# PREPARATION

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

- Is the organizational part taken care of?
- Do you use the latest LUCY version and updated all templates? Did you make sure to reboot after the update?
- Did you make sure that you have LUCY's IP or domain whitelisted at your receiving mail server?
- If you send the mails via LUCY: did you set a hostname for LUCY's mailserver?
- 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**".
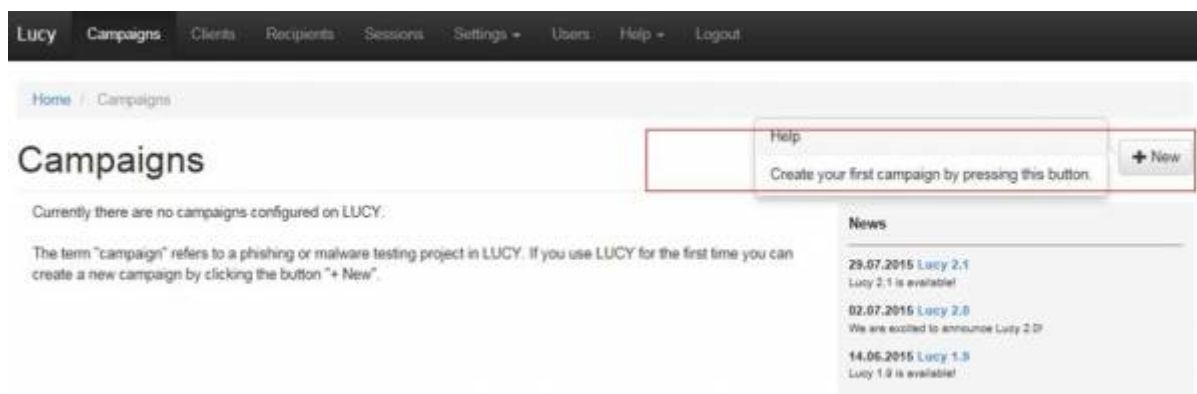
STEP 2 - Select or Create a Client

Create a client or choose the built in client (a client can be your own organization or the company who asked you to perform a phishing test). This is important because you can also create view only accounts which are associated with those clients.

New clients can be created under "clients". In LUCY v. 2.5 and higher this is created under settings/clients.
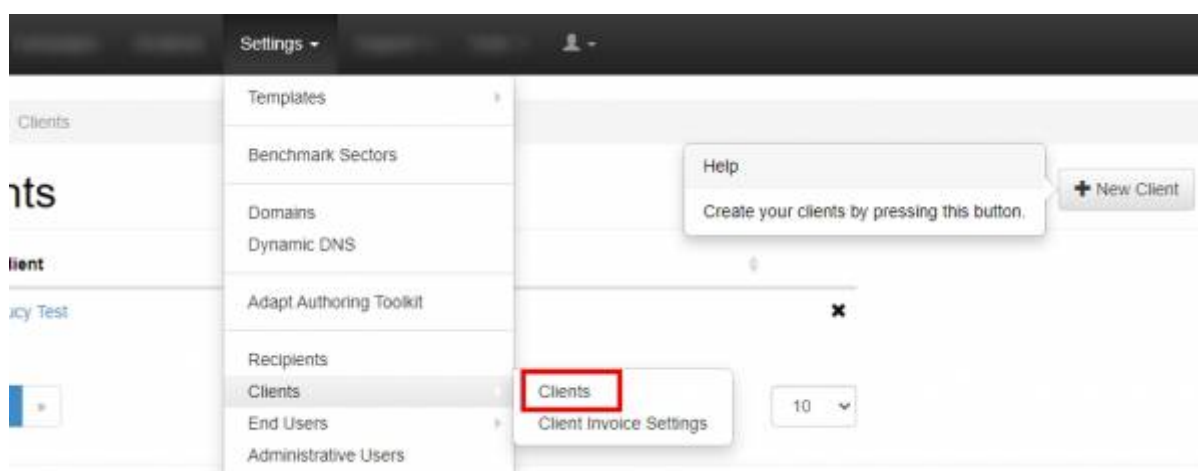
STEP 3 - Choose Your Configuration Mode

You have different setup options like the **Expert Setup**, the **Setup Wizard** or a **Start with predefined campaign Template** (called sample campaign in LUCY < 3.0). We recommend using the Setup Wizard when used for the first time. Another optional is to set a Benchmark for a campaign.

Sometimes a remote Firewall, Spam filter or Virus Filter might automatically scan all the URL's within a link. As a result you end up with false positives and LUCY will show all link clicked (success). To avoid such automatic link requests by some 3rd party application you can enable the antivirus/firewall protection and LUCY will ignore all GET requests for the first 30 or 60 seconds:


To make sure that the campaign runs as expected you may also enable the email tracking functionality.

STEP 4 - Select one or multiple Phishing Scenario(s)

Now you need to select one or multiple phishing scenarios. Please check out what different scenario types are available. Make sure you have downloaded all the latest scenarios first. If you allocate multiple scenarios in a campaign, you can still activate or deactivate them at a later point.

Please note: If you edit a scenario template within a campaign, the changes in the template will only apply to the campaign. If you change a scenario template in the generic settings, then the changes in the template are permanent.
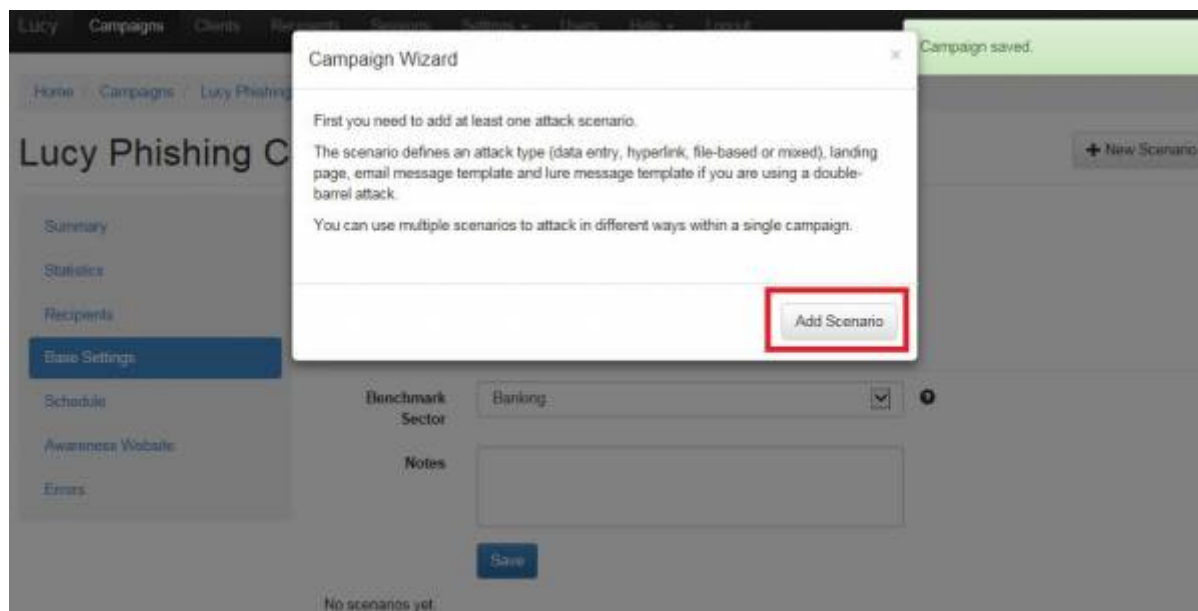

You are able to preview every template before selecting it. In the **Preview Mode** you can test the site using all the features (just enter some random login to get to the next page).
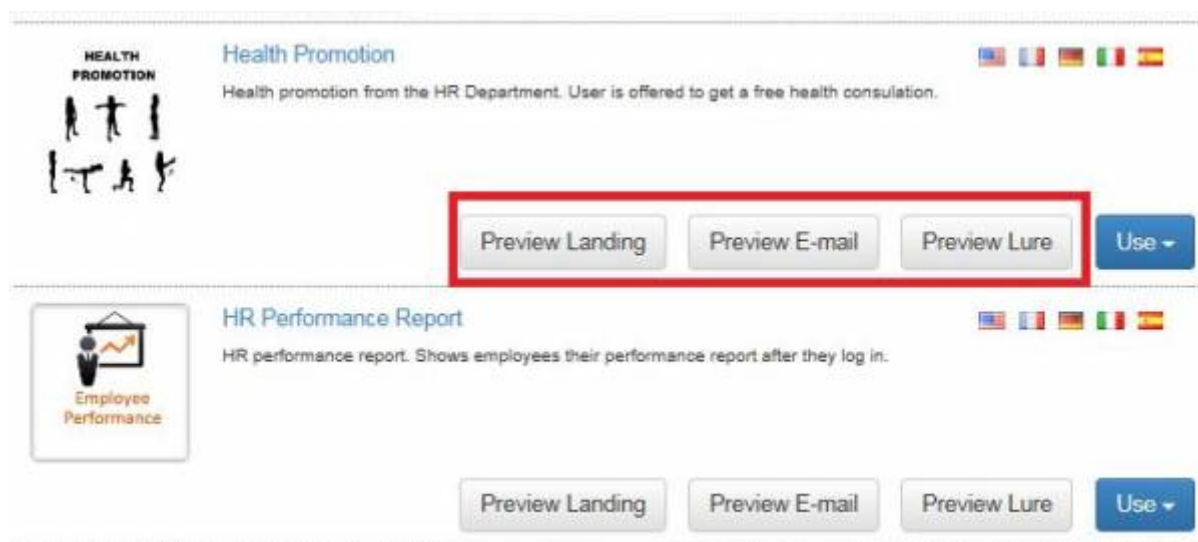
Note: **You can allocate multiple scenarios within one campaign** and they can all be started simultaneously! Example: A company might want to split the employees into 2 or 3 groups. One group could get a phishing mail with a landing page that contains many obvious errors and should be easily detectable while the other scenario is almost perfect. This way the client can identify the variables that drive the awareness in one single campaign.

STEP 5: For this tutorial, as an example, we select the "Encrypted Email Scenario", where the user will be asked to login with their Windows username and password to access an encrypted email message.
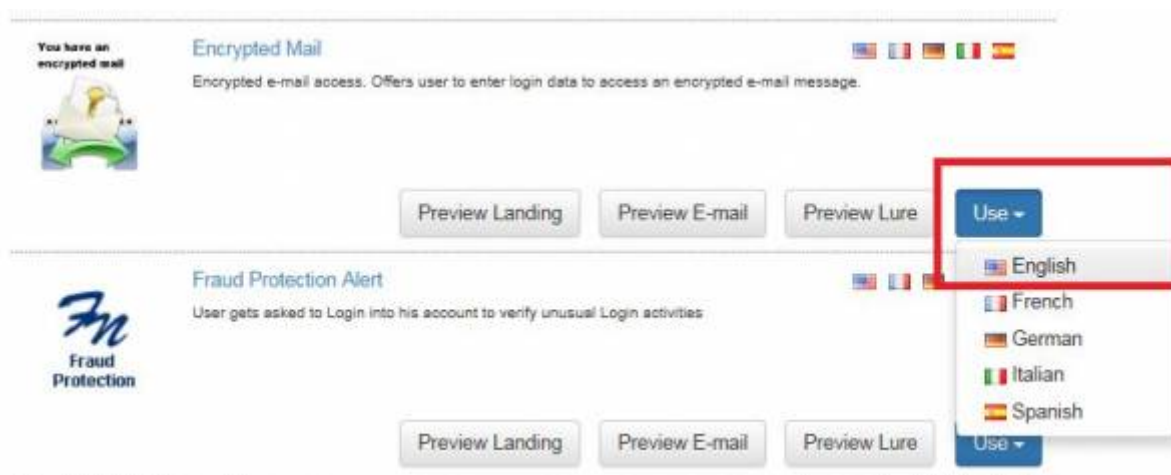
STEP 6 - Configure the Base Settings of Your Campaign

Once you have selected the scenario, you need to configure the **Base Settings** of the campaign. First give your campaign a name and then choose how your recipients will be able to access LUCY by defining the Domain. Finding the appropriate domain name is a very important step for the success and it depends very much on your campaign scenario. If you plan to create a fake web mail login you might try to reserve a domain like "webmail-server365.com" and point it to LUCY.

Note: Each scenario has its own Base Settings.

There a few **Optional Settings** that you can apply within the Base Settings. Lucy comes with certain Default Settings. You can change these setting as you like. The settings are:

- **Setup Wizard**: You can always Unselect the Setup Wizard and continue with the Expert Mode.
- **Use SSL**: If you decide to use SSL for the campaign (either generate a custom certificate or import a trusted certificate) you can do this via the SSL Wizard.
- **Anonymous Mode**: Use this mode to hide all "Victim" data (IP address, login details, etc.) from statistics and reports.
- **Success Action**: Defines what LUCY considers as an successful attack. There are four options.
- **Track Opened Emails**: Inserts an invisible image into outgoing emails to track if users opened the message. Use this feature carefully as some email servers may put such emails into the Spam Folder. Also some email clients (like Outlook) block the automatic downloading of images in the Preview window.
- **Send Link to Awareness Website Automatically**: Send a link to the Awareness Website after user has been successfully attacked. Please note that the Awareness Website should be published for this feature to work.
- **Advanced Information Gathering** : Check this option to enable information gathering. This helps LUCY collect advanced information about your users. More background info can be found

here.

- **Collect Data**: Choose "Full" if you want to record all entered logins and passwords, "Partial" to record only the first 3 letters (remaining letters will be masked with asterisks) or "No" to skip user data collection.
- **Double Barrel Attack**: When using Double Barrel Attack, the system first sends a "Lure" email containing some teaser text. After that the system waits for a while (you can configure that time in settings below) and sends an actual phishing email. The "Lure" delay defines, in seconds, the time frame between the Lure and the attack emails for a Double-Barrel Attack.
- **Login Regexp**: Another option is to define some login filters to only catch valid logins (you could define the Domain Name in the User Name field or say that the Password has to be at least 8 characters to be accepted from LUCY). Example: This filter here ^(?=.*\d)(?=.*[A-Za-z])[A-Za-z0-9].{8,}$ would only allow logins with minimum 1 alphabetic character, minimum 1 digit & minimum length 8.
- **Redirect URL**: This is used for hyperlink based scenarios or within a landing page to redirect to an awareness page.
- **URL Shorting**: Details here

STEP 7 - Edit your Landing Web Page within Your Campaign

After saving the Base Settings, you can now Edit the Landing Page, Upload Your Own Webpage or simply copy any website on the internet. The Landing Page is the webpage that the users will see when they click on the link in the email they receive. First select the drop-down menu at the top the page where you want to edit. Please note that the same landing page may be available in different languages. So make sure you edit the correct language.
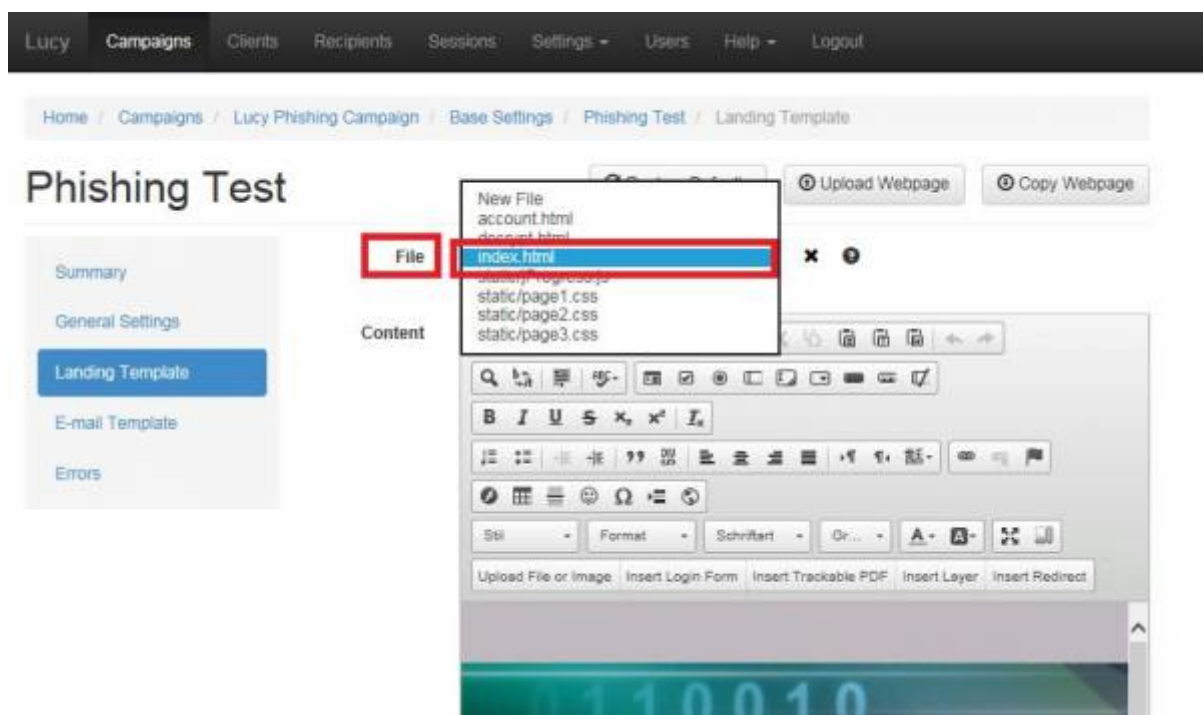

Note: If you edit a Landing Page which is based on a pre-defined scenario template in a campaign, it won't affect the default scenario templates. Only if you go into Settings/Scenario templates and start

editing the templates outside the campaign will all changes be stored permanently to this specific scenario.

Let's assume that you want to replace the logo on the Landing Page: Just double click on the existing logo (1). Select your own image (2), upload it (3) and save the changes by clicking "OK".
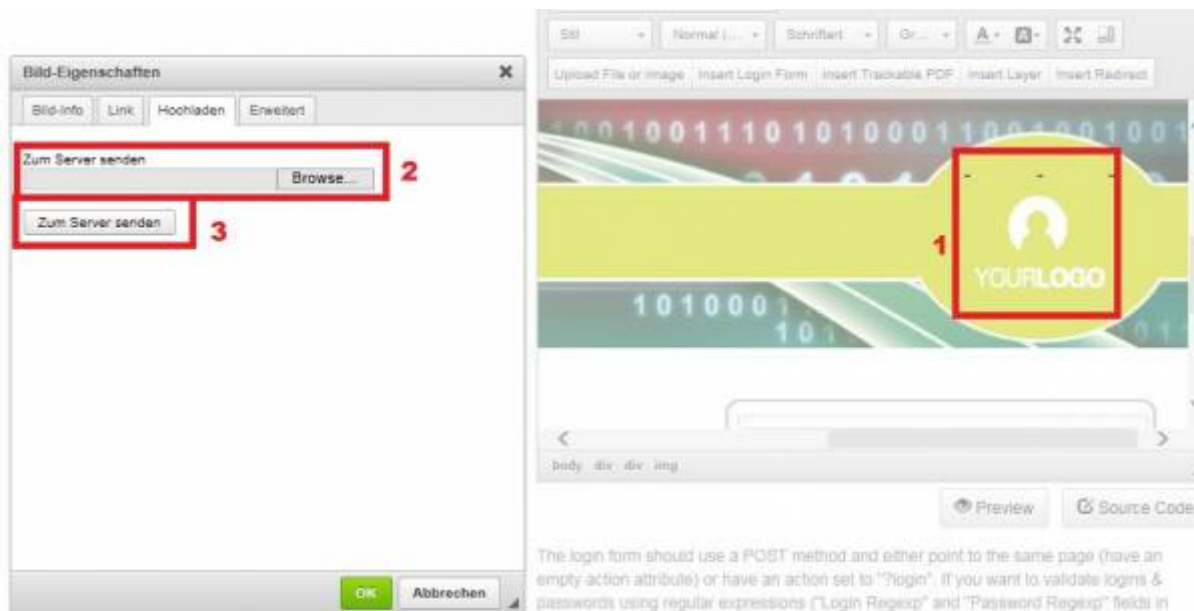
STEP 8 - Configure the Message Template (Email or SMS)

It's time to setup email communication (if you want you can also use SMS as an alternative).

- **Step 8a:** Choose your **sender's name, email address and subject** (**Note**: The most common reason for emails not arriving at your Recipient's Inbox are SPAM filters. When using a known email domain like test@microsoft.com or a non-existing email domain like test@nonexistant.com, your email might get deleted by SPAM filters. Some public email providers are very restrictive and might not even forward emails to your Recipient's SPAM folder. To verify this you can use LUCY's built in SPAM Checker).

- **Step 8b**: Please also **choose the language** for each group. If you configured an English landing page, then select English also within that recipient group. If you have different groups with different languages within your company you can simply create a group and select a language for each recipient. LUCY then will direct each user to an individual landing page that matches that language.

- **Step 8c**: **Insert a link**. The editor allows you to insert a link. You have two options: either insert %link% somewhere in your email body (this will generate a randomized link to identify the user) or select and mark a word in your mail body (1) and then click on the link symbol (2) and then insert the "LUCY link" with %link% in the input field.
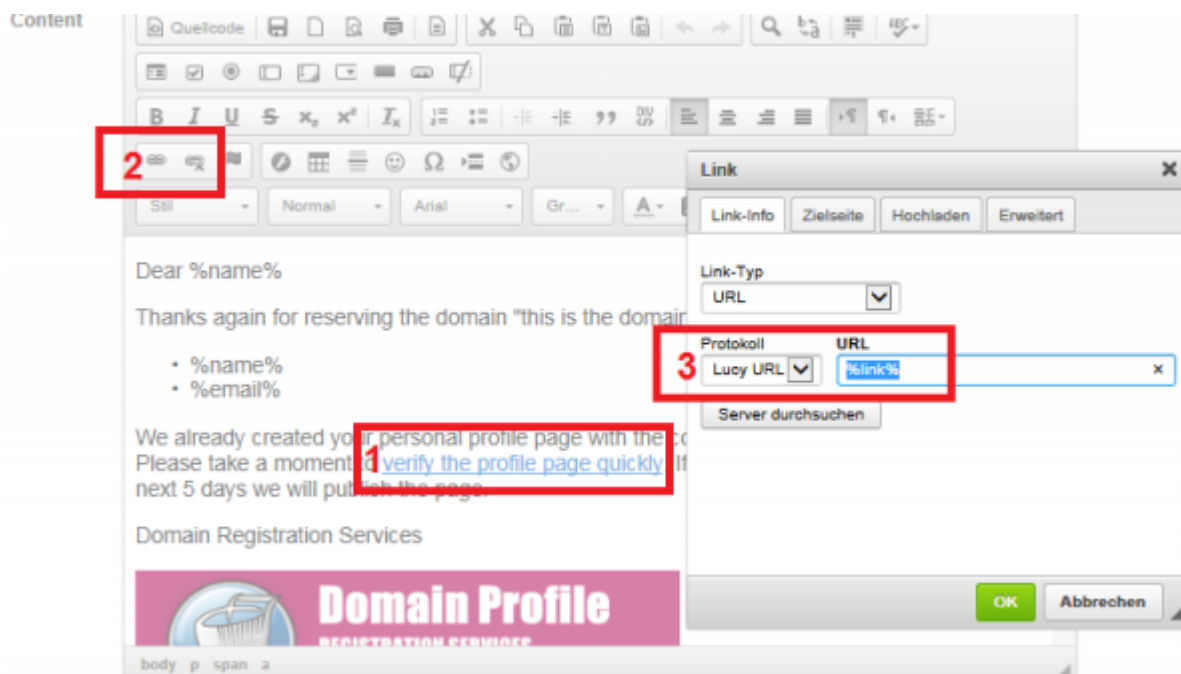

Please make sure the link variable is set in the HTML code, if you hide it behind another Link. If you type a hyperlink instead a word, the editor will automatically detect that, and create the link in the code. But this link will be wrong: If you type http://www.example.com in the editor, LUCY will automatically create a hyperlink to http://www.example.com in the HTML code (1) and underline the URL. But if you want http://www.example.com pointing to your LUCY URL, please remove the link pointing to http://www.example.com in the source code directly, or remove it by clicking on the "unlink" symbol (2), and then select the text "http://www.example.com" and click on the link symbol again and insert %link% in the HTML code (3).
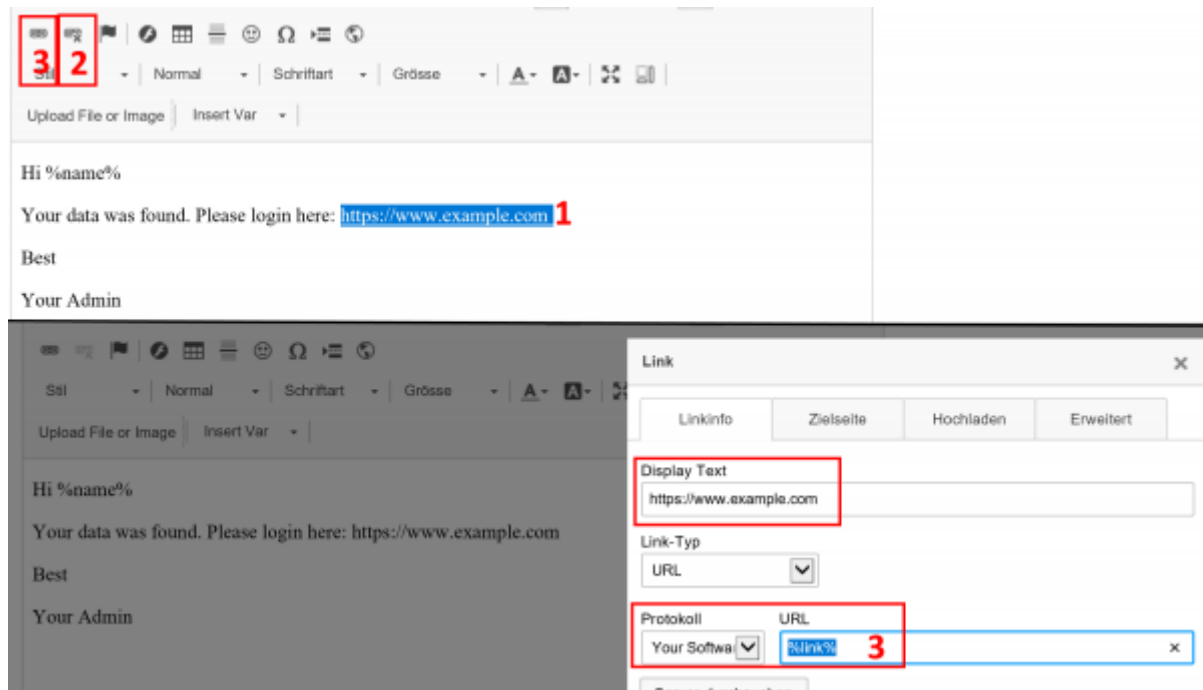
For all other settings please read the Mail Settings Chapter.

STEP 9 - Configure the Mail Delivery Method

You can define the mail delivery method on a globally within the settings menu. If you do so, it will overwrite all individual settings in a campaign. The second possibility is to configure the delivery methods within a campaign:
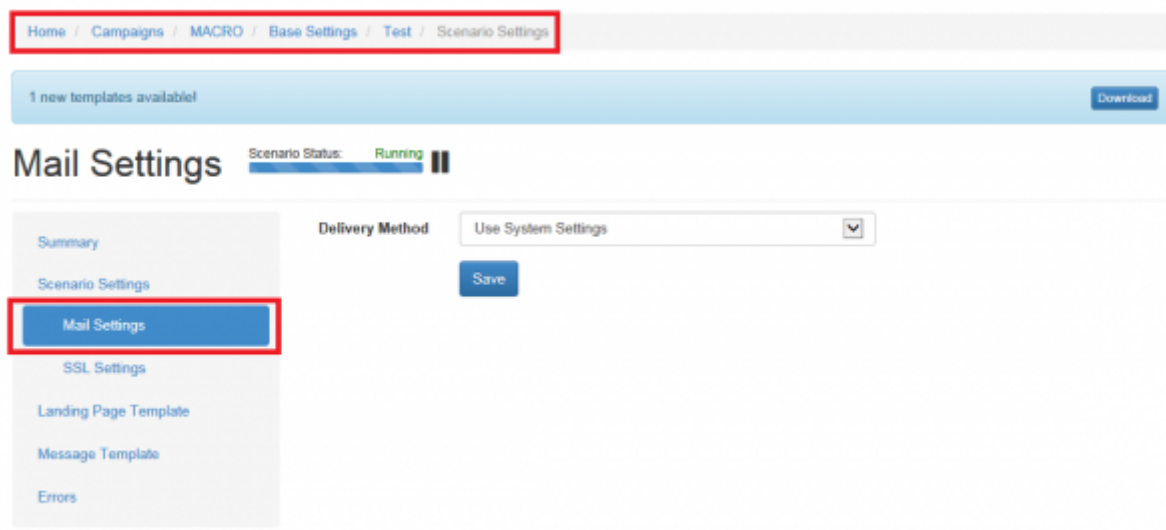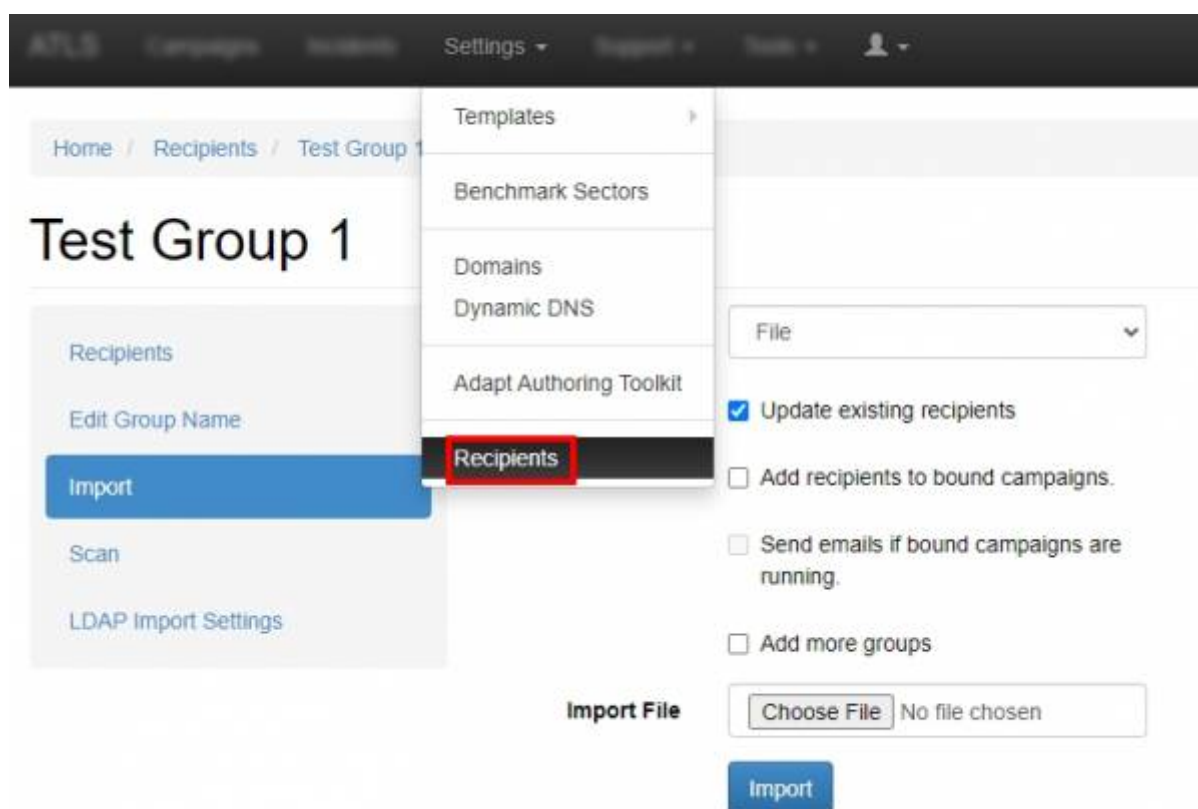

In LUCY the default delivery method for mails is using the build-in Postfix mail server. As many SPAM

filters will block mails coming from an new IP-address that has no reputation, the administrator can decide to configure an external mail relay.

STEP 10 - Add recipients

You need to create the Recipients List in the Menu item "Recipients".

This is the list of users that will get the phishing emails. You can add them manually, import a file with all your recipients or even search them on the internet. Once you have created that group, you can select it in your campaign and map them to a specific scenario. You can also define if they should be used only for the Landing Page link, the Awareness site link (e-learning) or both.

Please read the Recipients Settings Chapter for more configuration options.

STEP 11 - Add Scheduling Options to Your Campaign

If you want, you can create a schedule to run the campaign using a delay or customized time delays between campaign phases. If you are new to the system, we'd recommend that you go with the Default Timing Settings and skip this step. Please read the Schedule Settings Chapter for more configuration options.

Step 12 - Add E-learning Content to Your Campaign

You have the ability to provide the user with some awareness training in case he fails the phishing simulation. A failure to pass the phishing simulation is considered as a successful attack in LUCY. Therefore, it is very important that you define what you consider as an successful attack (because only those who have been successfully tested, will receive an awareness training). The awareness training can be done in two ways:

- **Send the eLearning via Mail**: There is the option to have LUCY automatically send some e-learning content to all users or only users who have failed the phishing test. This configuration

setting is part of an Separate Chapter (E-learning). If you want the users to get an e-mail with a link to the awareness content, you need make sure that in "STEP 7 - Configure Basic Settings" the checkbox "Send Link to Awareness Website Automatically" is selected and you configured an awareness template (mail and optional landing page).

- **Redirect the user from the phishing simulation directly to the eLearning page:** If you don't want the e-learning content to be delivered via mail you can also redirect the user directly to a landing page with the awareness content. Among the many variables that may be used in LUCY there is one called %link-awareness%. You can place that in the redirect input field described above (hyperlink based or web based). It will redirect the user automatically to the eLearning content when a link is clicked or data is submitted.

Step 13 - Start Your Campaign

Now you are ready to start. Although we recommend performing a test run with a single recipient before you start attacking all users, additionally it is a good idea to use the LUCY SPAM Checker. Just click "Real Attack" and LUCY will test your settings before starting the campaign. If you want to skip

the checks, press "Skip Checks". Your first recipients should receive the emails within seconds. Please read the Start Campaign Settings Page for more configuration options. If you experience any problems with starting/running your campaign, please Consult the Troubleshoot Section first.

Step 14 - Monitor Your Campaign

The progress of the campaign can always be monitored in Real-Time. Click "Statistics" within your campaign. Please read the Statistics Chapter for more configuration options.

Step 15 - Create Reports

Once you have finished the campaign, you may either export the raw data (CSV export) or create different types of reports (PDF, HTML or raw export). Please read the Creating Reports Chapter for more configuration options.

Troubleshooting

If you experience problems with your campaign please use this WIKI with the free text search option or contact us under support (at) lucysecurity.com