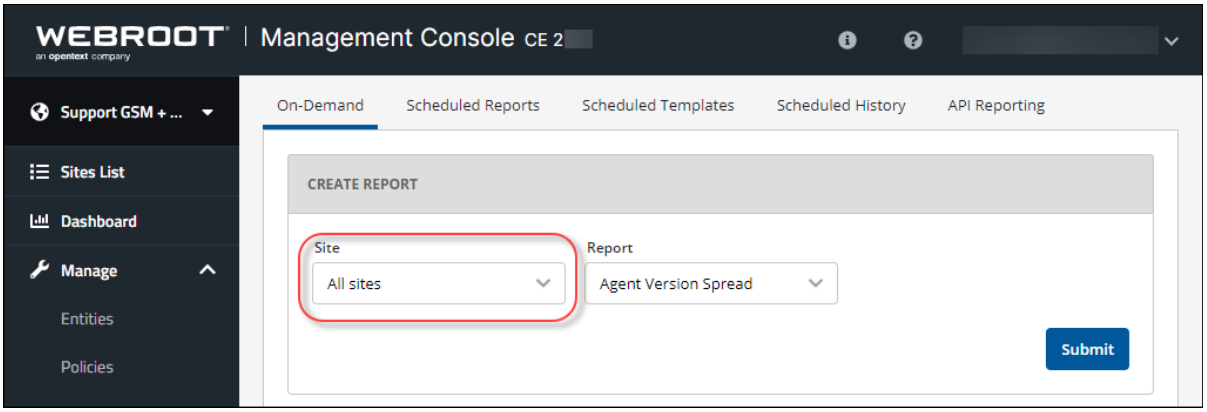


2. Click the **Reports** tab.

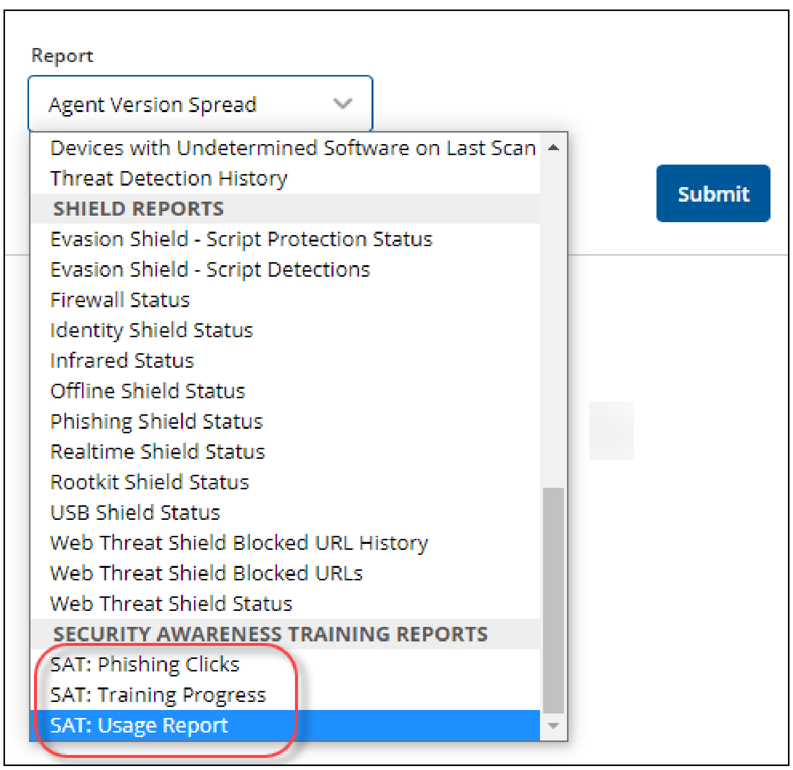


The Reports tab displays.

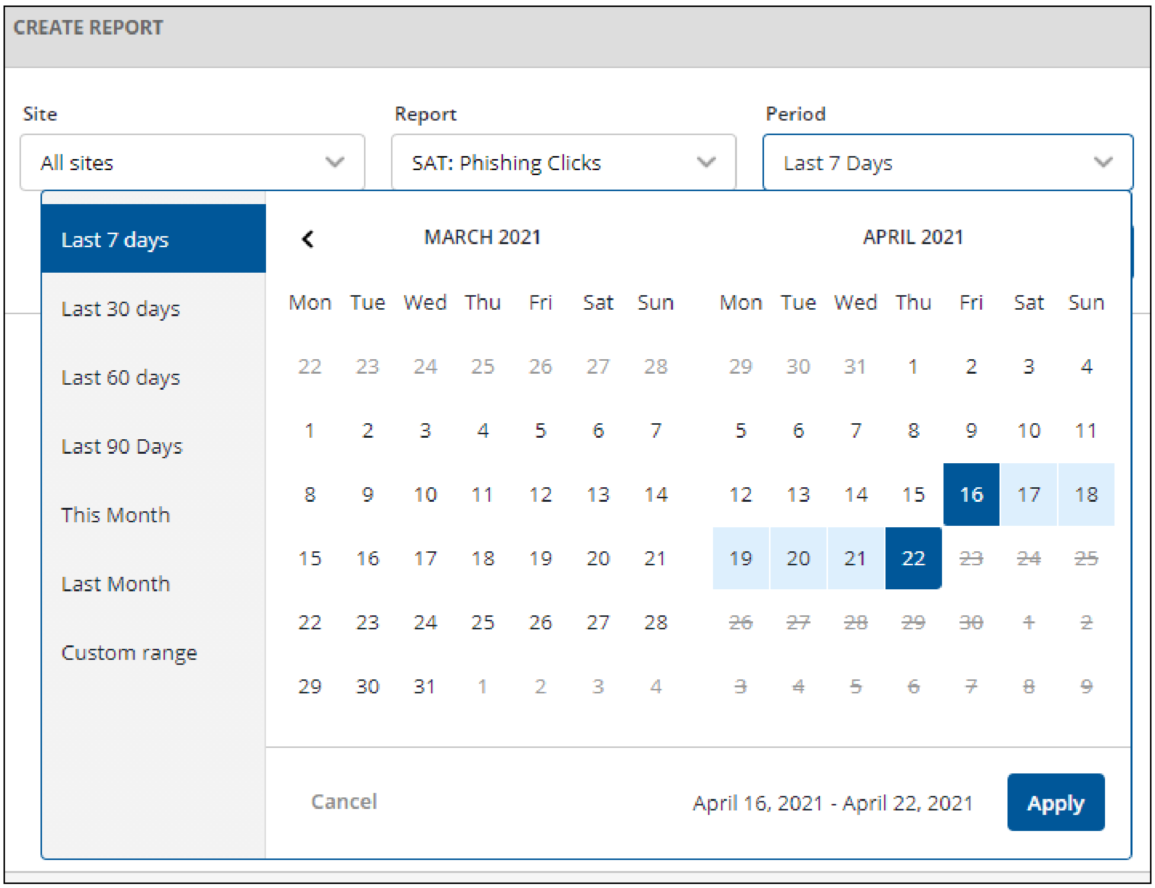
3. From the Site drop-down menu, select the site you want to run the report for.



4. From the Report drop-down menu, select any of the following reports:
   - SAT: Phishing Clicks
   - SAT: Training Progress
   - SAT: Usage Report

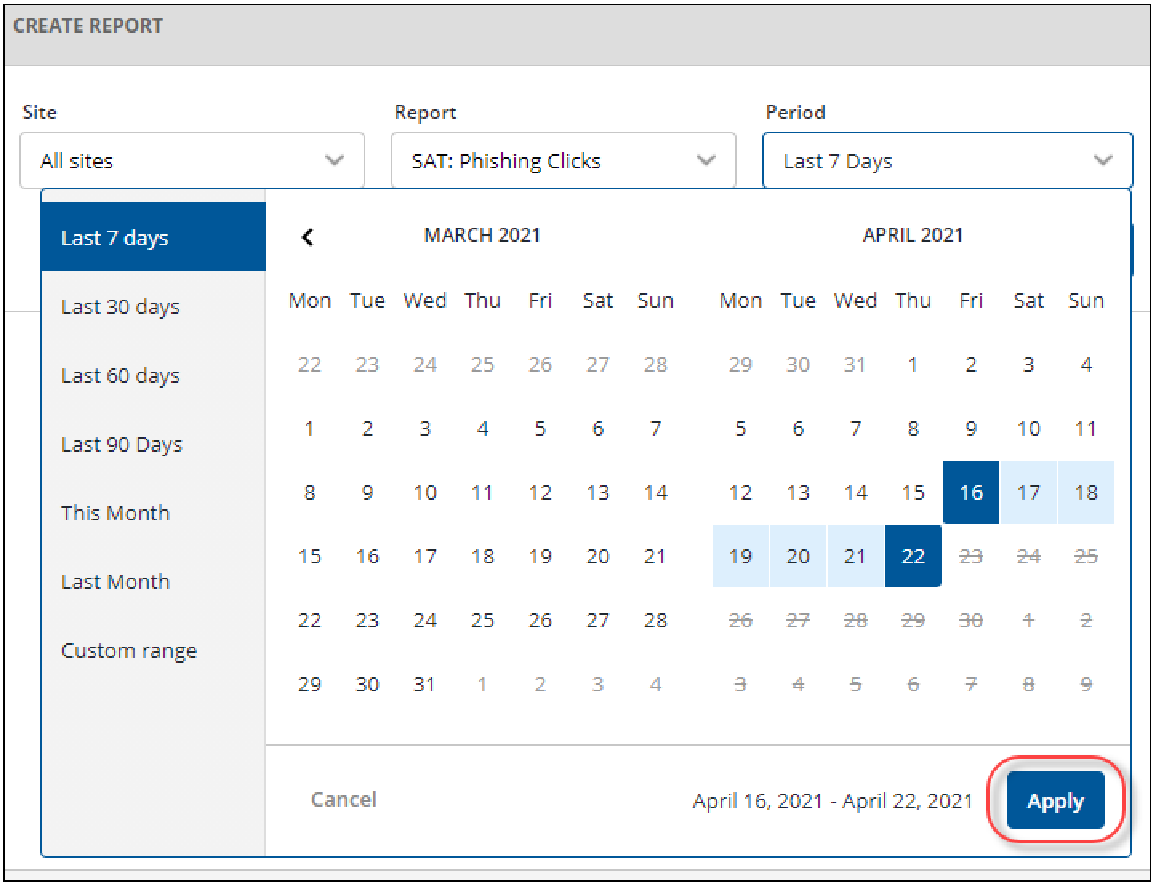


5. From the Period drop-down menu, select one of the following date ranges or select a custom date range:
   - Last 7 days
   - Last 30 days
   - Last 60 days
   - This month
   - Last month
   - Custom range

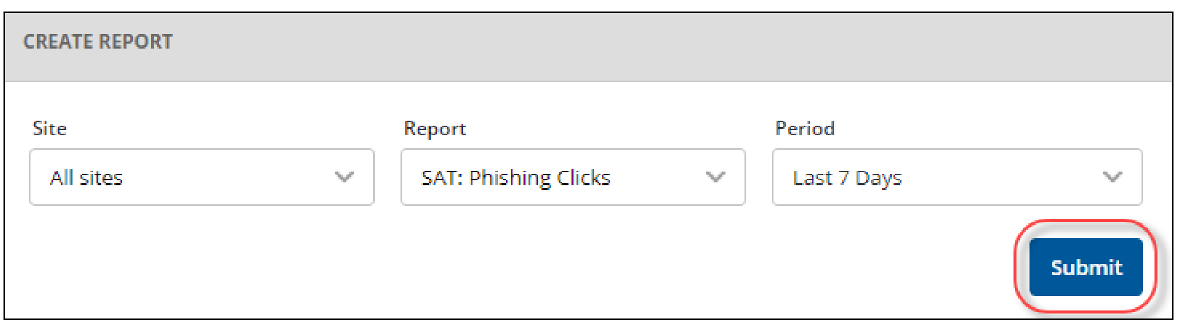


Note: The Period drop-down menu does not display until you have selected one of the Security Awareness Training reports.

6. When you're done selecting the date range, click the **Apply** button.



7. When you're ready to run the report, click the **Submit** button.



The report displays in the bottom pane, and includes the following columns:

REPORT NAME	COLUMNS
SAT: Phishing Clicks Report	• Site • Target Email • Phishing Campaigns • Email Clicks • Lure Clicks
SAT: Training Progress Report	• Site • Target Email • Training Campaigns • Training Progress
SAT: Usage Report	• Site • Target Email • Training Campaigns • Training Progress

Accessing Breach Reports

The Breach Report and risk assessment tool now allows Security Awareness Training admins to generate a report that outlines breaches associated with any client's domain. The report includes a breach summary, a list of breached data by category, as well as the users impacted at each client site.

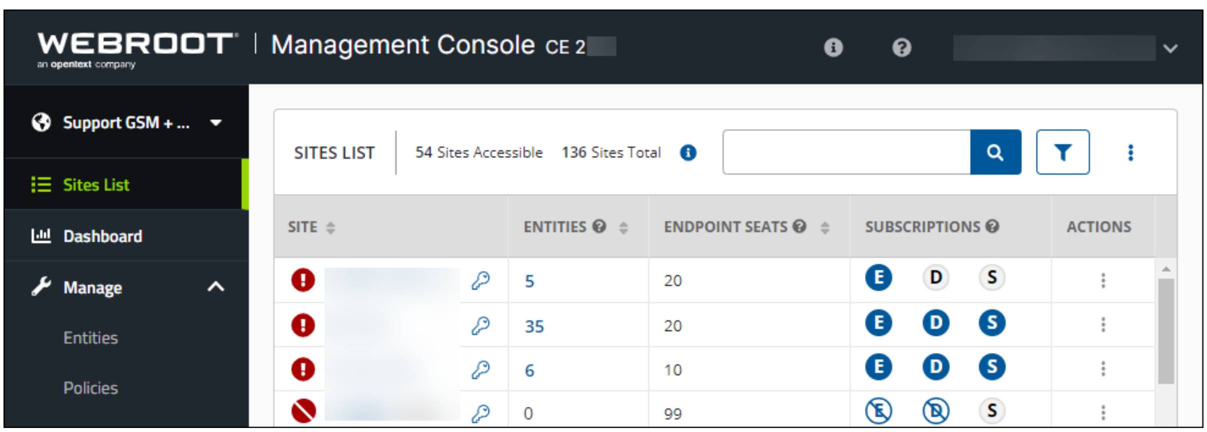
The report provides ideal documentation to help admins determine and demonstrate real world risks so they can advise clients' executive management on services and tactics accordingly to avoid future security incidents.

> **Note:** With enhanced domain verification to support access to the Breach Report you must use a domain admin level email address such as admin@domain.com or postmaster@domain. com, etc, to view the Breach Report.

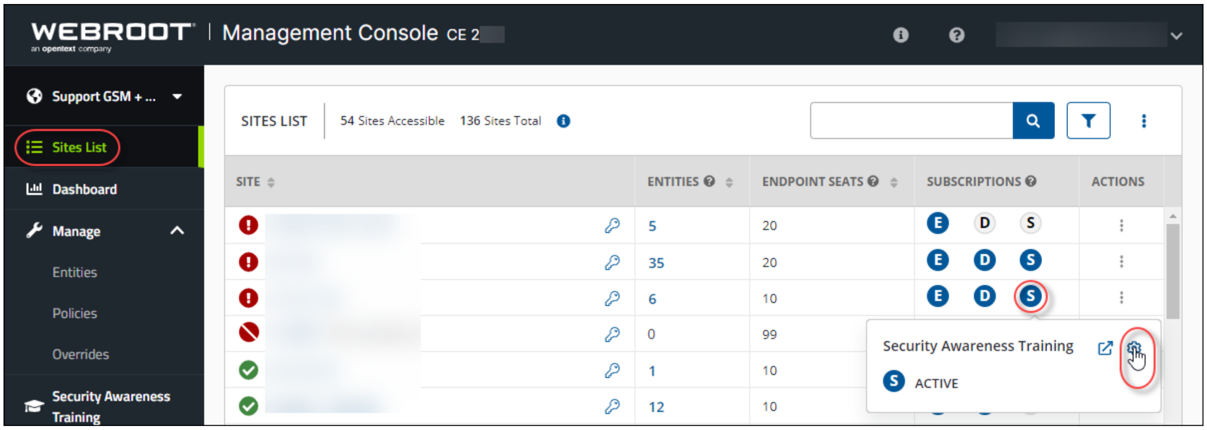
To access a Breach report:

1. Log in to the Management Console.

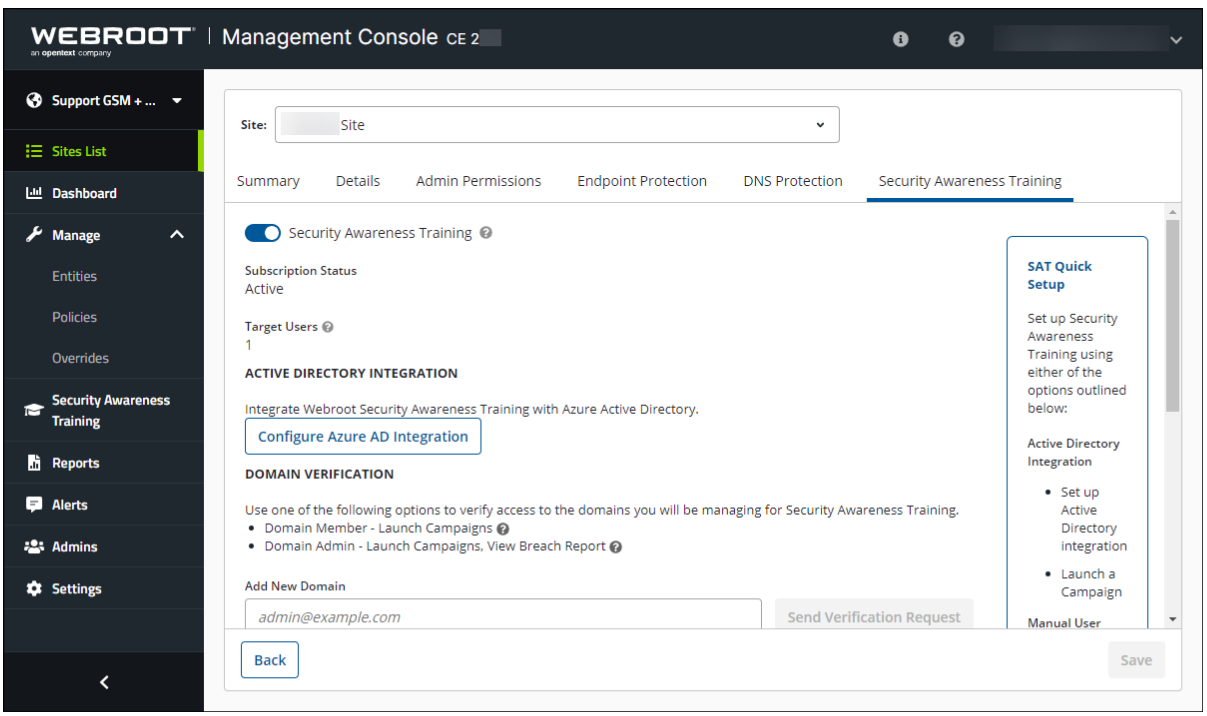
   The Management Console displays.



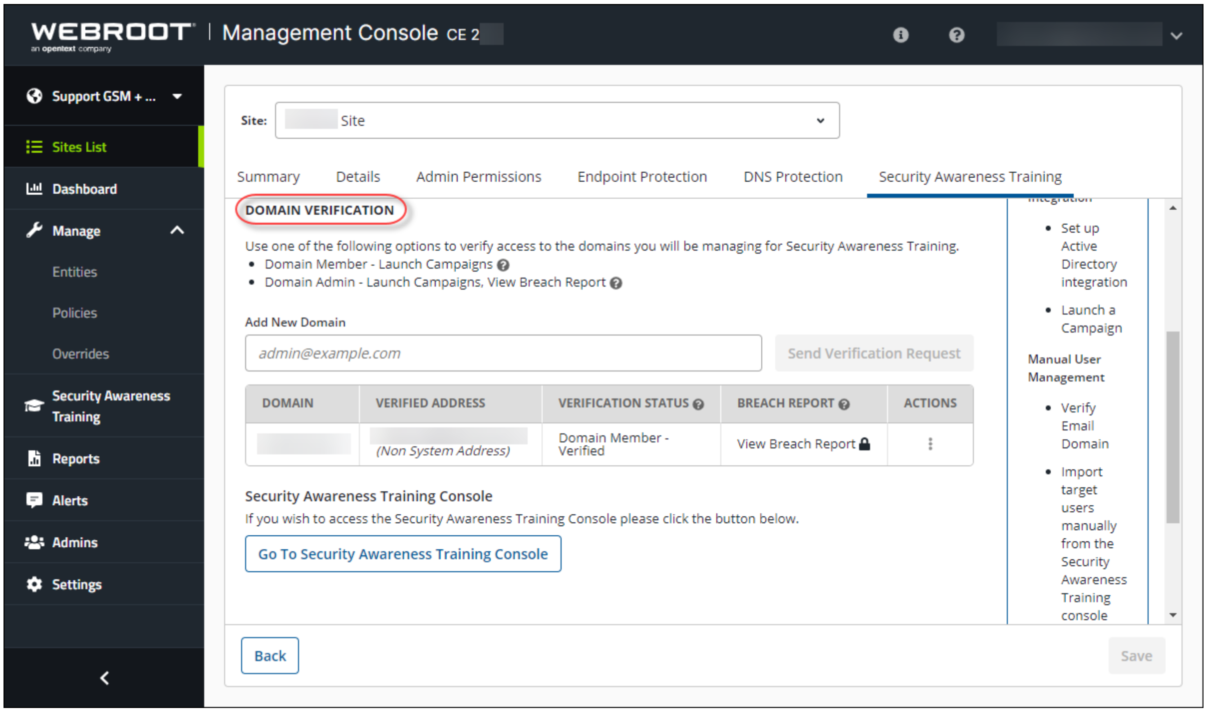
2. Click the **Settings** icon.



The Security Awareness Training tab displays.



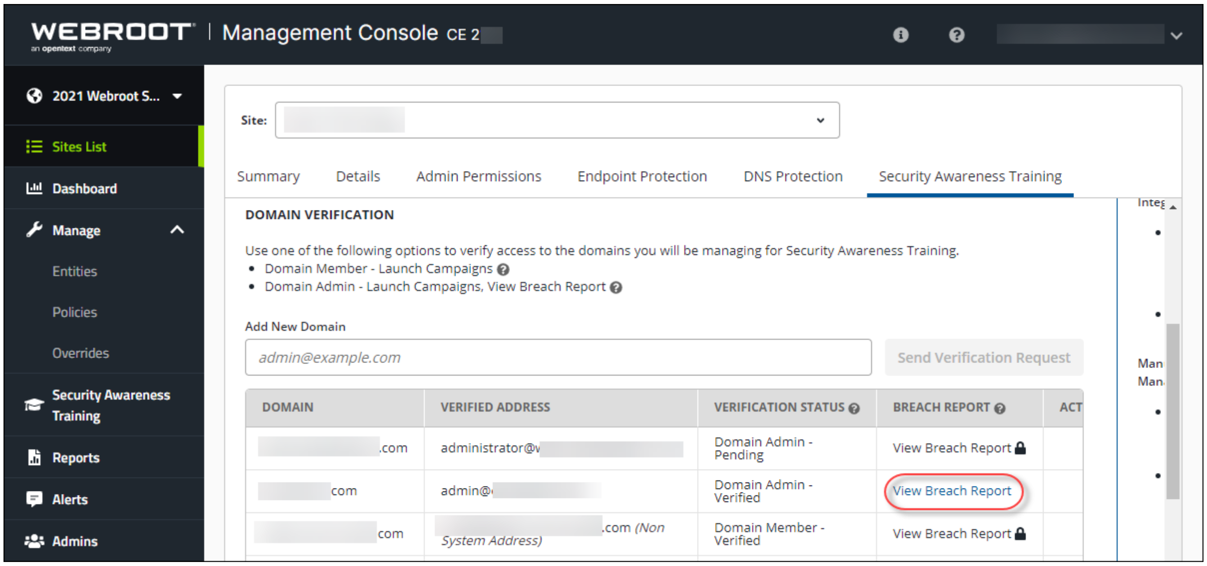
3. Scroll down to the Domain Verification area.



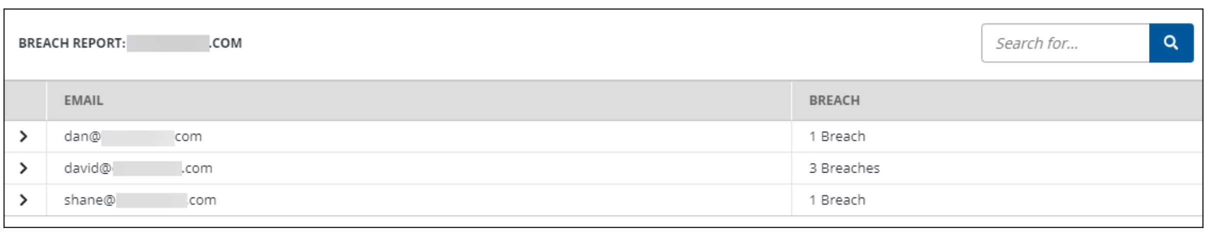
4. In the Add New Domain field, add one of the following two email types to verify access to domains you will be managing:
   - **Domain Member** – You can launch campaigns.
   - **Domain Admin** – You can launch campaign and view breach reports.

Note: Hover over the Question Mark icon for additional information.

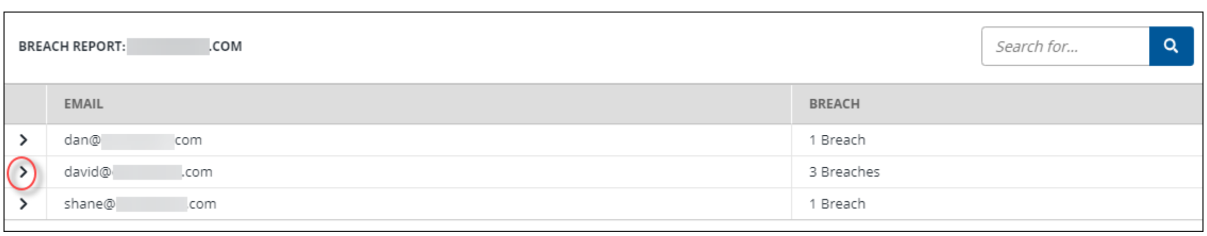
5. For the domain you want to view the Breach report for, click **View Breach Report**.



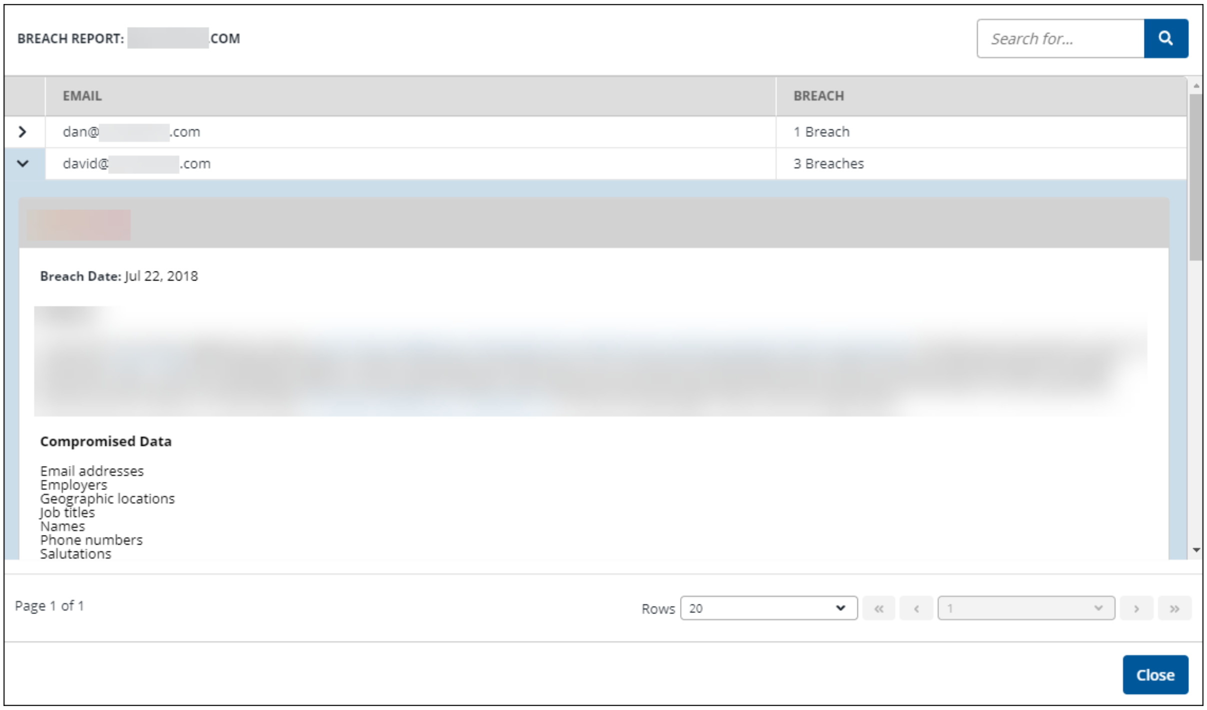
The Breach Report displays, with information about the emails that were breached and the sources of the breach.



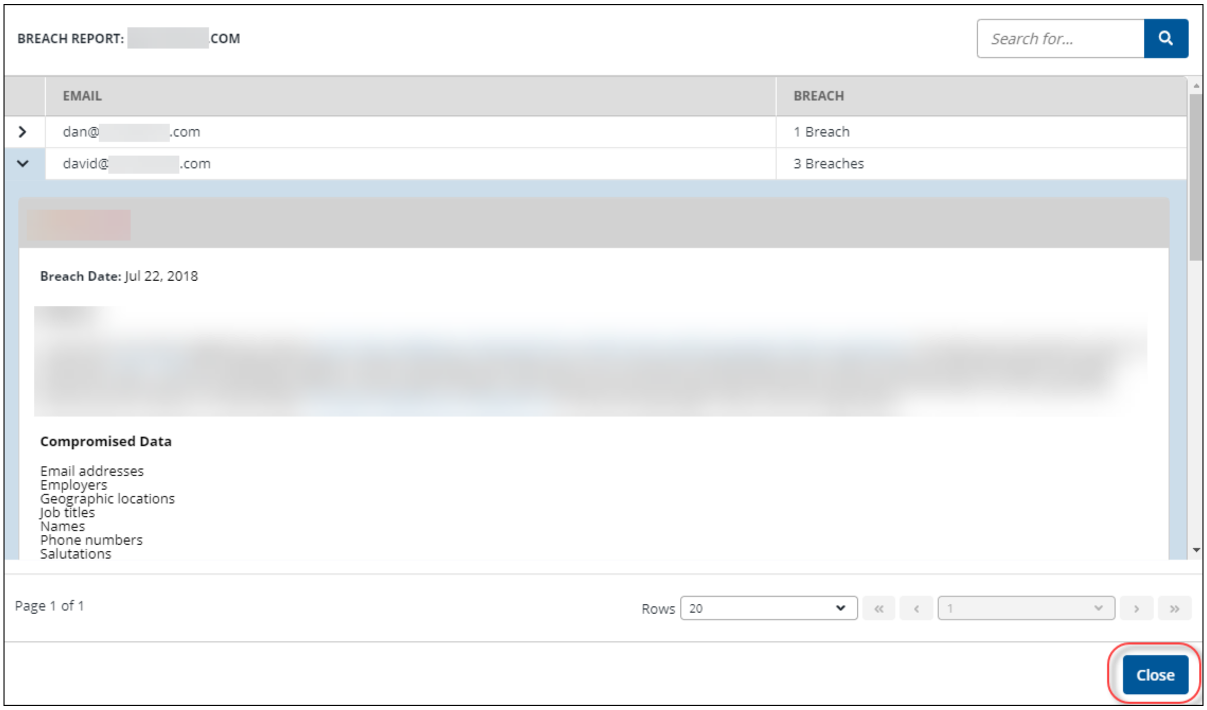
6. For additional information, click on the arrow next to the email in question.



Additional information about the breach displays, including the date, the name of the company, and the type of information that was compromised.


BREACH REPORT: COM
Search for...
EMAIL
BREACH
dan@ .com
1 Breach
david@ .com
3 Breaches
Breach Date: Jul 22, 2018
Compromised Data
Email addresses
Employers
Geographic locations
Job titles
Names
Phone numbers
Salutations
Page 1 of 1
Rows 20
Close

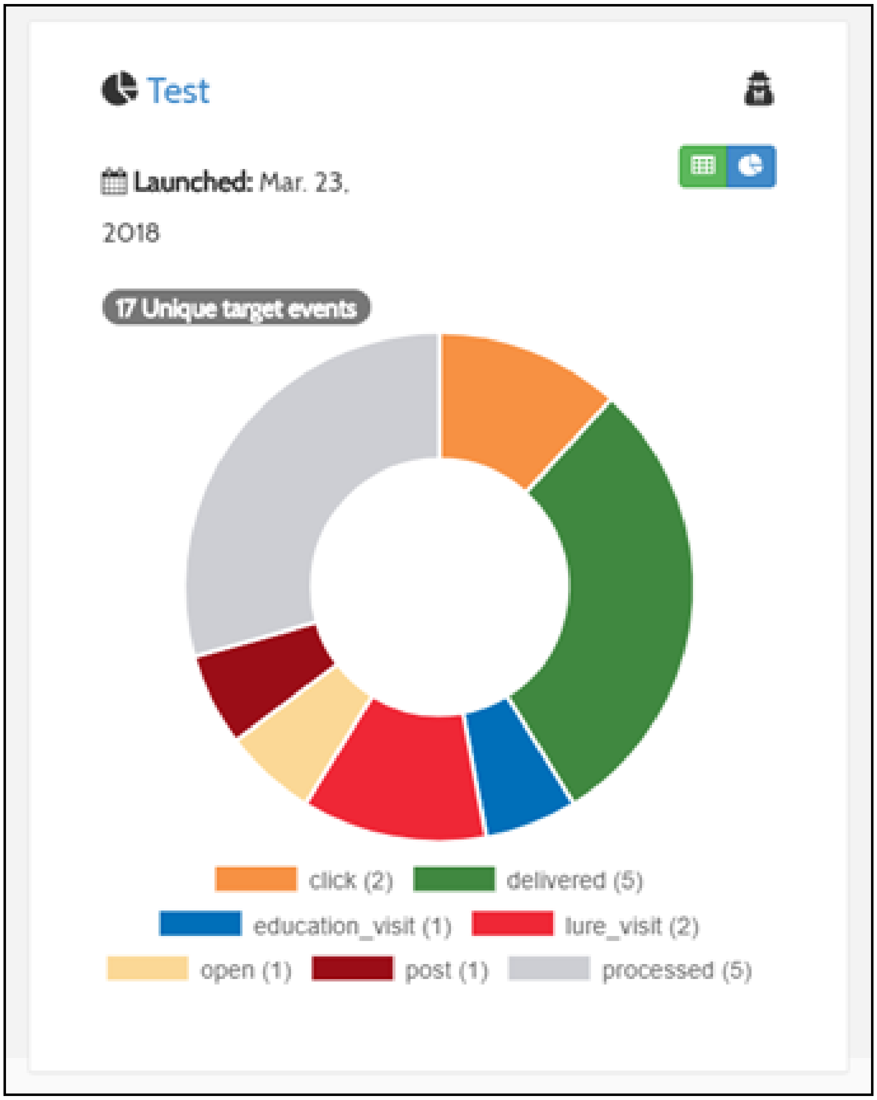
7. When you're done, click the **Close** button.



About Phishing Simulation Reports

Webroot Security Awareness Training includes the ability to create phishing simulation campaigns that mimic a real-world phishing scenario. Webroot uses a transaction email service to track delivery, opens, clicks and data posts for every phishing simulation sent on a per-user basis.

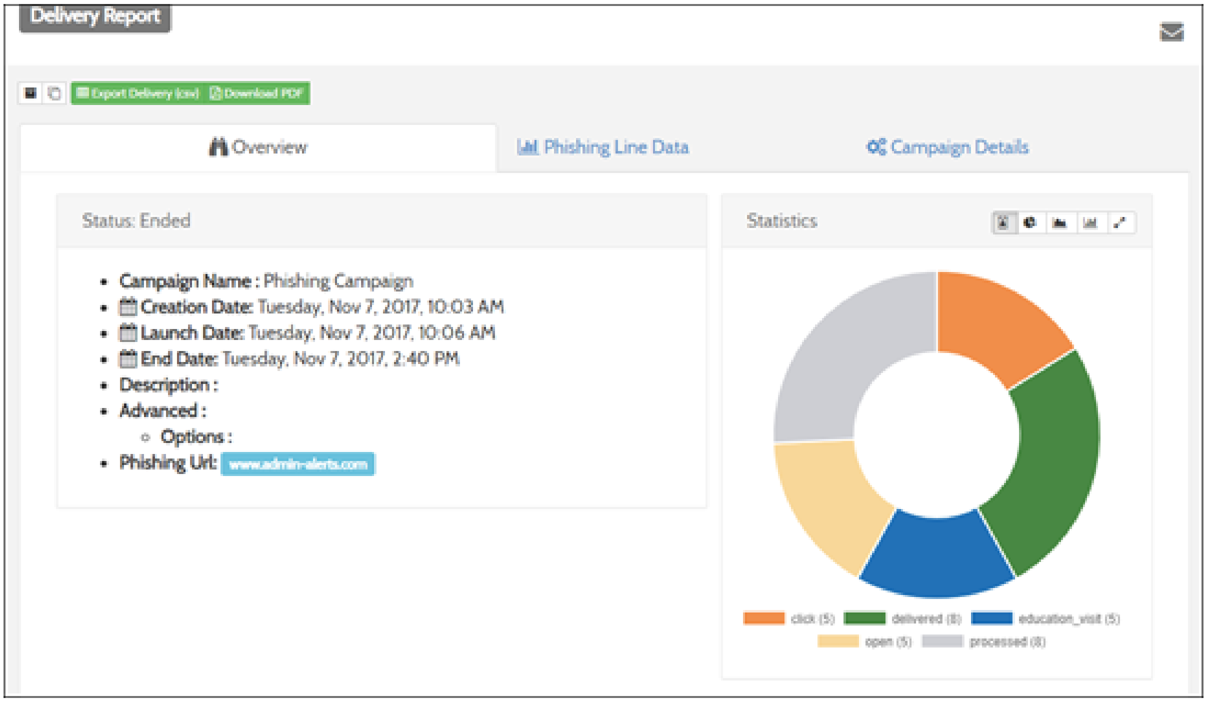
Sample Phishing Report Campaign Summary



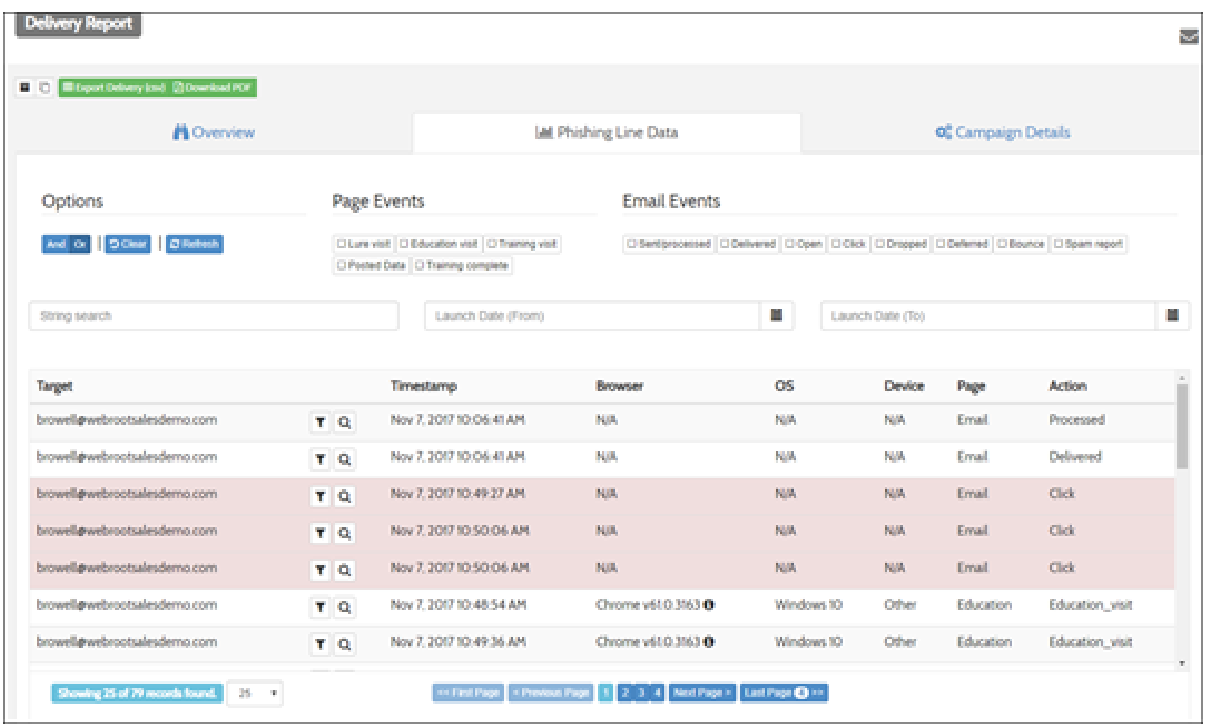
Understanding Email Events

You will be able to see data about the following types of email events in the Email Activity Feed:

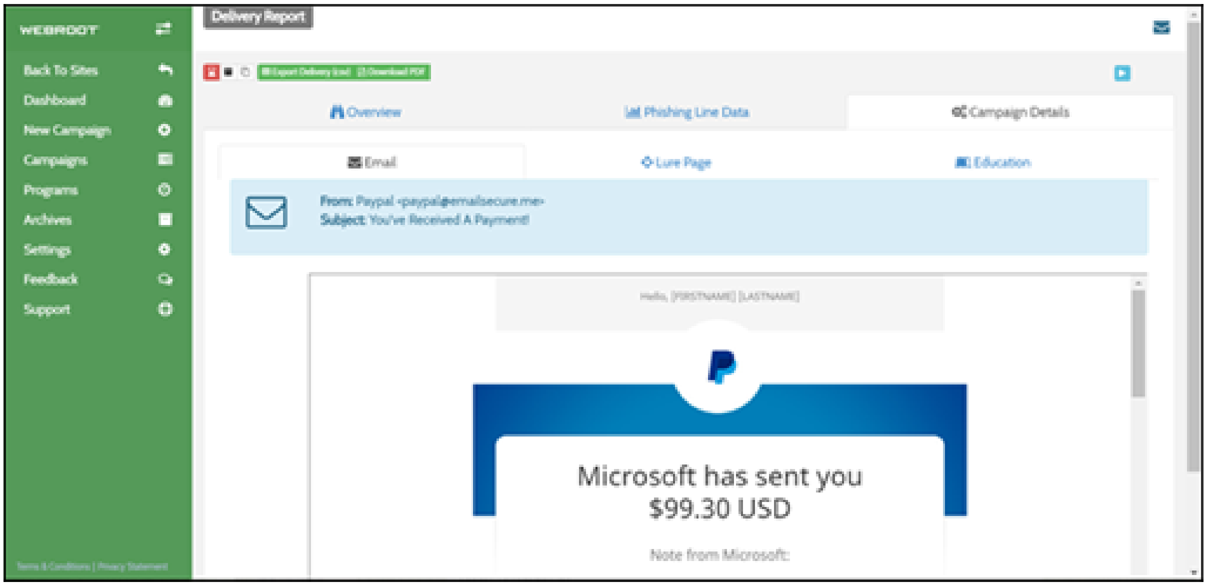
- **Processed** — Requests from your website, application, or mail client via SMTP Relay or the API that the emailer processed.
- **Clicks** — When a recipient clicks one of the Click Tracked links in your email.
- **Delivered** — An email that was delivered to a recipient.
- **Opens** — When an email is opened by a recipient.
- **Deferred** — The recipient mail server asked the emailer to stop sending emails so quickly.
- **Drops** — The emailer drops an email when one of the following occurs:
  - The contact on that email is in one of your suppression groups.
  - The recipient email previously bounced.
  - The recipient has marked your email as spam.
- **Bounces** — When an attempt is made to deliver an email, but the recipient mail server rejects it.
- **Spam Reports** — When a recipient marks your email as spam and their mail server tells us about it.



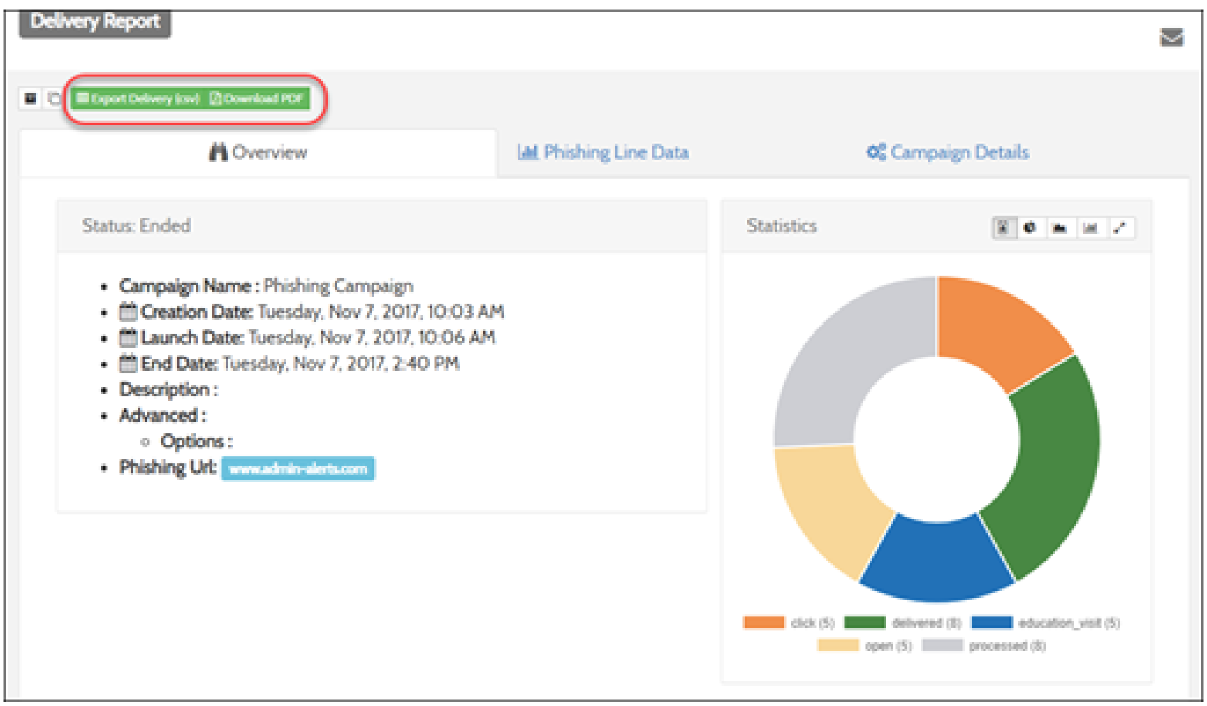
The Interactive Phishing Line report allows a user to select actions and filter in real-time.



A summary of the phishing simulation details can be seen within the campaign report.

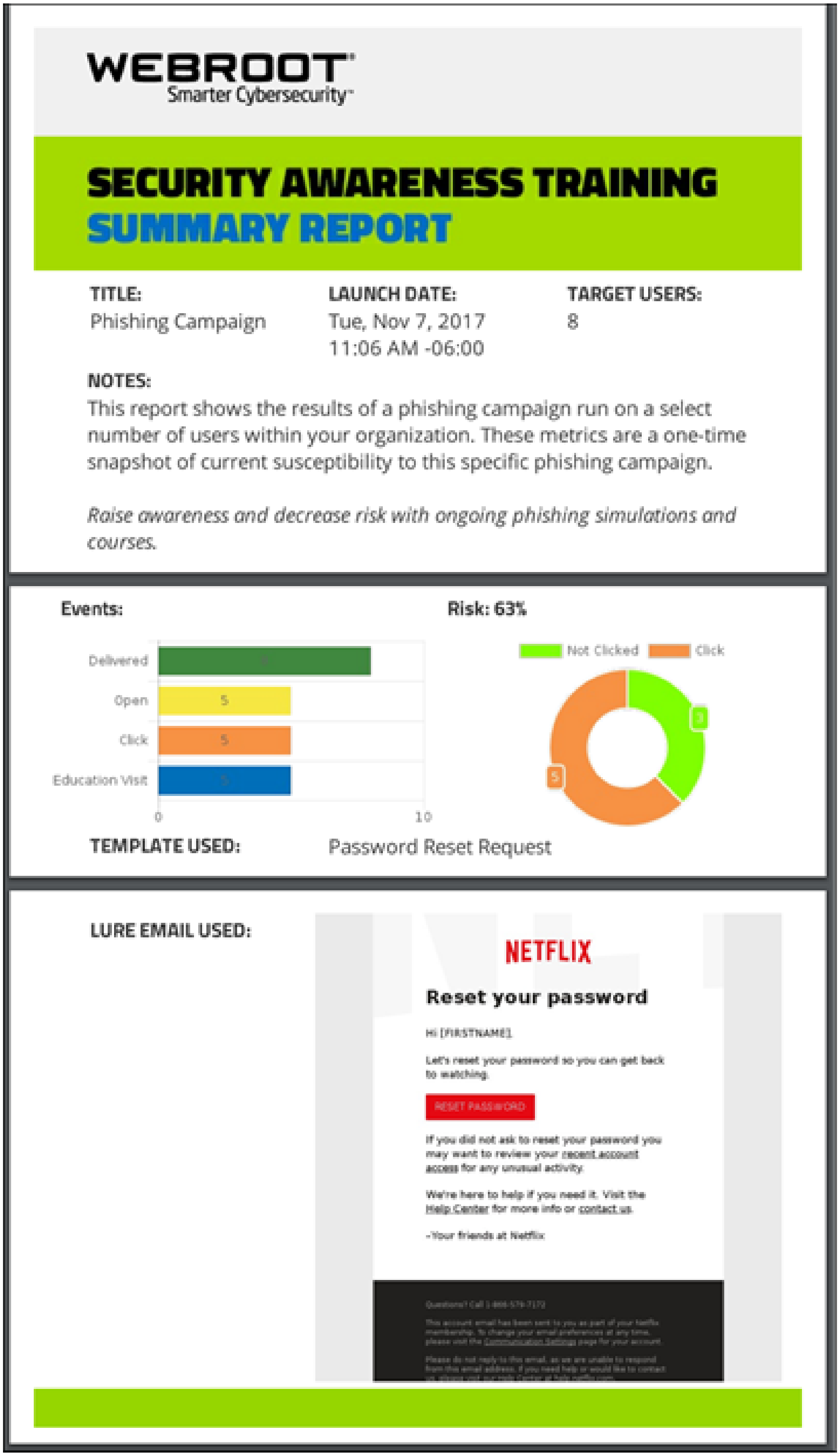


Reports can be exported to CSV, PDF or screen captured and shared as needed.



Sample PDF Summary Report

The PDF report can be downloaded at any time or set to automatically deliver at the end of a campaign to a pre-set list of recipients.



WEBROOT
Smarter Cybersecurity

SECURITY AWARENESS TRAINING
SUMMARY REPORT

TITLE: Phishing Campaign

LAUNCH DATE: Tue, Nov 7, 2017 11:06 AM -06:00

TARGET USERS: 8

NOTES:
This report shows the results of a phishing campaign run on a select number of users within your organization. These metrics are a one-time snapshot of current susceptibility to this specific phishing campaign.

Raise awareness and decrease risk with ongoing phishing simulations and courses.

Events:

Risk: 63%

TEMPLATE USED: Password Reset Request

LURE EMAIL USED:

Chapter 6: Managing Spam Filters

To start managing spam filters, see the following topics:

Allowing Emails In Proofpoint Essentials 157
Allowing Email In Microsoft Exchange and Microsoft 365 158
Allowing Emails In Google Workspace 172
Allowing Webroot Training Email Servers 173

Allowing Emails In Proofpoint Essentials

To prevent or resolve mail delivery issues when using Webroot Security Awareness Training with Proofpoint Essentials, you can create a filter in Proofpoint to allow mail sent from the Webroot Security Awareness Training email servers, which are specified in the Knowledge Base.

Follow these instructions to add a filter to allow email from Webroot's email servers:

1. Navigate to **Security Settings > Email > Filter Policies**.
2. On the Inbound tab, click **New Filter**.
3. Enter a descriptive **Filter Name**.
4. For Direction, select **Inbound** (it should have defaulted to the tab being used for the procedure).
5. Click **Continue**.
6. For Scope, select **Company**.
7. For the first condition (if statement):
   - Select **Email Headers** from the drop-down list of message elements.
   - Select **Contain(s) Any Of** from the drop-down list of operators.
   - Enter the first Webroot Security Awareness Training email server, which is specified in the Knowledge Base.
8. Repeat the above step, entering a condition (if statement) for each of the remaining Webroot Security Awareness Training email servers, which are specified in the Knowledge Base.
9. For Action (Do statement), from the drop-down list select **Allow**.
10. Click Save.

Click here to see an article from Proofpoint on how to set up filters for Proofpoint Essentials.

Allowing Email In Microsoft Exchange and Microsoft 365

If you use Microsoft Exchange or Microsoft 365, you need to allow the IP address for the mail servers that Webroot Security Awareness Training uses to send email messages to targets.

The Webroot Security Awareness Training email servers are specified in the Knowledge Base.

Here are the parts involved with allowing email in Microsoft Exchange and Microsoft 365:

Part 1: Create an IP Allow List with Webroot's email server IP address.

Part 2: Set up a mail flow rule to bypass spam filtering and the Clutter folder.

Part 3:[Microsoft 365 only] Set up a rule to bypass the Junk Folder.

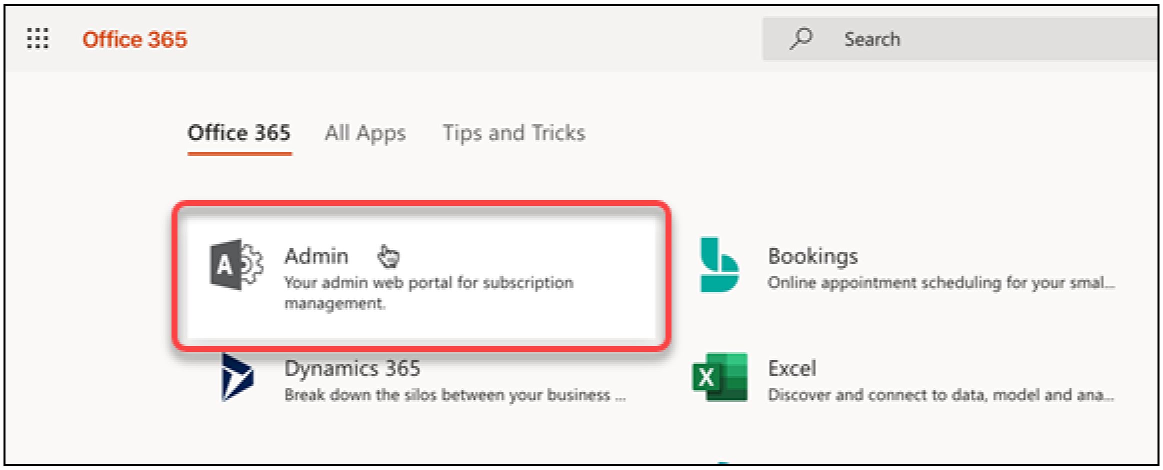
Part 4: Testing.

Note: We recommend waiting 1 to 2 hours before testing to allow the settings to propagate across your environment. You can use a small phishing campaign to test that inbound email is working properly. Please see Creating Phishing Simulations on page 8 for help setting up a campaign.

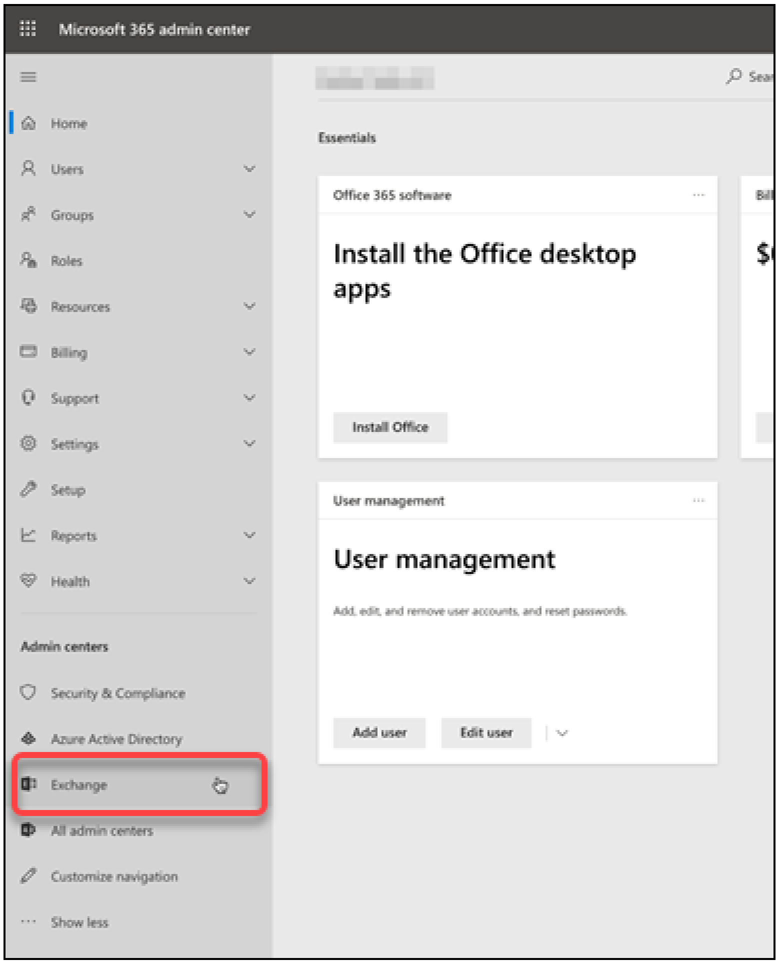
Part 1: Creating an IP Allow List with Webroot's email server IP address:

This step enables Webroot's email server to be allowed to deliver mail inbound to your Exchange or Microsoft 365 server.

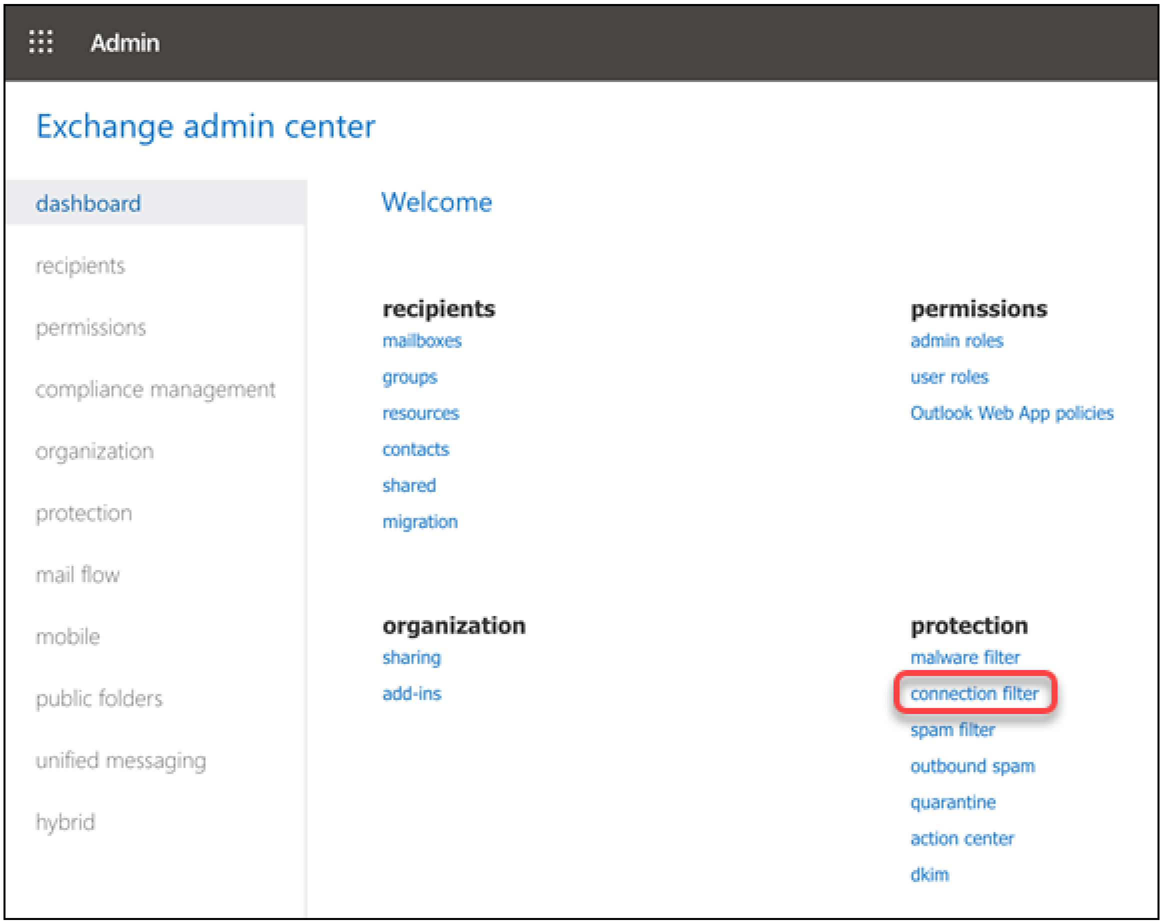
1. Navigate to your **Exchange admin center (EAC)** by signing into Microsoft 365 using your account, and then choose the **Admin** tile.



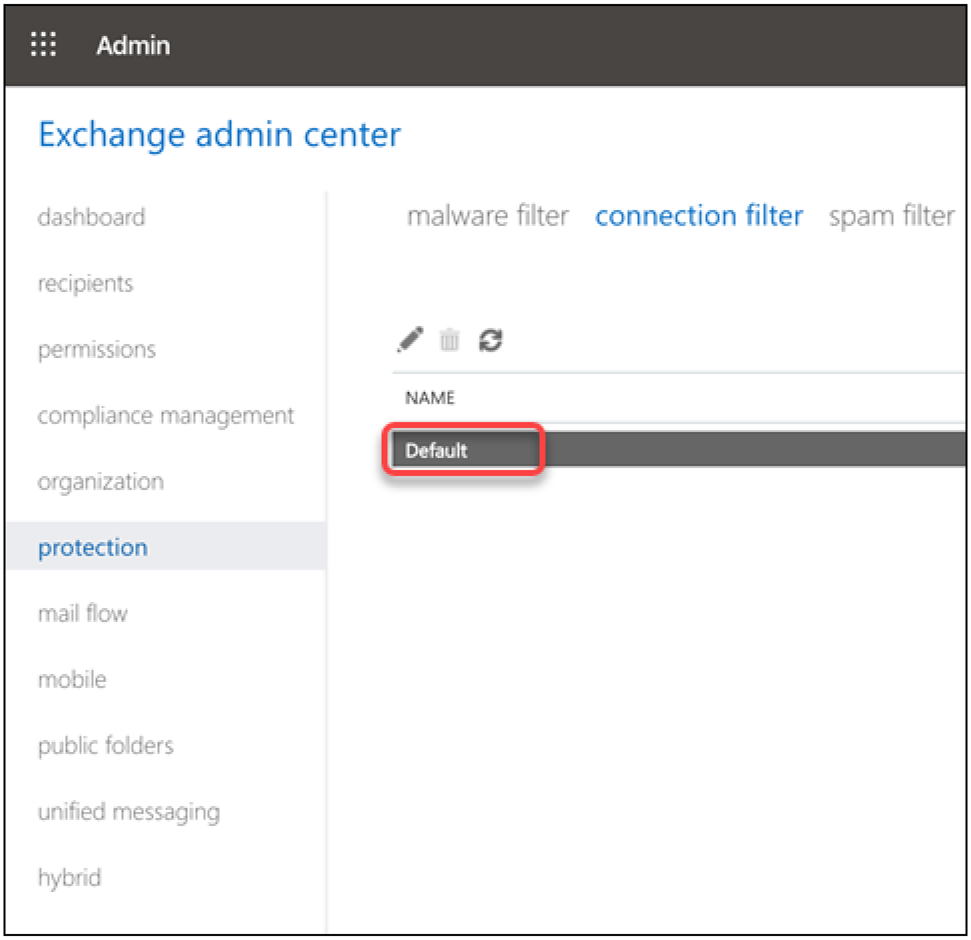
2. You are now in the Microsoft Microsoft 365 admin center. Use the left navigation list to choose **Admin centers > Exchange**.



3. In the **Exchange admin center (EAC)**, navigate to **Protection > Connection filter**.


Admin
Exchange admin center
dashboard
recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging
hybrid
Welcome
recipients
mailboxes
groups
resources
contacts
shared
migration
permissions
admin roles
user roles
Outlook Web App policies
organization
sharing
add-ins
protection
malware filter
connection filter
spam filter
outbound spam
quarantine
action center
dkim

4. Double-click the **Default** policy to start editing it.

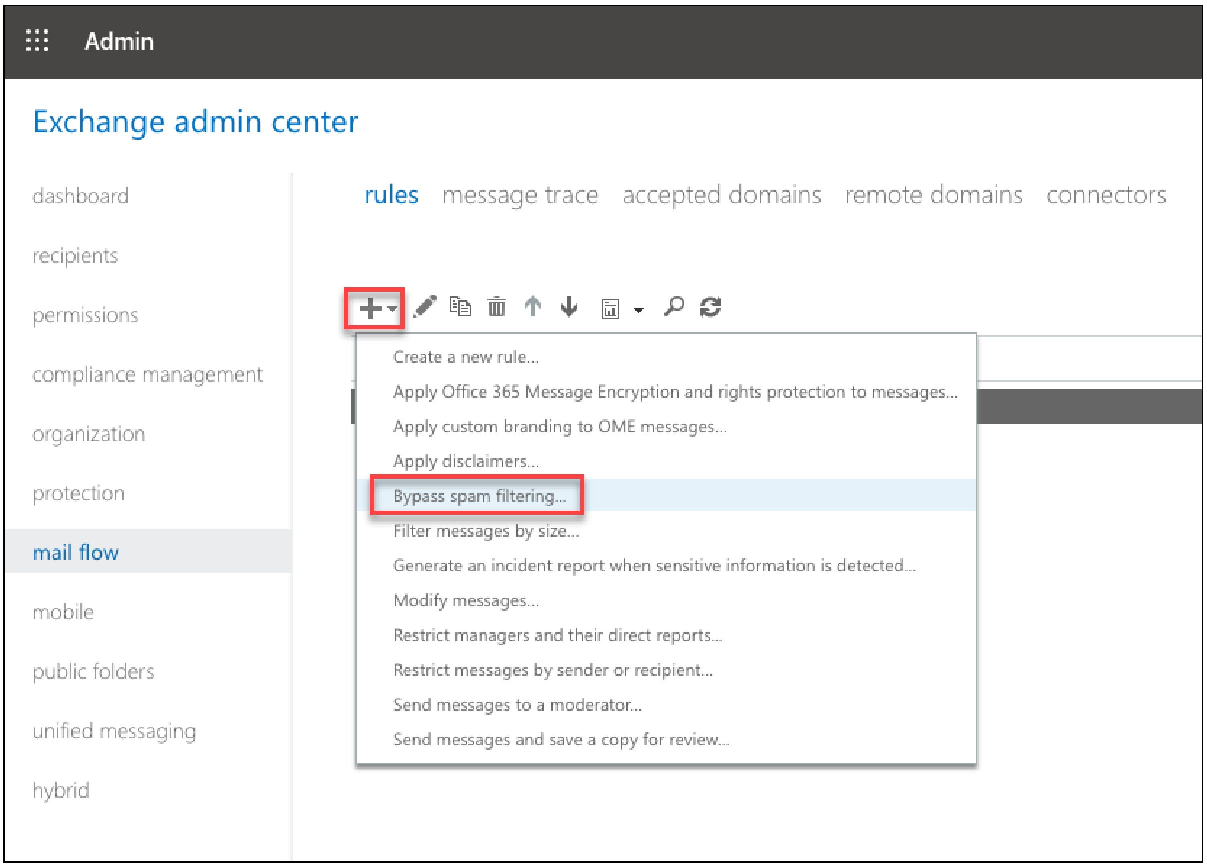


5. Click the **Connection filtering** menu item and then create an IP Allow list with Webroot's sender email IP addresses:
   - Under the **IP Allow list**, click on the click the **Add icon (+)**.
   - In the dialog box, enter the IP address for each of the Webroot Security Awareness Training email servers, which are specified in the Knowledge Base.
6. Click **OK**, then **Save** to complete part 1.

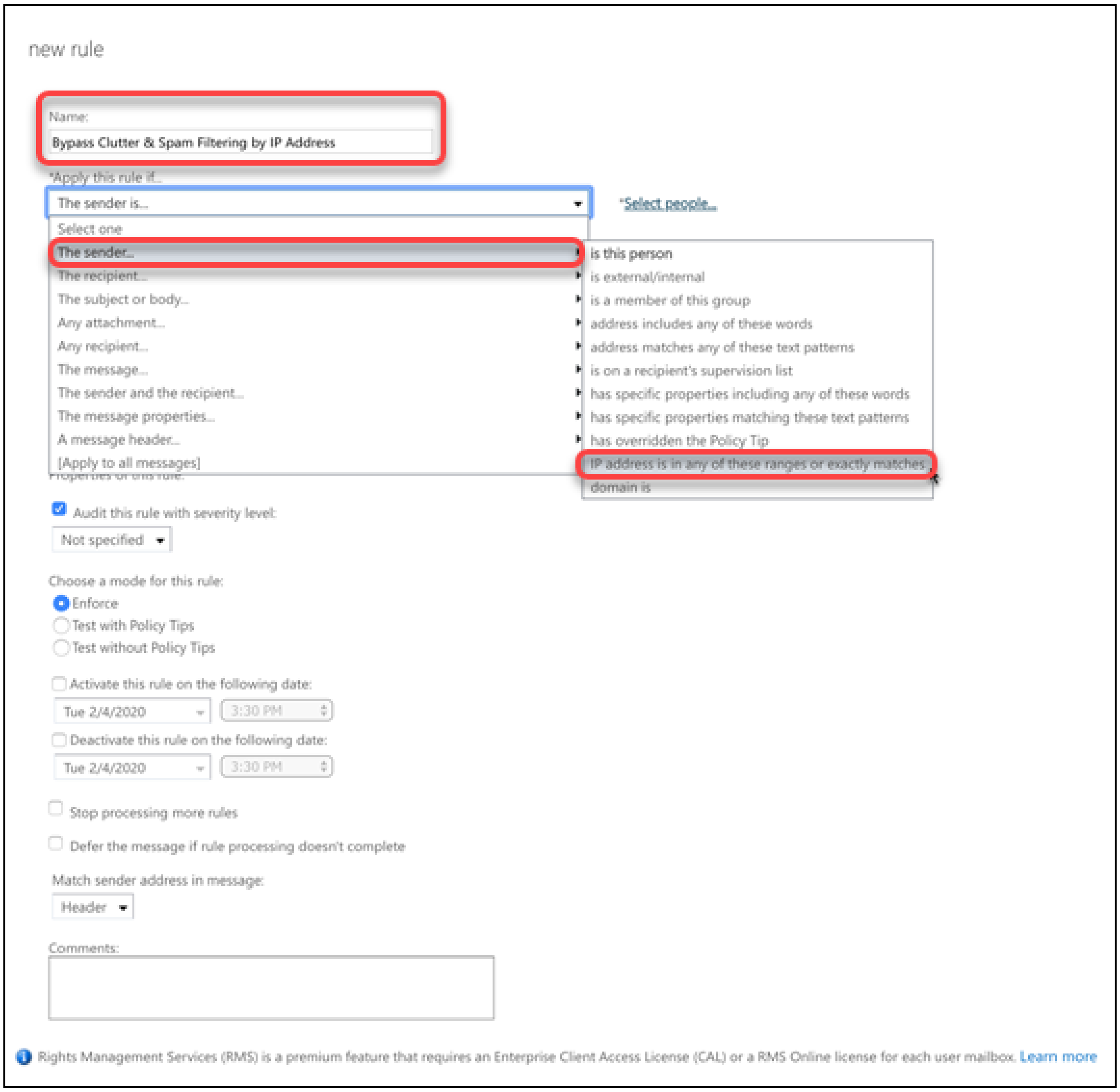
Part 2: Setting up a mail flow rule to bypass spam filtering and the Clutter folder

In part 2, you will set up a mail flow rule (AKA transport rule) to ensure Webroot's training email messages will bypass your Clutter folder as well as any spam filtering enabled, for both Microsoft Exchange and Microsoft 365.

1. Open the **Exchange admin center (EAC)**. See Part 1, Step 1 above for help if needed.
2. In the **EAC**, go to **mail flow > rules**, click the **Add icon (+)** > **Bypass spam filtering...**.

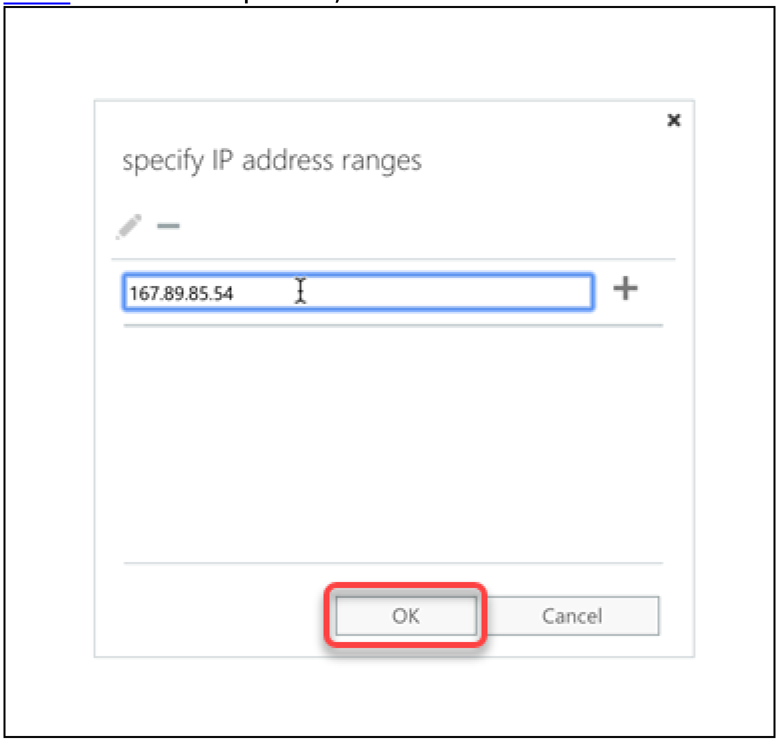


3. Provide a **Name** and add conditions for the new rule.

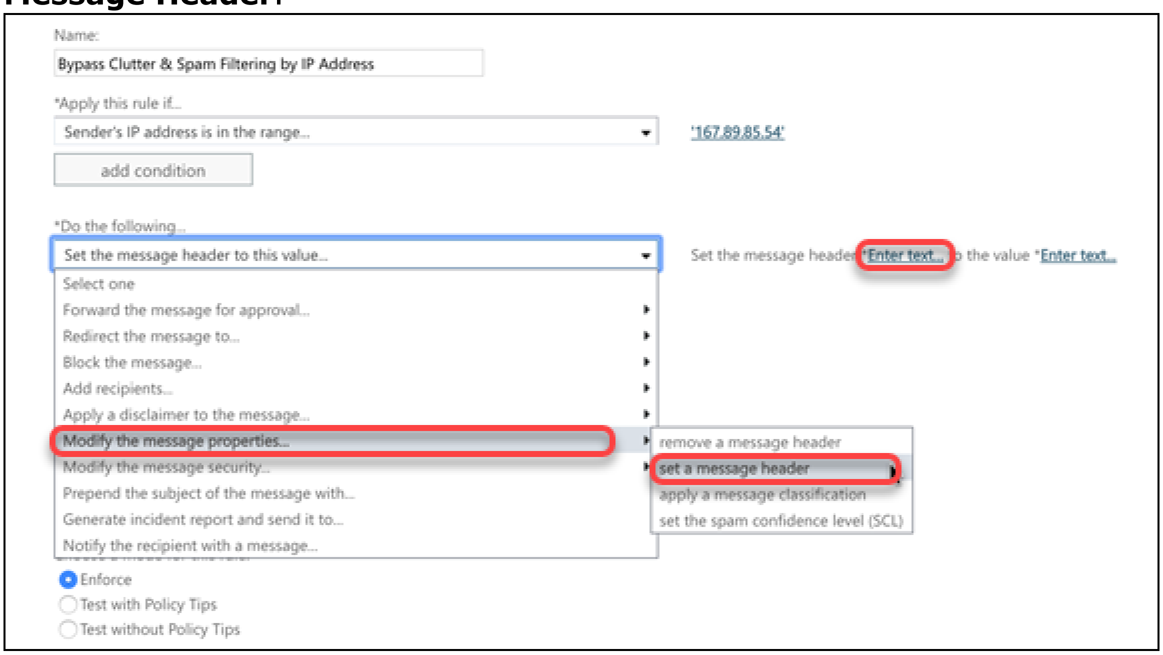


4. Add the condition **Apply this rule if...**
   - Select **The Sender**, then click on **More Options** and select **IP address is in any of these ranges or exactly matches**. Add the IP addresses for the Webroot Security Awareness Training email servers, which are specified in the [Knowledge](#)

Base. When completed, click **OK**.

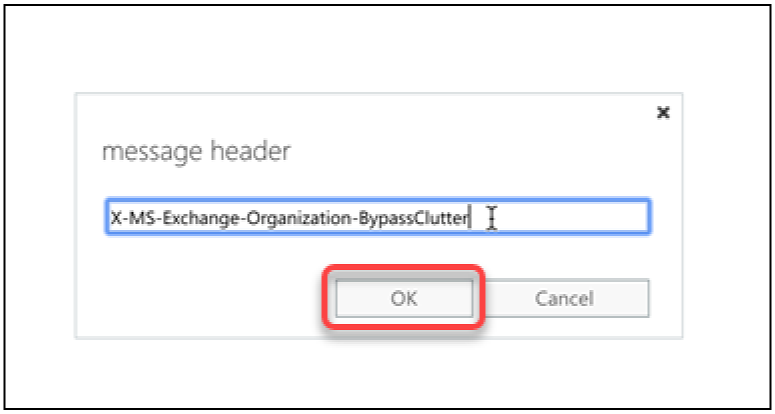


5. Beneath **Do the following**, click **Modify the message properties** then **Set a Message Header**.

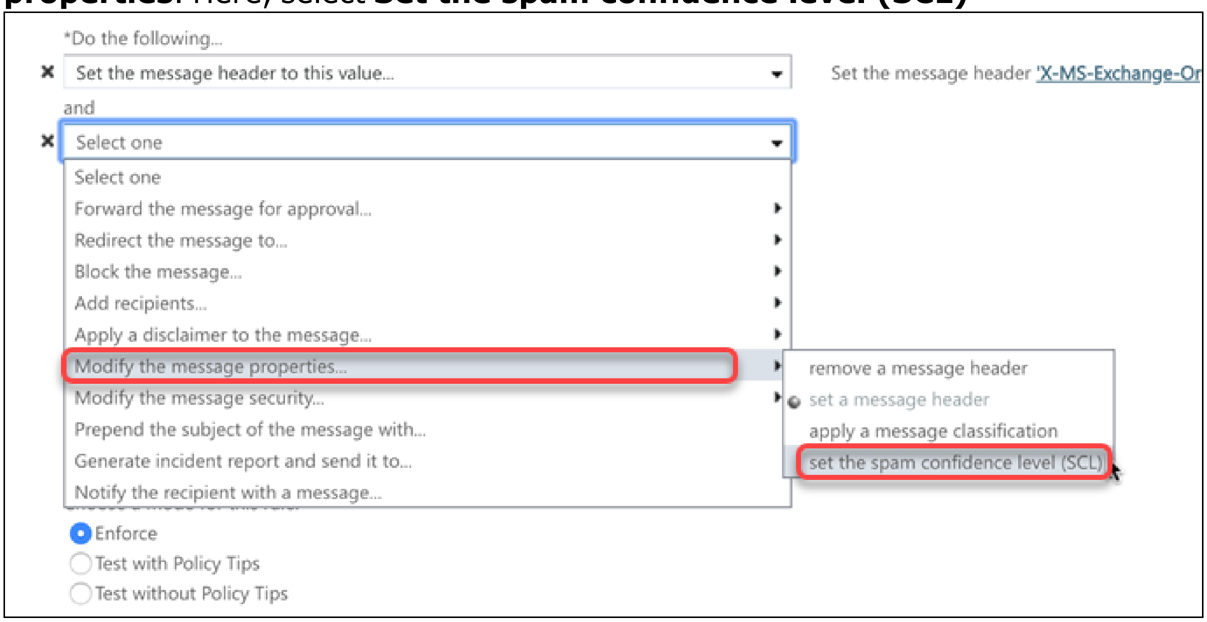


6. Click the ***Enter text...** button to set the message header to the value below. Click **OK** to continue.
   - **X-MS-Exchange-Organization-BypassClutter** to the value **true**

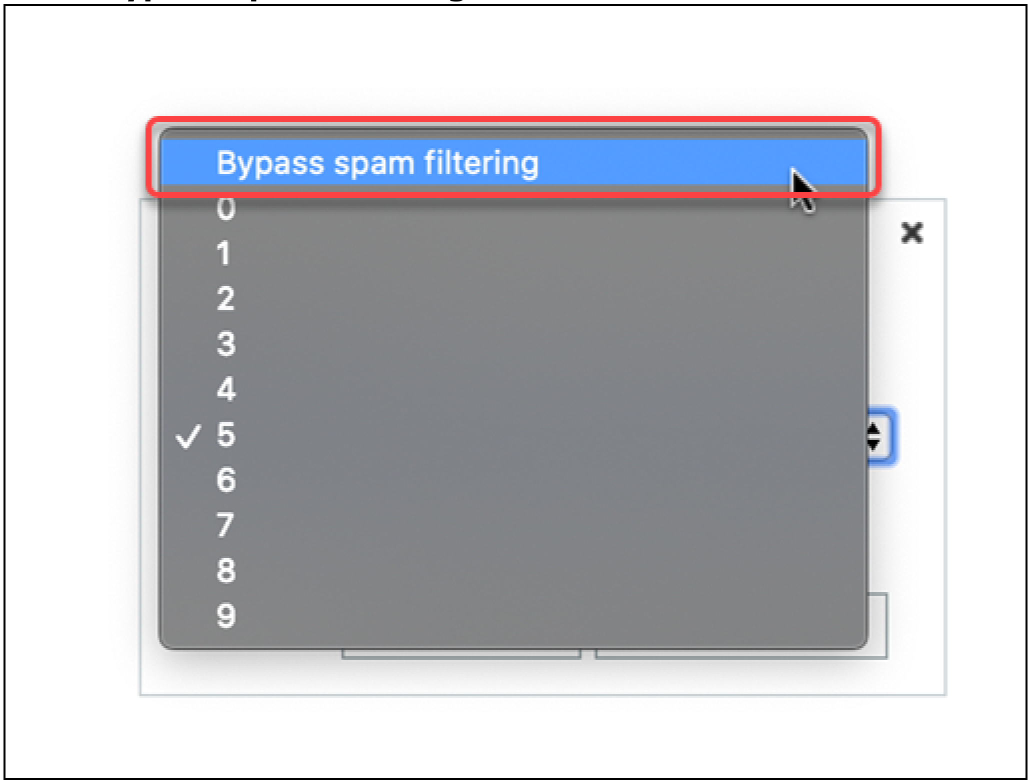
   Note:Both values are case sensitive.



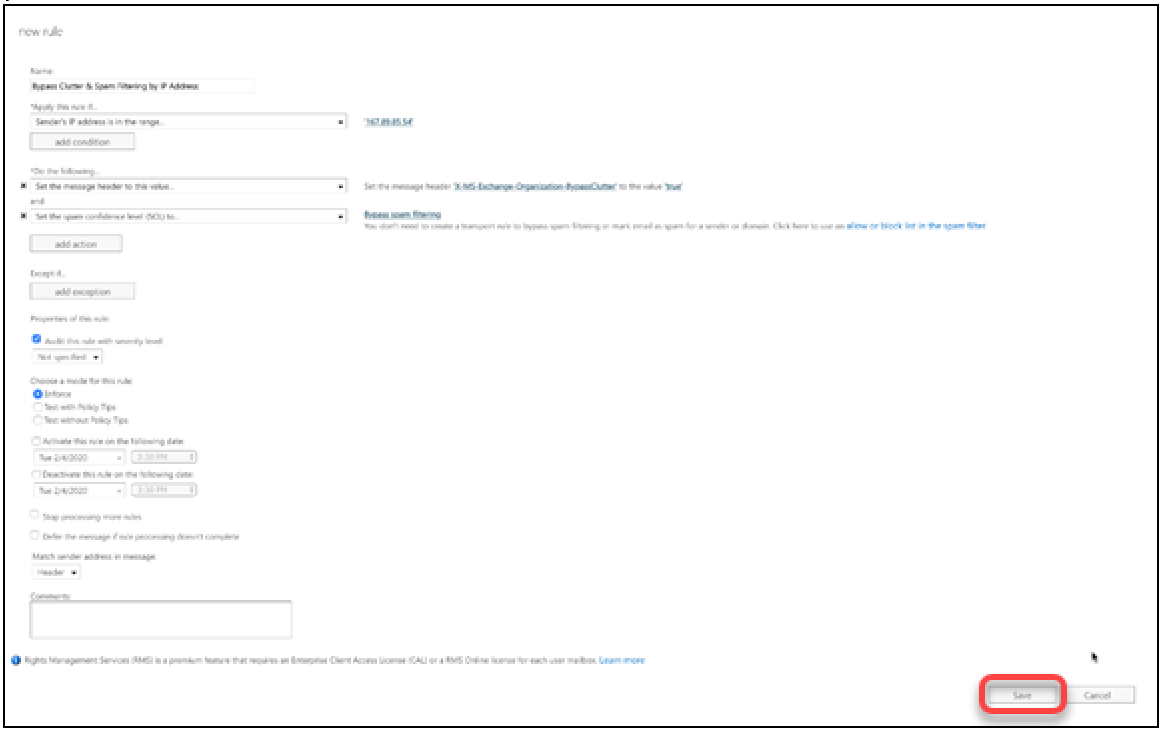
7. Add an additional action beneath **Do the following** to **Modify the message properties**. Here, select **Set the spam confidence level (SCL)**



8. Select **Bypass Spam Filtering**.



9. Review the settings and once verified, click **Save** to proceed and complete the process.



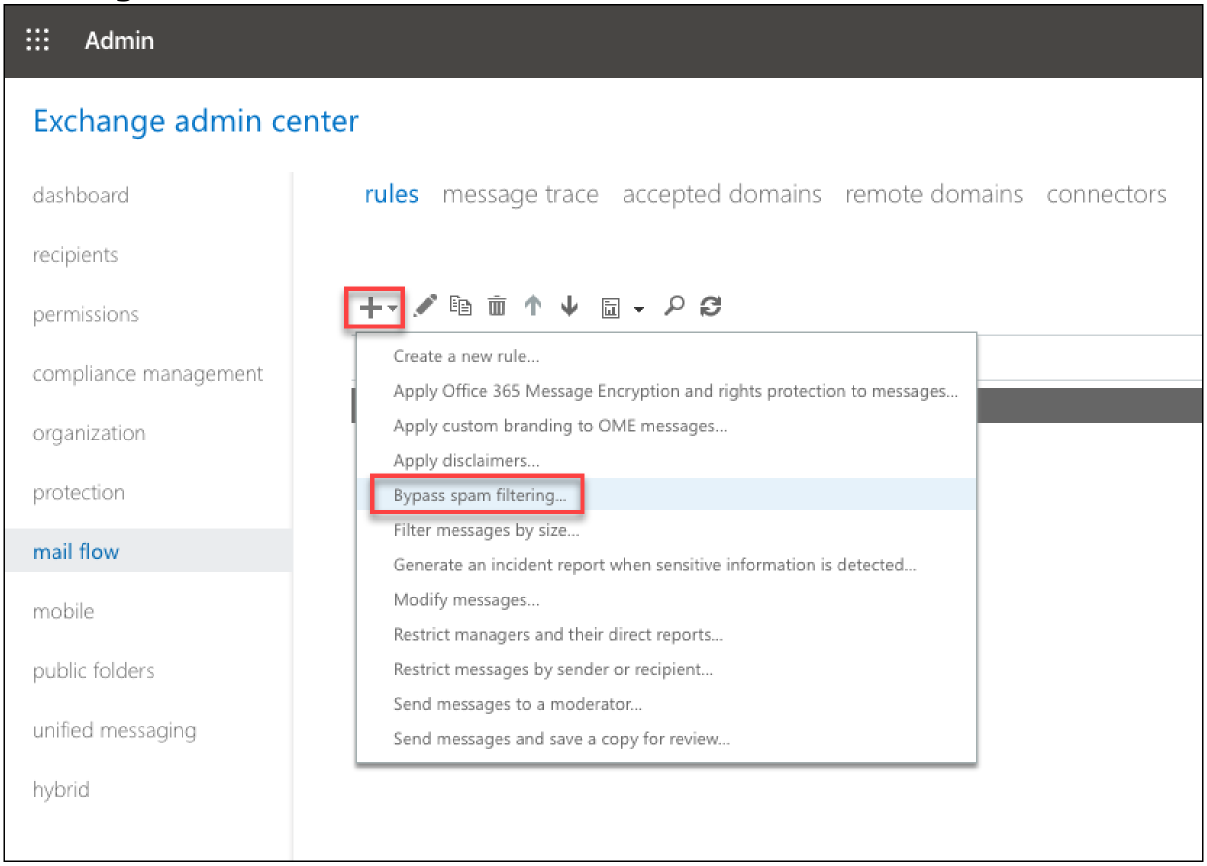
Part 3: [Microsoft 365 ONLY] Creating a rule to bypass the Junk Folder for M365 mail servers

Note: If you are using Microsoft 365, follow these steps, otherwise ignore them and move to **Part 4: Testing.**

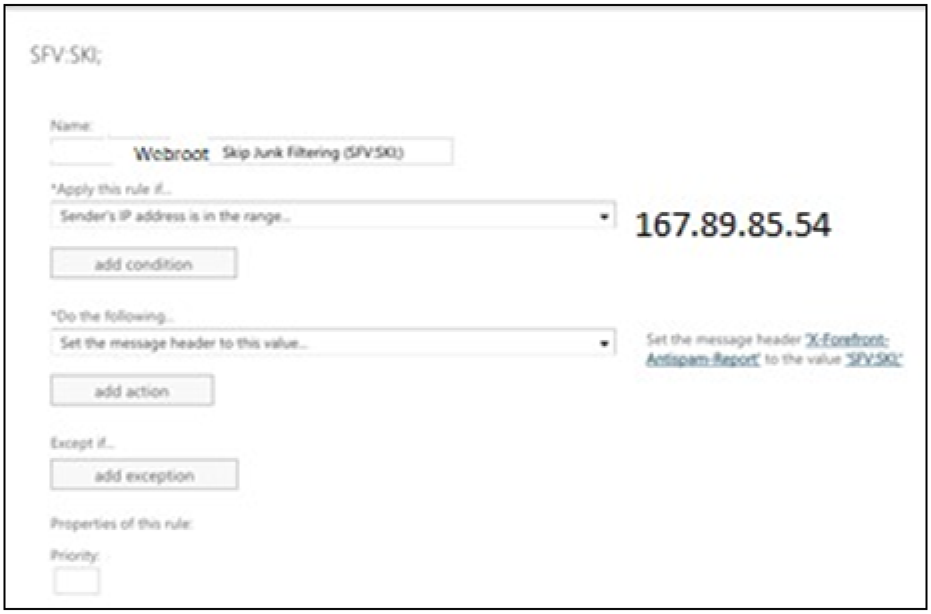
This rule will allow Webroot training and simulated phishing emails to bypass the Junk folder, ensuring that your users are getting tested on their security awareness.

1. Open the **Exchange admin center (EAC)**. See Part 1, Step 1 above for help if needed.

2. In the **EAC**, go to **mail flow > rules**, click the **Add icon (+)**), then **Bypass spam filtering...**.



3. Provide a **Name** and add conditions for the new rule.



4. The **Name** provided for this rule is **Webroot Skip Junk Filtering**, feel free to use whatever name you like.
5. Click **More options**.
6. Add the condition **Apply this rule if...**
   - Select **The Sender**, then click on **More Options** and select **IP address is in any of these ranges or exactly matches**. Enter the IP addresses for the Webroot Security Awareness Training email servers, which are specified in the [Knowledge Base](). When completed, click **OK**.
7. Beneath **Do the following**, click **Modify the message properties** then **Set a Message Header**.
   - Set the message header "**X-Forefront-Antispam-Report**" to the value "**SFV:SKI**;".
8. Beneath **Properties of this rule** set the priority to directly follow the rule created in Part 2 to bypass spam filtering, click **Save** to complete the process.
9. You have now completed the process to allow email for Microsoft Exchange/Microsoft 365.

Part 4: Testing

Webroot recommends a test campaign be executed to test that mail is flowing properly and inbound email is working as expected. Please allow 1-2 hours for settings to replicate, it may take a little longer for M365.

Allowing Emails In Google Workspace

In order to prevent or resolve problems related to mail delivery when using Webroot Security Awareness Training with Google Workspace (formerly known as Google G Suite), follow the processes outlined in the Knowledge Base.

Allowing Webroot Training Email Servers

Webroot Security Awareness Training uses email to deliver welcome messages, training invitations and phishing simulation messages. For the service to function properly, email delivery must work in a timely and dependable manner.

Occasionally, before email is allowed to be delivered, some domains will require that the sending mail server be allowed. This action places the sending mail server on a safe list and allows mail from its IP address or server name to be accepted. The steps required to create entries varies from email platform to email platform.

If you are having problems with mail getting stopped by your mail server as spam, add allow entries for the Webroot Security Awareness Training email servers, which are specified in the Knowledge Base.

Chapter 7: Working With Settings

To start working with Settings, see the following topics:

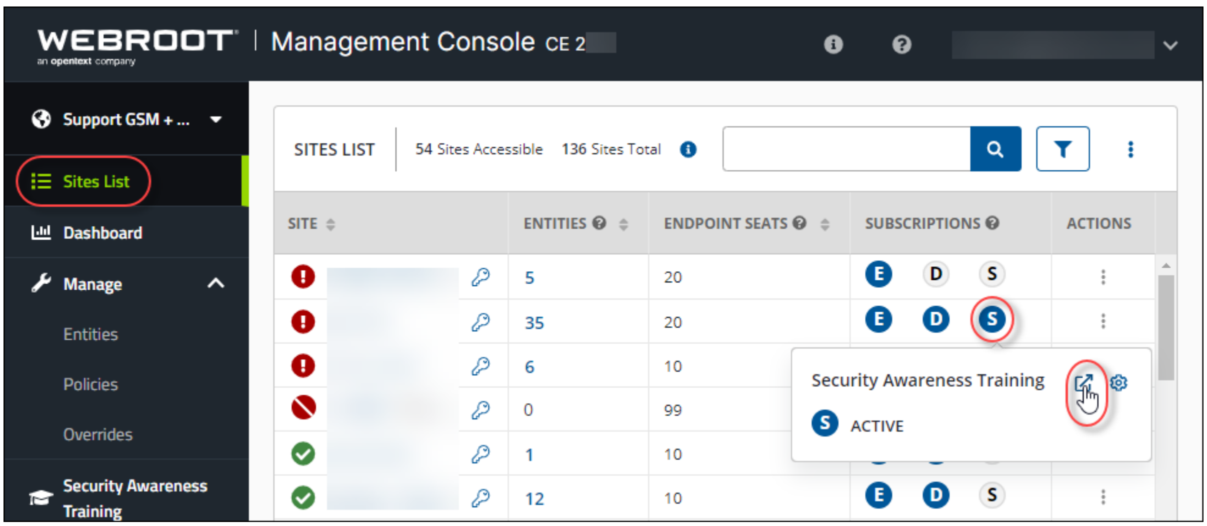
Verifying Domains 175
Importing Targets 179
Integrating with Microsoft Azure Active Directory 188
Microsoft Azure Active Directory Frequently Asked Questions 197

Verifying Domains

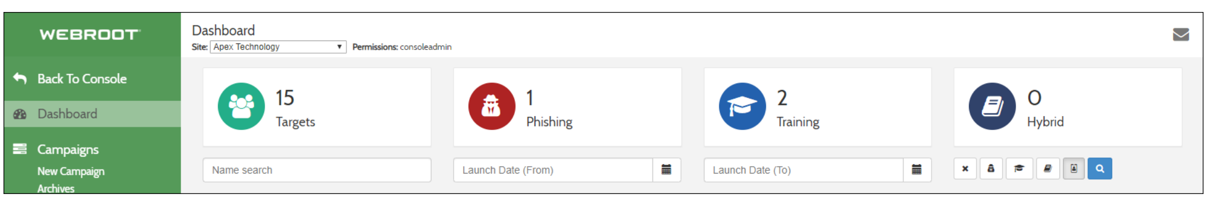
You must verify a domain before you can send phishing simulations to users in that domain.

To verify a domain:

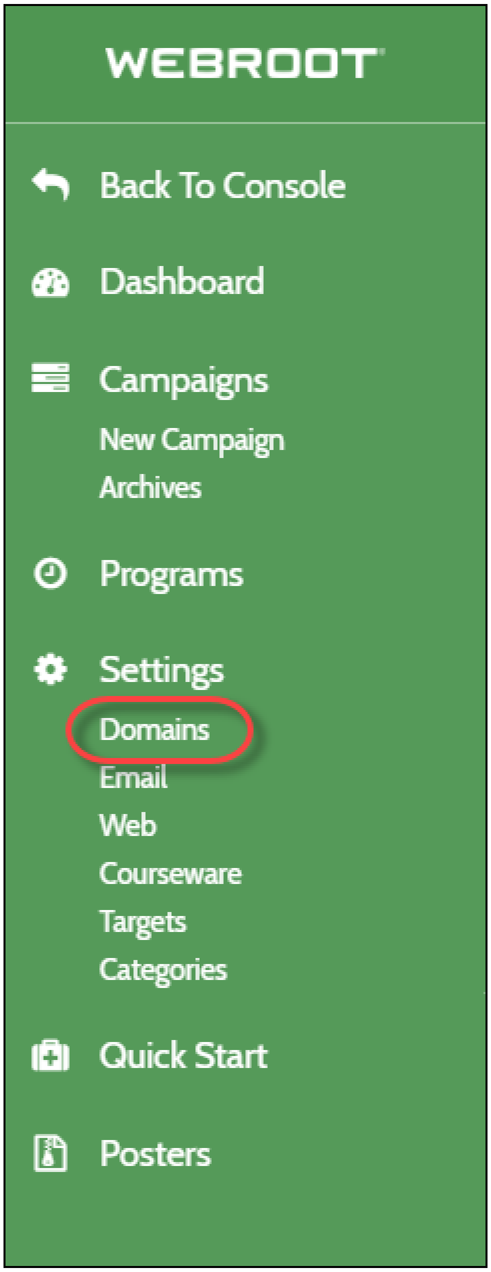
1. Log in to the Management Console.
2. Select a Site from the **Sites List** and click the **Go to the Security Awareness Training Console** icon.



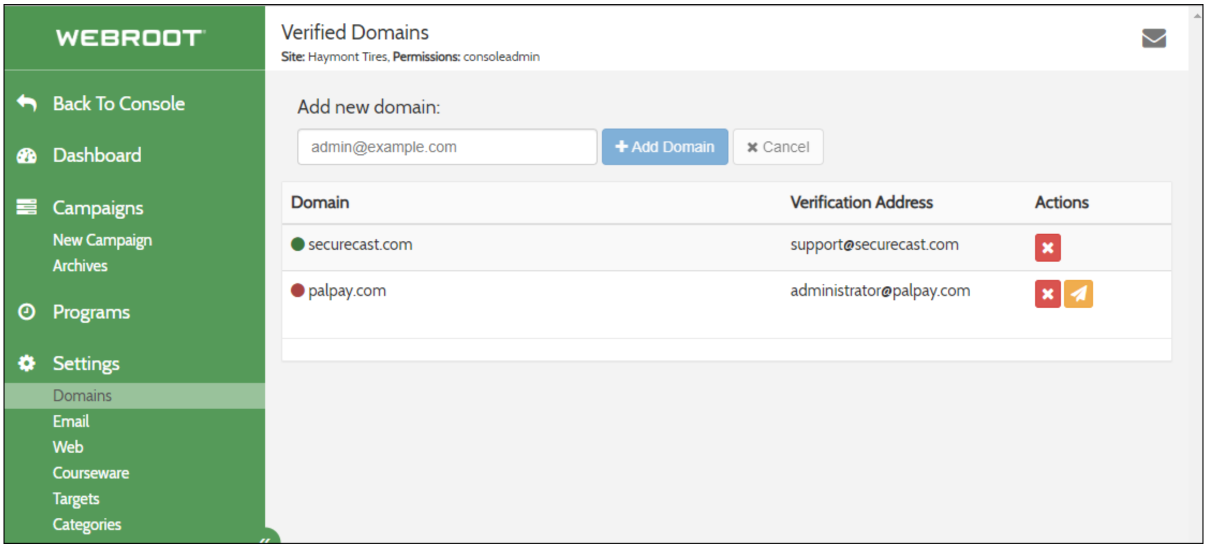
The Security Awareness Training dashboard displays.



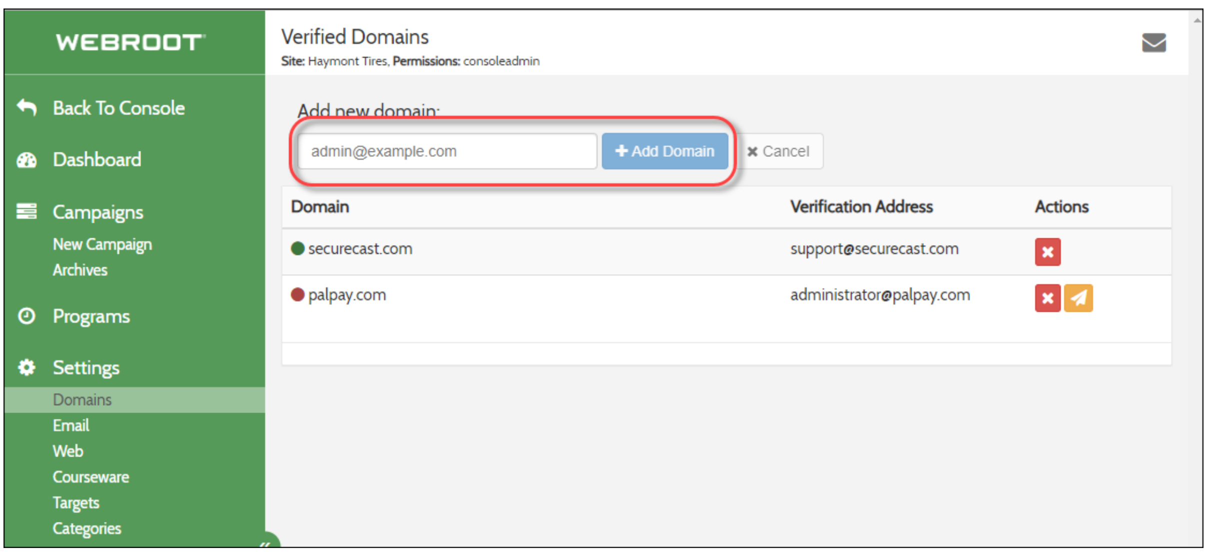
3. In the Nav bar, click **Settings > Domains**.



The Domains pane displays.

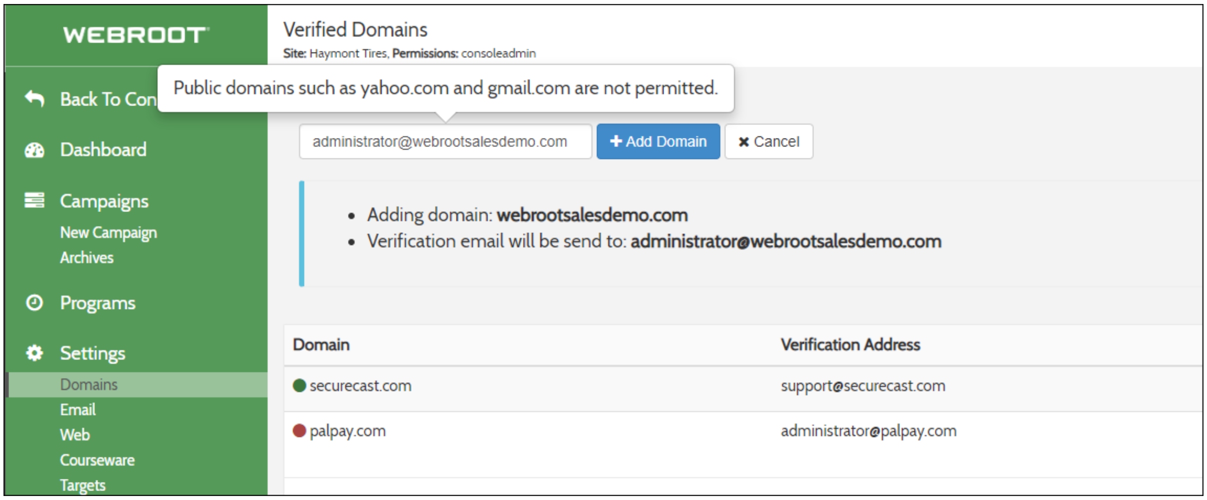


4. In the Add new domain field, enter a domain you want to verify and click the **Add Domain** button.



Note: Public domains such as yahoo.com and gmail.com are not permitted.

The system does indicates the domain that is being added and the email address where the verification will be sent.



5. When you receive the verification email, click the link and log in to the Management Console again.

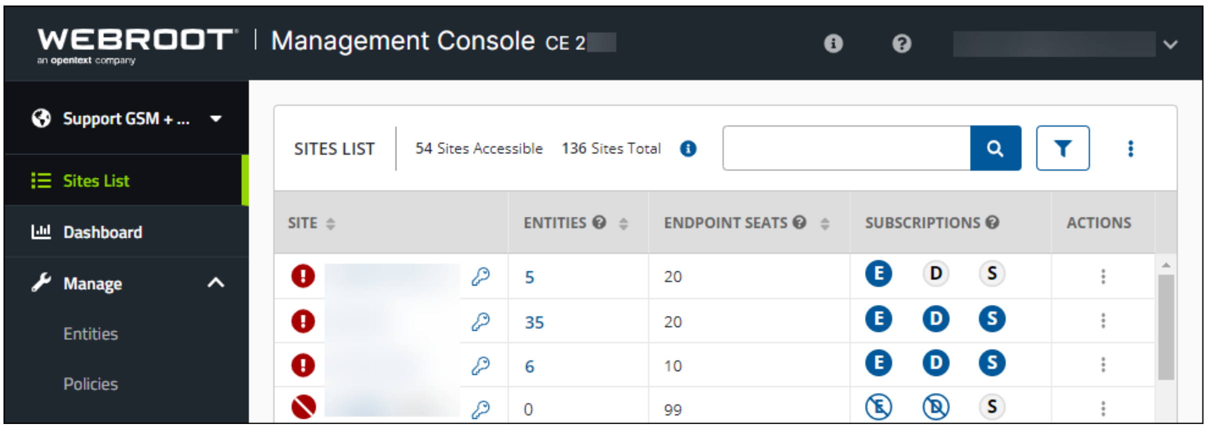
Importing Targets

Follow this procedure to import targets for your phishing or training campaigns.

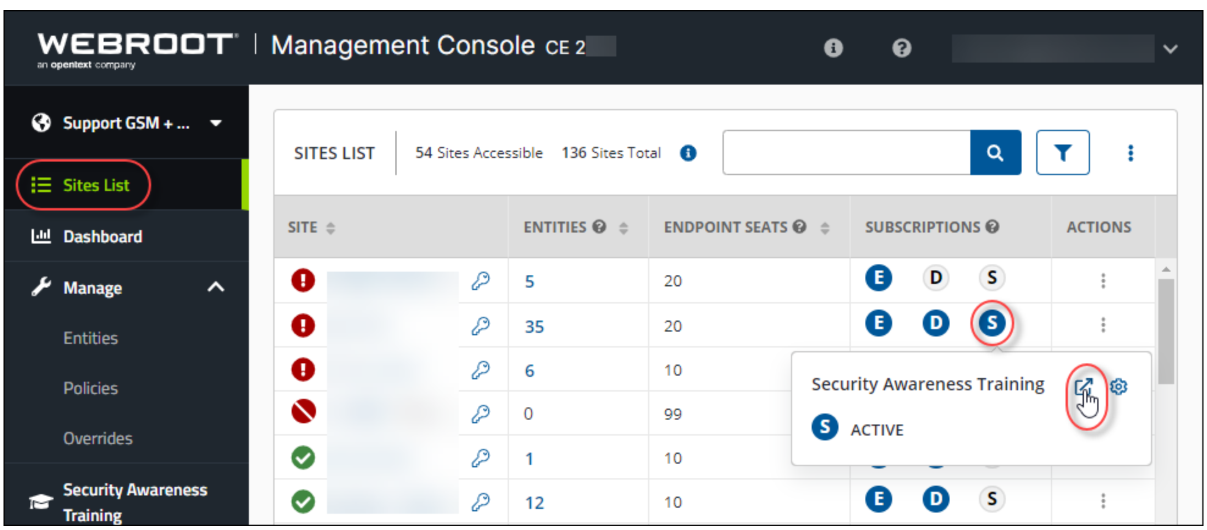
To import a target:

1. [Log in to the Management Console](#).

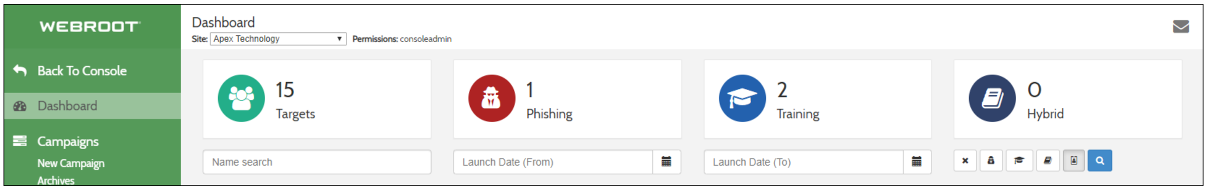
   The Sites tab displays.



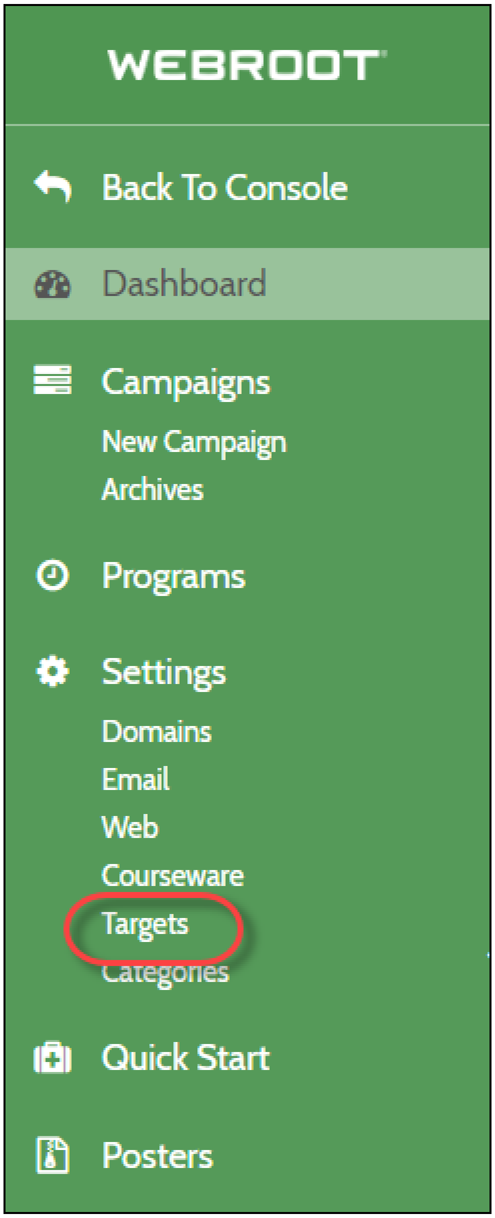
2. Select a Site from the **Sites List** and click the **Go to the Security Awareness Training Console** icon.



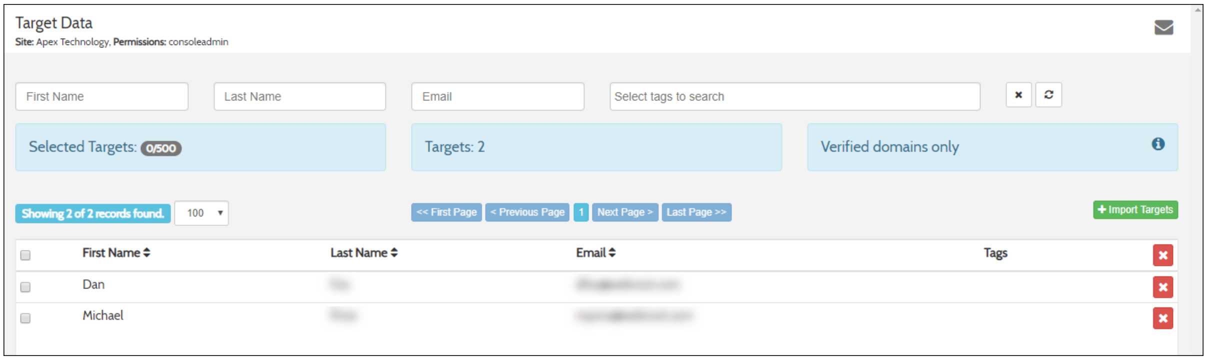
The Security Awareness Training dashboard displays.


WEBROOT
Back To Console
Dashboard
Campaigns
New Campaign
Archives
Dashboard
Site: Apex Technology
Permissions: consoleadmin
15
Targets
1
Phishing
2
Training
0
Hybrid
Name search
Launch Date (From)
Launch Date (To)

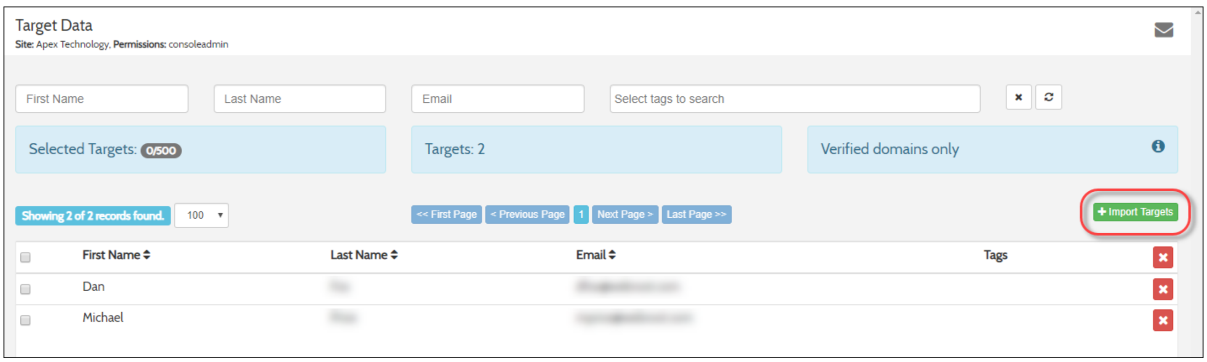
3. In the Nav bar, click **Settings > Targets**.



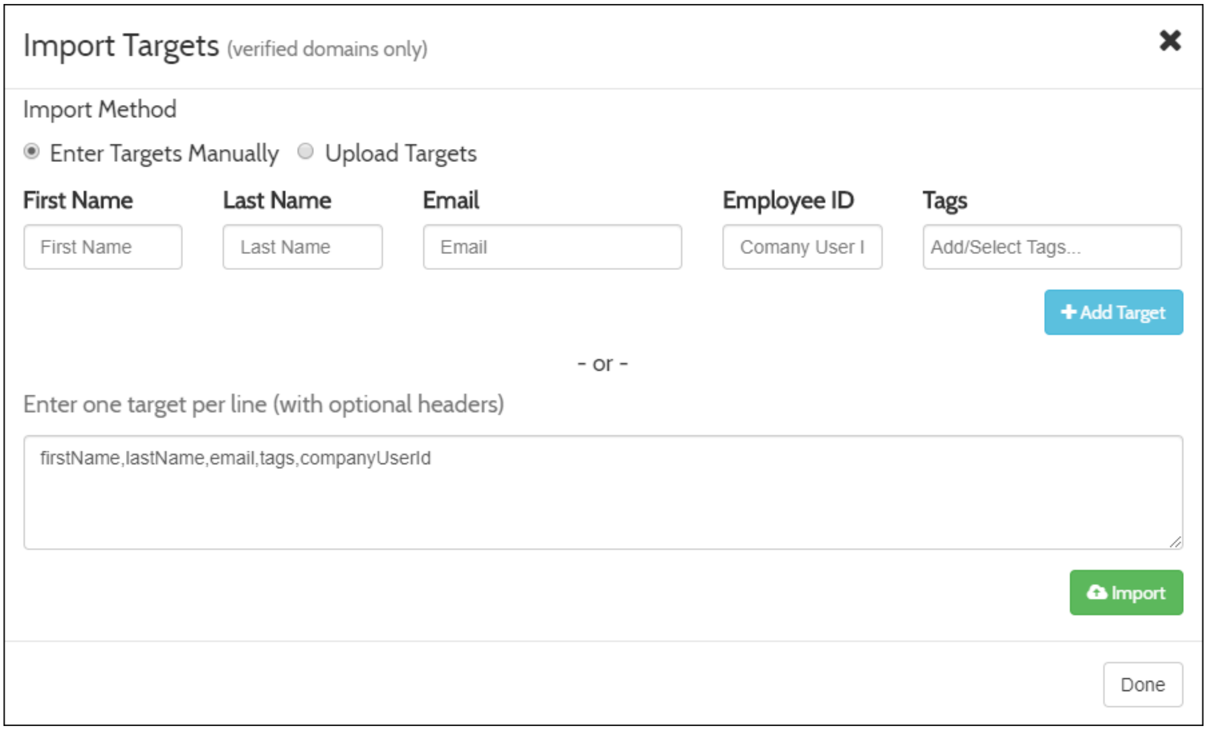
The Target Data panel displays.



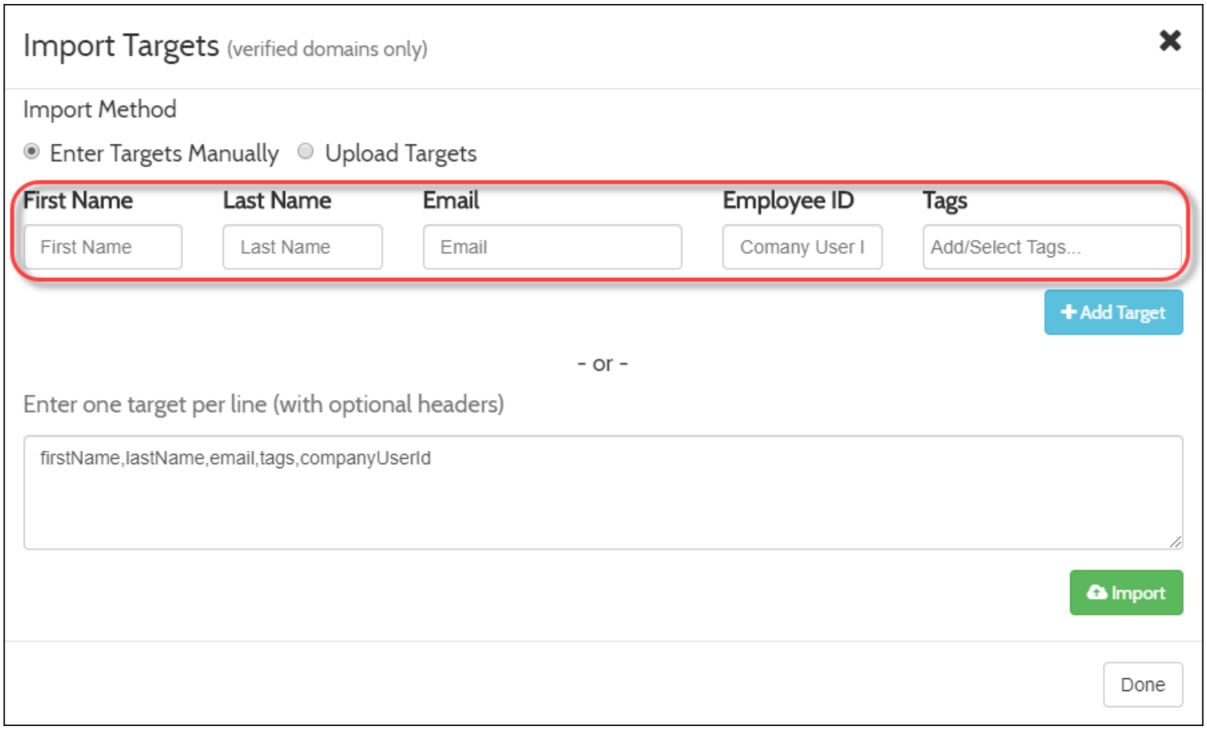
4. Click the **Import Targets** button.



The Import Targets window displays.

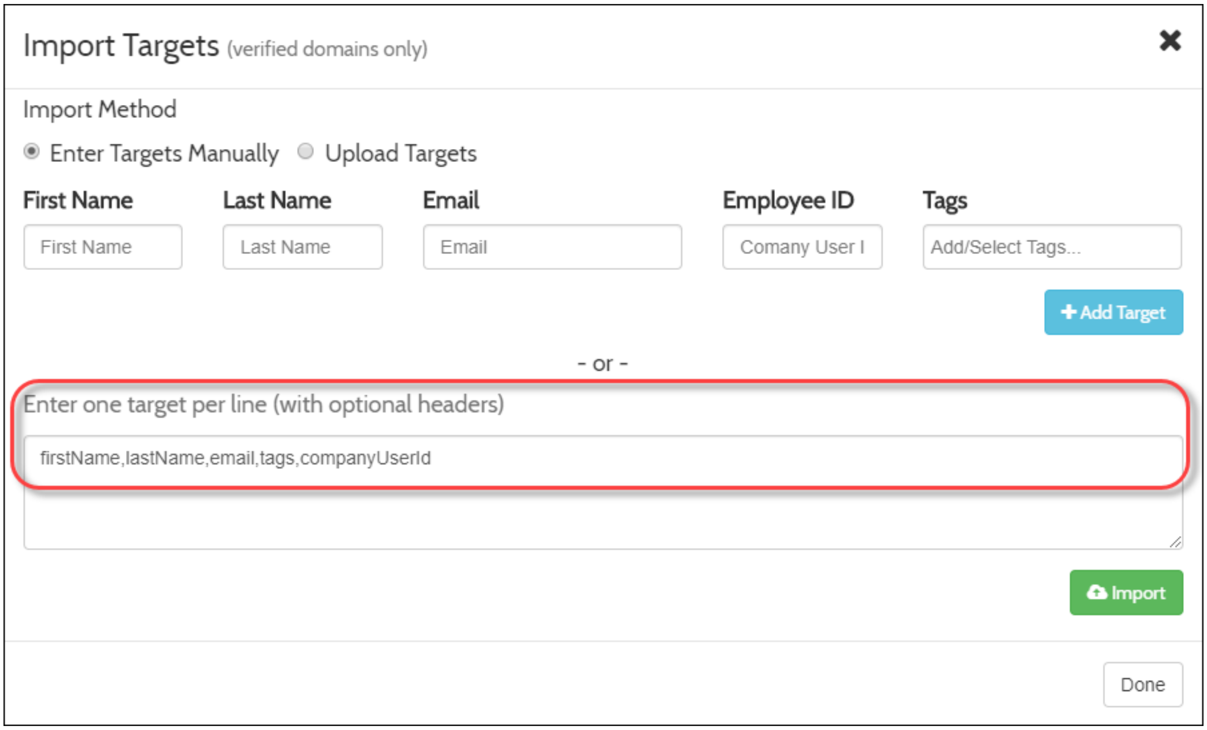


5. Do any of the following:
    - To enter targets manually, one by one, populate the fields and click the **Add Target** button.

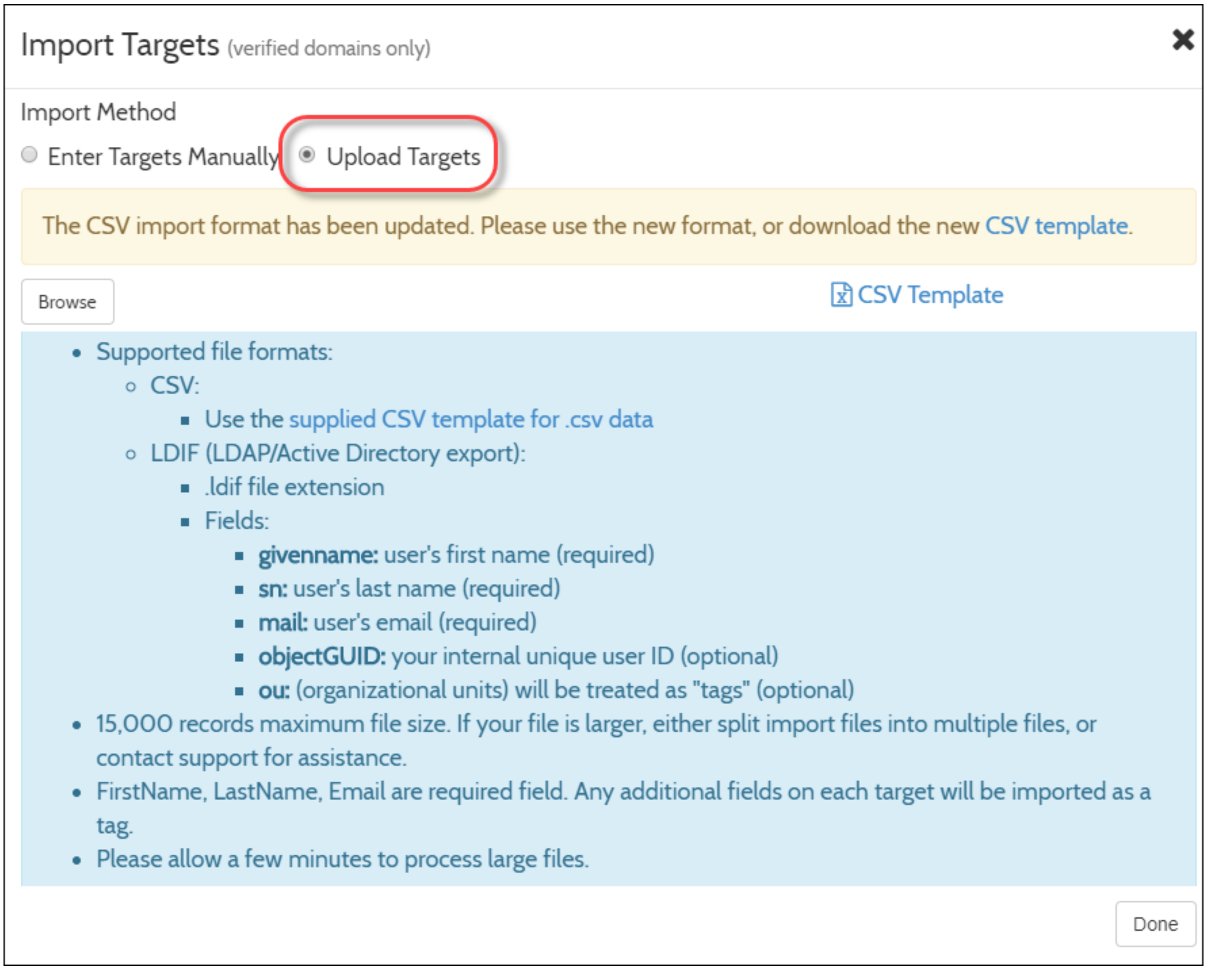


Note: You can create Tags on the fly by populating the Tags field.

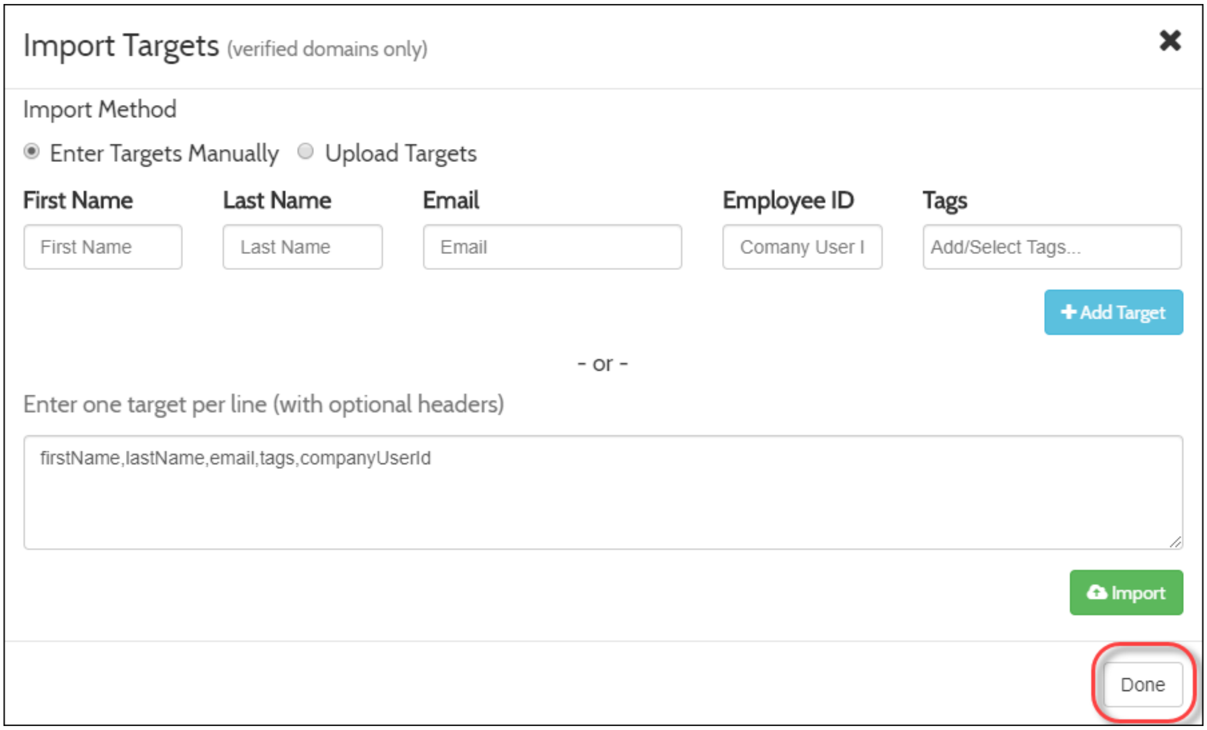
- To enter a few targets, in the Enter one target per line field, enter the target's information, and click the **Import** button.



- To upload a spreadsheet with target information, click the **Upload Targets** radio button, then browse for the CSV file that contains the information you want to upload, then click the **Done** button.


Import Targets (verified domains only)
Import Method
Enter Targets Manually
Upload Targets
The CSV import format has been updated. Please use the new format, or download the new CSV template.
Browse
CSV Template
Supported file formats:
CSV:
Use the supplied CSV template for .csv data
LDIF (LDAP/Active Directory export):
.ldif file extension
Fields:
givenname: user's first name (required)
sn: user's last name (required)
mail: user's email (required)
objectGUID: your internal unique user ID (optional)
ou: (organizational units) will be treated as "tags" (optional)
15,000 records maximum file size. If your file is larger, either split import files into multiple files, or contact support for assistance.
FirstName, LastName, Email are required field. Any additional fields on each target will be imported as a tag.
Please allow a few minutes to process large files.
Done

6. When you're done importing targets, click the **Done** button.



Integrating with Microsoft Azure Active Directory

You can integrate Webroot Security Awareness Training (WSAT) with Microsoft Azure Active Directory (Azure AD). When you integrate WSAT with Azure AD, you can:

- Control in Azure AD what users and groups should be synced with WSAT to serve as targets for campaigns.
- Enable your list of available targets in WSAT to be automatically updated as users are added, updated, or removed in Azure AD.

To get started with the integration, you will need:

- A Microsoft Azure AD subscription. If you do not have a subscription, you can get a free account.
- A Webroot management console that manages multiple sites with WSAT enabled for at least one of your sites.

There are two parts to completing the integration. Part 1 involves adding Webroot Security Awareness Training from the gallery to your list of managed SaaS apps. Part 2 involves obtaining and entering the secret token, selecting which users to sync with WSAT and confirming users were imported properly.

Part 1: Add Webroot Security Awareness Training from the gallery to the list of managed SaaS apps

1. Sign in to the **Azure portal** using either a work or school account, or a personal Microsoft account.
2. On the left navigation pane, select the **Azure Active Directory** service.
3. Navigate to **Enterprise Applications** and select **All Applications**.
4. To add a new application, select **New application**.
5. In the **Add from the gallery** section, type **Webroot Security Awareness Training** in the search box.
6. Select **Webroot Security Awareness Training** from the results panel and then add the app. Wait a few seconds while the app is added to your tenant.

Part 2: Configure Azure AD integration

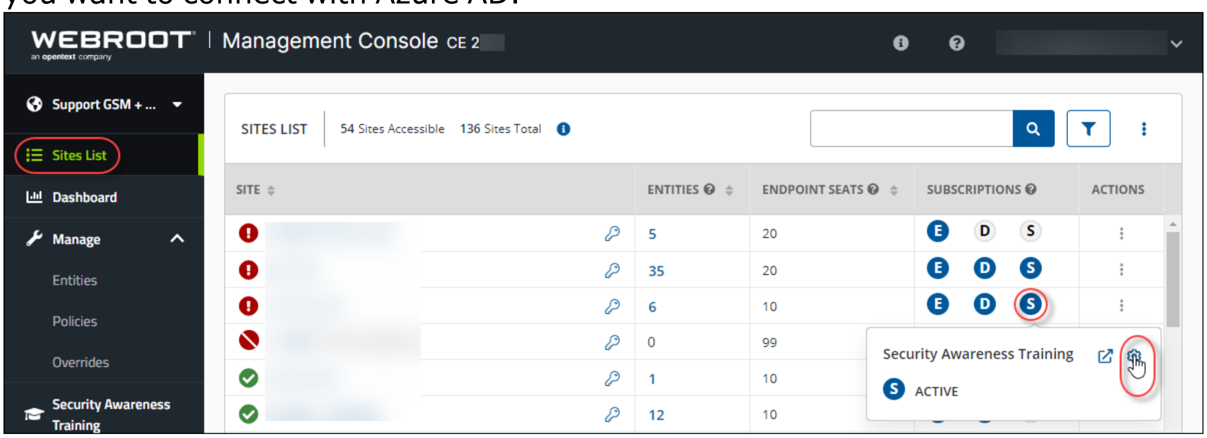
To complete the WSAT integration with Azure AD, you will perform the following steps:

1. Obtain a **Secret Token**.
2. Select users in Azure AD that you want to sync with WSAT.
3. Enter the **Secret Token** in the **Azure portal**.
4. Confirm that users were imported.

Step 1: Obtain a Secret Token

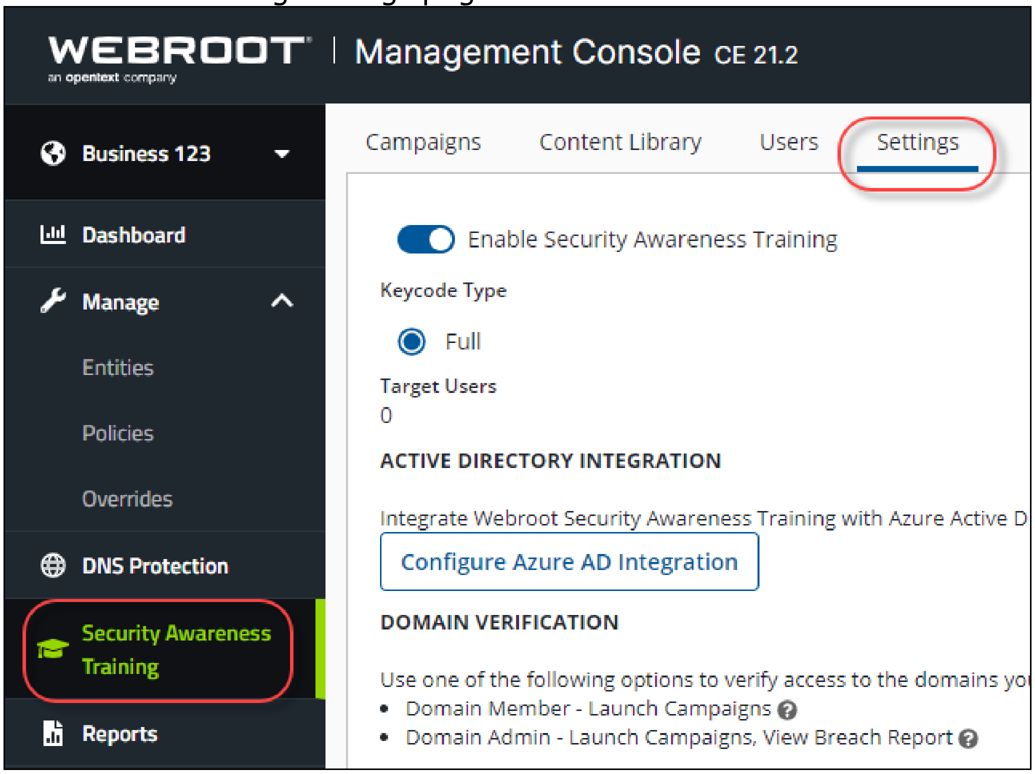
To connect your site to Azure AD, you will need to obtain a **Secret Token** for that site in the Webroot management console.

1. Sign in to your **Webroot management console**.
2. The Security Awareness Training settings page is accessed differently depending on the type of Webroot Management console you are using.
   a. For the **multi-site** Webroot Management console: From the **Sites List** tab, click the gear icon under the Security Awareness Training column for the site you want to connect with Azure AD.

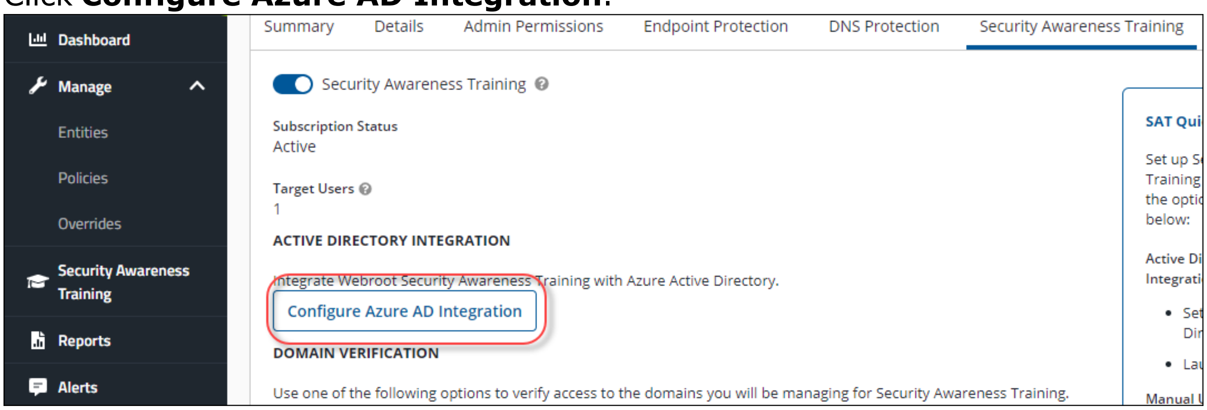


   b. For the **single site** Webroot Management console: In the left navigation bar, click **Security Awareness Training** and then **Settings** to open the Security

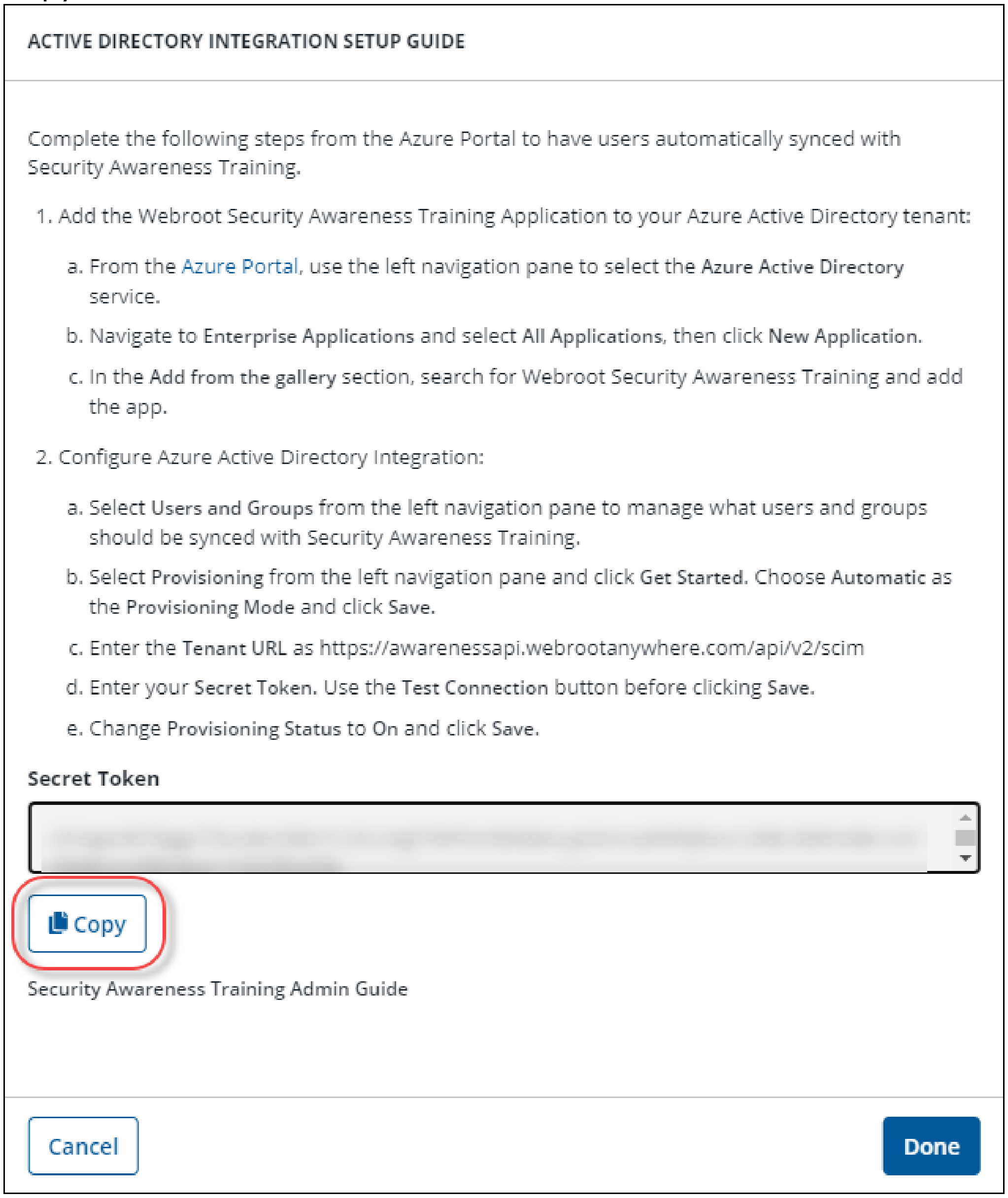
Awareness Training settings page.



3. Click **Configure Azure AD Integration**.

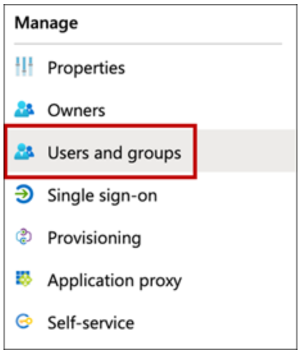


4. Copy the **Secret Token**.

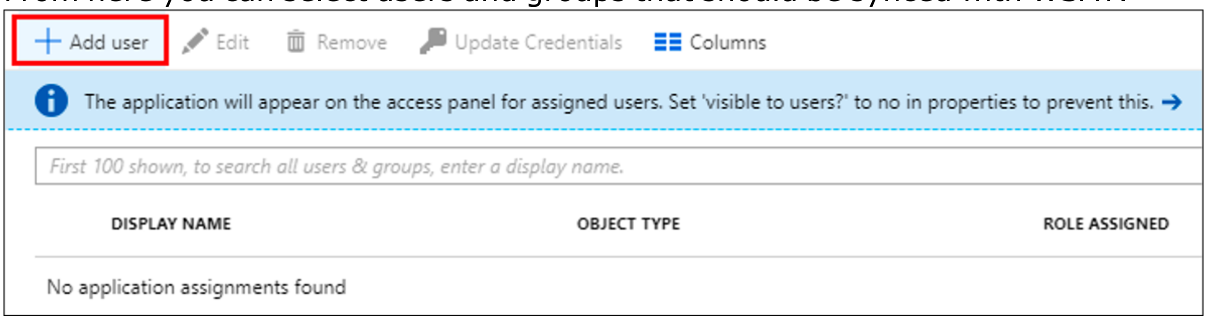


Step 2: Select users in Azure AD that you want to sync with WSAT

1. In the **Azure portal**, on the **Webroot Security Awareness Training** application integration page, click **Users and groups**.



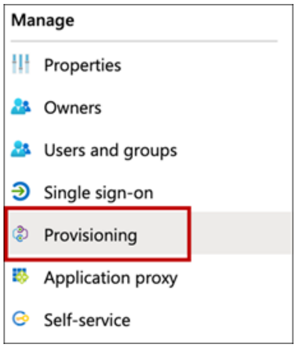
2. From here you can select users and groups that should be synced with WSAT.



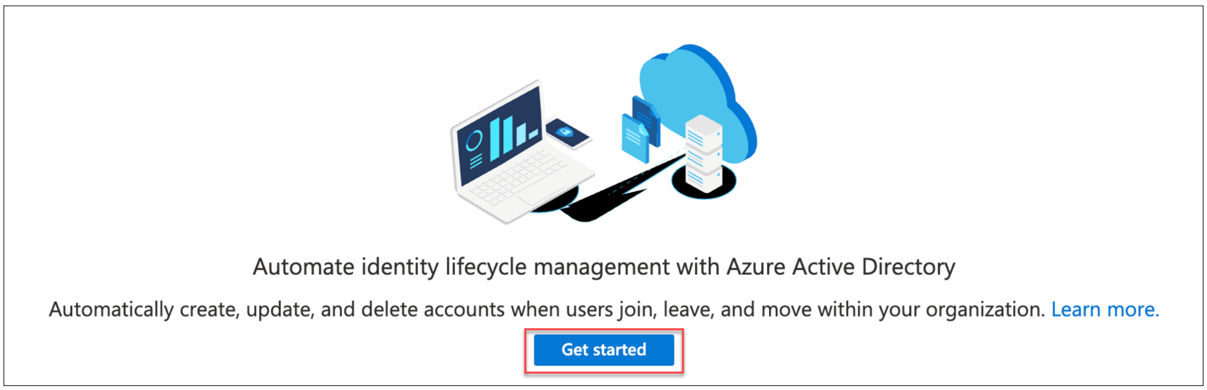
> **Note**: You can optionally skip this step and choose to **Sync all users and groups** as your **Scope** in the **Provisioning** section. Depending on your Active Directory Level, you may be able to create groups for assignment. If you have access to the groups functionality in Active Directory, we recommend syncing specific groups, or creating a group in Azure AD to capture all the users you want to target for training. This helps to prevent the accidental inclusion of guests and external collaborators, if you have them in your directory.

Step 3: Enter the Secret Token in the Azure portal

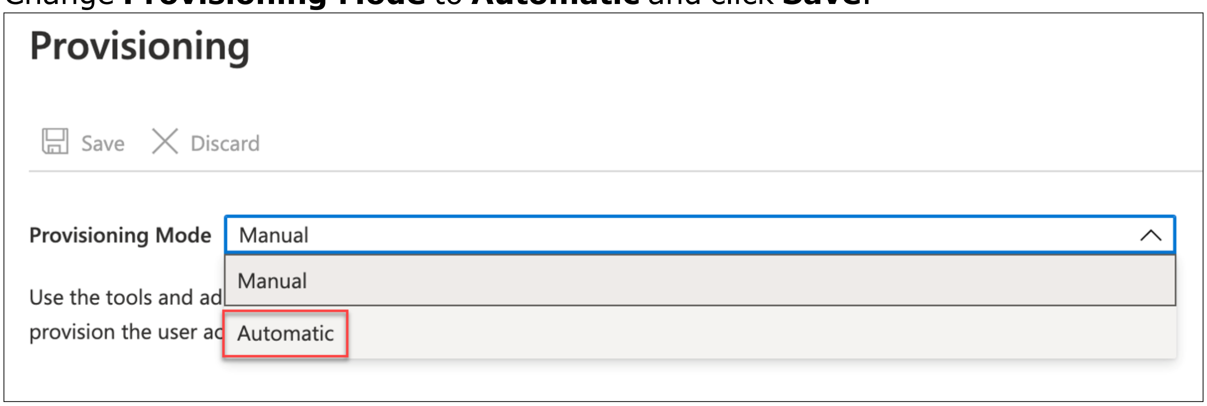
1. In the Azure portal, on the **Webroot Security Awareness Training** application integration page, click **Provisioning**.



2. Click **Get started**.

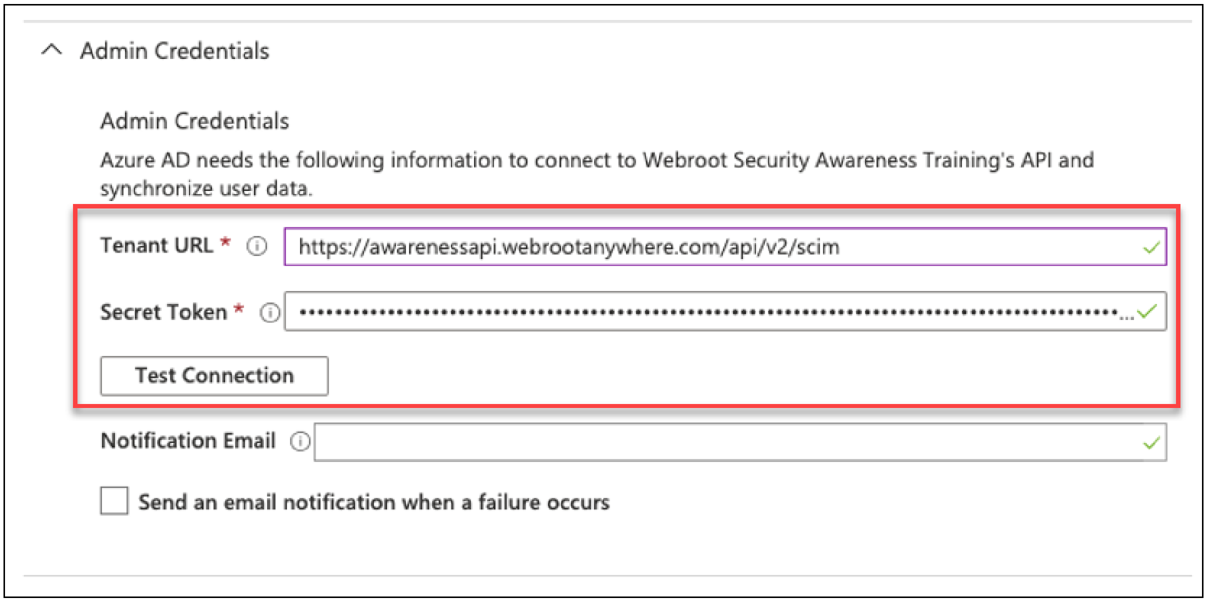


3. Change **Provisioning Mode** to **Automatic** and click **Save**.

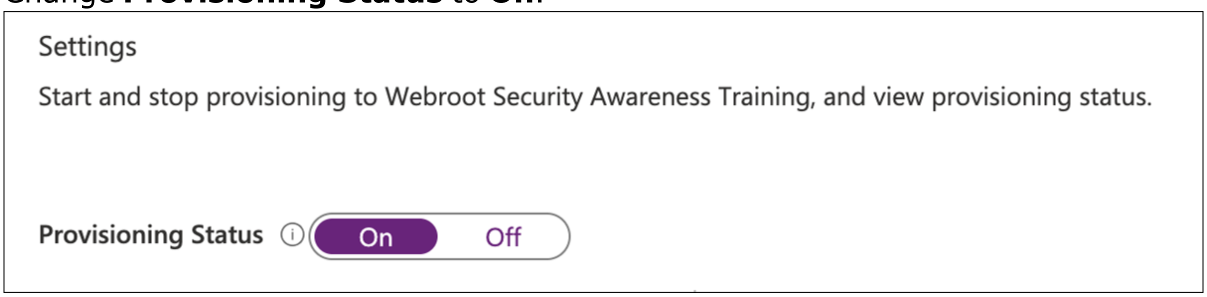


4. Paste the **Secret Token** you copied from the Webroot management console into the **Secret Token** field.
   Enter the **Tenant URL** as https://awarenessapi.webrootanywhere.com/api/v2/scim

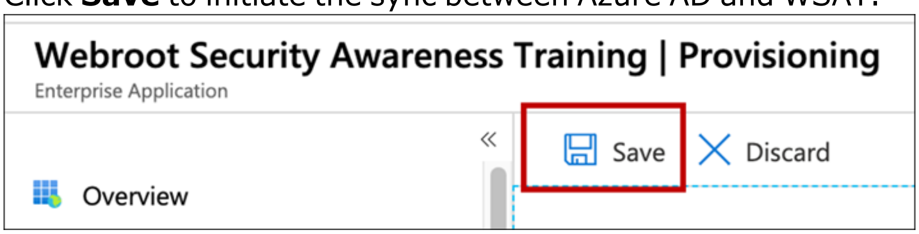
Click **Test Connection** and then click **Save**.



5. Change **Provisioning Status** to **On**.



6. Click **Save** to initiate the sync between Azure AD and WSAT.

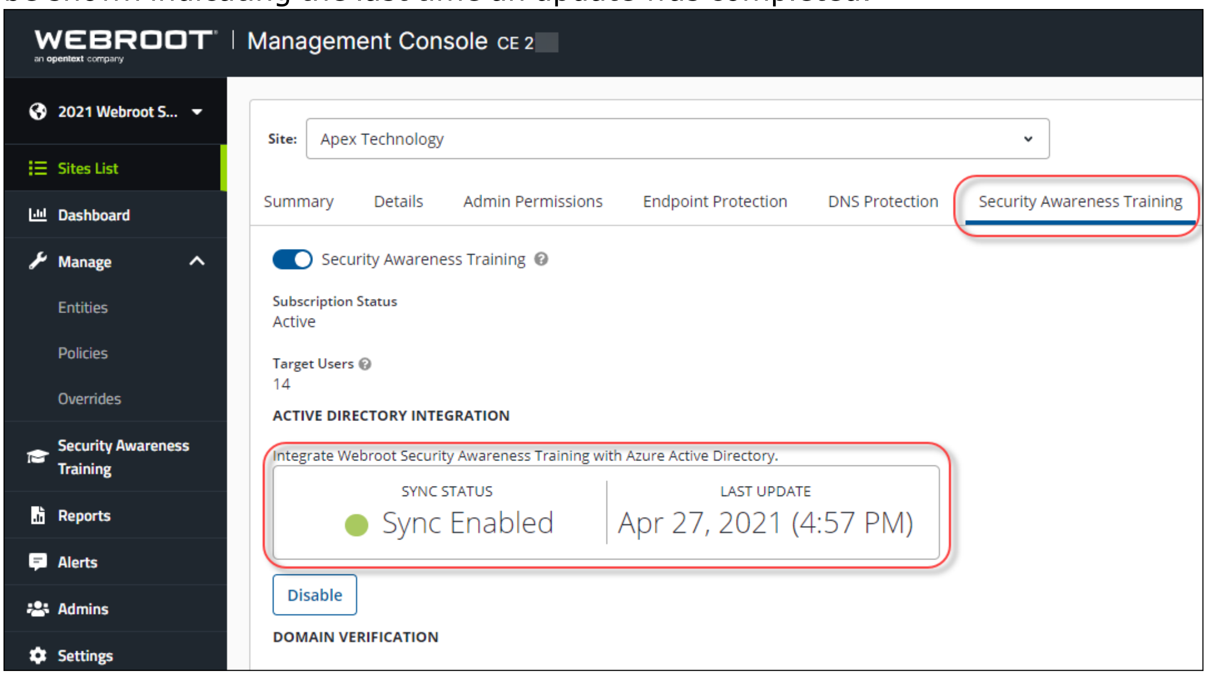


Step 4: Confirm that users were imported

Depending on the size of your directory, it could take several minutes to complete the initial sync.

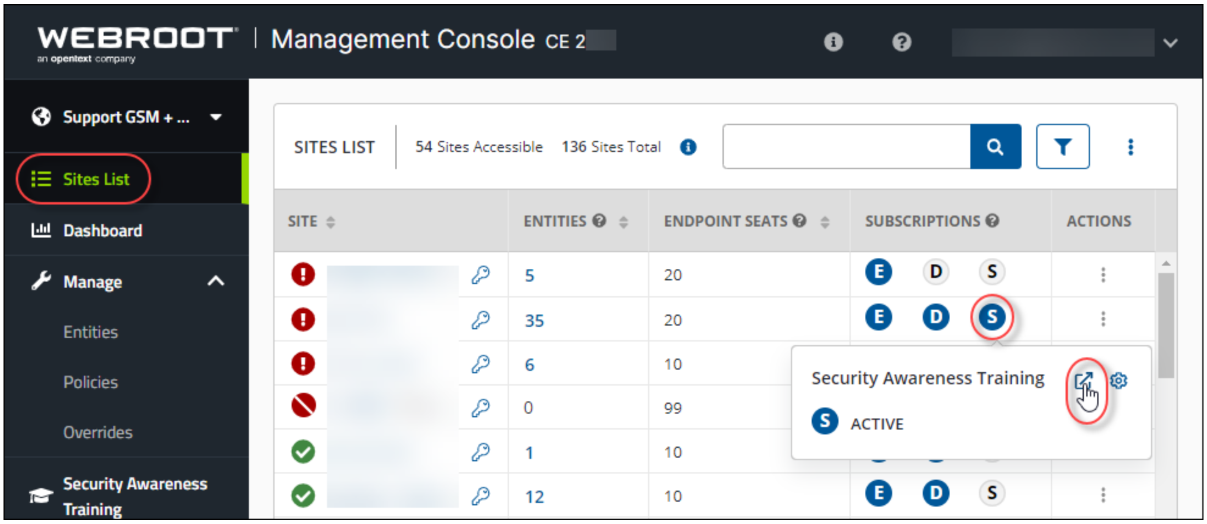
In the Webroot management console, the **Security Awareness Training** settings page for your site shows the status of the Active Directory Integration as **Sync Pending** or **Sync Enabled**.

- **Sync Pending** – Connection has yet to be established and is not ready for use.
- **Sync Enabled** – Connection is established and data has been obtained. A timestamp will be shown indicating the last time an update was completed.

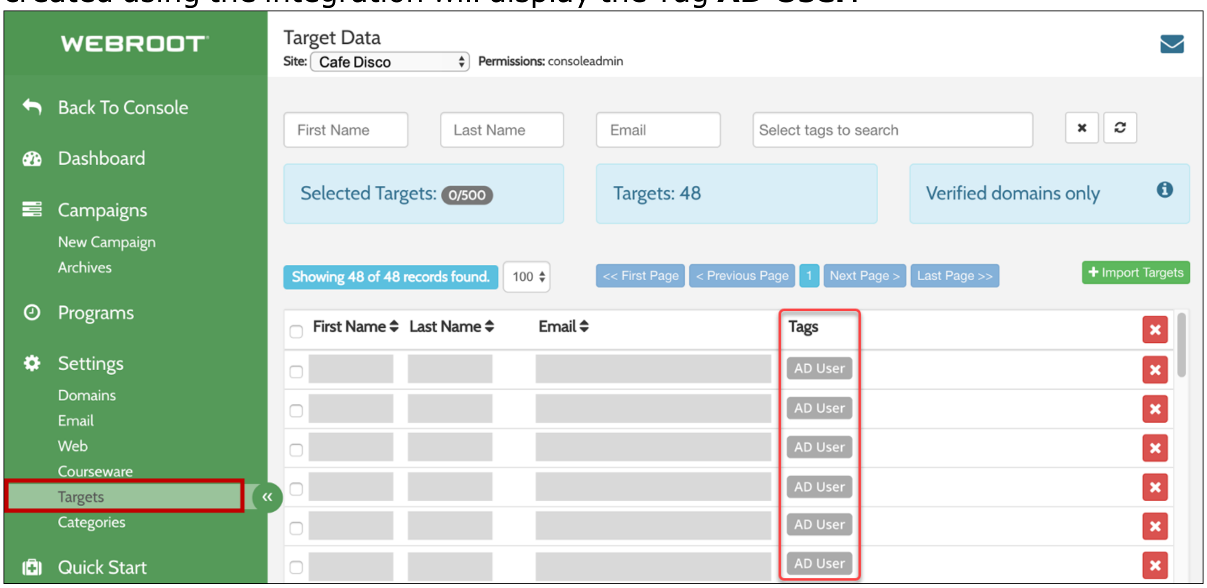


To see the users that were imported:

1. In the **Webroot management console**, click the **Go To Security Awareness Console** icon to open the Security Awareness console.



2. In the left navigation menu of the Security Awareness console, click **Targets**. Users created using the integration will display the Tag **AD User**.



After the initial sync, Azure AD will continue to make updates to target users in WSAT as often as every 40 minutes (if there have been any changes to the users and groups you selected to be synced).

Microsoft Azure Active Directory Frequently Asked Questions

You can integrate Webroot Security Awareness Training (WSAT) with Microsoft Azure Active Directory (Azure AD). When you integrate WSAT with Azure AD, you can:

- Control in Azure AD what users and groups should be synced with WSAT to serve as targets for campaigns.
- Enable your list of available targets in WSAT to be automatically updated as users are added, updated, or removed in Azure AD.

This topic includes a number of frequently asked questions and is helpful to review if you plan to use the integration.

How do I disable the Active Directory integration?
From the Security Awareness Training settings page there is a button to Disable the integration. Doing this will delete all Active Directory target users from WSAT and stop all further updates from Active Directory. Once you have disabled the integration here, please go to the Webroot Security Awareness Training application in the Azure portal and switch Provisioning Status to Off.

What happens when there is a conflict and a user that already exists is created by the Active Directory integration?
An existing target user with the same email address as a user that is imported from Active Directory will become managed by Active Directory. The target user’s campaign history will remain intact. However, you will no longer be able to manually delete the user and would have to delete it from Active Directory.

How do I switch the sync mode between 'Sync all users' and 'Sync only assigned users and groups'?
First, disable the integration (see Disabling Active Integration above), then re-enable it with the new setting in the Azure portal. Making this change without disabling and re-enabling the integration will not have any effect on the users and groups already synced.

What do I do if users are not getting synced?
Make sure all users have Office 365 email accounts associated with their profiles. Also see Switching between 'Sync all users' and 'Sync only assigned users and groups' above. If problems persist, open a ticket with Webroot Support for assistance.

Chapter 8: Security Awareness Training Technical Support

For information about support, see the following topics:

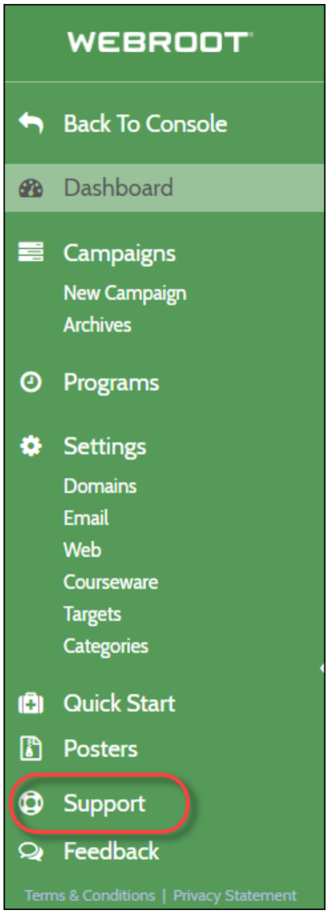
Accessing Technical Support **199**
Leaving Feedback **201**

Accessing Technical Support

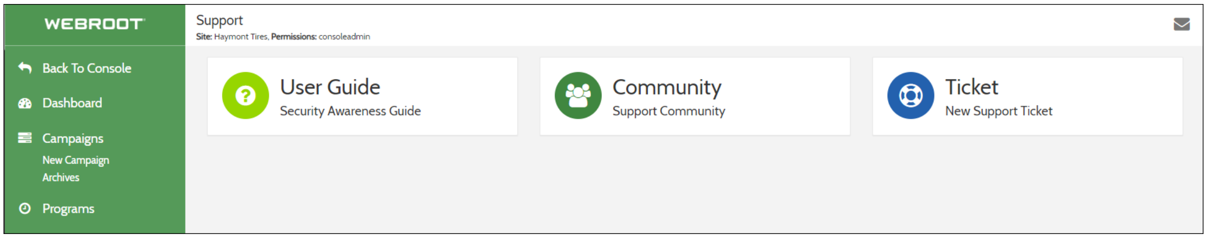
Webroot offers a variety of support options.

To access technical support:

1. In the Tab menu, click the **Support** tab.



The Support panel displays.



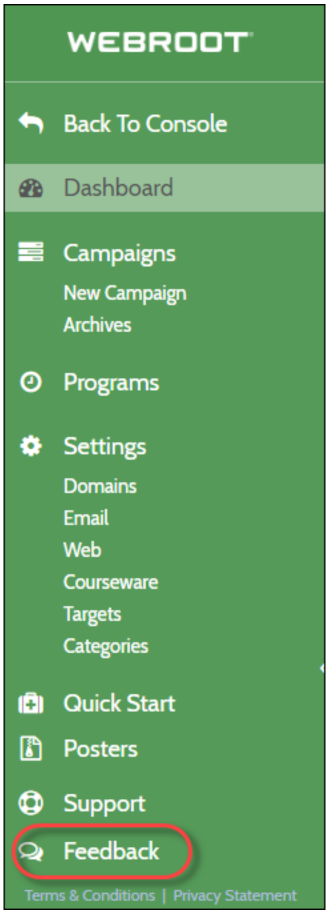
2. From there, you can do any of the following:
   - Look for the answer in our online documentation.
   - Connect to the Webroot Online Business Forum.
   - Enter a help ticket.

Leaving Feedback

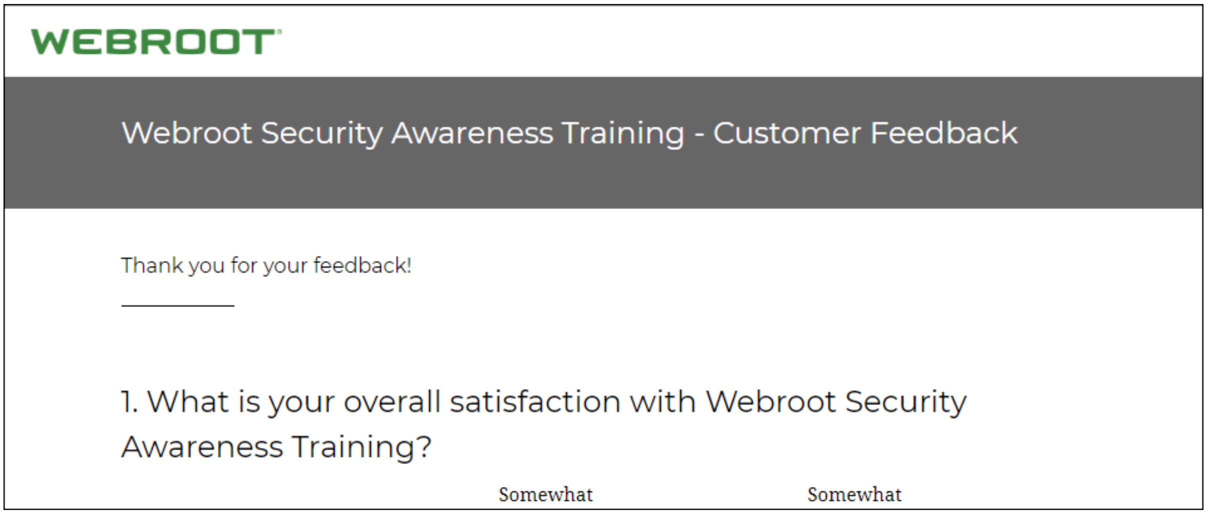
If you'd like to leave feedback, we'd love to hear from you!

To leave feedback:

1. In the Tab menu, click the **Feedback** tab.



The Webroot Security Awareness Training survey displays.



2. Respond to the questions.
3. When you’re done, click the **Done** button.

Index

A

about
    phishing simulation reports 149
accessing
    breach reports 143
    delivery reports 114
    Security Awareness Training Reports 138
    technical support 199
    training session report cards 126
allowing
    emails in google apps 172
    emails in Proofpoint Essentials 157
    Webroot email servers 173
Azure Active Directory 188, 197
Azure AD 188, 197

B

breach reports, accessing 143
broken link pages
    designing 57

C

campaign scheduling, overview 85
campaign summary reports, sending 111
creating
    infographics 43
    invitation emails 75
    phishing simulations 7-8
    templates 43
    training campaigns 105
    training modules 37
creating training sessions, overview 67

D

delivery reports
    accessing 114

designing
    broken link pages 57
    education pages 36, 78
    lure pages 53
    phishing emails 22
    phishing sites 29
domains
    verifying 175

E

education pages
    designing 36
education pages, designing 78
email types, understanding 112
enabling
    existing sites 4
    new sites 5
enabling sites 3
existing sites, enabling for 4

F

feedback, leaving 201

G

google apps, allowing emails 172

I

importing
    targets 179
infographics
    creating 43
Integrating
    AD 188, 197
    Azure Active Directory 188, 197
    Azure AD 188, 197
invitation emails
    creating 75

L

launching
    phishing simulations 7
leaving feedback 201
lure pages
    designing 53

M

microsoft 365, whitelisting emails 158

N

new sites, enabling for 5

O

office 365, whitelisting emails 158
overview
    campaign scheduling 85
    creating training sessions 67
    phishing simulations 7
    programs 85
    Security Awareness Training 2

P

phishing campaigns, scheduling 98
phishing emails
    designing 22
phishing simulation reports, about 149
phishing simulations
    creating 7-8
    launching 7
    overview 7
    sending 60
phishing sites
    designing 29
phishing siumlations
    reviewing 60
programs, overview 85
Proofpoint Essentials, allowing emails 157

R

reporting, understanding 134
reviewing
    phishing simulations 60

S

scheduling phishing campaigns 98
Security Awareness Training reports, accessing 138
Security Awareness Training, overview 2
selecting
    trainees 68
sending
    campaign summary reports 111
    phishing simulations 60
    welcome emails 86
sites
    selecting in dashboard 64
sites, enabling 3

T

targets
    importing 179
technical support, accessing 199
templates
    creating 43
trainees
    selecting 68
training campaigns, creating 105
training modules
    creating 37
training session report cards, accessing 126

U

understanding
    email types 112
    reporting 134

V

verifying
    domains 175

W

Webroot email servers, allowing 173
welcome emails, sending 86
whitelisting 157, 172-173
    emails in microsoft 365 158
    emails in office 365 158