Introduction

Data anonymization is a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets so that the people whom the data describe remain anonymous. This is required by law in different countries. Before we explain the Anonymisation of data, we want to answer a few questions regarding data security & privacy:

- **Where is LUCY storing and processing data?** Lucy can be installed On-Site or on a cloud server. All data is stored within LUCY, no matter where it is installed.
- **Where is data sent?** No personalized information that falls under GDPR ever gets transmitted outside of LUCY. As you can see in this chapter, LUCY uses some connections to centralized servers (e.g. update server). This is only for maintenance reasons and to maintain the functionality.
- **Do we have a data processing agreement**: We do. Please visit this chapter
- **Protecting personal data**: Lucy encrypts the data and offers many possibilities to secure access to the data.
- **Collecting personal data**: In certain countries, you are not allowed to collect personalized data (e.g. who failed a phishing simulation and who did not pass a training). In such a case you need to enable anonymous mode in LUCY. This will be described in the next chapter.

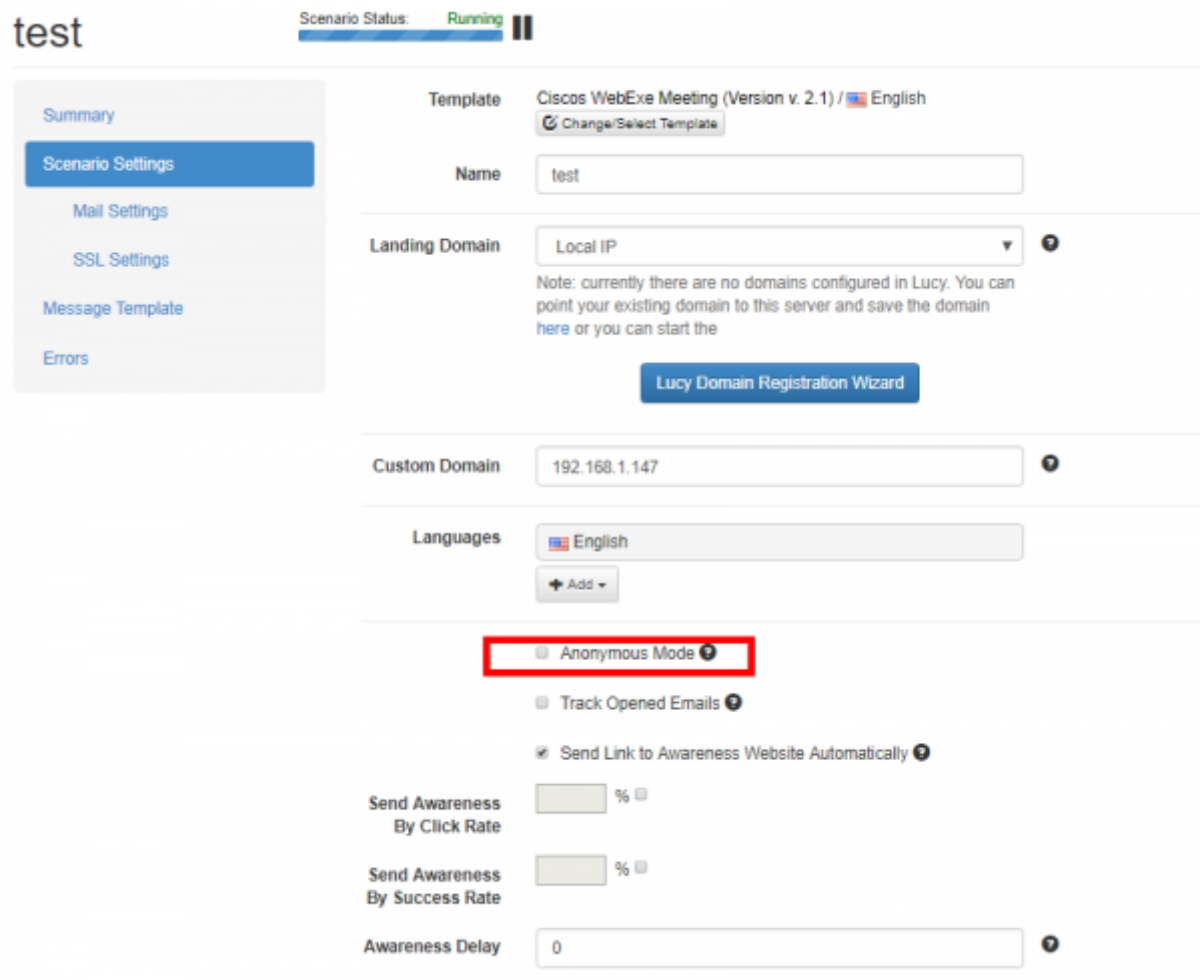
What type of data get logged in LUCY?

The following (not complete) list of information can be collected within a phishing or awareness campaign:

1. **Emails Opened**: Recipients opened the email
2. **Link Clicks**: Recipients clicked the link in the email
3. **Successful Attacks**: Recipients submitted data in a form (e.g. login data that is submitted via a form based POST request), clicked on a link, executed a file etc.
4. **Hourly Stats**: Page views, link clicks, successful attacks, invalid submits, etc.
5. **Daily Stats**: Page views, link clicks, successful attacks, invalid submits, etc.
6. **Recipient Criteria's**: Based on the usage of additional fields in the recipients list you can sort and filter the statistics for each field
7. **Operating System** Of recipient. This information is based on the user agent string
8. **Browser type** of the recipient
9. **Browser Plugins** of the recipient
10. **File downloads**
11. **IP**: Remote IP address of your recipient.
12. **Vulnerable Browser | Vulnerable Client**: Based on the user agent, LUCY will tell you if there is any vulnerability.
13. **Time based stats**: How long does the user stay on each landing page
14. **User history**: Historical user statistics
15. **Awareness stats**: Number of users trained, % correct questions, training results, users who did not start/finish training etc.

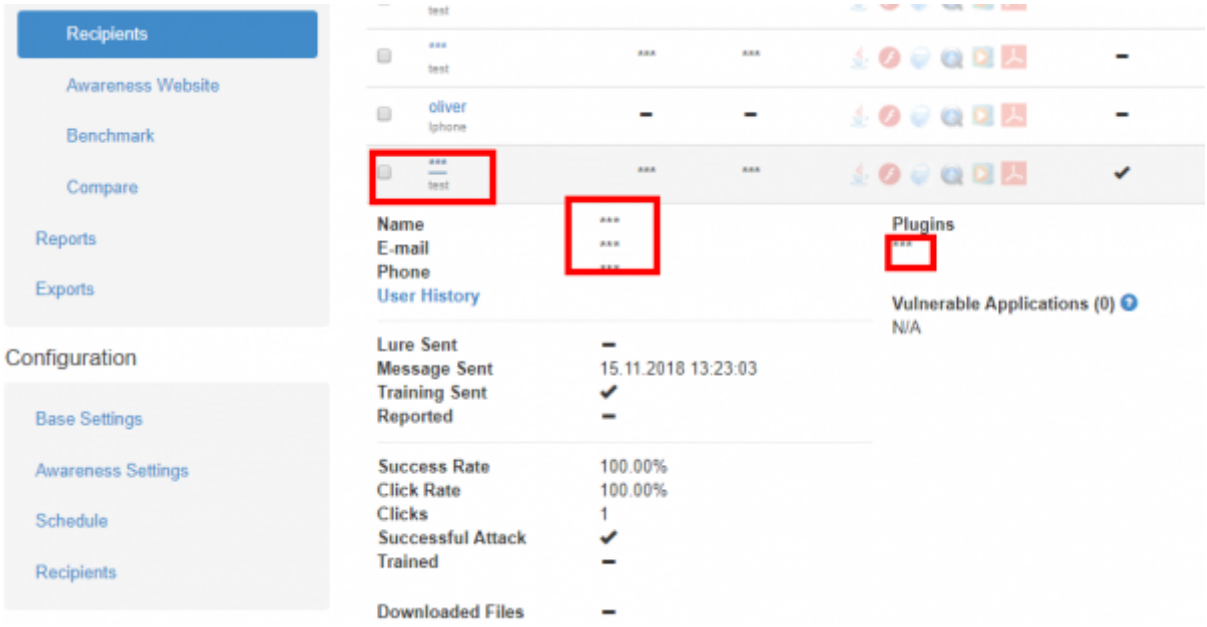
Anonymisation of personal data within a campaign

Within a campaign you can enable anonymous mode in the matching scenario settings:

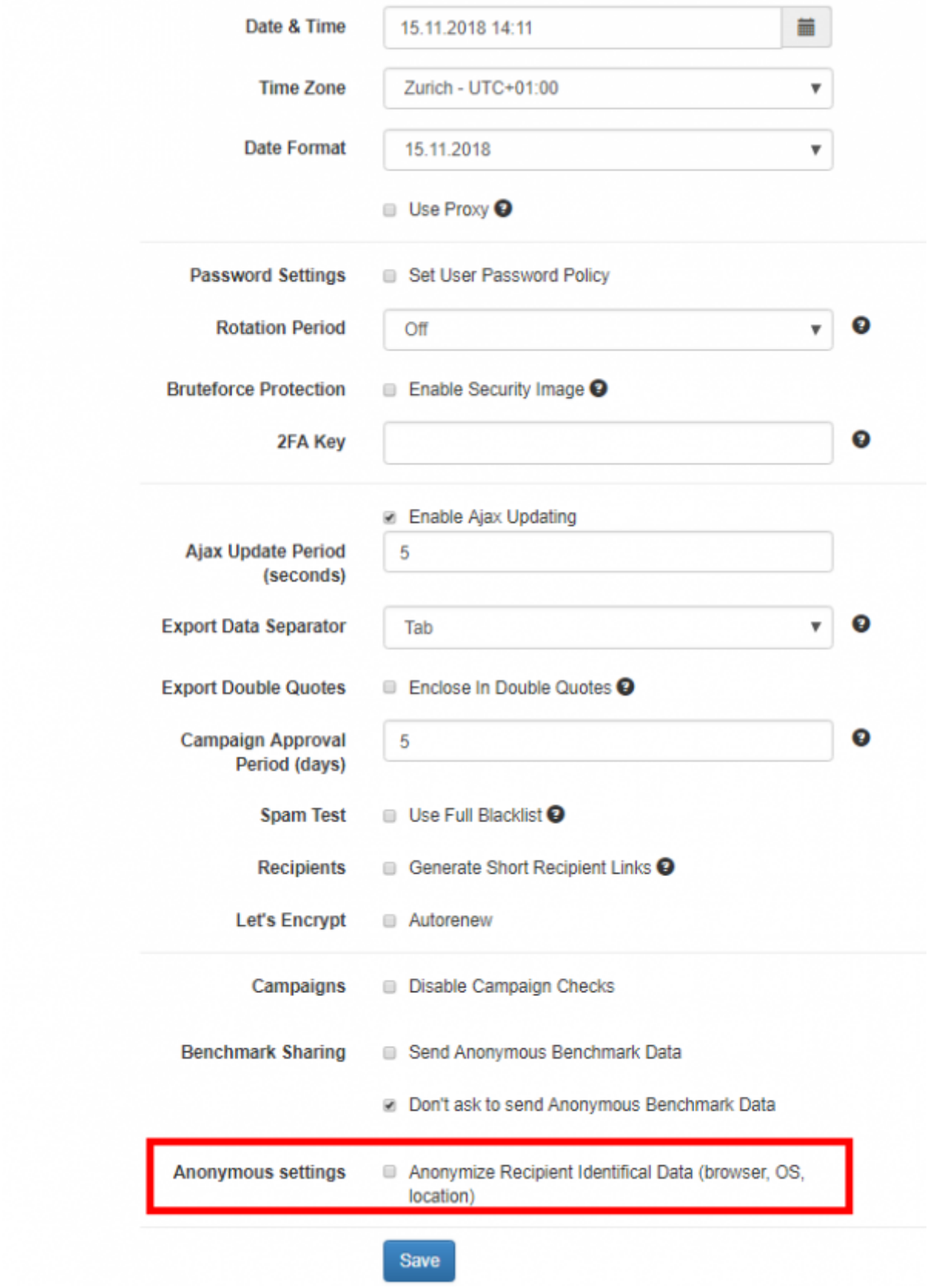


Please note that this operation cannot be undone!

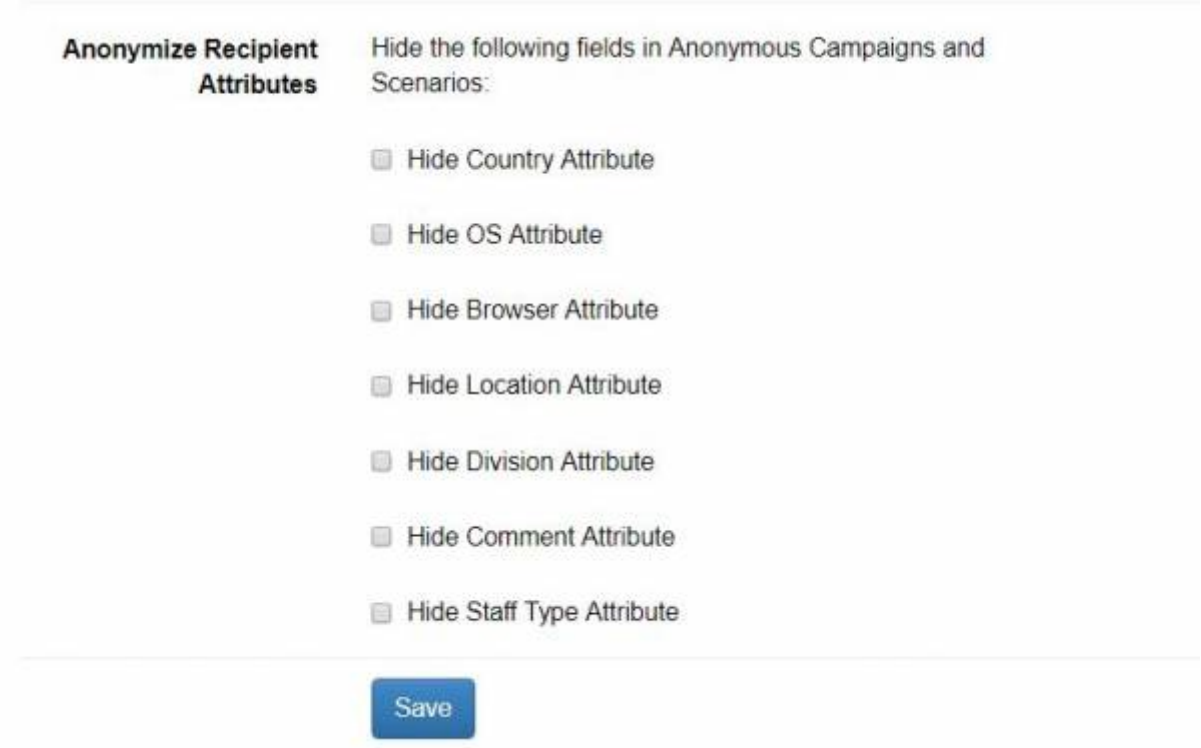
The personal information is then no longer visible:



If you also want to anonymize additional statistical data (browser, IP, etc.), you can set this in the advanced settings:



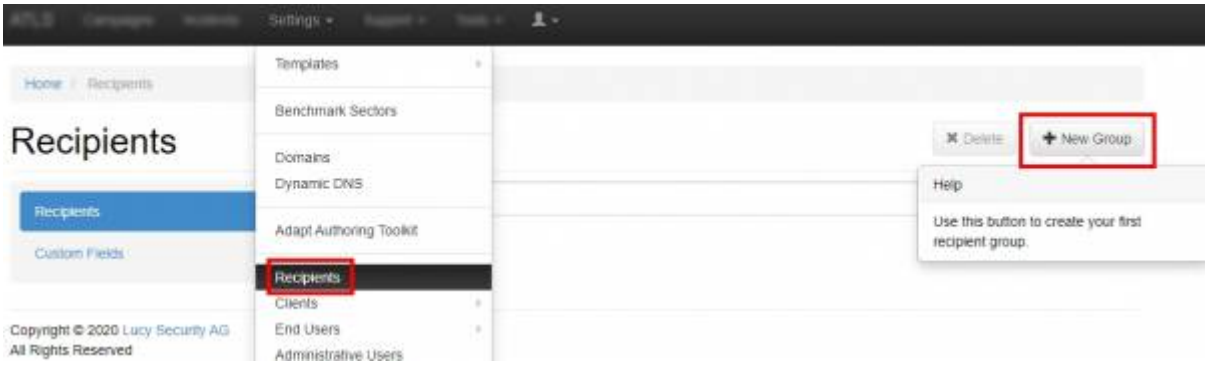
Additional anonymization options are possible in LUCY (under /settings/advanced settings):



Every campaign needs a recipient group to work. The recipient group are the users who receive the attack simulation or awareness content. You can create multiple groups for a single campaign. Groups can be used within LUCY to target users with specific phishing or training campaigns. Many organizations start by grouping users by department, location (if you have multiple office locations), or even domains (if there are multiple domains). The recipients can be in any number of groups and you can set up an unlimited number of groups.

How to Enter Your Recipients?

Recipients and groups can be configured under Admin/Recipients.



You can either add them manually (1), import them (2) or search the internet by using the "SCAN FEATURE" (3). The groups are always defined globally and you can re-use them among different campaigns.

We recommend importing them because it will enable you to create a custom text file with additional information about each target user (e.g. defining the division or location where they work). This information can later be used for automatic analysis and statistics. The more information you provide, the better.

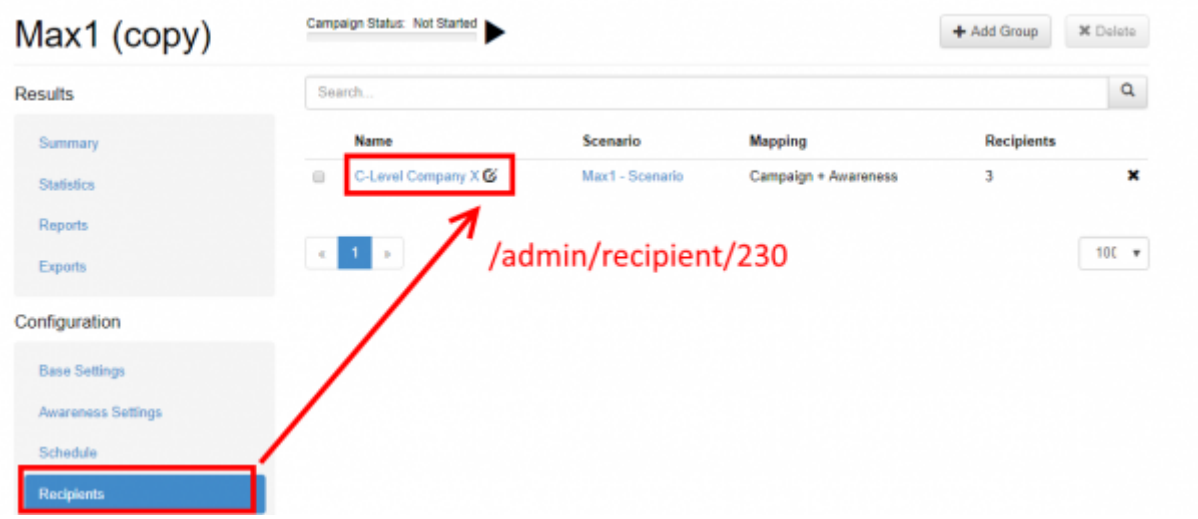
Note: Searching the internet without a Bing or Google API won't get you the same results as if you searched directly with a search engine.

Process of anonymization

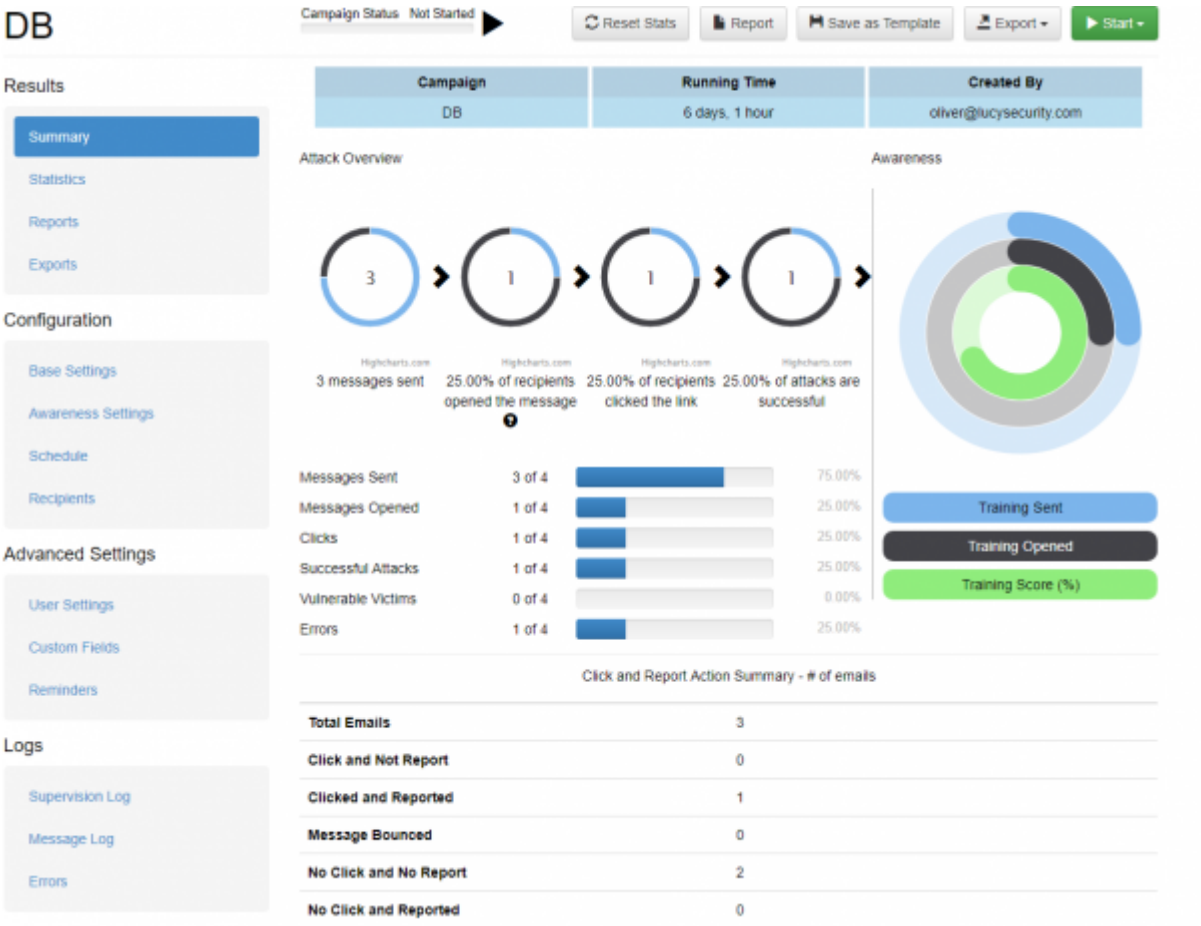
The recipients for the campaign can be imported via file or via LDAP. The recipients can contain the following attributes:

- 1.Email - Recipient's e-mail address
- 2.Name - Recipient's name
- 3.Staff - Job position or related
- 4.Location - Recipient's location
- 5.Division - Company division
- 6.Comment - Any custom comment
- 7.Link - Unique link part for the Landing Page.
- 8.Phone - recipient phone number
- 9.Language - recipient language

Once you imported the recipients, you have to associate the recipients with a specific campaign(attack simulation or awareness training):

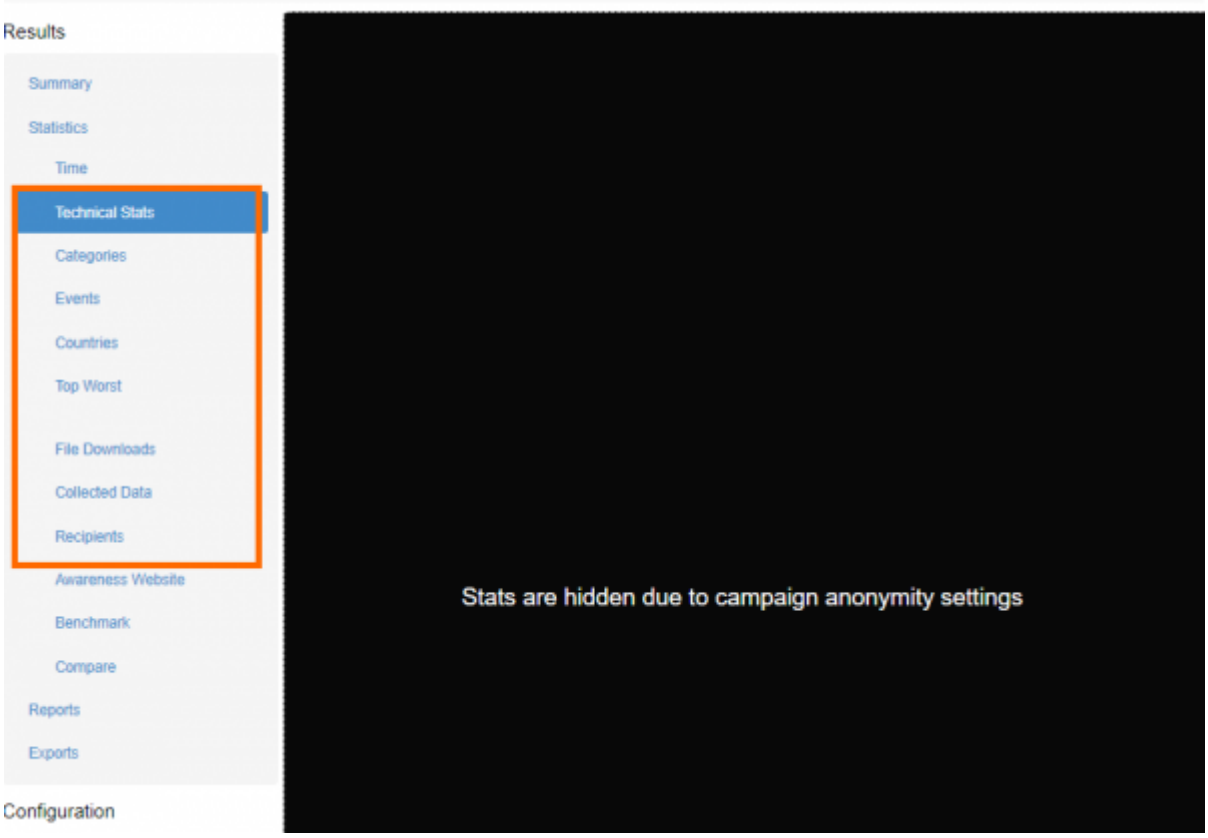


After you start a campaign in anonymous mode you will only be able to see general statistics:




Home / Campaigns / DB / Statistics
4 new templates available!
Download
DB
Campaign Status Not Started
Generated: 24.06.2019 12:27:39
Summary Chart
Add Chart
Results
Summary
Statistics
Time
Technical Stats
Categories
Events
Countries
Top Worst
File Downloads
Collected Data
Recipients
Awareness Website
Benchmark
Compare
Reports
Exports
Configuration
Base Settings
Awareness Settings
Schedule
Recipients
Advanced Settings
User Settings
Custom Fields
Reminders
Logs
Supervision Log
Message Log
Errors
3
1
1
1
1
75.00 % messages sent
25.00% of recipients reported the message
25.00% of recipients opened the message
25.00% of recipients clicked the link
25.00% of attacks are successful
Scenario Stats
Show All
Values
https://www.deutsche-finanzagentur.de/ - Scenario
Messages Sent
Clicks
Success
Total Stat
Sent
Opened
Clicks
Successful Attacks
Reported
Invalid Submits
Vulnerable Victims
Replied
Bounced
Out of Office
Average Time Per Scenarios
19.006666666667
https://www.deutsche-finanzagentur.de/ - Scenario
Average Time Per Page In https://www.deutsche-finanzagentur.de/ - Scenario Scenario
19.497
18.7615
index.html
account.html

If you have less than 10 employees in a division, location etc, the marked stats will also not be visible:



From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=anonymisation&rev=1561408324

Last update: **2019/07/25 12:52**