

## Security Awareness Training Partner Guide

# — Simulated Phishing Whitelisting, Campaign Setup & Overview

*Internal Use Only*



**#HACKERS SUCK**

[www.TrustTelesystem.com](http://www.TrustTelesystem.com)

# Simulated Phishing Partner Guide

## Table of Contents

Resources <i>partner guides &amp; marketing content</i> .....	page 3
Simulated Phishing Overview <i>getting started &amp; feature overview</i> .....	pages 4 – 5
Whitelisting <i>options and quick steps</i> .....	page 6 – 7
One-Time Phishing Campaigns <i>setup &amp; initiation</i> .....	pages 8 – 13
AutoPhish Automated Phishing Campaigns <i>campaign configuration &amp; initiation</i> .....	pages 14 - 19
Phishing Reports <i>modifying campaigns &amp; reporting</i> .....	page 20

# Simulated Phishing Partner Guide

## Resources

- [BSN Service Breakdown](#)
- [Feature Comparison](#)
- [User Management Partner How-To Guide](#)
- [Whitelisting Instructions](#)
- [Catch Phish Go-to-Market Kit](#)

# Simulated Phishing Overview

With phishing, one of the top attack methods of choice by cyber criminals, having a robust phishing education program in place is key to mitigating human vulnerabilities. Our simulated phishing platform has a variety of tools you can use to prospect & educate!

## Getting Started

In order to set up a simulated phishing campaign, you will first need to [add users](#) and follow our [whitelisting](#) instructions to ensure deliverability of the emails. Users can be added manually, by bulk upload using a .csv file, or by using Azure Active Directory.

If you have a Breach Prevention Platform (BPP), HIPAA Breach Prevention Platform (HIPAA BPP), or EVA MD clients, we recommend deploying our Catch Phish Email Analysis Tool to increase engagement, provide real-time phishing education on REAL emails, and reduce service tickets for email verification!

### What is the Catch Phish Email Analysis Tool?

Our Catch Phish Email Analysis Tool is available as a Microsoft Outlook Add-In. This in-email tool allows users to send ANY email “for analysis” where machine learning and artificial intelligence identify any red flags in the links, language, and attachments. In addition to training users in real-time on how to spot phishing emails, Catch Phish also provides positive reinforcement through increased Employee Secure Scores (ESS) and gamification.



# Simulated Phishing Overview

With phishing, one of the top attack methods of choice by cyber criminals, having a robust phishing education program in place is key to mitigating human vulnerabilities. Our simulated phishing platform has a variety of tools you can use to prospect & educate!

## Feature Overview

Routinely phishing users is one of the key security measures you can implement that will lead to a high return on investment, improving phishing click rates by an average of 64% according to the Ponemon Institute. That's why we include a test campaign and initial baseline campaign for all Unlimited Training clients and provide AutoPhish, our automated phishing platform, for your clients subscribed to a service with our Employee Vulnerability Assessment, EVA! See our feature comparison for eligible upgrades.

### **One-Time Phishing Campaigns – Setup starts on page 8**

Unlimited Training clients not only get access to an initial dark web scan and your annual security awareness training course, but also a one-time simulated phishing campaign – plus a test campaign – for our partners to leverage as an unbeatable prospecting tool! This “Baseline Security Assessment” is included in your Partner Subscription for an unlimited number of client organizations! Don't forget to leverage our partner-branded landing pages to bring awareness to your free assessment!

### **AutoPhish Automated Campaigns – Setup starts on page 14**

Take the labor out of phishing management with AutoPhish! With AutoPhish, you can setup ongoing simulated phishing campaigns for the *entire year* in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are setup with our Catch Phish Email Analysis Tool so they can earn back points on their Employee Secure Score (ESS).

# Whitelisting – General Instructions

Ensure phishing message delivery by whitelisting. We've provided several options to help assist with the whitelisting process. Contact our team for further assistance and troubleshooting.

## Whitelisting Options

Whitelisting is required to ensure that phishing emails are successfully received and properly tracked. We provide several options for whitelisting and our team is always available to assist with whitelisting issues.

### **Direct Mail Delivery – [More information on page 7](#)**

Bypass those pesky spam filters that (rightfully) may be blocking or inhibiting your phishing efforts.

### **Whitelisting Instructions**

We provide a simple download of our whitelisting instructions to easily copy and paste the IP addresses and domains that phishing emails will send from and whitelisting steps for popular platforms.

### **Powershell Script**

We provide a powershell script to copy for those looking to whitelist for Microsoft 365 Advanced Delivery.

### **Test Whitelisting**

Quickly validate that your whitelisting was successfully by sending a test message to an email of your choice.

# Whitelisting – Direct Mail Delivery

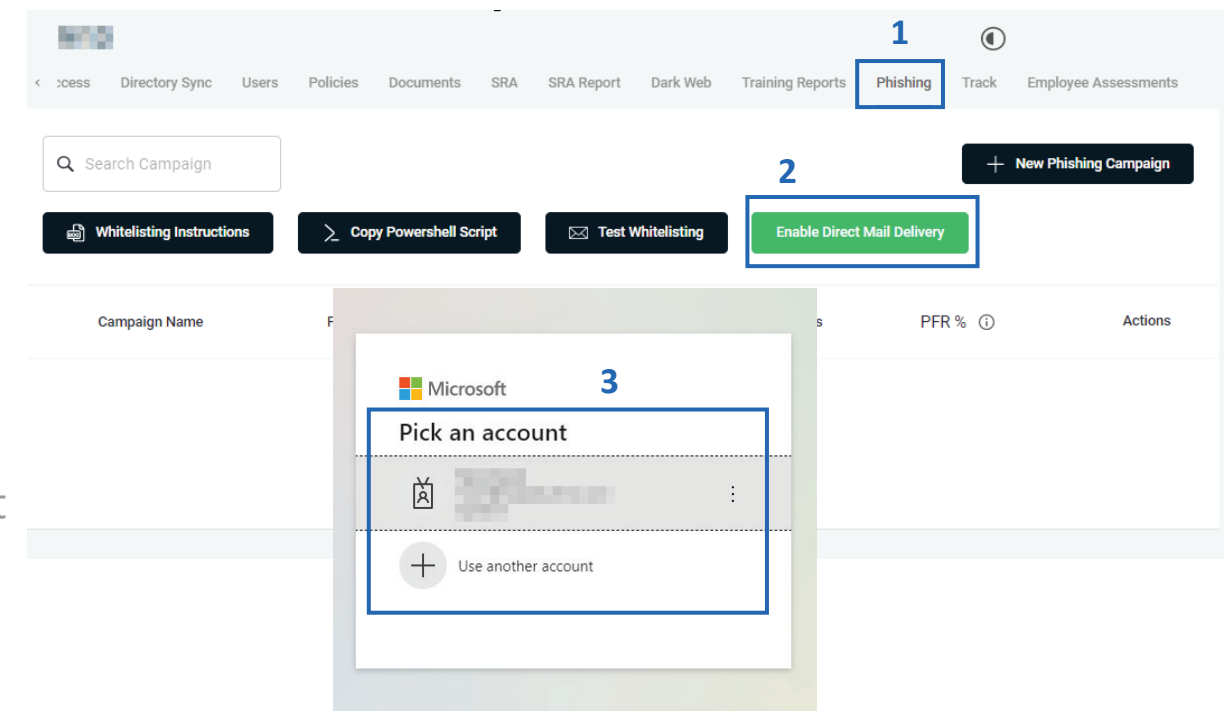
Tired of troubleshooting whitelisting issues with phishing simulations? Enable Direct Mail Delivery, the creme de la crème of whitelisting solutions.

## Feature Overview – Direct Mail Delivery

Our new Direct Mail Delivery feature will help you quickly guarantee these future phishing emails reaching your target's inbox by bypassing spam filters. Avoid the extra steps of whitelisting, testing, and troubleshooting with this easy to enable feature.

**Note:** Direct Mail Delivery is only available to configure for clients in an upgraded (paid) monthly subscription. Additionally, the client needs to have [Azure Active Directory sync](#) enabled in order to use Direct Mail Delivery.

1. Open your desired client and click on the Phishing tab.
2. Click on the “Enable Direct Mail Delivery” button. A confirmation page will appear, click “Enable”
3. You will be directed to the Microsoft Login screen. Select an account that is listed as a Global Admin within your client's tenant to log in with. That's it!
4. You can disable this feature at any time, or you can test the delivery of a phishing message using the “Test Whitelisting” button.



**Note:** We strongly recommend you ensure your portal accounts is protected with the highest security options available including strong passwords, federated login, or MFA.

# One-Time Phishing Campaigns

Learn how to set up your one-time phishing campaign for all Unlimited Training clients – a GREAT prospecting tool – or send a single campaign to any of your subscribing clients. Want to setup an AutoPhish campaign for paying clients? Skip to page 14!

## Navigating to the Phishing Campaign Setup Screen

Name ↑	Branding	Consulting	Insurance	RA	Users	Breaches	ESS	Active	New UI
ABC Worldwide Product: Unlimited Cybersecurity Training					0			✓	✗
Charitable Electronics Product: Unlimited Cybersecurity Training					0			✓	✗
Dunder Mifflin Infinity Product: Unlimited Cybersecurity Training					0			✓	✗
Hermey's Dentistry Product: Unlimited Cybersecurity Training					0			✓	✗

1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in, select “Manage Clients” to access your client list (above).
2. Select the client you would like to begin a Phishing campaign for.
3. Select the “**Phishing**” tab
4. Click the “**New Phishing Campaign**” button to begin

# One-Time Phishing Campaigns

Learn how to set up your one-time phishing campaign for all Unlimited Training clients – a GREAT prospecting tool – or send a single campaign to any of your subscribing clients. Want to setup an AutoPhish campaign for paying clients? Skip to page 14!

## New One-Time Phishing Campaign Setup

1. Create a new campaign

**Campaign Name** 5

**Frequency** 6

☒ Once ☐ Weekly ☐ Bi-Weekly ☐ Monthly ☐ Quarterly

**Choose the dates to run the campaign** 7

**Begin date \*** 2022-12-25 8

☒ Demo campaign 8

**Send between business hours** 9

**Start time \*** 09:00 AM **To** **End time \*** 05:00 PM **Time zone**

**Notification \*** 10 10

2 Days prior 10

**Send Emails Over** 1 11

1 - 6 11

**Enter Notification Email \***

5. Enter a “**Campaign Name**”
6. Select “Once” as the “**Frequency**” of the campaign.  
**Note:** this section of the guide focuses on the single campaign. For ongoing campaigns, view the AutoPhish campaigns which begin on page 14.
7. Set the “**Begin Date**” of your campaign.
8. If “**Demo Campaign**” is selected (optional), this campaign will not affect a user’s Employee Secure Score (ESS).
9. Select the business hours you wish for this campaign to send between along with your client’s time zone.
10. Select if you’d wish to send a notification email two days prior to launch then type in the email (only one email can be added)
11. Select the number of days (1-6) you’d wish the campaign to send over. Selecting “1” will send all the emails on the start day. Numbers higher than 1 will split and send campaigns equally across the selected days.
12. Click “**Next**” to proceed to the next section.

# One-Time Phishing Campaigns

Learn how to set up your one-time phishing campaign for all Unlimited Training clients – a GREAT prospecting tool – or send a single campaign to any of your subscribing clients. Want to setup an AutoPhish campaign for paying clients? Skip to page 14!

## New One-Time Phishing Campaign Setup

2. Select the Recipients

14

Search Role Tag Include New Users ⓘ 3 Items selected

15

13

	Name ↑	Email	Role	Tag	ESS
<input type="checkbox"/>	[Redacted]	[Redacted]	PA		427
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	PA		456
<input type="checkbox"/>	[Redacted]	[Redacted]	M		390
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	PA		350
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	PA		350
<input type="checkbox"/>	[Redacted]	[Redacted]	PA		390

13. Select the recipient(s) you would like to send the campaign to.

14. The employees can be filtered by **Tag** level and **Role**. Additionally, a Search feature is available to quickly find a specific employee.

15. To select all users, click on the checkbox at the top of the user list next to “Name”

16. Click “**Next**” to proceed to the next section

# One-Time Phishing Campaigns

Learn how to set up your one-time phishing campaign for all Unlimited Training clients – a GREAT prospecting tool – or send a single campaign to any of your subscribing clients. Want to setup an AutoPhish campaign for paying clients? Skip to page 14!

## New One-Time Phishing Campaign Setup

✓

Settings

✓

Recipients

11

3

Scenarios

4

Review

3. Select Scenarios

Search

19

Country

Difficulty

Capture Submitted Data

Randomize

Re-use Scenarios

Include New Scenarios

	Name ↑	Country	Difficulty	Capture Submitted Data ⓘ	Actions
<div>17</div> <div><input checked="" type="checkbox"/></div>	Adobe Flash Player Outdated	US	Medium	<div>Yes</div>	<div>18</div> <div><div>Preview Template</div></div>
<div><input type="checkbox"/></div>	Adobe Flash Player Outdated	US	Easy	<div>No</div>	<div>Preview Template</div>
<div><input checked="" type="checkbox"/></div>	Amazon Refund Notification	US	Medium	<div>No</div>	<div>Preview Template</div>
<div><input type="checkbox"/></div>	Amazon Security Alert	US	Hard	<div>No</div>	<div>Preview Template</div>
<div><input type="checkbox"/></div>	Amex Account Update (Mailing Address)	US	Hard	<div>No</div>	<div>Preview Template</div>

17. Select a phishing scenario(s) you would like to send. Use the “**Next**” and “**Last**” buttons at the bottom of the box to page through the library of templates. If multiple campaigns are selected, they will be randomly distributed amongst the selected users.

18. Click on “Preview Template” to preview what users will be sent once the campaign is initiated.

19. The scenarios can be filtered by **Difficulty** level and **Country**. Additionally, a Search feature is available to quickly find a specific scenario.

Continued on next page...

# One-Time Phishing Campaigns

Learn how to set up your one-time phishing campaign for all Unlimited Training clients – a GREAT prospecting tool – or send a single campaign to any of your subscribing clients. Want to setup an AutoPhish campaign for paying clients? Skip to page 14!

## New One-Time Phishing Campaign Setup

✓

Settings

✓

Recipients

3

Scenarios

4

Review

3. Select Scenarios

Search

Country

Difficulty

Capture Submitted Data  
All

☒ Randomize ⓘ

☐ Re-use Scenarios ⓘ

☐ Include New Scenarios ⓘ

<input checked="" type="checkbox"/>	Name ↑	Country	Difficulty	Capture Submitted Data ⓘ	Actions
<input checked="" type="checkbox"/>	Adobe Flash Player Outdated	US	Medium	<div>Yes</div>	<a href="#">Preview Template</a>
<input type="checkbox"/>	Adobe Flash Player Outdated	US	Easy	<div>No</div>	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>	Amazon Refund Notification	US	Medium	<div>No</div>	<a href="#">Preview Template</a>
<input type="checkbox"/>	Amazon Security Alert	US	Hard	<div>No</div>	<a href="#">Preview Template</a>
<input type="checkbox"/>	Amex Account Update (Mailing Address)	US	Hard	<div>No</div>	<a href="#">Preview Template</a>

20. Certain campaigns now offer a “Capture Submitted Data” feature. If “Yes” is shown in this column, the scenario includes a fake landing page that users will be directed to after clicking on the initial phishing link. The fake landing page will prompt the user to enter their login credentials or other information. If submitted, no data will be saved, but the user will lose more points off their ESS than they would for just clicking on the link.

21. Click “**Next**” to proceed to the next section



# One-Time Phishing Campaigns

Learn how to set up your one-time phishing campaign for all Unlimited Training clients – a GREAT prospecting tool – or send a single campaign to any of your subscribing clients. Want to setup an AutoPhish campaign for paying clients? Skip to page 14!

## New One-Time Phishing Campaign Setup

22

Settings

Recipients

Scenarios

4 Review

1.Campaign settings

Campaign Name: [text] Frequency: Once Dates: [text] Hours: 9:00 am to 5:00 pm Notification: None

Send Emails Over : 1 Days

2.Recipients (1)

Employee: 1

3.Scenarios (2)

Medium Difficulty: 1 Hard Difficulty: 1

22

Previous Step

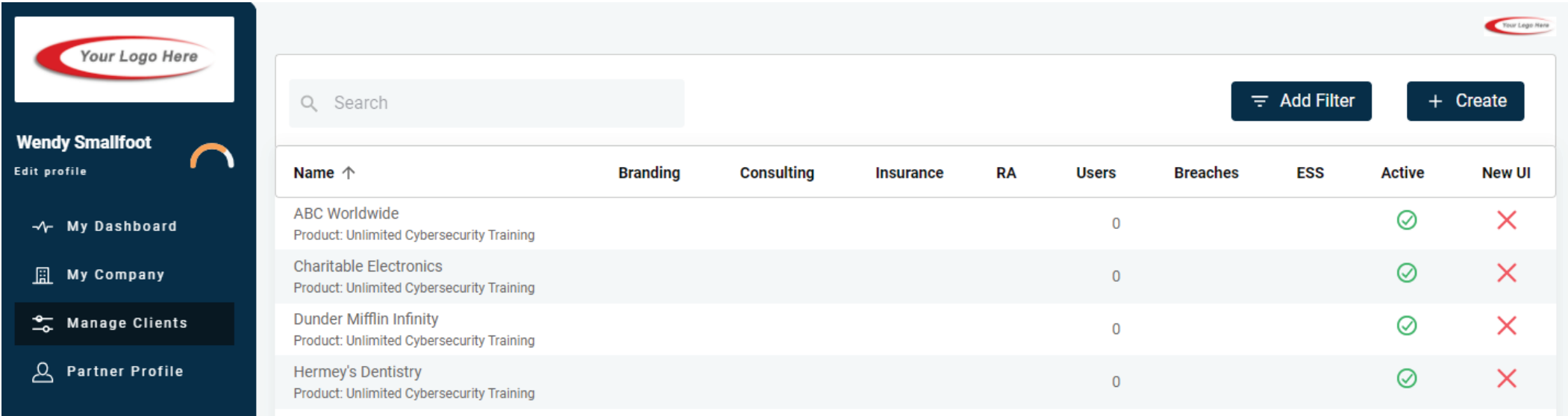
Create Campaign

22. Review your phishing settings and click “**Create Campaign**” to launch your campaign! You may View, Edit, or Delete this at any time in the Phishing Campaign List.

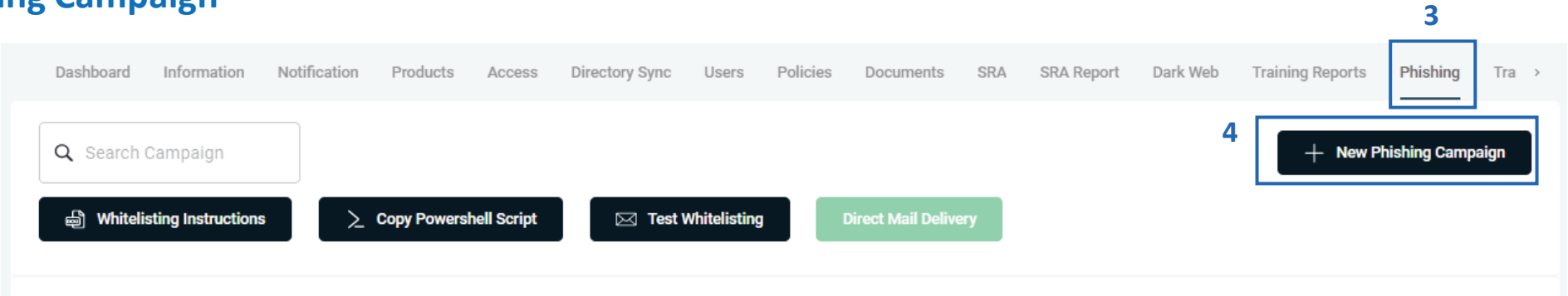
# AutoPhish Automated Phishing Campaigns

Set up ongoing simulated phishing campaigns for the entire year in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are set up with our Catch Phish Email Analysis Tool.

## Navigating to the AutoPhish Setup Screen



- 1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged click the “Manage Clients” application to see your full list of clients.
- 2. Select the client you would like to setup an AutoPhish campaign for. Note: Client must be in a BPP, HIPAA BPP, or EVA MD product to complete ongoing phishing with AutoPhish.
- 3. Select the “**Phishing**” tab to view the Phishing page.
- 4. Click “**New Phishing Campaign**” to begin.



# AutoPhish Automated Phishing Campaigns

Set up ongoing simulated phishing campaigns for the entire year in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are set up with our Catch Phish Email Analysis Tool.

## New AutoPhish Campaign Setup

1. Create a new campaign

5 Campaign Name

Frequency ⓘ

6 ☐ Once ☐ Weekly ☒ Bi-Weekly ☐ Monthly ☐ Quarterly

7 Choose the dates to run the campaign ⓘ

Begin date \*  End date \*

8 Send between business hours ⓘ

Start time \*  To End time \*  Time zone

9 Notification \*  ⓘ

10 Send Emails Over  1 - 6 Days ⓘ

Enter Notification Email \*

5. Enter a “**Campaign Name**”
6. Select a the “**Frequency**” of the campaign, either Bi-Weekly, Monthly, or Quarterly. **Note:** this section of the guide focuses on an ongoing campaign. For single campaigns, view the One Time campaigns which begin on page 8.
7. Set the “**Begin date**” of your campaign then select the “**End date**”.
8. Select the business hours you wish for this campaign to send between along with your client’s time zone.
9. Select if you’d wish to send a notification email two days prior to launch then type in the email (only one email can be added)
10. Select the number of days (1-6) you’d wish the campaign to send over. Selecting “1” will send all the emails on the start day. Numbers higher than 1 will split and send campaigns equally across the selected days.
11. Click “**Next**” to proceed to the next section.

# AutoPhish Automated Phishing Campaigns

Set up ongoing simulated phishing campaigns for the entire year in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are set up with our Catch Phish Email Analysis Tool.

## New AutoPhish Campaign Setup

✓

2

3

4

Settings

Recipients

Scenarios

Review

2. Select the Recipients

13

Search

Role

Tag

15

Include New Users

106 Items selected

14

12

✓

Name ↑

✓

✓

✓

✓

✓

Email

PA

PA

M

PA

PA

Role

PA

PA

M

PA

PA

Tag

ESS

427

456

390

350

350

12. Select the recipient(s) you would like to send the campaign to.

13. The employees can be filtered by **Tag** level and **Role**. Additionally, a Search feature is available to quickly find a specific employee.

14. To select all users, click on the checkbox at the top of the user list next to “Name”

15. If you’d want newly added users to the portal to receive future campaigns, switch the “Include New Users” toggle on.

16. Click “**Next**” to proceed to the next section

# AutoPhish Automated Phishing Campaigns

Set up ongoing simulated phishing campaigns for the entire year in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are set up with our Catch Phish Email Analysis Tool.

## New One-Time Phishing Campaign Setup

3.Select Scenarios

19

Search

CountryDifficultyCapture Submitted DataAll

RandomizeRe-use ScenariosInclude New Scenarios

17

<input checked="" type="checkbox"/>	Name ↑	Country	Difficulty	Capture Submitted Data ⓘ	Actions
<input checked="" type="checkbox"/>		US	Medium	Yes	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>		US	Easy	No	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>		US	Medium	No	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>		US	Hard	No	<a href="#">Preview Template</a>

18

17. Select the phishing scenario(s) you would like to send. Use the “Next” and “Last” buttons at the bottom of the box to page through the library of templates. If multiple campaigns are selected, they will be randomly distributed amongst the selected users.
18. Click on “Preview Template” to preview what users will be sent once the campaign is initiated.
19. The scenarios can be filtered by Difficulty level and Country. Additionally, a Search feature is available to quickly find a specific scenario.
- Continued on next page...

# AutoPhish Automated Phishing Campaigns

Set up ongoing simulated phishing campaigns for the entire year in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are set up with our Catch Phish Email Analysis Tool.

## New One-Time Phishing Campaign Setup

3. Select Scenarios

Search

Country

Difficulty

Capture Submitted Data

Yes

21

Randomize ⓘ

Re-use Scenarios ⓘ

Include New Scenarios ⓘ

20

<input checked="" type="checkbox"/>	Name ↑	Country	Difficulty	Capture Submitted Data ⓘ	Actions
<input checked="" type="checkbox"/>		US	Medium	Yes	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>		US	Easy	Yes	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>		US	Medium	Yes	<a href="#">Preview Template</a>
<input checked="" type="checkbox"/>		US	Hard	Yes	<a href="#">Preview Template</a>

20. Certain campaigns now offer a “Capture Submitted Data” feature. If “Yes” is shown in this column, the scenario includes a fake landing page that users will be directed to after clicking on the initial phishing link. The fake landing page will prompt the user to enter their login credentials or other information. If submitted, no data will be saved, but the user will lose more points off their ESS than they would for just clicking on the link.

21. Options to “Randomize” the campaigns, which will send different templates amongst users each campaign, “Re-use Scenarios”, which will repeat already used scenarios, and “Include New Scenarios”, which will include newly created scenarios to the pool, are available to be enabled or disabled.

22. Click “Next” to proceed to the next section

# AutoPhish Automated Phishing Campaigns

Set up ongoing simulated phishing campaigns for the entire year in just a few simple steps! View our service comparison here to see eligible subscriptions. Make sure your users are set up with our Catch Phish Email Analysis Tool.

## New One-Time Phishing Campaign Setup

✓

Settings

✓

Recipients

✓

Scenarios

4

Review

1.Campaign settings23

Campaign Name: Test Campaign

Frequency: Bi-weekly

Dates: 2022-10-25 to 2024-10-25

Hours: 9:00 am to 5:00 pm

Notification: None

Send Emails Over : 1 Days

2.Recipients (1)

Include New Users: No

Manager Admin: 1

3.Scenarios (23)

Include New Scenarios: Yes

Countries: AU - 3, CA - 3, GB - 1, US - 16,

Easy Difficulty: 2

Hard Difficulty: 12

Medium Difficulty: 9

Capture Submitted Data: Yes

Previous Step

Create Campaign

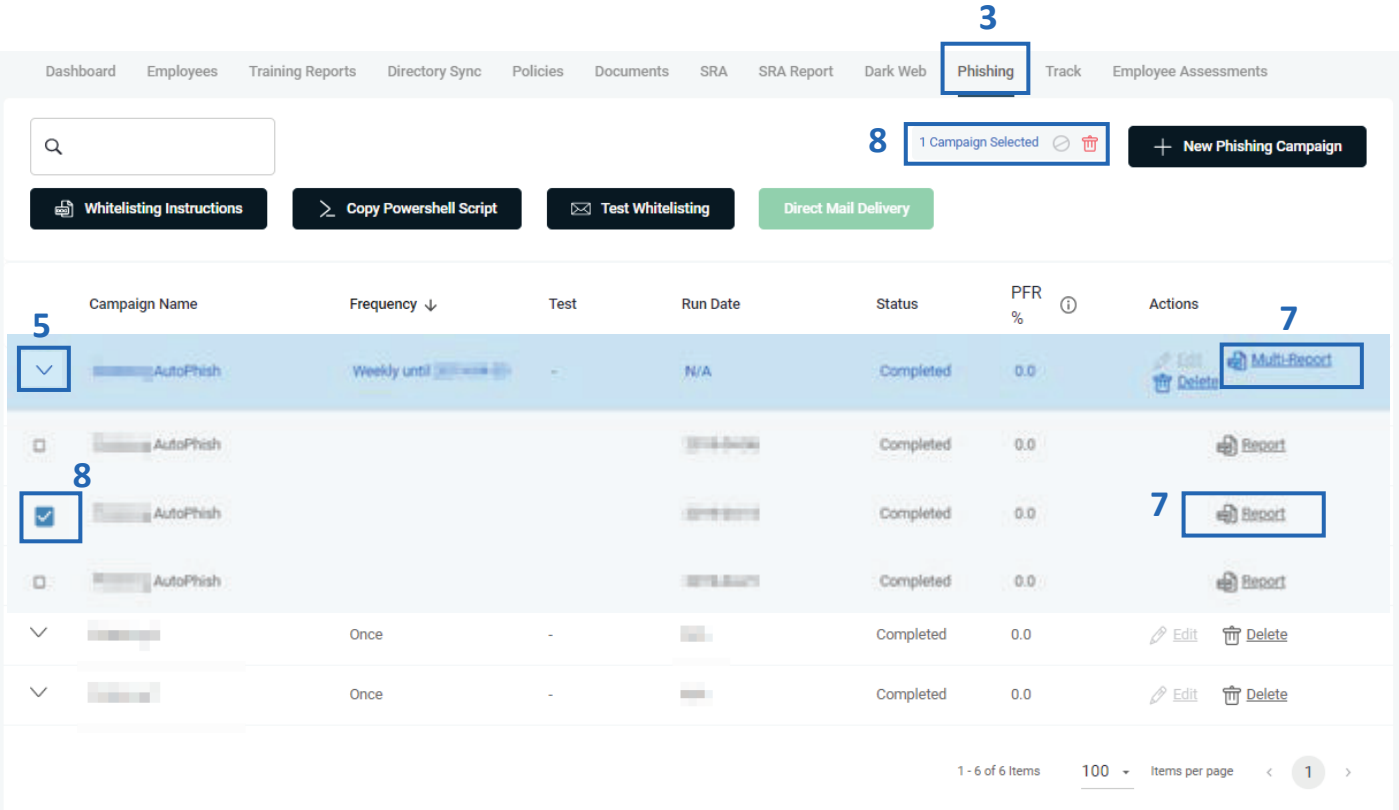
23. Review your phishing settings and click “**Create Campaign**” to launch your campaign! You may View, Edit, or Delete this at any time in the Phishing Campaign List.

23

# Phishing Reports

View the results of any initiated phishing campaign – One-Time or AutoPhish – in the Phishing Campaign List.  
Get details including email deliverability, scenario difficulty and summary, and user result list!

## Navigating to the Phishing Campaign List



1. Login as a Partner Administrator to the PII-Protect portal [here](#). Once logged in, select “Manage Clients” to access your client list (above).
2. Select the client you would like to view the Phishing results for.
3. Select the “**Phishing**” tab
4. The list of active and completed campaigns will be shown within the table.

5. For ongoing campaigns, click the “down” arrow icon next to the Campaign Name to view all the sub-campaigns sent.
6. Clicking on the campaign will open a quick view of the campaign statistics.
7. A single “**Report**” is available for each campaign, or a “**Multi-Report**” can be downloaded which encapsulates the entire subset of campaigns within the AutoPhish campaign.
8. A phishing campaign can be ended early and/or deleted. Select the campaign so the “checkmark” appears, then click the “**Stop**” or “**Delete**” icon in the top right.





☞ You're All Set!

 **Telesystem**<sup>®</sup>  
IT's About Trust<sup>®</sup>

**#HACKERS SUCK**

[www.TrustTelesystem.com](http://www.TrustTelesystem.com)