Note: Please always verify that you run the latest LUCY version. Bug fixes are not included in the security patches - only within the regular updates, which are available for commercial clients. Community Edition Users therefore need to make sure, that they first download the latest version!

Some buttons or certain features don’t work

Always make sure you are running the latest version of LUCY by checking if there are any updates available. If updating the system via HTTP does not work: download the latest version from the internet.

The scheduler uses a wrong time zone to send out mails

Please define your time zone within the settings menu.

We use a proxy to connect to the internet

Within the settings menu you can specify a proxy server together with the port and login credentials. LUCY will use those settings to connect to the internet.

Mail communication issues

If you experience mail issues we recommend first checking the error log within your campaign:

There are many reasons for mail communication errors. Example: In LUCY mails appeared to be send to your recipients. But mails never arrived or arrived very late. There a few issues to check:

- Did you use a mail address with a domain that points to a different MX record? If you use attacker@gmail.com as an example for the sender most mail servers will block that mail since LUCY is not the official mail server for this service.
- Did you use a valid recipient address? If you uploaded a recipient like

"info@domain_does_not_exist.com no mail will arrive since there is no mail server for the domain domain_does_not_exist.com"

- Mail might have arrived in the spam inbox because some spam filters may classify mails as spam if the subject or body contains specific words. You can verify your mail content by using a free service like https://www.mail-tester.com/ (german) or http://isnotspam.com/ (English).
- Mail might have been rejected at the recipient mail server because many mail servers reject mails from a server, that has no valid MX record. You would see the status within LUCY in the error log.
- LUCY is sending mails in most cases via SMTP (port 25). If you place LUCY in a company LAN keep in mind that in most cases port 25 to your official MX (mail server) is not opened from the LAN to the DMZ or wherever your mail server is located. LUCY also needs to be able to resolve DNS (port 53) to make that MX lookup.
- Did you define your own company domain as a sender? Example: you try to phish your employees with the domain mycompany.com, which actually is the official domain for your company? Problem is: there might be a DNS record (example SPF) that defines, which mail server is allowed to send mails on behalf of this domain. If such a record exists your mail server will deny mails coming from a different server using this domain. The solution here: if you still want to perform a phishing test with a domain like the one from your company we recommend reserving a similar domain like "my-company.com" or place a typo in there like "myconpany.com". Most users won't recognize the difference and you have an additional feature to test the awareness.
- Did you also modify your DNS entries to match the scenario? Some SPAM filters for example will test if there is a valid PTR (reverse DNS) set for the host that sends a mail. If it doesn't exist, it will be rejected. Most providers allow you to define MX, TXT, A records for your domain/host. But not only the PTR is required. Your SMTP banner sometimes also gets checked, if it matches the hostname. To change the hostname within the mail service you can set the hostname within /etc/postfix/main.cf like this: "myhostname=server.example.com". Then restart the mail server: "postfix stop && postfix start"

LUCY says "mail test failed" when I start a campaign

To make sure mails arrive we recommend defining a test mail recipient and conducting a test run. If the mail does not arrive you can contact us and we will help you.

Mails may arrive delayed

This is usually not caused by LUCY. If we cannot establish a SMTP connection we won't retry for many hours. This is easy to verify: LUCY tells you if all mails have been send. Usually this is done within seconds or minutes and can also be tracked with Wireshark or similar tools. So if all mails have been sent then technically there is nothing left for LUCY to do to accelerate delivery. So in over 95% of cases the process of delivery takes less than a minute. In a few cases the message could take as long as 5 days to complete its trip from sender to recipient. It rarely takes more than 5 days, as one of the SMTP servers will send the message back as undeliverable. And yes, the e-mail that contains the error message could take 5 days to get back! You also have to remember that there is a lot of software and hardware in between that your email has to pass through to get from the point of origin to its destination. Whether is server hardware, software, routers, switches, copper or fiber optic cables, power grids, or even your own computer, there are many potential points of failure along the way. If

any one of these has an outage or is overloaded, a delay can occur.

Setup Issues: LUCY does not get an IP address

- Make sure your VMWARE setting is set to "bridged" (not NAT!)
- Use the build in network tools within VMWARE to verify if you can reach external servers

Accessibility: I cannot reach LUCY Webgui

- Did you to setup a host file with a server name, that points to the IP you have configured within the initial setup script?
- Are you using the correct IP address/port (you cannot reach a private IP address from the internet. If you don’t have a public IP address you need to create a free DynDNS or similar service account to be able to match the private IP address with a public reachable DNS name)
- Make sure the firewall allows access to LUCY on port 80/443

I can reach LUCY via HTTP/S – but I only see the pink LUCY 404 not found page

- This happens, if your webserver is running and the port is accessible, but you either mistyped the URL or used a domain name, that is not configured in the initial VMware setup (example: your server is configured within VMware with a private ip 192.168.10.10 and a domain like lucy.local but try to access LUCY with a domain like example.com which you defined for that IP on your DNS server. To solve this you simply need to go into the VMware setup again and define your domain (e.g. example.com) as a domain name.
- If you stopped a campaign but click on the old link you will get a 404 page
- You might see a 404 when you try to access the landing page from a phishing mail created by LUCY. This might happen if you have accessed the scenario already as an LUCY administrator before accessing the link in the email. In that case LUCY will have set a cookie that causes the problem. This cookie will tell LUCY to directly forward you to the authenticated landing page which sometimes causes a 404 error. The solution is to delete all cookies in your browser and restart the browser and try to access the link in the mail again.

Exe Collection Data: Lucy cannot see any data from users that clicked on the executable

- Is the Exe running on Win7/Win8 with Internet Explorer? If not it won’t work (e.g. if it gets executed on a MAC or Linux Host). We support Mozilla Firefox too. But there might be issues depending on the browser settings.
- Can you reach LUCY from the internet via HTTP or HTTPS? If not the tool also won’t be able to save the data. Make sure the DNS resolution works and the according firewall port mappings are set.

Malware Simulation: The Malware sample gets “detected/blocked” by my

Antivirus

It is very unlikely that the file is classified as a virus since we don't simulate any virus behaviors (we don't do any changes on the system). But we noticed that certain vendors have a category like "suspicious. insight" or "unknown". Basically it gets classified comes from an unknown source and there is no record of this file in the internet. As a result any unknown software would be put in this category.

Recipient Statistics: a user has accessed LUCY for example with MAC OS & Safari but in the browser and OS stats it says for example Windows /IE

- Unordered List ItemThis could happen if the access over the internet from the client is going over some gateway (proxy, content filter etc.). LUCY might only see the connection details from that gateway.

Statistics Page: I see way more page views than send out mails

- It is possible a user forwards the mail or clicks on the same link more than one time
- It is possible the user re-visits/re-fresh's the page
- Page views are always higher than the amount of mails send since each page (login page, account page or refresh of the browser counts as a page view).

Statistics Page: I see way more link clicks than send out mails

- There are circumstances where automated SPAM filters on a mail gateway will first visit and test all the links before sending out the mail. LUCY records those links as visited, even though the mail might not have arrived at the user yet.

Running a Campaign: the link does not work anymore

- After starting your campaign the users will get a randomized URL send via Mail that might look like this: Users will get some random link send within a campaign that might look like this: https://phishing.withlucy.net/a5b371863fc2d6b5e2bf2bc2199597135f3db17c9a9194247002ae86e24c75ff. This is a system generated link that cannot be altered! Each user gets a different link. In case you changed the link in the mail manually it won't work.
- Another reason why the URL is not reachable anymore is when the campaign is stopped. Only when it is started the URL will work.

Running a Campaign: It takes me automatically to the "authenticated" account page when I click on the URL in the mail

- This means that you have already clicked on that URL in the mail before and authenticated. As an authenticated user you will have a session cookie stored in your browser which takes you automatically to the authenticated page. This is intended since we don't want users to

authenticate twice. By deleting your browser cache you will get to the login page again after clicking on the link in the URL

I ran a campaign with a test group, modified the templates and wanted to run it again. But mails then are not sending out to the same group again.

To solve this you simply need to stop the campaign, delete the recipient group, then add the same recipient group again and start the campaign again.

Awareness Website: the awareness website is not working.

Opposite to the phishing website the awareness website has to be started manually in order to work (has to be published and started). Sometimes the automatic sending of the awareness site also depends, if LUCY has recorded an successful attack. This depends on the scenario type. Example: if you create a file based campaign and then use a data entry template LUCY won’t consider the login from the user as a “success”. Only the file download from a user would be a “success” and start the automatic awareness mail.

Infrastructure Issue: Links in mails in my company cannot be opened

You might not allow direct access to the internet via a web browser. Instead you might allow access to the internet using a physical different PC or a different infrastructure (e.g. accessing the internet via Citrix etc.). As a result a link sent in a mail can’t be opened). The only way to conduct a phishing attack in such an environment without having the user to type a long randomized URL into a different system is by setting a directory within the URL manually. This can be done within the recipient file. There is a variable which you can set called “Link” – a unique link part for the landing page. If you specify this, please make sure it is unique across all recipients in the scenario and does not contain any special characters. If you skip this, the link will be generated automatically. You can choose a simple name for a link for a group of recipients (keep in mind that you can upload different recipient groups per scenario). Recipient group 1 could look like this:

john.smith@example.com:Smith:::::USA.

Recipient group 2 could look like this:

peter.meier@example.com:Meier:::::Switzerland

The user from Recipient group 1 would then receive a link to your campaign which he can remember easily (and therefore manually type in a different browser) like http://your.phishing-domain.com/USA. The user from Recipient group 2 would get a link like http://your.phishing-domain.com/Switzerland.

Running LUCY without access to the Internet: is it possible to operate LUCY even if there is no connection to the Internet?

LUCY can run without any internet connection. But there are certain scenarios where an internet connection might be required:

- License: after booting LUCY tries to contact our licensing server to get a workstation ID & key. If no internet connection exists, no key will be downloaded. If you switch from the community edition to a commercial license LUCY needs to be able to connect at least one time to our license server
- Updates: all updates require a http connection to our update server in Germany
- SSH: if you want to enable SSH access for remote support, LUCY will connect via port 22 to our SSH hopping station. On this host we can connect via SSH as well with the port and password which is provided by you.

When you perform a test run with your campaign the SPAM check hangs

If you’re using Debian 7 and installing the software through the shell script, then you might need to reboot the system for Spam Assassin to start. It may fail to start automatically sometimes - that’s why the Spam Check may hang. That behavior has been fixed in 2.2. In LUCY 2.2-2.5 the SPAM check will verify over 200 online DB's. This takes at least 10-15 minutes for this check to be finished! Starting from 2.6 the SPAM check is optional and not enabled by default.