



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>.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Open Text.

© 2004-2024 Open Text. All rights reserved.

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.

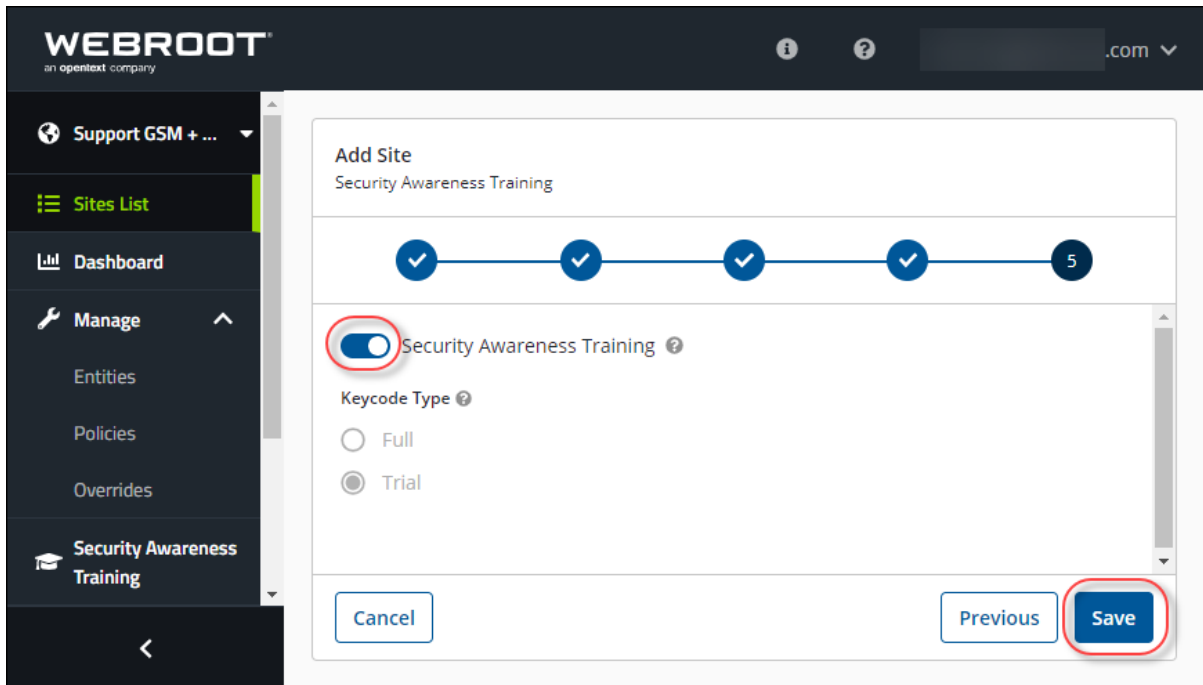
4. Click **Save Changes**.
-

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](#)
-

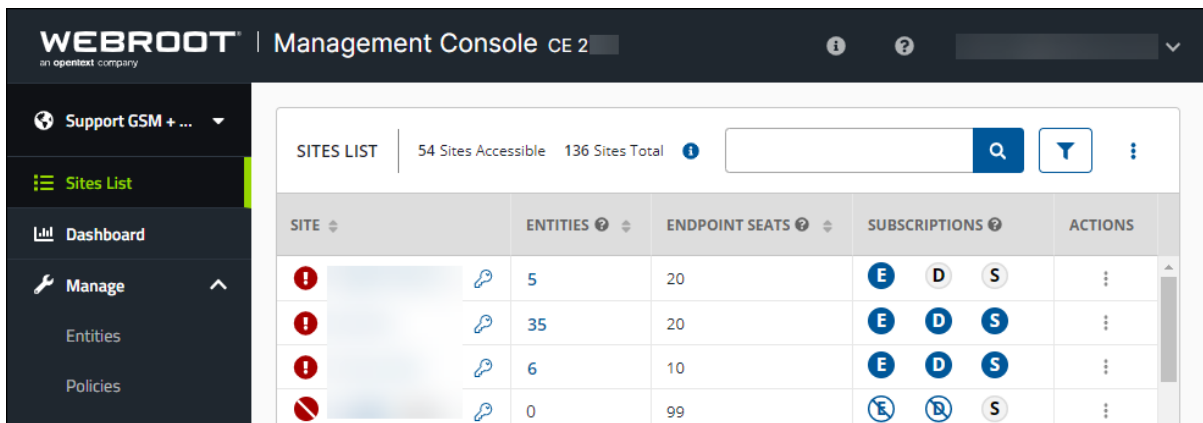
Creating Phishing Simulations

Follow this procedure to create a phishing simulation.

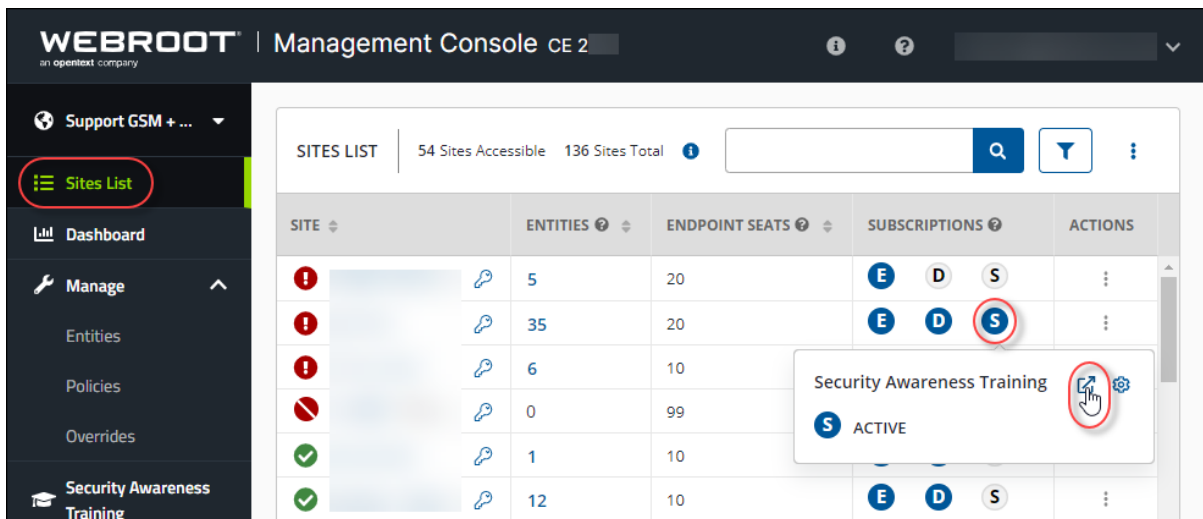
To create a phishing simulation:

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

The Management Console displays.

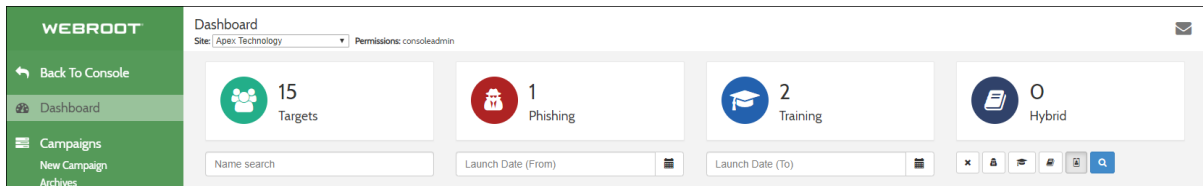


2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.

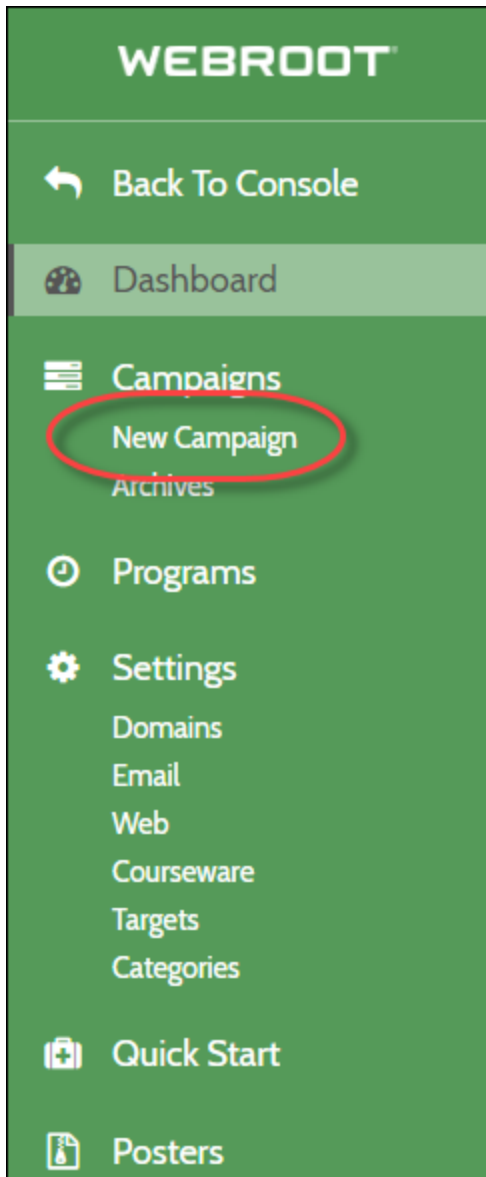


The Security Awareness Training console displays.

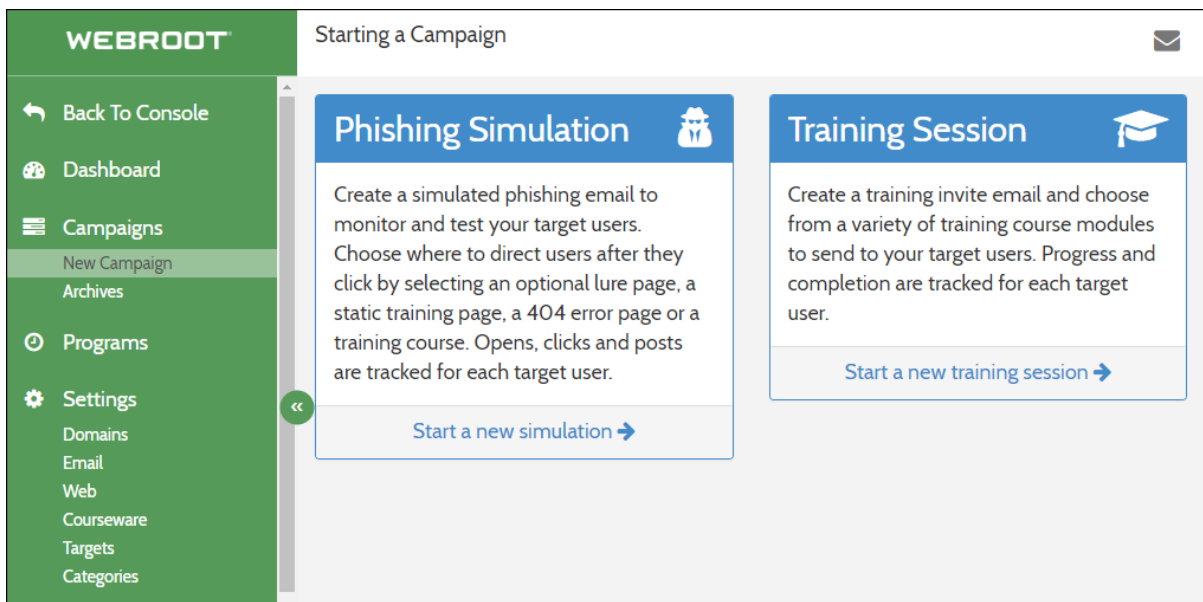
Chapter 2: Creating and Launching Phishing Simulations



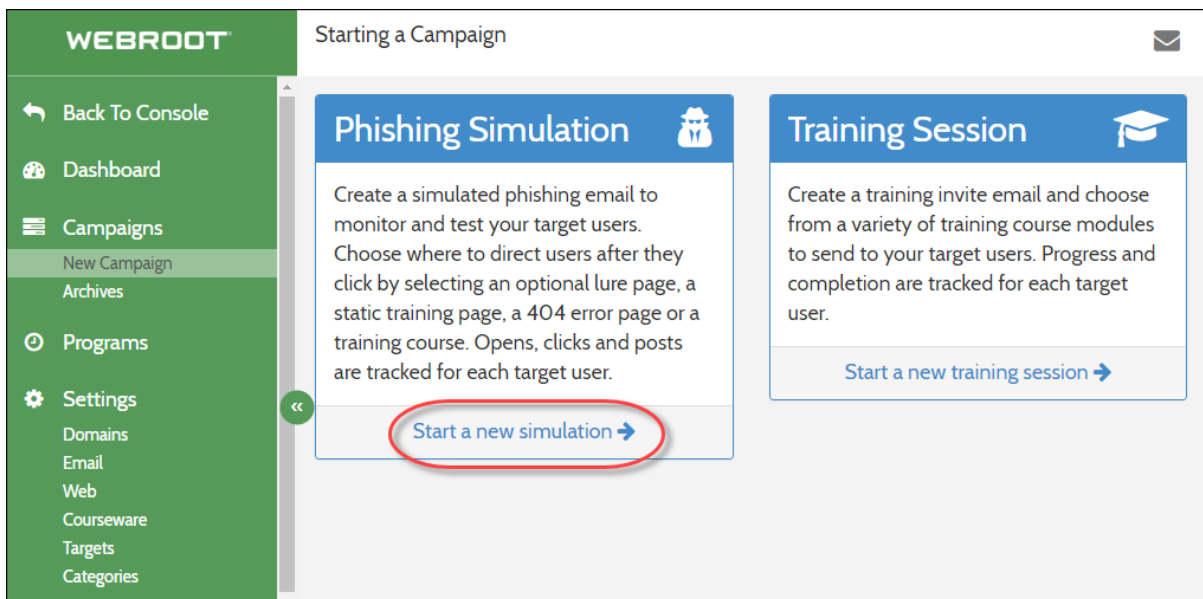
3. In the Nav bar, click the **New Campaign** icon.



The Starting a Campaign panel displays.



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



The New Campaign Wizard panel displays.

Chapter 2: Creating and Launching Phishing Simulations

WEBROOT

Back To Console

Dashboard

Campaigns

New Campaign

Archives

Programs

Settings

Domains

Email

Web

Courseware

Targets

Categories

Quick Start

Posters

Support

Feedback

New Campaign Wizard

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

- 11 -

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.

The screenshot displays the 'New Campaign Wizard' interface in the Webroot console. The left sidebar contains navigation links: Back To Console, Dashboard, Campaigns (with sub-links for New Campaign and Archives), Programs, Settings (with sub-links for Domains, Email, Web, Courseware, Targets, and Categories), Quick Start, Posters, Support, and Feedback. The main content area is titled 'New Campaign Wizard' and includes a 'Previous' button. Below this, the 'Simulation Basics' section is active, featuring a disclaimer about the use of sample phishing emails. Two input fields are highlighted with a red rounded rectangle: 'Simulation Name' with the example 'New Hire Test' and 'Description' with the example 'April: Testir'. Below these fields is a 'Show Advanced Options' checkbox and a 'Save Simulation' button.

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

Chapter 2: Creating and Launching Phishing Simulations

The screenshot shows the 'New Campaign Wizard' interface in the Webroot console. On the left is a green sidebar with navigation links: 'Back To Console', 'Dashboard', 'Campaigns' (with sub-links 'New Campaign' and 'Archives'), 'Programs', 'Settings' (with sub-links 'Domains', 'Email', 'Web', 'Courseware', 'Targets', and 'Categories'), 'Quick Start', 'Posters', 'Support', and 'Feedback'. The main content area is titled 'New Campaign Wizard' and has a 'Previous' button. Below this is a 'Simulation Basics' section. A light blue box contains a disclaimer: '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.' Below the disclaimer are two text input fields: 'Simulation Name' with a hint 'Simulation name. Example: New Hire Test' and 'Description' with a hint 'Describe your campaign. Example: April: Testir'. A checkbox labeled 'Show Advanced Options' is circled in red. At the bottom is a blue 'Save Simulation' button with a save icon.

WEBROOT New Campaign Wizard

Back To Console 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

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 click
 - 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: +

Options:

- ☐ Anonymize target email addresses after sending

Save Simulation 

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

Simulation Wizard: Unlaunched

Site: Haymont Tires, Permissions: consoleadmin

20% Complete

< Previous

Save/Next >

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 ⓘ

New Hire Test

Description ⓘ

Testing New Hires

Chapter 2: Creating and Launching Phishing Simulations

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

The screenshot shows the 'Simulation Wizard: Unlaunched' interface. At the top, it indicates 'Site: Haymont Tires, Permissions: consoleadmin' and a progress bar at '20% Complete'. A 'Previous' button is on the left, and a 'Save/Next' button is on the right, highlighted with a red rectangle. The main section is titled 'Simulation Basics' and contains a disclaimer about the simulation email. Below this, there are two input fields: 'Simulation Name' with the value 'New Hire Test' and 'Description' with the value 'Testing New Hires'.

The Targets pane displays, with the Target tab active.

The screenshot shows the 'Simulation Wizard: Unlaunched' interface with the 'Targets' tab active. The progress bar is now at '80% Complete'. The 'Previous' button is on the left, and the 'Save/Next' button is on the right. The main section is titled 'Targets' and contains a search bar with 'Available Targets' and a 'Targets' tab. Below the search bar, there are filters for 'Selected Targets: 0/500', 'Targets: 9', and 'Verified domains only'. A table displays the results, showing 9 records found. The table has columns for 'First Name', 'Last Name', 'Email', and 'Tags'. The first four rows are visible, showing names like Roland, Dan, Clifford, and Cecelia.

First Name	Last Name	Email	Tags
Roland			
Dan			
Clifford			
Cecelia			

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.

<input type="checkbox"/>	First Name ↕	Last Name ↕	Email ↕
<input checked="" type="checkbox"/>	Roland	Roller	roland.roller@webrootsalesdemo.com
<input checked="" type="checkbox"/>	Dan	Roller	dan.roller@webrootsalesdemo.com
<input checked="" type="checkbox"/>	Clifford	Roller	clifford.roller@webrootsalesdemo.com
<input type="checkbox"/>	Cecelia	Roller	cecilia.roller@webrootsalesdemo.com
<input type="checkbox"/>	Leroy	Roller	leroy.roller@webrootsalesdemo.com

- 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.

The screenshot shows the 'Tags' tab in the 'Targets' section. A red box highlights the 'Select tags to search' dropdown menu, which has 'Floor' selected. Below the dropdown, a blue bar indicates 'Targets: 10' and 'Verified domains only'. At the bottom, a table shows the email 'administrator@webrootsalesdemo.com' with the tag 'Floor' selected in the 'Tags' column.

Save/Next >

Targets Tags

Email

Select tags to search

Floor

Targets: 10

Verified domains only

<< First Page < Previous Page 1 Next Page > Last Page >>

+ Import Targets

Email

Tags

administrator@webrootsalesdemo.com

Floor

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.

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

40% Complete

< Previous

Save/Next >

Targets

Available Targets

Targets Tags

First Name Last Name Email Select tags to search x ↺

Selected Targets: 3/500

Targets: 9

Verified domains only

Showing 9 of 9 records found. 100

<< First Page < Previous Page 1 Next Page > Last Page >>

+ Import Targets

	First Name	Last Name	Email	Tags
<input checked="" type="checkbox"/>	Roland			

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 screenshot shows the 'Simulation Wizard: Unlaunched' interface. At the top, it indicates the site is 'Haymont Tires' with 'Permissions: consoleadmin'. A progress bar shows '60% Complete'. Below the progress bar are 'Previous' and 'Save/Next' buttons. The main section is titled 'Design Phishing Email'. Underneath, there's an 'Email Template' section with a search bar. A dropdown menu is open, showing a list of templates. The first template, 'ADP Account Locked', is highlighted. The list includes the following details for each template:

- Name: ADP Account Locked
Categories: Login
- Name: ADP Password Reset
Categories: Login Password
- Name: Active Directory Password Reset
Categories: Login Password
- Name: Adobe Password Reset
Categories: Password Adobe


The template you have selected displays.

Simulation Wizard: Unlaunched

Site: Haymont Tires, Permissions: consoleadmin

60% Complete

< Previous

 Design Phishing Email

Email Template

Adobe Password Reset

Customize this template

Use empty template

From: "Adobe Systems" <adobe@admin-alerts.com>
Subject: Your Adobe Account Has Been Compromised

Dear {FIRSTNAME} {LASTNAME}

Your Adobe account has been compromised. To reset your password, click this link.
https://adobe.adobe-services.adobe.com/resetpw_USY63CH87AGS7D3CF8U8A63KA

Please note:
For security purposes, this link will expire 72 hours from the time it was sent.
If you cannot access this link, copy and paste the entire URL into your browser.

The Adobe Team
Copyright 2018 Adobe Systems Incorporated. All rights reserved.
Adobe Systems Incorporated. All rights reserved. 340 Park Avenue, San Jose, CA 95110 USA

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.

Simulation Wizard: Unlaunched

Site: Haymont Tires, Permissions: consoleadmin

60% Complete

< Previous

✉ Design Phishing Email

Email Template

Adobe Password Reset

Customize this template

Use empty template

From: "Adobe Systems" <adobe@admin-alerts.com>
Subject: Your Adobe Account Has Been Compromised

Dear {FIRSTNAME} {LASTNAME}

Your Adobe account has been compromised. To reset your password, click this link.
https://adobeid.services.adobe.com/resetten_USY00CH8YAGQ-3D-C3F8V8AKGE4

Please note:
For security purposes, this link will expire 72 hours from the time it was sent.
If you cannot access this link, copy and paste the entire URL into your browser.

The Adobe Team
Copyright 2018 Adobe Systems Incorporated. All rights reserved.
Adobe Systems Incorporated. All rights reserved. 245 Park Avenue, San Jose, CA 95110 USA

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

Simulation Wizard: Unlaunched

Site: Haymont Tires, Permissions: consoleadmin

60% Complete

< Previous

✉ Design Phishing Email

Email Template

Adobe Password Reset

Customize this template

Use empty template

From: "Adobe Systems" <adobe@admin-alerts.com>
Subject: Your Adobe Account Has Been Compromised

Dear {FIRSTNAME} {LASTNAME}

Your Adobe account has been compromised. To reset your password, click this link.
https://adobeid.services.adobe.com/resetten_j8cY00CH8YAGQ-3D-C3F8V84K6E4

Please note:
For security purposes, this link will expire 72 hours from the time it was sent.
If you cannot access this link, copy and paste the entire URL into your browser.

The Adobe Team
Copyright 2018 Adobe Systems Incorporated. All rights reserved.
Adobe Systems Incorporated. All rights reserved. 245 Park Avenue, San Jose, CA 95110 USA

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

Simulation Wizard: Unlaunched

Customize Email Template

(Changes made here affect only this campaign. The original email template will not be modified)

From Name
Adobe Systems

From Address
adobe @admin-alerts.com

Subject
Your Adobe Account Has Been Compromised

Email Body

Dear [FIRSTNAME] [LASTNAME]

Your Adobe account has been compromised. To reset your password, click this link.
https://adobeid.services.adobe.com/reset/en_US/Y63QH8YAS5CJ0C5PRVBMGK4

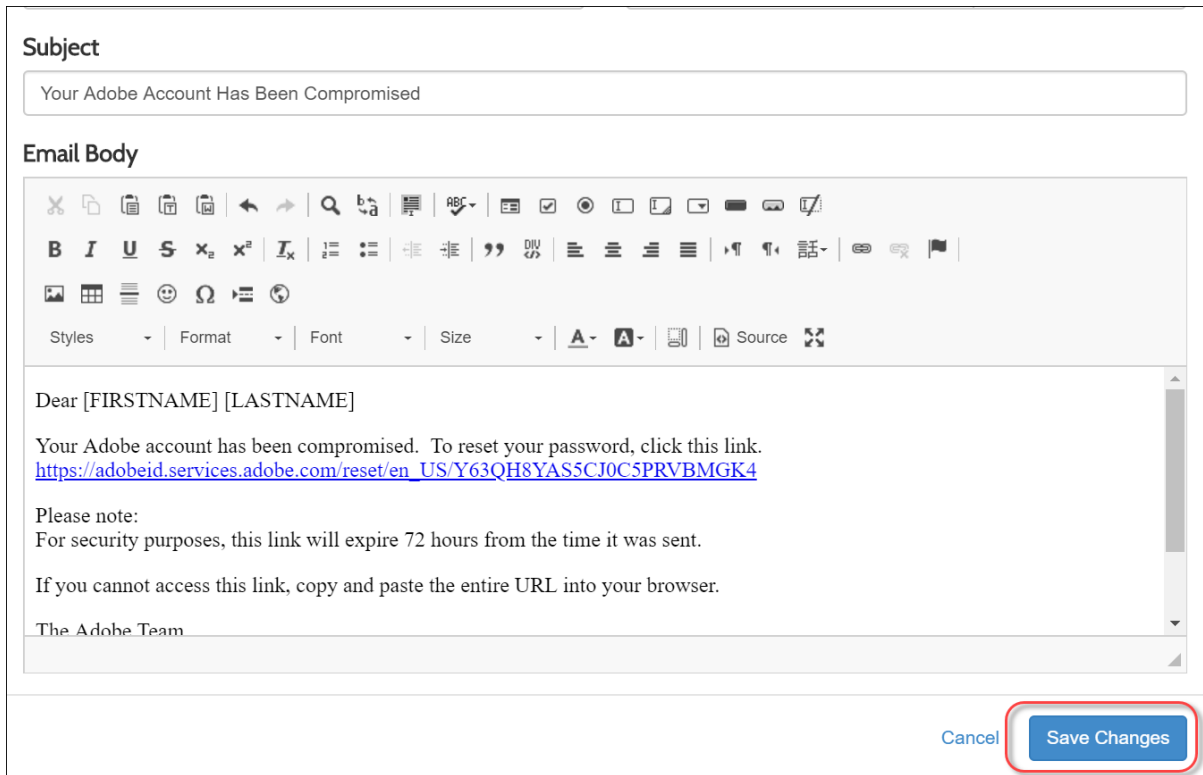
Please note:
For security purposes, this link will expire 72 hours from the time it was sent.

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.



Subject

Your Adobe Account Has Been Compromised

Email Body

Dear [FIRSTNAME] [LASTNAME]

Your Adobe account has been compromised. To reset your password, click this link.
https://adobeid.services.adobe.com/reset/en_US/Y63QH8YAS5CJ0C3PRVBMGK4

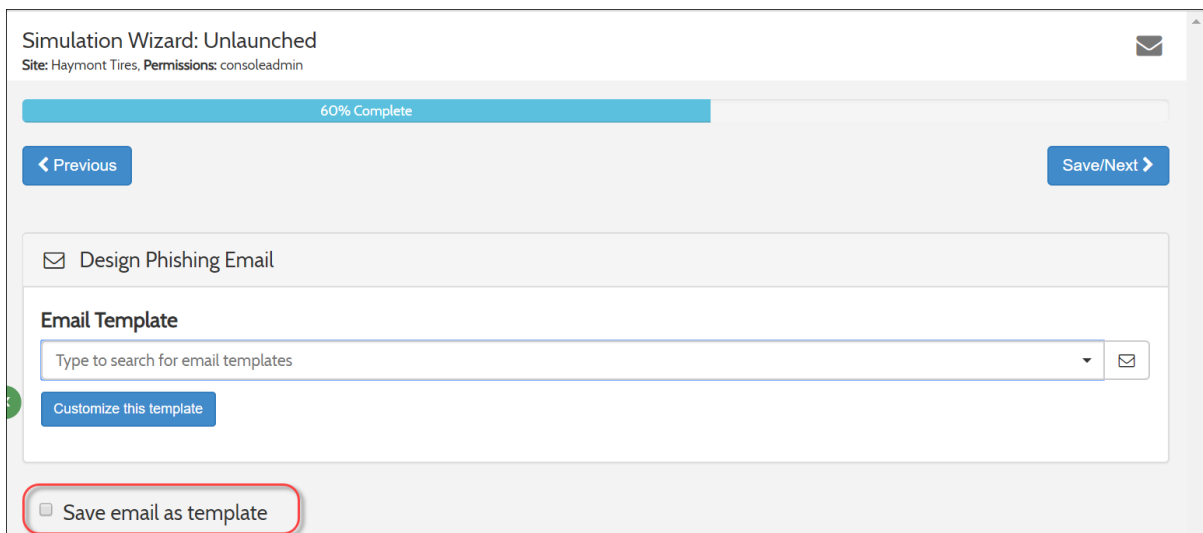
Please note:
For security purposes, this link will expire 72 hours from the time it was sent.

If you cannot access this link, copy and paste the entire URL into your browser.

The Adobe Team

Cancel **Save Changes**

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



Simulation Wizard: Unlaunched

Site: Haymont Tires, Permissions: consoleadmin

60% Complete

Previous Save/Next

Design Phishing Email

Email Template

Type to search for email templates

Customize this template

☐ Save email as template

10. You've now created a phishing simulation and can move on with the next step, [Designing Phishing Sites on page 29](#).
-

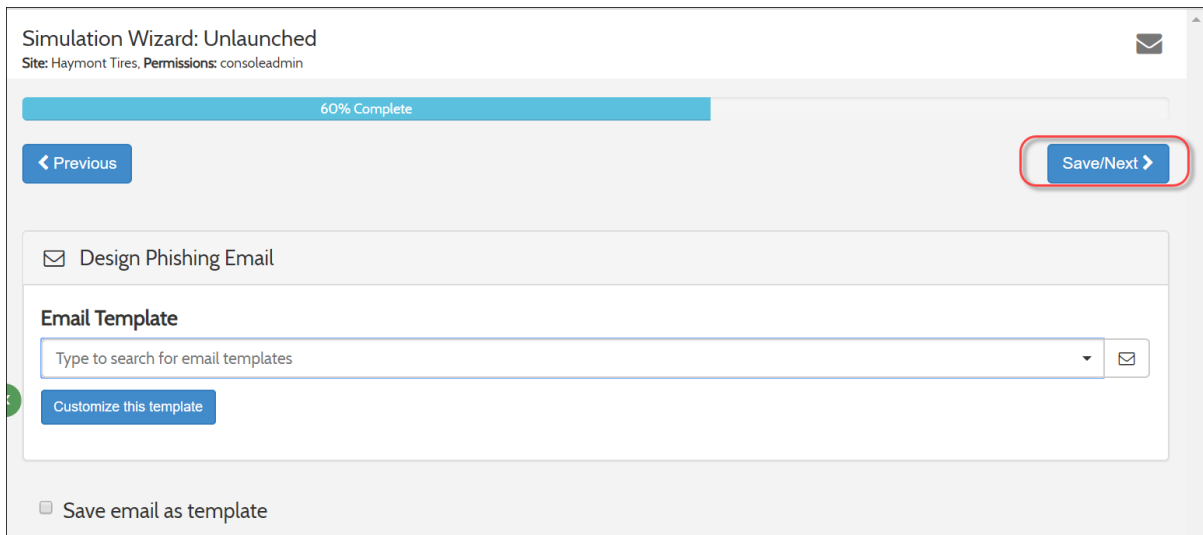
Designing Phishing Sites

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 screenshot shows the 'Simulation Wizard: Unlaunched' interface. At the top, it displays 'Site: Haymont Tires, Permissions: consoleadmin'. A progress bar indicates '60% Complete'. Below the progress bar, there are two buttons: 'Previous' on the left and 'Save/Next' on the right. The 'Save/Next' button is highlighted with a red rectangle. The main content area is titled 'Design Phishing Email' and contains an 'Email Template' section. This section has a search bar with the placeholder text 'Type to search for email templates' and a 'Customize this template' button. At the bottom of the panel, there is a checkbox labeled 'Save email as template'.

The Design Phishing Site panel displays.

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

80% Complete

< Previous Save/Next >

✉ Design Phishing Site

URL Hostname

http:// www .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.

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.

The screenshot shows a web interface for designing a phishing site. At the top, a blue progress bar indicates '80% Complete'. Below this are two buttons: '< Previous' on the left and 'Save/Next >' on the right. The main section is titled 'Design Phishing Site' with an envelope icon. Under the 'URL Hostname' section, there is a text input field containing 'http:// www' and a dropdown menu showing '.admin-alerts.com'. Below the input field, a red box highlights a list of suggested URL types: 'www securities warning dropbox facebook twitter linkedin gmail lotusnotes microsoft office365 icloud ups usps fedex'. Under the 'Site Type' section, there are three buttons: 'Education Page' (which is selected and highlighted in grey), 'Lure Page', and 'Broken Link'. At the bottom, a light blue box contains the text: 'When a target clicks the link in the email, they will be taken directly to the education page.'

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	<p>The Education Page button.</p> <p>When you click this button, scroll down the page and create an education page.</p> <p>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.</p> <p>For more information, see Designing Education Pages on page 36.</p>
A Lure Page	<p>The Lure Page button.</p> <p>When you click this button, scroll down the page and create a lure page.</p> <p>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.</p> <p>For more information, see Designing Lure Pages on page 53.</p> <p>These templates are customizable, or you can create your own. Lure pages are optional and used to add an 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.</p>

To Create This...	Click This...
<p>A Broken Link Page</p>	<p>The Broken Link button.</p> <p>When you click this button, scroll down the page and create a Broken Link page.</p> <p>When a target clicks the link in the email, they will be taken to the 404 page.</p> <p>For more information, see Designing Broken Link Pages on page 57.</p> <div data-bbox="712 804 1458 938"> <p>Note: An Education page cannot be used with a Broken Link page.</p> </div>

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

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

The final review panel displays.

Chapter 2: Creating and Launching Phishing Simulations

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

100% Complete - Ready to launch!

[< Previous](#) [Launch Simulation](#)

noreply @ securecast.com [Send test](#)

[Send test to JDoe@gmail.com](#)

Review and Launch

Simulation Details Targets Phishing Email Phishing Websites

- Simulation Name: Test
- Description: Test
- Advanced:
 - Notifications:
 - On mail open: false
 - On link click: false
 - On form post: false
 - Send notifications to:
 - JDoe@gmail.com
 - Options:
 - Anonymize target email addresses after sending: false
- Phishing Url: gmail.admin-alerts.com

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	<p>Click the Training Module button, then select the module you want to send the user to.</p> <p>For more information, see Creating Training Modules on page 37.</p>
A Template or Infographic	<p>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.</p> <p>For more information, see Creating Templates and Infographics on page 43.</p>

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.

For 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.

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.

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

The screenshot shows the 'Simulation Wizard: Unlaunched' interface. At the top, it indicates 'Site: Haymont Tires, Permissions: consoleadmin' and a progress bar at 80% Complete. Navigation buttons for '< Previous' and 'Save/Next >' are present. The 'Design Phishing Site' section includes a 'URL Hostname' field with 'http:// gmail' and a dropdown for '.admin-alerts.com'. Below this is a 'Site Type' section with three tabs: 'Education Page' (selected), 'Lure Page', and 'Broken Link'. A blue box explains: 'When a target clicks the link in the email, they will be taken directly to the education page.' The 'Design Education Page' section features a row of two buttons: 'Training Module' (highlighted with a red circle) and 'Template or Infographic'. Below this is an 'Education Template' section with a search bar 'Type to search web templates', a 'Customize this template' button, and two checkboxes: 'Disable "Powered By" logo (Powered by WEBROOT)' and 'Add branding to Education'.

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.

☒ Design Education Page

Training Module 

Select a training module

2FA - Factor Fake Out Publisher: NINJIO >

401k Scams - 401 Chaos Publisher: NINJIO >

Amazon SAT test Publisher: Webroot >

Auditing - Network and System Compliance Auditing Publisher: SAP Litmos >

BEC - A Compromising Crash Publisher: NINJIO >

BEC - Phishing the Stream Publisher: NINJIO >

BEC - You Never Call... Publisher: NINJIO >

Breach Awareness - Breach Avoidance Publisher: Webroot >

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

Template or Infographic ⓘ

Module:

Landing Page Content: ⓘ

Landing Page Title (Optional):

Assigned Training

Message (Optional):

Please complete the following training

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

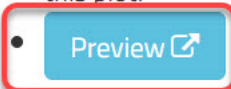
Training Module

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.



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

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

80% Complete

[< Previous](#) [Save/Next >](#)

☒ Design Phishing Site

URL Hostname

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

Education Template

☐ Disable "Powered By" logo (Powered by **WEBROOT**)

☐ Add branding to Education

Creating Templates and Infographics

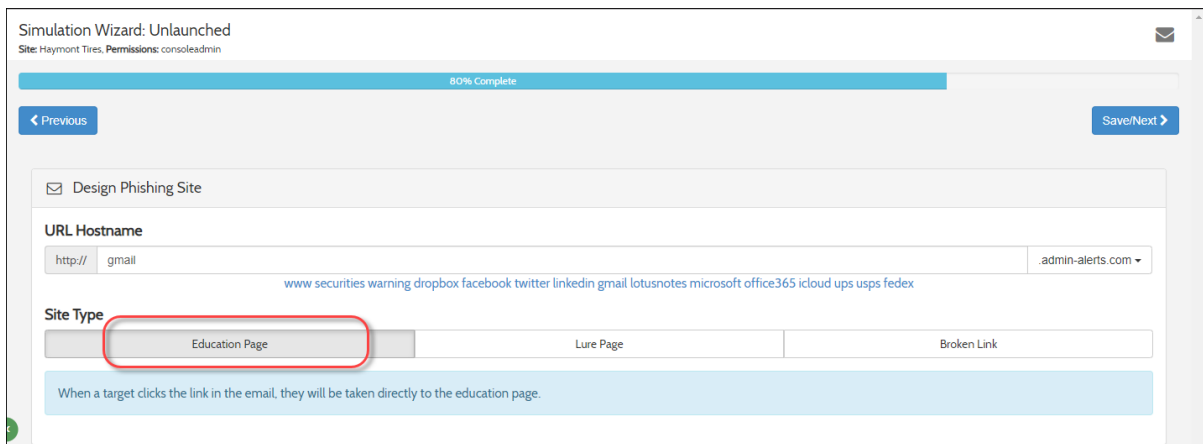
Follow this procedure when you've decided to create an Infographic Page where your targets will be taken when they click on a link in a phishing email.

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.

For more information, see [Designing Phishing Sites on page 29](#).

To create an infographic:

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



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.

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

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

The Education Template displays.

Chapter 2: Creating and Launching Phishing Simulations

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.

The screenshot shows the 'Simulation Wizard: Unlaunched' interface. At the top, it indicates 'Site: Haymont Tires, Permissions: consoleadmin' and a progress bar at '60% Complete'. Navigation buttons for '< Previous' and 'Save/Next >' are present. The 'Design Phishing Site' section includes a 'URL Hostname' field with 'http:// gmail' and a dropdown set to '.admin-alerts.com'. Below this is a 'Site Type' section with three tabs: 'Education Page' (selected), 'Lure Page', and 'Broken Link'. A descriptive text box states: 'When a target clicks the link in the email, they will be taken directly to the education page.' The 'Design Education Page' section has two tabs: 'Training Module' and 'Template or Infographic'. The 'Education Template' dropdown menu is highlighted with a red box, showing the text 'Type to search web templates'. Below the dropdown is a 'Customize this template' button. At the bottom, there are two checkboxes: 'Disable "Powered By" logo (Powered by WEBROOT)' and 'Add branding to Education'.

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

Chapter 2: Creating and Launching Phishing Simulations

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](#)

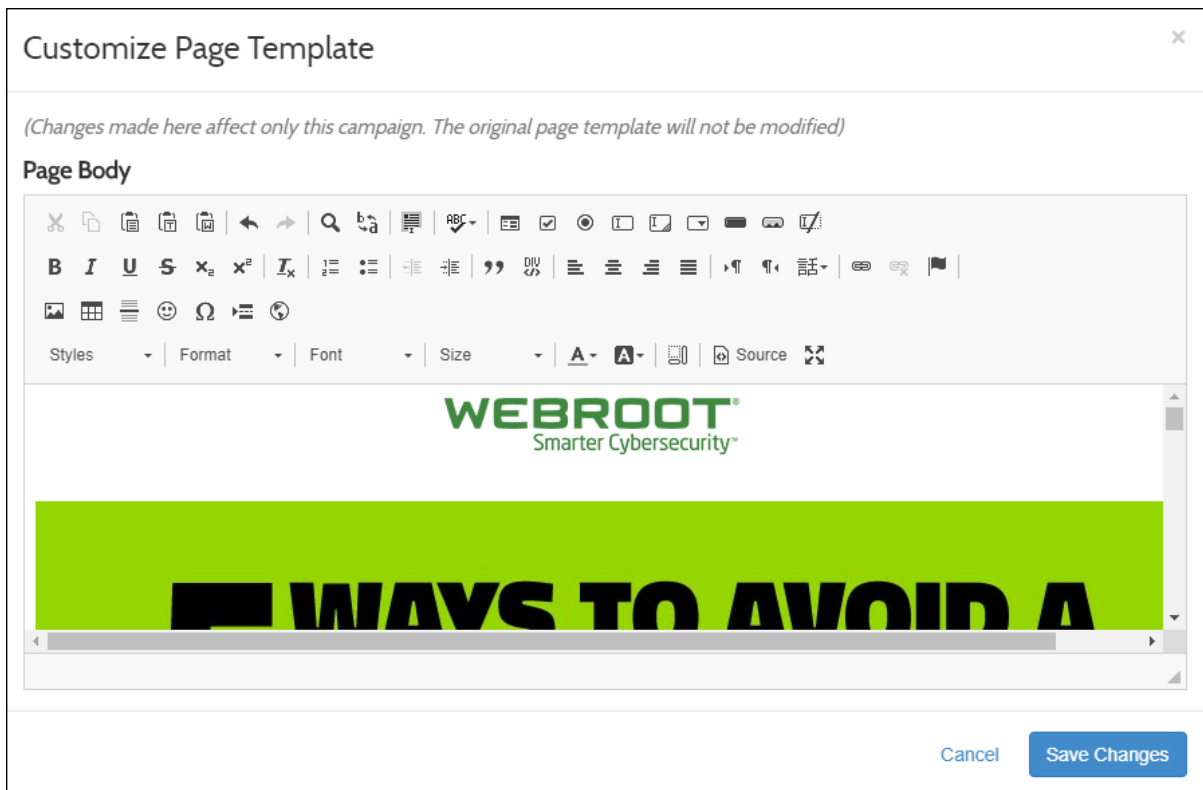
☐ Disable "Powered By" logo (Powered by **WEBROOT**)

☐ Add branding to Education

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.

Chapter 2: Creating and Launching Phishing Simulations

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

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

Security Awareness Training Admin Guide

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

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

Text

Link URL

Preview

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

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

60% 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

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.

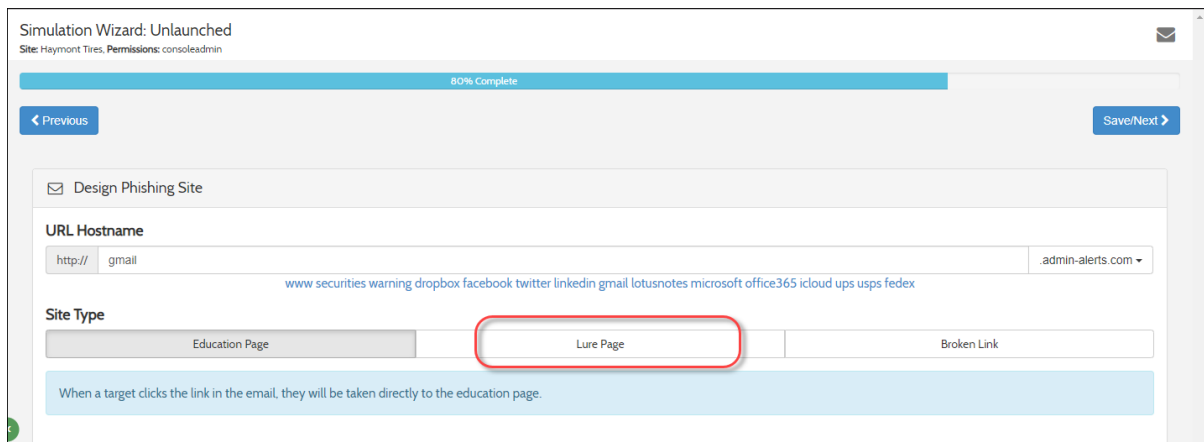
Lure Page templates are customizable, or you can create your own. Lure pages are optional and used to add an extra web landing page after a user clicks an email lure and before you take the user to [education](#) or a [broken link](#) page.

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.

For 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.



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.

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

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

If your victim clicks through from the phishing lure email, they will be directed to the page below.

Lure Template

Type to search web templates

- Name: Community Test
Categories: Amazon
Scope: global
- Name: Dropbox Login
Categories: Login English (US) - [en-us] Dropbox
Scope: system
- Name: Google Login
Categories: Login Google English (US) - [en-us]
Scope: system

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

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

If your victim clicks through from the phishing lure email, they will be directed to the page below.

Lure Template

Community Test

Customize this template Use empty template

Just testing this page.

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.

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](#)

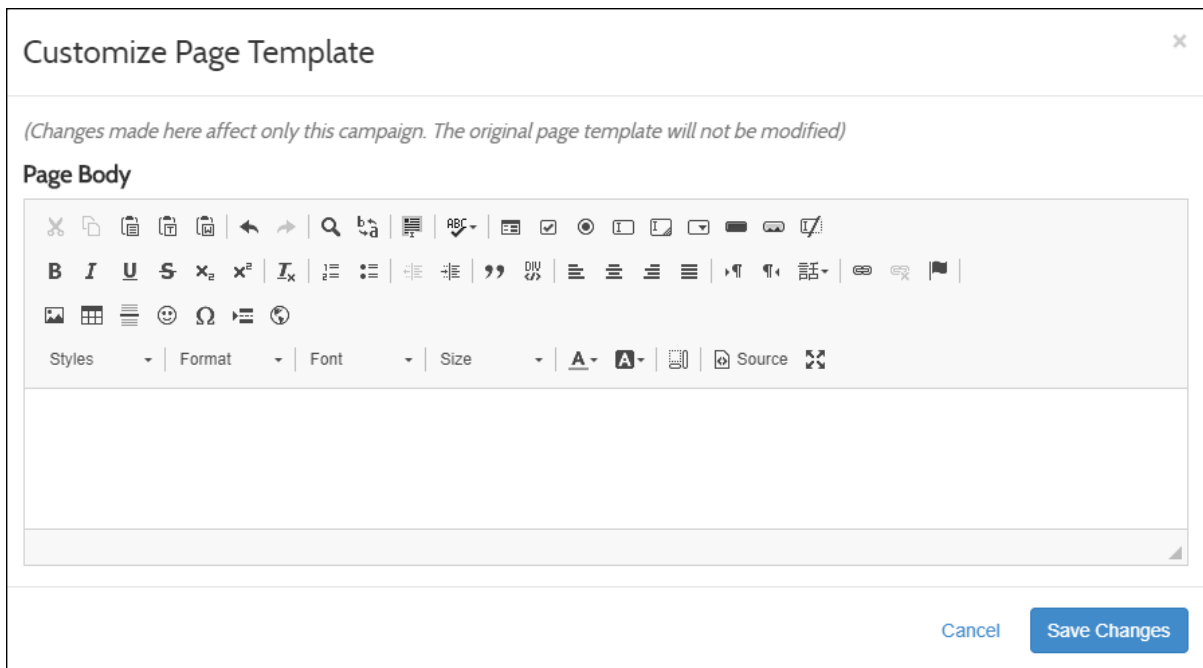
Site Type
Education Page Lure Page Broken Link

If your victim clicks through from the phishing lure email, they will be directed to the page below.

Lure Template
Community Test

Customize this template Use empty template

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.

For 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.

The screenshot shows the 'Simulation Wizard: Unlaunched' interface. At the top, it indicates 'Site: Haymont Tires, Permissions: consoleadmin' and a progress bar at 60% Complete. Navigation buttons for 'Previous' and 'Save/Next' are present. The main section is titled 'Design Phishing Site'. Under 'URL Hostname', there are input fields for 'http://' and 'gmail', and a dropdown menu currently showing '.admin-alerts.com'. Below this is a list of suggested domains: 'www securities warning dropbox facebook twitter linkedin gmail lotusnotes microsoft office365 icloud ups usps fedex'. The 'Site Type' section has three radio buttons: 'Education Page', 'Lure Page', and 'Broken Link'. The 'Broken Link' option is selected and highlighted with a red circle. A blue informational box below states: 'When a target clicks the link in the email, they will be taken directly to the education page.' The bottom section is titled 'Design Education Page' and contains options for 'Training Module' and 'Template or Infographic', an 'Education Template' search bar, and checkboxes for 'Disable "Powered By" logo (Powered by WEBROOT)' and 'Add branding to Education'.

A list of broken link types displays.

Security Awareness Training Admin Guide

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

You may want to discourage office-talk between recipients on a campaign. A link resulting in a 404 is often discarded as a bad link/forgotten, and may not be talked about as often internally as opposed to an education or lure page ("Hey Dave, someone tried phishing my email today!"). Use a 404 dead-end link to send users to an emulated 404 page. Statistics are still tracked for this option as a visit. You may emulate many common 404 types:

- Apache 404
- IIS6 404
- IIS7 404
- Nginx 404
- Refused: (dynamicly changes depending on client browser)
 - Chrome broken link
 - Edge broken link
 - Internet Explorer broken link
 - Safari broken link

404 Type:

apache

Design Education Page

(An education page cannot be used with a Broken Link site type)

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

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

You may want to discourage office-talk between recipients on a campaign. A link resulting in a 404 is often discarded as a bad link/forgotten, and may not be talked about as often internally as opposed to an education or lure page ("Hey Dave, someone tried phishing my email today!"). Use a 404 dead-end link to send users to an emulated 404 page. Statistics are still tracked for this option as a visit. You may emulate many common 404 types:

- Apache 404
- IIS6 404
- IIS7 404
- Nginx 404
- Refused: (dynamicly changes depending on client browser)
 - Chrome broken link
 - Edge broken link
 - Internet Explorer broken link
 - Safari broken link

404 Type:

apache

Design Education Page

(An education page cannot be used with a Broken Link site type)

- 58 -

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

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

60% 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

- Continue with [Reviewing and Sending Phishing Simulations on page 60](#).

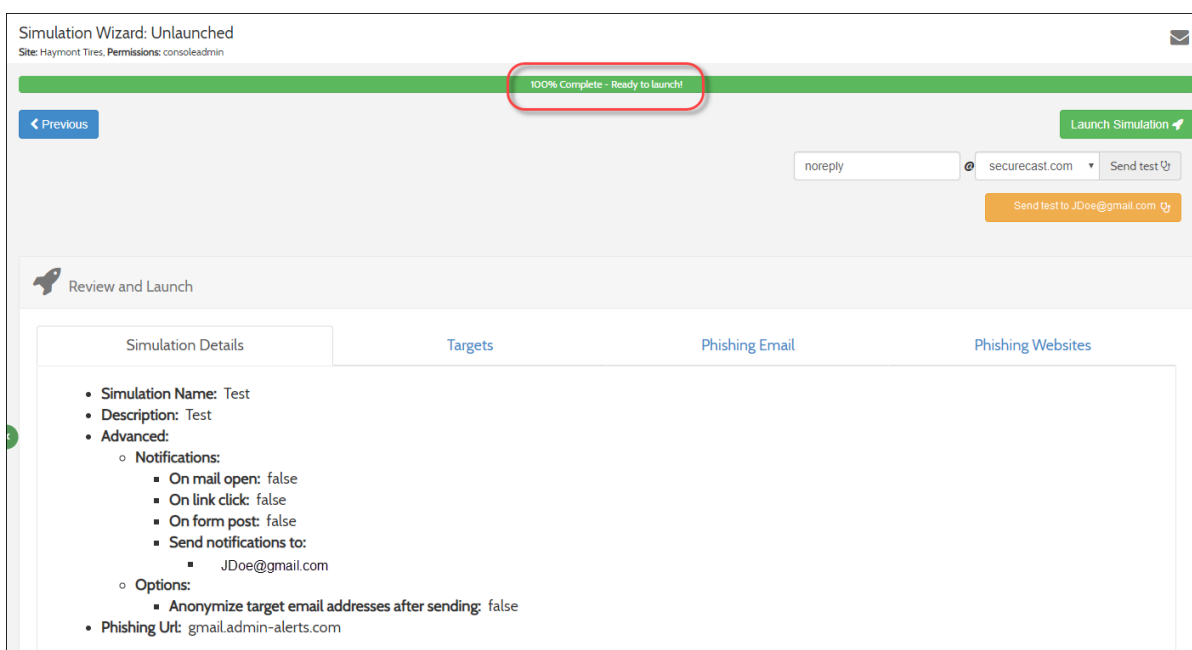
Reviewing and Sending Phishing Simulations

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](#).

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

100% Complete - Ready to launch!

Previous Launch Simulation

noreply @ securecast.com Send test

Send test to JDoe@gmail.com

Review and Launch

Simulation Details Targets Phishing Email Phishing Websites

- Simulation Name: Test
- Description: Test
- Advanced:
 - Notifications:
 - On mail open: false
 - On link click: false
 - On form post: false
 - Send notifications to:
 - JDoe@gmail.com
 - Options:
 - Anonymize target email addresses after sending: false
- Phishing Url: gmail.admin-alerts.com

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

Security Awareness Training Admin Guide

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

100% Complete - Ready to launch!

[< Previous](#) [Launch Simulation](#)

noreply @ securecast.com [Send test](#)

[Send test to JDoe@gmail.com](#)

[Review and Launch](#)

Simulation Details Targets Phishing Email Phishing Websites

- Simulation Name: Test
- Description: Test
- Advanced:
 - Notifications:
 - On mail open: false
 - On link click: false
 - On form post: false
 - Send notifications to:
 - JDoe@gmail.com
 - Options:
 - Anonymize target email addresses after sending: false
- Phishing Url: gmail.admin-alerts.com

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

Simulation Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

100% Complete - Ready to launch!

[< Previous](#) [Launch Simulation](#)

noreply @ securecast.com [Send test](#)

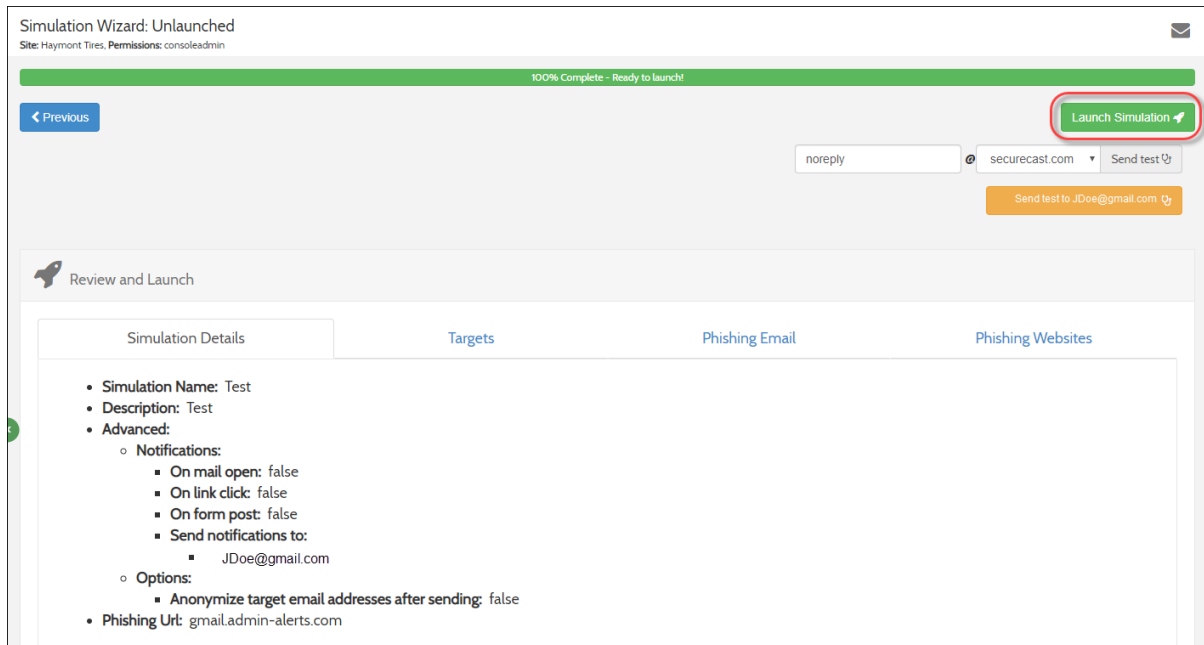
[Send test to JDoe@gmail.com](#)

[Review and Launch](#)

Simulation Details Targets Phishing Email Phishing Websites

- Simulation Name: Test
- Description: Test
- Advanced:
 - Notifications:
 - On mail open: false
 - On link click: false
 - On form post: false
 - Send notifications to:
 - JDoe@gmail.com
 - Options:
 - Anonymize target email addresses after sending: false
- Phishing Url: gmail.admin-alerts.com

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](#).

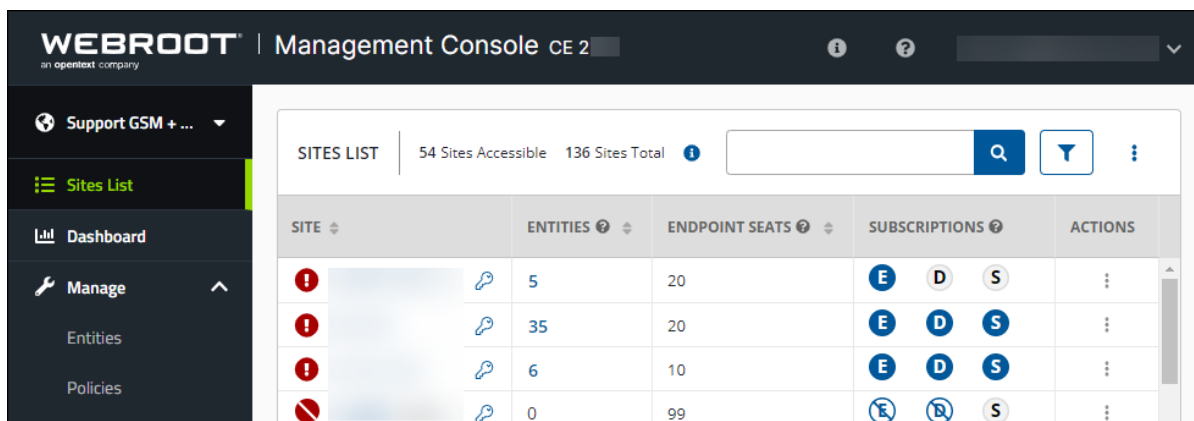
Selecting Sites in the Dashboard

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

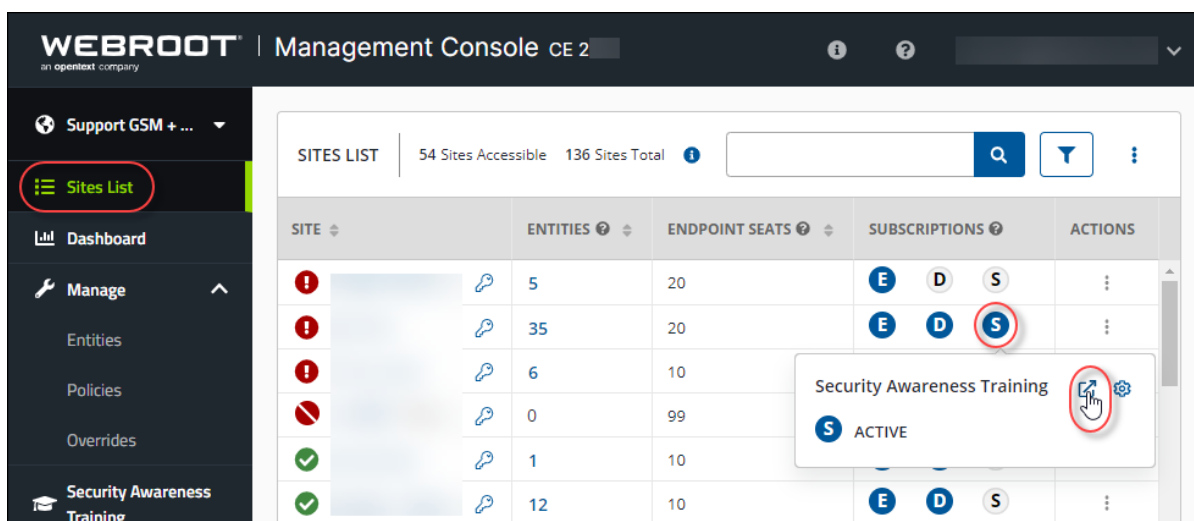
To select a site:

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

The Management Console displays.

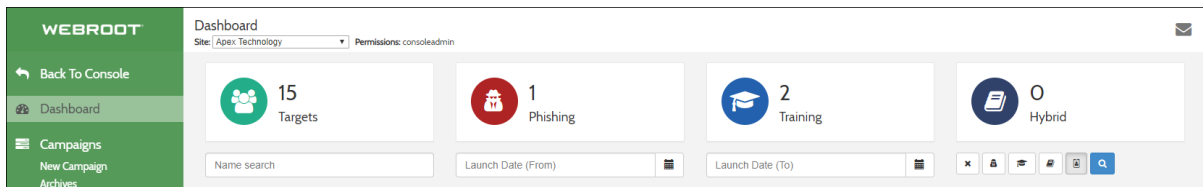


2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.

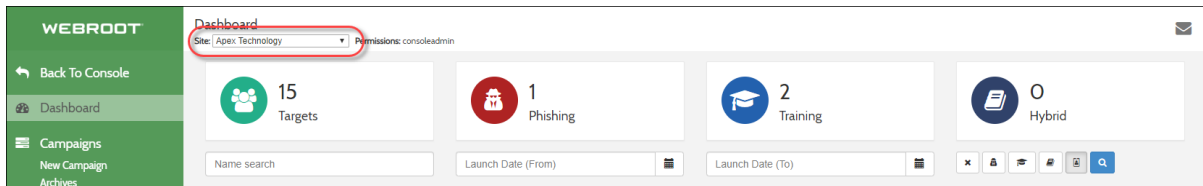


Chapter 2: Creating and Launching Phishing Simulations

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](#)

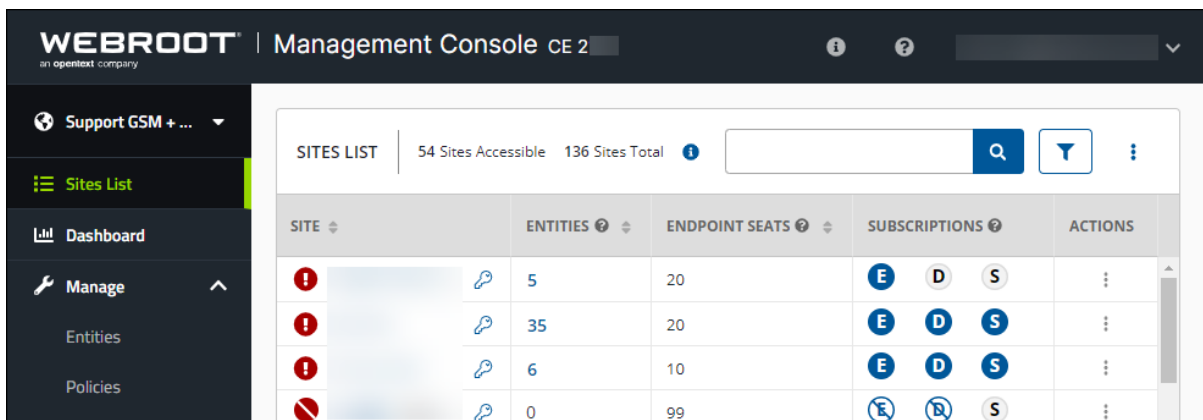
Note: You can send employees to a training campaign, even without sending them a phishing campaign.

Selecting Trainees

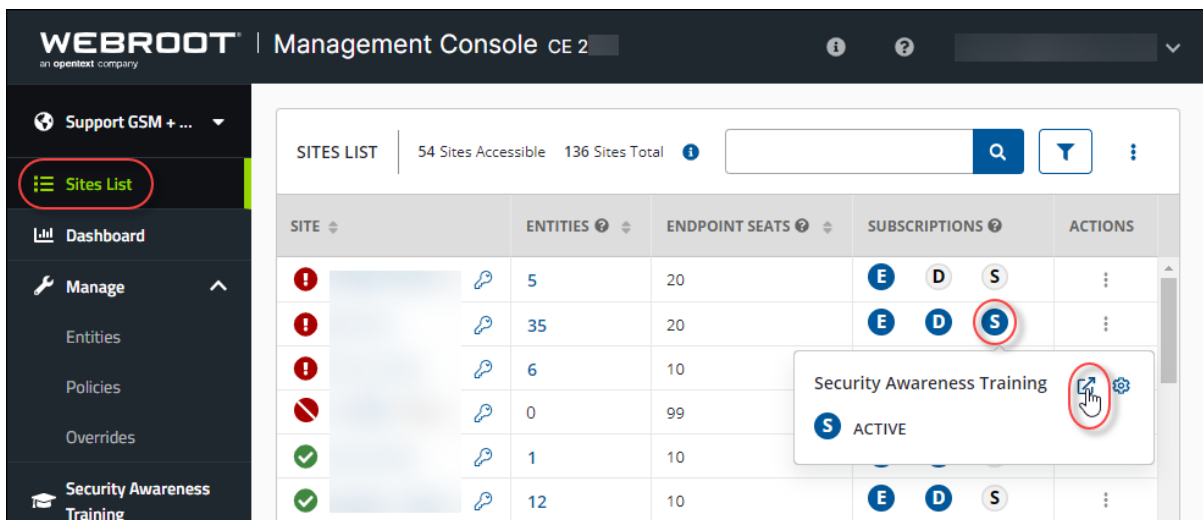
Use the following procedure to select trainees for training sessions.

To select a trainee:

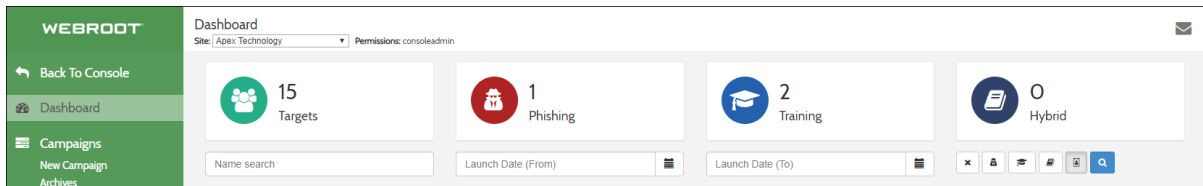
1. [Log in to the Management Console.](#)



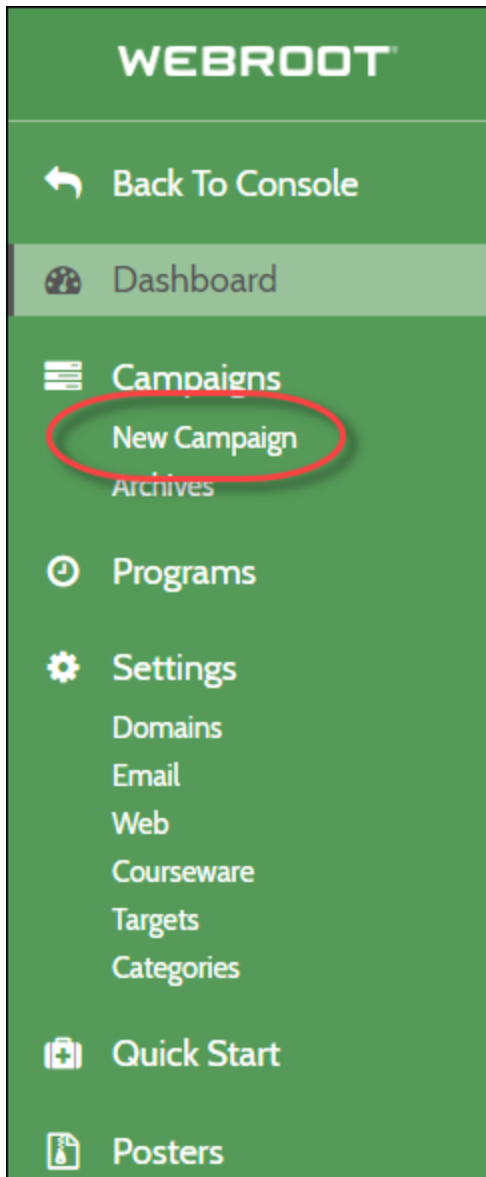
2. In the **Sites List** tab, choose a Site and click the **Go to Security Awareness Training** icon in the **Actions** column.



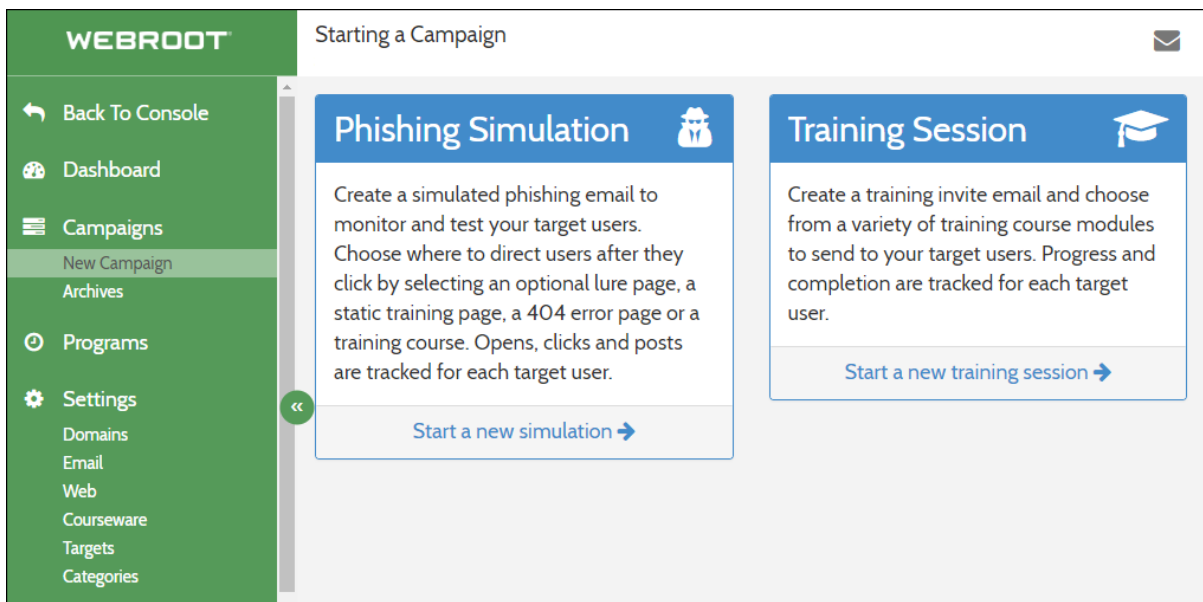
The Security Awareness Training console displays.



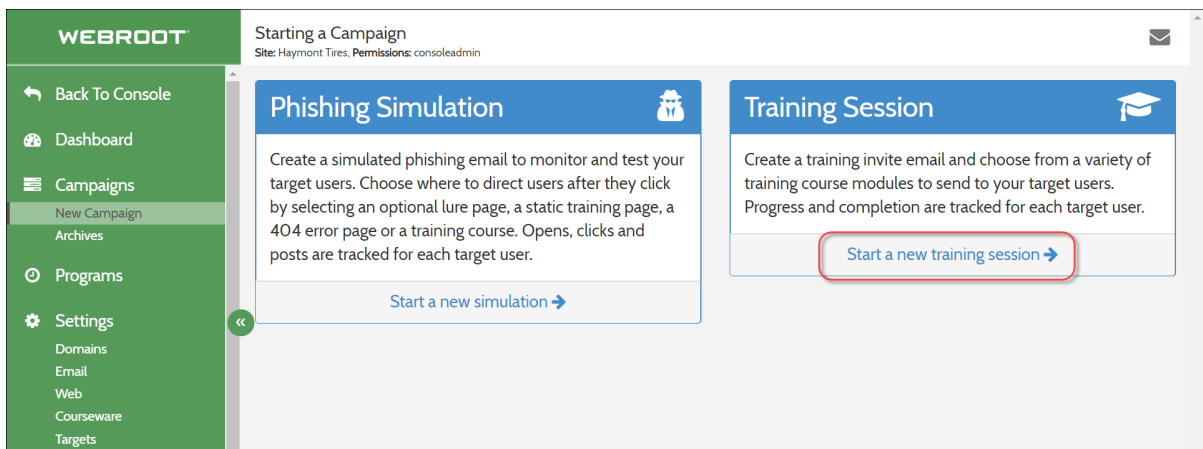
3. In the navigation pane, click **New Campaign**.



The **Starting a Campaign** panel displays.



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



The **New Campaign Wizard** displays.

WEBROOT

New Campaign Wizard
Site: Haymont Tires, Permissions: consoleadmin

0%

< Previous

Training Session Basics

Session Name
Example: Training Session 101

Description
Describe your campaign

☐ Show Advanced Options

Save Training Session


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.


Advanced Options:

☐ Enable Registration 



Start Date:





Expiration



Reminders

:

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.

The screenshot shows the 'Targets' interface with the following elements:

- Available Targets** header with 'Targets' and 'Tags' buttons.
- Search filters: First Name, Last Name, Email, and a 'Select tags to search' dropdown.
- Summary boxes: 'Selected Targets: 3/500', 'Targets: 9', and 'Verified domains only'.
- Table of targets with columns: First Name, Last Name, Email, and Tags.

	First Name	Last Name	Email	Tags
<input checked="" type="checkbox"/>	Roland	Roland	roland@company.com	
<input checked="" type="checkbox"/>	Dan	Dan	dan@company.com	
<input checked="" type="checkbox"/>	Clifford	Clifford	clifford@company.com	
<input type="checkbox"/>	Cecelia	Cecelia	cecilia@company.com	
<input type="checkbox"/>	Leroy	Leroy	leroy@company.com	

- 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.

The screenshot shows the 'Targets' tab in the Security Awareness Training Admin interface. A red box highlights the 'Select tags to search' dropdown menu, which has 'Floor' selected. The interface includes a 'Save/Next' button, a 'Targets' tab, a search bar, a list of targets, and a table with columns for Email and Tags.

Email	Tags
administrator@webrootsalesdemo.com	Floor

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.

Wizard: Unlaunched
Site: Haymont Tires, Permissions: consoleadmin

60% Complete

< Previous Save/Next >

✉ Design Invitation Email

Email Template

Type to search for email templates

Name: Basic Training Invitation
Categories: English (US) - [en-us]

From: "Webroot Training Invites" <training-invites@webroottraining.com>
Subject: Webroot Training Invite

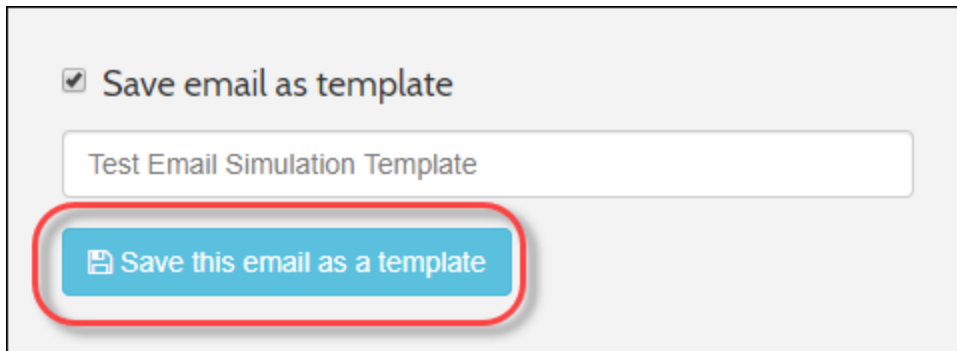
[FIRSTNAME],
You have been invited to take part in a training session by your company. Please [click here](#)
to start the course.
If you have any questions, please contact your administrator.

☐ Save email as template

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


The screenshot shows a web interface titled "Wizard: Unlaunched" with a sub-header "Site: Haymont Tires, Permissions: consoleadmin". A progress bar indicates "60% Complete". Navigation buttons include "< Previous" and "Save/Next >". The main section is titled "Design Invitation Email" and contains an "Email Template" section. A dropdown menu shows "Basic Training Invitation" with a red circle highlighting the "Customize this template" button. Next to it is a "Use empty template" button. Below the buttons, the email preview shows "From: 'Webroot Training Invites' <training-invite@webroottraining.com>" and "Subject: Webroot Training Invite". The body text includes a placeholder "[FIRSTNAME]", a link to start the course, and a note to contact the administrator. At the bottom, there is a checkbox labeled "Save email as template".

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.



☒ Save email as template

Test Email Simulation Template

 Save this email as a template

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.

The screenshot shows the 'Design Education Page' interface. At the top, there are two tabs: 'Training Module' (selected) and 'Template or Infographic'. Below the tabs, the 'Select a training module' section displays a list of modules, each with a right-pointing arrow. A red rounded rectangle highlights this list. The modules are:

- 2FA - Factor Fake Out Publisher: NINJIO
- 401k Scams - 401 Chaos Publisher: NINJIO
- Amazon SAT test Publisher: Webroot
- Auditing - Network and System Compliance Auditing Publisher: SAP Litmos
- BEC - A Compromising Crash Publisher: NINJIO
- BEC - Phishing the Stream Publisher: NINJIO
- BEC - You Never Call... Publisher: NINJIO
- Breach Awareness - Breach Avoidance Publisher: Webroot

To the right of the list, the 'Module:' field is populated with the selected module. Below it, the 'Landing Page Content:' field is empty. The 'Landing Page Title (Optional):' field contains the text 'Assigned Training'. The 'Message (Optional):' field contains the text 'Please complete the following training'.

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.

Design Education Page


Training Module

Template or Infographic

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

Module: 2FA - Factor Fake Out

Landing Page Content:


Landing Page Title (Optional):

Assigned Training


Message (Optional):


Please complete the following training

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


 Design Education Page

Select a training module

2FA - Factor Fake Out Publisher: NINJIO

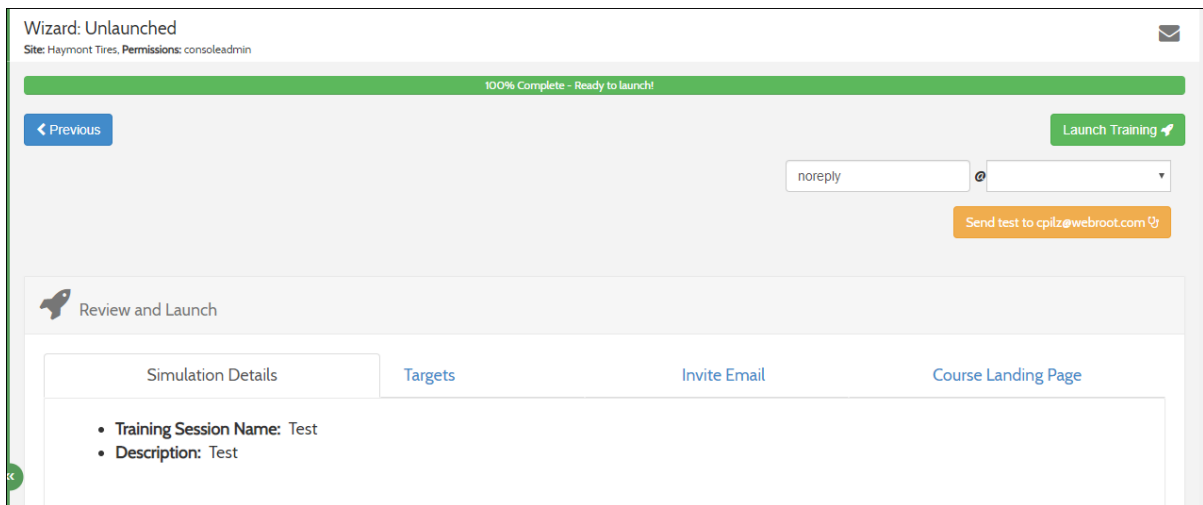


- Description: 2-Factor Authentication using your mobile phone (SMS) is a great security measure, and countless end-users have it in place – but that’s bad news for Nico as he tries to use some stolen credentials. Nico and his hacking buddy think of a scheme to get around 2FA via SMS, opening the potential 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.

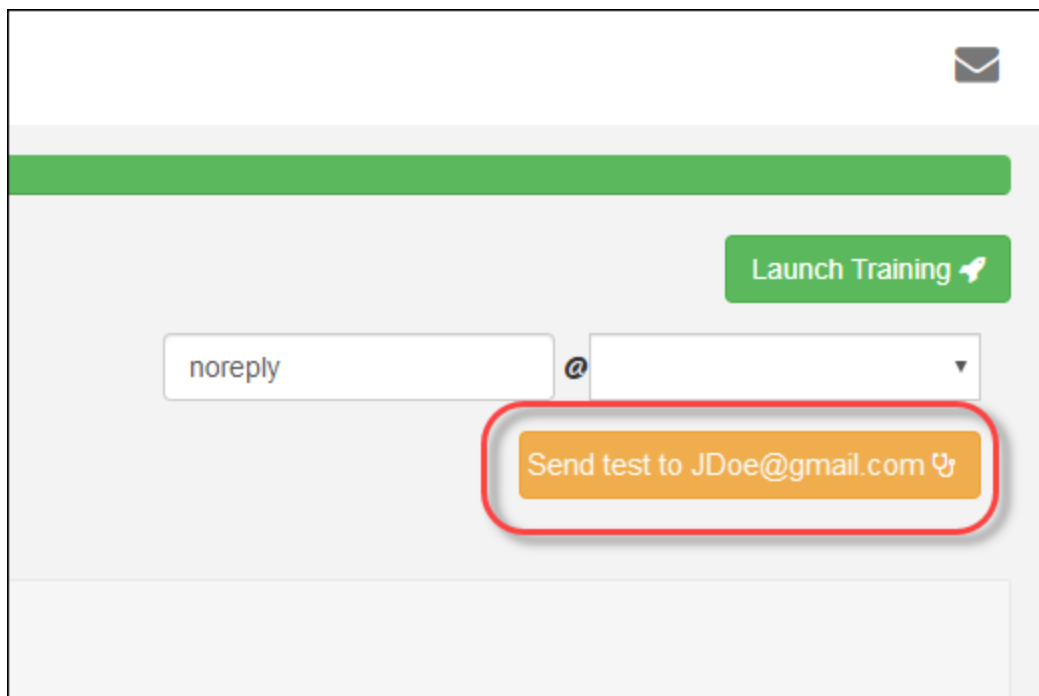
- [Preview](#) 

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

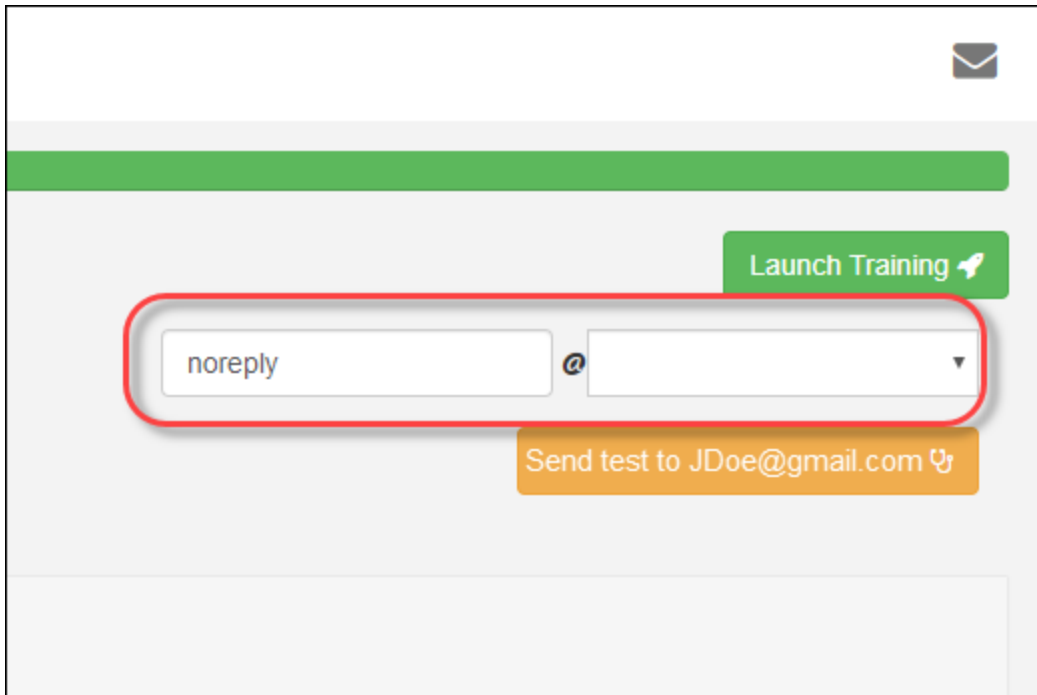
The Review and Launch panel displays.



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.

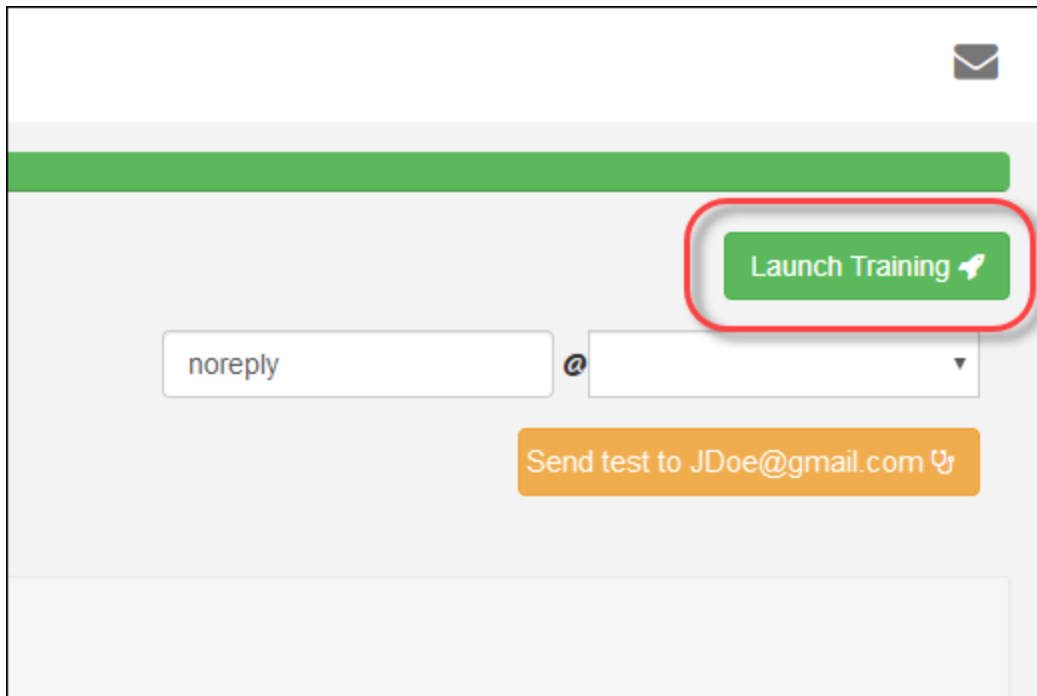


- Send out a test invitation to another individual for review.



The screenshot shows a web interface for sending test invitations. At the top right is an envelope icon. Below it is a green horizontal bar. To the right of the bar is a green button labeled "Launch Training" with a rocket icon. Below the bar is a form with two input fields: the first contains "noreply" and the second is empty. A red rounded rectangle highlights both input fields. Between the fields is an "@" symbol. Below the form is an orange button labeled "Send test to JDoe@gmail.com" with a cursor icon.

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



The screenshot shows a web interface for creating training sessions. At the top right is an envelope icon. Below it is a green horizontal bar. In the center-right, a green button labeled "Launch Training" with a white rocket icon is highlighted by a red rounded rectangle. To the left of this button is a text input field containing "noreply" followed by an "@" symbol and a dropdown menu. Below the input field is an orange button that reads "Send test to JDoe@gmail.com" with a small icon.

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

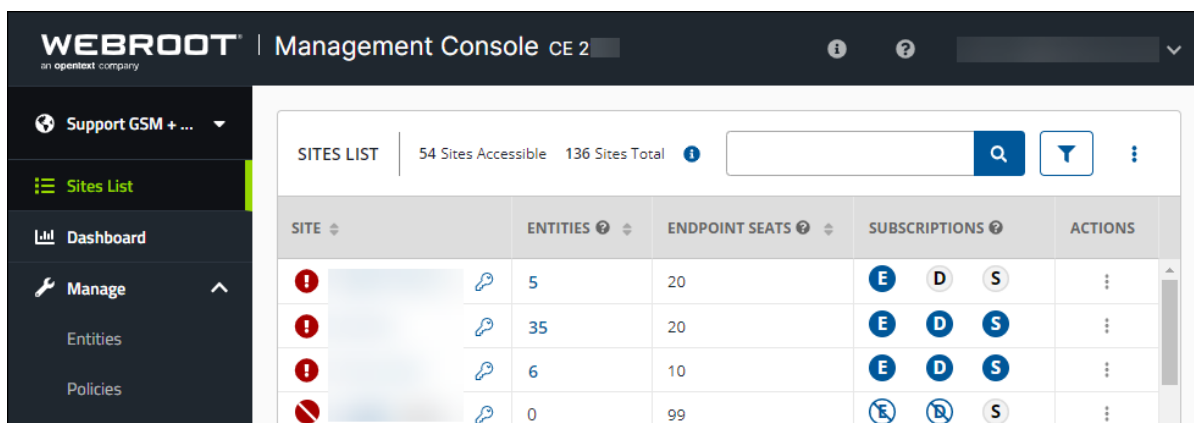
Welcome Emails are generally used for sending out an introduction to your new Security Awareness program to end users, management, IT staff, etc.

- 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:

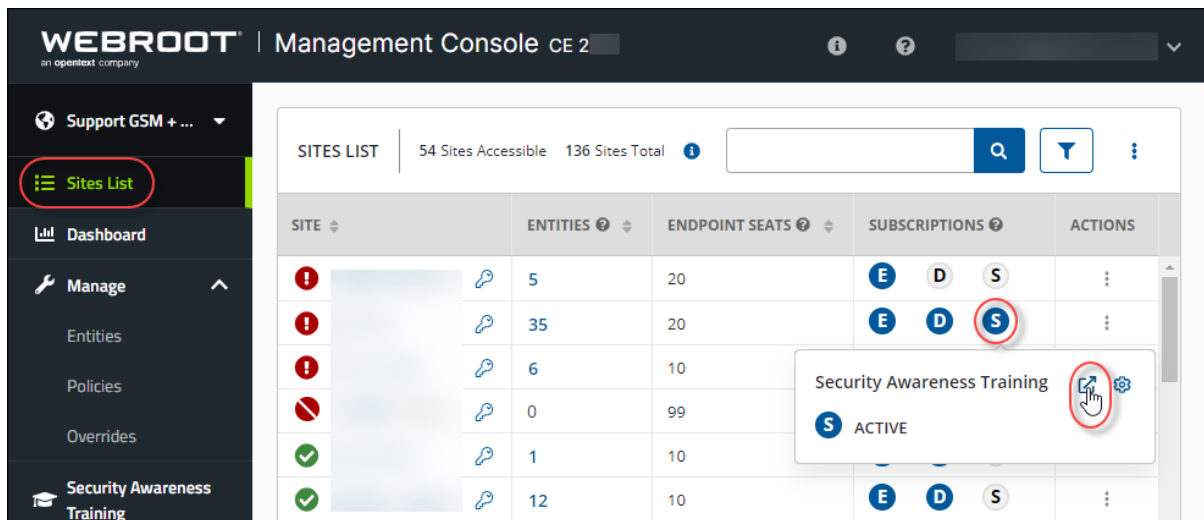
1. [Log in to the Management Console](#).

The Management Console displays.

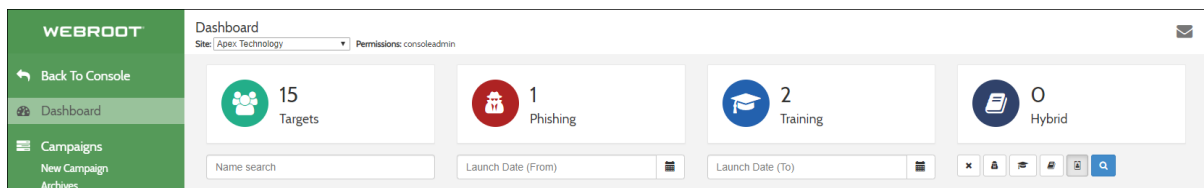


2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.

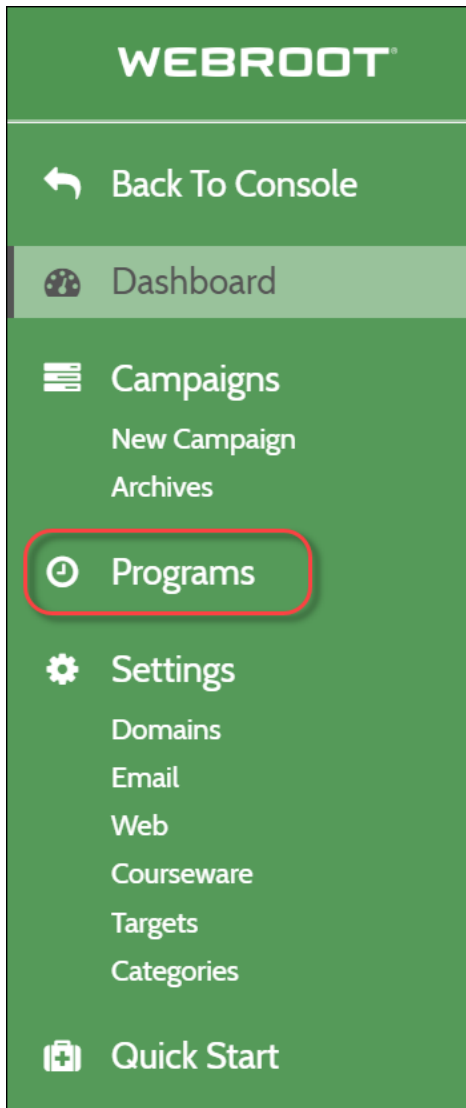
Chapter 4: Working With Programs and Campaign Scheduling



The Security Awareness Training dashboard displays.

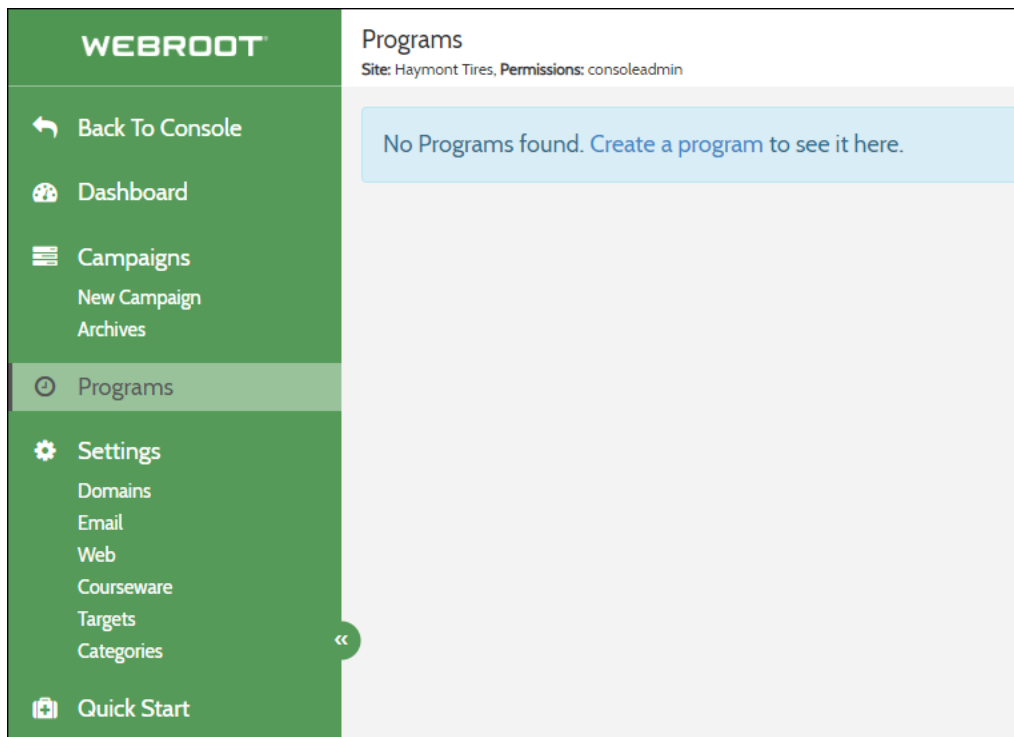


3. In the Nav bar, click the **Programs** tab.



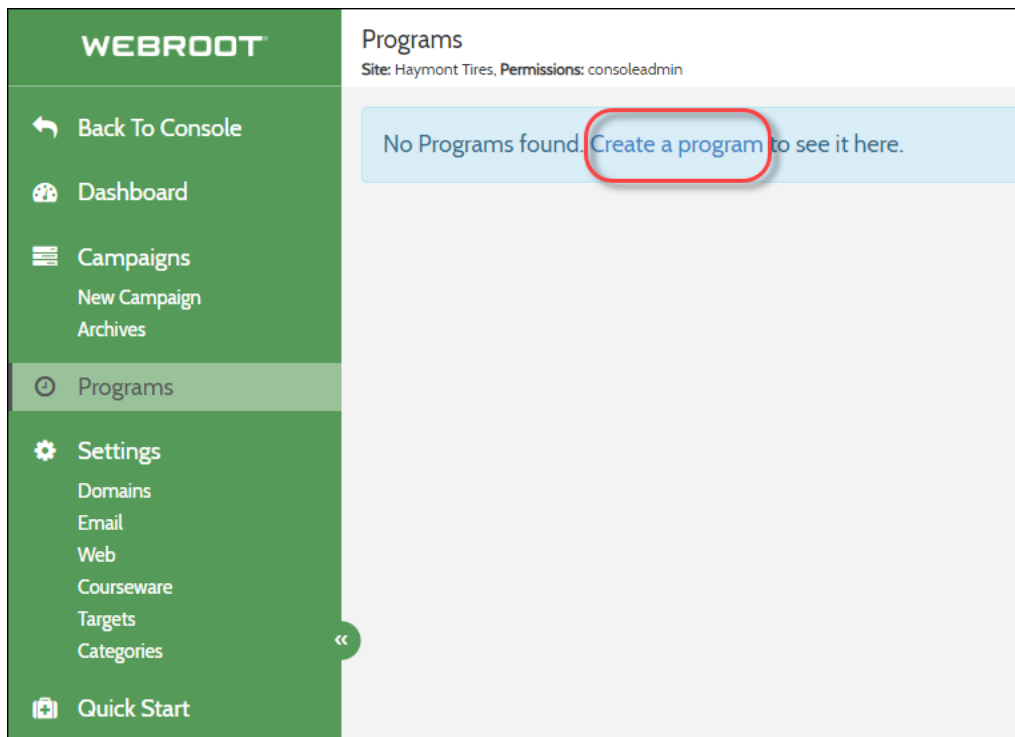
The Programs panel displays.

Chapter 4: Working With Programs and Campaign Scheduling

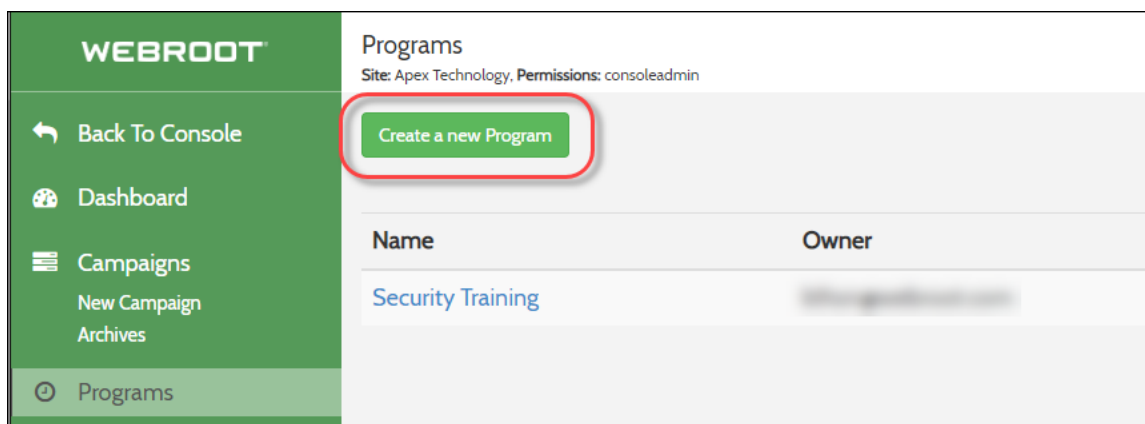


4. Do one of the following:

- If this is the first program you're creating, click the **Create a program** link.

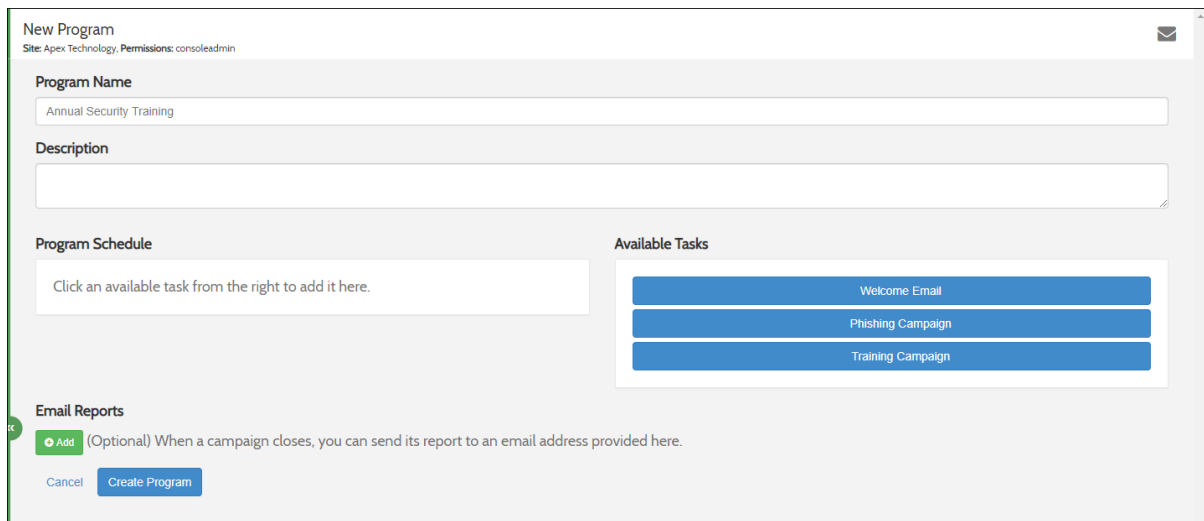


- If this is not the first program you're creating, click the **Create a new Program** button.



In either case, the New Program panel displays.

Chapter 4: Working With Programs and Campaign Scheduling



The screenshot shows a 'New Program' form. At the top, it says 'New Program' and 'Site: Apex Technology, Permissions: consoleadmin'. Below this, there are three main sections: 'Program Name', 'Description', and 'Program Schedule'. The 'Program Name' section has a text input field containing 'Annual Security Training'. The 'Description' section has a large text area. The 'Program Schedule' section has a text box with the instruction 'Click an available task from the right to add it here.' To the right of this section is a box titled 'Available Tasks' containing three blue buttons: 'Welcome Email', 'Phishing Campaign', and 'Training Campaign'. Below the 'Program Schedule' section is an 'Email Reports' section with an 'Add' button and a text input field for an email address. At the bottom of the form are 'Cancel' and 'Create Program' buttons.

New Program
Site: Apex Technology, Permissions: consoleadmin

Program Name
Annual Security Training

Description

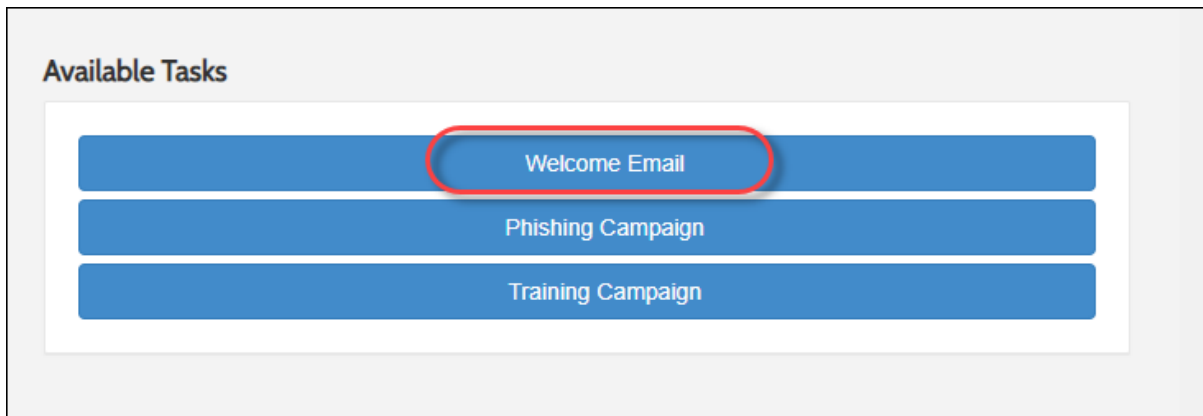
Program Schedule
Click an available task from the right to add it here.

Available Tasks

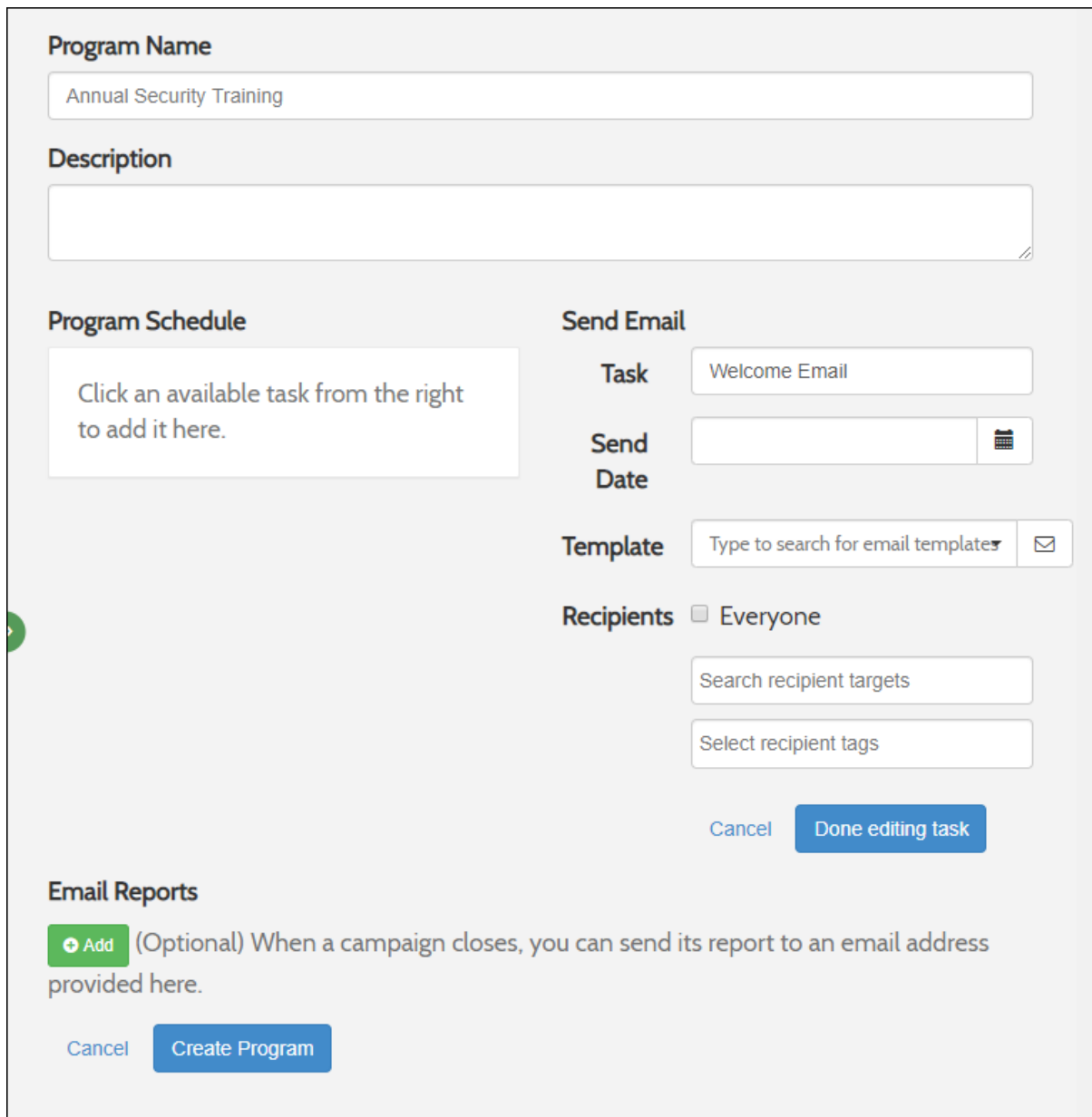
- Welcome Email
- Phishing Campaign
- Training Campaign

Email Reports
Add (Optional) When a campaign closes, you can send its report to an email address provided here.
Cancel Create Program

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



The Welcome Email edit panel displays.



The screenshot shows a web form for creating a security awareness training program. The form is divided into several sections: 'Program Name' with a text input field containing 'Annual Security Training'; 'Description' with a large text area; 'Program Schedule' with a box containing the instruction 'Click an available task from the right to add it here.'; 'Send Email' with fields for 'Task' (set to 'Welcome Email'), 'Send Date' (with a calendar icon), and 'Template' (with a search bar and an envelope icon); 'Recipients' with a checkbox for 'Everyone' and two search bars for 'Search recipient targets' and 'Select recipient tags'; and 'Email Reports' with an 'Add' button and a description: '(Optional) When a campaign closes, you can send its report to an email address provided here.' At the bottom, there are 'Cancel' and 'Create Program' buttons.

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

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

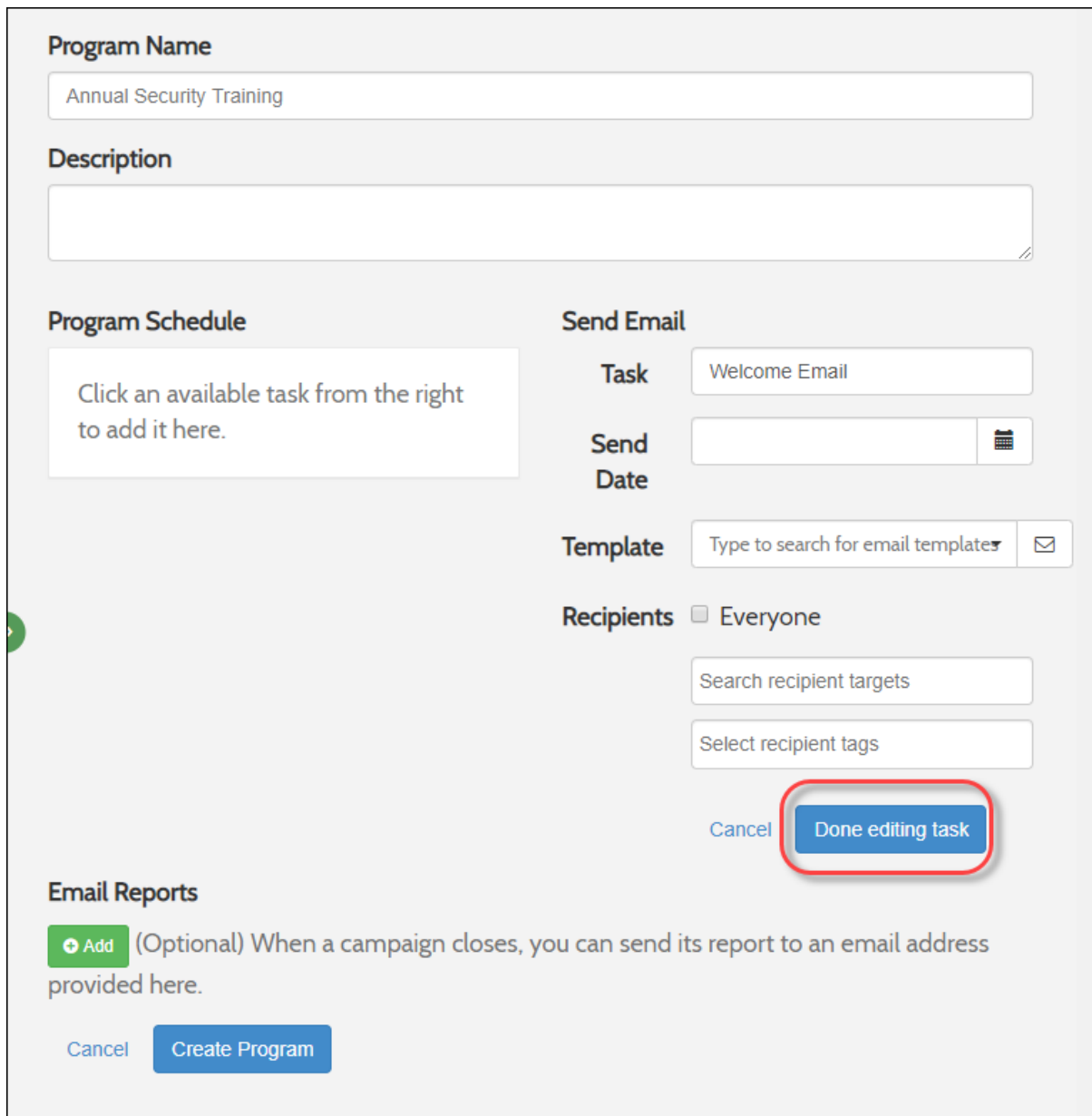
Add

(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.



The screenshot shows a web form for creating or editing a program. The form is divided into several sections: 'Program Name' with a text input field containing 'Annual Security Training'; 'Description' with a large text area; 'Program Schedule' with a placeholder text 'Click an available task from the right to add it here.'; 'Send Email' with fields for 'Task' (set to 'Welcome Email'), 'Send Date' (with a calendar icon), and 'Template' (with a search bar 'Type to search for email templates'); 'Recipients' with a checkbox for 'Everyone' and search bars for 'Search recipient targets' and 'Select recipient tags'; and 'Email Reports' with an 'Add' button and a description. At the bottom, there are 'Cancel' and 'Create Program' buttons. The 'Done editing task' button, located below the 'Recipients' section, is highlighted with a red rounded rectangle.

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**

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

The screenshot displays a web form for creating a security awareness training program. The form is organized into several sections:

- Program Name:** A text input field containing "Annual Security Training".
- Description:** A large text area for providing details about the program.
- Program Schedule:** A section with a placeholder text: "Click an available task from the right to add it here."
- Send Email:** A section for configuring email notifications, including:
 - Task:** A dropdown menu currently set to "Welcome Email".
 - Send Date:** A date picker field.
 - Template:** A search bar with the placeholder "Type to search for email templates" and a search icon.
 - Recipients:** A checkbox labeled "Everyone" and two input fields for "Search recipient targets" and "Select recipient tags".
- Email Reports:** A section with an "Add" button and text: "(Optional) When a campaign closes, you can send its report to an email address provided here."

At the bottom of the form, there are two buttons: "Cancel" and "Create Program". The "Create Program" button is highlighted with a red circle, indicating it is the next step in the process.

The Welcome Email is now listed in the Programs panel.

Chapter 4: Working With Programs and Campaign Scheduling

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

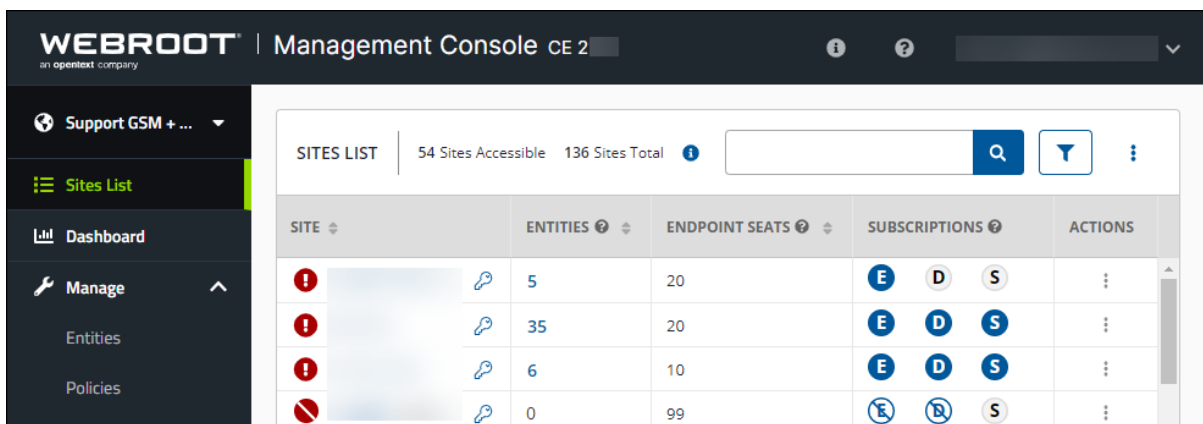
Scheduling Phishing Campaigns

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.

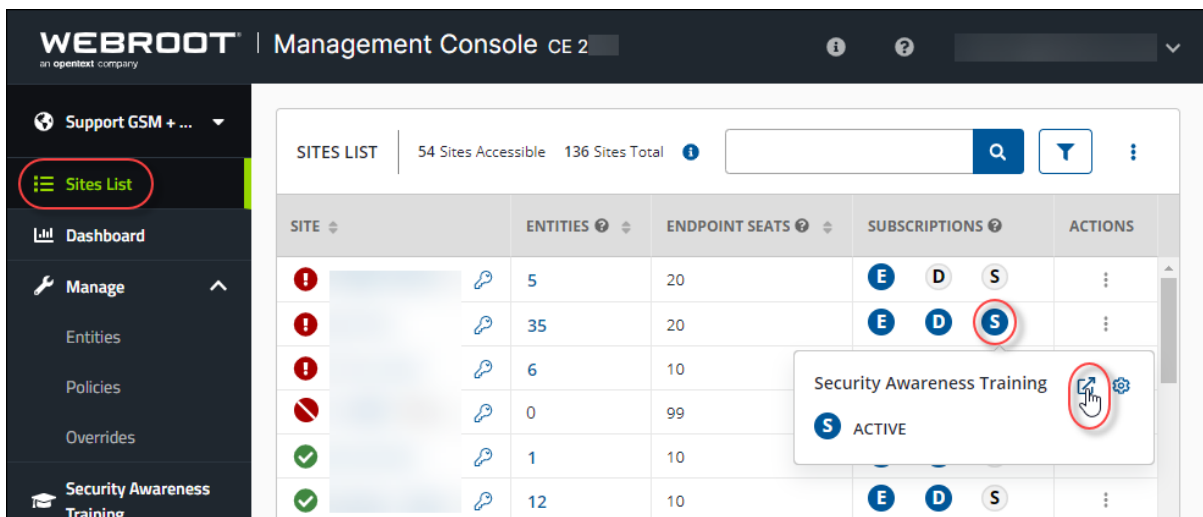
To schedule a phishing campaign:

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

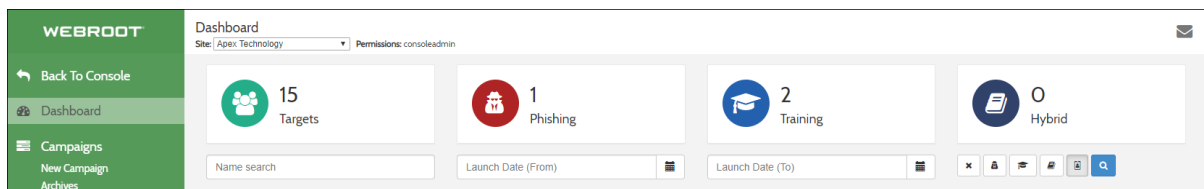
The Management Console displays.



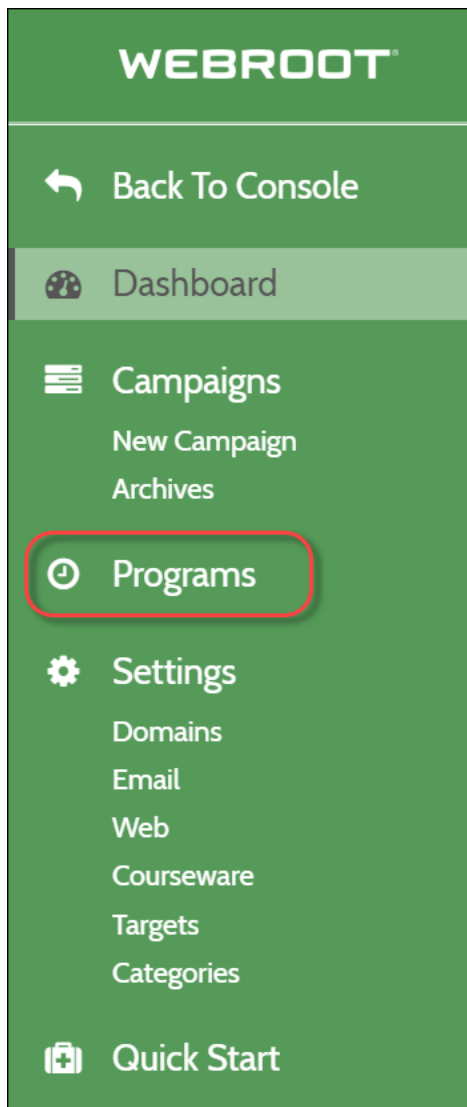
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



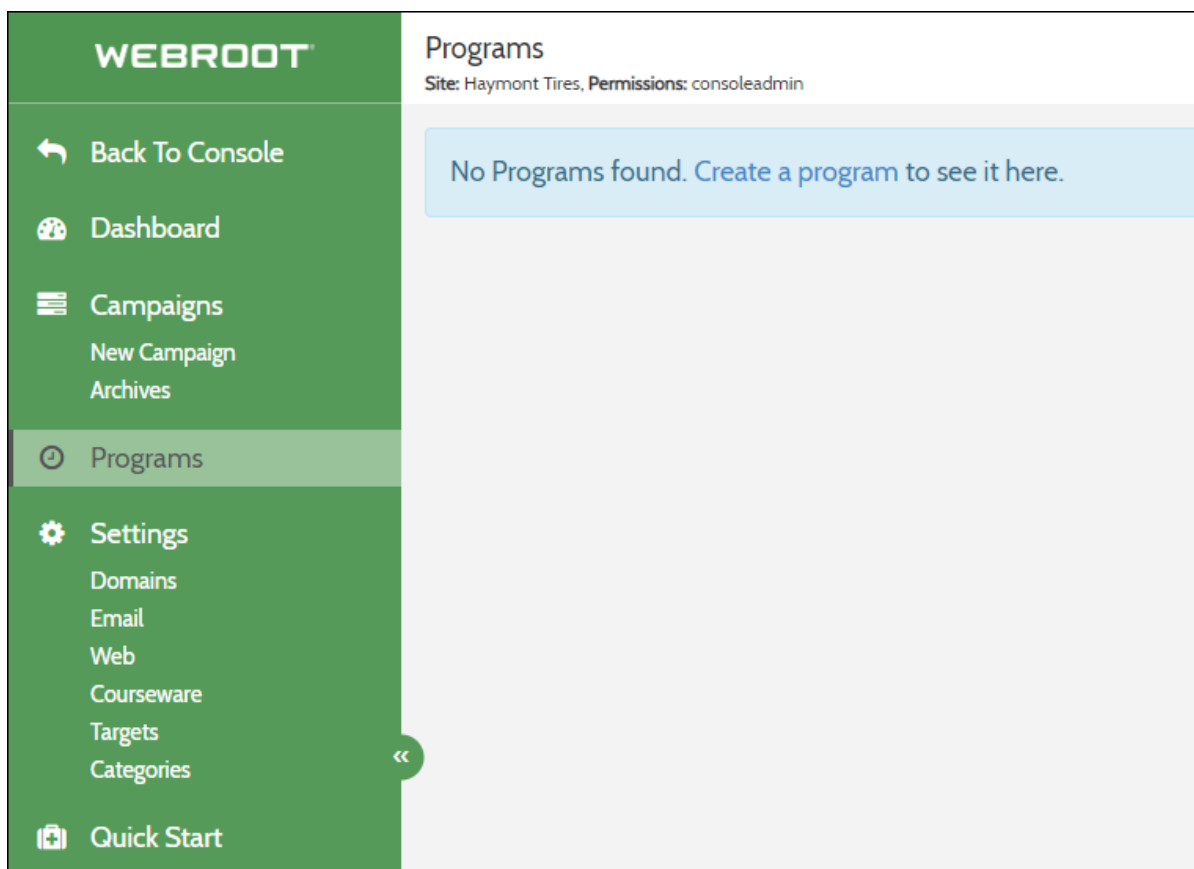
The Security Awareness Training dashboard displays.



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

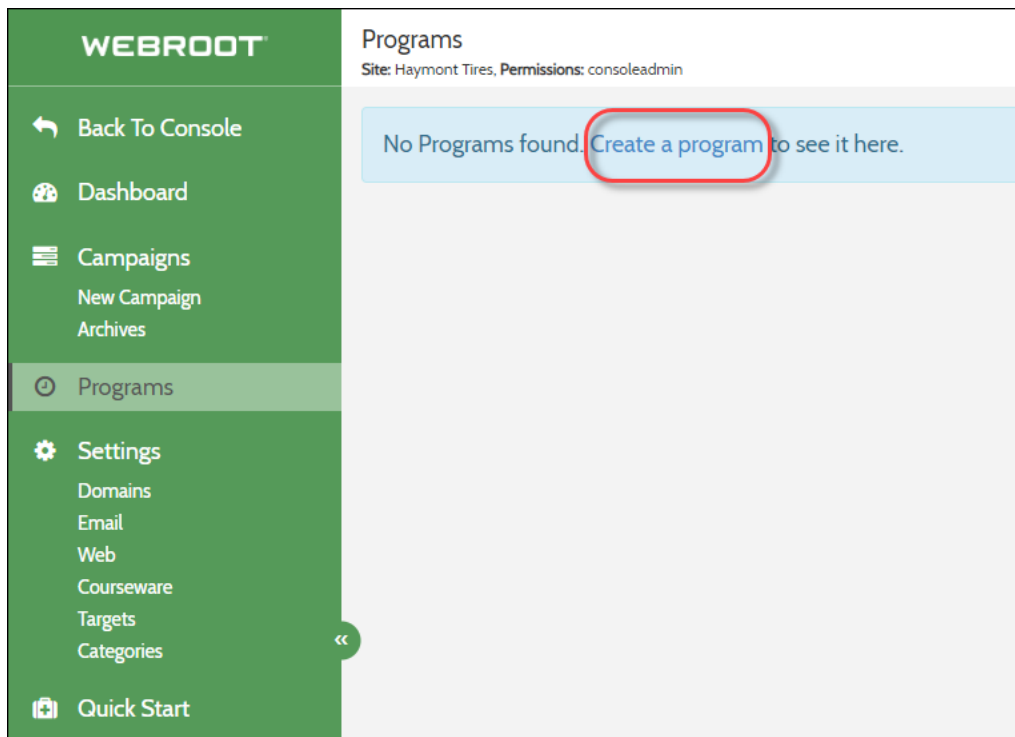


The Programs panel displays.

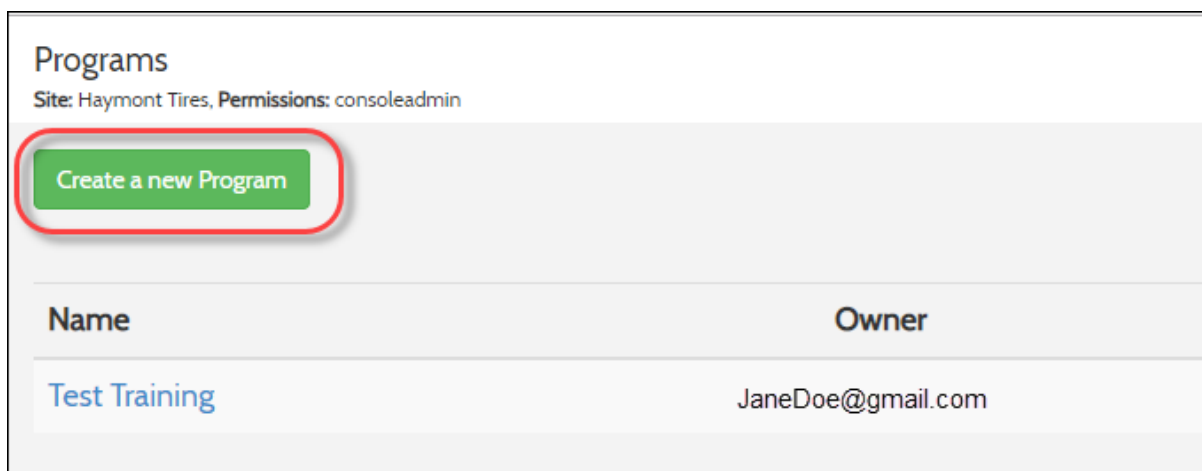


4. Do one of the following:

- 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.

New Program
Site: Apex Technology, Permissions: consoleadmin

Program Name
Annual Security Training

Description

Program Schedule
Click an available task from the right to add it here.

Available Tasks
Welcome Email
Phishing Campaign
Training Campaign

Email Reports
Add (Optional) When a campaign closes, you can send its report to an email address provided here.
Cancel Create Program

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

New Program
Site: Apex Technology, Permissions: consoleadmin

Program Name
Annual Security Training

Description

Program Schedule
Click an available task from the right to add it here.

Available Tasks
Welcome Email
Phishing Campaign
Training Campaign

Email Reports
Add (Optional) When a campaign closes, you can send its report to an email address provided here.
Cancel Create Program

The edit area displays.

Chapter 4: Working With Programs and Campaign Scheduling

New Program
Site: Haymont Tires, Permissions: consoleadmin

Program Name
Annual Security Training

Description

Program Schedule
Click an available task from the right to add it here.

Phishing Campaign
Task
Phishing Campaign
Campaign
Type to search for campaigns
Start Date
End Date
Recipients
☐ Everyone
Search recipient targets
Select recipient tags
☐ Send a report after this campaign closes
Provide an email address below.
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

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.

New Program
Site: Haymont Tires, Permissions: consoleadmin

Program Name
Annual Security Training

Description

Program Schedule
Click an available task from the right to add it here.

Phishing Campaign

Task
Phishing Campaign

Campaign
Type to search for campaigns

Start Date

End Date

Recipients

March 2019

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
9	24	25	26	27	28	01	02
10	03	04	05	06	07	08	09
11	10	11	12	13	14	15	16
12	17	18	19	20	21	22	23
13	24	25	26	27	28	29	30
14	31	01	02	03	04	05	06

Today Clear Close

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.

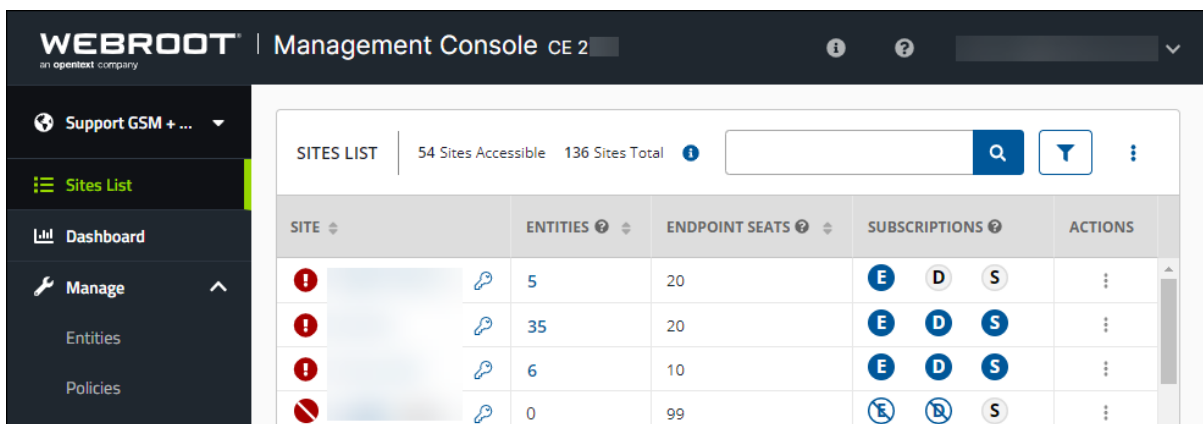
Creating Training Campaigns

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.

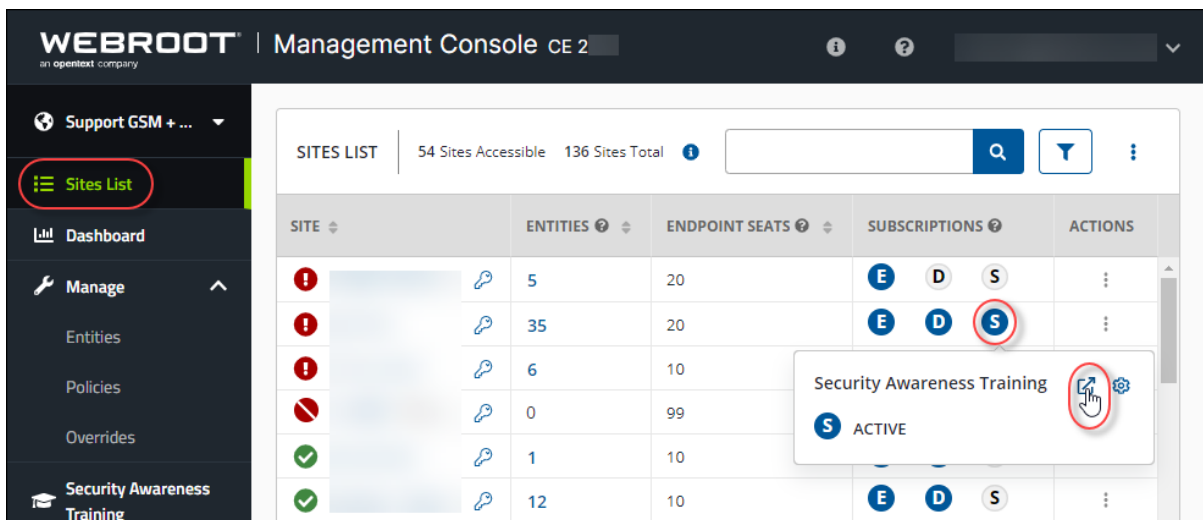
To create a training campaign:

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

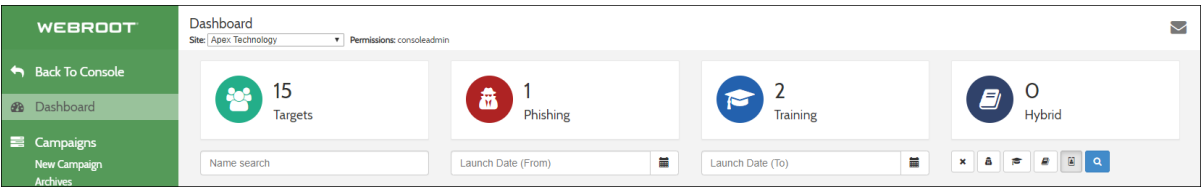
The Management Console displays.



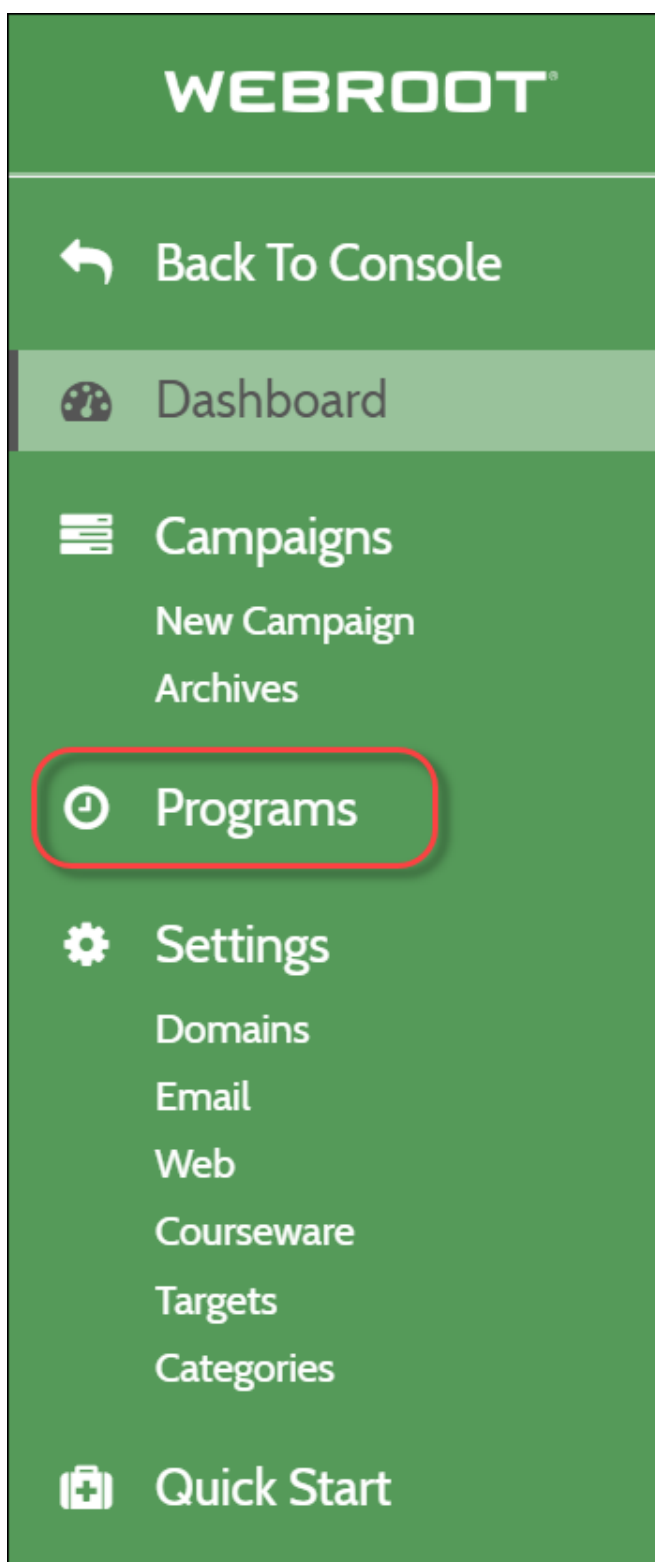
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



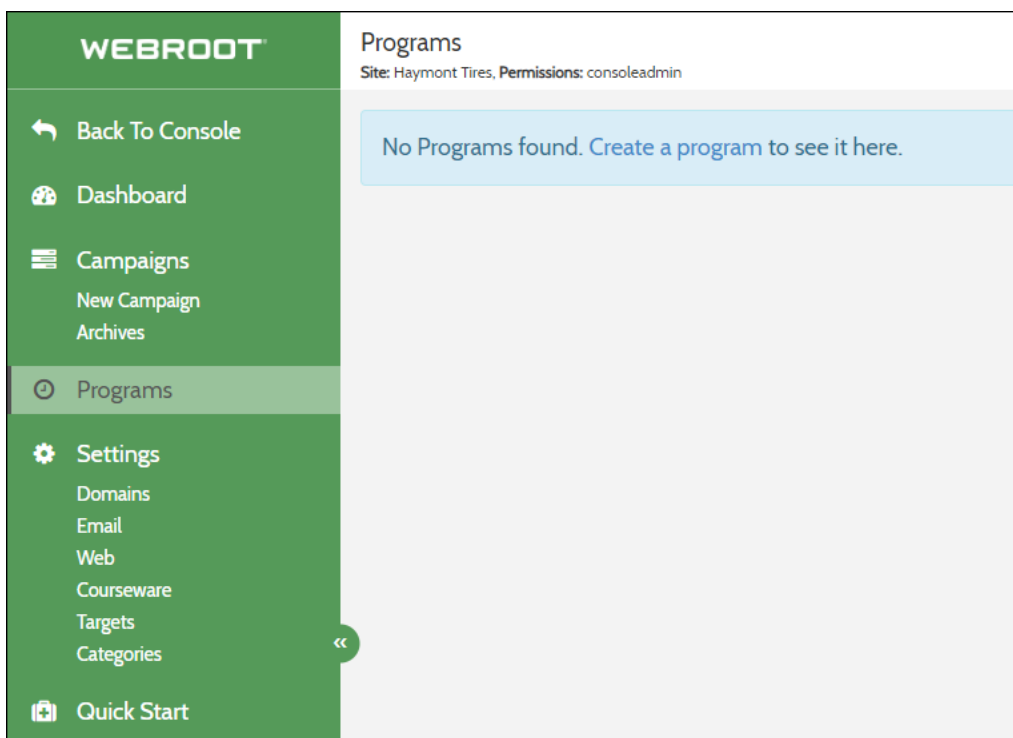
The Security Awareness Training dashboard displays.



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



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:

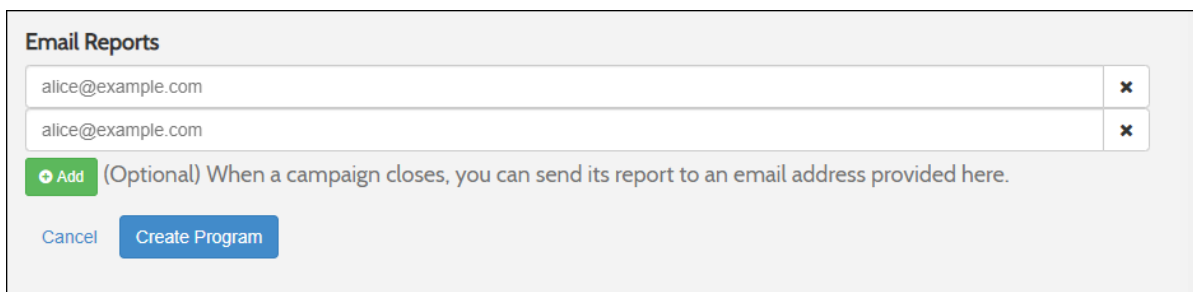
- Name of campaign
- Date of campaign
- Key statistics, along with a summary of the campaign templates used

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.



Email Reports

alice@example.com	✕
alice@example.com	✕

Add (Optional) When a campaign closes, you can send its report to an email address provided here.

[Cancel](#) [Create Program](#)

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

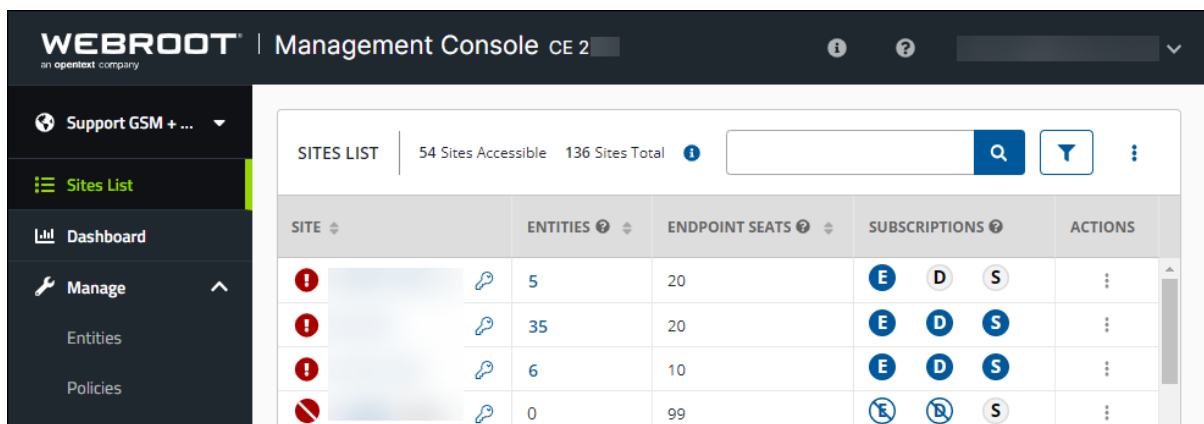
Accessing Delivery Reports

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](#).

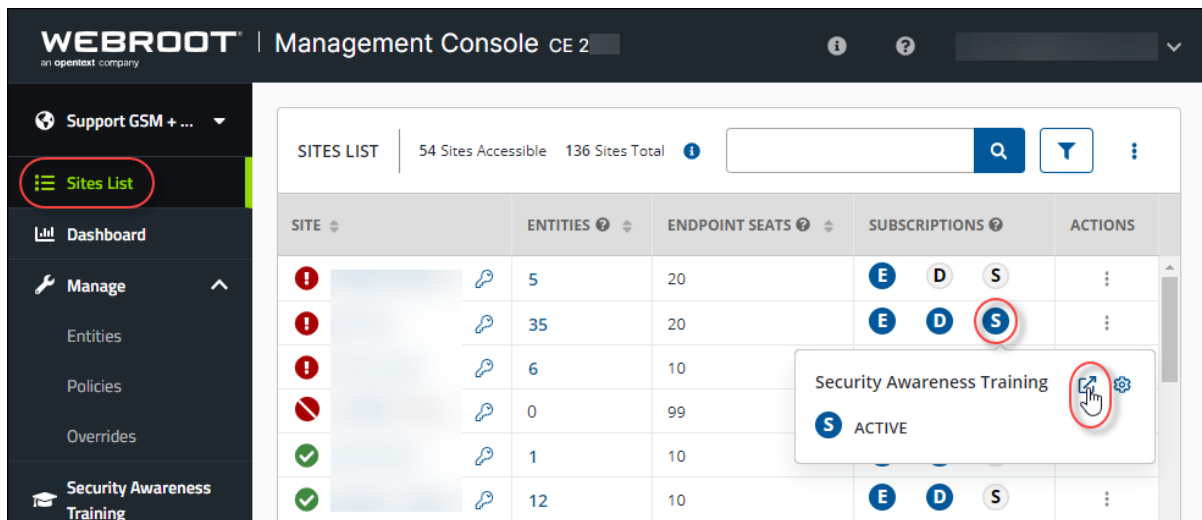
The Management Console displays.



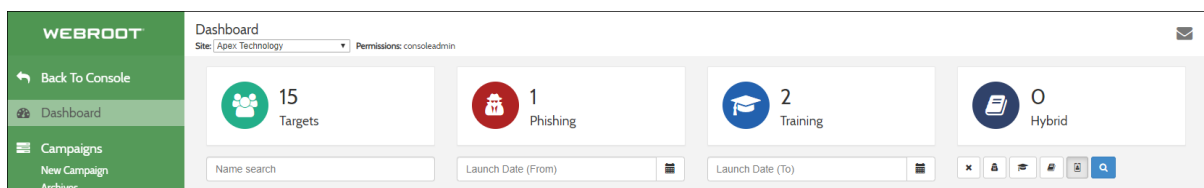
The screenshot shows the Webroot Management Console interface. The header includes the Webroot logo, 'an opentext company', and the title 'Management Console CE 2'. A sidebar on the left contains navigation links: 'Support GSM + ...', 'Sites List' (highlighted), 'Dashboard', 'Manage' (with a sub-menu for 'Entities' and 'Policies'), and 'Go to Security Awareness Training' (with a right arrow). The main content area displays a 'SITES LIST' table. Above the table, it shows '54 Sites Accessible' and '136 Sites Total'. The table has columns for 'SITE', 'ENTITIES', 'ENDPOINT SEATS', 'SUBSCRIPTIONS', and 'ACTIONS'. The 'SITE' column includes a status icon (red exclamation mark or red circle with slash) and a link icon. The 'ENTITIES' column shows counts (5, 35, 6, 0). The 'ENDPOINT SEATS' column shows counts (20, 20, 10, 99). The 'SUBSCRIPTIONS' column shows status icons (E, D, S) for each site. The 'ACTIONS' column shows a three-dot menu icon for each site.

SITE	ENTITIES	ENDPOINT SEATS	SUBSCRIPTIONS	ACTIONS
[Red Exclamation Mark] [Link]	5	20	[E] [D] [S]	[More]
[Red Exclamation Mark] [Link]	35	20	[E] [D] [S]	[More]
[Red Exclamation Mark] [Link]	6	10	[E] [D] [S]	[More]
[Red Circle with Slash] [Link]	0	99	[E] [D] [S]	[More]

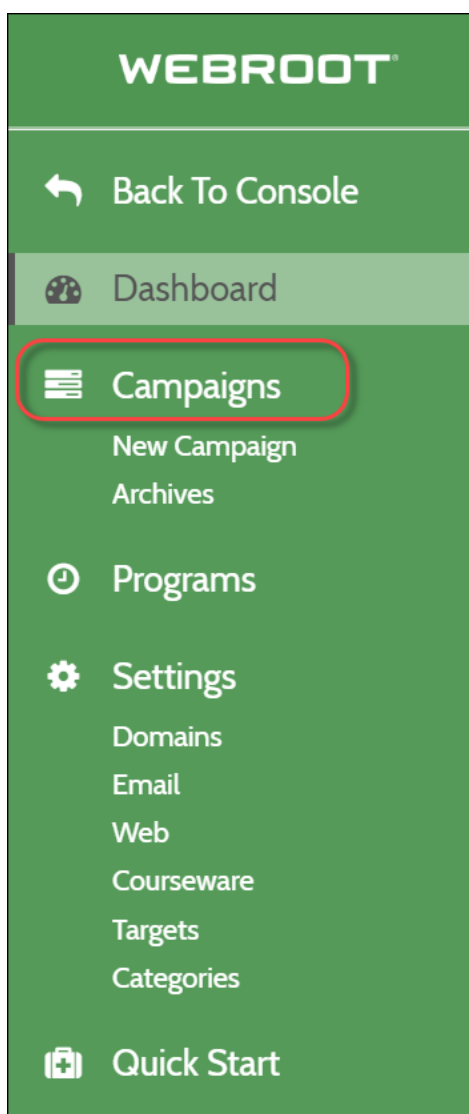
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



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.

Campaign List
Site: Haymont Tires, Permissions: consoleadmin

Name search Launch Date (From) Launch Date (To)

Showing 12 of 12 records found

Name	Status	Dates	Description	Ⓢ	📧	📧	📧	📧	📧	📧	📧	📧	📧
Test		Created: Thu Mar 14 2019		0	0	0	0	0	0	0	0	0	0
Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0
Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0
New Hire Test		Created: Thu Mar 14 2019	Testing New Hir...	0	0	0	0	0	0	0	0	0	0
Password Course...		Created: Fri Mar 01 2019		0	0	0	0	0	0	0	0	0	0
Test Sim Learn		Created: Wed Sep 26 2018	Test Sim Learn	0	0	0	0	0	0	0	0	0	0
the		Created: Fri Sep 21 2018	the	0	0	0	0	0	0	0	0	0	0
Test55		Created: Tue May 29 2018		0	0	0	0	0	0	0	0	0	0
test12		Created: Thu May 10 2018		0	0	0	0	0	0	0	0	0	0
training		Created: Fri May 04 2018		0	0	0	0	0	0	0	0	0	0
t		Launched: Fri Nov 03 2017	t	0	0	0	0	0	0	0	0	0	0
Test Simulation		Launched: Thu Nov 02 2017		3	1	2	3	0	1	0	0	0	0

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

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

Security Awareness Training Admin Guide

Campaign List

Site: Haymont Tires, Permissions: consoleadmin

Name search

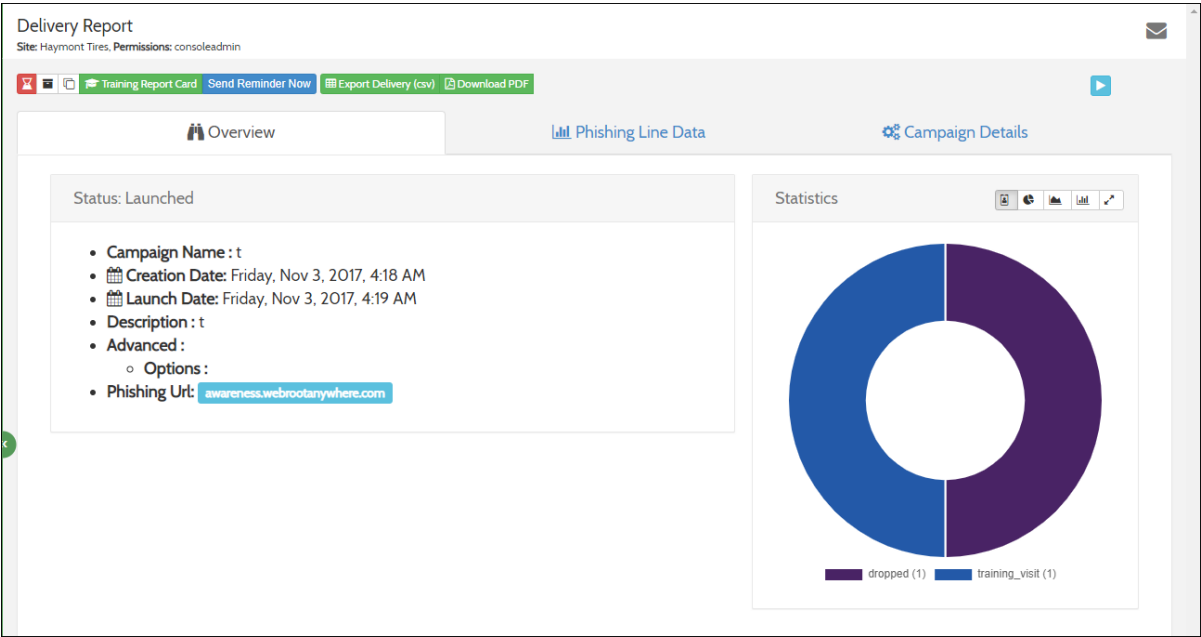
Launch Date (From)

Launch Date (To)

Showing 12 of 12 records found

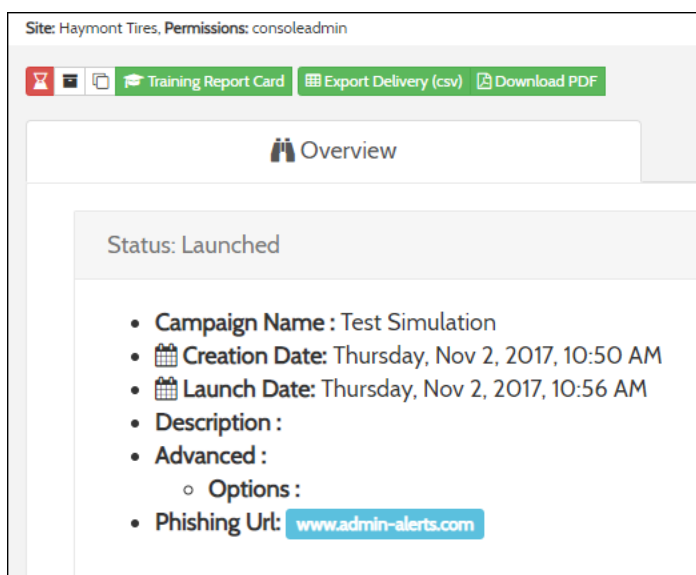
	Name	Status	Dates	Description										
	Test		Created: Thu Mar 14 2019		0	0	0	0	0	0	0	0	0	0
	Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0
	Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0
	New Hire Test		Created: Thu Mar 14 2019	Testing New Hir...	0	0	0	0	0	0	0	0	0	0
	Password Course...		Created: Fri Mar 01 2019		0	0	0	0	0	0	0	0	0	0
	Test Sim Learn		Created: Wed Sep 26 2018	Test Sim Learn	0	0	0	0	0	0	0	0	0	0
	the		Created: Fri Sep 21 2018	the	0	0	0	0	0	0	0	0	0	0
	Test55		Created: Tue May 29 2018		0	0	0	0	0	0	0	0	0	0
	test12		Created: Thu May 10 2018		0	0	0	0	0	0	0	0	0	0
	training		Created: Fri May 04 2018		0	0	0	0	0	0	0	0	0	0
	t		Launched: Fri Nov 03 2017	t	0	0	0	0	0	0	0	0	0	0
	Test Simulation		Launched: Thu Nov 02 2017		3	1	2	3	0	1	0	0	0	0

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



5. The Status area displays the following information:

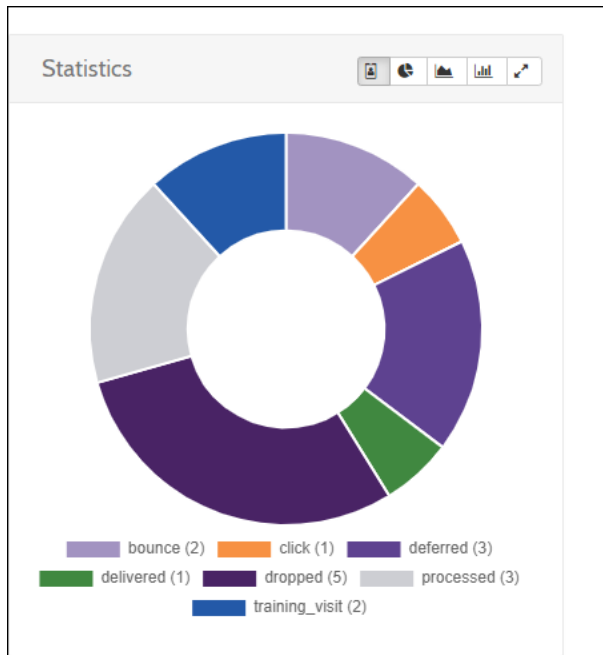
- Campaign Name
- Creation Date
- Launch Date
- Description
- Advanced/Options
- Phishing URL



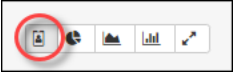
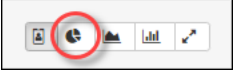
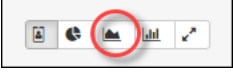
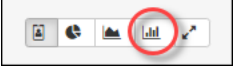
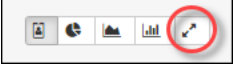
6. The Statistics area displays the following information in a graph format. Hover over the various sections of the graph to display specific information:

- **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.

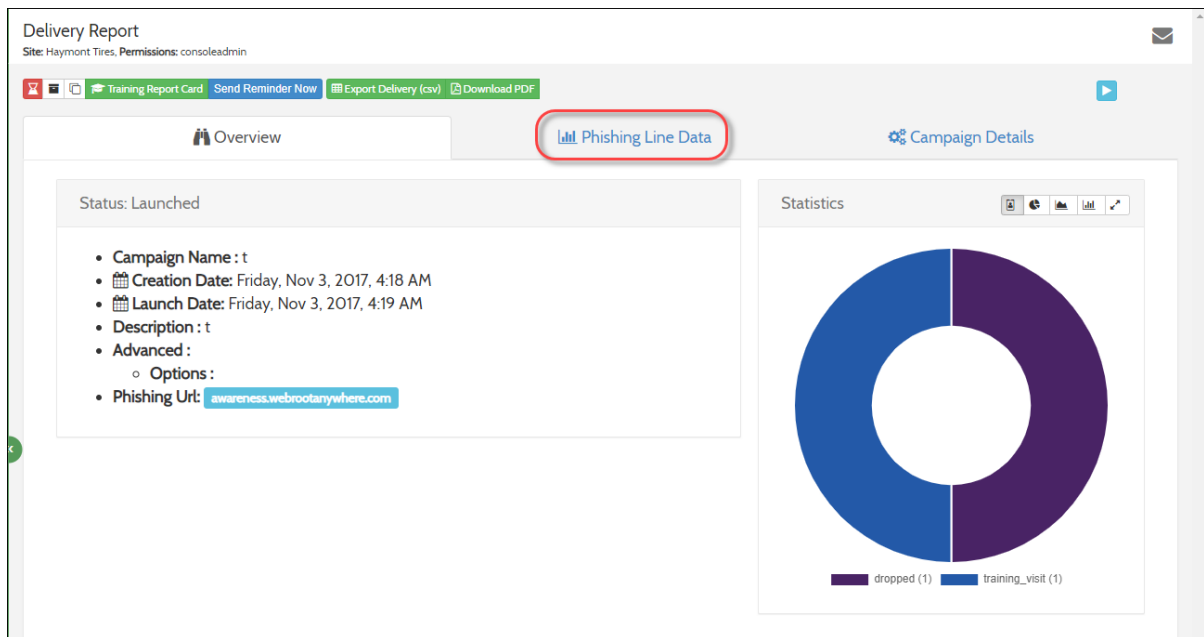
- The recipient email previously bounced.
- The recipient has marked your email as spam.
- **Bounces** — When an attempt is made to deliver an email, but the recipient mail server rejects it.
- **Spam Reports** — When a recipient marks your email as spam and their mail server tells us about it.



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.

Chapter 5: Working With Reports

Delivery Report
Site: Haymont Tires, Permissions: consoleadmin

Training Report Card Export Delivery (csv) Download PDF

Overview Phishing Line Data Campaign Details

Options Page Events Email Events

And Or Clear Refresh

☐ Lure visit ☐ Education visit ☐ Training visit
☐ Posted Data ☐ Training complete

☐ Sent/processed ☐ Delivered ☐ Open ☐ Click ☐ Dropped ☐ Deferred ☐ Bounce ☐ Spam report

String search Launch Date (From) Launch Date (To)

Target	Timestamp	Browser	OS	Device	Page	Action
demoaccount@securecast.com	Nov 2, 2017 10:57:08 AM	N/A	N/A	N/A	Email	Processed
demoaccount@securecast.com	Nov 2, 2017 10:57:08 AM	N/A	N/A	N/A	Email	Deferred
demoaccount@securecast.com	Nov 2, 2017 10:59:18 AM	N/A	N/A	N/A	Email	Delivered
demoaccount@securecast.com	Nov 2, 2017 11:25:45 AM	N/A	N/A	N/A	Email	Click
demoaccount@securecast.com	Nov 2, 2017 11:25:14 AM	Chrome v62.0.3202	Windows 10	Other	Education	Training_visit
test@testemail.com	Sep 26, 2018 2:40:51 AM	Chrome v69.0.3497	Windows	Other	Education	Training_visit
test@testemail.com	Sep 26, 2018 2:41:06 AM	Chrome v69.0.3497	Windows	Other	Education	Training_visit

Showing 16 of 18 records found. 25

<< First Page < Previous Page 1 Next Page > Last Page >>

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

Delivery Report
Site: Haymont Tires, Permissions: consoleadmin

Training Report Card Send Reminder Now Export Delivery (csv) Download PDF

Overview Phishing Line Data Campaign Details

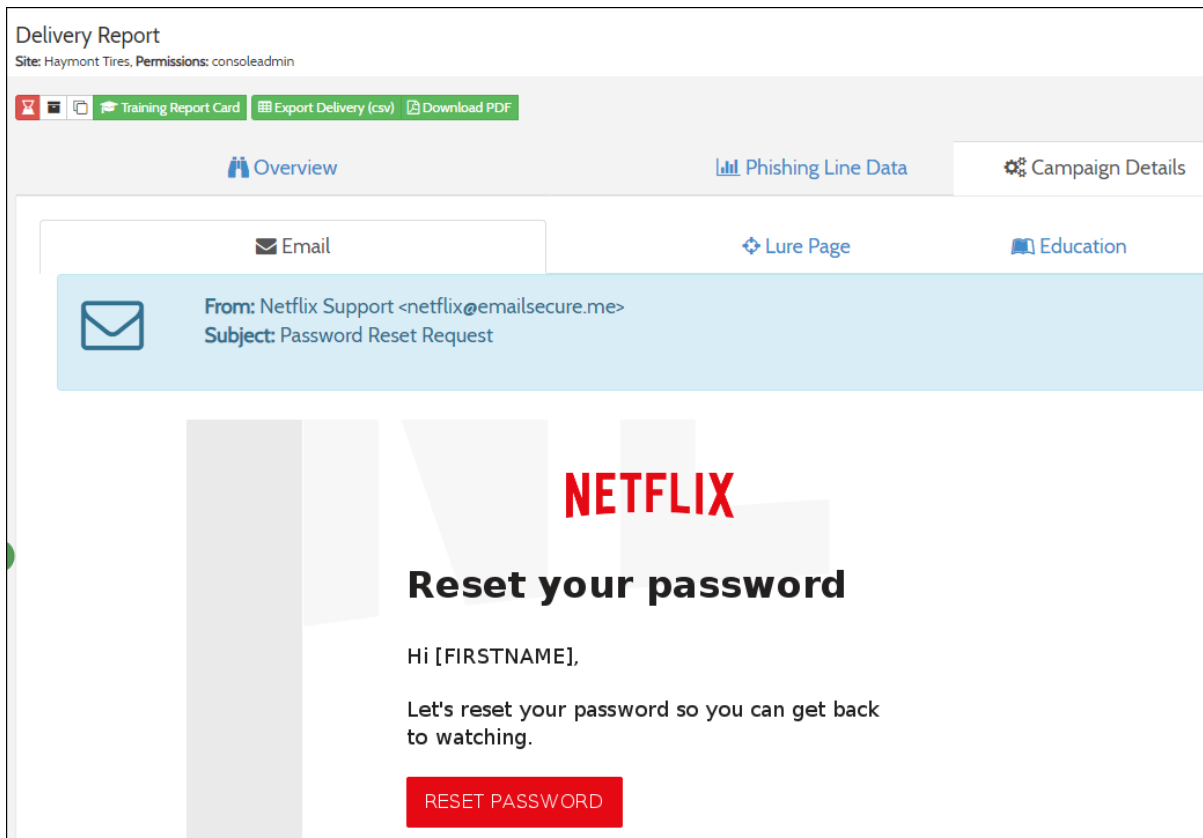
Status: Launched

- Campaign Name : t
- Creation Date: Friday, Nov 3, 2017, 4:18 AM
- Launch Date: Friday, Nov 3, 2017, 4:19 AM
- Description : t
- Advanced :
 - Options :
- Phishing Url: awareness.webrootanywhere.com

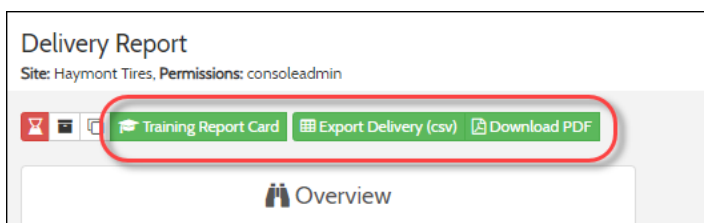
Statistics

dropped (1) training_visit (1)

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.



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.

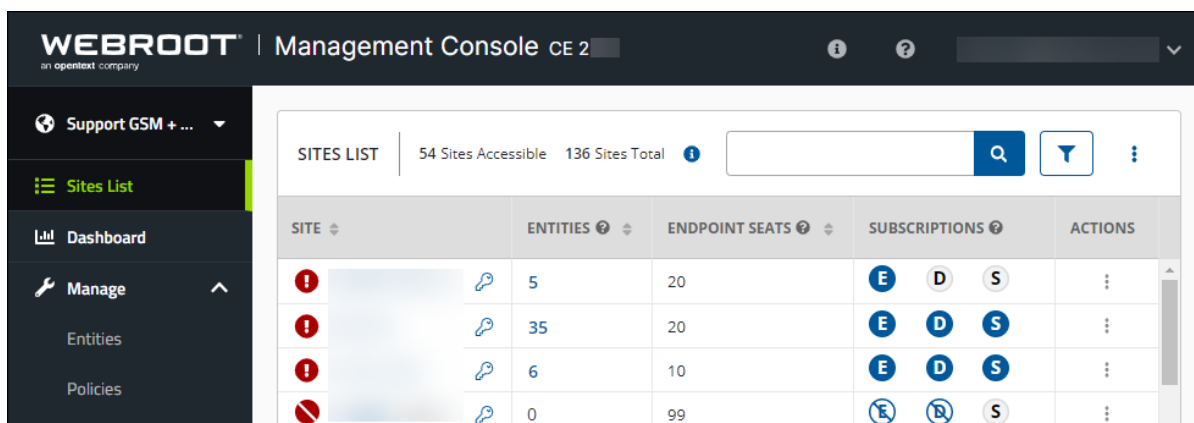
All actions and progress of a trainee user are tracked and logged in Webroot SAT reporting including user invite delivery, trainee user progress and completion. Reporting is available to both summarize training activity and provide detail on a per trainee user level.

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](#).

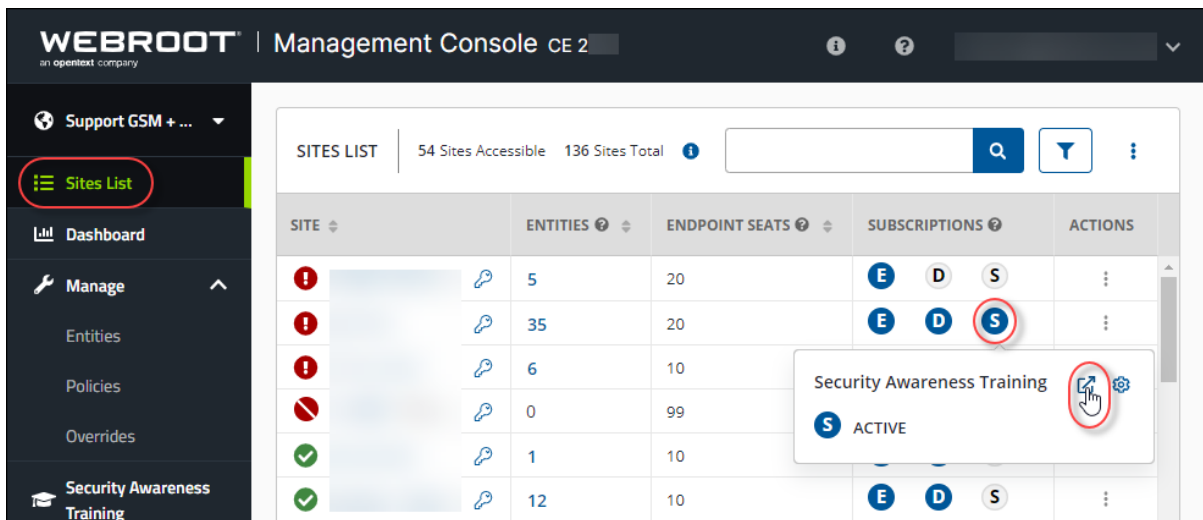
The Management Console displays.



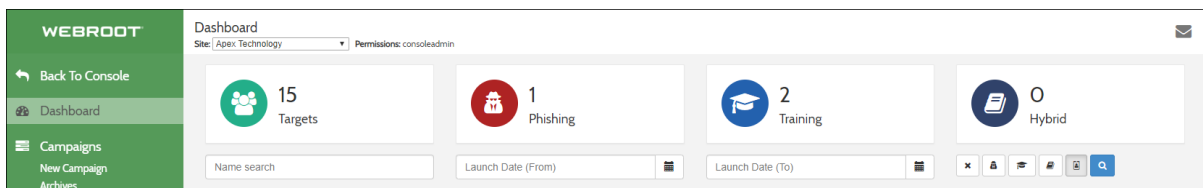
The screenshot shows the Webroot Management Console interface. The header includes the Webroot logo and 'Management Console CE 2'. The left sidebar has navigation options: Support GSM + ..., Sites List (highlighted), Dashboard, and Manage (with sub-options: Entities, Policies). The main content area displays a 'SITES LIST' table with 54 Sites Accessible and 136 Sites Total. The table has columns for SITE, ENTITIES, ENDPOINT SEATS, SUBSCRIPTIONS, and ACTIONS. The first four rows of data are visible, each with a status icon, a site name, and numerical values for entities, endpoint seats, and subscriptions.

SITE	ENTITIES	ENDPOINT SEATS	SUBSCRIPTIONS	ACTIONS
[Red exclamation mark icon]	5	20	E D S	...
[Red exclamation mark icon]	35	20	E D S	...
[Red exclamation mark icon]	6	10	E D S	...
[Red prohibition icon]	0	99	E D S	...

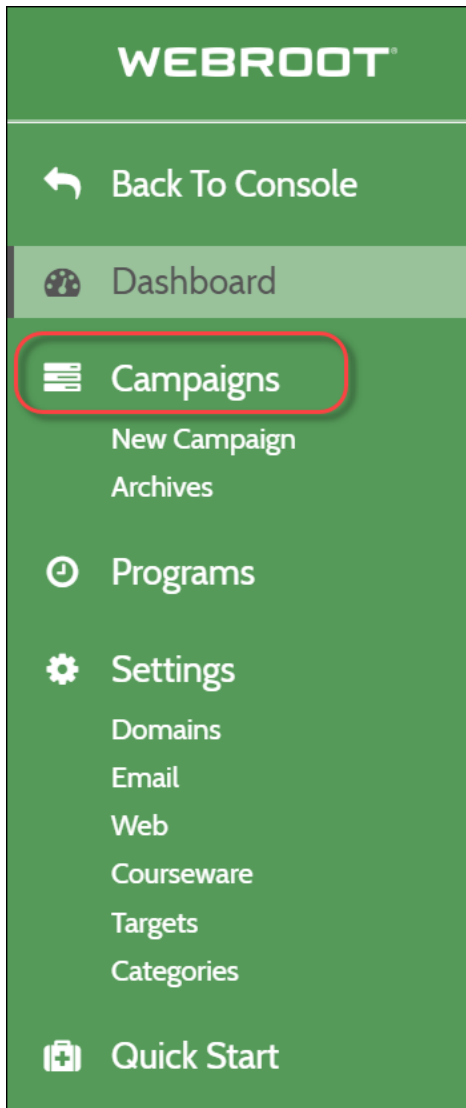
2. Select a Site from the **Sites List** and click the **Go to Security Awareness Training** icon.



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.

Campaign List
Site: Haymont Tires, Permissions: consoleadmin

Name search Launch Date (From) Launch Date (To)

Showing 12 of 12 records found

Name	Status	Dates	Description												
Test		Created: Thu Mar 14 2019		0	0	0	0	0	0	0	0	0	0	0	0
Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0	0	0
Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0	0	0
New Hire Test		Created: Thu Mar 14 2019	Testing New Hir...	0	0	0	0	0	0	0	0	0	0	0	0
Password Course...		Created: Fri Mar 01 2019		0	0	0	0	0	0	0	0	0	0	0	0
Test Sim Learn		Created: Wed Sep 26 2018	Test Sim Learn	0	0	0	0	0	0	0	0	0	0	0	0
the		Created: Fri Sep 21 2018	the	0	0	0	0	0	0	0	0	0	0	0	0
Test55		Created: Tue May 29 2018		0	0	0	0	0	0	0	0	0	0	0	0
test12		Created: Thu May 10 2018		0	0	0	0	0	0	0	0	0	0	0	0
training		Created: Fri May 04 2018		0	0	0	0	0	0	0	0	0	0	0	0
t		Launched: Fri Nov 03 2017	t	0	0	0	0	0	0	0	0	0	0	0	0
Test Simulation		Launched: Thu Nov 02 2017		3	1	2	3	0	1	0	0	0	0	0	0

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

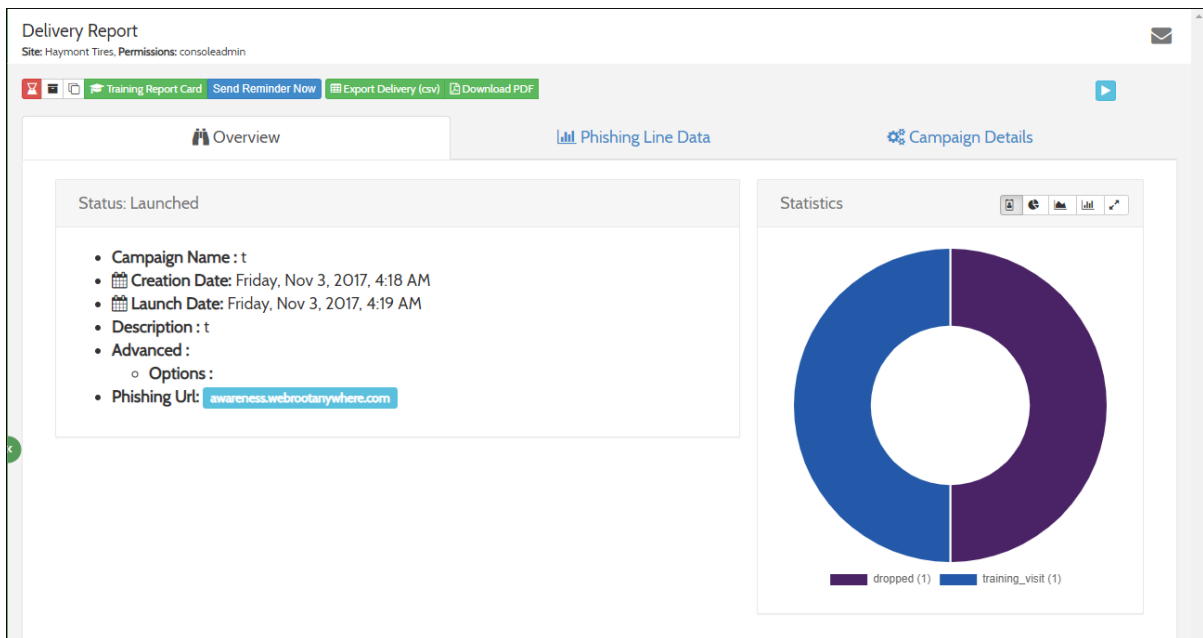
Campaign List
Site: Haymont Tires, Permissions: consoleadmin

Name search Launch Date (From) Launch Date (To)

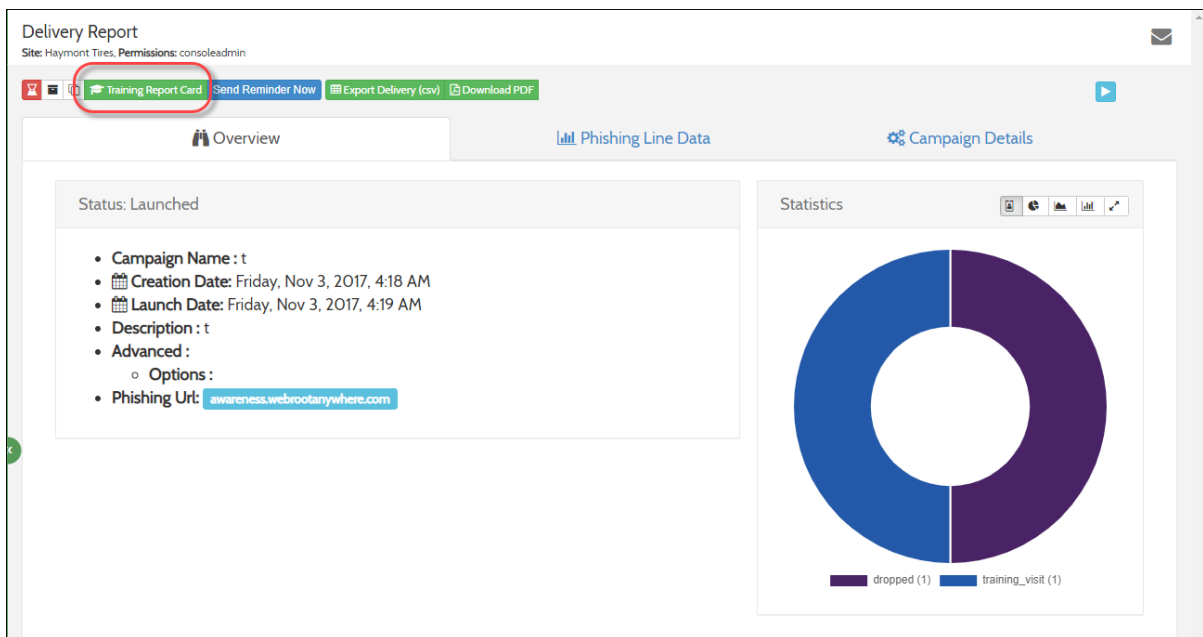
Showing 12 of 12 records found

Name	Status	Dates	Description												
Test		Created: Thu Mar 14 2019		0	0	0	0	0	0	0	0	0	0	0	0
Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0	0	0
Test		Created: Thu Mar 14 2019	Test	0	0	0	0	0	0	0	0	0	0	0	0
New Hire Test		Created: Thu Mar 14 2019	Testing New Hir...	0	0	0	0	0	0	0	0	0	0	0	0
Password Course...		Created: Fri Mar 01 2019		0	0	0	0	0	0	0	0	0	0	0	0
Test Sim Learn		Created: Wed Sep 26 2018	Test Sim Learn	0	0	0	0	0	0	0	0	0	0	0	0
the		Created: Fri Sep 21 2018	the	0	0	0	0	0	0	0	0	0	0	0	0
Test55		Created: Tue May 29 2018		0	0	0	0	0	0	0	0	0	0	0	0
test12		Created: Thu May 10 2018		0	0	0	0	0	0	0	0	0	0	0	0
training		Created: Fri May 04 2018		0	0	0	0	0	0	0	0	0	0	0	0
t		Launched: Fri Nov 03 2017	t	0	0	0	0	0	0	0	0	0	0	0	0
Test Simulation		Launched: Thu Nov 02 2017		3	1	2	3	0	1	0	0	0	0	0	0

The Delivery Report panel displays.



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



The Training Reports panel displays.

Training Reports
Site: Haymont Tires, Permissions: consoleadmin

[Delivery Report](#)
[Export Training \(csv\)](#)
[Export Student Completion \(csv\)](#)
[Export Delivery \(csv\)](#)
[Download PDF](#)

Training Session Report Card

Training session name: Test Simulation

Session description:

Training Module:

- Name:** Understanding Malware
- Description:** This course will help you understand malware. You will watch short videos about malware. Afterwards, you will be asked a few questions to test your new knowledge.

Student count: 3

Launch date: Thursday, November 2nd 2017, 10:56 am

End date:

Grades

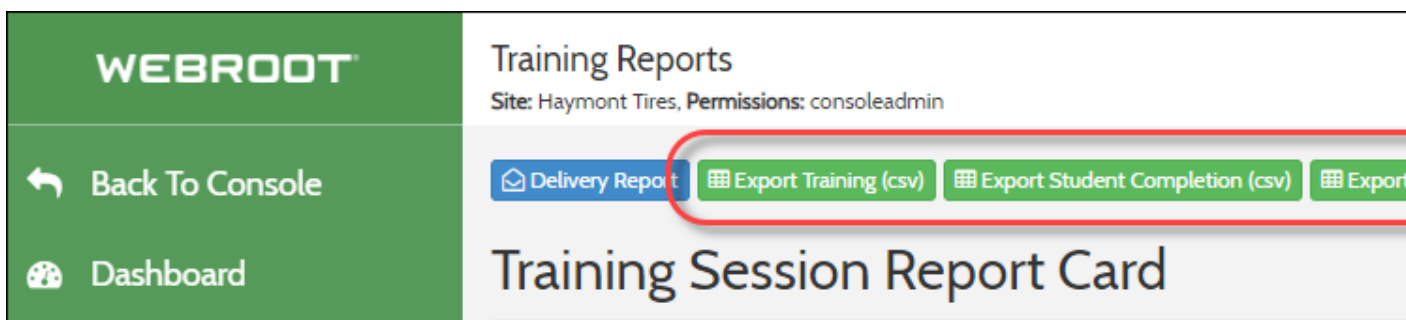
Metric	Count	Percent
Attempts	1	33.3% ✖
Completed	0	0 / 3 (0.0%) ✖
Incomplete	3	3 / 3 (100.0%) ✔

There are three sections available for your review.

SECTION	DESCRIPTION
Training Session Report Card	<p>Displays the following information:</p> <ul style="list-style-type: none">• Training session name• Session description• Training Module• Student count• Launch date• End date
Grades	<p>Displays the following information:</p> <ul style="list-style-type: none">• 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	<p>Displays the following information:</p> <ul style="list-style-type: none"> • 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)	<p>Total number of phishing campaigns a client launched. Phishing campaigns consist of:</p> <ul style="list-style-type: none"> • Simulated phishing lure to entice the user to open/click through to a lure page. For example, a phishing message could be the following: <i>Please log in to your bank verify your credentials.</i> • 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)	<p>Total number of training campaigns the client launched. A training campaign consists of:</p> <ul style="list-style-type: none"> • 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)	<p>Total number of emails bounced by the recipient email systems. Bounced messages are generally reported by one of the following:</p> <ul style="list-style-type: none"> • 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.

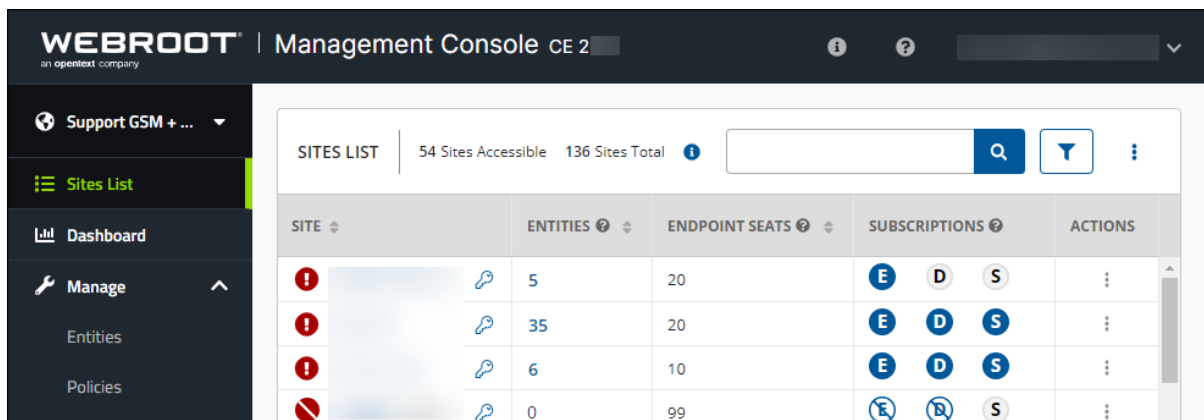
DATA	DESCRIPTION
Open (Emails)	Total number of users that clicked on email messages sent across all campaigns.
Lure_visit	Total number of visits by users to simulated phishing lure pages.
Post	Total number of attempts to post data to a simulated phishing lure page form (login creds, bank info, etc.).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

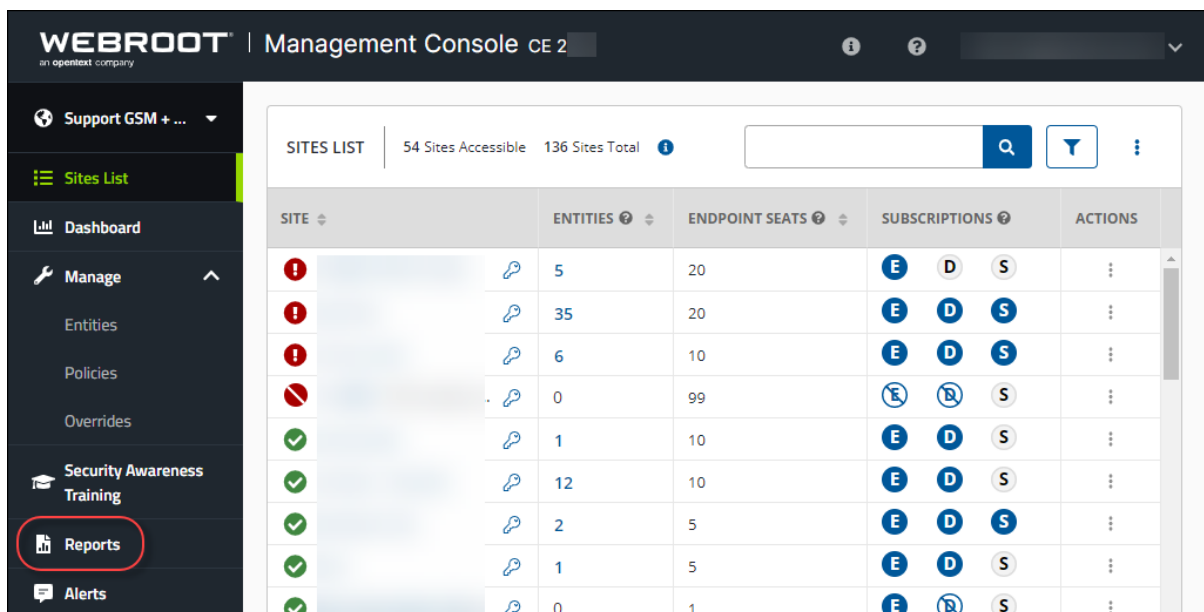
Follow this procedure to access Security Awareness Training reports.

To access a Security Awareness Training report:

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

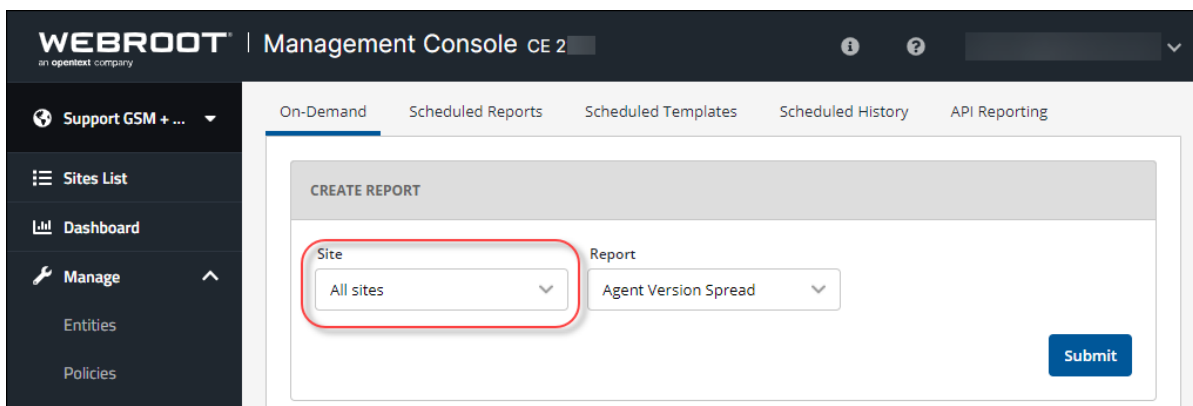


2. Click the **Reports** tab.



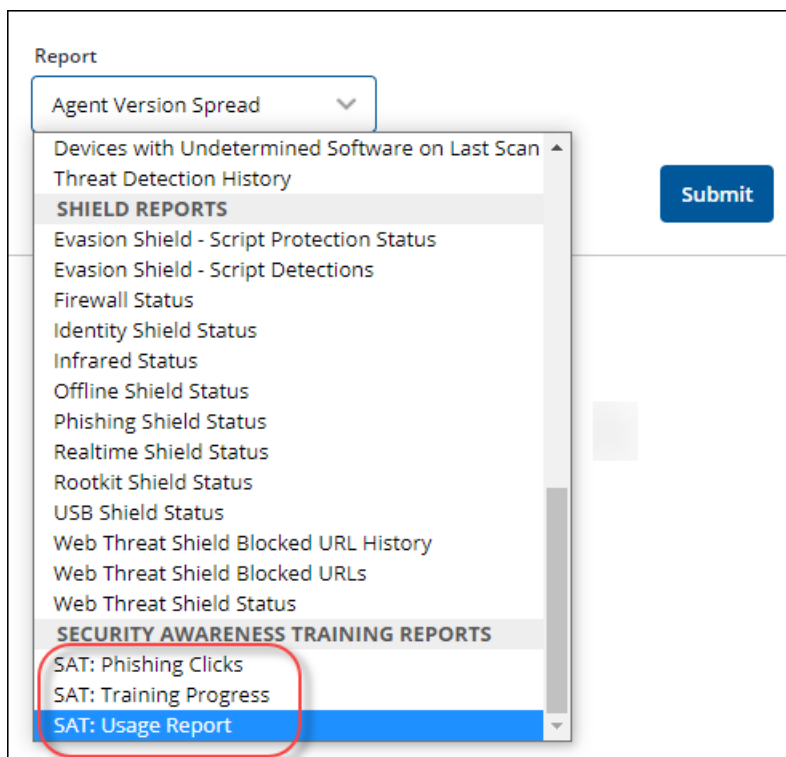
The Reports tab displays.

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

The screenshot shows the 'CREATE REPORT' interface. At the top, there are three dropdown menus: 'Site' (set to 'All sites'), 'Report' (set to 'SAT: Phishing Clicks'), and 'Period' (set to 'Last 7 Days'). The 'Period' dropdown is open, showing a list of options on the left and a calendar view on the right. The calendar view shows March 2021 and April 2021. The dates April 16, 17, 18, 19, 20, 21, and 22 are highlighted in blue, indicating the selected date range. At the bottom of the calendar view, there are 'Cancel' and 'Apply' buttons, and the text 'April 16, 2021 - April 22, 2021'.

MARCH 2021							APRIL 2021						
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun
22	23	24	25	26	27	28	29	30	31	1	2	3	4
1	2	3	4	5	6	7	5	6	7	8	9	10	11
8	9	10	11	12	13	14	12	13	14	15	16	17	18
15	16	17	18	19	20	21	19	20	21	22	23	24	25
22	23	24	25	26	27	28	26	27	28	29	30	1	2
29	30	31	1	2	3	4	3	4	5	6	7	8	9

Cancel April 16, 2021 - April 22, 2021 Apply

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.

CREATE REPORT

Site: All sites | Report: SAT: Phishing Clicks | Period: Last 7 Days

☒ Last 7 days
☐ Last 30 days
☐ Last 60 days
☐ Last 90 Days
☐ This Month
☐ Last Month
☐ Custom range

MARCH 2021							APRIL 2021						
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Sun
22	23	24	25	26	27	28	29	30	31	1	2	3	4
1	2	3	4	5	6	7	5	6	7	8	9	10	11
8	9	10	11	12	13	14	12	13	14	15	16	17	18
15	16	17	18	19	20	21	19	20	21	22	23	24	25
22	23	24	25	26	27	28	26	27	28	29	30	1	2
29	30	31	1	2	3	4	3	4	5	6	7	8	9

Cancel
 April 16, 2021 - April 22, 2021

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

CREATE REPORT

Site: All sites | Report: SAT: Phishing Clicks | Period: Last 7 Days

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

REPORT NAME	COLUMNS
SAT: Phishing Clicks Report	<ul style="list-style-type: none">• Site• Target Email• Phishing Campaigns• Email Clicks• Lure Clicks
SAT: Training Progress Report	<ul style="list-style-type: none">• Site• Target Email• Training Campaigns• Training Progress
SAT: Usage Report	<ul style="list-style-type: none">• 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.

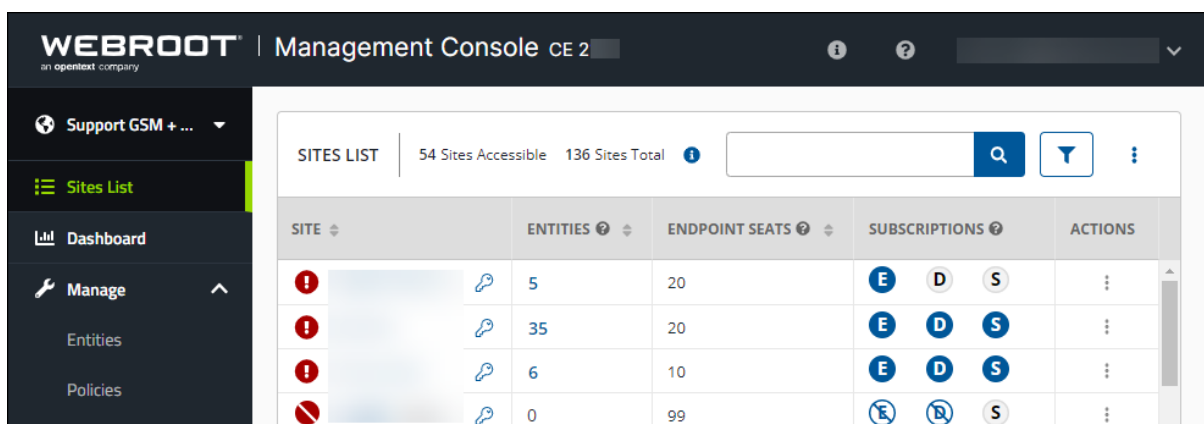
The report provides ideal documentation to help admins determine and demonstrate real world risks so they can advise clients' executive management on services and tactics accordingly to avoid future security incidents.

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.



The screenshot shows the Webroot Management Console interface. The top header includes the Webroot logo and the text 'Management Console CE 2'. A left sidebar contains navigation links: 'Support GSM + ...', 'Sites List' (highlighted), 'Dashboard', and 'Manage' (with sub-links for 'Entities' and 'Policies'). The main content area displays a 'SITES LIST' table with the following data:

SITES LIST		54 Sites Accessible	136 Sites Total			
SITE	ENTITIES	ENDPOINT SEATS	SUBSCRIPTIONS	ACTIONS		
[Red exclamation mark icon]	[Link icon] 5	20	[E] [D] [S]	[More actions icon]		
[Red exclamation mark icon]	[Link icon] 35	20	[E] [D] [S]	[More actions icon]		
[Red exclamation mark icon]	[Link icon] 6	10	[E] [D] [S]	[More actions icon]		
[Red circle with slash icon]	[Link icon] 0	99	[E] [D] [S]	[More actions icon]		

Security Awareness Training Admin Guide

2. Click the **Settings** icon.

The screenshot shows the Webroot Management Console interface. On the left is a sidebar with navigation options: Support GSM + ..., Sites List (highlighted with a red circle), Dashboard, Manage (with a sub-menu: Entities, Policies, Overrides), and Security Awareness Training. The main area displays a 'SITES LIST' table with columns: SITE, ENTITIES, ENDPOINT SEATS, SUBSCRIPTIONS, and ACTIONS. The table contains six rows of data. In the third row, the 'SUBSCRIPTIONS' column shows icons for E, D, and S, with the 'S' icon circled in red. A tooltip for 'Security Awareness Training' is visible, showing an 'S ACTIVE' status and a settings icon circled in red.

SITE	ENTITIES	ENDPOINT SEATS	SUBSCRIPTIONS	ACTIONS
[Redacted]	5	20	E D S	⋮
[Redacted]	35	20	E D S	⋮
[Redacted]	6	10	E D S	⋮
[Redacted]	0	99		⋮
[Redacted]	1	10		⋮
[Redacted]	12	10		⋮

The Security Awareness Training tab displays.

The screenshot shows the 'Security Awareness Training' settings page in the Webroot Management Console. The left sidebar is the same as the previous screenshot. The main area has tabs for Summary, Details, Admin Permissions, Endpoint Protection, DNS Protection, and Security Awareness Training (selected). The 'Security Awareness Training' tab is active, showing a toggle switch for 'Security Awareness Training' which is turned on. Below this, it shows 'Subscription Status: Active' and 'Target Users: 1'. There are sections for 'ACTIVE DIRECTORY INTEGRATION' with a 'Configure Azure AD Integration' button, and 'DOMAIN VERIFICATION' with instructions and a list of options. At the bottom, there is a 'Send Verification Request' button and a 'Manual User' section. A 'SAT Quick Setup' sidebar on the right provides a guide for setting up training.

Site: [Dropdown: Site]

Summary Details Admin Permissions Endpoint Protection DNS Protection **Security Awareness Training**

☒ Security Awareness Training

Subscription Status: Active

Target Users: 1

ACTIVE DIRECTORY INTEGRATION

Integrate Webroot Security Awareness Training with Azure Active Directory.

[Configure Azure AD Integration](#)

DOMAIN VERIFICATION

Use one of the following options to verify access to the domains you will be managing for Security Awareness Training.

- Domain Member - Launch Campaigns
- Domain Admin - Launch Campaigns; View Breach Report

Add New Domain: [Send Verification Request](#)

[Back](#) [Save](#)

SAT Quick Setup

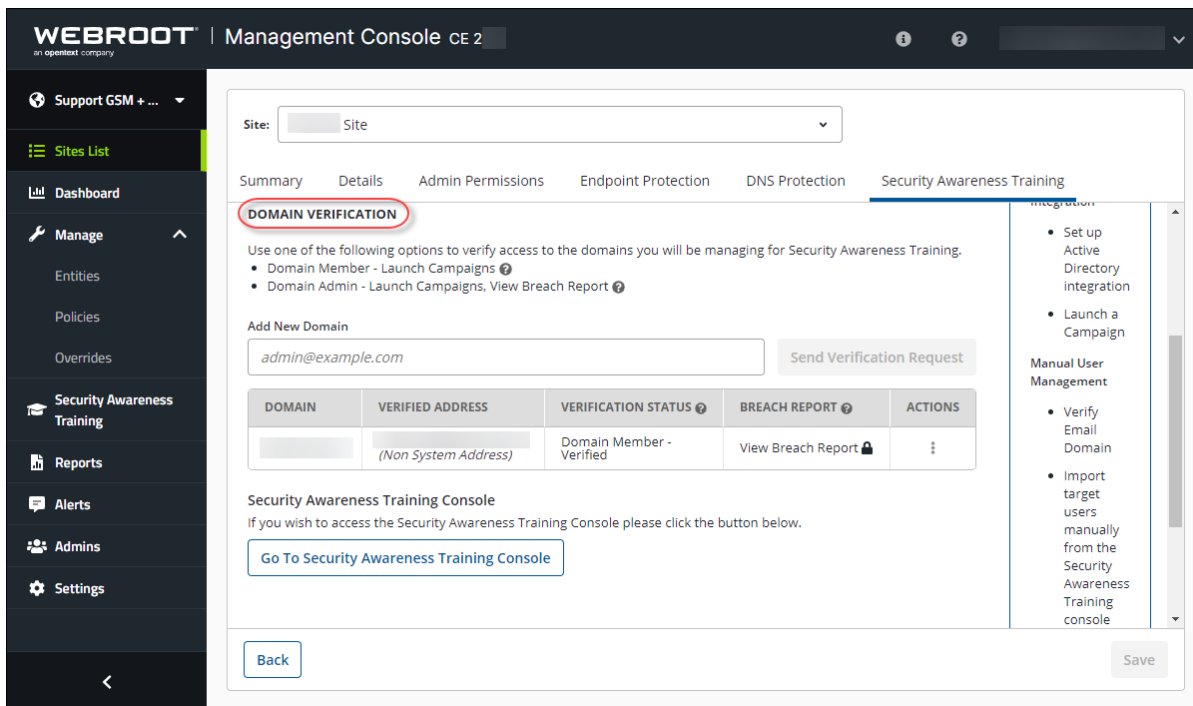
Set up Security Awareness Training using either of the options outlined below:

Active Directory Integration

- Set up Active Directory integration
- Launch a Campaign

Manual User

3. Scroll down to the Domain Verification area.

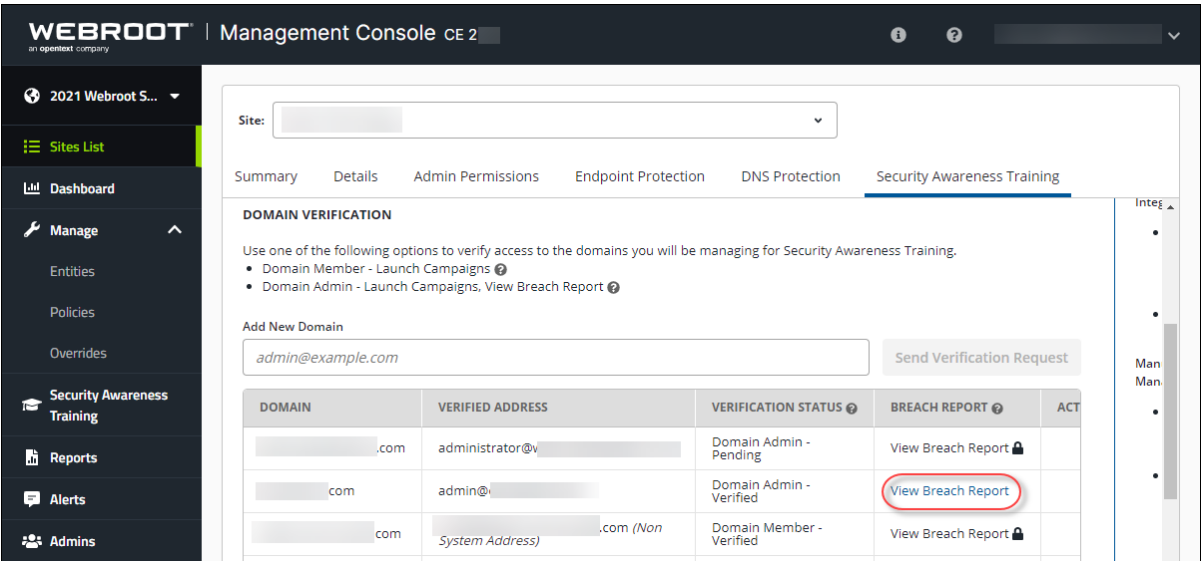


4. In the Add New Domain field, add one of the following two email types to verify access to domains you will be managing:

- **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.

BREACH REPORT: .COM		Search for...	Q
	EMAIL	BREACH	
>	dan@.com	1 Breach	
>	david@.com	3 Breaches	
>	shane@.com	1 Breach	

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

BREACH REPORT: .COM		Search for...	Q
	EMAIL	BREACH	
>	dan@.com	1 Breach	
>	david@.com	3 Breaches	
>	shane@.com	1 Breach	

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

<<

<

1


>

>>

Close


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

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

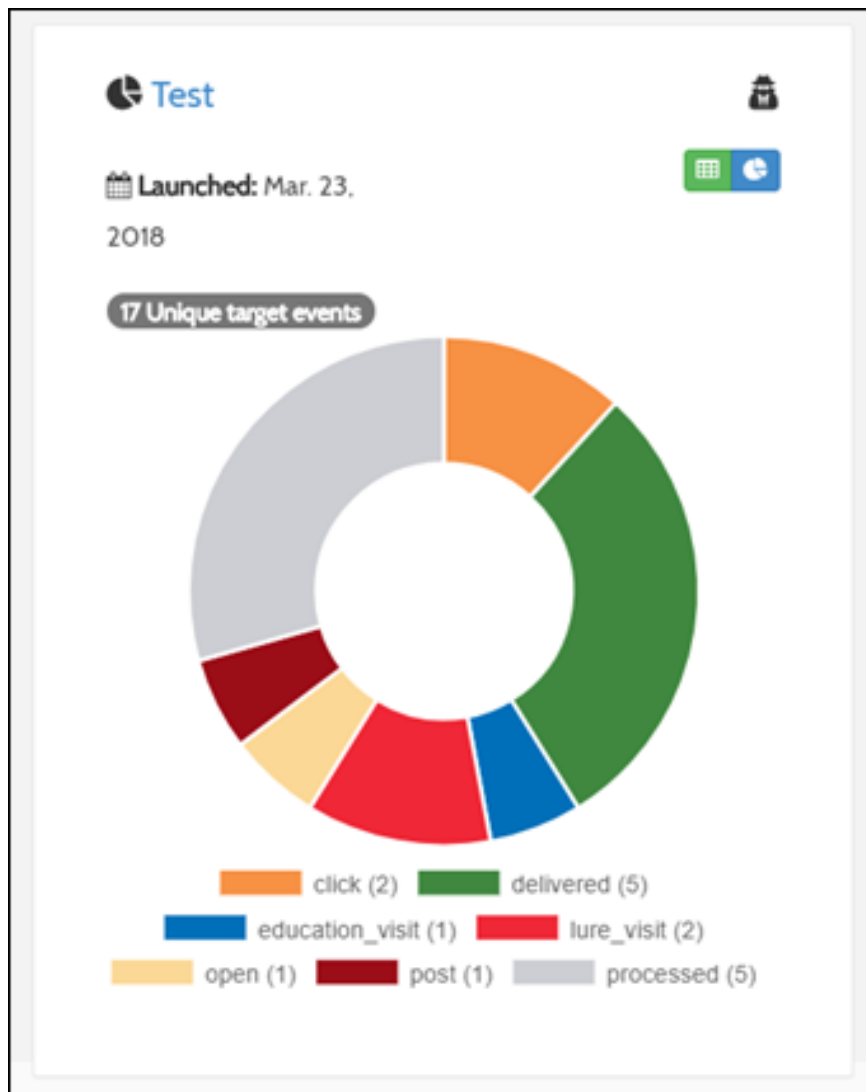
Rows 20    1  

Close

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.

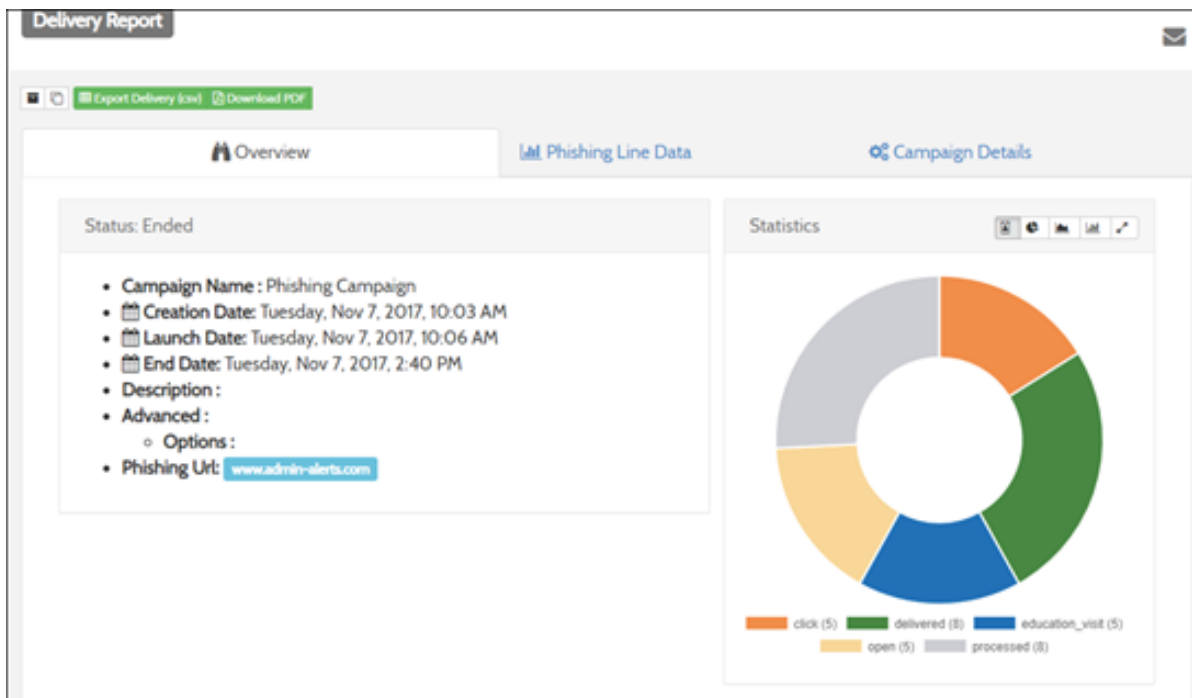
Sample Phishing Report Campaign Summary



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.

Delivery Report

Export Delivery (csv) Download PDF

Overview Phishing Line Data Campaign Details

Options

Page Events

Email Events

String search

Launch Date (From)

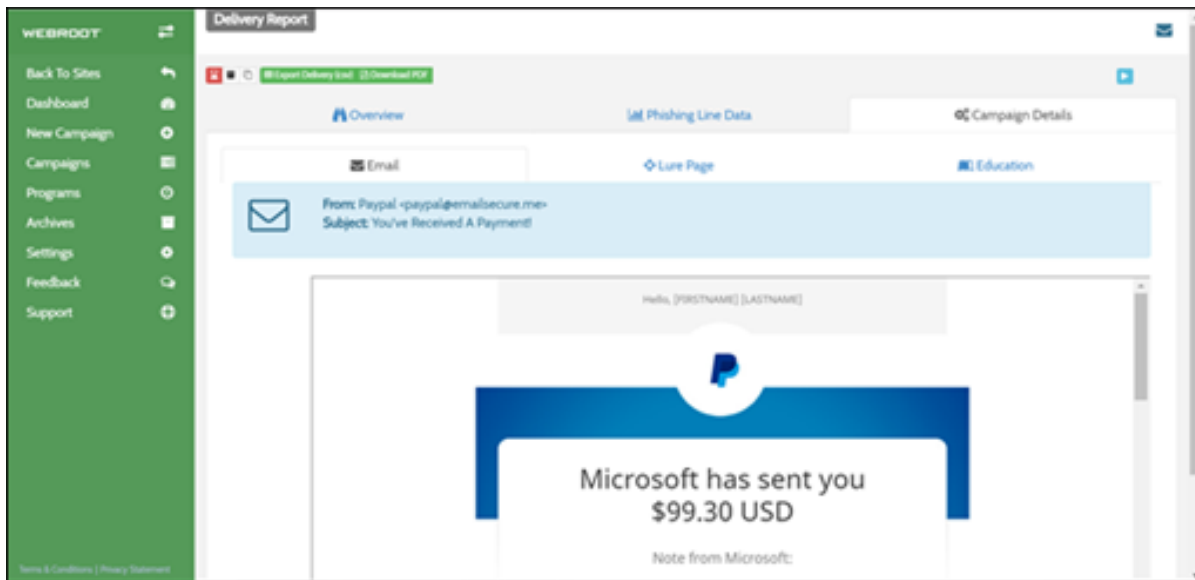
Launch Date (To)

Target	Timestamp	Browser	OS	Device	Page	Action
browell@webrootsalesdemo.com	Nov 7, 2017 10:06:41 AM	N/A	N/A	N/A	Email	Processed
browell@webrootsalesdemo.com	Nov 7, 2017 10:06:41 AM	N/A	N/A	N/A	Email	Delivered
browell@webrootsalesdemo.com	Nov 7, 2017 10:49:27 AM	N/A	N/A	N/A	Email	Click
browell@webrootsalesdemo.com	Nov 7, 2017 10:50:06 AM	N/A	N/A	N/A	Email	Click
browell@webrootsalesdemo.com	Nov 7, 2017 10:50:06 AM	N/A	N/A	N/A	Email	Click
browell@webrootsalesdemo.com	Nov 7, 2017 10:48:54 AM	Chrome v61.0.3163	Windows 10	Other	Education	Education_visit
browell@webrootsalesdemo.com	Nov 7, 2017 10:49:36 AM	Chrome v61.0.3163	Windows 10	Other	Education	Education_visit

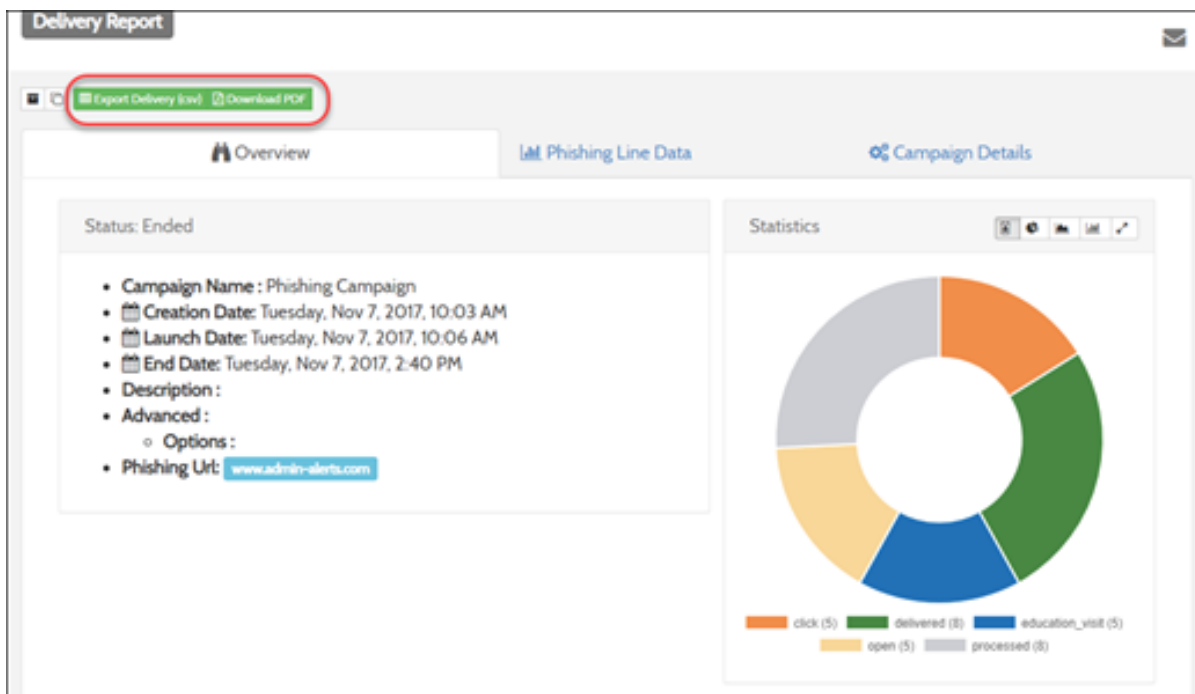
Showing 25 of 79 records found. 25

First Page Previous Page 1 2 3 4 Next Page Last Page

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.



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.

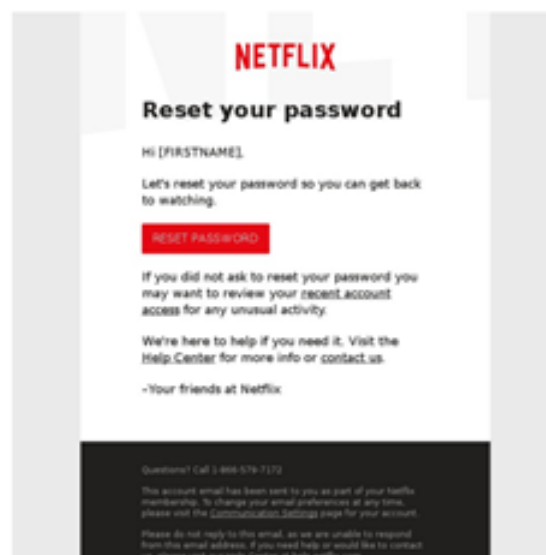
Events:

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.

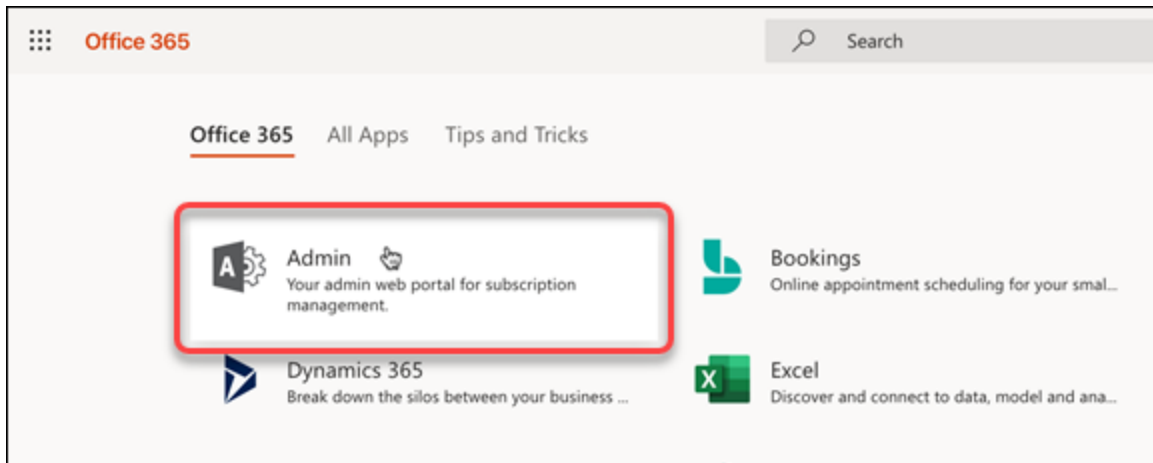
Part 4: Testing.

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.

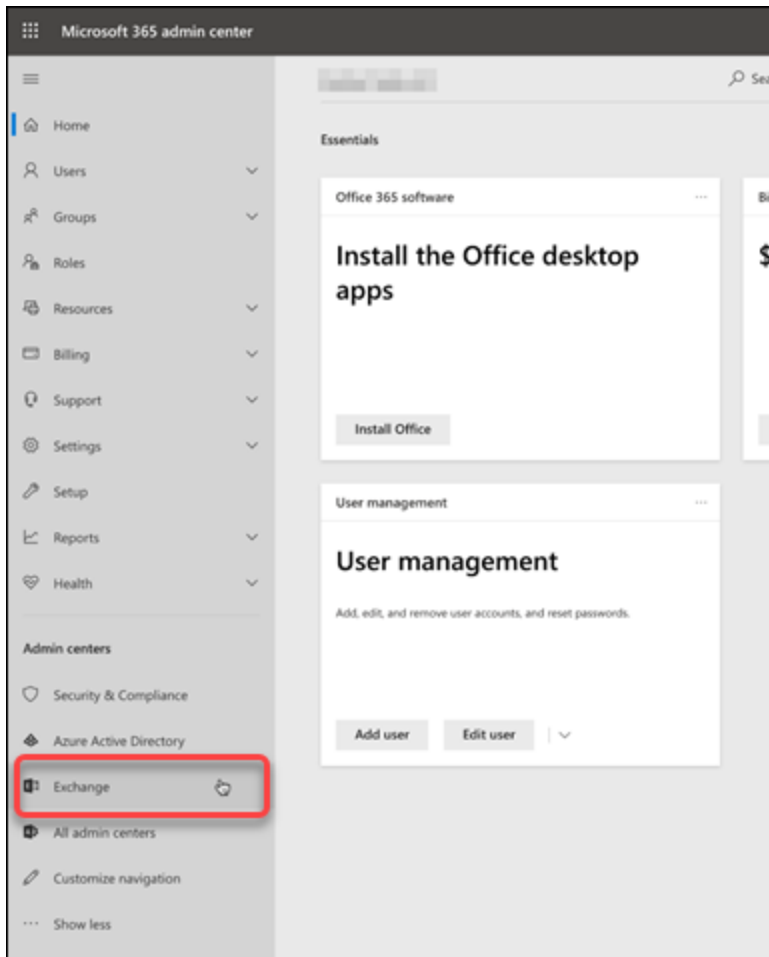
Part 1: Creating an IP Allow List with Webroot's email server IP address:

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

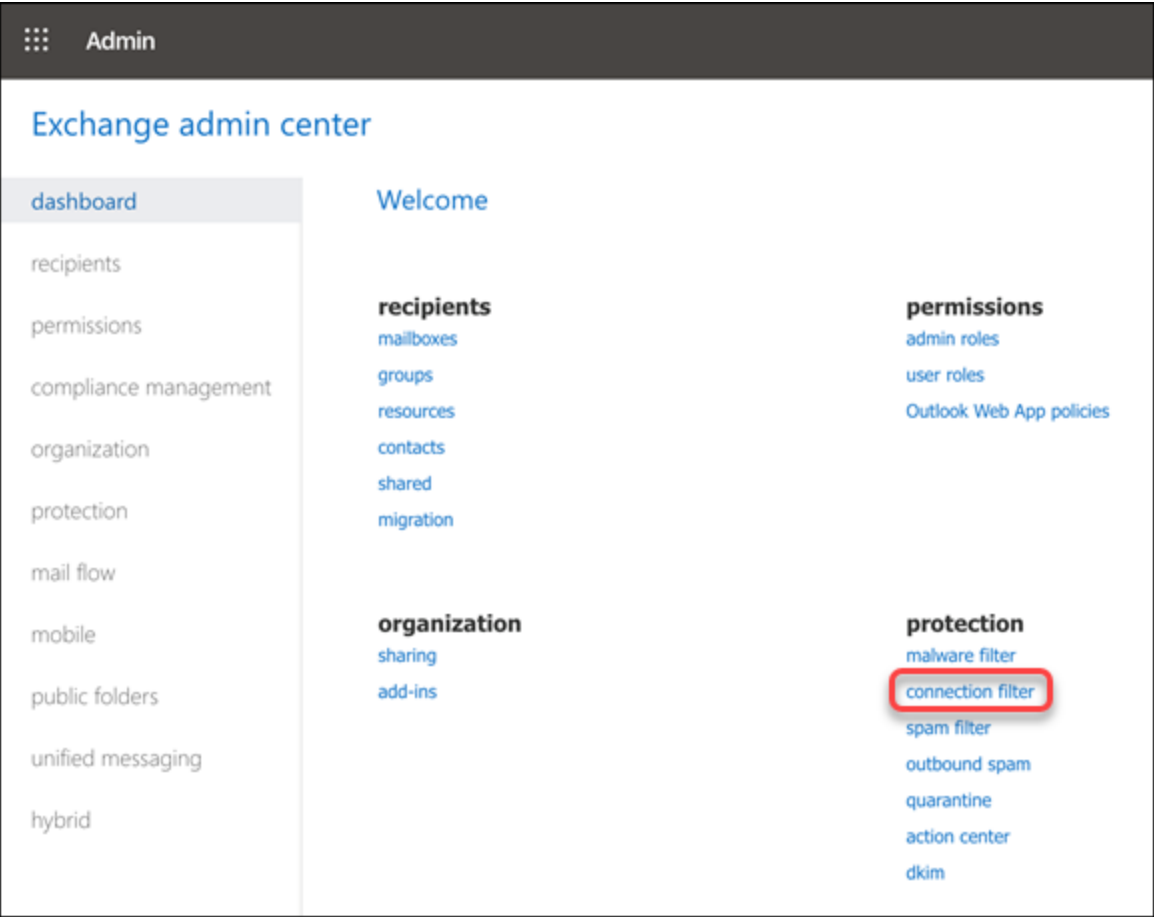
1. Navigate to your **Exchange admin center (EAC)** by signing into Microsoft 365 using your account, and then choose the **Admin** tile.



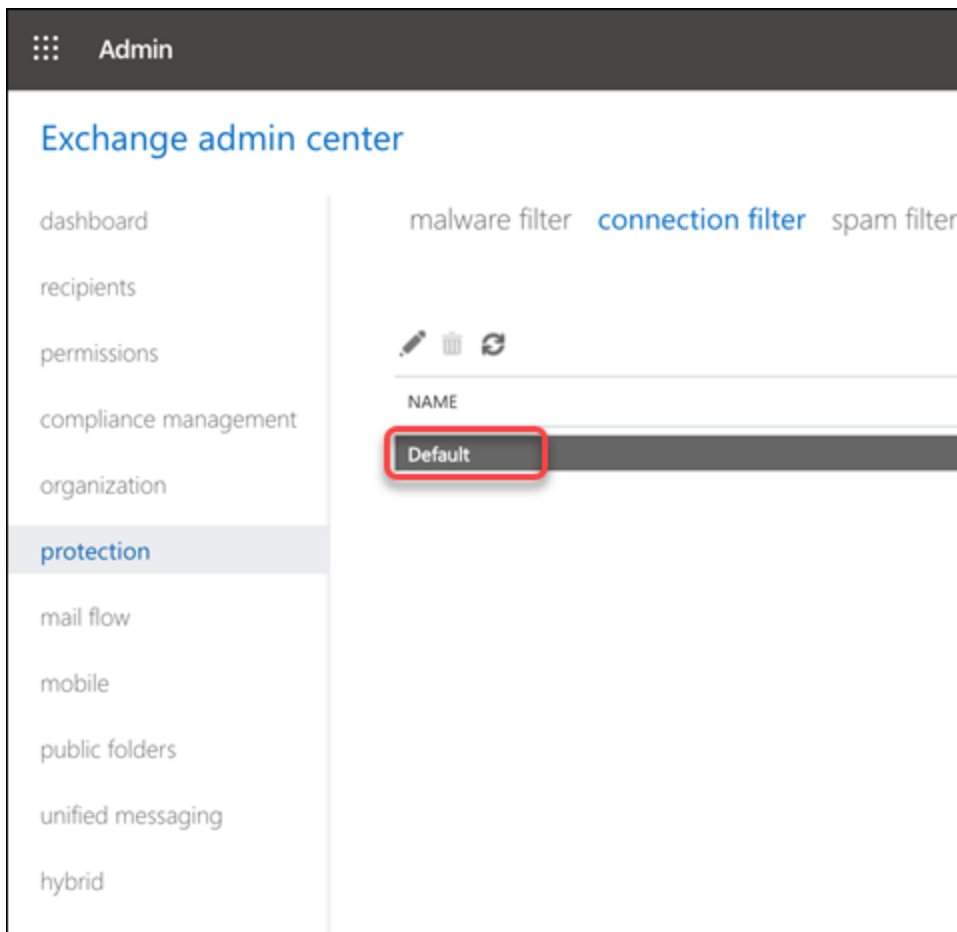
2. You are now in the Microsoft Microsoft 365 admin center. Use the left navigation list to choose **Admin centers > Exchange**.



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



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

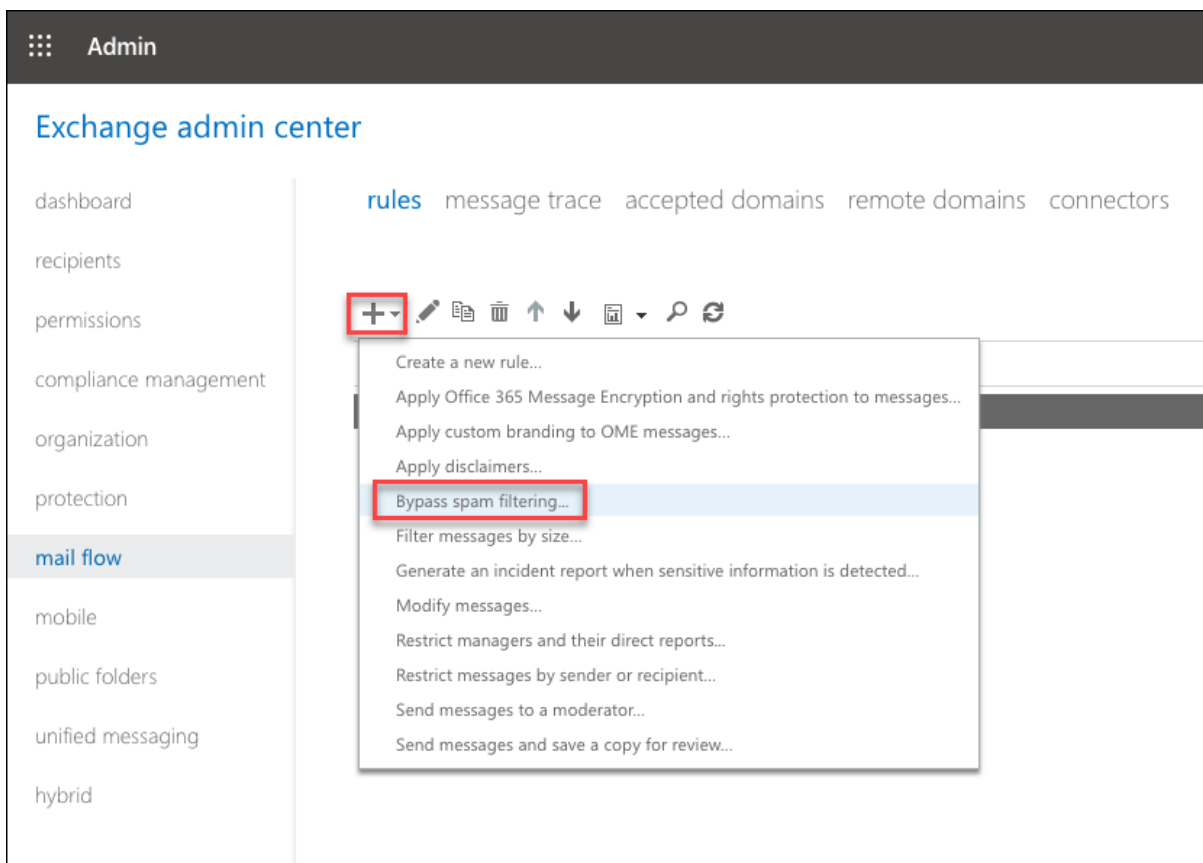


5. Click the **Connection filtering** menu item and then create an IP Allow list with Webroot's sender email IP addresses:
 - Under the **IP Allow list**, click on the **Add icon (+)**.
 - In the dialog box, enter the IP address for each of the Webroot Security Awareness Training email servers, which 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.

new rule

Name:
Bypass Clutter & Spam Filtering by IP Address

*Apply this rule if...

The sender is...
Select one
The sender...
The recipient...
The subject or body...
Any attachment...
Any recipient...
The message...
The sender and the recipient...
The message properties...
A message header...
[Apply to all messages]
Properties of this rule...

*Select people...

is this person
is external/internal
is a member of this group
address includes any of these words
address matches any of these text patterns
is on a recipient's supervision list
has specific properties including any of these words
has specific properties matching these text patterns
has overridden the Policy Tip
IP address is in any of these ranges or exactly matches
domain is

☒ Audit this rule with severity level:
Not specified

Choose a mode for this rule:
☒ Enforce
☐ Test with Policy Tips
☐ Test without Policy Tips

☐ Activate this rule on the following date:
Tue 2/4/2020 3:30 PM

☐ Deactivate this rule on the following date:
Tue 2/4/2020 3:30 PM

☐ Stop processing more rules
☐ Defer the message if rule processing doesn't complete

Match sender address in message:
Header

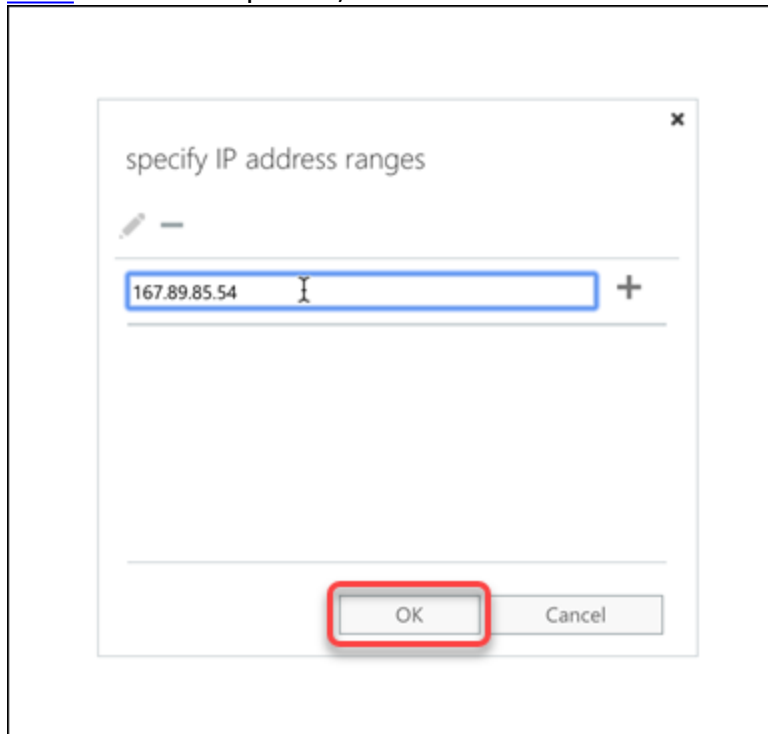
Comments:

1 Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS Online license for each user mailbox. [Learn more](#)

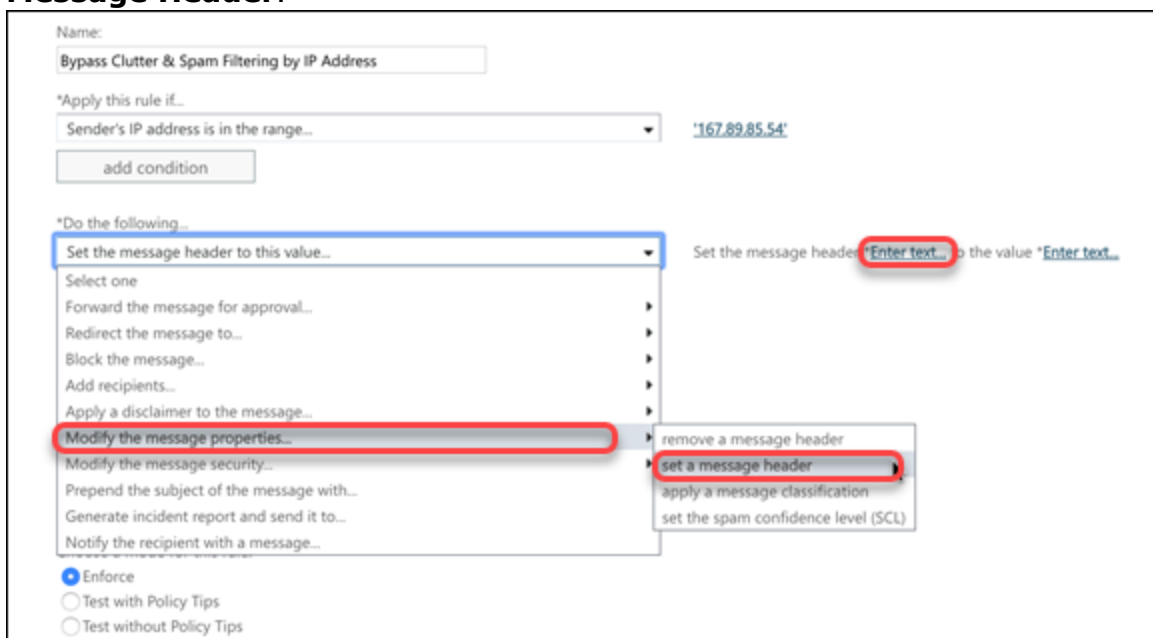
4. Add the condition **Apply this rule if...**

- 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**.



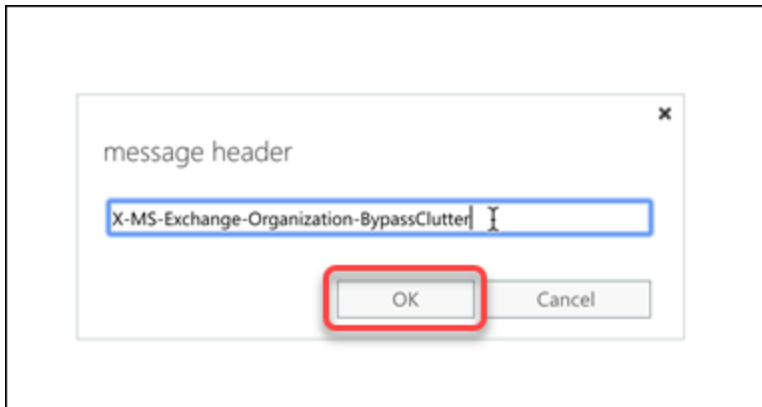
5. Beneath **Do the following**, click **Modify the message properties** then **Set a Message Header**.



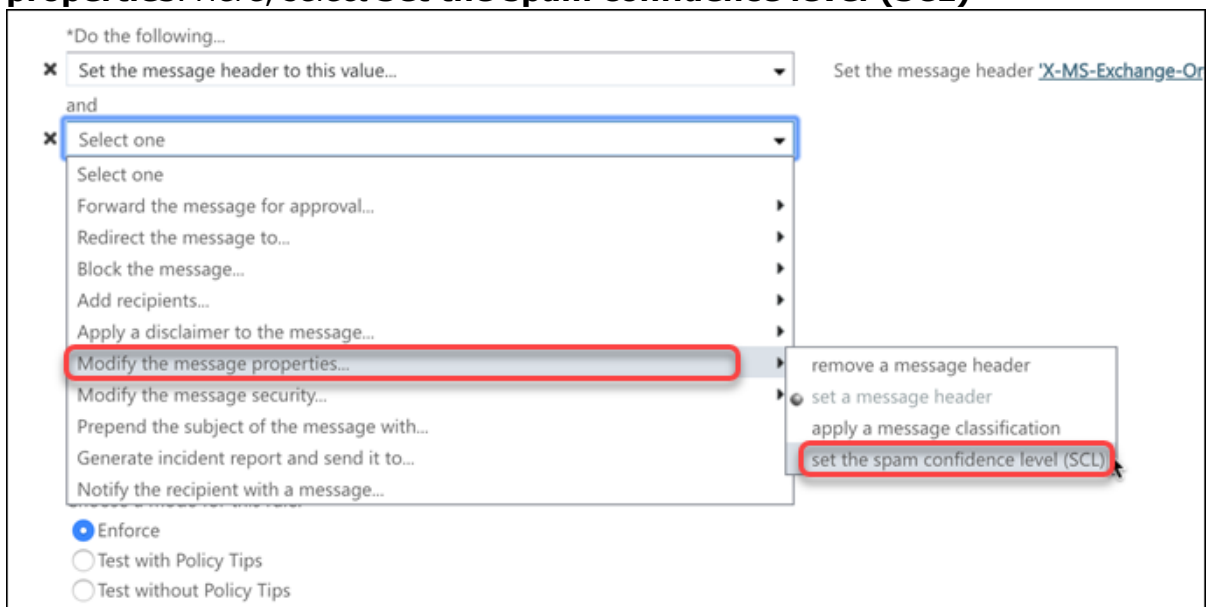
6. Click the ***Enter text...** button to set the message header to the value below. Click **OK** to continue.

- **X-MS-Exchange-Organization-BypassClutter** to the value **true**

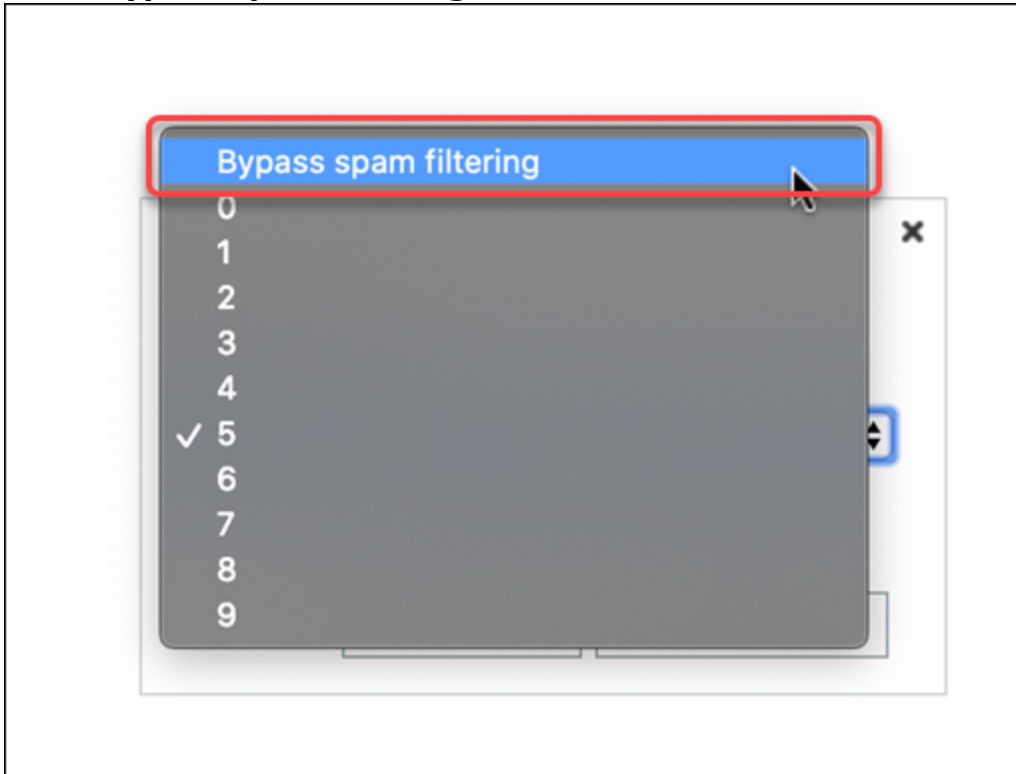
Note: Both values are case sensitive.



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**.



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

The screenshot shows the 'new rule' configuration page in the Exchange Admin Center. The rule is named 'Bypass Outlook & Spam filtering by IP Address'. It has a condition: 'Sender's IP address is in the range' with the value '192.168.0.0/24'. The actions are: 'Set the message header "X-MS-Exchange-Organization-BypassOutlook" to the value "True"' and 'Set the spam confidence level (SCL) to: Bypass spam filtering'. The rule is set to 'Enforce' and is active. The 'Save' button is highlighted with a red rectangle.

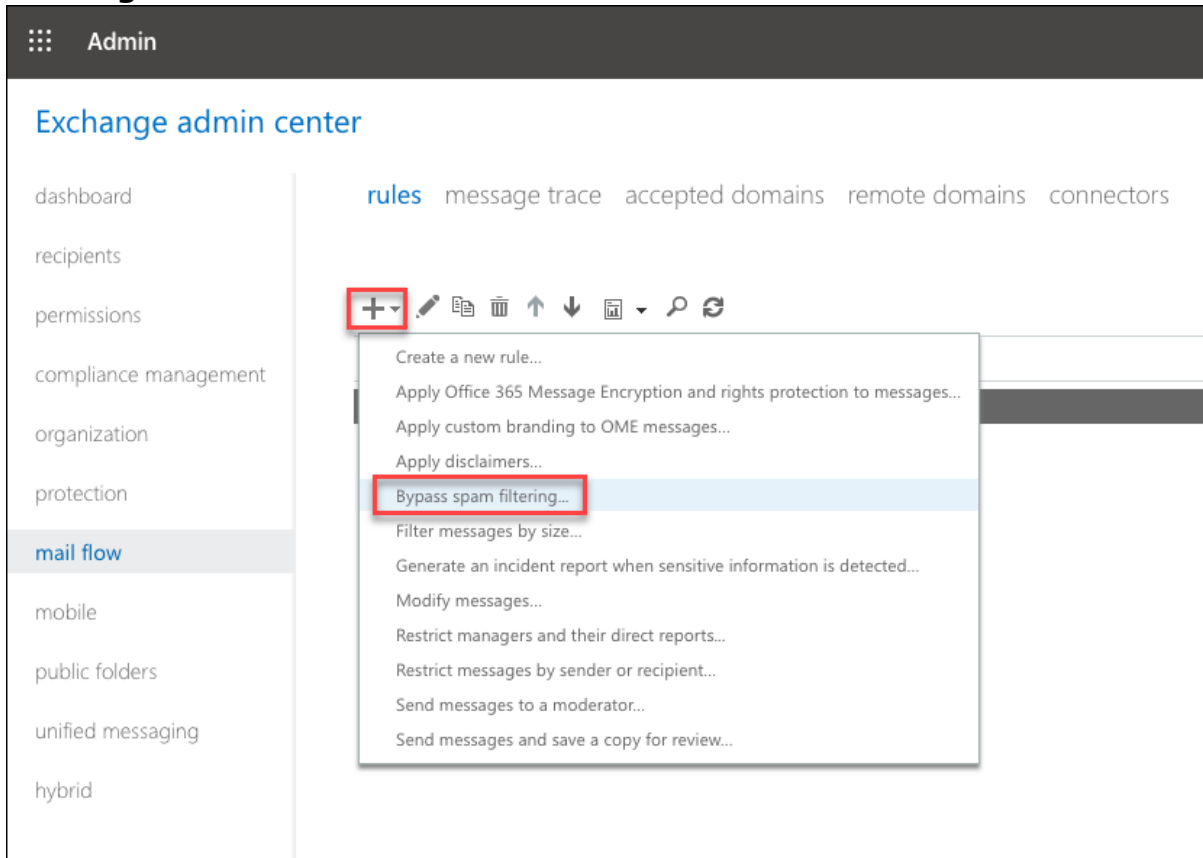
Part 3: [Microsoft 365 ONLY] Creating a rule to bypass the Junk Folder for M365 mail servers

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.

- 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.

SFVSKI;

Name:

*Apply this rule if...

Sender's IP address is in the range...

*Do the following...

Set the message header to this value...

Except if...

Properties of this rule:

Priority:

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 "**SFVSKI;**".
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:

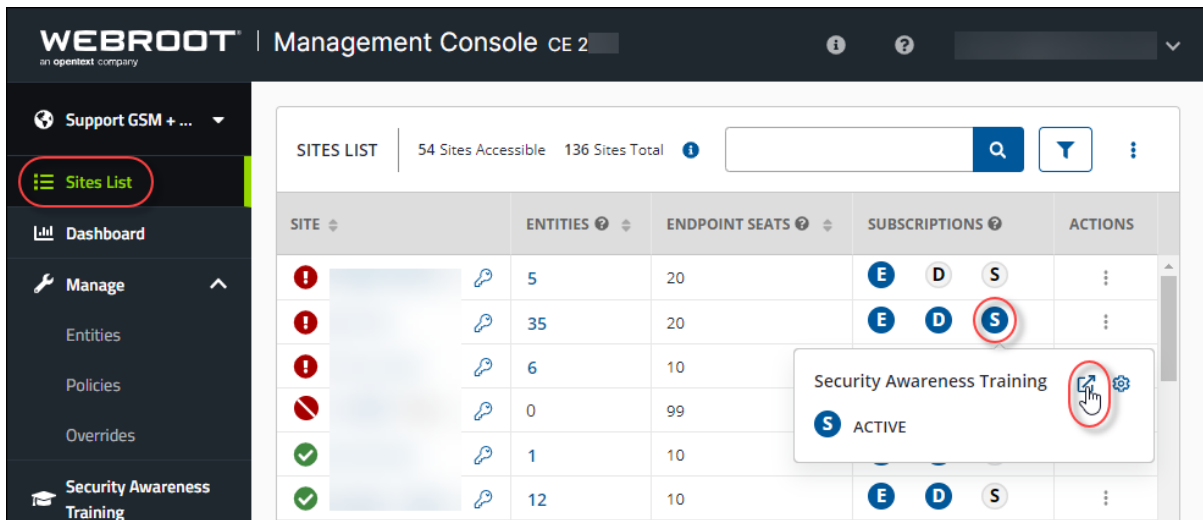
Verifying Domains	175
Importing Targets	179
Integrating with Microsoft Azure Active Directory	188
Microsoft Azure Active Directory Frequently Asked Questions	197

Verifying Domains

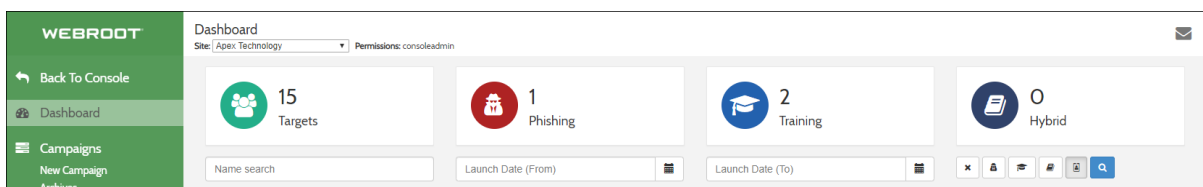
You must verify a domain before you can send phishing simulations to users in that domain.

To verify a domain:

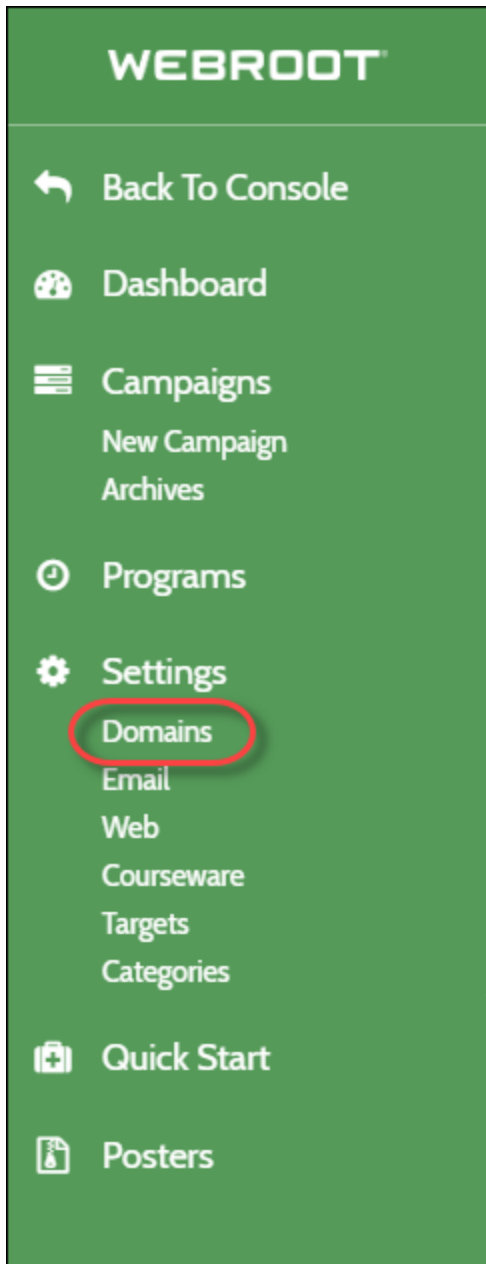
1. [Log in to the Management Console](#).
2. Select a Site from the **Sites List** and click the **Go to the Security Awareness Training Console** icon.



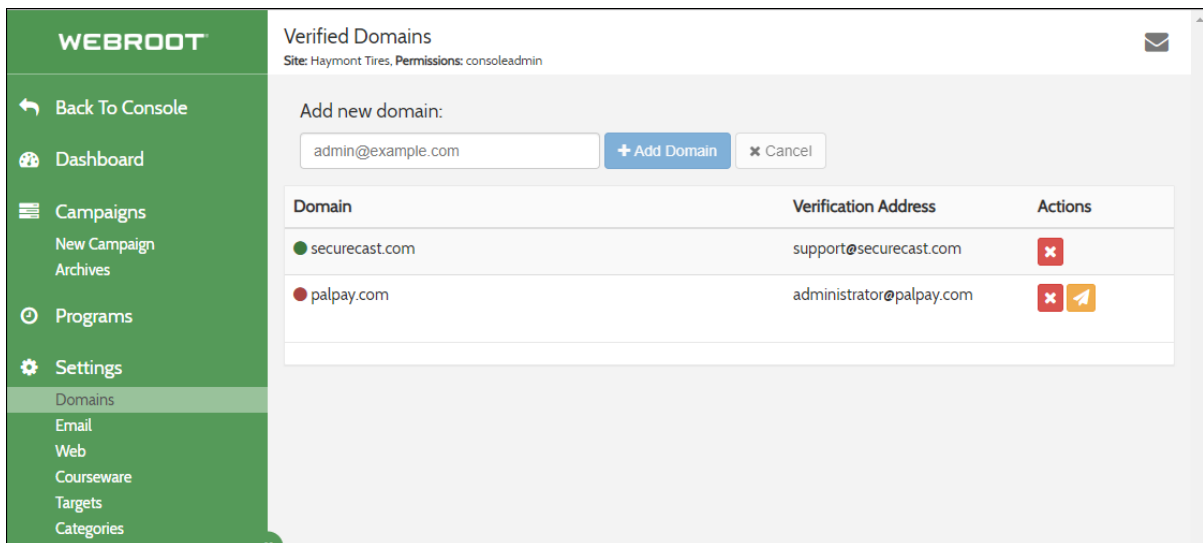
The Security Awareness Training dashboard displays.



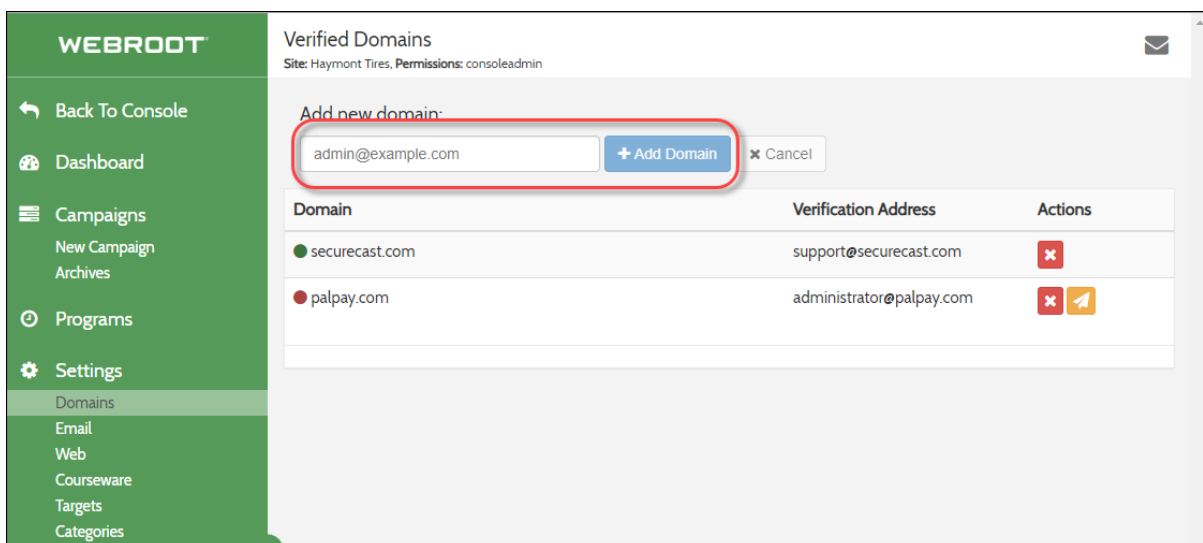
3. In the Nav bar, click **Settings > Domains**.



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.

WEBROOT

Back To Console

Dashboard

Campaigns

New Campaign

Archives

Programs

Settings

Domains

Email

Web

Courseware

Targets

Verified Domains

Site: Haymont Tires, Permissions: consoleadmin

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

administrator@webrootsalesdemo.com

+ Add Domain

✕ Cancel

• Adding domain: webrootsalesdemo.com

• Verification email will be send to: administrator@webrootsalesdemo.com

Domain	Verification Address
<div>securecast.com</div>	support@securecast.com
<div>palpay.com</div>	administrator@palpay.com

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

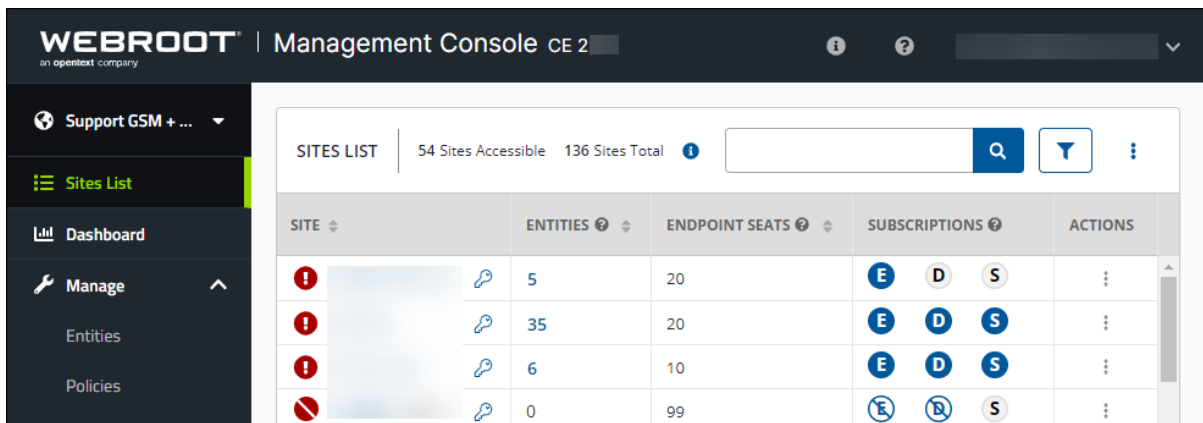
Importing Targets

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

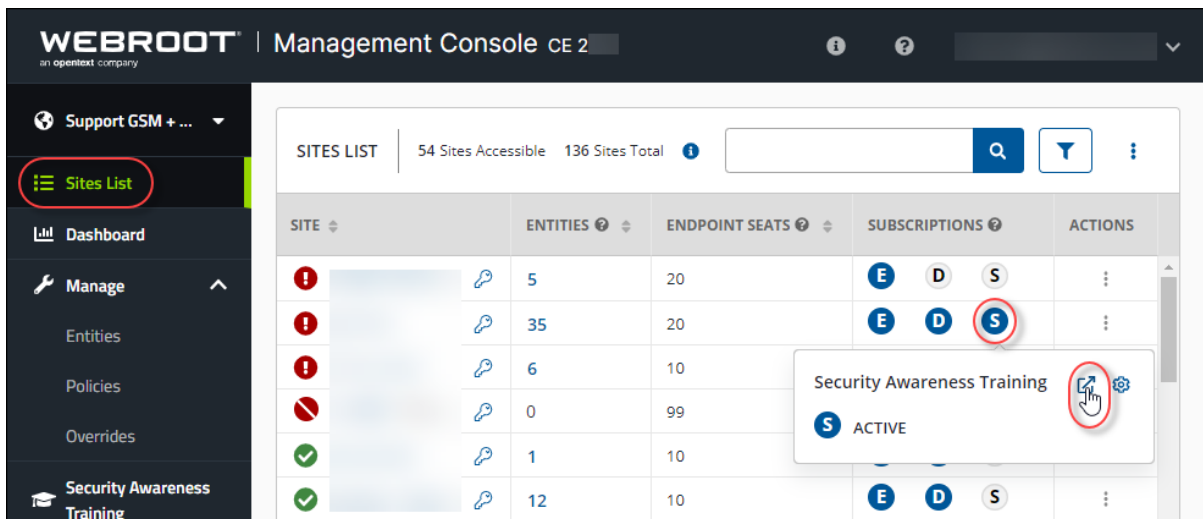
To import a target:

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

The Sites tab displays.

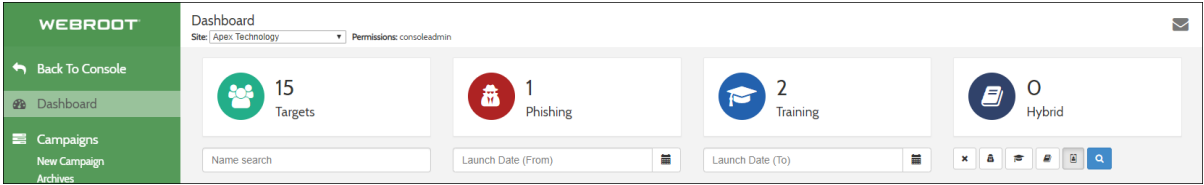


2. Select a Site from the **Sites List** and click the **Go to the Security Awareness Training Console** icon.

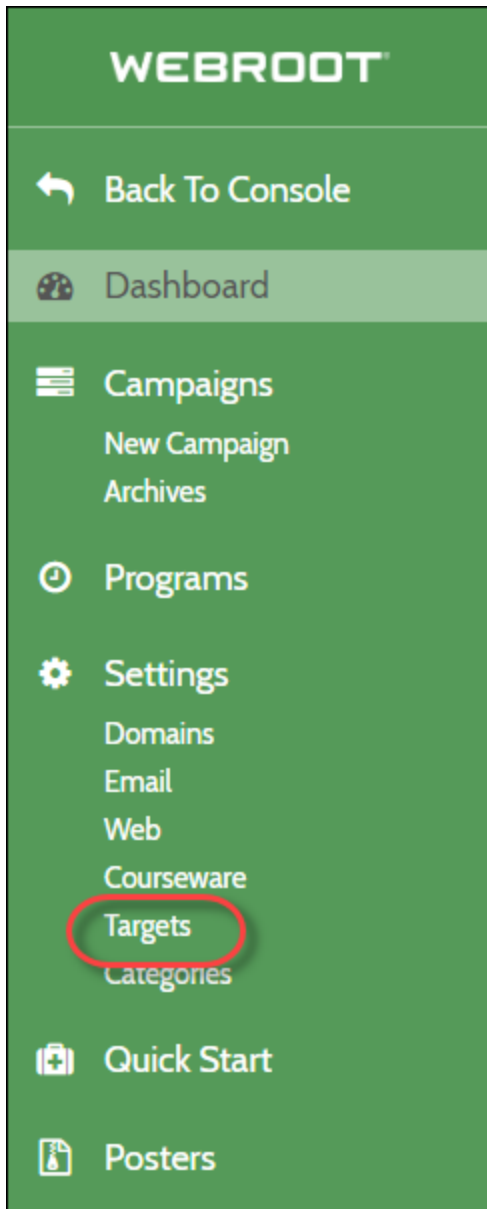


The Security Awareness Training dashboard displays.

Security Awareness Training Admin Guide



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



The Target Data panel displays.

The screenshot shows the 'Target Data' interface. At the top, it says 'Site: Apex Technology, Permissions: consoleadmin'. Below this are search filters: 'First Name', 'Last Name', 'Email', and 'Select tags to search'. There are also buttons for 'x' and 'refresh'. Below the filters are three blue boxes: 'Selected Targets: 0/500', 'Targets: 2', and 'Verified domains only' with an information icon. Below these boxes is a pagination bar: 'Showing 2 of 2 records found.', a dropdown for '100', and navigation buttons: '<< First Page', '< Previous Page', '1', 'Next Page >', and 'Last Page >>'. On the right of the pagination bar is a green button '+ Import Targets'. Below the pagination bar is a table with columns: 'First Name', 'Last Name', 'Email', and 'Tags'. The table has two rows: 'Dan' and 'Michael'. Each row has a checkbox on the left and a red 'x' button on the right.

	First Name	Last Name	Email	Tags
<input type="checkbox"/>	Dan			
<input type="checkbox"/>	Michael			

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

This screenshot is identical to the one above, but the '+ Import Targets' button is highlighted with a red circle.

The Import Targets window displays.

Import Targets (verified domains only)

Import Method

☒ Enter Targets Manually ☐ Upload Targets

First Name

Last Name

Email

Employee ID

Tags

First Name

Last Name

Email

Comany User I

Add/Select Tags...

+ Add Target

- or -

Enter one target per line (with optional headers)

firstName,lastName,email,tags,companyId

Import

Done

5. Do any of the following:

- To enter targets manually, one by one, populate the fields and click the **Add Target** button.

Import Targets (verified domains only)

Import Method

☒ Enter Targets Manually ☐ Upload Targets

First Name

Last Name

Email

Employee ID

Tags

First Name

Last Name

Email

Comany User I

Add/Select Tags...

+ Add Target

- or -

Enter one target per line (with optional headers)

firstName,lastName,email,tags,companyId

Import

Done

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.

Import Targets (verified domains only) ✕

Import Method

☒ Enter Targets Manually ☐ Upload Targets

First Name

First Name

Last Name

Last Name

Email

Email

Employee ID

Comany User I

Tags

Add/Select Tags...

+ Add Target

- or -

Enter one target per line (with optional headers)

firstName,lastName,email,tags,companyId

Import

Done

- 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.

Import Targets (verified domains only)

Import Method

☒ Enter Targets Manually

☐ Upload Targets

First Name

First Name

Last Name

Last Name

Email

Email

Employee ID

Comany User I

Tags

Add/Select Tags...

+ Add Target

- or -

Enter one target per line (with optional headers)

firstName,lastName,email,tags,companyId

Import

Done

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

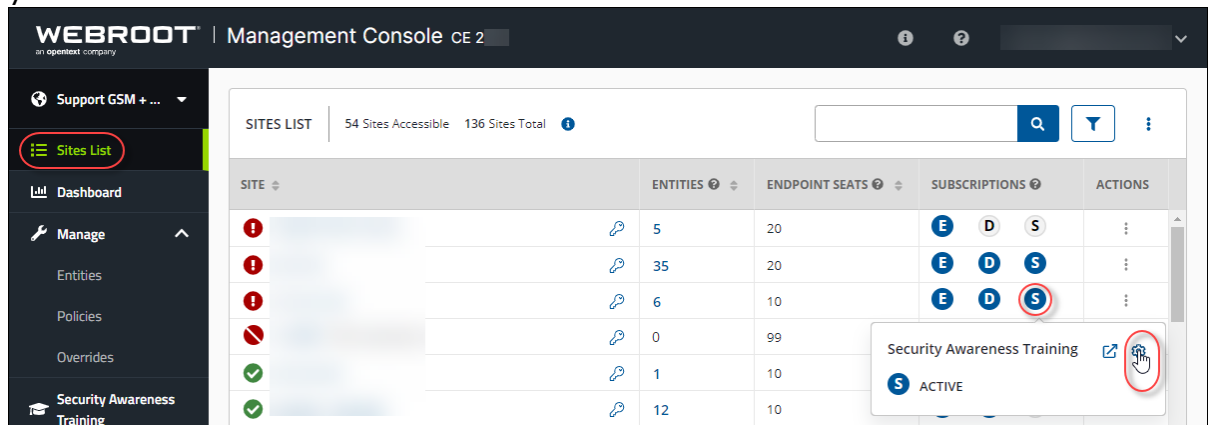
To complete the WSAT integration with Azure AD, you will perform the following steps:

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

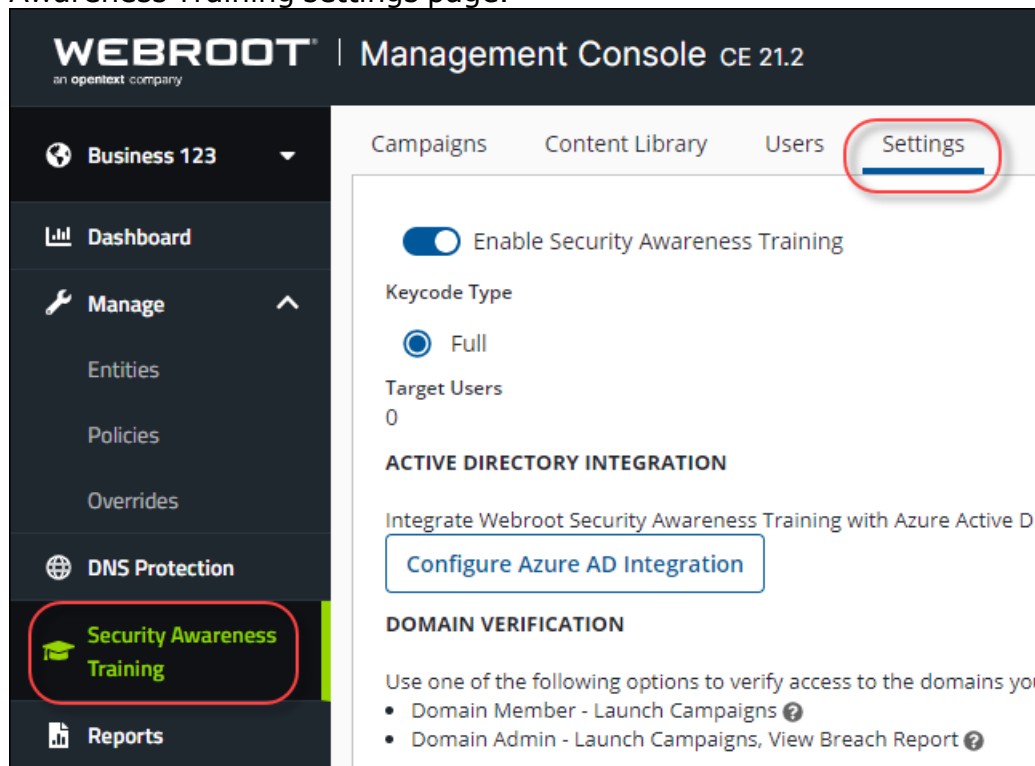
To connect your site to Azure AD, you will need to obtain a **Secret Token** for that site in the Webroot management console.

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.

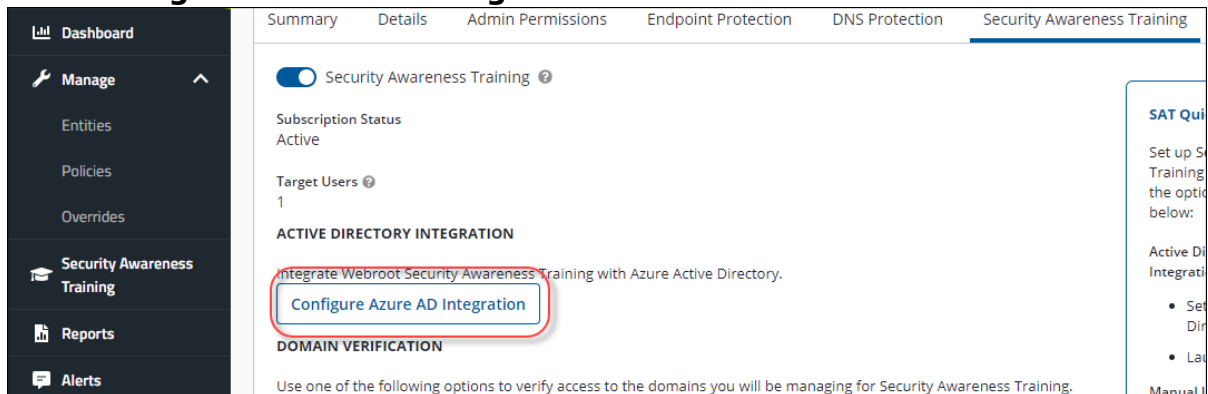


- b. For the **single site** Webroot Management console: In the left navigation bar, click **Security Awareness Training** and then **Settings** to open the Security

Awareness Training settings page.



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



4. Copy the **Secret Token**.

ACTIVE DIRECTORY INTEGRATION SETUP GUIDE

Complete the following steps from the Azure Portal to have users automatically synced with Security Awareness Training.

1. Add the Webroot Security Awareness Training Application to your Azure Active Directory tenant:
 - a. From the [Azure Portal](#), use the left navigation pane to select the Azure Active Directory service.
 - b. Navigate to Enterprise Applications and select All Applications, then click New Application.
 - c. In the Add from the gallery section, search for Webroot Security Awareness Training and add the app.
2. Configure Azure Active Directory Integration:
 - a. Select Users and Groups from the left navigation pane to manage what users and groups should be synced with Security Awareness Training.
 - b. Select Provisioning from the left navigation pane and click Get Started. Choose Automatic as the Provisioning Mode and click Save.
 - c. Enter the Tenant URL as `https://awarenessapi.webrootanywhere.com/api/v2/scim`
 - d. Enter your Secret Token. Use the Test Connection button before clicking Save.
 - e. Change Provisioning Status to On and click Save.

Secret Token

Copy

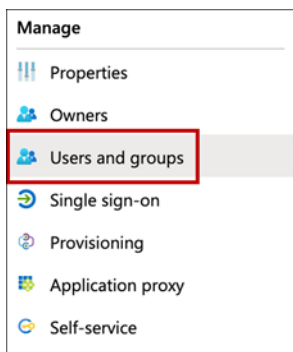
Security Awareness Training Admin Guide

Cancel

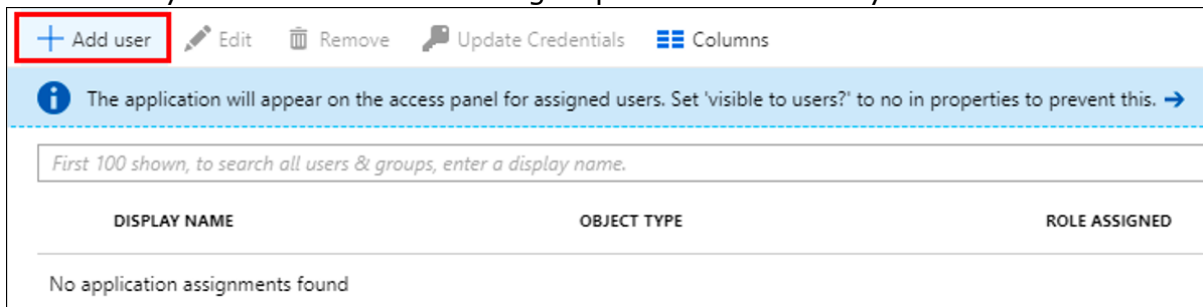
Done

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**.



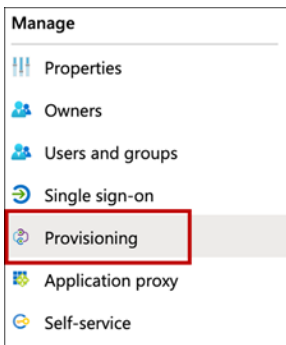
2. From here you can select users and groups that should be synced with WSAT.



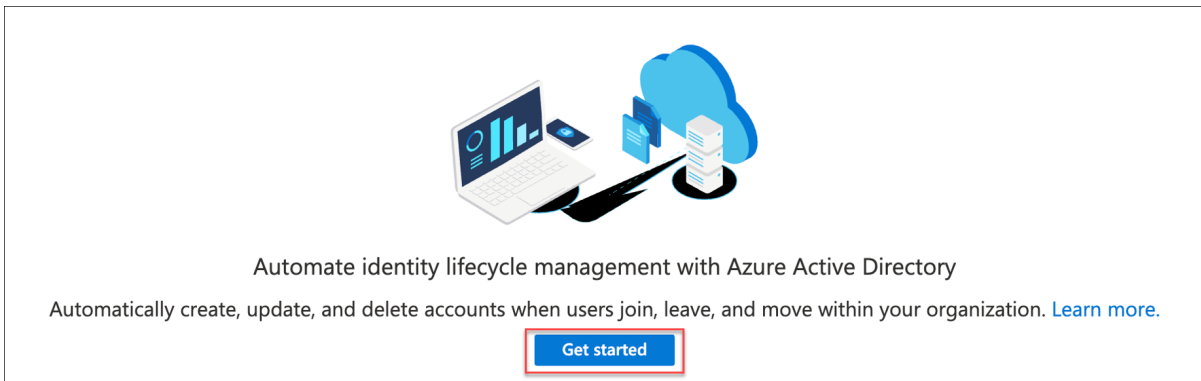
Note: You can optionally skip this step and choose to **Sync all users and groups** as your **Scope** in the **Provisioning** section. Depending on your Active Directory Level, you may be able to create groups for assignment. If you have access to the groups functionality in Active Directory, we recommend 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

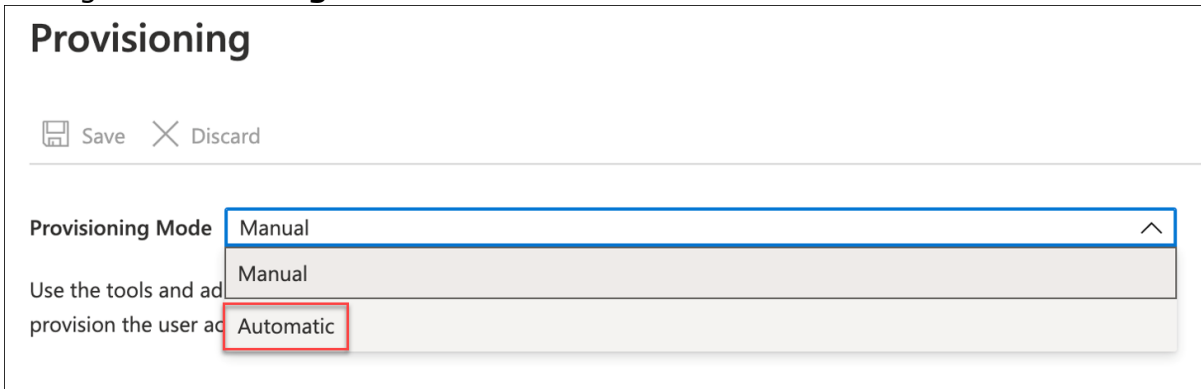
1. In the [Azure portal](#), on the **Webroot Security Awareness Training** application integration page, click **Provisioning**.



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**.

Admin Credentials

Admin Credentials

Azure AD needs the following information to connect to Webroot Security Awareness Training's API and synchronize user data.

Tenant URL * ⓘ https://awarenessapi.webrootanywhere.com/api/v2/scim ✓

Secret Token * ⓘ ✓

Test Connection

Notification Email ⓘ ✓

☐ Send an email notification when a failure occurs

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

Settings

Start and stop provisioning to Webroot Security Awareness Training, and view provisioning status.

Provisioning Status ⓘ On Off

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

Webroot Security Awareness Training | Provisioning

Enterprise Application

Overview

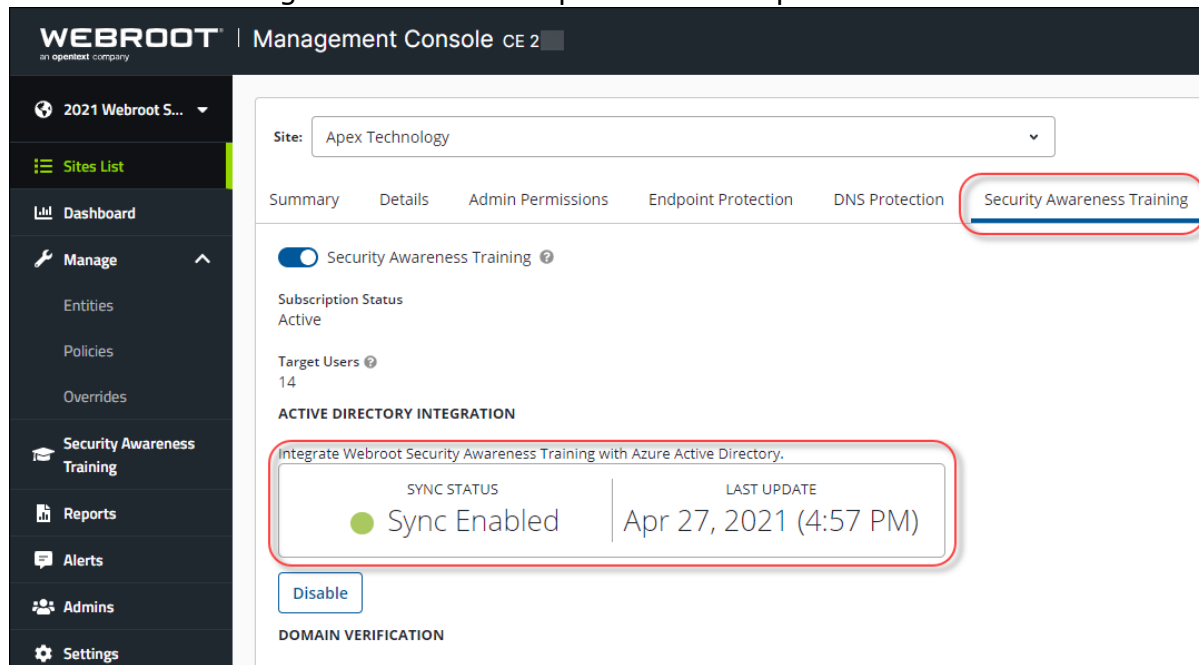
Save Discard

Step 4: Confirm that users were imported

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

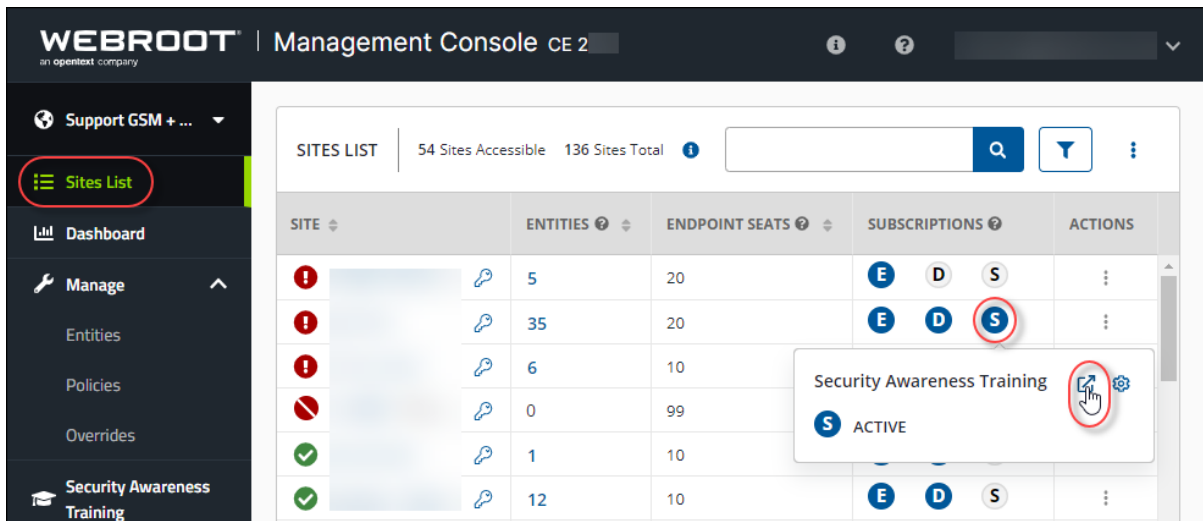
In the Webroot management console, the **Security Awareness Training** settings page for your site shows the status of the Active Directory Integration as **Sync Pending** or **Sync Enabled**.

- **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.

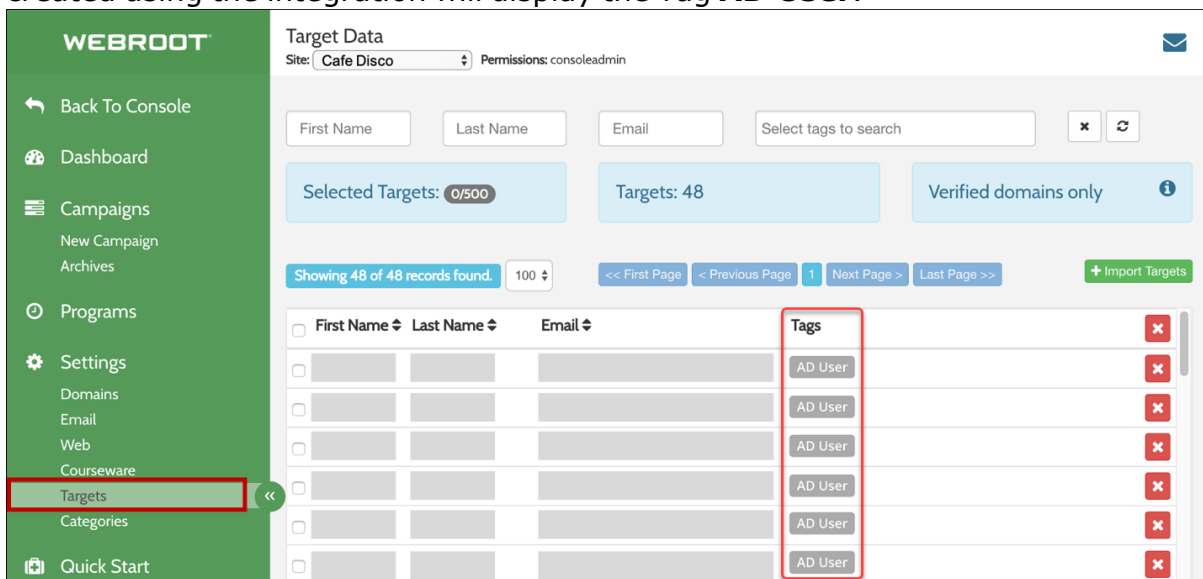


To see the users that were imported:

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:

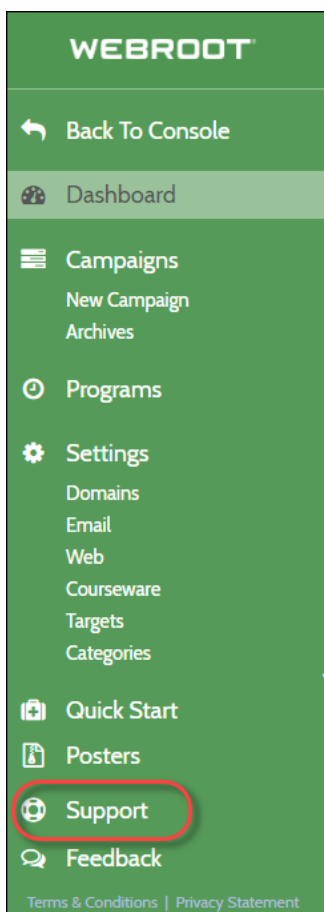
Accessing Technical Support	199
Leaving Feedback	201

Accessing Technical Support

Webroot offers a variety of support options.

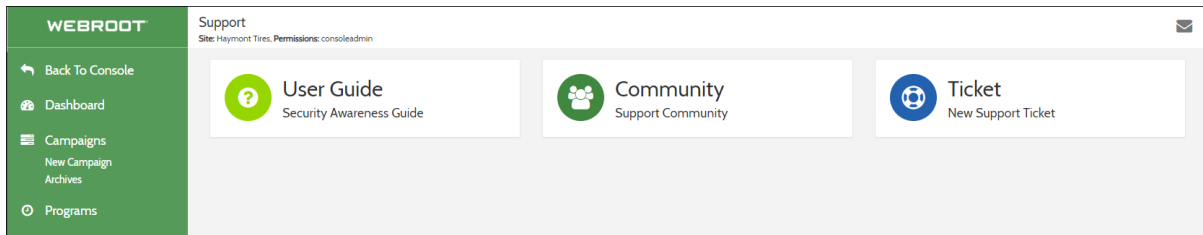
To access technical support:

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



The Support panel displays.

Security Awareness Training Admin Guide



2. From there, you can do any of the following:

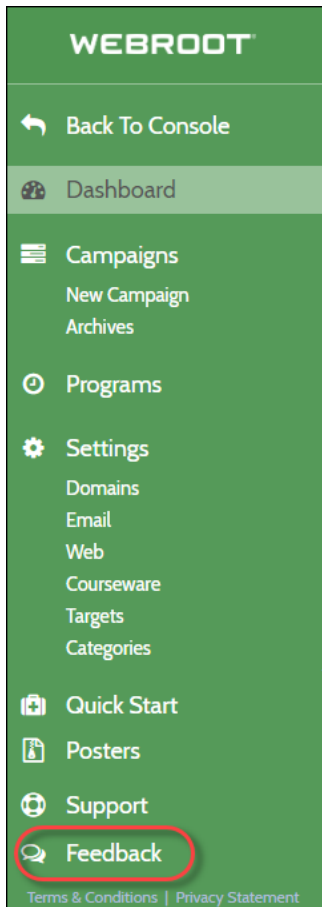
- [Look for the answer in our online documentation.](#)
 - [Connect to the Webroot Online Business Forum.](#)
 - [Enter a help ticket.](#)
-

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.

WEBROOT®

Webroot Security Awareness Training - Customer Feedback

Thank you for your feedback!

1. What is your overall satisfaction with Webroot Security Awareness Training?

Somewhat

Somewhat

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 simulations
 - 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