

Risk Assessment

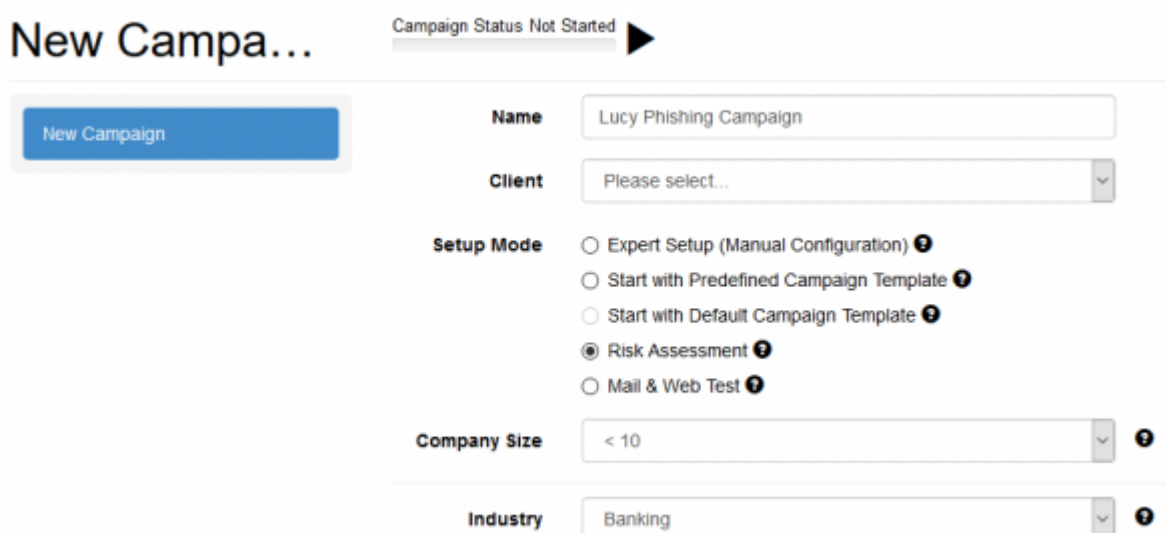
Instead of showing only raw data about how many users have been successfully phished, we can additionally provide a risk assessment methodology in LUCY, that shows the exposure to certain threats. We can classify different types of threats/Likelihoods such as

- Technical threats (e.g. unsecured windows PC, unsecure browser etc.),
- Internal threat (e.g. uneducated user who clicks on certain content) and
- Externals threats through hackers (latest trends in attacks, e.g. exploiting a specific browser vulnerability).

In LUCY 4.0 we implemented only a part of the 2nd analysis step and in the coming releases, this feature will be improved.

Using the risk assessment in LUCY

Select a new campaign and choose "risk assessment":



The screenshot shows the 'New Campaign' setup interface. At the top left is the title 'New Campa...' and a status indicator 'Campaign Status Not Started' with a right-pointing arrow. Below the title is a blue button labeled 'New Campaign'. The form contains the following fields:

- Name:** A text input field containing 'Lucy Phishing Campaign'.
- Client:** A dropdown menu with the placeholder text 'Please select...'.
- Setup Mode:** A group of radio buttons with the following options:
 - ☐ Expert Setup (Manual Configuration) ⓘ
 - ☐ Start with Predefined Campaign Template ⓘ
 - ☐ Start with Default Campaign Template ⓘ
 - ☒ Risk Assessment ⓘ
 - ☐ Mail & Web Test ⓘ
- Company Size:** A dropdown menu with the value '< 10' and a help icon ⓘ.
- Industry:** A dropdown menu with the value 'Banking' and a help icon ⓘ.

Select your company size and industry type. Then you will be presented a recommended set of attack templates:

New Scenario

[New Scenario](#)


Risk Assessment

Use as many various scenario templates as possible, in order to test your recipients more efficiently.

In order to properly perform a risk assessment, please use templates of the following types:

- 1 scenarios of type Web Based
- 1 scenarios of type File-Based
- 1 scenarios of type Hyperlink
- 1 scenarios of type Mixed

☐ - Recommended Scenario



You have an encrypted mail

11.01.2018 18:37

Encrypted Mail 1.1

Encrypted e-mail access. Asks the user to enter login data to access an encrypted e-mail message. In this scenario we ask the user for his/her username and password.

Preview Landing ▾ Preview Message ▾ Preview Lure ▾ **Use ▾**



11.01.2018 18:37

Fakebook 1.2

In this web-based scenario, we ask the user to login to "fakebook" and upload his own profile picture to the new corporate "fakebook" site.

Preview Landing ▾ Preview Message ▾ Preview Lure ▾ **Use ▾**

Please try to use a variation of different attack types (hyperlink, web based & file based) to get a better understanding, how your employees react to different threats. You will find the risk specific threats within the campaign statistics under "risk assessment".

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=risk_assessment&rev=1555922373

Last update: **2019/07/25 12:51**

