

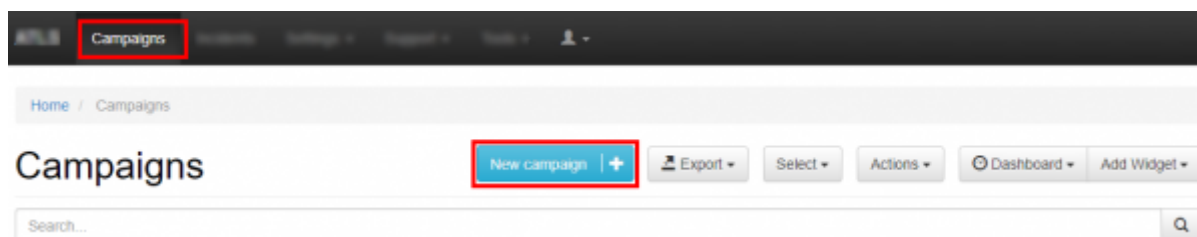
# PREPARATION

Before creating your first campaign you need to go through a few questions:

- Is the [organizational part](#) taken care of?
- Are you using [latest LUCY version and updated all templates](#)? Did you make sure to reboot after the update?
- If you send emails via LUCY: did you [set a hostname](#) for LUCY's mail server?
- Did you already reserve a [domain](#) that points to LUCY?
- Are the [necessary ports](#) open from and to LUCY?
- Is LUCY able to send mails correctly? This can be tested under [support/test mail](#).
- Do you have the correct [time/time zone](#) set in advanced settings?
- Does your hardware meet the [Requirements](#)?
- Did you whitelist LUCY's domain/IP and did you make sure that [mails don't end up in SPAM](#)?
- Does your [License](#) meet the requirements for your campaign?

## STEP 1 - Create a New Campaign

After the login, you can create your first phishing campaign by pressing the button "New Campaign". This will start Campaign Wizard.



## STEP 2 - Select Type of a Campaign

A wizard menu appears which lets you choose the type of your campaign. There are several types:

1. [Attack Simulation](#)
2. [Educate Employees](#)
3. [Infrastructure Tests](#)
4. [Engage Employees](#)

**Campaign Wizard: Type** ✕ Close

1. Type



2. Campaign

3. Recipients

4. Review

5. Finish

Please choose a campaign type you would like to use.

Type	Description
 <b>Attack Simulation</b>	With an attack simulation (phishing, malware, smishing, USB attacks, etc.) you can test whether your employees are really familiar with the dangers of the Internet. LUCY provides a "safe learning environment" where employees can experience what real attacks would feel like.
 <b>Educate Employees</b>	Close knowledge gaps with Lucy's E-Learning. LUCY offers more than 200 interactive, web-based training modules (videos, tests, quizzes, games, etc.) on various security topics that can be provided to employees based on the results of the attack simulations or independently of them.

Skip the wizard and enable expert setup Next >

The next menu lets you choose a type of attack. There are also several types:

1. [Data Entry Attack](#)
2. [Hyperlink Attack](#)
3. [File Attack](#)
4. [Portable Media Attack](#)
5. [Smishing](#)

**Campaign Wizard: Attack Simulation** ✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Training Template


5. Training Settings

6. Recipients


7. Review

8. Finish


Please choose an attack simulation type you would like to use.

**Data Entry Attack**


Data entry attack can include one or more web pages that intercept the input of sensitive information. The available web pages can be easily customized with a LUCY web editor. Additional editing tools allow you to quickly set up functions such as log-in forms, download areas, etc. without HTML knowledge.

**Hyperlink Attack**

A hyperlink-based attack will send users an e-mail that contains a randomized tracking URL to identify the user who clicked the link. There is no landing page involved in this campaign type. But you can redirect the user to any webpage after he clicked the link.

**File Attack**

File-based attacks allow the LUCY administrator to integrate different file types (office documents with macros, PDFs, executables, MP3s, etc.) into mail attachments or websites generated on LUCY and to measure their download or execution rate.

**Portable Media Attack**

LUCY offers the option to perform portable media attacks where a file template (e.g., executable, archive, office document with macros, etc.) can be stored on a portable media device such as USB, SD card, or CD. The activation (execution) of these individual files can be tracked in LUCY.

Skip the wizard and enable expert setup < Back Next >

## STEP 3 - Basic Campaign Settings

Type in name of your first campaign (e.g.: "My Test Campaign") and [choose a client](#).

**Campaign Wizard: Campaign** ✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. Recipients

7. Review

8. Finish

Here you configure basic campaign settings - its name and the client it is attached to.

**Name**

My Test Campaign

**Client**

Please select...

Please select...

Lucy

[↓ Advanced Settings](#)

← BackNext →

## STEP 4 - Choose Attack Template

At this step, you'll see the list of templates that your LUCY instance has available. You can preview each template before selecting it by hitting on the "Preview" button. When you have selected your template, choose its language, hover over the "Next" button and press it. List of templates and the preview ability could vary according to the type of chosen scenario.

**Campaign Wizard: Attack Template** ✕ Close

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings


6. Recipients

7. Review

8. Finish


this campaign, you may add extra scenarios after finishing the wizard.

☐ Only display recommended templates according to your industry type and size




**Access to online surveillance portal**  
The user is asked to use a portal with their windows credentials to occasionally access the companies online surveillance system and report unusual observations.

Preview ▾Select Language ▾



**Adobe Document Reader DC security update**  
Adobe asks the user to download the latest version of Adoba Acrobat Reader DC, for security reasons.

Preview ▾German ▾



**Affordable car leasing for employees**  
Employees can lease a company car for a fraction of the original cost

EnglishGerman

← BackNext →

LUCY - <https://wiki.lucysecurity.com/>

## STEP 5 - Configure Basic Attack Settings

**Domain** - Domain name for your scenario. It is possible to set an IP address as well. LUCY detects its local and external addresses. The addresses are available in the drop-down list. However, you can set an IP address manually. A [domain](#) name can be set as well if you have it.

**Sender Name** - Define a name that will be seen by recipients of the campaign in the field "Mail From". More can be found [here](#)

**Sender Email** - Insert an email address that will be set by Lucy as the email address of a sender. More in [the same article](#).

**Subject** - Insert text for the subject of your phishing email. Now, select "Next".

Campaign Wizard: Attack Settings Close

1. Type  
2. Attack Simulation  
3. Campaign  
4. Attack Template  
5. Attack Settings  
6. Recipients  
7. Review  
8. Finish

Configure basic attack settings.

Domain: Local IP

Attack Template: 192.168.1.104

SSL: ☐ Use Custom SSL Certificate ⓘ

Mail Configuration

Sender Name: Lucy Wiki Writer

Sender Email: writer@lucy.com

Subject: The mailbox above does not exist.

[Advanced Settings](#)

Back Next

## STEP 6 - Add Recipients

There are 2 options:

**Select Existing Group** of recipients.

More in [this](#) article.

The screenshot shows the 'Campaign Wizard: Recipients' window. On the left is a vertical list of steps: 1. Type, 2. Attack Simulation, 3. Campaign, 4. Attack Template, 5. Attack Settings, 6. Recipients (highlighted), 7. Review, and 8. Finish. The main area has the heading 'It's time to add recipients or choose an existing recipient group.' Under 'Mode', the 'Select Existing Group' radio button is selected. Below it, the 'Group' dropdown menu is open, showing options: 'Please select...', 'Please select...', 'Test Recipient Group', and 'Recipients Group For That Wiki Article' (which is highlighted in blue). At the bottom right are 'Back' and 'Next' buttons.

**Enter Manually** each recipient. Each time you press the "Add" button, a new field appears allowing you to enter an email address of a recipient for this campaign and a name of the recipient. The name is required for some templates to insert a name variable in the text of a phishing email. This makes attacks more "personal".

The screenshot shows the 'Campaign Wizard: Recipients' window with the 'Enter Manually' mode selected. Under 'Recipients', there is an '+ Add' button and a table of three entries. Each entry has an email address field, a name field, and a delete 'X' button.

Email Address	Name	Delete
onebottle@onthe.shelf	Alber's bottle	X
twobottles@onthe.shelf	Brian's bottle	X
nobottles@onthe.shelf	Sam	X

At the bottom right are 'Back' and 'Next' buttons.

As soon as you are done with this step, use the "Next" button.

## STEP 7 - Review

Review the information that you've entered. If everything is correct, press the "Next". If you see a

typo or want to modify something, hover over the list of steps and click on any desired. It is possible to switch quickly between the Wizard Steps by a single mouse click.

**Campaign Wizard: Review** ✕ Close

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. Recipients

**7. Review**

8. Finish

Please review your configuration settings. In case you would like to change something please use the menu on the left or press Back button.

Type

Attack Simulation

Attack Simulation

Data Entry Attack

Campaign

Name	My Test Campaign
Client	Lucy
Benchmark Sector	N/A

◀ Back Next ▶

## STEP 8 - Finish

*I'll just duplicate the words from the wizard:*

You're all set!

Hit Start if you would like to start the campaign right away. You will be able to start the campaign any time later from the campaign summary page.

Campaign Wizard: Finish

1. Type

2. Attack Simulation

3. Campaign

4. Attack Template

5. Attack Settings

6. Recipients

7. Review

8. Finish

You're all set!

Hit Start if you would like to start the campaign right away.

You will be able to start the campaign any time later from the campaign summary page.

Go to Campaign

Start

From:  
<https://wiki.lucysecurity.com/> - LUCY

Permanent link:  
[https://wiki.lucysecurity.com/doku.php?id=create\\_your\\_first\\_phishing\\_campaign](https://wiki.lucysecurity.com/doku.php?id=create_your_first_phishing_campaign)

Last update: 2020/08/20 10:48

