Security Awareness Training

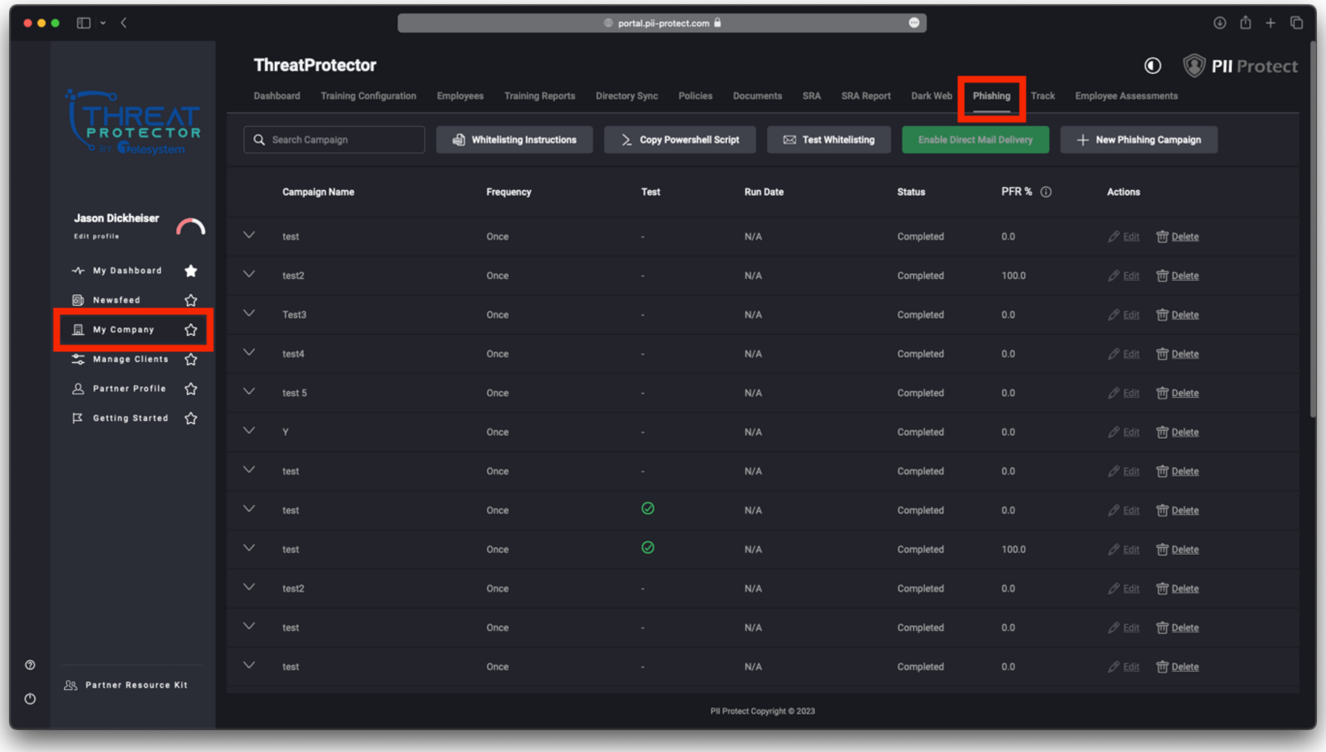
Phishing Campaigns

Telesystem IT's About Trust | #HackersSuck

Phishing Campaigns use simulated phishing emails that can be sent to members of your team to allow them the opportunity to identify what a phishing email may look like. Company administrators can use the portal to create and manage phishing campaigns that can be sent across your entire organization or targeted to specific roles or departments within an organization. This guide will help you navigate the portal to setup and manage your Phishing Campaigns.

Accessing Phishing Campaigns in the ThreatProtector PII Portal

Once logged into the ThreatProtector PII Portal (https://portal.breachsecurenow.com/#/login), use the sidebar vertical menus and select **My Company** then use the menu options at the top of the screen to select **Phishing**.

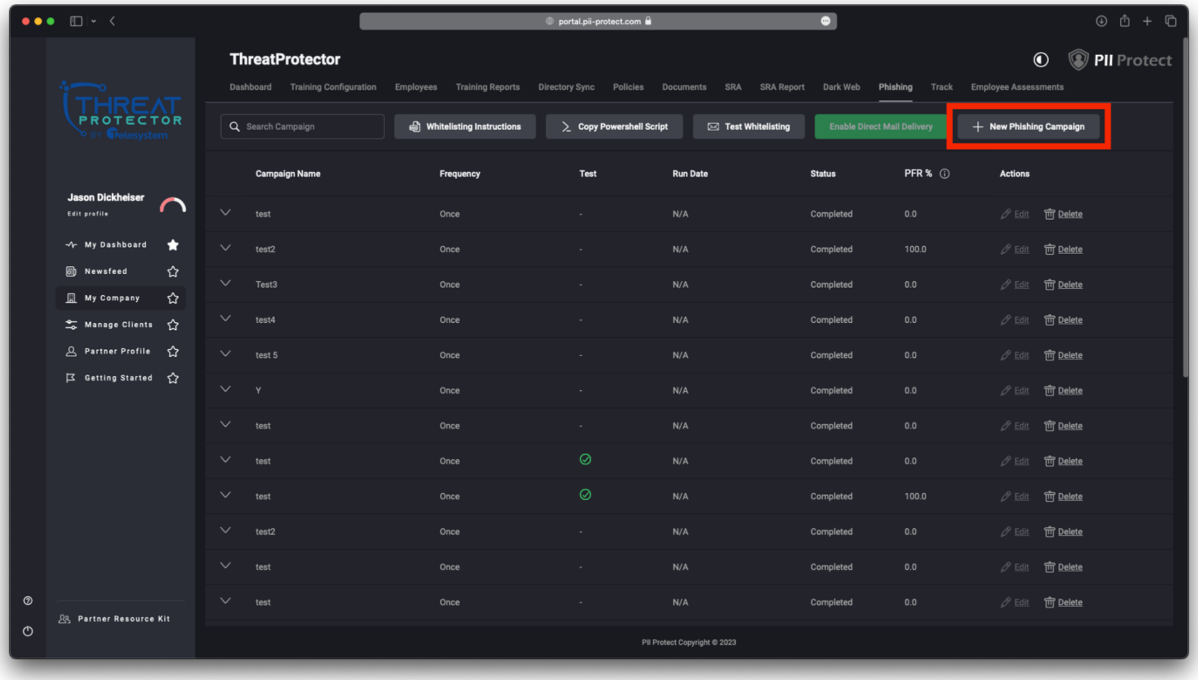


Campaign Name	Frequency	Test	Run Date	Status	PFR %	Actions
test	Once	-	N/A	Completed	0.0	Edit Delete
test2	Once	-	N/A	Completed	100.0	Edit Delete
Test3	Once	-	N/A	Completed	0.0	Edit Delete
test4	Once	-	N/A	Completed	0.0	Edit Delete
test 5	Once	-	N/A	Completed	0.0	Edit Delete
Y	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	✓	N/A	Completed	0.0	Edit Delete
test	Once	✓	N/A	Completed	100.0	Edit Delete
test2	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete

This page will display a list of all Phishing Campaigns that have run, are currently running, or are setup to run in the future.

Creating a New Phishing Campaign

To create a new Phishing Campaign, from the Phishing menu, click on the "**+ New Phishing Campaign**" button first.



Campaign Name	Frequency	Test	Run Date	Status	PFR %	Actions
test	Once	-	N/A	Completed	0.0	Edit Delete
test2	Once	-	N/A	Completed	100.0	Edit Delete
Test3	Once	-	N/A	Completed	0.0	Edit Delete
test4	Once	-	N/A	Completed	0.0	Edit Delete
test 5	Once	-	N/A	Completed	0.0	Edit Delete
Y	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	✓	N/A	Completed	0.0	Edit Delete
test	Once	✓	N/A	Completed	100.0	Edit Delete
test2	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete

New Campaign - Settings

On the **New Campaign Settings** screen you will be asked to do the following:

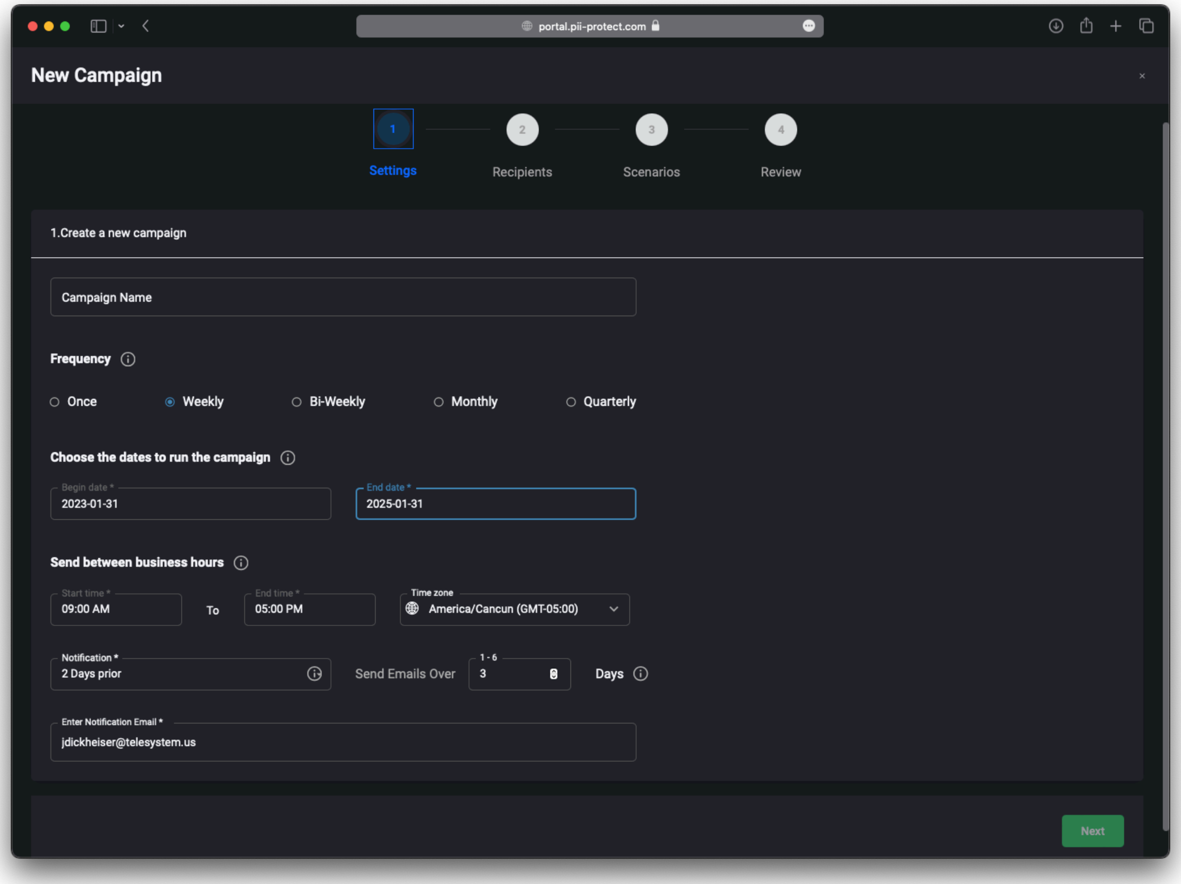
1. Create a name for the campaign
2. Choose the Frequency for the campaign to determine how often the campaign will be sent. Options include:
    a. Once
    b. Weekly
    c. Bi-Weekly
    d. Monthly
    e. Quarterly
3. Choose the dates to run the campaign. If you only choose to run the campaign once in the previous selection you only need to select the start date. If you choose a recurring frequency, you must also select an end date for the campaign.
    a. If frequency is set to "Once" there will also be an option to mark the campaign as a Demo campaign. If this is enabled, the campaign will not impact the Phishing Fail Rate (PFR) and ESS of the selected recipients if links are clicked.
4. Configure the **Send between business hours** to determine what time of day the campaign will run.
5. The **Notification** option allows you to choose if you would like to be sent a notification before the campaign runs.

a. **None –** Choose this option if you do not wish to be notified prior to the campaign being run

b. **2 Days prior** – Choose this option if you would like to be notified 2 days prior to the campaign starting. Note that if you choose this option, the Begin date must be set at least 2 days from the day you are configuring the campaign.

   i. **If you choose to be notified 2 Days prior,** you must also enter an email address for where the notification should be sent. By default, the system will populate the email address associated with your admin account to login to the portal.

6. **Send Emails Over *x* Days –** This setting allows you to choose the span of days the campaign will be sent to users over. Minimum setting allowed is 1-day, maximum number of days is 6.
7. **Click the Next button to proceed to the Recipients configuration**



1.Create a new campaign

Campaign Name

Frequency

○ Once ● Weekly ○ Bi-Weekly ○ Monthly ○ Quarterly

Choose the dates to run the campaign

Begin date * 2023-01-31

End date * 2025-01-31

Send between business hours

Start time * 09:00 AM To End time * 05:00 PM

Time zone America/Cancun (GMT-05:00)

Notification * 2 Days prior

Send Emails Over 1 - 6 3 Days

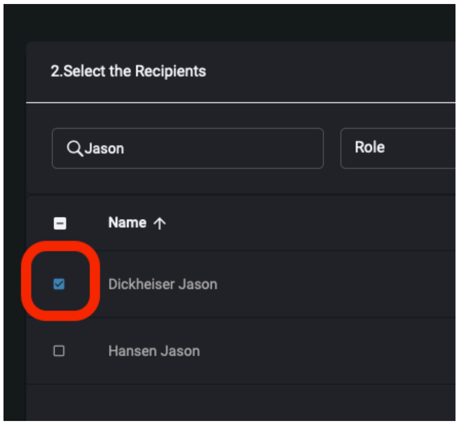
Enter Notification Email * jdickheiser@telesystem.us

New Campaign - Recipients

On the **New Campaign Recipients** screen you will need to select the users who will receive the Phishing Campaign.

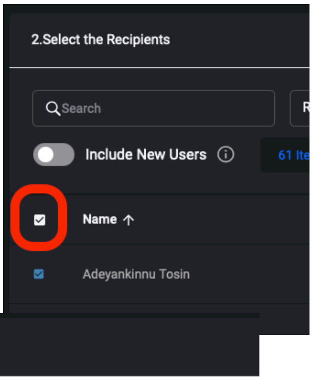
You can select individual users by locating them in the list or using the Search box to find them, and the check the box to the left of their names.

Select all available users quickly by checking the box in the header column next to the **Name** field.

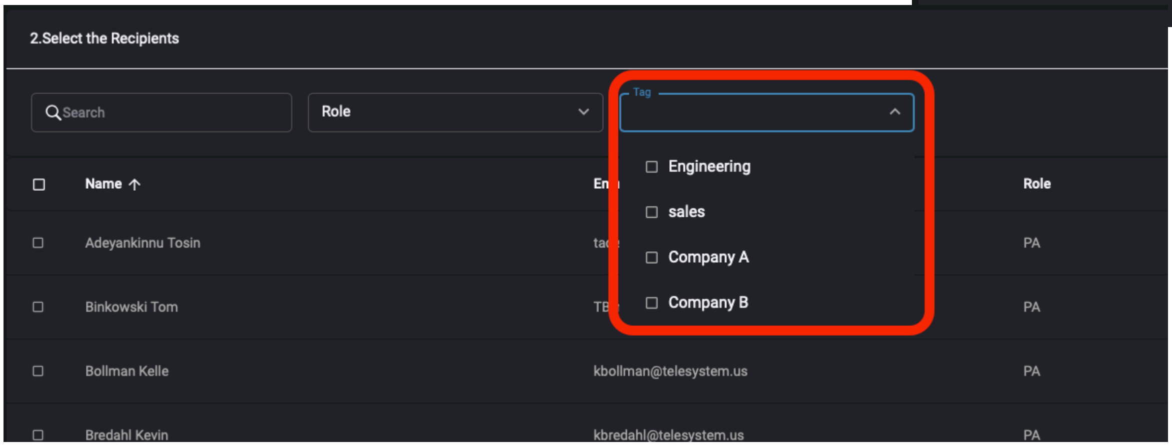


☑ Dickheiser Jason
□ Hansen Jason

If you have users categorized by Role or by Tag, you can filter the list of available users using the drop-down box to only show those users with the selected filter to quickly locate and select those users.

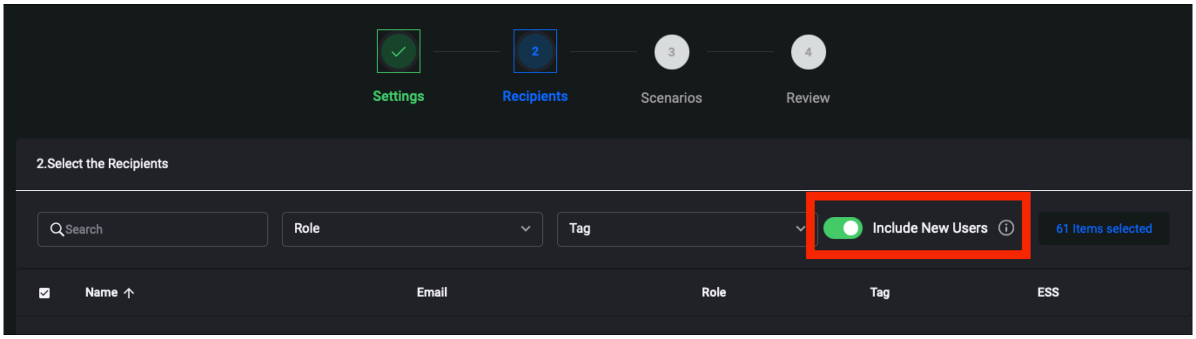


☑ Adeyankinnu Tosin



□	Name ↑	En	Role
□	Adeyankinnu Tosin	ta	PA
□	Binkowski Tom	TB	PA
□	Bollman Kelle	kbollman@telesystem.us	PA
□	Bredahl Kevin	kbredahl@telesystem.us	PA

You can also choose to **Include New Users** with an available Toggle Switch. When this is enabled, newly added users will be automatically enrolled in this campaign to receive future simulations. If filtering by a role or tag, new users will automatically be included.



Once you have completed adding all recipients to the campaign, click **Next** at the bottom of the page to proceed.

New Campaign - Scenarios

The **New Campaign Scenarios** screen is where you select what simulated phishing email message will be sent to users.

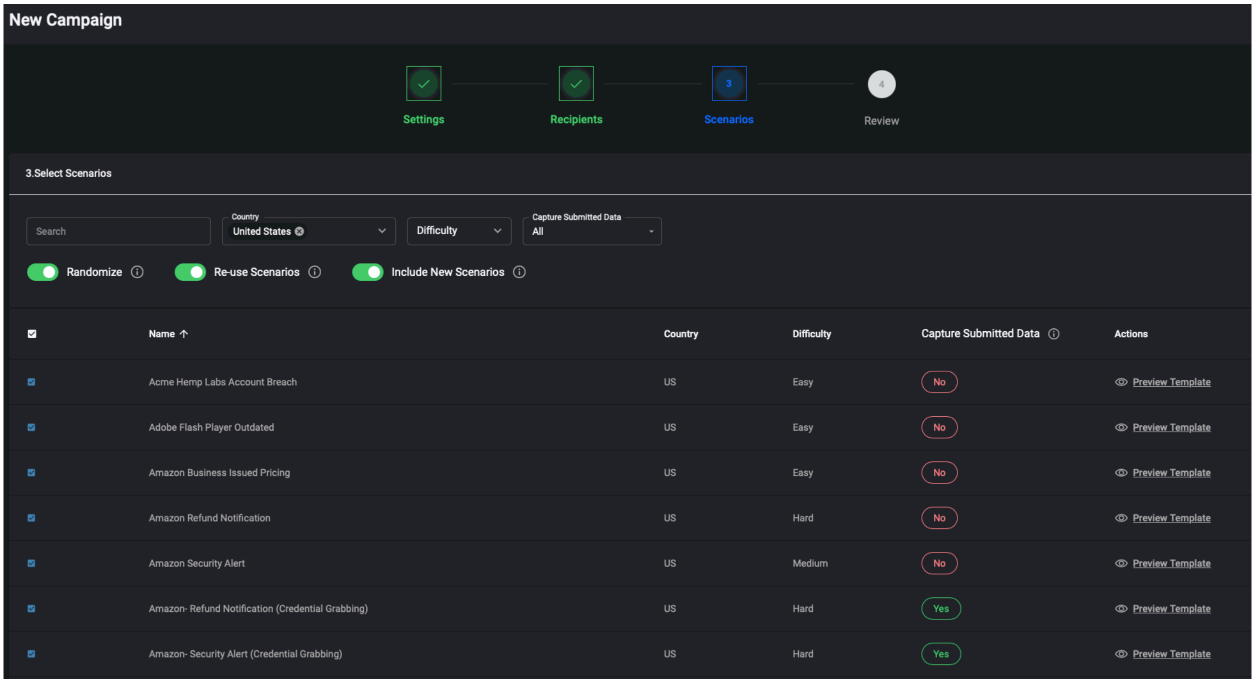
Here you can select specific scenarios from the list available by checking the box to the left of the name of the scenario. The list will identify:

- The country the campaign is intended for
- The difficulty for the end user to identify if the phishing attempt
- Whether the scenario will capture data the user might submit after clicking on any links
    - Campaigns that capture submitted data (Yes) will bring users to a fake landing page if a link is clicked. Additional ESS points will be lost, and results will be tracked if users submit any data on this fake landing page. No submitted data will be saved or accessible.
- The Actions column allows you to click on the link to Preview the template which will allow you to review an example of what the simulated phishing email will look like.

Along the top of the page, you can search for a specific campaign to run or use the sorting options to only display and select from campaigns based on the Country they are intended for, the difficulty of the campaign (Easy, Medium, or Hard), and whether the campaign captures submitted data.

There are also radials to choose to Randomize the campaign sent out based on multiple options being selected, Re-User Scenarios for recurring campaigns (weekly, monthly or quarterly) and to include new scenarios for when new options are added during the course of a recurring campaign.

In the example below, we've sorted by campaigns for the United States with any difficulty rating, and include campaigns with or without captured submitted data. The campaigns will be randomized, and we will re-use scenarios and include any new scenarios that become available over the course of our campaign:



3.Select Scenarios

Search

Country: United States

Difficulty

Capture Submitted Data: All

Randomize: on

Re-use Scenarios: on

Include New Scenarios: on

☑	Name ↑	Country	Difficulty	Capture Submitted Data	Actions
☑	Acme Hemp Labs Account Breach	US	Easy	No	Preview Template
☑	Adobe Flash Player Outdated	US	Easy	No	Preview Template
☑	Amazon Business Issued Pricing	US	Easy	No	Preview Template
☑	Amazon Refund Notification	US	Hard	No	Preview Template
☑	Amazon Security Alert	US	Medium	No	Preview Template
☑	Amazon- Refund Notification (Credential Grabbing)	US	Hard	Yes	Preview Template
☑	Amazon- Security Alert (Credential Grabbing)	US	Hard	Yes	Preview Template

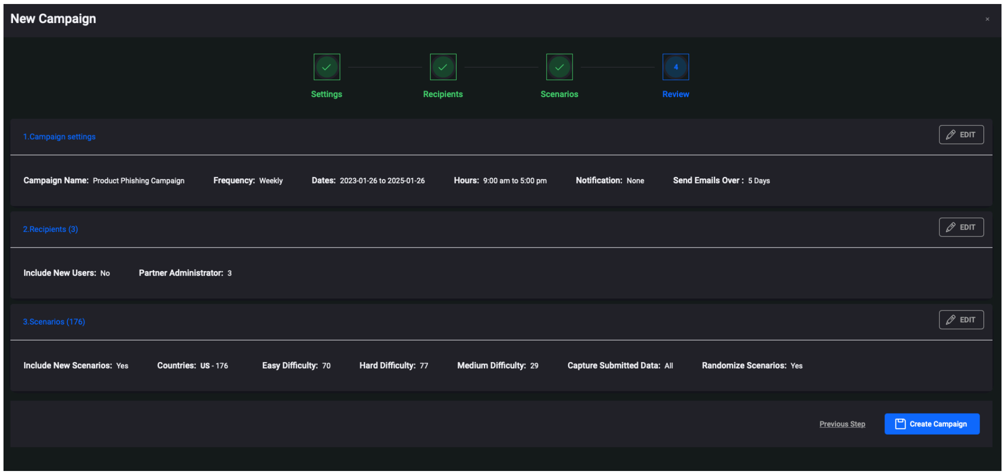
Once you completed the setup of your campaign, click Next at the bottom of the page.

New Campaign - Review

The **New Campaign Review** screen is the final screen for creating a new campaign. Here you will see a high-level overview of the selections you have made over the past 3 screens to setup your campaign.

Review the selections you have made. If you choose to modify anything at this time, you can do so by clicking on the **Edit** button for the section you wish to modify, and the system will jump you back to that screen. If you choose to edit the campaign settings you will be sent back to the beginning of the configuration for the campaign and must click **Next** to go through each page of settings, but it will remember your configuration options for each page.

Once you are satisfied with the configuration of the campaign, click the **Create Campaign** button at the bottom of the page.



1.Campaign settings

Campaign Name: Product Phishing Campaign Frequency: Weekly Dates: 2023-01-26 to 2025-01-26 Hours: 9:00 am to 5:00 pm Notification: None Send Emails Over : 5 Days

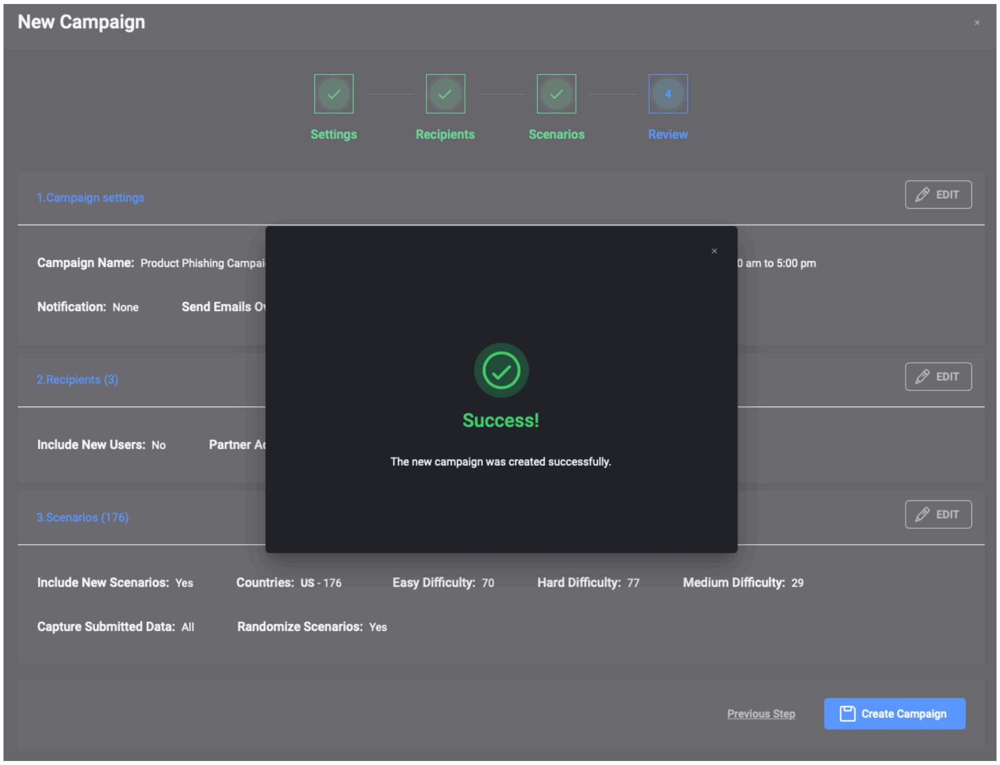
2.Recipients (3)

Include New Users: No Partner Administrator: 3

3.Scenarios (176)

Include New Scenarios: Yes Countries: US - 176 Easy Difficulty: 70 Hard Difficulty: 77 Medium Difficulty: 29 Capture Submitted Data: All Randomize Scenarios: Yes

The system will notify you that the new campaign was created successfully. Click the X in the corner of that popup box to close it and return to the list of Phishig Campaigns setup for your organization.



1.Campaign settings

Campaign Name: Product Phishing Campai 0 am to 5:00 pm

Notification: None Send Emails O

2.Recipients (3)

Include New Users: No Partner A

3.Scenarios (176)

Include New Scenarios: Yes Countries: US - 176 Easy Difficulty: 70 Hard Difficulty: 77 Medium Difficulty: 29

Capture Submitted Data: All Randomize Scenarios: Yes

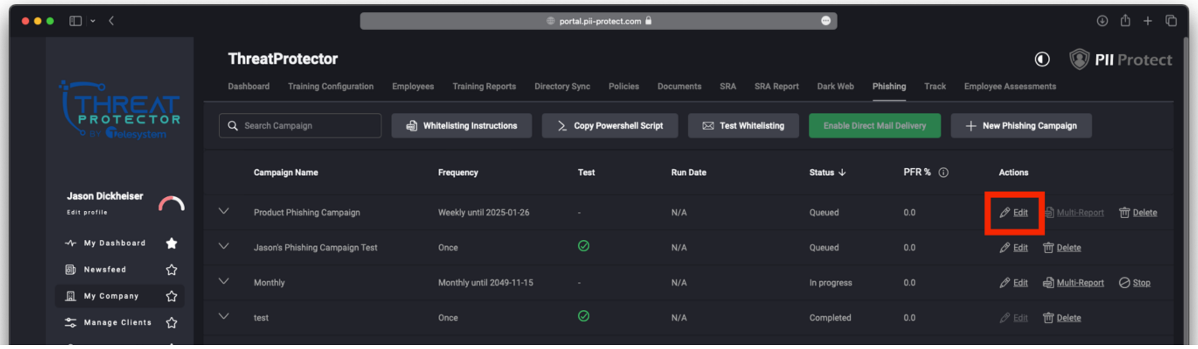
Success!

The new campaign was created successfully.

Edit an existing Campaign

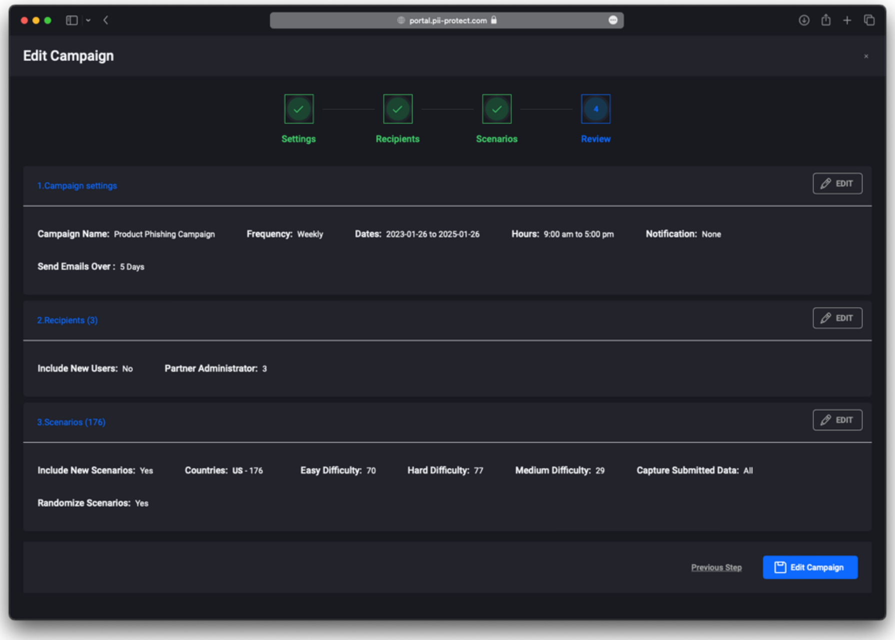
You can edit any existing campaign by going to My Company→Phishing. You will be presented with the list of Phishing Campaigns in your organization. Under the status column, you can identify if a campaign has been Completed, is Queued or In Progress.

Campaigns that are Queued or In Progress can be edited as needed. If you need to edit the campaign, find it in the list and click the **Edit** link in the corresponding **Actions** column.



Campaign Name	Frequency	Test	Run Date	Status ↓	PFR %	Actions
Product Phishing Campaign	Weekly until 2025-01-26	-	N/A	Queued	0.0	Edit Multi-Report Delete
Jason's Phishing Campaign Test	Once	✓	N/A	Queued	0.0	Edit Delete
Monthly	Monthly until 2049-11-15	-	N/A	In progress	0.0	Edit Multi-Report Stop
test	Once	✓	N/A	Completed	0.0	Edit Delete

Choosing to edit a campaign will take you into the campaign settings where you can make any necessary changes when the campaign will run and what the frequency is, the recipients of the campaign, and what scenarios will be assigned to the campaign. Go through the different menus using the first part of this guide to assist you with the different settings available and then click the **Edit Campaign** button on the review screen to save your changes.



1.Campaign settings

Campaign Name: Product Phishing Campaign Frequency: Weekly Dates: 2023-01-26 to 2025-01-26 Hours: 9:00 am to 5:00 pm Notification: None

Send Emails Over : 5 Days

2.Recipients (3)

Include New Users: No Partner Administrator: 3

3.Scenarios (176)

Include New Scenarios: Yes Countries: US - 176 Easy Difficulty: 70 Hard Difficulty: 77 Medium Difficulty: 29 Capture Submitted Data: All

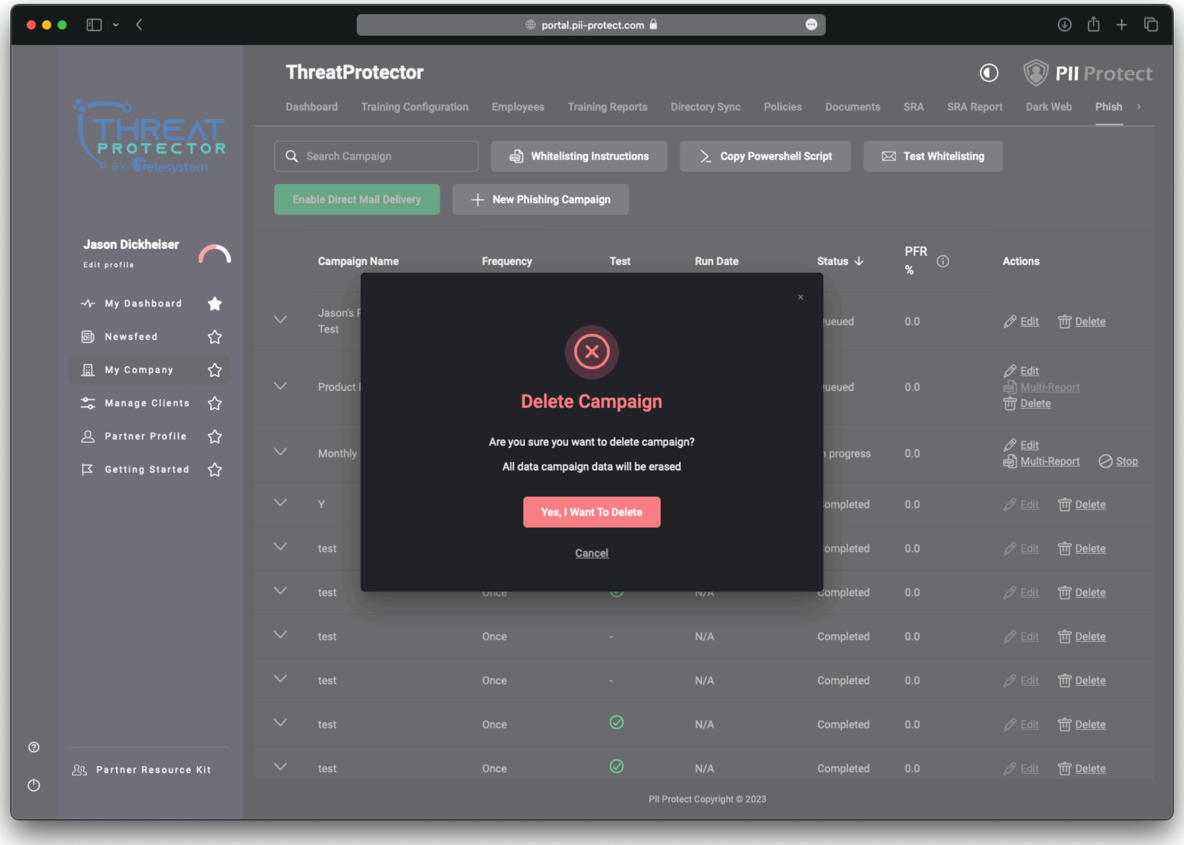
Randomize Scenarios: Yes

Delete a Campaign

You can edit any existing campaign by going to My Company>Phishing. You will be presented with the list of Phishing Campaigns in your organization. Under the status column, you can identify if a campaign has been Completed, is Queued or In Progress.

Any campaign in the list can be deleted by clicking the **Delete** link in the **Actions** column for the corresponding campaign.

The system will prompt you through a pop-up window to ask if you are sure you want to delete the campaign. All campaign data is erased when the campaign is deleted. To proceed with deletion of the campaign click the red **“Yes, I Want to Delete”** button, or to keep the campaign and associated data, click the **Cancel** link.



Campaign Name	Frequency	Test	Run Date	Status	PFR %	Actions
Jason's F Test				ueued	0.0	Edit Delete
Product I				ueued	0.0	Edit Multi-Report Delete
Monthly				progress	0.0	Edit Multi-Report Stop
Y				ompleted	0.0	Edit Delete
test				ompleted	0.0	Edit Delete
test	Once	✓	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	-	N/A	Completed	0.0	Edit Delete
test	Once	✓	N/A	Completed	0.0	Edit Delete
test	Once	✓	N/A	Completed	0.0	Edit Delete

Delete Campaign

Are you sure you want to delete campaign?

All data campaign data will be erased

Yes, I Want To Delete

Cancel

PII Protect Copyright © 2023