

Phishing Simulation Manual

Overview

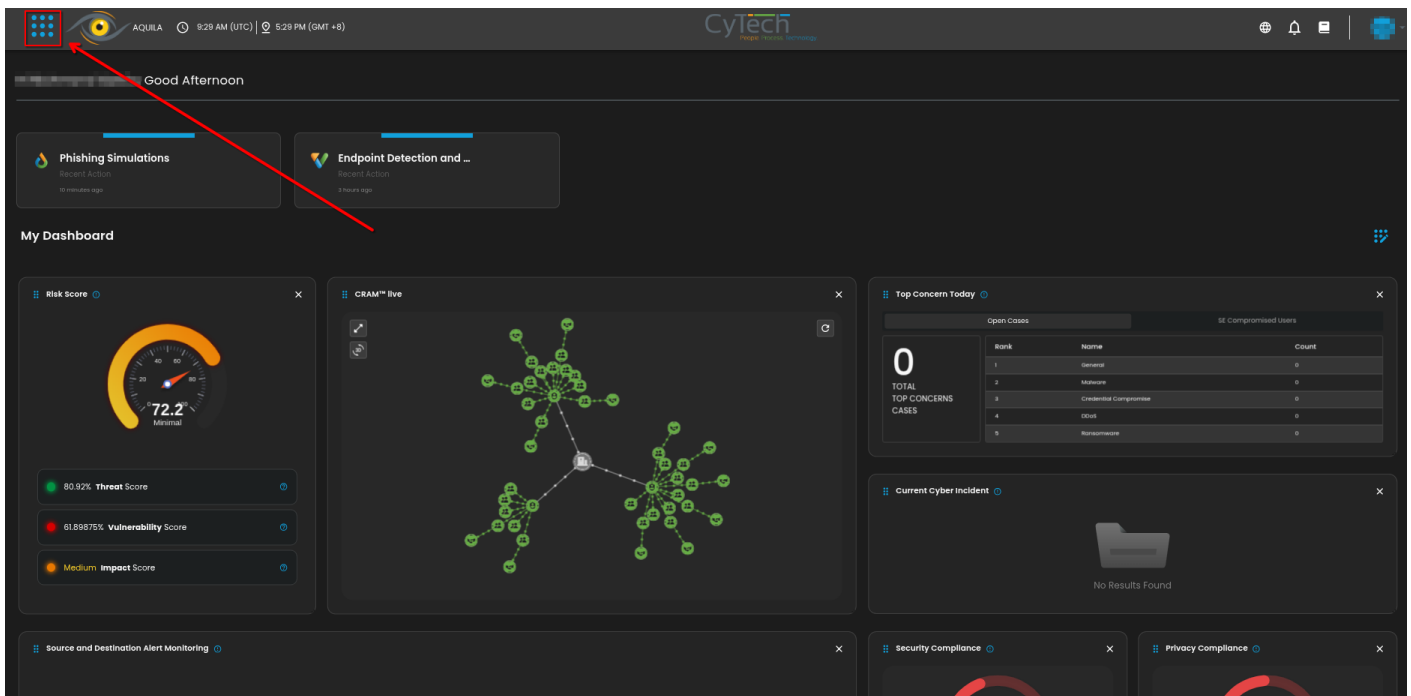
Welcome to the Phishing Simulation module. In this section, you'll be guided through the process of using our Phishing Simulation tool. You'll learn how to:

- Navigate through the module interface.
- Understand and utilize the dashboard and its components.
- Navigate through different templates
- Navigate and understand the Recipients Dashboard
- Create and initiate a Phishing Campaign simulation.

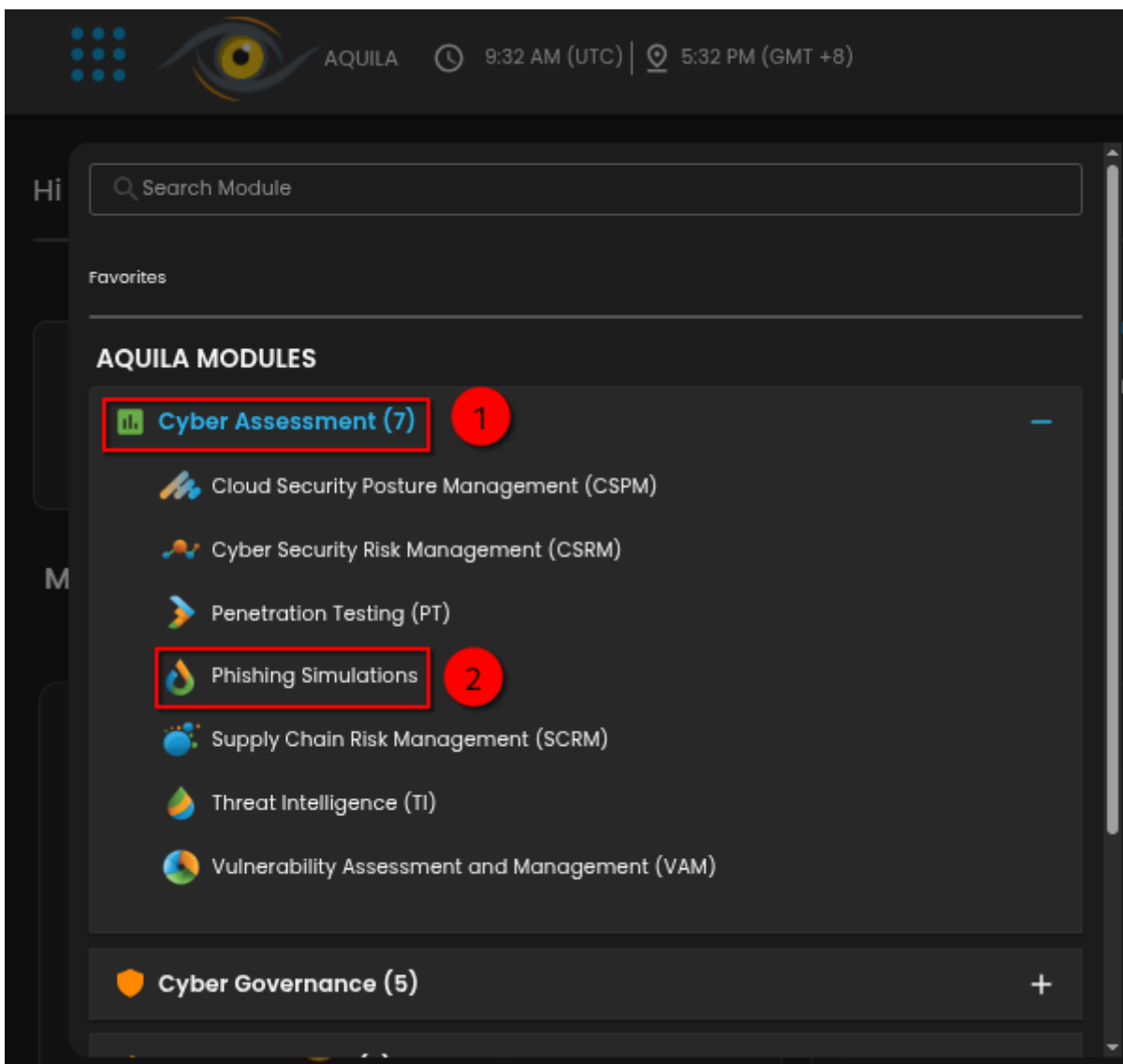
Phishing simulation is a cybersecurity training method where fake phishing emails or messages are sent to employees within an organization to test their ability to recognize and respond to such threats. By mimicking real phishing attempts, these simulations track user interactions, such as clicking on malicious links or entering sensitive information, and provide feedback to improve awareness and prevent actual attacks. This approach helps identify vulnerabilities, educates users on best practices, and enhances overall security by reinforcing the skills needed to detect and handle phishing threats.

Navigate to the module:

- Click on the menu icon to show all the different modules

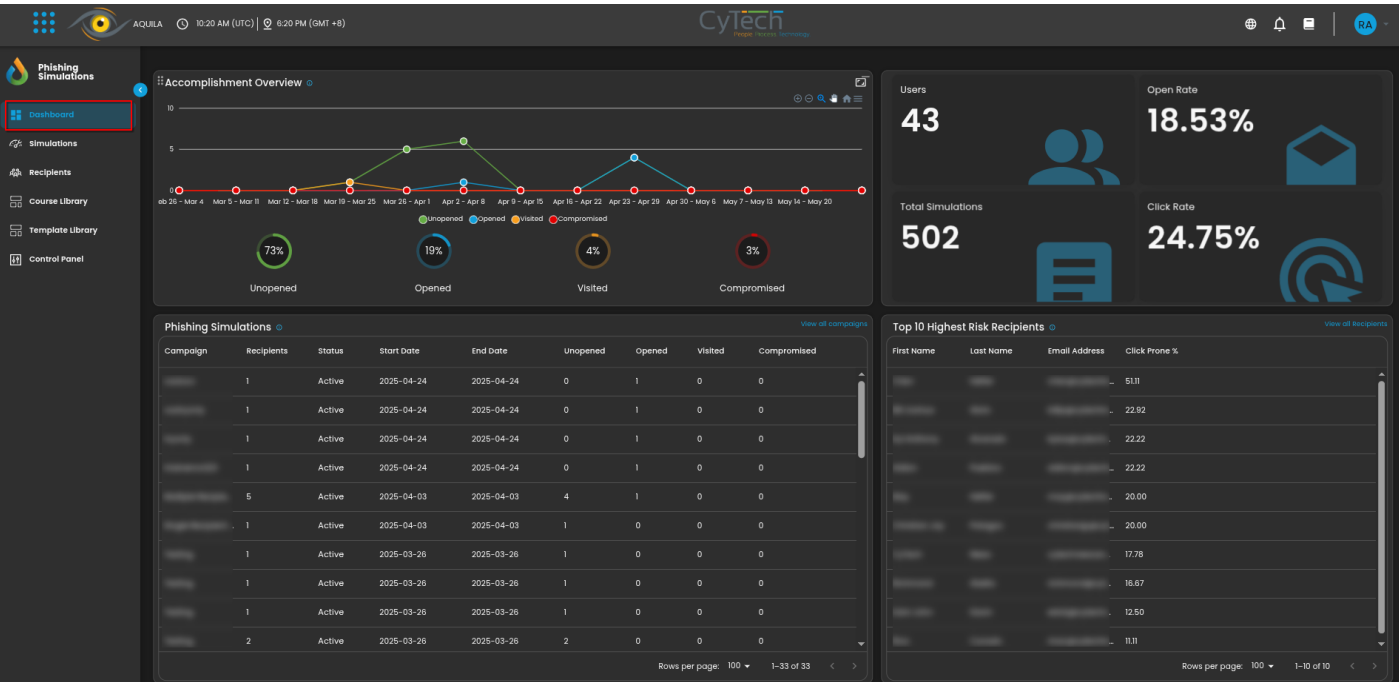


- Under Cyber Assessment, click on Phishing Simulations

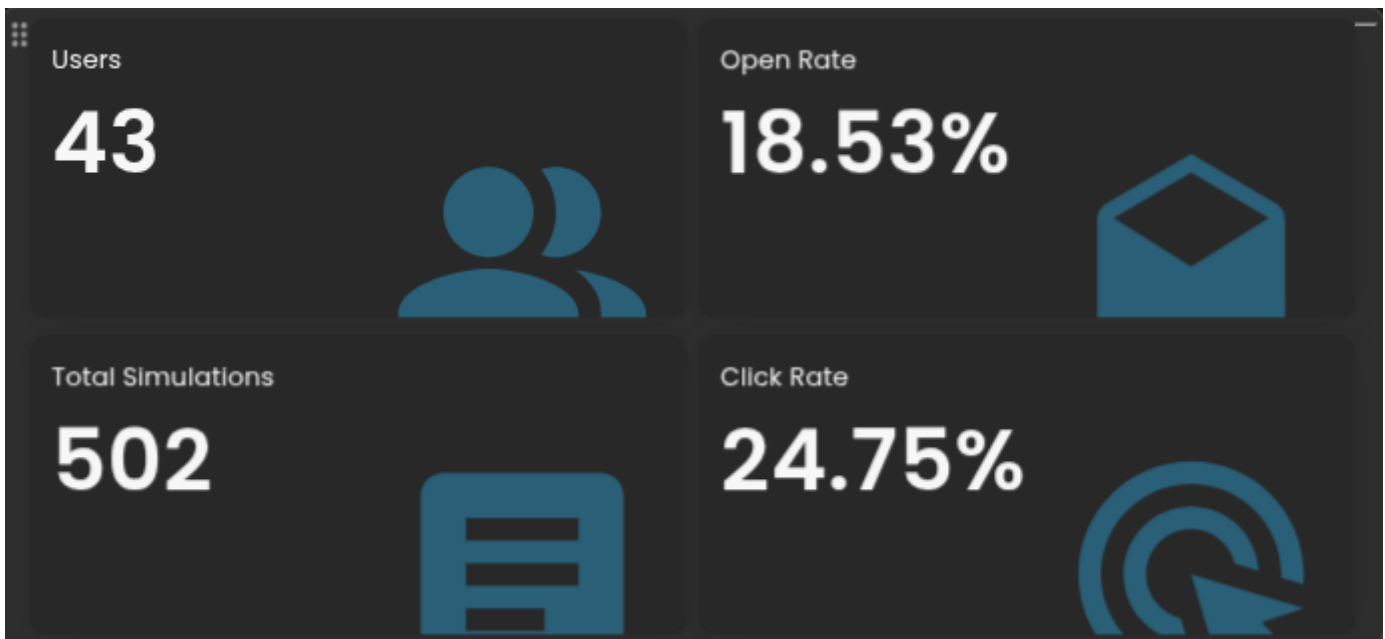


Phishing Simulation Dashboard:

- The dashboard provides a comprehensive view of phishing simulation campaigns, helping organizations monitor and analyze their effectiveness. It tracks key metrics such as the number of active campaigns, start and end dates, and recipient engagement, including how many recipients opened the email, clicked on links, or were compromised. The dashboard features visual tools like charts and graphs to represent these metrics, making it easier to assess overall campaign performance and identify trends over time. Detailed and summary reports offer insights into individual and collective recipient behavior, enabling organizations to gauge the impact of their phishing simulations, improve security awareness, and tailor additional training efforts. This tool is essential for evaluating the effectiveness of security training programs and enhancing overall organizational security.



- On the right-hand side of the phishing simulation dashboard, key metrics provide a snapshot of the organization’s phishing simulation efforts. This section displays the total number of users within the organization, offering insight into the scope of the simulations. It also shows the total number of phishing simulations executed, tracking the volume of tests conducted. Additionally, the dashboard presents open rates, which reflect the percentage of users who opened the phishing emails, and click rates, indicating the percentage of users who clicked on links within those emails. These metrics collectively help assess the effectiveness of the phishing simulations, gauge user engagement, and evaluate the impact of security awareness initiatives.



- The top 10 Highest risk recipients shows the top users in an organization that is more likely to be susceptible to phishing attacks based on their interactions with the simulation emails. It typically includes metrics such as the number of emails opened, the frequency of clicks on malicious links, and instances of compromised actions. By focusing on these high-risk individuals, organizations can tailor targeted training and support to improve their security awareness and reduce their vulnerability to real phishing attacks. This feature allows security teams to prioritize their efforts and address potential weaknesses in their organization's defenses more effectively.

Top 10 Highest Risk Recipients

View all Recipients

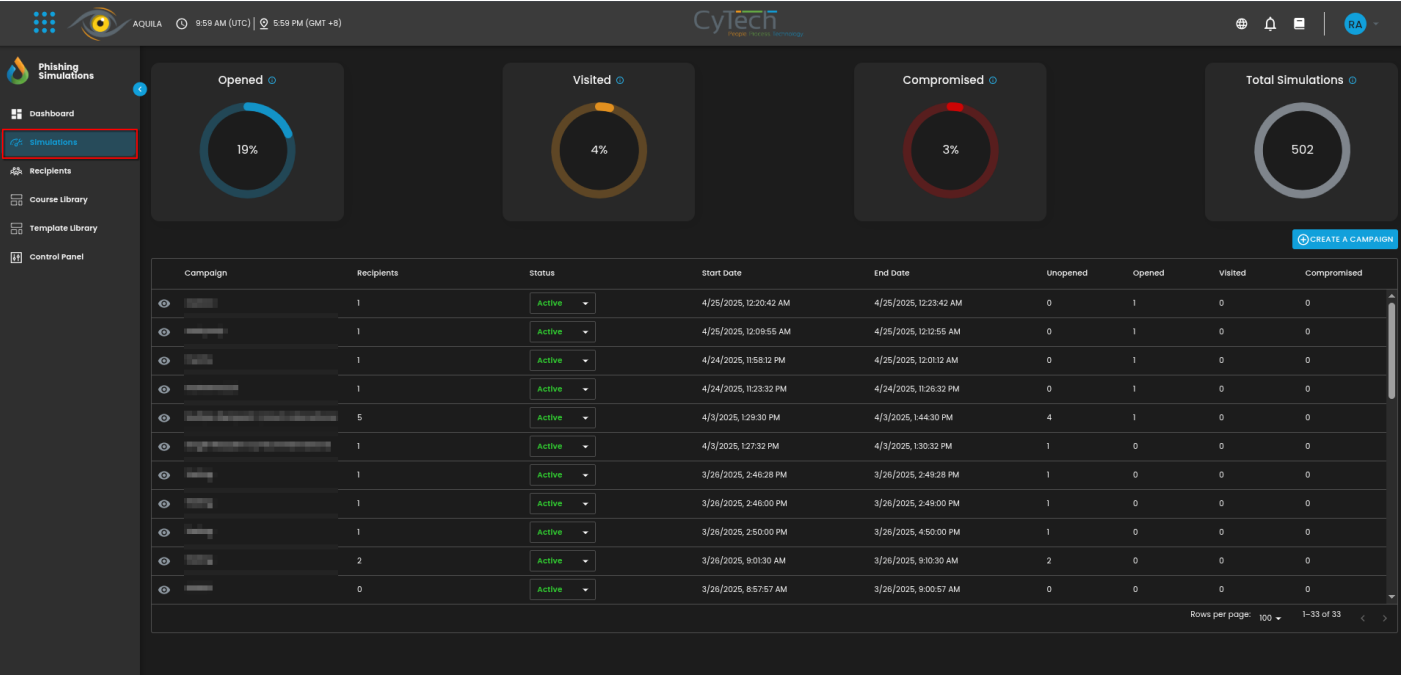
First Name	Last Name	Email Address	Click Prone %
C			51.11
E			22.92
E			22.22
A			22.22
I			20.00
C			20.00
C			17.78
E			16.67
E			12.50
E			11.11

Rows per page: 1001-10 of 10

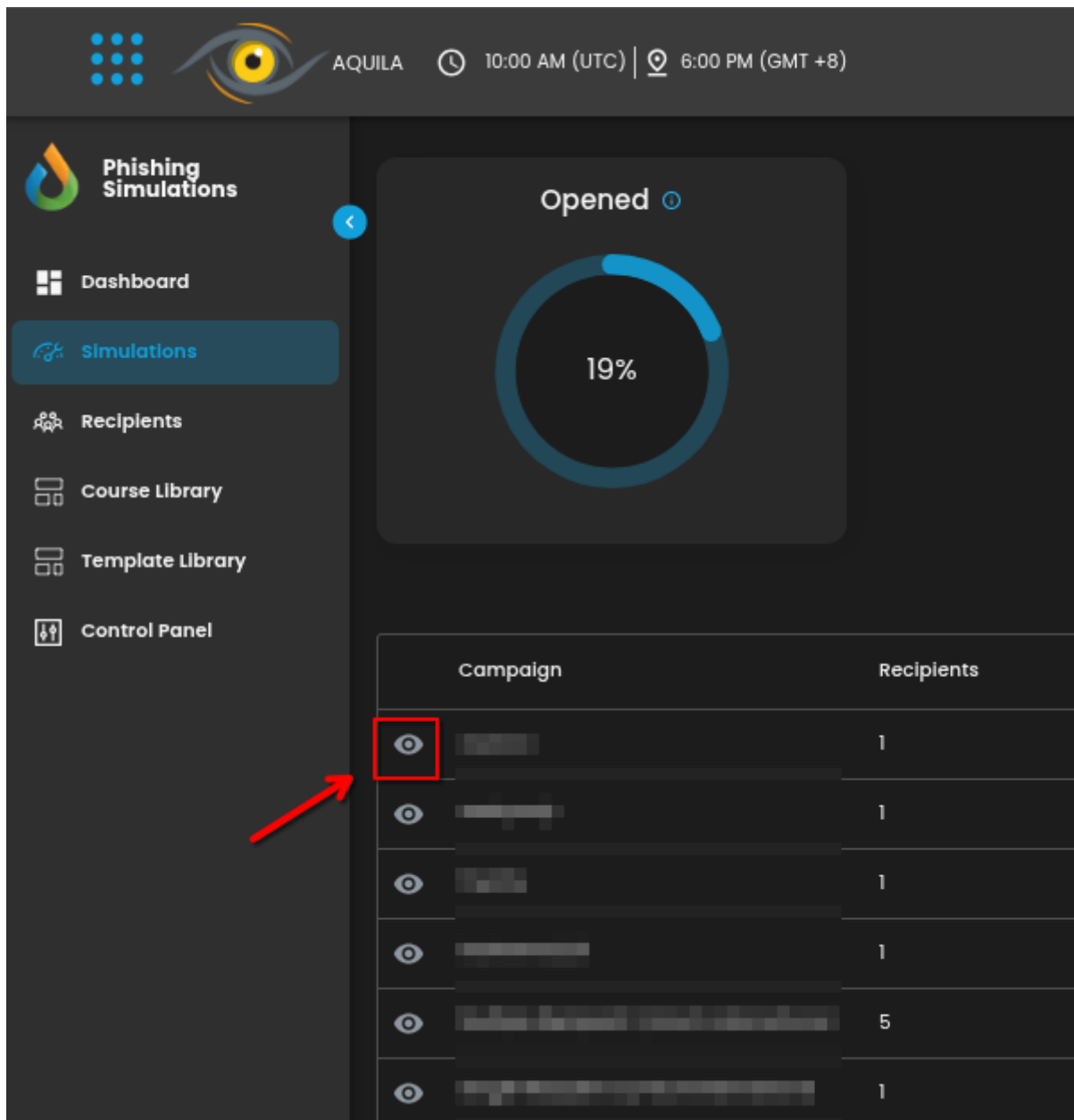
Simulations Campaign Dashboard:

The dashboard offers a detailed overview of phishing simulation campaigns, showcasing critical information about each campaign's status and performance. It indicates whether a campaign is active and provides the start and end dates. The dashboard also tracks recipient engagement, displaying counts of those who have not opened, opened, visited, or been compromised by the simulations, allowing for effective monitoring and impact assessment.

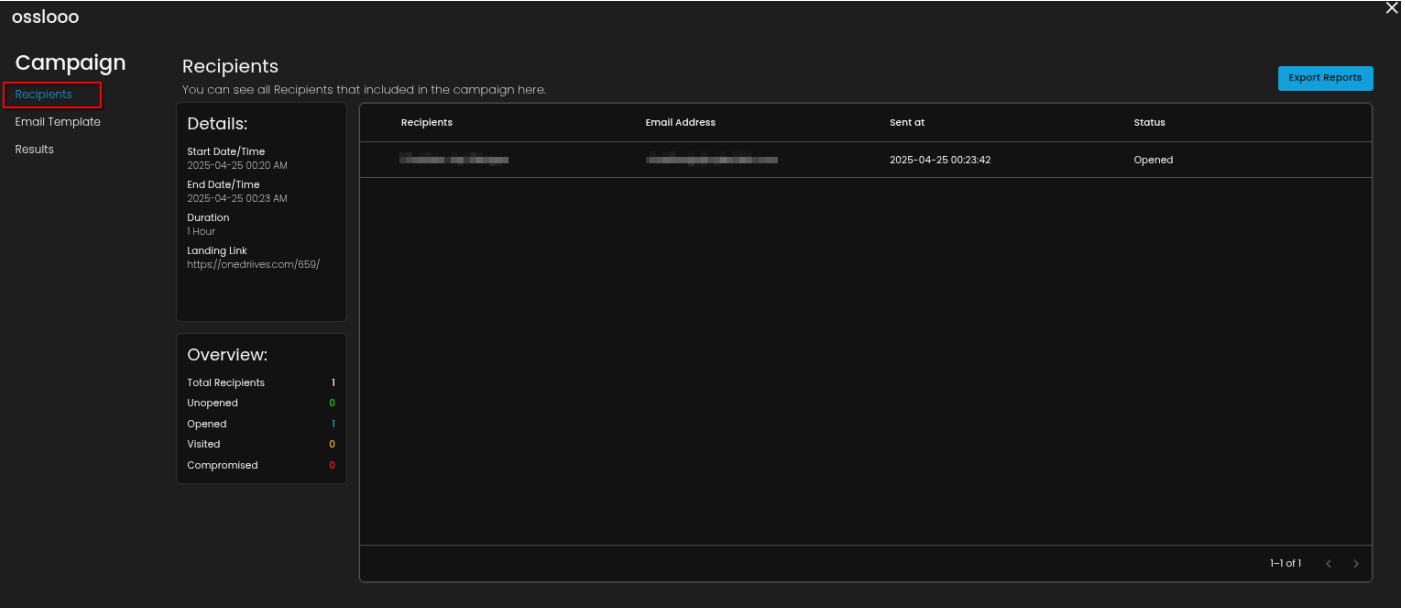
Additionally, a chart visualizes the percentage of recipients who opened, visited, or were compromised, relative to the total number of simulations conducted. This visualization helps you quickly grasp the effectiveness of your phishing campaigns and their overall impact.



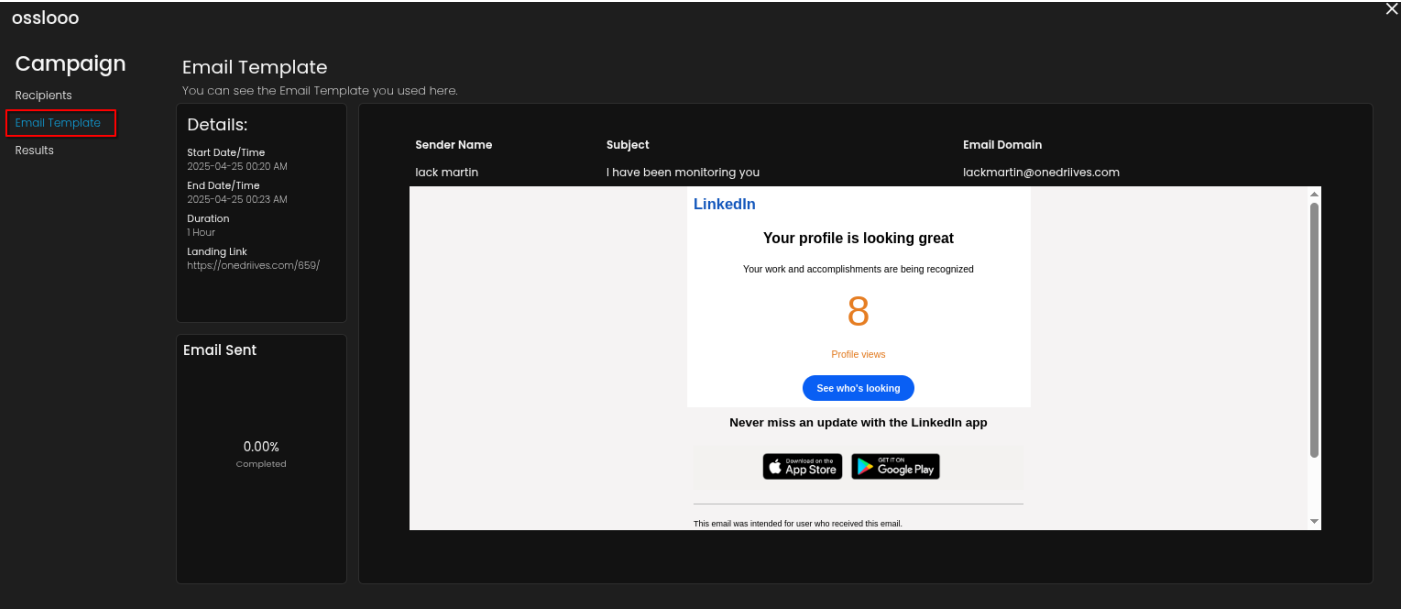
- To view more details about a specific campaign, click on a specific campaign.



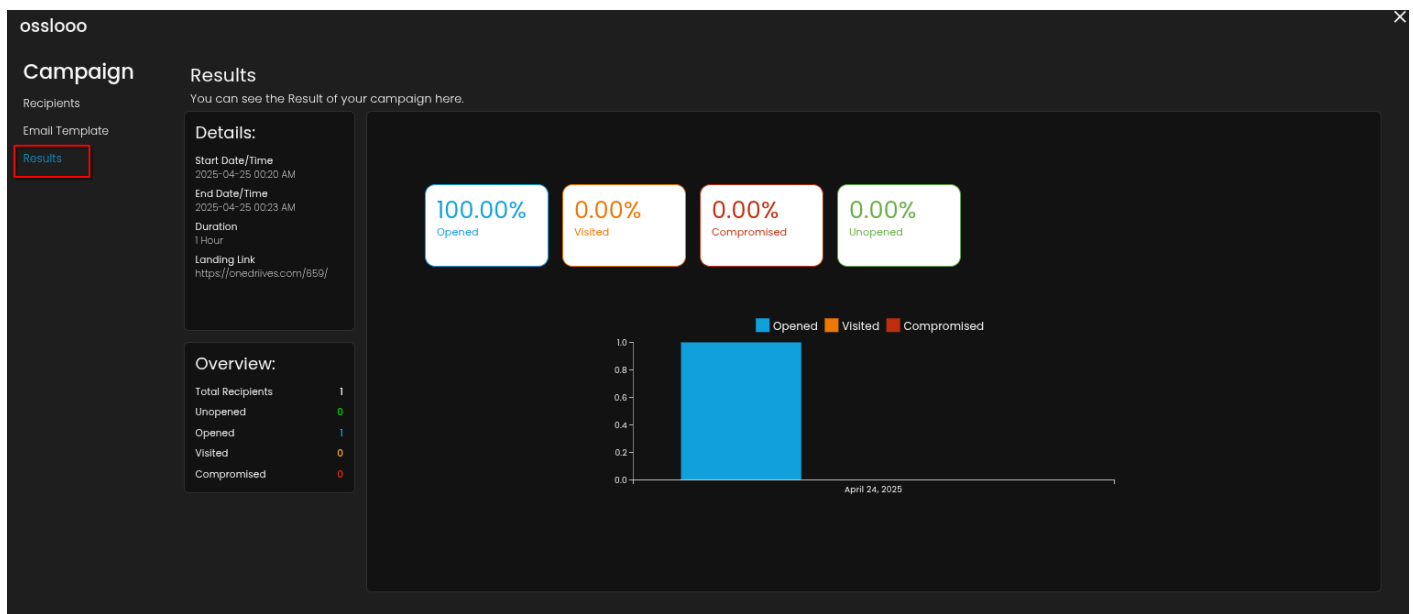
- This section provides an in-depth view of a specific phishing simulation campaign, offering detailed insights into the participants and the campaign's outcomes. It includes a list of all recipients involved, complete with their respective details.



- Additionally, it features information about the email template used in the campaign, along with a preview of how the email appeared to the recipients.

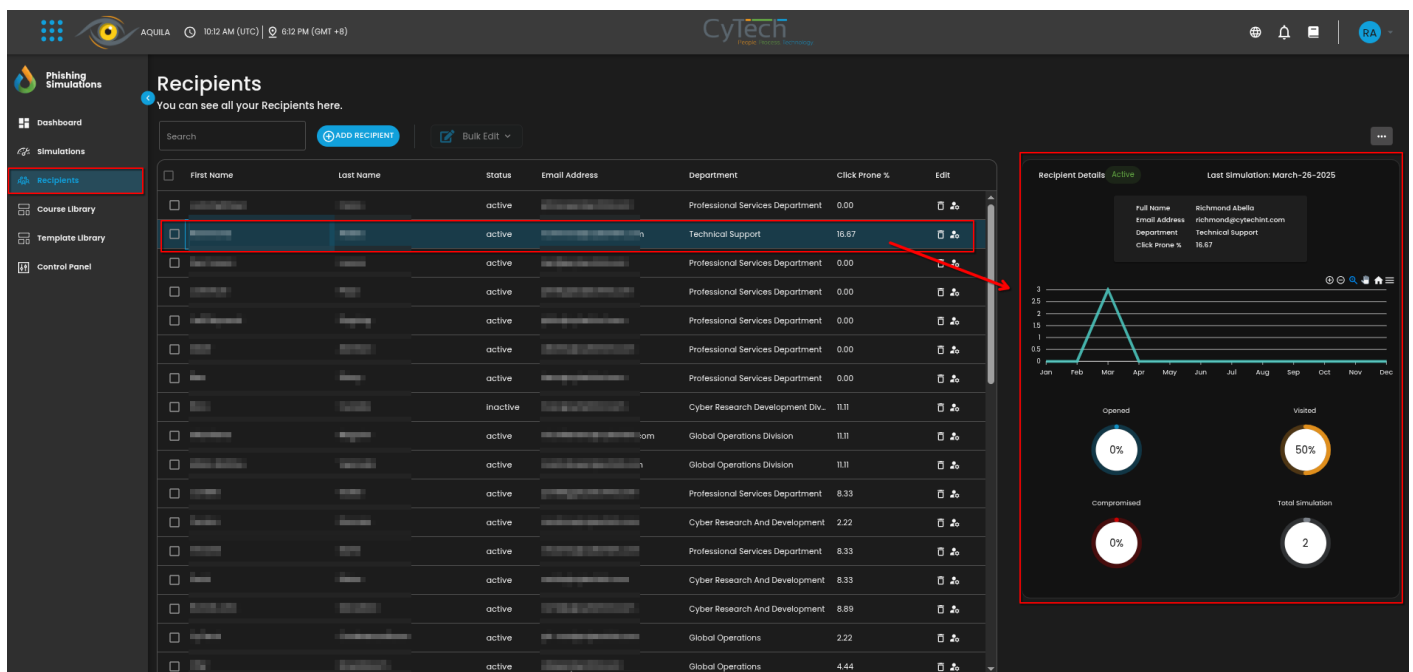


- The results of the campaign are displayed in this modal view, including a comprehensive summary of recipient interactions. A graph visualizes key statistics, showing the number of users who opened the phishing email, visited the links, were compromised, or did not open the email. This detailed overview allows for a thorough analysis of the campaign's effectiveness and recipient engagement.



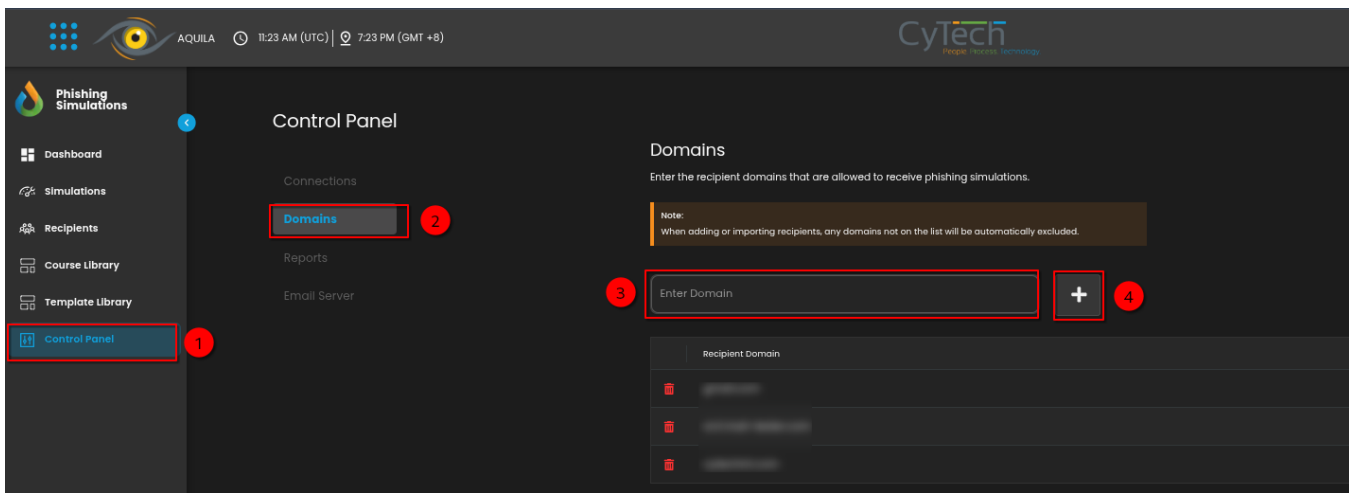
Recipients Dashboard:

The recipients dashboard shows all the recipients of an organization that will be monitored during phishing simulations. It shows information such as their full name, status, email address, department in the organization, as well as the click prone percentage. The click prone percentage shows how likely they are to click on phishing emails when simulations are being conducted.



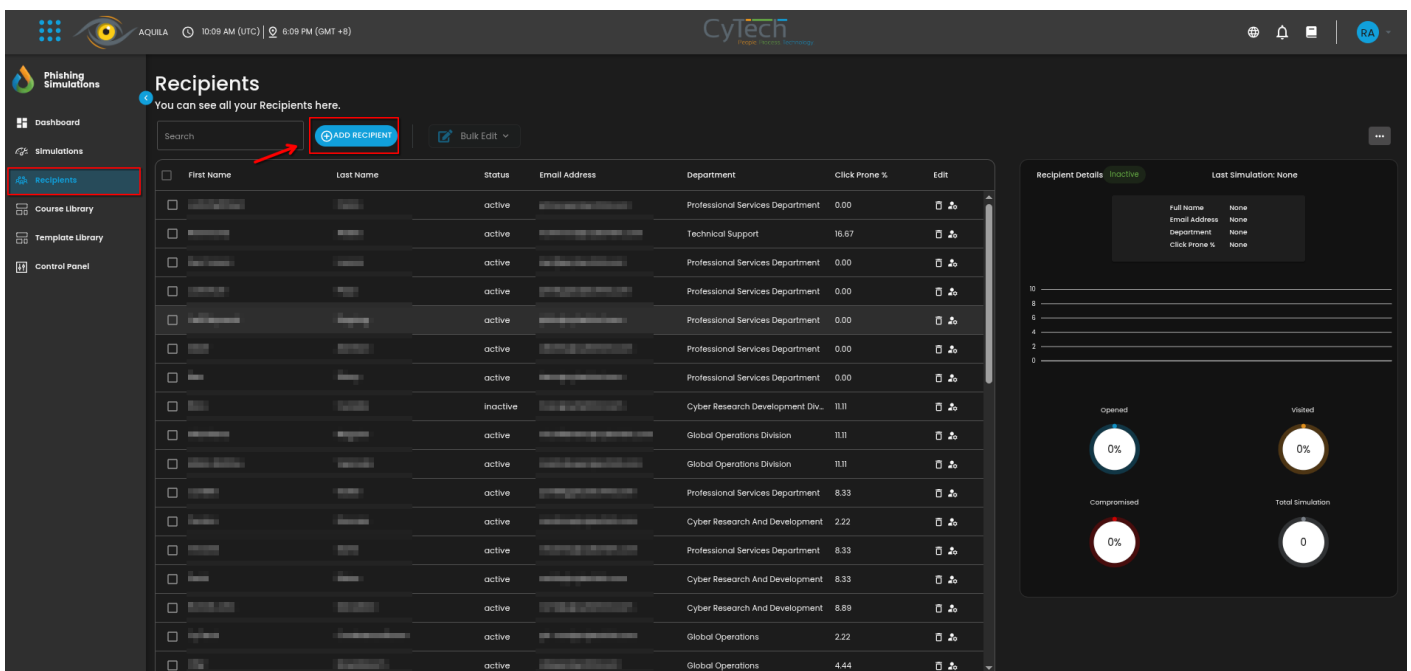
Add Domain:

- You must add the domains before adding recipients to the list. This ensures that the specified domains are authorized to receive phishing simulations.

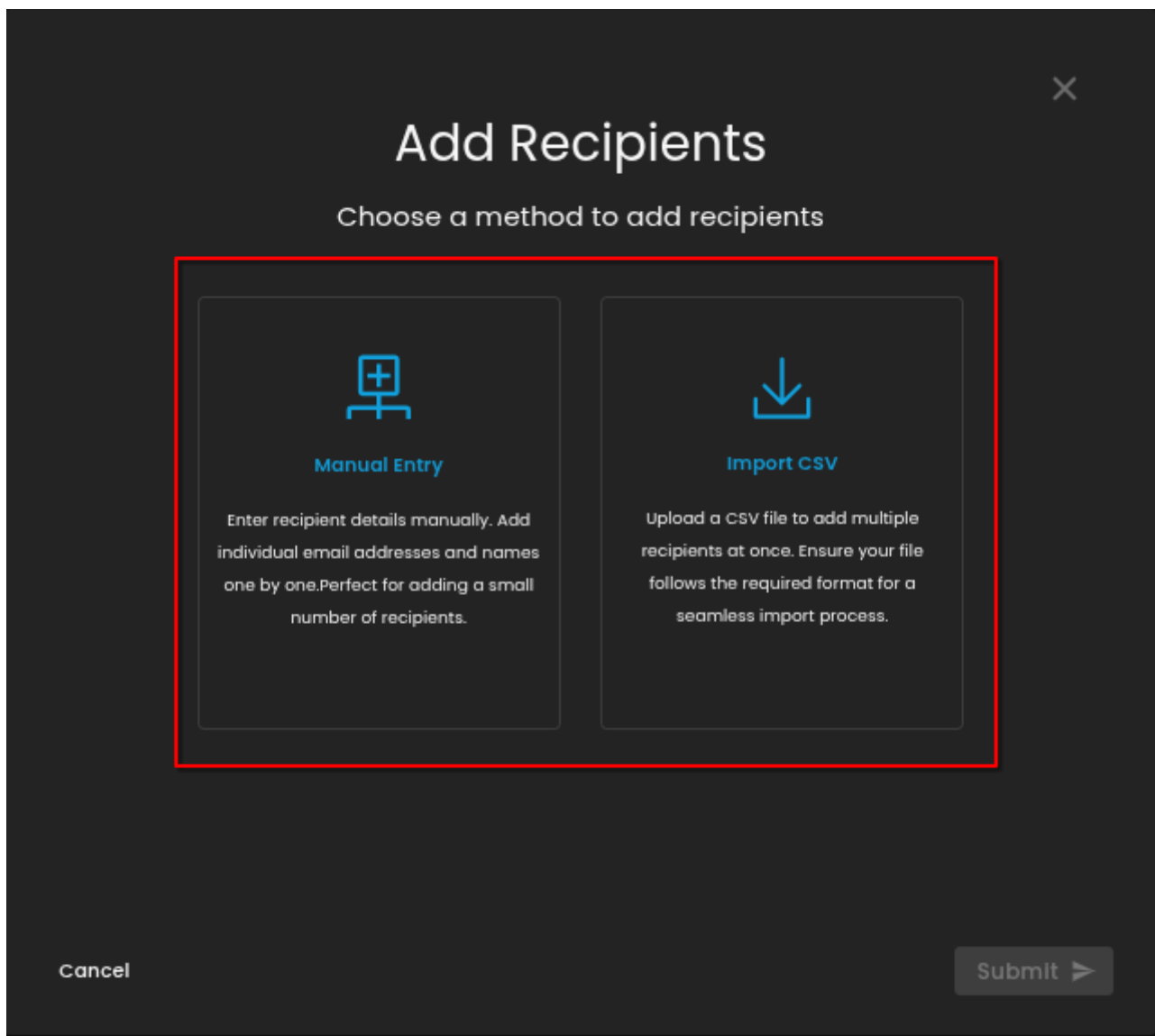


Add Recipients:

- Click on the add recipient button to add recipients



- A modal is then shown with options such as manual entry or import CSV.



- **Manual Entry** - Manually enter a recipient's individual details. Perfect for adding only a small number of recipients.

✕

Manual Entry

Please enter all the necessary details in the provided fields.

Note: Only email addresses from the domains listed in your control panel are accepted here.

First Name

Last Name

Email

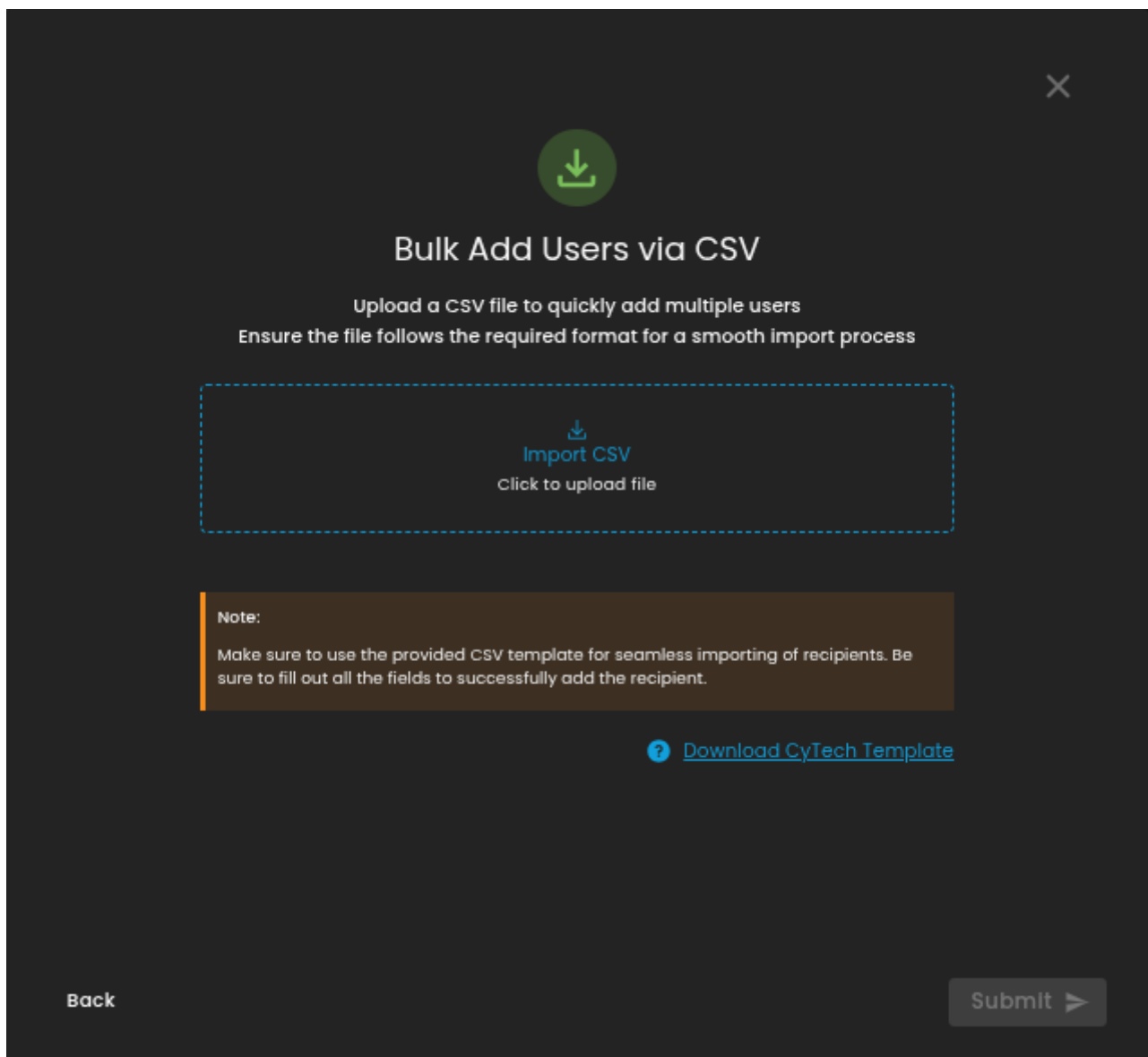
Department

+

Back

Submit ➤

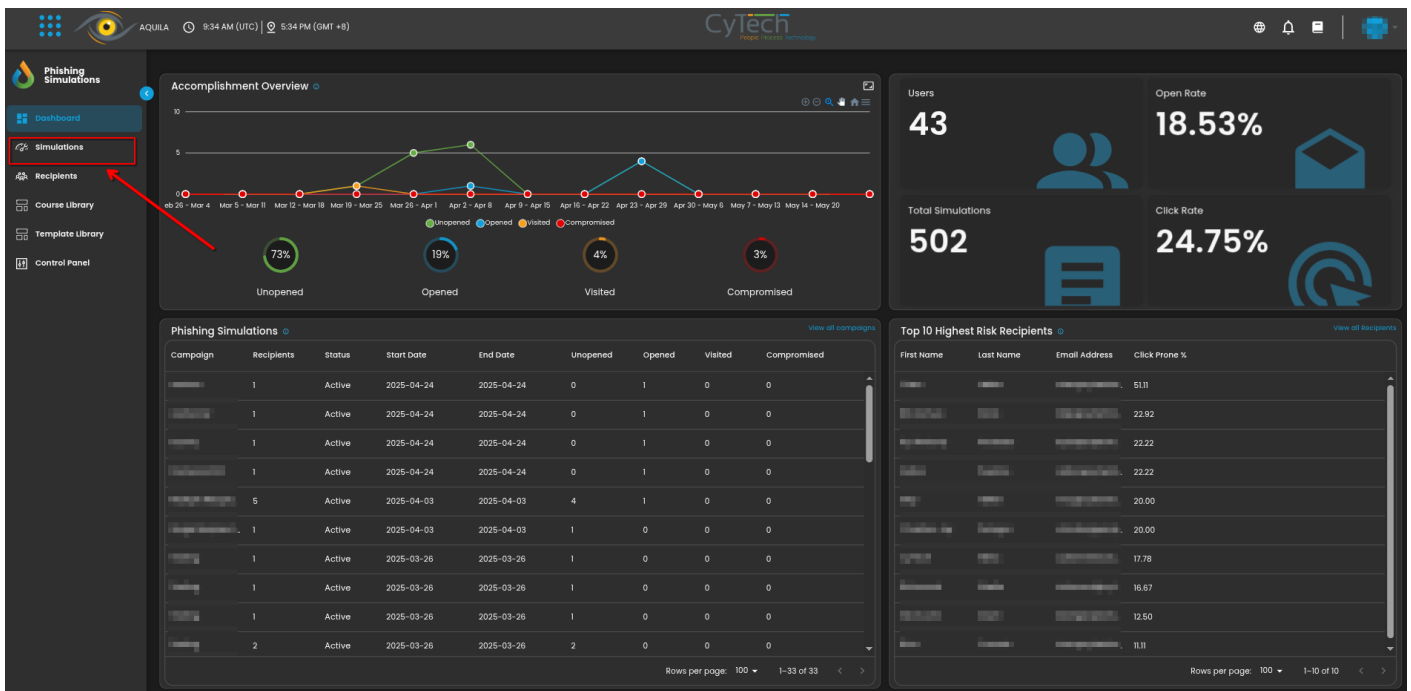
- **Import CSV** - A CSV file can be uploaded to add multiple recipients all at once. The file must follow the required format for ease of transport process. Perfect for a large number of recipients.



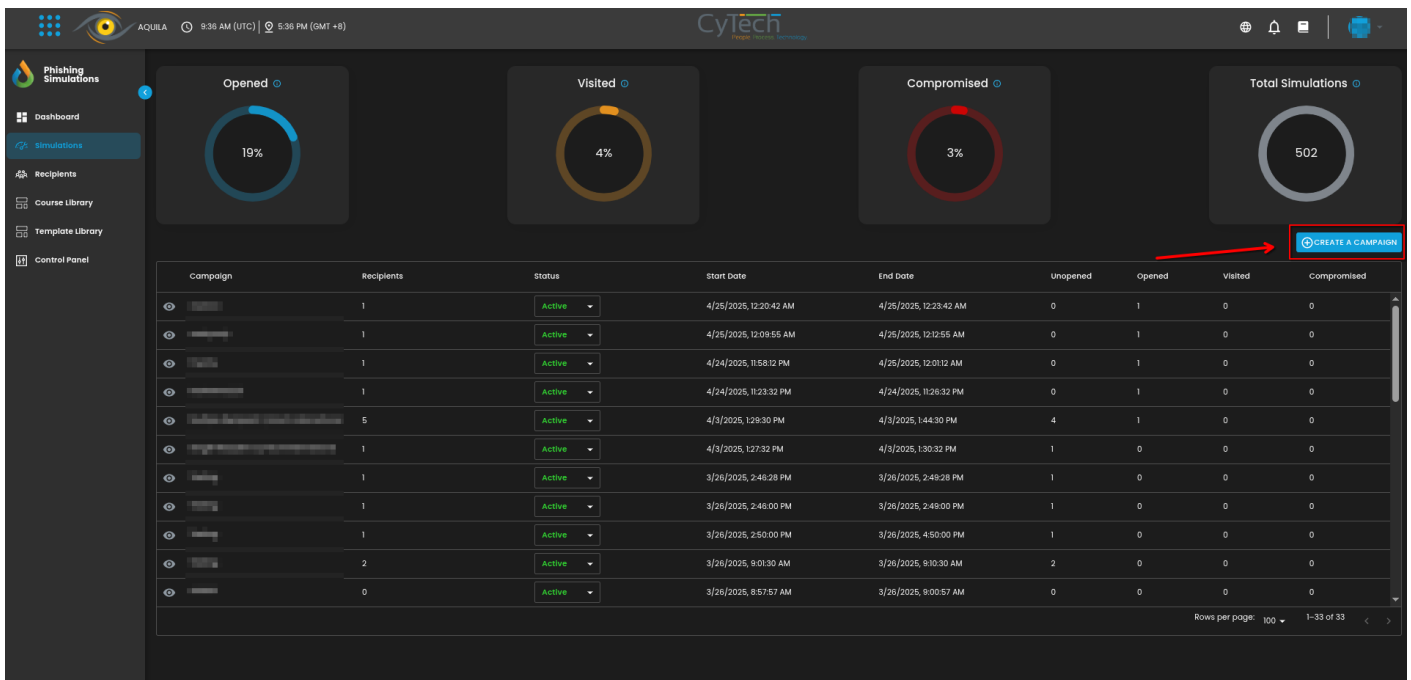
- Once the information is filled out, click submit or finish and a new recipient has been added to the phishing simulation module.

Create a Phishing Campaign:

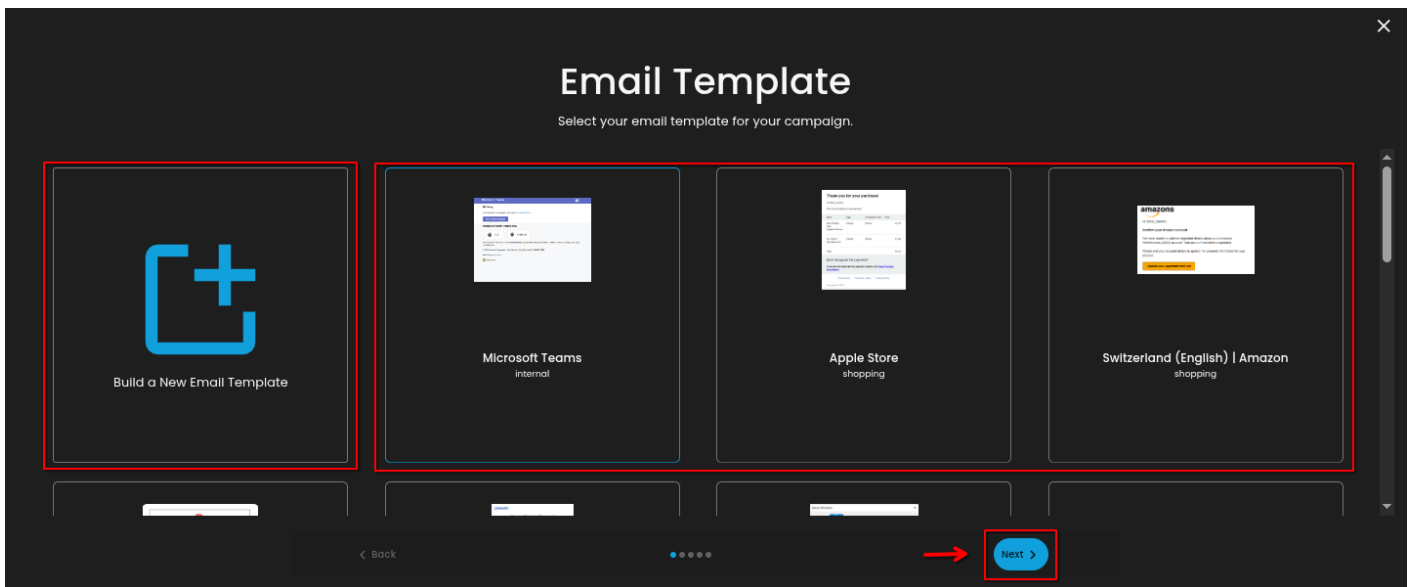
- To start, click on the simulations icon.



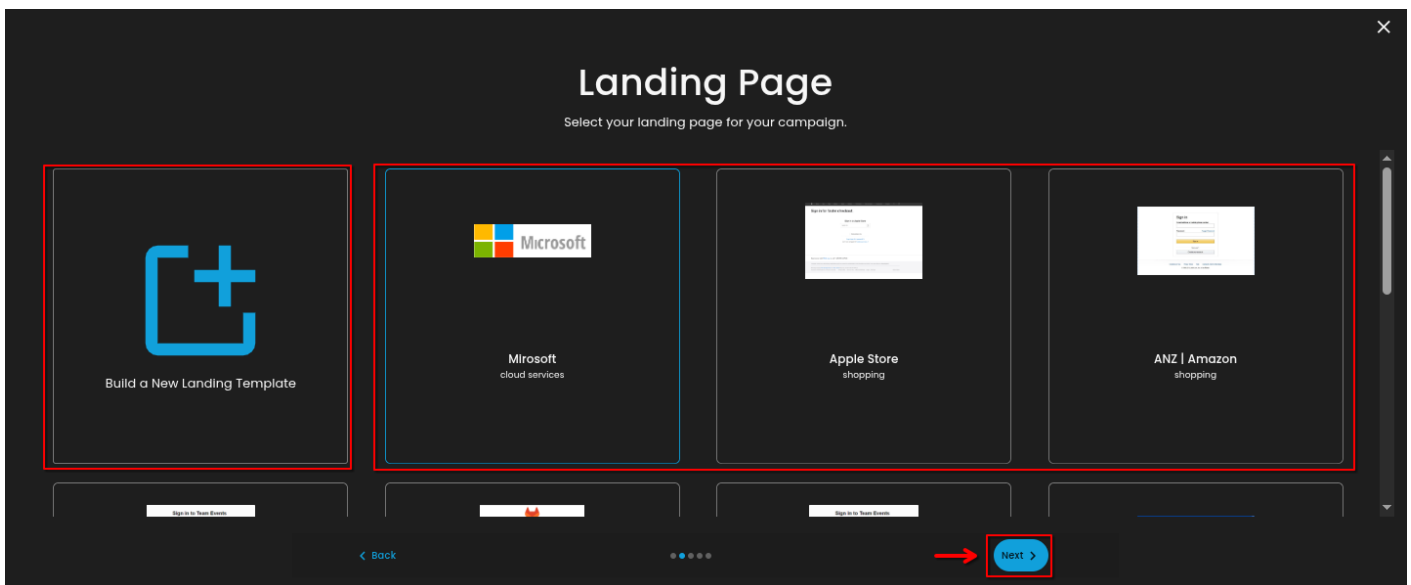
- Then click on create a campaign.



- From here you can choose any email templates to run the phishing simulations, or create a new email template.



- From here you can choose any landing page template, or create a new landing template.



- Then fill in the information needed to be placed on the phishing simulation campaign. These information are used as the phishing simulation's sender details.

Build

You're almost there! Input the details for your campaign.

Sender Details

1. Simulation Name
2. Subject
3. Sender Name
4. Sender Email Name
5. Email Domain
6. Landing Page Domain

Email Preview

< Back
.....
Next >

- Then choose the recipients you want to partake in the phishing campaign and check there status whether they'll open, click, or ignore the phishing email.

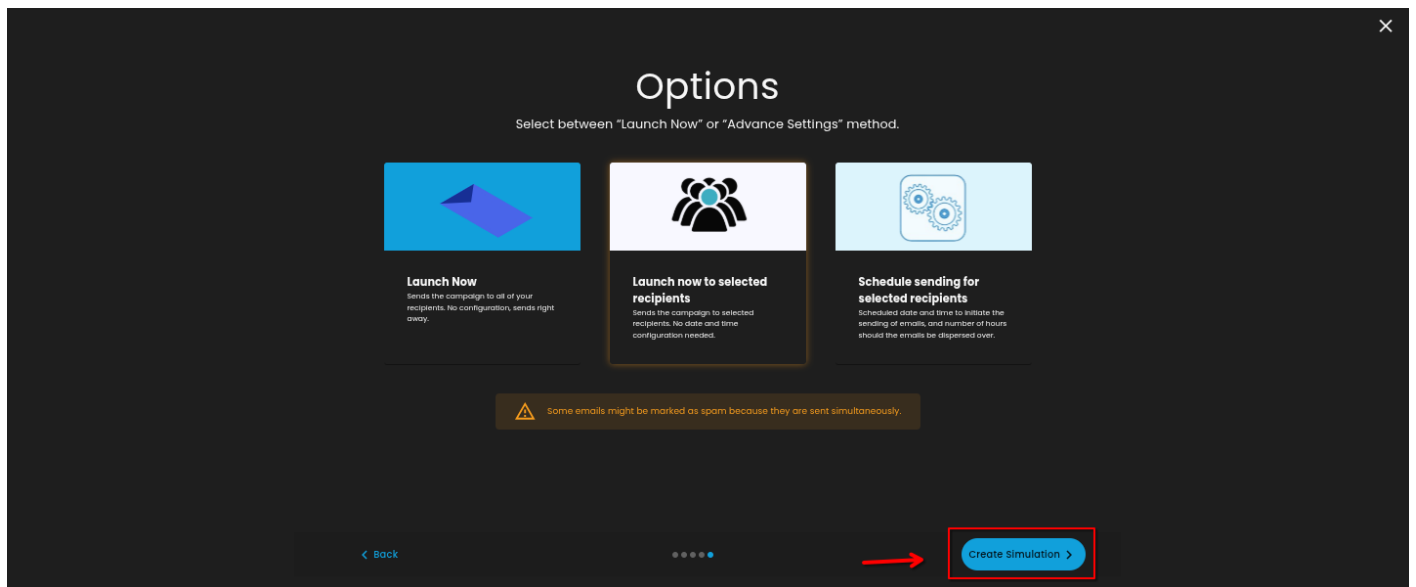
Select Recipients

Set your recipient list.

<input type="checkbox"/>	ID	First Name	Last Name	Status	Department	Email
<input checked="" type="checkbox"/>	6340	[Redacted]	[Redacted]	Active	[Redacted]	Professional Services Department
<input type="checkbox"/>	6225	[Redacted]	[Redacted]	Active	[Redacted]	Technical Support
<input type="checkbox"/>	6210	[Redacted]	[Redacted]	Active	[Redacted]	Professional Services Department
<input type="checkbox"/>	6209	[Redacted]	[Redacted]	Active	[Redacted]	Professional Services Department
<input type="checkbox"/>	6208	[Redacted]	[Redacted]	Active	[Redacted]	Professional Services Department
<input type="checkbox"/>	6207	[Redacted]	[Redacted]	Active	[Redacted]	Professional Services Department
<input type="checkbox"/>	6096	[Redacted]	[Redacted]	Active	[Redacted]	Professional Services Department

< Back
.....
Next >

- Then you click on any of the options to launch the phishing simulation campaign to the target recipients.
 - **Launch Now** – Sends the campaign immediately to **all recipients** under the module (not just the selected ones).
 - **Launch Now to Selected Recipients** – Sends immediately to **only** the recipients you've selected.
 - **Schedule Sending for Selected Recipients** – Allows you to schedule the date and time for sending, and specify how many hours the emails should be spread over.



If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #9

Created 19 April 2024 05:16:47

Updated 21 May 2025 11:32:35 by Richmond Abella