

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:

test Scenario Status: Running ||

[Summary](#)
[Scenario Settings](#)
[Mail Settings](#)
[SSL Settings](#)
[Message Template](#)
[Errors](#)

Template

Cisco WebEx Meeting (Version v. 2.1) / English
[Change/Select Template](#)

Name

test

Landing Domain

Local IP

Note: currently there are no domains configured in Lucy. You can point your existing domain to this server and save the domain [here](#) or you can start the

[Lucy Domain Registration Wizard](#)

Custom Domain

192.168.1.147

Languages

English
[+ Add](#)

☒ Anonymous Mode

☐ Track Opened Emails

☒ Send Link to Awareness Website Automatically

Send Awareness By Click Rate

%

Send Awareness By Success Rate

%

Awareness Delay

0

Please note that this operation cannot be undone!

The personal information is then no longer visible:

Recipients

Awareness Website

Benchmark

Compare

Reports

Exports

Configuration

Base Settings

Awareness Settings

Schedule

Recipients

test

test

oliver
iphone

test

test

test

test

Name

E-mail

Phone

User History

Lure Sent

Message Sent

Training Sent

Reported

Success Rate

Click Rate

Clicks

Successful Attack

Trained

Downloaded Files

Plugins

Vulnerable Applications (0)

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

Date & Time	<input type="text" value="15.11.2018 14:11"/>	
Time Zone	<input type="text" value="Zurich - UTC+01:00"/>	
Date Format	<input type="text" value="15.11.2018"/>	
<input type="checkbox"/> Use Proxy		

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

	<input checked="" type="checkbox"/> Enable Ajax Updating
Ajax Update Period (seconds)	<input type="text" value="5"/>
Export Data Separator	<input type="text" value="Tab"/>
Export Double Quotes	<input type="checkbox"/> Enclose In Double Quotes
Campaign Approval Period (days)	<input type="text" value="5"/>
Spam Test	<input type="checkbox"/> Use Full Blacklist
Recipients	<input type="checkbox"/> Generate Short Recipient Links
Let's Encrypt	<input type="checkbox"/> Autorenew

Campaigns	<input type="checkbox"/> Disable Campaign Checks
Benchmark Sharing	<input type="checkbox"/> Send Anonymous Benchmark Data
	<input checked="" type="checkbox"/> Don't ask to send Anonymous Benchmark Data
Anonymous settings	<input type="checkbox"/> Anonymize Recipient Identical Data (browser, OS, location)

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

**Anonymize Recipient
Attributes**

Hide the following fields in Anonymous Campaigns and Scenarios:

- ☐ Hide Country Attribute
- ☐ Hide OS Attribute
- ☐ Hide Browser Attribute
- ☐ Hide Location Attribute
- ☐ Hide Division Attribute
- ☐ Hide Comment Attribute
- ☐ Hide Staff Type Attribute

Save

From:

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

Permanent link:

<https://wiki.lucysecurity.com/doku.php?id=anonymisation&rev=1561407519>

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

