WEBROOT®

Security Awareness Training
Getting Started Guide

Copyright

Security Awareness Training Getting Started Guide

Table of Contents

Chapter 1: Security Awareness Training Getting Started Guide *1*

Security Awareness Training Getting Started Guide Overview *2*

Chapter 2: Enabling Webroot Security Awareness Training *3*

Enabling Security Awareness Training Overview *4*
Verifying the Product is Active *5*
Adding Security Awareness Training to Sites *6*
Opening the Security Awareness Training Console *8*
Verifying Your Company's Email Domain *9*
Importing Users Emails As Targets *11*

Chapter 3: Using Security Awareness Training *13*

Using Security Awareness Training Overview *14*
About Campaigns *14*
Creating Phishing Campaigns *15*
Step 1 — Simulation Basics *15*
Step 2 — Available Targets *16*
Step 3 — Design Phishing Email *16*
Step 4 — Design Phishing Site *16*
Step 5 — Review and Launch *17*
Creating Training Campaigns *18*
Creating Your First Training Campaign *18*
Step 1 — Training Session Basics *18*
Step 2 — Available Targets *19*
Step 3 — Design Invitation Email *19*
Step 4 — Design Education Page *19*
Step 5 — Review and Launch *19*
Assembling Training Programs *21*
New Program Form *22*
Welcome Email *22*
Phishing Campaign *22*
Training Campaign *22*
Whats Next? *24*

Chapter 4: Security Awareness Training Support *25*

Accessing Technical Support *26*

Index ..... *i*

Chapter 1: Security Awareness Training Getting Started Guide

To get started using the DNS Protection Getting Started guide, see the following topics:

Security Awareness Training Getting Started Guide Overview *2*

Security Awareness Training Getting Started Guide Overview

Webroot Security Awareness Training (WSAT) trains your workforce against cybercriminals who target end users. Security Awareness Training has two main functions:

- Simulate phishing attacks by sending mock phishing emails and identifying susceptible users who click on the phishing link.
- Train users on cybersecurity and security compliance topics.

The Security Awareness Training product is only accessible through the global console. You must have an Endpoint Protection subscription to access the management console. Click here to log in.

To enable Security Awareness Training, you'll do all of the following:

1. *Verifying the Product is Active on page 5*
2. *Adding Security Awareness Training to Sites on page 6*
3. Open the Security Awareness Training console.
4. Verify your email domain.
5. Import your user email addresses as targets for phishing campaigns.

To use Security Awareness Training, you'll do all of the following:

1. Create your first phishing campaign.
2. Create your first training campaign.
3. Assemble a program to schedule and automate your campaigns and training.

Chapter 2: Enabling Webroot Security Awareness Training

To get started enabling Security Awareness Training, see the following topics:

Enabling Security Awareness Training Overview *4*
Verifying the Product is Active *5*
Adding Security Awareness Training to Sites *6*
Opening the Security Awareness Training Console *8*
Verifying Your Company's Email Domain *9*
Importing Users Emails As Targets *11*

Enabling Security Awareness Training Overview

We'll begin by enabling Security Awareness Training in five easy steps:

1. Verify that the product is active in your global console.
2. Add Security Awareness Training to a site.
3. Open the Security Awareness Training console.
4. Verify your email domain.
5. Import your user email addresses as targets for the phishing campaign.

Verifying the Product is Active

To start using Security Awareness Training, you will verify that the product is active in your online business console and add it to a site.

To verify the product is active:

1. In the global console, click the **Settings** tab.
2. The Security Awareness Training panel will show your days remaining.

   Note: You can start a free trial of Security Awareness Training if you have not activated the product.

3. Continue with *Adding Security Awareness Training to Sites on page 6*.

Adding Security Awareness Training to Sites

Once you've verified that the product is active, you'll 'll need to add the product to a site. There are two ways to add Security Awareness Training to a site:

- Enabling when creating a new site.
- Enabling for an existing site.

To enable Security Awareness Training when creating a new site:

1. Select the **Enable Security Awareness Training** checkbox.

   Note: Enabling Security Awareness Training is the final step when you create a new site.

2. Click the **Finish** button.

   For more information, see the Enabling for New Sites topic in the Security Awareness Training Admin Guide.

3. Continue with *Opening the Security Awareness Training Console on page 8*

To enable Security Awareness Training for an existing site:

1. Click the **Sites** tab.
2. Find the site you want to enable and in the Actions column, click the **Manage** button.

   The view will change context based on your site, with the Summary tab active.

3. Click the **Security Awareness Training** tab.
4. Select the **Enable Security Awareness Training** checkbox.
5. Click the **Save Changes** button to activate the product.

   For more information, see the Enabling for Existing Sites topic in the Security Awareness Training Admin Guide.

6. Click the **Back Arrow** button to return to the Sites view.

Whether you enabled Security Awareness Training for a new site or an existing site, the product is now activated and enabled for a site.

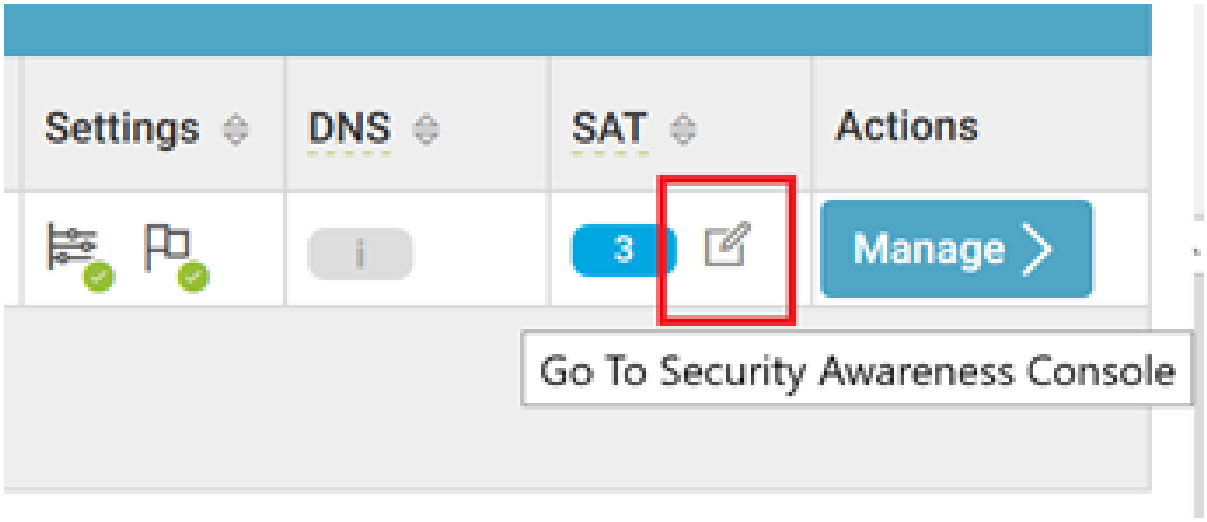
Next, you'll do two one-time setup tasks so you can start using Security Awareness Training. Continue with Opening the Security Awareness Training Console.

Opening the Security Awareness Training Console

The most efficient way to open the Security Awareness Console is from the Sites tab.

To open the Security Awareness Training console:

1. Launch the Security Awareness Training console by clicking on the **Edit** (pencil and box) icon in the SAT column, located in the global console.



Pencil icon in the SAT column

2. If you are in the site management view, click the **Security Awareness Training** tab.
3. Click the **Go To Security Awareness Console** button to open the Security Awareness Console.
4. Continue with *Verifying Your Company's Email Domain on page 9*.

Verifying Your Company's Email Domain

You'll need to perform a one-time setup to verify your email domain. Later, you'll import your user email addresses as targets so that you can to use Security Awareness Training's phishing simulator.

- Start by clicking on the **Dashboard** menu item in the left navigation bar in the Security Awareness Training console.
- There will be two messages. We'll be going through each of these one-time setups.

Adding the domain does not expose any email accounts – you will add selected email addresses in the next step. Email addresses on ISP or public domains, for example gmail.com, hotmail.com, yahoo.com, apple.com, cannot be used.

What Is A Target?

For this product, a target is any of your end users that you send mock phishing emails. The product uses your company's email addresses that you will want to use to send mock phishing emails.

To verify an email domain:

1. Click the**This site currently does not have any verified domains. Please verify your domain(s) before continuing** button.
2. In the Add new domain field, provide your company email address. Some validation text will display.
3. Click the **Add Domain** button.

   The domain will now display as a row and a message displays indicating that you'll need to click on the verification link in the email that was sent to your address.

4. Open your email.
5. Open the email message from securityawareness@webrootanywhere.com with the subject *Please verify your email address*.

   Note: For security reasons, we'll send a verification email to an address you provide. When you click on the verification link in the email, the domain for the email address will be validated.

6. Click the verification link.

   Clicking the link opens a new browser tab with the same Verified Domains view

7. Close any extra Security Awareness Training browser tabs.
8. Click the **Dashboard** menu item on the left navigation bar in the Security Awareness Console to return to the Dashboard view.

   Note for Managed Service Providers: When setting up Security Awareness Training for a client, you will need to coordinate with a client admin who can verify access to their domain. Someone on the client domain will need to receive and click the link in the domain verification email before campaigns can be sent to that client.

9. Continue with *Importing Users Emails As Targets on page 11*.

Importing Users Emails As Targets

You need to import your user's email addresses as targets for the phishing simulator to send out mock phishing emails.

Note: For security reasons, you can only add email addresses with verified email domains. Go back to the *Verifying Your Company's Email Domain on page 9* topic if you have not verified the domain for any of your user's email addresses.

To see how Security Awareness Training works, you can type in your own information using the Paste CSV method. You need to type in your first name, last name, and email address separated by commas.

To import your user's email addresses as targets:

1. Click the **This site currently does not have any targets. Please import targets before sending campaigns** button.
2. Click the **Import Targets** button on the far right above the list of email addresses.
3. Import email addresses in one of the following ways:
   - **Importing email addresses by Paste CSV** — You can paste in a text list of comma-separated values (CSV). Clicking the **CSV template** button should download and open the file in a spreadsheet app on most browsers.
     - If you use a spreadsheet like Excel, you can complete your work, save the .csv file, and upload it in the Upload File tab
     - The data fields are: First Name, Last Name, Email Address, Company User Id, and Tags.
     - The Company User ID and tags are optional fields used in Active Directory or for larger companies.
   - **Importing email addresses by Upload File** — The file upload process supports different file formats like CSV and LDIF. The instructions are included on the screen.

     The console will message you that the import has started. When the import is finished, the page will refresh with the new email addresses listed. A message will be delivered to your console, and you will see an active and shaking email icon in the upper right.
4. Click the icon to read your messages.
5. After you have validated your first email domain and have added targets, the panels no longer appear under the Dashboard.

6. You can add more email domains or email addresses as user targets by selecting an option in the **Settings** area in the left navigation bar.
7. You are all set. Next, you'll start using Security Awareness Training. Continue with *Using Security Awareness Training Overview on page 14*.

Chapter 3: Using Security Awareness Training

To get started using Security Awareness Training, see the following topics:

Using Security Awareness Training Overview *14*
About Campaigns *14*
Creating Phishing Campaigns *15*
Step 1 — Simulation Basics *15*
Step 2 — Available Targets *16*
Step 3 — Design Phishing Email *16*
Step 4 — Design Phishing Site *16*
Step 5 — Review and Launch *17*
Creating Training Campaigns *18*
Creating Your First Training Campaign *18*
Step 1 — Training Session Basics *18*
Step 2 — Available Targets *19*
Step 3 — Design Invitation Email *19*
Step 4 — Design Education Page *19*
Step 5 — Review and Launch *19*
Assembling Training Programs *21*
New Program Form *22*
Welcome Email *22*
Phishing Campaign *22*
Training Campaign *22*
Whats Next? *24*

Using Security Awareness Training Overview

To use Security Awareness Training, you'll do all of the following:

1. Create your first phishing campaign.
2. Create your first training campaign.
3. Assemble a program to schedule and automate your campaigns and training.

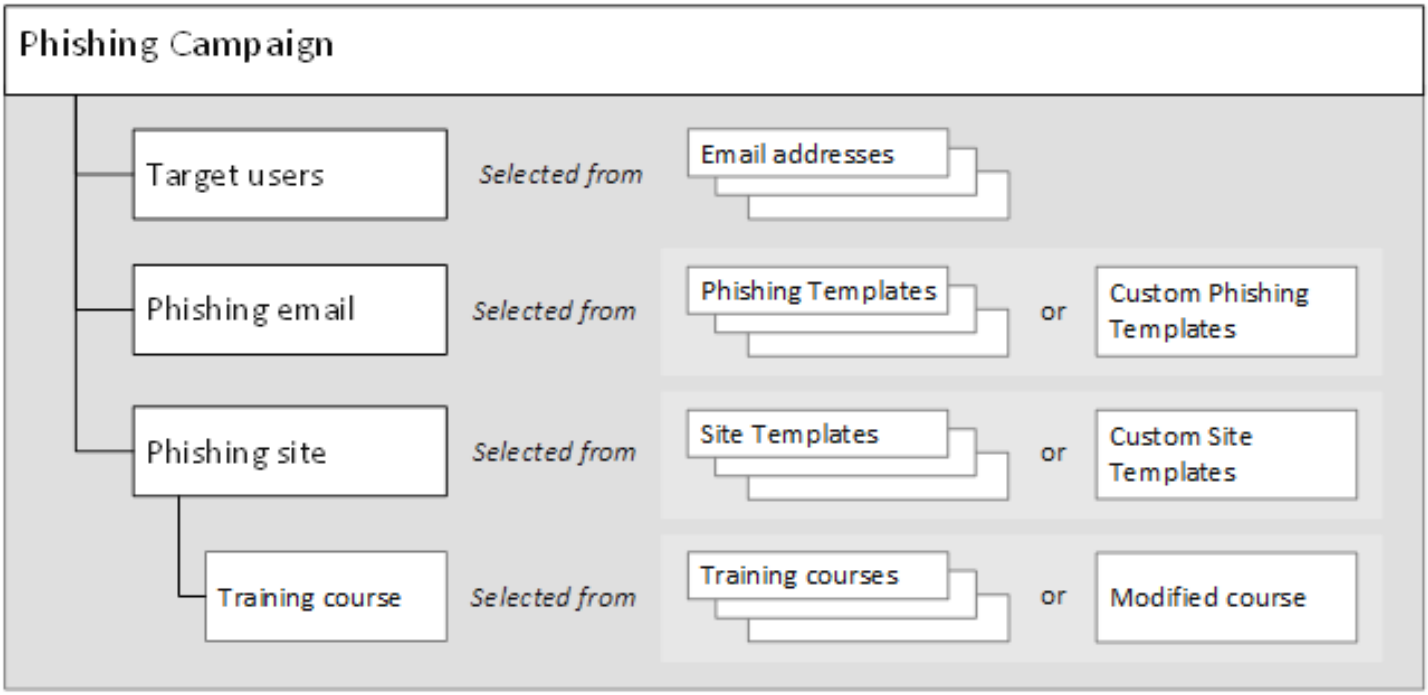
About Campaigns

In the first and second steps, you will create your first phishing campaign and a training campaign.

What Is A Campaign?

A campaign is the basis for reporting and managing Security Awareness Training. A campaign can be either a phishing campaign or a training campaign. Campaigns are how this product delivers mock phishing emails or training courses to your workforce.

Creating Phishing Campaigns



A phishing campaign includes users' email addresses, a phishing email, and a phishing site with an optional training course.

We'll start with the Phishing Simulation area.

1. Click the **New Campaign** button in the left navigation bar. This menu item does not display until you have verified an email domain.
2. Click the **Start a new simulation** button in the Phishing Simulation area. The New Campaign Wizard displays.

Step 1 — Simulation Basics

In this step, you determine the name and basic information for your phishing simulation.

1. Give your simulation a name and description by completing the Simulation Name and Description fields.
2. You can select the **Show Advanced Options** checkbox to reveal additional settings covered in the Creating Phishing Simulations topic in the Security Awareness Training Admin Guide.

3. Click the **Save Simulation** button. The campaign will be created and saved.
4. Click the **Save/Next** button in the upper right corner to start setting up the campaign.

Step 2 — Available Targets

In this step, you choose which email addresses to target for your phishing simulation.

1. A list of your targets you set up earlier in the *Importing Users Emails As Targets on page 11* topic are displayed under some filter fields.
2. Select the targets you want included in the phishing simulation by selecting the checkbox.
3. You can import more targets by clicking the **Import Targets** button on the right above the list.
4. Click the **Save/Next** button in the upper right corner to continue.

Step 3 — Design Phishing Email

In this step, you set up how the mock phishing email will look to your users, and what email address is used to send the email.

1. There is only one field: **Type to search for email templates**. Click in the field to see all preformatted templates in a drop-down menu. You can type keywords to filter the drop-down menu. Click on a template to select it.
2. To the far right of this field, there is an **Envelope** icon. Clicking this icon allows you to browse the preformatted templates, with the ability to filter the templates based on certain criteria, and see a preview. Clicking a template will select it
3. When you select a template, a preview displays. You can modify the email template by doing either of the following:
   - Click **Customize the template** button.
   - Make your own from scratch by clicking the **Use empty template** button.

   Both buttons open an email tool with a WYSIWYG editor. Email template editing is covered in the Designing Phishing Emails topic in the Security Awareness Training Admin Guide.

4. Click the **Save/Next** button in the upper right corner to continue.

Step 4 — Design Phishing Site

In this step, you set up where the simulated malware link will take the user.

1. **URL Hostname** — Type in a subdomain for your page.
   - You can use a realistic domain to try to fool users who will hover over the link before clicking on it, or you can reward users by using an obviously false subdomain.
   - To the right, choose a domain following the reasoning: Choosing a domain that reflects the email content is recommended.
2. **Site Type** — You have three choices for what type of web page will display if someone clicks on the email link:
   - **Education Page** — The targeted user is sent directly to a page for required education on phishing.
   - **Lure Page** — You can continue the simulation by having a lure page presented where the user could fill in their credentials.
   - **Broken Link** — If you are concerned that users will talk to each other about your security campaign while it is running, you can present a simulated 404 page.
3. **Design Education Page** — As an outcome for falling for the phishing simulation, you can deliver training to the targeted user in two ways:
   - **Training Module** — You can deliver training as a result of clicking the link. Select a training course. The Module information will pre-populate on the right. You can customize the content.
   - **Template or Infographic** — You can choose to deliver a warning message or infographic. Select a template from the Education Template drop-down menu.
4. Click the **Save/Next** button in the upper right corner to continue.

Step 5 — Review and Launch

In this step, you review your campaign and launch the simulation.

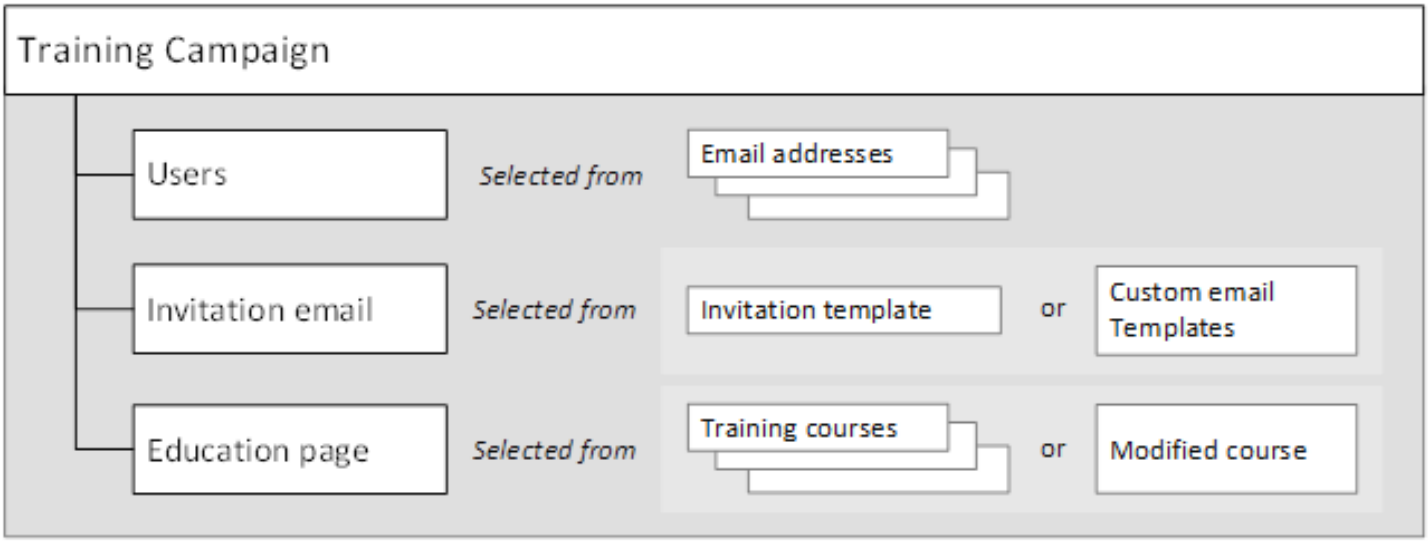
1. A summary of the campaign is listed in the tabs.
2. In the upper right, you can send a test email to the account email address by clicking the orange button. You can also type in any email address above the button and click the **Send Test** button.
3. Click the **Launch Simulation** button in the upper right corner to finish and save your campaign. Once you click the button, your campaign will now be sent to the emails of the target you selected.

Now that you've created your first campaign, you will be able to see progress on the Dashboard area, as well as the Campaigns area. Both are in the left navigation bar.

Continue with *Creating Training Campaigns on page 18*.

Creating Training Campaigns

A training campaign includes users' email addresses, an invitation, and an education page.



A training campaign includes users' email addresses, an invitation, and an education page.

Creating Your First Training Campaign

To create your first training campaign:

1. Click the **New Campaign** icon in the left navigation.
2. Click the **Start a new training session** button in the Training Session area. The New Campaign Wizard displays.

Step 1 — Training Session Basics

In this step, you choose the name and basic information for your training session.

1. Give your training session a name and description by completing the Session Name and Description fields.
2. You can select the **Show Advanced Options** checkbox to display additional settings covered in the Security Awareness Training Admin Guide.
3. Click the **Save Training Session** button. The campaign will be created and saved.
4. Click the **Save/Next** button in the upper right corner to start setting up the campaign.

Step 2 — Available Targets

In this step, you determine which student email addresses to deliver your training.

1. A list of your targets you set up earlier in *Importing Users Emails As Targets on page 11* are displayed under some filter fields.
2. Determine the targets you want included in the training session by selecting the checkbox.
3. You can import more targets by clicking the **Import Targets** button on the right above the list.
4. Click the **Save/Next** button in the upper right corner to continue.

Step 3 — Design Invitation Email

In this step, you set up how the training invitation email will look to your users, and what email address is used to send the email.

1. There is only one field: **Basic Training Invitation**. Click it and select the only entry to continue.
2. When you select a template, the From and Subject fields display. You can do either of the following:
   - Modify the sender email address and/or email template by clicking the **Customize the template** button.
   - Make your own from scratch by clicking the **Use empty template** button.

   Both buttons open an email tool with a WYSIWYG editor. Email template editing is covered the Designing Phishing Emails topic in the Security Awareness Training Admin Guide.

3. Click the **Save/Next** button in the upper right corner to continue.

Step 4 — Design Education Page

In this step, you set up where the training link will take the user.

1. The Design Education page is where you select what training course to deliver:
2. Training Module is where you select a training course from the list of training modules. The training module information will pre-populate on the right. You can customize the content.
3. Click the **Save/Next** button in the upper right hand to continue.

Step 5 — Review and Launch

In this step, you review your campaign and launch the training session.

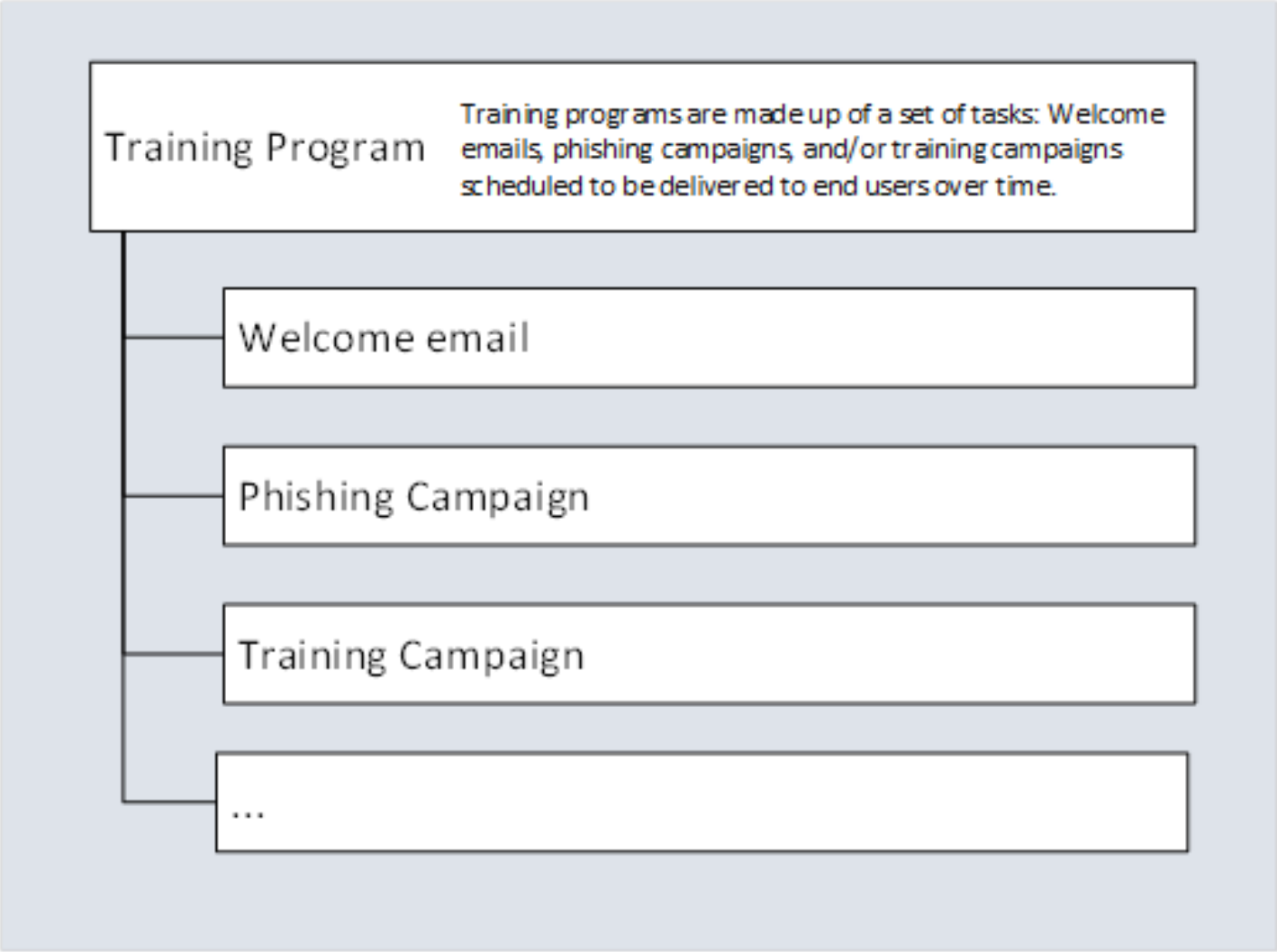
1. A summary of the campaign is listed in Tabs.
2. You can do either of the following:
   - In the upper right corner, you can send a test email to the account email address by clicking the Orange button.
   - You can also type in any email address above the button and click the **Send Test** button.
3. Click the **Launch Training** button in the upper right corner to finish and save your campaign.

Now that you've created your second campaign, you will be able to see progress on the Dashboard area, as well as the Campaigns area. Both are in the left navigation bar.

Continue with *Assembling Training Programs on page 21*.

Assembling Training Programs

Now that you've created a phishing campaign and a training campaign, you can use a training program to schedule and automate your campaigns.



A training program can include a welcome email, a phishing campaign, or a training campaign.

What Is A Program?

For Security Training, a training program is a schedule of welcome emails, phishing simulations, or training courses. You can build full training programs for your end users with this feature.

To start your first program:

1. Click the **Programs** menu in the left navigation bar.
2. In the message *No Programs found. Create a program to see it here*, click the **Create a program** link.

New Program Form

The New Program form is where you create your programs.

- Complete the program name and description.
- Under Available Tasks, there are three possible 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 the **Welcome Email** button. You 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 the **Phishing Campaign** button.

You provide a task name, select one of your Phishing Campaigns from a 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 the **Training Campaign** button.

You provide 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 add an optional report to additional email addresses using the Email Reports section at the bottom of the view.

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

Continue with *Whats Next? on page 24*.

Whats Next?

You've finished setting up and using the main features of Webroot Security Awareness Training.

- Try sending a mock phishing email to your own account and clicking on the link to see how the resulting web page, training delivery, and reporting work.
- Webroot's user guides for business products are available online, and include PDF versions.
- To learn more about the business console, see the Global Site Manager online guides, which are listed under Global Site Manager.
- For information about advanced settings, we recommend you review the Security Awareness Training Admin Guide.

Chapter 4: Security Awareness Training Support

For information about support, see the following topic:

Accessing Technical Support *26*

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

A

accessing technical support *26*
adding security awareness training
to new sites *6*
adding security awareness training to existing sites *6*
assemble training programs *21*
available targets *16*, *19*

C

company's email domain, verifying *9*
creating phishing campaigns *15*
creating training campaigns *18*

D

design education page *19*
design invitation email *19*
design phishing email *16*
design phishing site *16*

E

education page, design *19*
emails as targets, importing *11*

G

getting started guide, overview *2*

I

importing, emails as targets *11*
invitation email, design *19*

N

new sites, adding security awareness training to *6*

O

opening security awareness training console *8*
overview
    getting started guide *2*
    security awareness training *4*
    using security awareness training *14*

P

phishing campaigns, creating *15*
product is active, verifying *5*

R

review and launch *17*
    training campaigns *19*

S

security awareness training
    adding to existing sites *6*
    overview *14*
security awareness training, opening the console *8*
security awareness training, overview *4*
simulation basics *15*

T

targets, available *19*
technical support, accessing *26*
training campaigns
    review and launch *19*
training campaigns, creating *18*
training programs, assemble *21*
training session basics *18*

V

verifying company's email domain *9*
verifying product is active *5*

W

what's next *24*