

Where can I create my phishing reports?

Within each campaign you will find a button that allows you to create a PDF, HTML, Word (docx) or raw CSV report based on a predefined template.

The screenshot shows the 'Lucy Phishi...' campaign page. At the top right, there is a 'New Report' button. A red arrow points from this button to the 'Generate Report' button located at the bottom of the configuration section. The configuration section includes fields for Template, Format, Font Size, Font Family, Scenarios (Chinese, Eng, German, Japanese), and Charts Options (Use Hourly Stats Period, Use Daily Stats Period, Customize Fields). The 'Generate Report' button is highlighted with a red box.

Once the report is created (please be patient - the report creation may take a few minutes) the status indicates that it is available for download (just click on the date/time to start the download):

The screenshot shows the 'Lucy Phishi...' campaign page. In the 'Results' section, a table lists the generated reports. The first report is 'Campaign Report 29.01.2019 15:43:43', which is highlighted with a red box. The 'Type' column shows 'PDF' and the 'Status' column shows a checkmark, indicating the report is ready for download. The table has columns for Name, Type, and Status. There are also pagination controls showing 1 of 10 items.

Name	Type	Status
Campaign Report 29.01.2019 15:43:43	PDF	✓

Below is an output of a LUCY sample report using the .docx template (please note that the recipient details are not included; this is a different template):



Phishing Test Result

04.03.2017

Prepared for Lucy Test

TABLE OF CONTENTS

1. INTRODUCTION AND GOALS
2. PROCEDURE, PREPARATION AND BASIC CAMPAIGN SETUP
3. MANAGEMENT SUMMARY
4. CHARTS
5. AWARENESS (E-LEARNING)

1. INTRODUCTION AND GOALS

What is a phishing simulation program?

A phishing simulation program (also commonly referred to as "self-phishing" or phishing assessment program) is a customizable awareness program used by information security professionals in higher education and private industry. This highly effective training program—which is typically incorporated into an existing campus information security awareness program—allows organizations to simulate phishing e-mails, help identify which users are more susceptible to such targeted e-mail attacks, and engage in more focused training opportunities to help users recognize phishing attempts.

What is the purpose of such a simulation?

According to the most recent data breach reports, a phishing email is often the first phase of an attack. That's because it works well with 30 percent of phishing messages ignored, but only 3 percent reported to management. But other employees are trained on how to spot phishing emails, and then get tested with mock phishing emails. The percent who fail within decreases with each round.

Why did we conduct a phishing simulation?

The current security awareness program of Company X (later referenced as X) does not include a process to verify the degree of awareness among employees. Without measurable data on the current awareness and training, the specific need of trainings as well as the benefit of future investments in this area cannot be clearly quantified. X is therefore asking Security Company Y to perform a security assessment for evaluating the effectiveness of the security mechanism as well as identifying the residual risks resulting from phishing and malware attacks.

What was the goal of this campaign?

The assessment should focus on the evaluation of the awareness of employees worldwide on phishing and malware attacks. This check of your employees and IT security should highlight the strengths and weaknesses in the area of external infrastructure (X). FTL, SMTP Filters & ECD products including an evaluation to

Campaign Status

Campaign: View Stats in 10sec Template

Started at: 2017-02-18 17:08:16

Stopped at: 2017-02-22 12:20:30

Notes:

Campaign Scenarios

Scenario	Stats
Template: Encrypted Mail	Encrypted e-mail access. Offers user to enter login data to access an encrypted e-mail message. In this scenario we ask the user for his username and password.
Domain: security-verification.tpc	
SSL: No	
E-Mail: No	
Attack: No	
Collect Data: Partial	
Redirect URL: No	
Double Barrel: No	
Regex: Login Regex: /a-zA-Z Password Regex: /a-zA-Z0-9	

3. MANAGEMENT SUMMARY

Summary results

The phishing attack against all XY users started on XY and ended on XY. The Test was stopped by X at the end of XY users.



In average about XY % of the people who clicked on a link in the mail submitted their respective username and password. We can exclude that people just entered some random data in the login field because we record the last three letters of the username. The following chart shows the overall success rate.



4. CHARTS

In this chapter we present the more detailed statistics.

Daily & hourly charts

The daily and hourly charts show how the success and success rate of the phishing campaign developed over the first few hours of the campaign and also over a longer time range.




BeEF Stats

BeEF is short for The Browser Exploitation Framework. By using techniques similar to common drive-by Malware, it can access the security of a target's internal environment, bypassing the hardened perimeter. Unlike other security frameworks, BeEF hooks past the hardened network perimeter and client systems, and examines exploitability within the context of the one open door: the web browser. BeEF can be used to "hijack" exposed files and browser-based vulnerabilities like cross-site scripting (XSS), using client-side attack vectors. If a user clicks on a link that BeEF put there, it will hook the user's browser into the BeEF server which is now also part of LUCY. The tool can also issue commands to the browser, such as: redirecting, changing URLs, generating dialogue boxes and more. It has the ability to run Malware on the hooked browser IP address and use it as a launching point to infects other computers on the same network, effectively spreading the Malware. With the integration of BeEF into LUCY, companies can now answer two main questions: "Is our employee safe for a phishing attack?" And if they do, would their browser security settings have prevented more damage from browser exploitation type attacks?

Client Statistics (OS, Plugins etc.)

In this chapter we show how the clients accessed the mails and answer the question what operating system, browser type and also browser plugins has been used.






Country Charts

The country charts show from which IP addresses and countries the users accessed the phishing links. Please note that if users are surfing over a proxy, the country source may be inaccurate.



Additional charts

The additional charts show custom statistical data specific to the campaign. Examples for such custom statistics could be:

- CERT (computer emergency response team) responses from users
- Users who replied to the attacker
- Users who participated in security training programs prior to the phishing campaign
- etc.






Country Success Rate

5. AWARENESS (E-LEARNING)

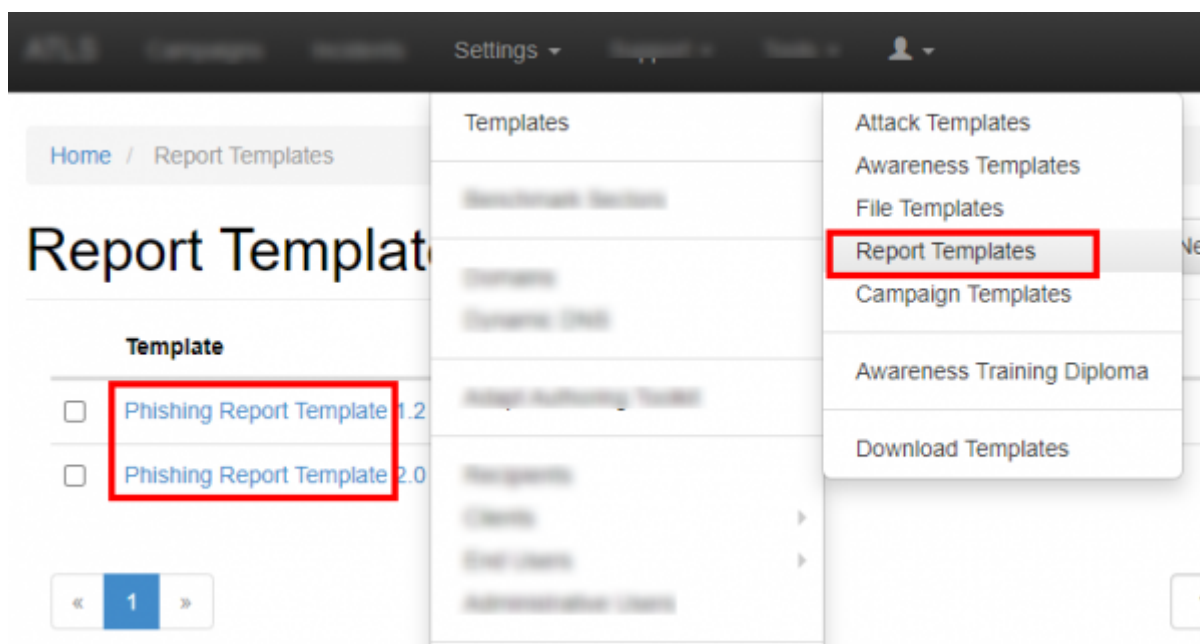
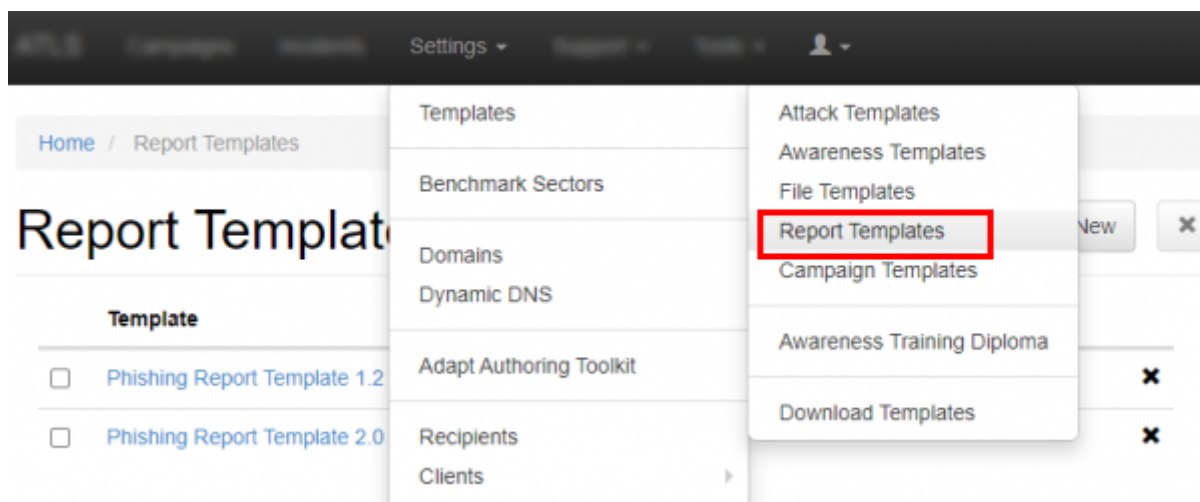
Awareness templates can be used to learn users about the risks of phishing and malware attacks. It helps reduce the users susceptibility to successful phishing attacks and malware infections. Here is the overall e-learning statistic.




Awareness E-learning

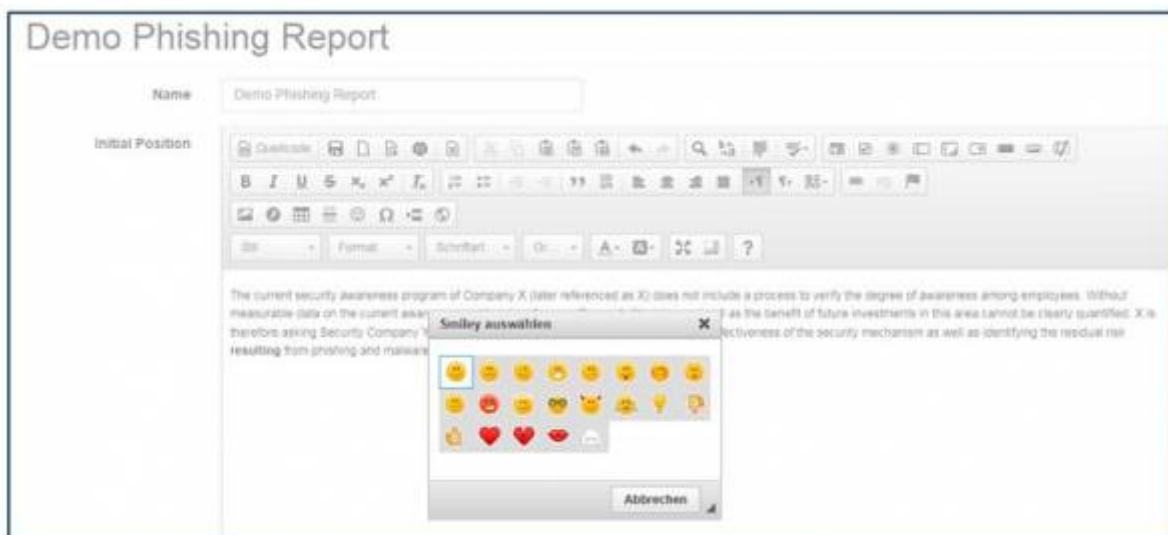
Where can I find my report templates?

LUCY comes with one predefined report template called "Demo Phishing Report". You find it under "Settings/Report-Templates".

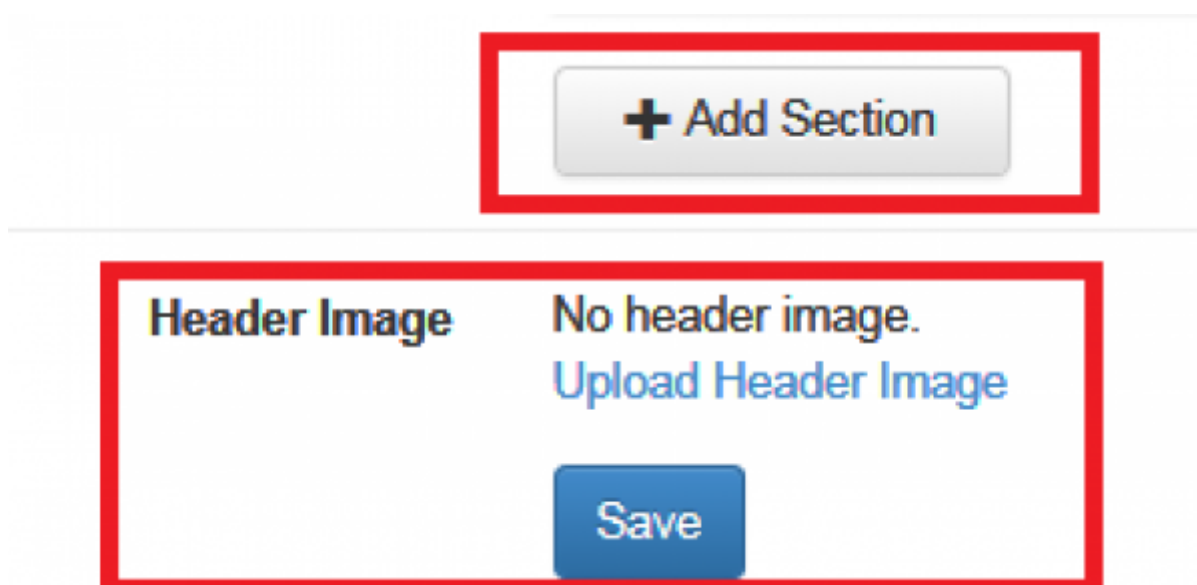


How can I edit my report templates?

You may either edit the existing template or create a new one. The template contains sections which can be freely edited. These sections can be used later in PDF, HTML or Word reports which are generated within a campaign.



You may add your own sections and also customize the title name and logo.



What variables can be used for the report?

Lucy comes with a constantly growing list of variables which are placeholders for specific statistics or graphics. Those placeholders can be inserted in the content of any section at any point. You find the variables within the variable list in LUCY:

Home / Report Templates / Phishing Report Template 1.2

1 new templates availableDownload

Phishing Report Template 1.2

Variable List

11

%report.createdate%	Create Date Of Report
%report.author%	Author Of Report
%startdate%	Start Date & Time Of Campaign
%finishdate%	Finish Date & Time Of Campaign
%creator%	User Who Created The Campaign
%file.formats%	File Based Attacks: Name Of File Formats Used In Campaign Scenarios
%scenarios.number%	Number Of Scenarios Used In Campaign
%scenarios.names%	Names Of Scenarios Used In Campaign
%scenarios.types%	Types Of Scenarios Used In Campaign
%client%	Client Name
%opened%	Percentage opened mail
%attacks.att%	Percentage attacks on site

Name

Phishing Report Template 1.2

Management Summary

Management Summary

Quellcode

Summary results

The phishing attack against all XY users started on XY and ended on XY. The Test was stopped by X at the count of XY users.

%charts.summary%

In average about XY % of the people who clicked on a link in the mail submitted their windows username and password. We can exclude that people just entered some random data in the login field because we record the 1st three letters of the username. The following chart shows the overall success rate:

%charts.totalstats%

About XY of the people who received the mail clicked on that link. Since not clicking on the link can be caused by many reasons (no interest in specific shopping offer, vacation etc.)

When you create the report within a campaign those variables will be populated with your specific campaign statistics (similar to the graphics you already know from the dashboard). Those variables are:

- %report.createdate% Create Date Of Report
- %report.author% Author Of Report
- %startdate% Start Date & Time Of Campaign
- %finishdate% Finish Date & Time Of Campaign
- %creator% User Who Created The Campaign
- %file.formats% File Based Attacks: Name Of File Formats Used In Campaign Scenarios
- %scenarios.number% Number Of Scenarios Used In Campaign
- %scenarios.names% Names Of Scenarios Used In Campaign
- %scenarios.types% Types Of Scenarios Used In Campaign
- %client% Client Name

- %opened% Percentage opened mail
- %clicked% Percentage clicked on link
- %domains% Domain(s) Used In Scenarios Settings
- %timezone% Timezone Setting Of LUCY
- %recipients.groups% Recipient Group Names In Campaign
- %awareness.name% Name Of Awareness Template Used
- %awareness.sent% Number Of Awareness Emails Sent
- %awareness.incomplete% Number Of Users With Incomplete Training
- %awareness.completed% Number Of Users Who Completed Training
- %questions.number% Number Of Questions In Quiz
- %data.number% Absolute Number & Relative Number Of Collected Data From Users
- %logo% Logo
- %table.contents% Table Of Contents
- %system.info% System Information
- %file.settings% File Based Attacks: Settings Table
- %scenarios.settings% Scenarios Settings
- %message.settings% Message Template Settings
- %schedulers% Scheduler Settings
- %awareness.settings% Awareness Website Settings
- %data% Reports the file attack output & form POST data
- %additional.fields% List Of Available Recipient Fields
- %victim.table% Detailed Victim Results
- %quiz% Quiz Questions
- %analyse.stats% Analyse Statistics
- %benchmark.stats% Benchmark Statistics
- %compare.stats% Campaign Comparison Statistics
- %charts% All Charts
- %charts.summary% Summary Chart
- %charts.totalstats% Total Stats Chart
- %charts.analyse% Analyse Stats Chart
- %charts.dailystats% Daily Stats Chart
- %charts.hourlystats% Hourly Stats Chart
- %charts.events% Events Chart
- %charts.os% Operating System Chart
- %charts.browsers% Browsers Chart
- %charts.files% Files Chart
- %charts.plugins% Plugins Chart
- %charts.countries% Countries Chart
- %charts.awareness% Awareness Stats Chart
- %charts.additional% Additional Charts
- %charts.custom% Custom Fields Charts
- %charts.responses% Track Responses Chart
- %awareness.website% Awareness Website Screenshot
- %awareness.mail% Awareness Mail Template Screenshot
- %message.screen% All Message Template Screenshots
- %landing.screen% All Landing Page Screenshots
- %message.screen#% Message Template Screenshot (# - replace on scenario id)
- %landing.screen#% Landing Page Screenshot (# - replace on scenario id)

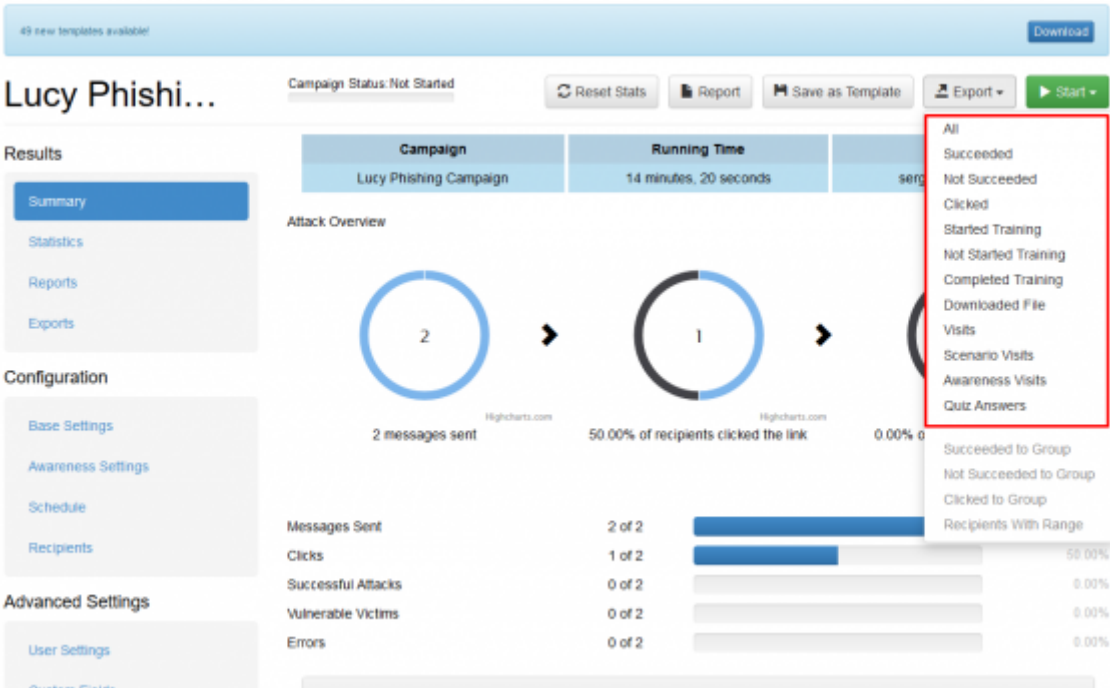
You can see the result of using each of the above variables [here](#).

Can I add custom parameters to my report?

Yes - with LUCY > 3.1 you can [add custom parameters](#) to your report.

How can I create raw CSV exports of my campaign data?

If you click on a campaign name you will be able to export all data to a raw CVS export:



The export then can be downloaded under support/exports:

Home / Exports				
1 new templates available! Download				
Exports				
Date	Name	Type	Status	
04.03.2017 17:23	Campaign - Video Stats in Mixed Template	Not Succeeded	✓	✗
04.03.2017 17:13	Campaign - Video Stats in Mixed Template	All Victims	✓	✗
04.03.2017 17:00	Total	Scenarios	✓	✗
03.03.2017 20:59	Total	Campaigns	✓	✗
03.03.2017 12:35	Total	Campaigns	✓	✗



Reports in the CSV format are generated using the default separator (tabulation). Please consider this when opening CSV files - in some versions of Excel you may need to manually specify the type of separator when opening the file.

You can change the default separator in the Advanced Settings section:

Date & Time	29.01.2019 16:00	
Time Zone	Zurich - UTC+01:00	▼
Date Format	29.01.2019	▼
<input type="checkbox"/> Use Proxy		

Password Settings	<input type="checkbox"/> Set User Password Policy	
Rotation Period	Off	▼
Bruteforce Protection	<input type="checkbox"/> Enable Security Image	
2FA Key		

<input checked="" type="checkbox"/> Enable Ajax Updating	
Ajax Update Period (seconds)	5
Export Data Separator	Tab ▼
Export Double Quotes	<input type="checkbox"/> Enclose In Double Quotes
Campaign Approval Period (days)	5
Spam Test	<input type="checkbox"/> Use Full Blacklist

Is it possible to automatically export report data?

You can have LUCY automatically create a report and send it to the email address associated with the user that created the campaign by clicking on the checkbox "After I stop the campaign, send me a report to...". As soon as you stop the campaign the report will be mailed to that address:

Summary

User Settings

Statistics

Recipients

Base Settings

Custom Fields

Schedule

Awareness

Reminders

Reports

Supervision Log

Message Log

Errors

Name

TEST

Client

Lucy Test

Setup Mode

☒ Expert Setup (Manual Configuration) ?

☐ Setup Wizard ?

Benchmark Sector

N/A

Notes

☐ Email Tracking ?

Antivirus/Firewall Protection Interval

off

☒ After I stop the campaign, send me a report to oliver@muenchow.ch

Template

Please select...

Format

Please select...

Font Size

12

Font Family

Helvetica

Scenarios

☒ Login to Microsoft

Save

Search...

Q


Scenario

Template

Type

Login to Microsoft

Edit Scenario Settings

Microsoft 365 Online Login /  English

Mixed

X

< 1 >

10

Is it possible to automatically pull report data from LUCY (e.g. from your SOC)?

You can fetch all campaign statistics by using our REST API.

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

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=create_campaign_reports&rev=1551184095

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

