WEBROOT®

an opentext™ company

Security Awareness Training Getting Started Guide

Copyright

Security Awareness Training Getting Started Guide

Table of Contents

Webroot® Security Awareness Training Overview

The goal of a security awareness program is to increase organizational understanding and practical implementation of security best practices. The program should apply to all hires—new and old, across every department—and it should be reinforced on a regular basis.

Cybersecurity awareness training, as a concept, is not a one-size fits all solution, so you will need to look at your sector to determine what types of training are relevant, both in terms of specific threats or risks, and industry regulations and compliance. You may need to divide your users into logical training groups to ensure the training they receive is relevant to their role.

This guide is designed to help you plan campaign activities and ongoing user education training programs successfully as suited to your business or client environments.

What your training program should cover

Pro tip: Do not assume your employees have technical knowledge. Instead, start with the basics, and get more specific from there.

A robust cybersecurity training program should educate employees about the following:

Phishing awareness

Phishing is used by many hackers for a variety of purposes. They send an official-sounding email, and innocent users click on it. The email may prompt users to enter sensitive information, such as bank account or Social Security numbers, or even to make a purchase or payment with company funds. Employees should be on guard against this sneaky type of attack.

Malware

Malware (from “malicious software”) is the term for dangerous programs and codes, including spyware, viruses and ransomware. These attacks, typically launched by clicking an infected attachment, are very common. In addition to installing antivirus software, employees should be trained to not open attachments from unknown sources.

Password security

Create password requirements that are complex enough to survive hackers’ attempts to brute force logins. Prompt employees to change passwords regularly and after any potential security breach. In addition, encourage employees to use multi-factor authentication to add an extra layer of security.

Desktop security

Keep all operating systems, programs, and applications patched and up to date. Hackers often take advantage of vulnerabilities in older or outdated systems and applications.

Working remotely using WiFi

Remote work options give employees flexibility and can improve job satisfaction. Make sure employees are trained in secure WiFi protocols. For example, hackers can intercept data transmitted over public WiFi networks, so employees should never use public WiFi to transmit sensitive information.

Social engineering

Social engineering is a tactic cybercriminals use to trick users into revealing sensitive information. Social engineering can also prompt users to download a harmful attachment that will infect their computer (and possibly the corporate network) with a virus. Social engineering includes: baiting, phishing, email hacking, and other manipulative ploys.

Email security

Most businesses require email for communication. But email can also serve as a tool for cybercrime, allowing hackers to invade your computer network. Install virus protection and set spam filters to catch unwanted email. Train employees to use caution when opening attachments or emails from unfamiliar senders.

Physical security

Employees work on a variety of electronic devices, including mobile phones, tablets, and laptops, all of which can be lost or stolen. Stress the importance of physical awareness of laptops and other portable devices.

Mobile device security

Mobile devices should only be used for company business on secure networks. Mobile devices pose a cybersecurity threat because employees use them for varied functions and often fail to secure them. Additionally, their small size and portability increase the risk of loss or theft.

Travel security

Stepping out of the office shouldn’t mean stepping away from secure mobile protocol. When traveling, make sure your employees keep all mobile devices secure and password-protected. They should never use public WiFi to transmit sensitive information while traveling.

General principles of successful cyber-training

- Behavioral change takes time
- Clear participation guidelines
- Phishing simulations: 1 or 2 per month
- Cyber awareness courses: 1 to 3 per quarter
- Compliance courses at audit
- Constantly measure and report

Note: If you are an MSP, be sure to train your own staff as well!

Implementing Security Awareness Training

- Train continuously
- Tailor training to audience (relevance)
- Include as onboarding topic
- Evaluate regularly
- Communicate results regularly
- Communicate new risks regularly
- Acknowledge employee participation
- Build-in feedback loops

Security Awareness Training (WSAT) Consoles

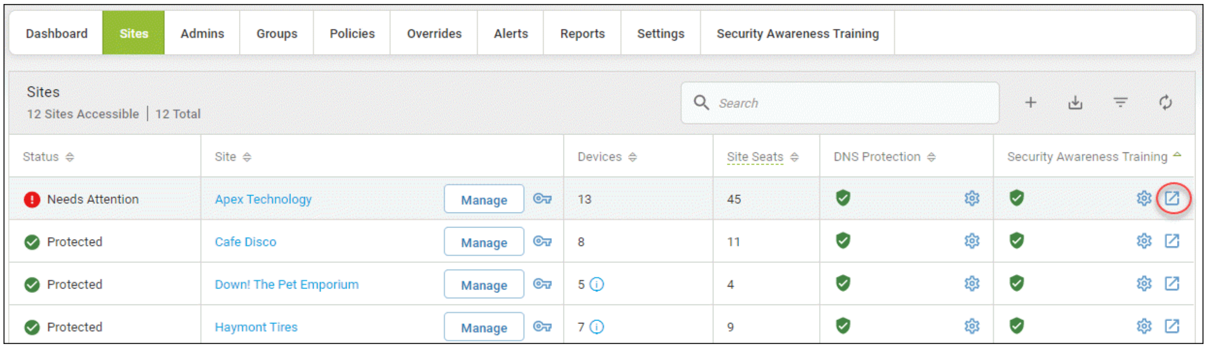
WSAT offers two primary management consoles that you can use depending on your needs, interest, and any agreements you have established with your clientele.

- Customer / Site Console
- Management Console

Customer / Site Console

When you start using WSAT, we recommend you begin with the individual site admin console to configure targets and to familiarize yourself with the various functions that are possible.

On the **Sites** tab, click the Go to WSAT icon ↗.



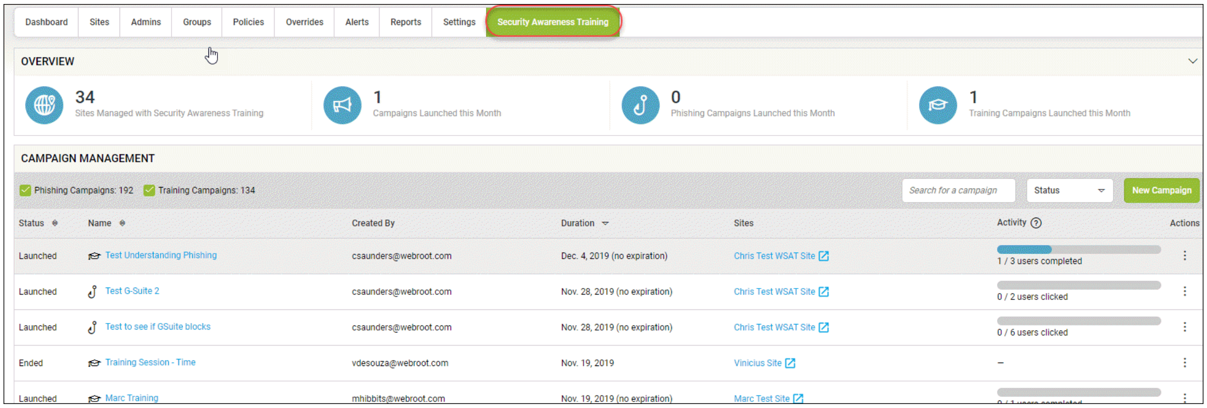
Sites
12 Sites Accessible | 12 Total

Status	Site		Devices	Site Seats	DNS Protection	Security Awareness Training
Needs Attention	Apex Technology	Manage	13	45	✓	✓
Protected	Cafe Disco	Manage	8	11	✓	✓
Protected	Down! The Pet Emporium	Manage	5	4	✓	✓
Protected	Haymont Tires	Manage	7	9	✓	✓

Global Console

You should use WSAT at the main Sites page or Management Console when you intend to establish a single phishing or training campaign that will be enabled across one or many customer sites. It is not as well-suited to a single campaign or group of campaigns for a single customer.

Click the **Security Awareness Training** tab to open the WSAT Management Console.



OVERVIEW

34 Sites Managed with Security Awareness Training

1 Campaigns Launched this Month

0 Phishing Campaigns Launched this Month

1 Training Campaigns Launched this Month

CAMPAIGN MANAGEMENT

☑ Phishing Campaigns: 192 ☑ Training Campaigns: 134

Status	Name	Created By	Duration	Sites	Activity	Actions
Launched	Test Understanding Phishing	csaunders@webroot.com	Dec. 4, 2019 (no expiration)	Chris Test WSAT Site	1 / 3 users completed	⋮
Launched	Test G-Suite 2	csaunders@webroot.com	Nov. 28, 2019 (no expiration)	Chris Test WSAT Site	0 / 2 users clicked	⋮
Launched	Test to see if GSuite blocks	csaunders@webroot.com	Nov. 28, 2019 (no expiration)	Chris Test WSAT Site	0 / 6 users clicked	⋮
Ended	Training Session - Time	vdesouza@webroot.com	Nov. 19, 2019	Vinicius Site	–	⋮
Launched	Marc Training	mhibbits@webroot.com	Nov. 19, 2019 (no expiration)	Marc Test Site	0 / 1 users completed	⋮

Note: To build and enable a global campaign, you will first need to configure each individual site manager for Security Awareness Training. Both the authorized domain AND a set of targets must be configured before you can establish a global campaign.

WSAT Training Elements

WSAT currently includes the following tools:

- A Phishing Simulator with an expanding real-world template library
- A Training Course Library
- A Learning Management Console

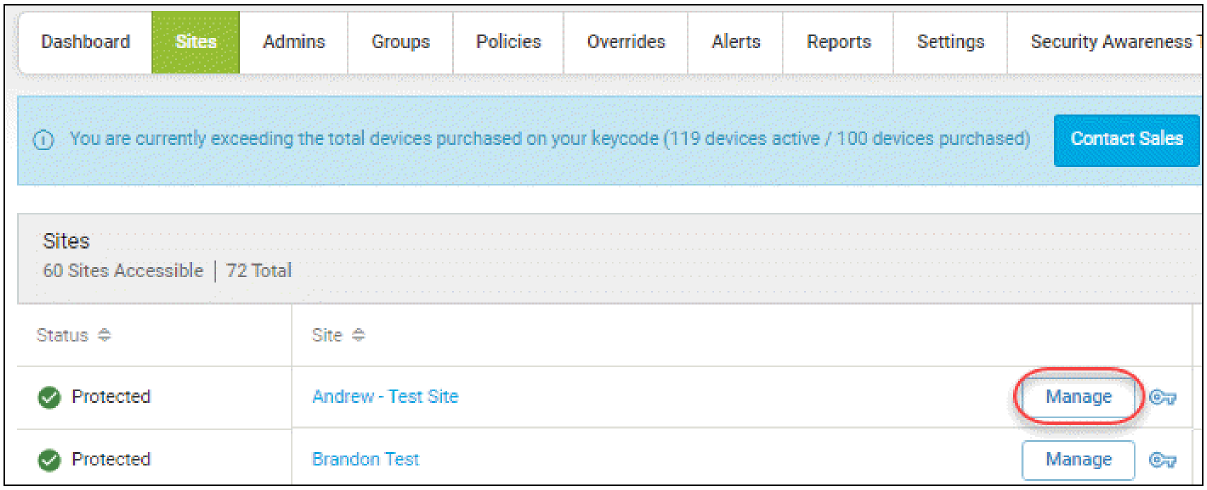
Getting Started

Deployment & Prerequisites

Before you can build and deploy your first campaign, you'll need to enable WSAT for the customer site you want to receive phishing or training campaigns.

Enabling Security Awareness Training

1. For the site you want to enable, click **Manage**.

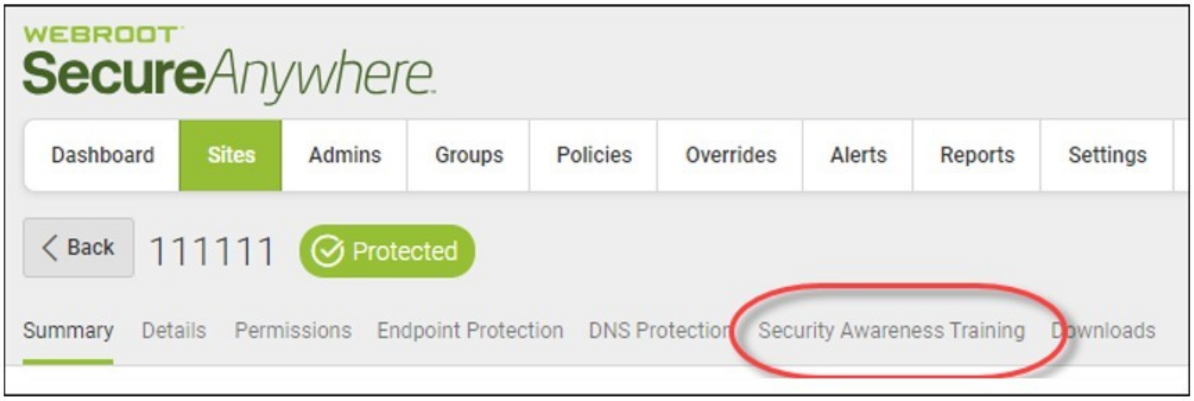


ⓘ You are currently exceeding the total devices purchased on your keycode (119 devices active / 100 devices purchased)

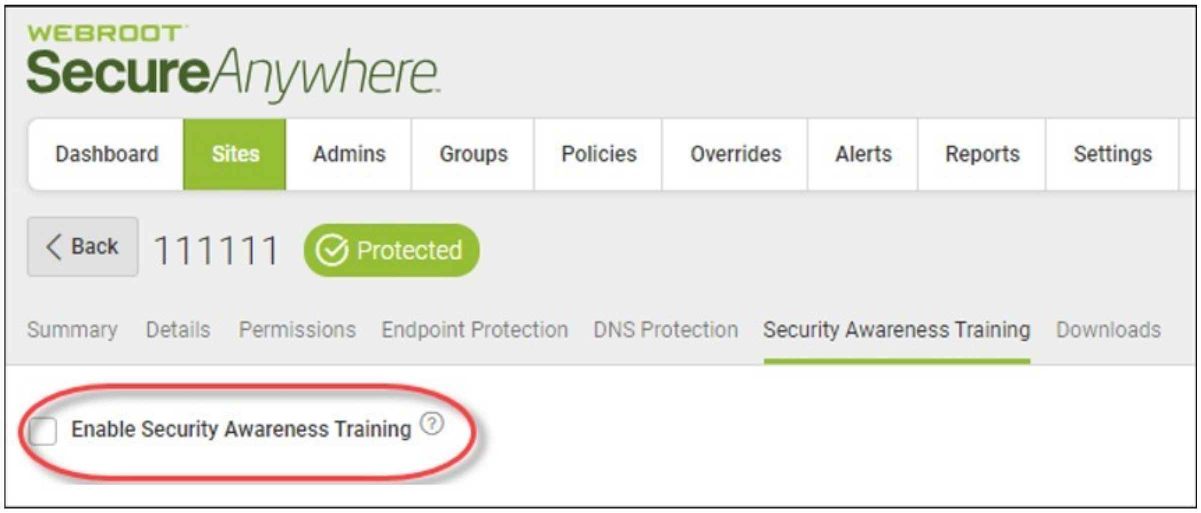
Sites
60 Sites Accessible | 72 Total

Status ≑	Site ≑
Protected	Andrew - Test Site
Protected	Brandon Test

2. Open the Security Awareness Training tab.

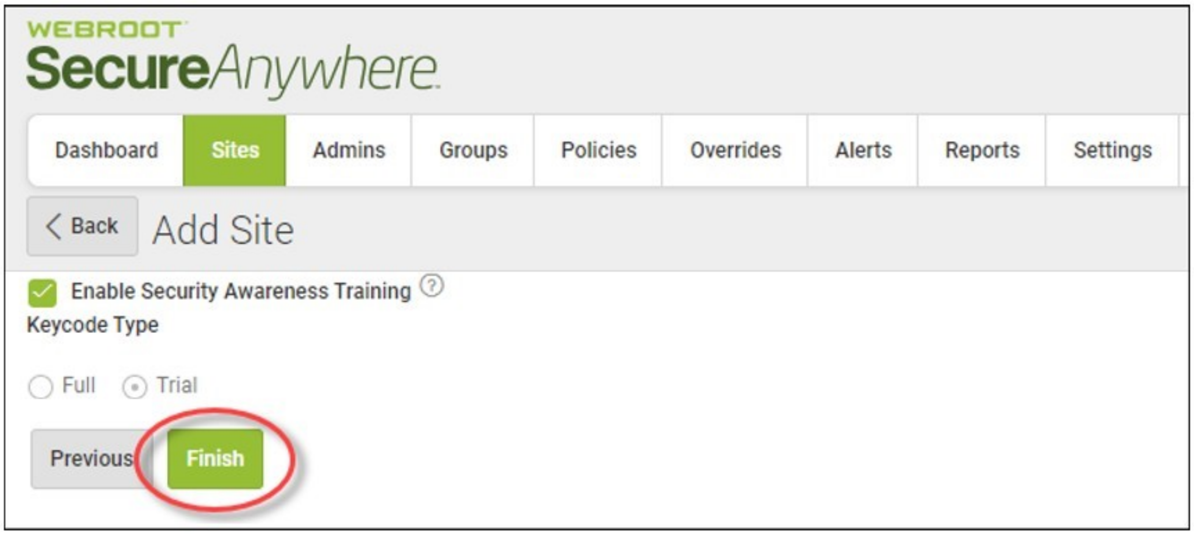


3. Check the box to Enable Security Awareness Training



□ Enable Security Awareness Training

4. Under **Keycode Type**, select either **Full** or **Trial**, then click **Finish**.



☑ Enable Security Awareness Training

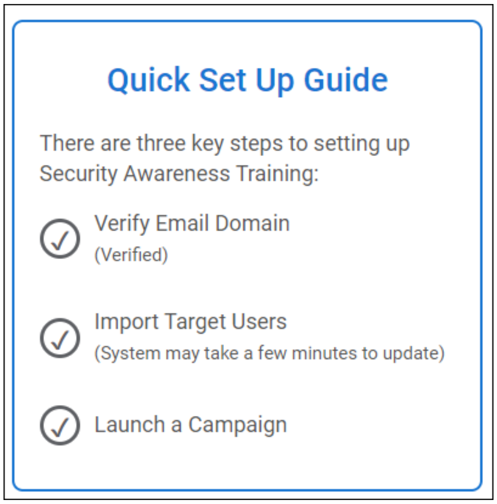
Keycode Type

○ Full ● Trial

Authorizing Test/Target Domain

Once you have enabled Security Awareness Training, you need to establish the domain for which you will add email targets. Without this step, you cannot proceed.

- **Authorized Domain Address**
  This is your own address on your organization's domain. When you add an Authorized Domain address, you will receive an email with a validation link. Click that link to verify that you can access that email box and have an account on your organization's domain. This will allow you to import any target email addresses on that domain.
- **Target Email Address**
  These are the email addresses belonging to your organization's employees/users which will be targeted in your simulation. These are necessary for the simulation to deliver bait emails. You can use the quick setup wizard to guide you through these steps.



Quick Set Up Guide

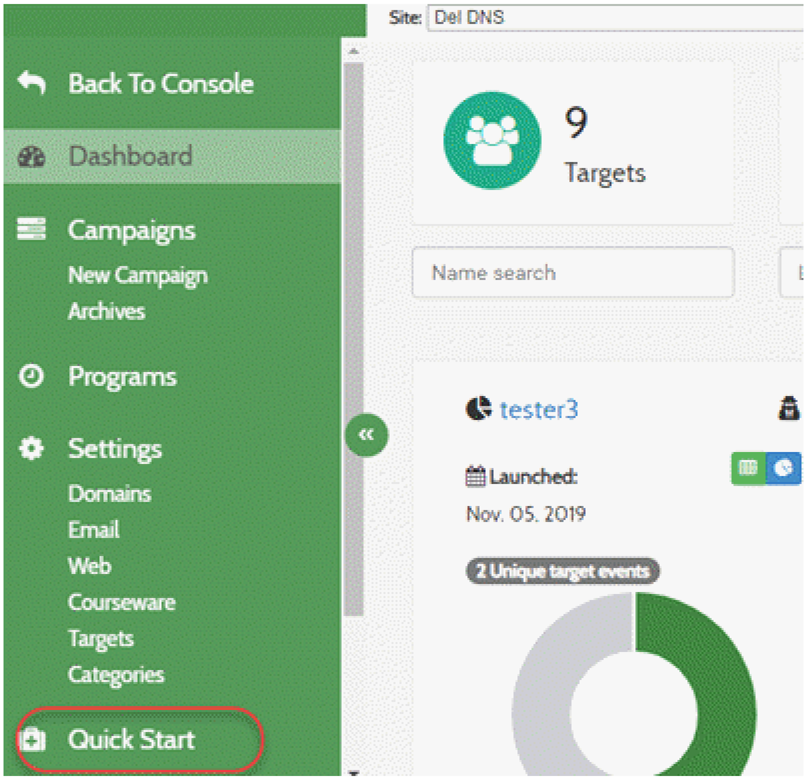
There are three key steps to setting up Security Awareness Training:

✓ Verify Email Domain
(Verified)

✓ Import Target Users
(System may take a few minutes to update)

✓ Launch a Campaign

1. Return to the Sites tab and click the Go to Security Awareness Training icon ↗.
2. In the Site Console, click **Quick Start** and follow the steps.



First Campaign

Consider starting your Security Awareness Training program with a phishing campaign. You can use your first phishing campaign to establish a baseline and gauge how susceptible your end users are to phishing, in addition to their general level of security awareness.

The Webroot Security Awareness Training console contains a variety of template options for your first campaign. We recommend choosing a template that mimics an internal communication from HR or the IT department to help get the most eyes on the email.

We also recommend you use Webroot’s 404 broken link template so that users who fall for the fake phish do not realize they were being tested and spread the word. By minimizing the amount of water cooler talk about a phishing simulation, you’ll get a more accurate baseline reading.

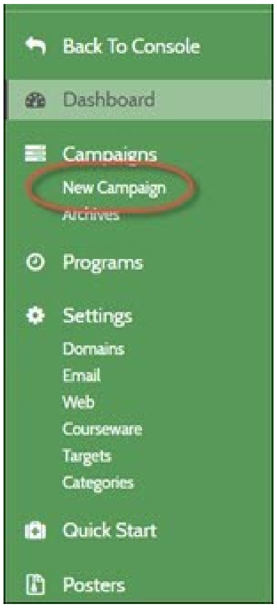
After that, be sure to link your phishing campaigns to training pages and courses to maximize the training opportunity and consider changing phishing templates by job role to create an effective phishing program.

How to Start a New Campaign from the Site Console

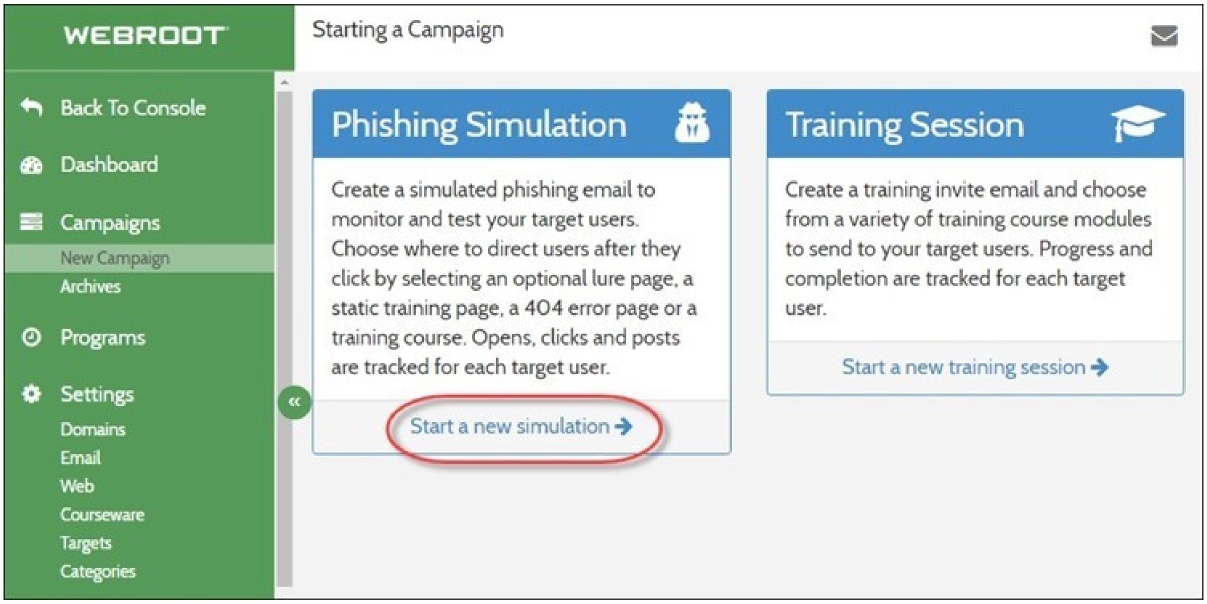
In this example, we'll show you how to create your first campaign in the Customer/Sites Console with our easy-to-use 5-step process. It will send any user that clicks on a link in the phishing email directly to a landing page with an info-graphic on phishing.

To get started, click the Go to Security Awareness Training icon for the desired site ↗**.**

Click **New Campaign** in the left navigation bar.



Part 1: Click **Start a new simulation** to open the **New Campaign Wizard**



Starting a Campaign

Phishing Simulation

Create a simulated phishing email to monitor and test your target users. Choose where to direct users after they click by selecting an optional lure page, a static training page, a 404 error page or a training course. Opens, clicks and posts are tracked for each target user.

Start a new simulation →

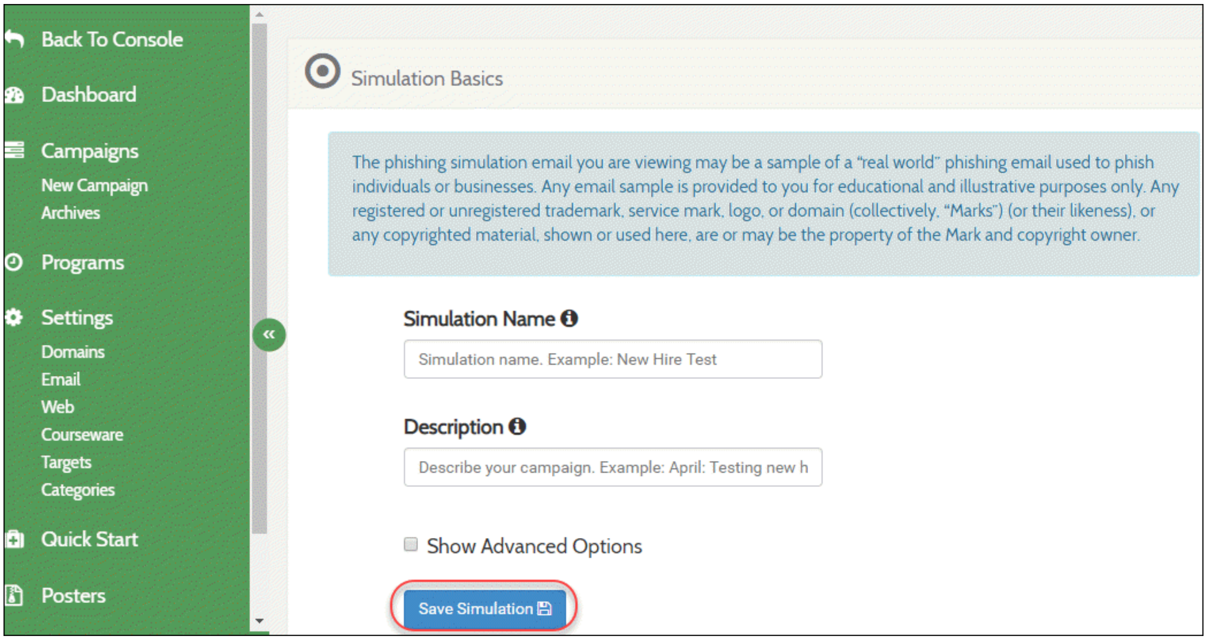
Training Session

Create a training invite email and choose from a variety of training course modules to send to your target users. Progress and completion are tracked for each target user.

Start a new training session →

In the **Simulation Basics** window, populate the following fields:

- **Simulation Name:** enter a name for your simulation
- **Description:** Enter a description for your simulation. This is optional.



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

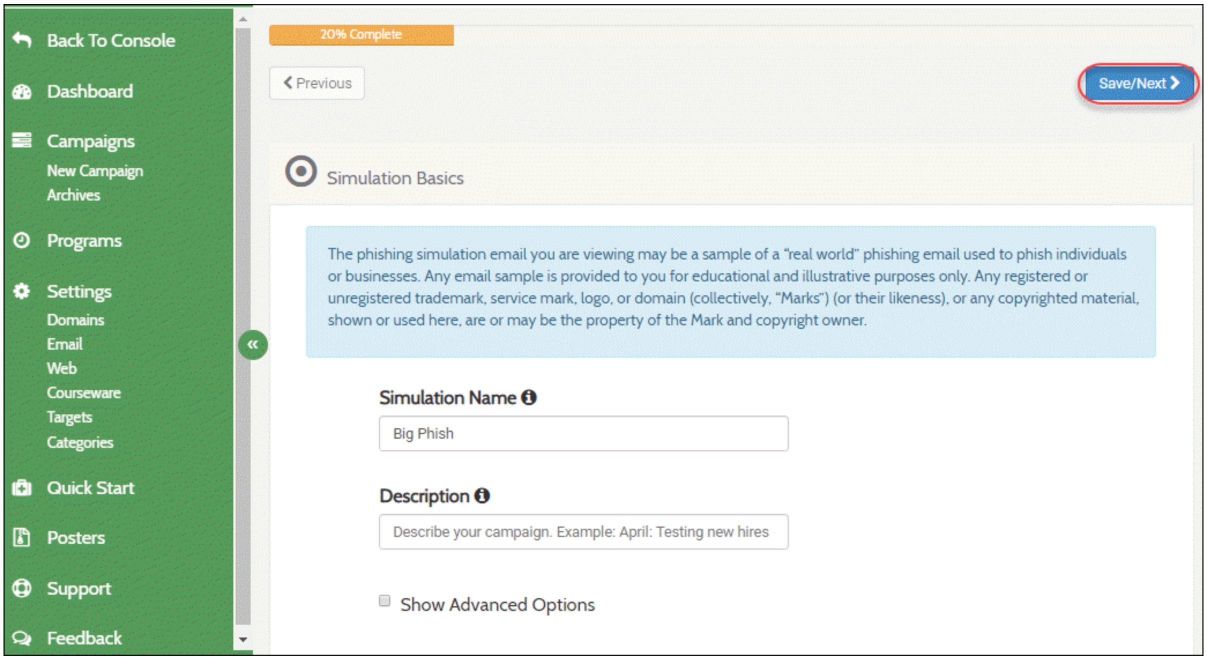
Describe your campaign. Example: April: Testing new h

□ Show Advanced Options

Save Simulation

Click **Save Simulation**.

When you are ready, click **Save/Next**, and the Targets window displays with the **Targets** tab active.



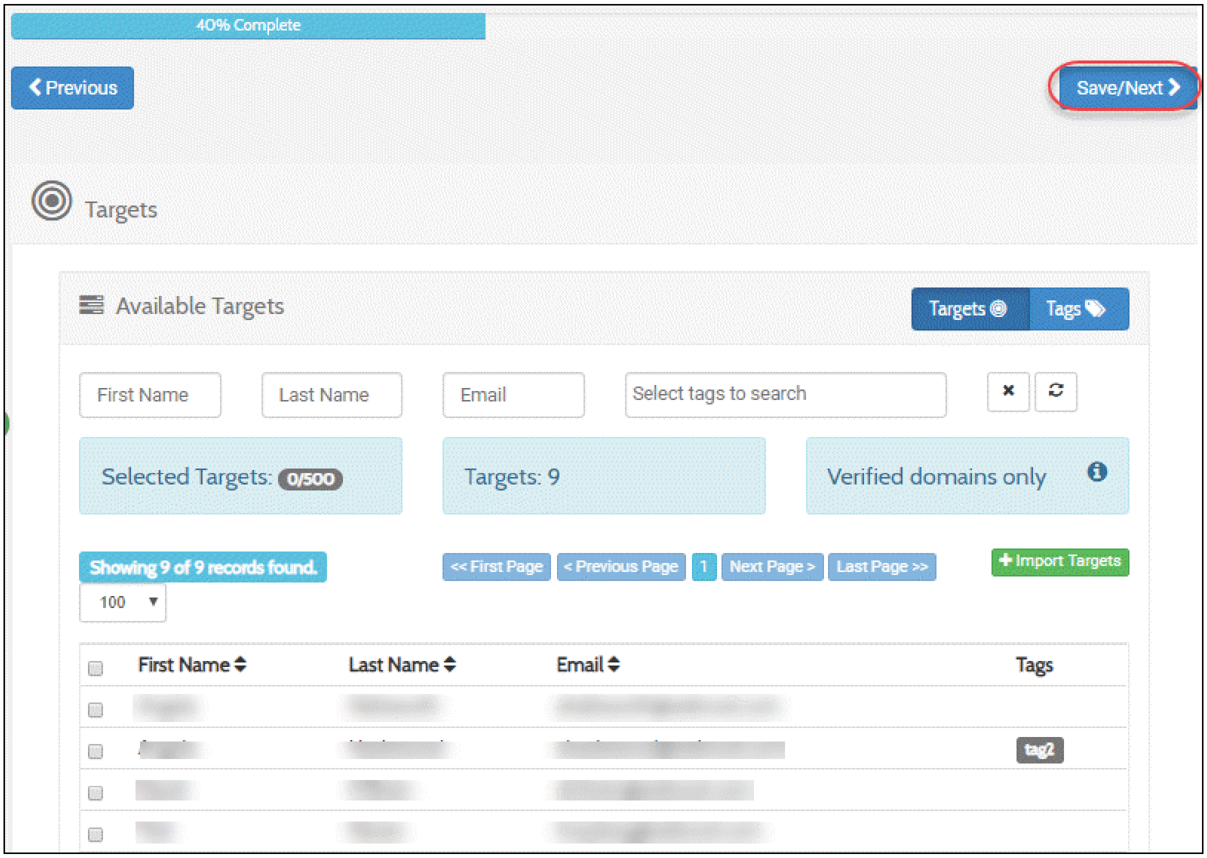
The phishing simulation email you are viewing may be a sample of a "real world" phishing email used to phish individuals or businesses. Any email sample is provided to you for educational and illustrative purposes only. Any registered or unregistered trademark, service mark, logo, or domain (collectively, "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: Big Phish

Description: Describe your campaign. Example: April: Testing new hires

□ Show Advanced Options

Part 2: Select one or more users by selecting the check box next to their name, and click **Save/Next.**



□	First Name	Last Name	Email	Tags
□	[redacted]	[redacted]	[redacted]	
□	[redacted]	[redacted]	[redacted]	tag2
□	[redacted]	[redacted]	[redacted]	
□	[redacted]	[redacted]	[redacted]	

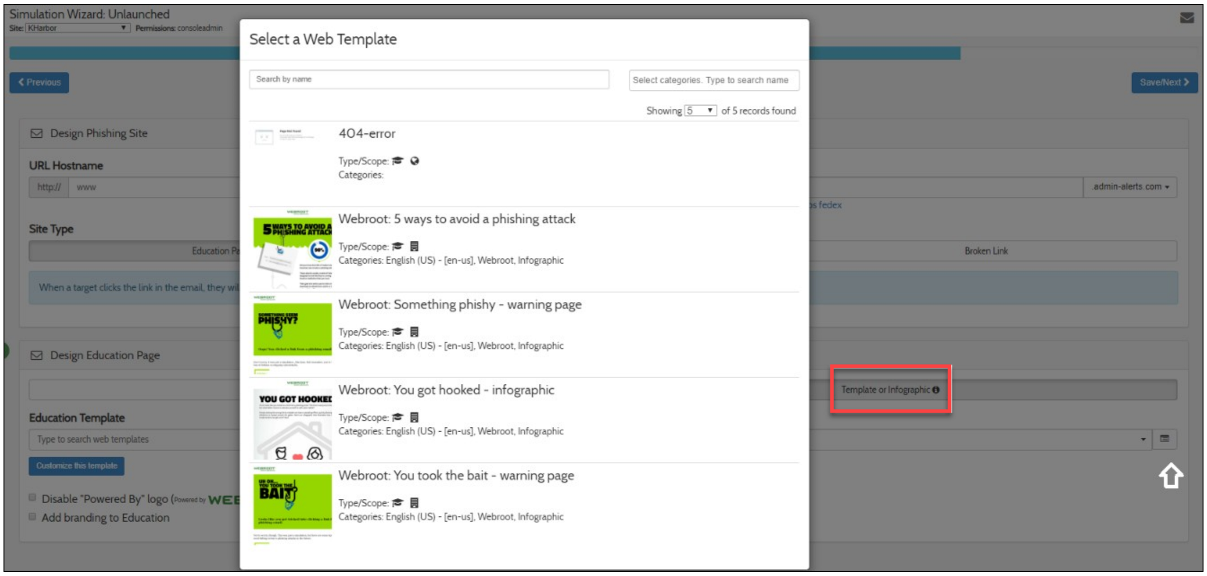
Part 3: In the Email Template drop-down menu, select a Phishing Email Template, and once you've created your phishing email, click **Save/Next**.

In the URL Hostname field, do either of the following:

- Enter a fake URL name.
- Choose one of the suggested URL types.

Part 4: Select your landing page (in this example, it will be an infographic).
When a target clicks the link in the email, they will be taken directly to the education page, which will provide

an infographic about phishing.



Select a Web Template

Search by name

Select categories. Type to search name

Showing 5 of 5 records found

404-error
Type/Scope:
Categories:

Webroot: 5 ways to avoid a phishing attack
Type/Scope:
Categories: English (US) - [en-us], Webroot, Infographic

Webroot: Something phishy - warning page
Type/Scope:
Categories: English (US) - [en-us], Webroot, Infographic

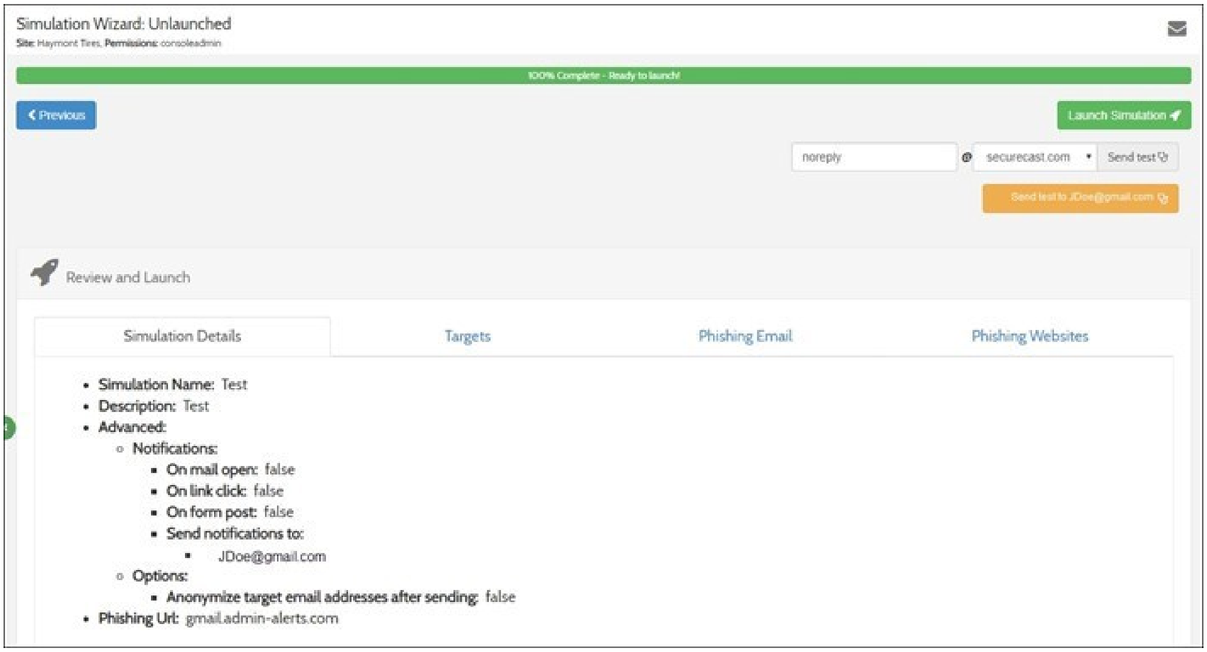
Webroot: You got hooked - infographic
Type/Scope:
Categories: English (US) - [en-us], Webroot, Infographic

Webroot: You took the bait - warning page
Type/Scope:
Categories: English (US) - [en-us], Webroot, Infographic

Click **Save/Next**.

Part 5: Before you launch the training, it is recommended that you do the following:

- Review your campaign settings.
- Send a test invitation to yourself to ensure you are satisfied with the look and feel of the phishing email and education landing page, then launch the simulation when ready.


Simulation Wizard: Unlaunched

Site: Haymont Tires, **Permissions:** consoleadmin

100% Complete - Ready to launch!

- **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

Congratulations, you have now completed your first campaign!

Note: Depending on the needs of each organization, you may want to increase the frequency and adjust intervals throughout the year.

We recommend you use the Program Scheduling feature to combine and schedule campaign training sessions and set up a continuous cybersecurity training program. With the program scheduling feature, you can choose to schedule one or many Welcome Emails, Phishing Simulations, and Training Courses. Plus, you can add in a follow-up campaign summary report to automate your entire training program.

Start your first program

Click the **Programs** menu in the left navigation bar.

Click **Create a program**. The New Program Form displays. This is where you create your programs. Complete the program name and description.

Under Available Tasks, there are three tasks you can perform in any order to create your training program schedule.

- Welcome Email
- Phishing Campaign
- Training Campaign

Welcome Email

You can decide to send a welcome email at the beginning of training as an introduction to a Phishing Campaign or Training Campaign.

To add a Welcome Email, click **Welcome Email**. Enter a task name, set a date for the email, select an email template, and then select the recipients.

Phishing Campaign

You can decide to include any of your phishing campaigns in a program.

To add a Phishing Campaign, click **Phishing Campaign**. Enter a task name, select one of your Phishing Campaigns from the drop-down menu, set a start and end date, and then choose the recipients.

Training Campaign

You can choose to include any of your Training campaigns in a program.

To add a Training Campaign, click **Training Campaign**. Enter a task name, select one of your Training Campaigns from a drop-down menu, set a start and end date, and then choose the recipients.

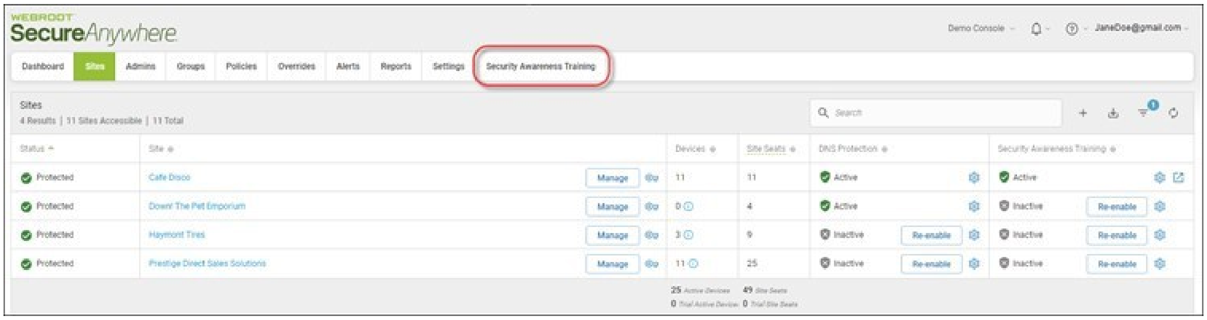
> **Note:** You can choose to send an optional report to additional email addresses using the Email Reports section at the bottom of the screen.

By adding welcome emails, phishing campaigns, and training campaigns over a scheduled time frame, you can build full training programs for your end users.

How to Start a New Campaign from the Management Console

In this example, we'll show you how to create your first campaign in the Management Console with our easy-to-use 5-step process. It will send any user that clicks on a link in the phishing email directly to a landing page with an infographic on phishing.

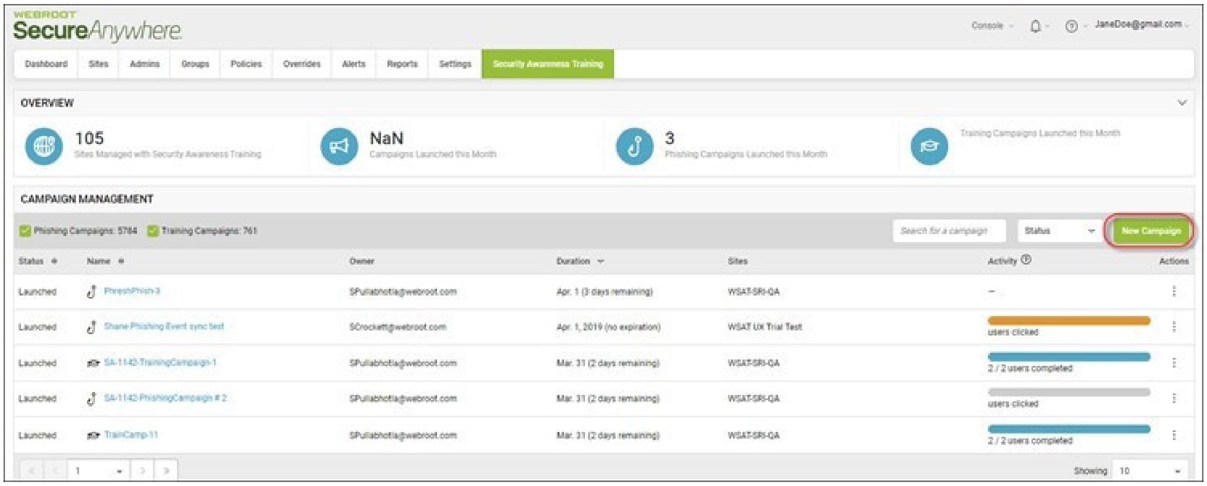
Open the **Security Awareness Training** tab.



Sites
4 Results | 11 Sites Accessible | 11 Total

Status	Site	Devices	Site Seats	DNS Protection	Security Awareness Training
Protected	Cafe Disco	11	11	Active	Active
Protected	Down' The Pet Emporium	0	4	Active	Inactive
Protected	Haymont Tires	3	9	Inactive	Inactive
Protected	Prestige Direct Sales Solutions	11	25	Inactive	Inactive
		25 Active Devices 0 Trial Active Devices	49 Site Seats 0 Trial Site Seats		

Part 1: Click **New Campaign**.



OVERVIEW

105 Sites Managed with Security Awareness Training

NaN Campaigns Launched this Month

3 Phishing Campaigns Launched this Month

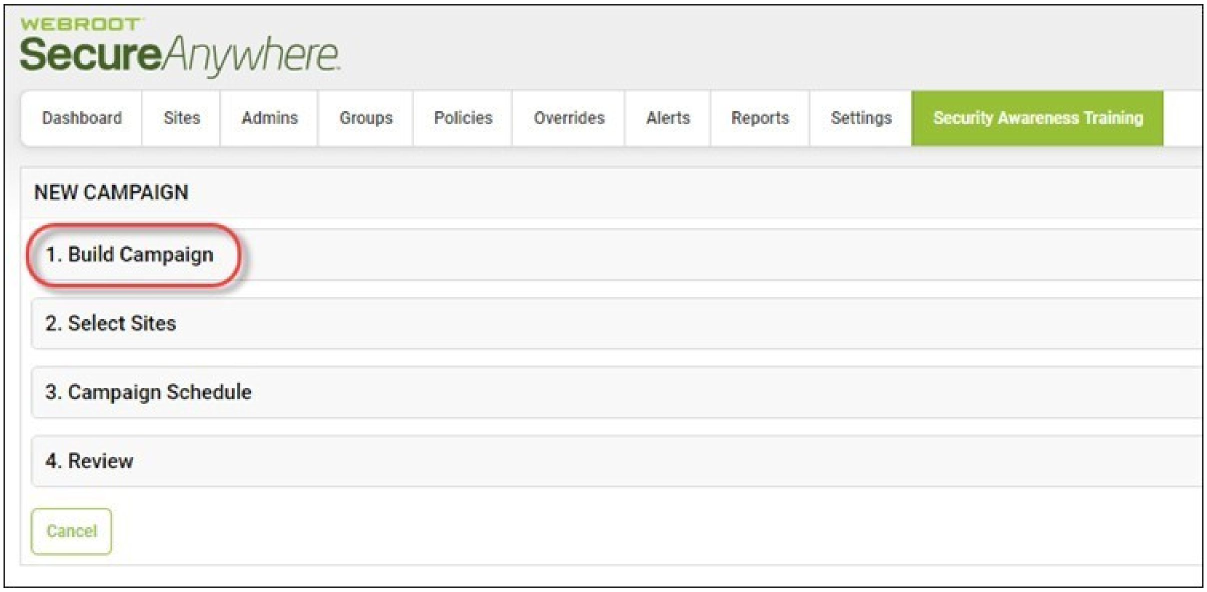
Training Campaigns Launched this Month

CAMPAIGN MANAGEMENT

☑ Phishing Campaigns: 5784 ☑ Training Campaigns: 761

Status	Name	Owner	Duration	Sites	Activity	Actions
Launched	PhreshPhish-3	SPullabhotla@webroot.com	Apr. 1 (3 days remaining)	WSAT-SRI-QA	–	⋮
Launched	Shane Phishing Event sync test	SCrockett@webroot.com	Apr. 1, 2019 (no expiration)	WSAT UX Trial Test	users clicked	⋮
Launched	SA-1142-TrainingCampaign-1	SPullabhotla@webroot.com	Mar. 31 (2 days remaining)	WSAT-SRI-QA	2 / 2 users completed	⋮
Launched	SA-1142-PhishingCampaign # 2	SPullabhotla@webroot.com	Mar. 31 (2 days remaining)	WSAT-SRI-QA	users clicked	⋮
Launched	TrainCamp-11	SPullabhotla@webroot.com	Mar. 31 (2 days remaining)	WSAT-SRI-QA	2 / 2 users completed	⋮

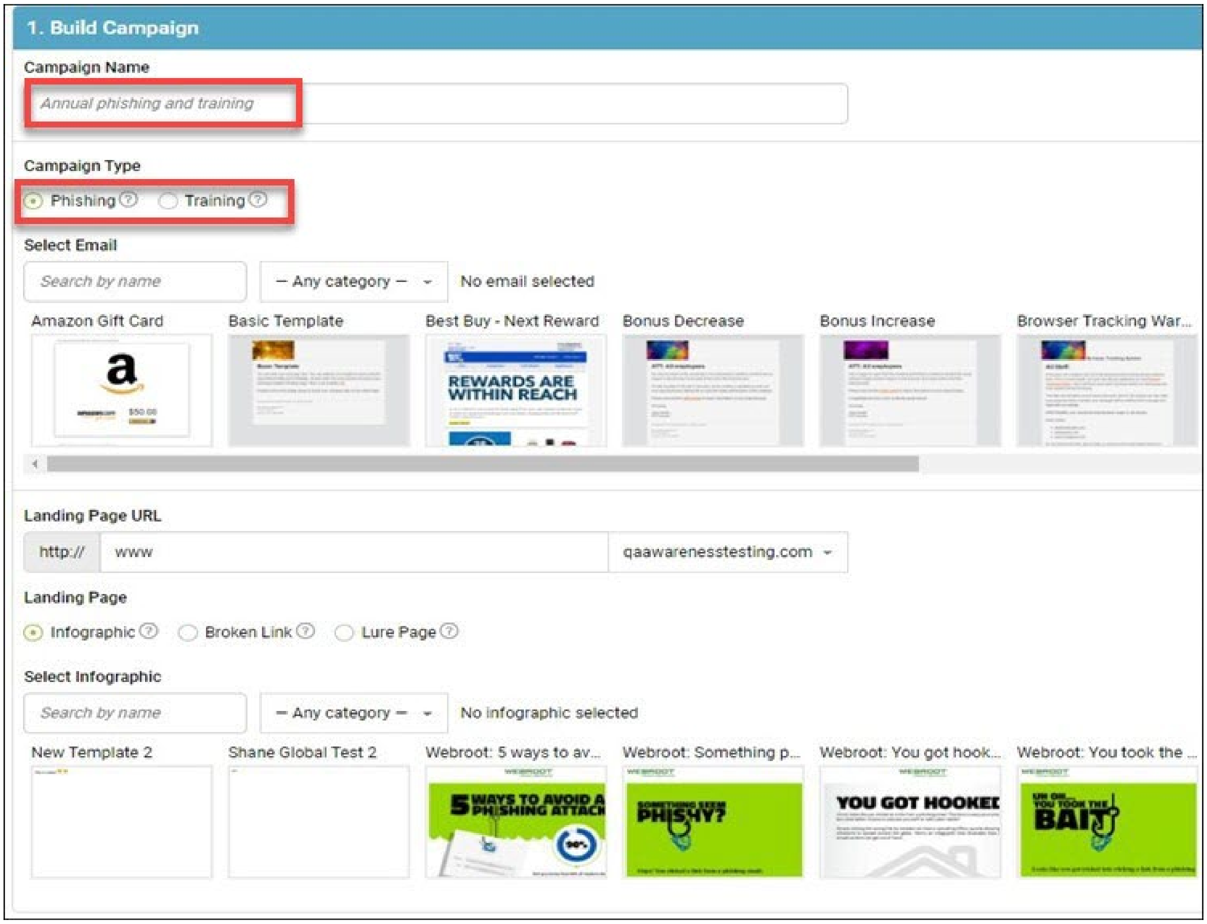
Part 2: Click **Build Campaign**.



NEW CAMPAIGN

1. Build Campaign
2. Select Sites
3. Campaign Schedule
4. Review

Enter a name for the campaign in the **Campaign Name** field.



1. Build Campaign

Campaign Name

Annual phishing and training

Campaign Type

● Phishing ○ Training

Select Email

Search by name | – Any category – | No email selected

Landing Page URL

http:// www qaawarenesstesting.com

Landing Page

● Infographic ○ Broken Link ○ Lure Page

Select Infographic

Search by name | – Any category – | No infographic selected

Under **Campaign Type**, select **Phishing**.

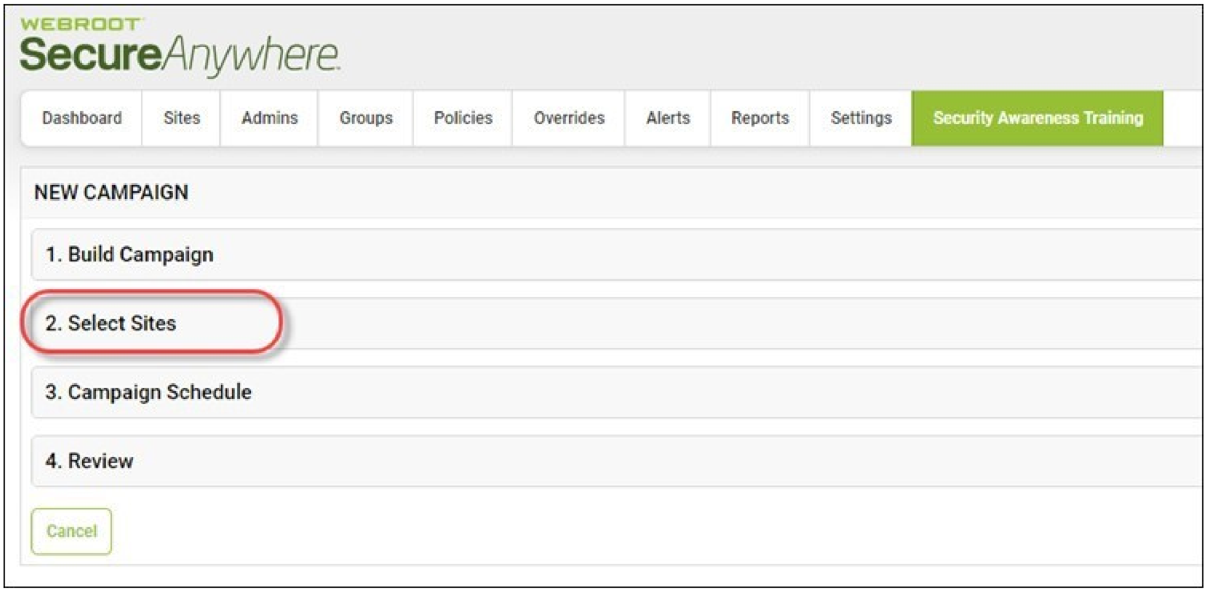
Select and email template by:

- Entering the name of the template
- Selecting a template from the **Any Category** drop-down menu.
- Using the slider to see and select the email template you want to use.

In the Landing Page URL drop-down menu, select the URL you want to use for your landing page.

- Select an infographic email template either by entering the name, selecting a category, or using the slider.

Part 3: Click **Select Sites**.



NEW CAMPAIGN

1. Build Campaign

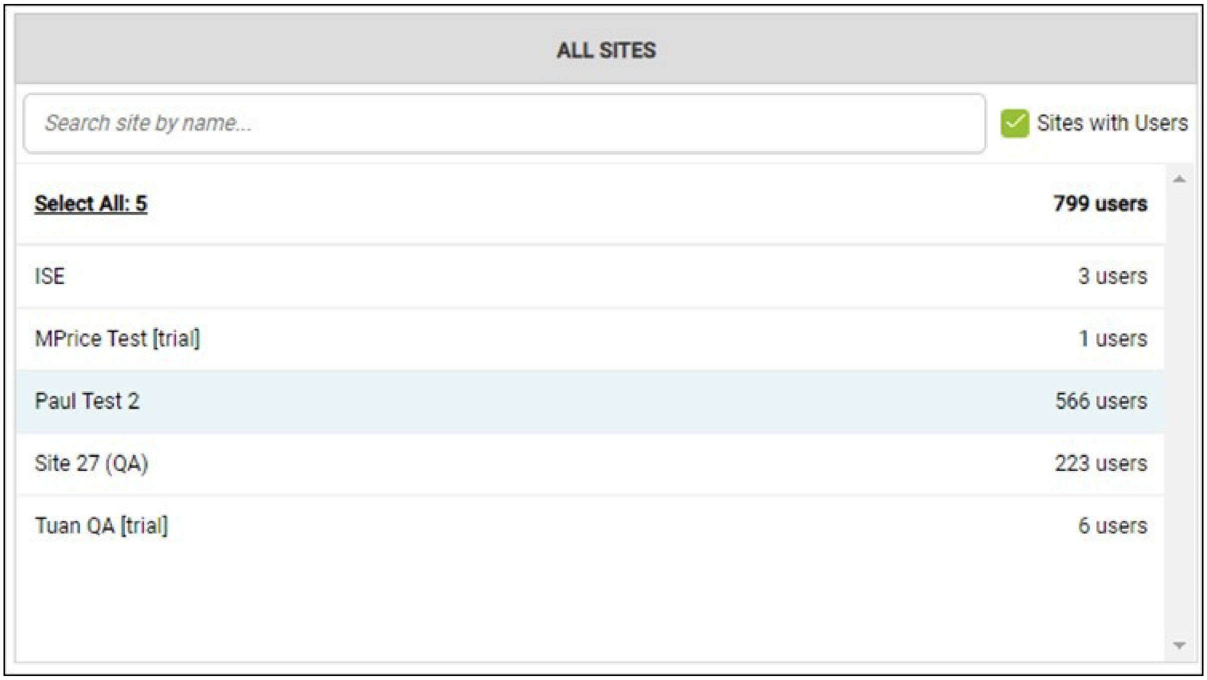
2. Select Sites

3. Campaign Schedule

4. Review

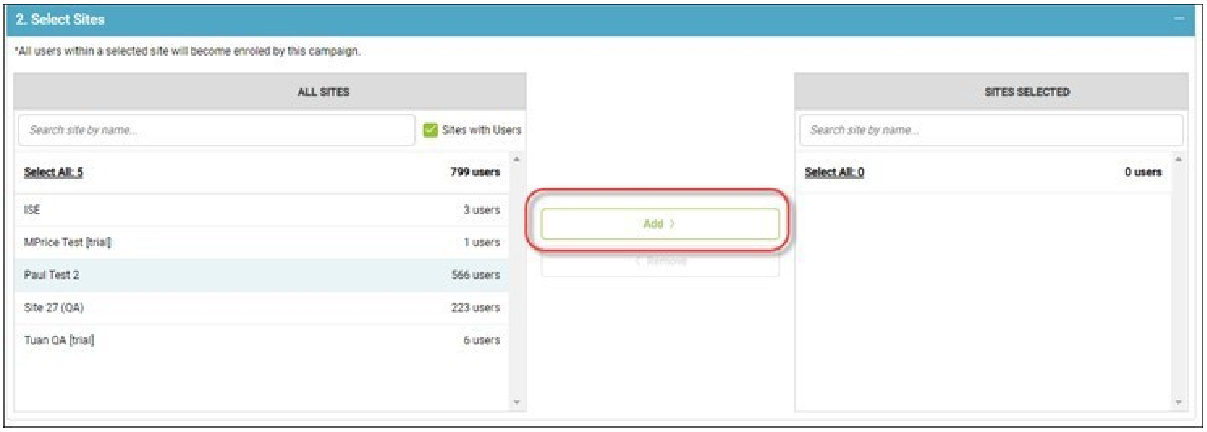
Do either of the following to select the site:

- Enter all or part of the site name, and then click the name of the site to select it.
- Click the name of one or more sites in the list so that they are highlighted.


ALL SITES

Select All: 5	**799 users**
ISE	3 users
MPrice Test [trial]	1 users
Paul Test 2	566 users
Site 27 (QA)	223 users
Tuan QA [trial]	6 users

When you have selected the site(s) you want to send a campaign to, click Add to move those sites to the Sites Selected column.



2. Select Sites

*All users within a selected site will become enroled by this campaign.

ALL SITES

Search site by name...

☑ Sites with Users

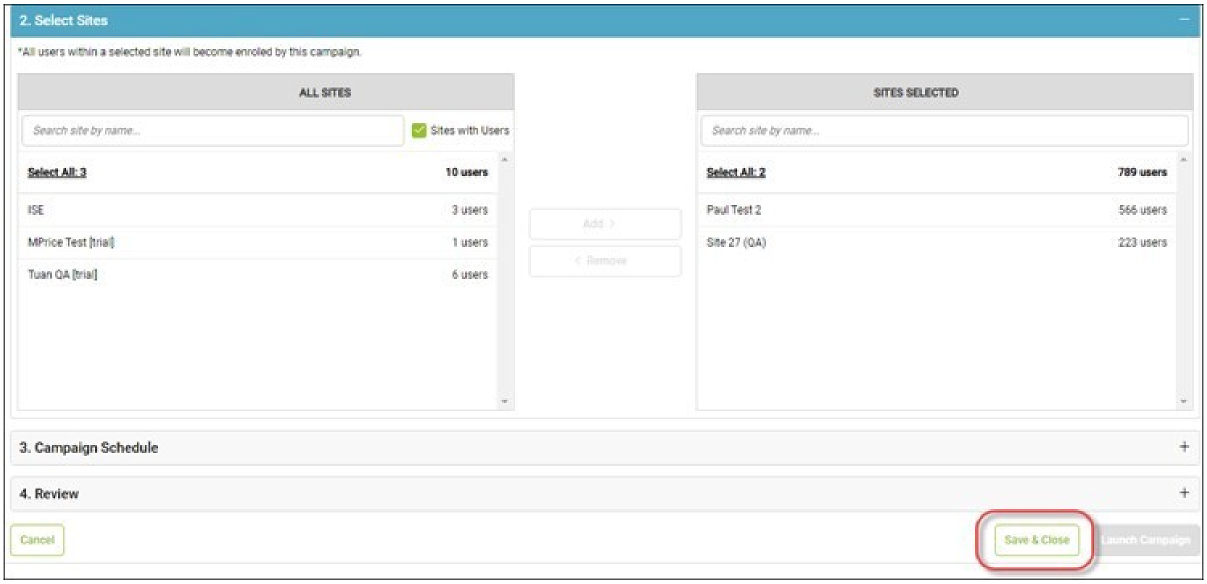
Select All: 5	799 users
ISE	3 users
MPrice Test [trial]	1 users
Paul Test 2	566 users
Site 27 (QA)	223 users
Tuan QA [trial]	6 users

SITES SELECTED

Search site by name...

Select All: 0	0 users

When you're finished, click **Save & Close**.



2. Select Sites

*All users within a selected site will become enroled by this campaign.

ALL SITES

Search site by name...

☑ Sites with Users

Select All: 3	10 users
ISE	3 users
MPrice Test [trial]	1 users
Tuan QA [trial]	6 users

SITES SELECTED

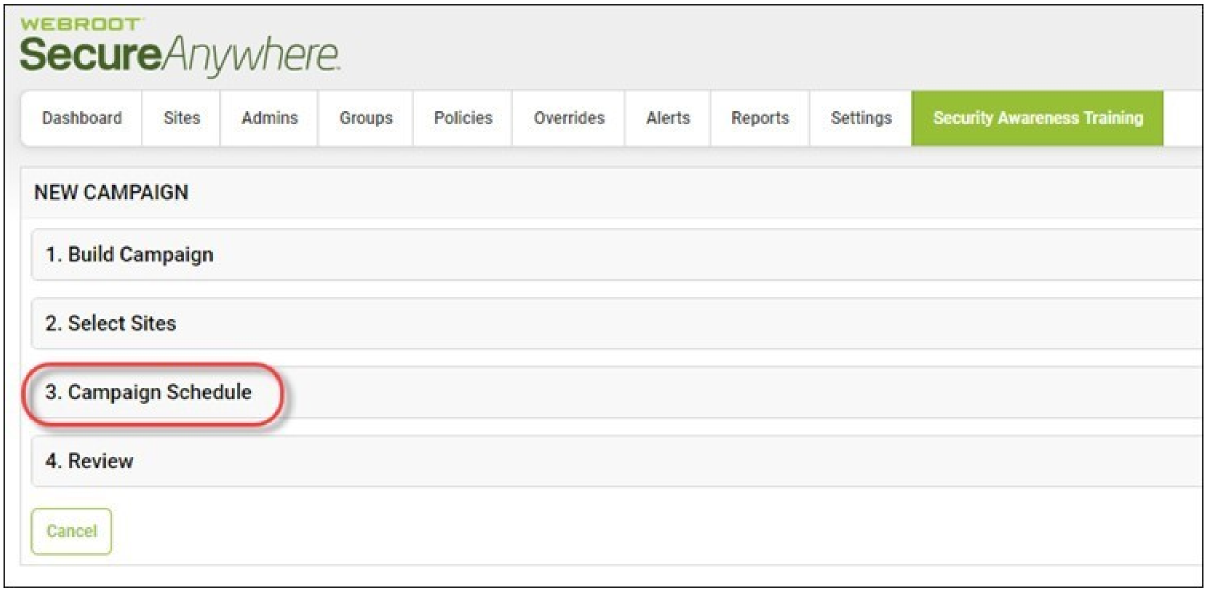
Search site by name...

Select All: 2	789 users
Paul Test 2	566 users
Site 27 (QA)	223 users

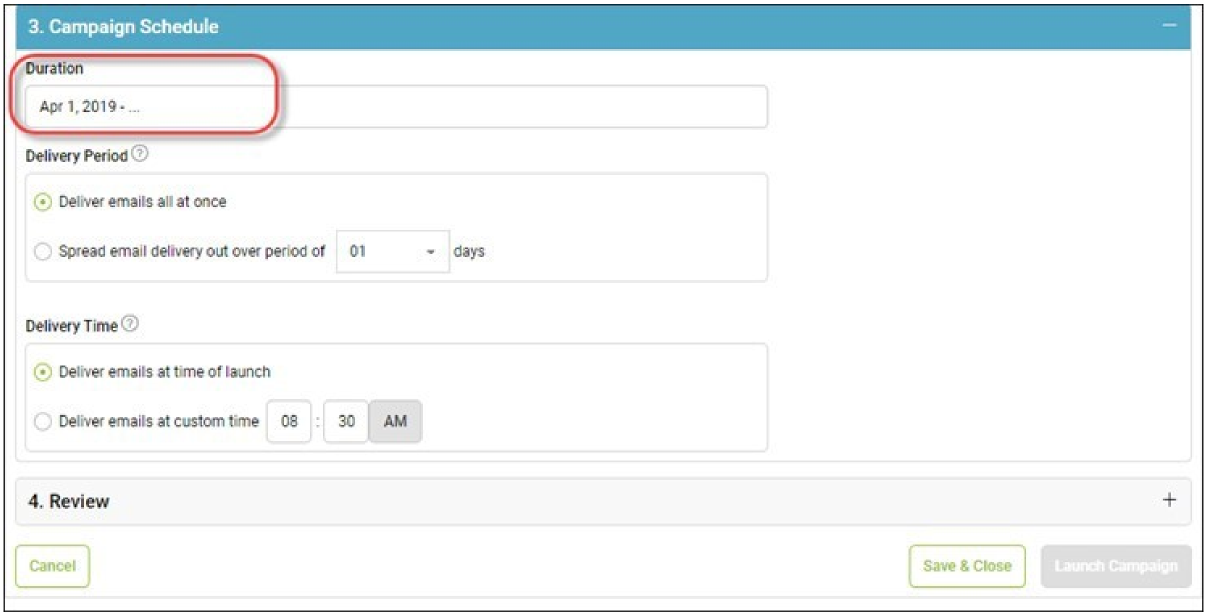
3. Campaign Schedule

4. Review

Part 4: Click **Campaign Schedule.**



In the **Duration** field, enter the date range for the campaign.


3. Campaign Schedule

Duration: Apr 1, 2019 - ...

Delivery Period

● Deliver emails all at once

○ Spread email delivery out over period of 01 days

Delivery Time

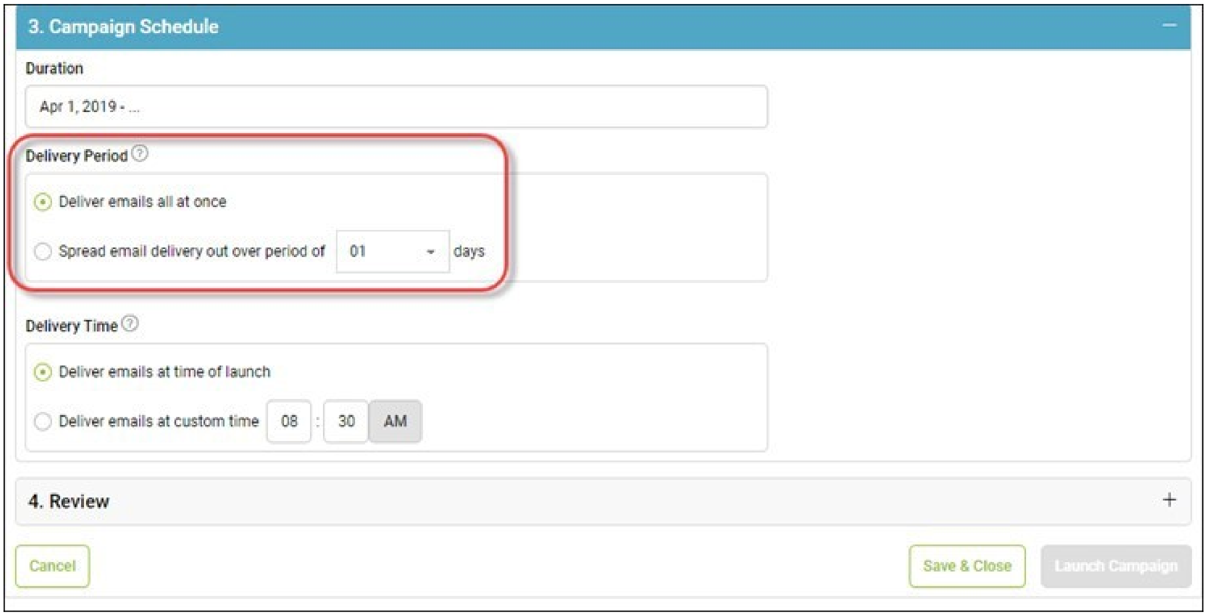
● Deliver emails at time of launch

○ Deliver emails at custom time 08 : 30 AM

In the Delivery Period area, select one of the following options:

- **Deliver emails all at once.**

- **Spread email delivery out over period of days**, then use the drop-down menu to select the number of days over which to spread email delivery.



3. Campaign Schedule

Duration

Apr 1, 2019 - ...

Delivery Period

● Deliver emails all at once

○ Spread email delivery out over period of 01 days

Delivery Time

● Deliver emails at time of launch

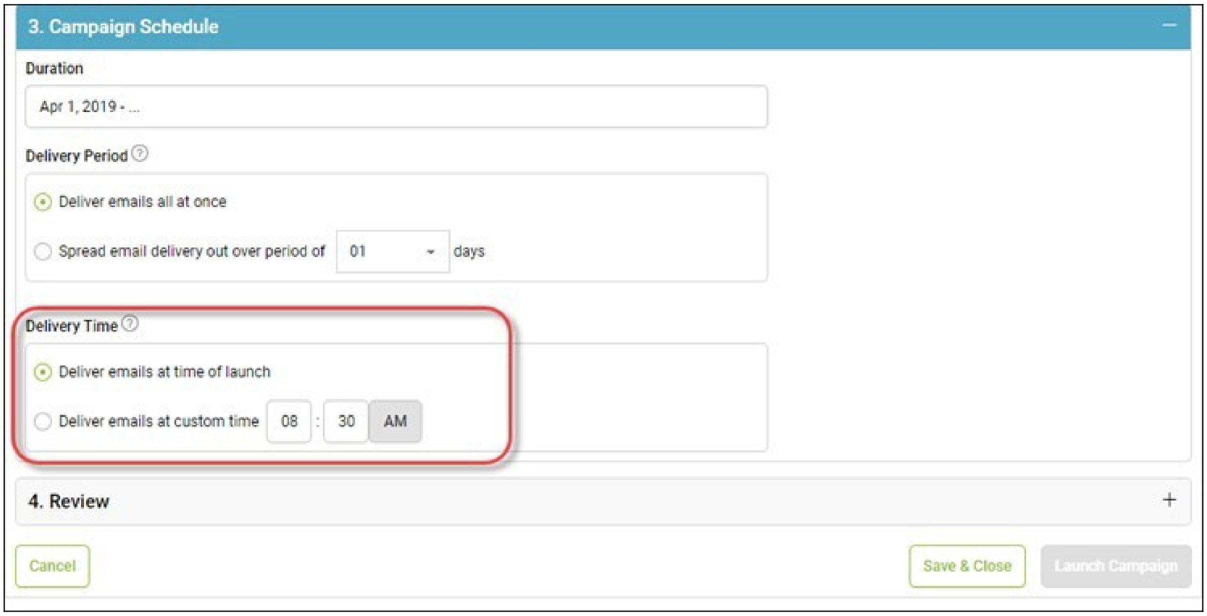
○ Deliver emails at custom time 08 : 30 AM

4. Review

In the Delivery Time area, select one of the following options:

- **Deliver emails at time of launch**.

- **Deliver emails at custom time**, then enter the time you want the emails to be delivered.



3. Campaign Schedule

Duration

Apr 1, 2019 - ...

Delivery Period

● Deliver emails all at once

○ Spread email delivery out over period of 01 days

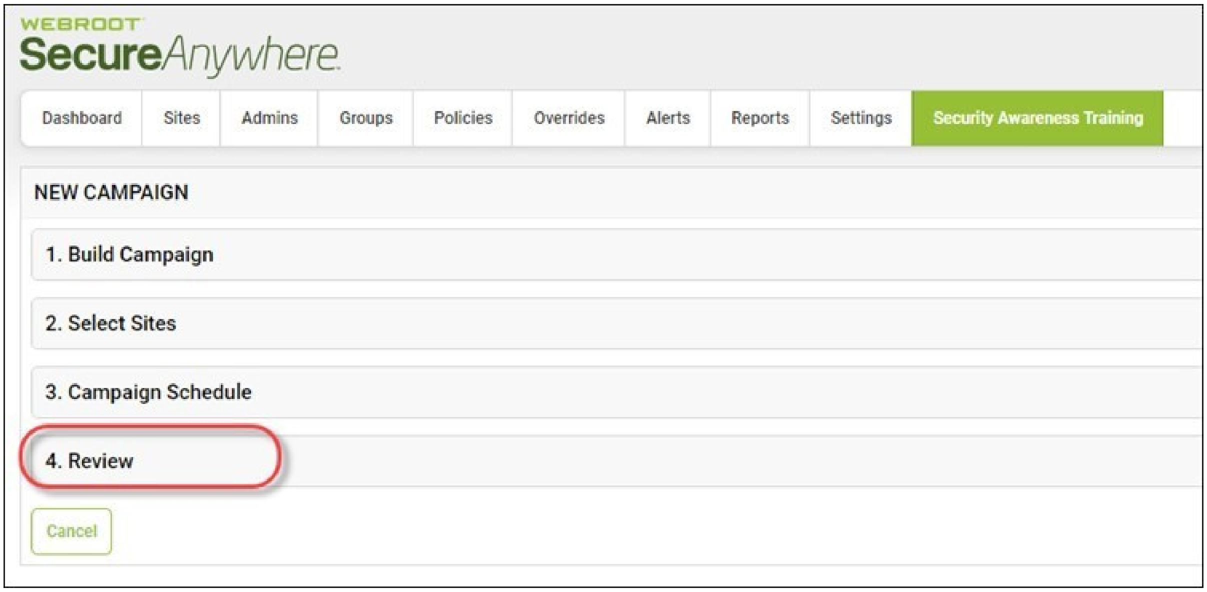
Delivery Time

● Deliver emails at time of launch

○ Deliver emails at custom time 08 : 30 AM

4. Review

Part 5: Click **Review**.



NEW CAMPAIGN

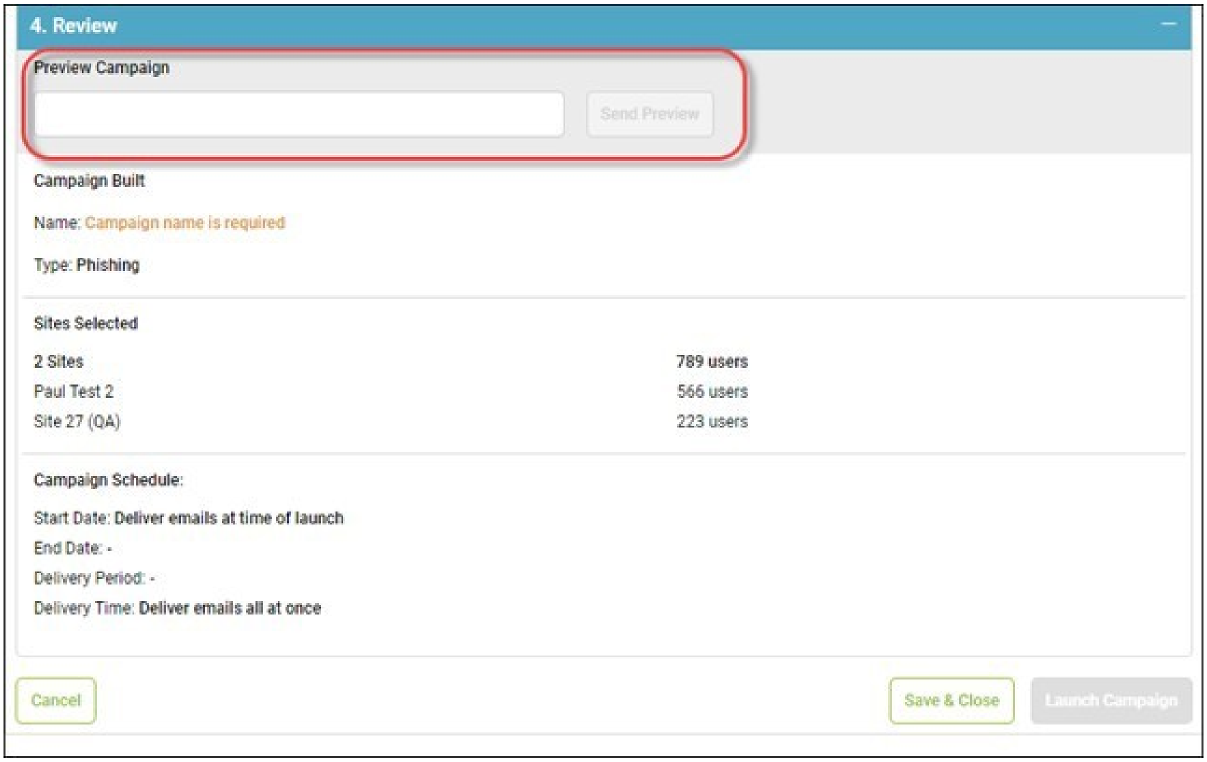
1. Build Campaign

2. Select Sites

3. Campaign Schedule

4. Review

In the **Preview Campaign** field, enter the email address of the person who will preview the campaign and click **Send Preview**.



Campaign Built

Name: Campaign name is required

Type: Phishing

Sites Selected

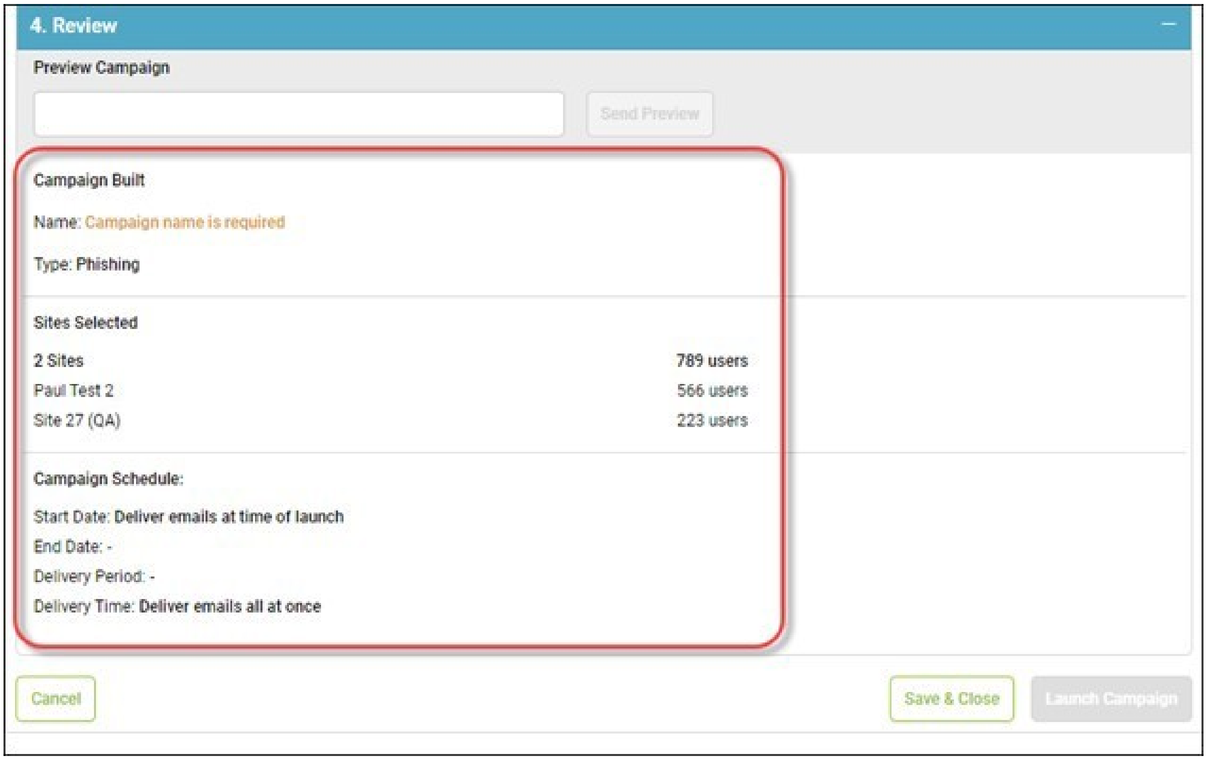
2 Sites	789 users
Paul Test 2	566 users
Site 27 (QA)	223 users

Campaign Schedule:

Start Date: Deliver emails at time of launch
End Date: -
Delivery Period: -
Delivery Time: Deliver emails all at once

Review the campaign information such as:

- Campaign build
- Sites Selected
- Campaign Schedule



Campaign Built

Name: Campaign name is required

Type: Phishing

Sites Selected

2 Sites	789 users
Paul Test 2	566 users
Site 27 (QA)	223 users

Campaign Schedule:

Start Date: Deliver emails at time of launch

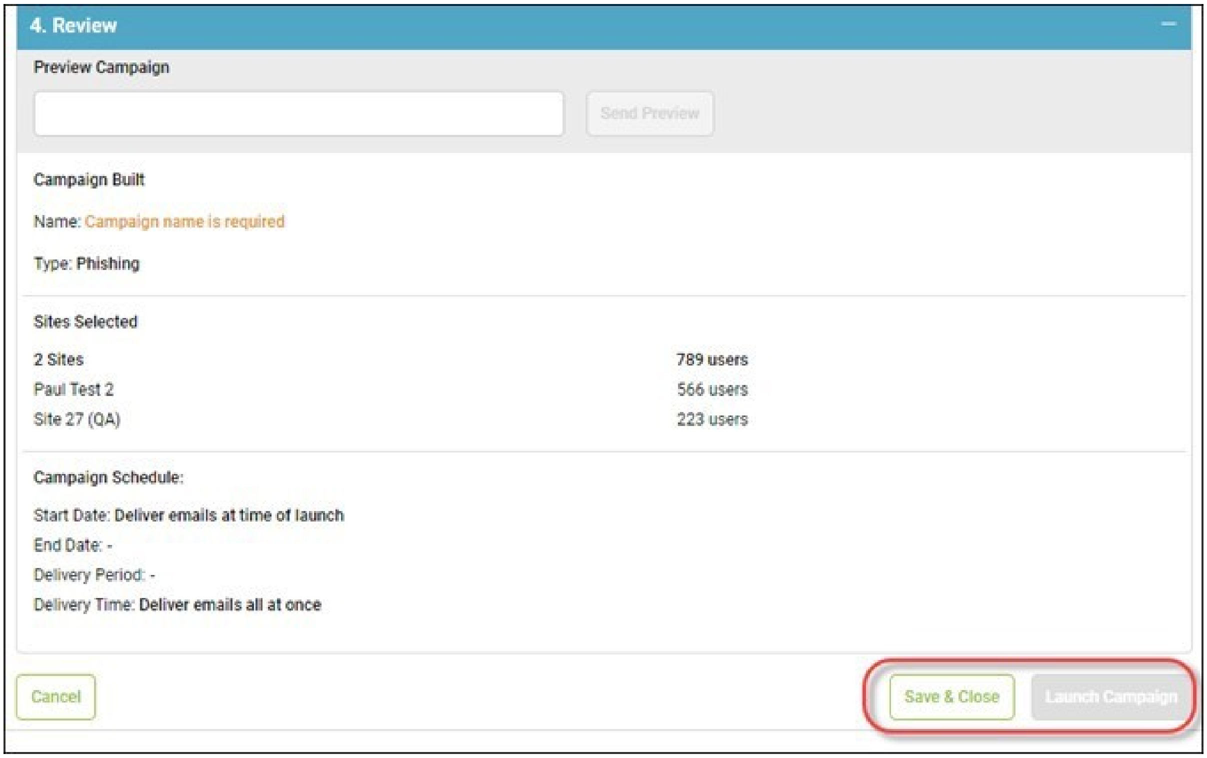
End Date: -

Delivery Period: -

Delivery Time: Deliver emails all at once

At this point, you can:

- Click **Save & Close** to review again later, or wait for additional information.
- Click **Launch Campaign** to launch the campaign.



Preview Campaign

Campaign Built

Name: Campaign name is required

Type: Phishing

Sites Selected

2 Sites	789 users
Paul Test 2	566 users
Site 27 (QA)	223 users

Campaign Schedule:

Start Date: Deliver emails at time of launch
End Date: -
Delivery Period: -
Delivery Time: Deliver emails all at once

Measuring Effectiveness

To help you measure the effectiveness of your training efforts and adjust them to suit your business needs, we provide Campaign Reports.

Campaign Reports have two main purposes:

1. To demonstrate the value of training by showing the results of each campaign over time
2. To help you identify users who may require extra training or attention

As with any educational approach, not all people absorb information in the same way or at the same rate. For users who need extra attention, you might consider increasing the training frequency.

In addition, Campaign Reports help you show the value security awareness training offers, quantify the return on investment to management, and, for managed service providers, to your clients as well.

Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Look for the answer in our knowledgebase.
- Look for the answer in our online documentation.
- Enter a help ticket .
- Connect to the Webroot Online Business Forum.

Index