

GUIDE TO USING THE GLOBALEAKS PLATFORM

Recipients

Whistleblowing Solutions¹ (WBS) is a non-profit social enterprise that supports the fight against corruption through the research, development and provision of specific digital technology and operational support to anti-corruption organisations. These organisations, in turn, support whistleblowers in reporting malpractice worldwide.

The goal of WBS is to support the development of the GlobaLeaks free software and to foster a large community of those who support whistleblowers.

This guide was produced as part of the “Speak Up Europe” project, which was funded by the European Union’s Internal Security Fund — Police. The content of this publication represents the views of the author only and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.



**Funded by
the European Union**

Guide to using the GlobaLeaks platform. Recipients

Author: Maria Sideri (Transparency International Secretariat)

Contributors: Giovanni Pellerano, Susanna Ferro (Whistleblowing Solutions) Anoukh de Soysa, Marie Terracol, Aram Khaghaghordyan, Shubham Kaushik (Transparency International Secretariat), Donncha Ó Giobúin (Transparency International Ireland), Vasja Cepic (Transparency International Slovenia), Giorgio Frascini (Transparency International Italy)

Every effort has been made to verify the accuracy of the information contained in this report. All information was believed to be correct as of May 2023. Nevertheless, Whistleblowing Solutions cannot accept responsibility for the consequences of its use for other purposes or in other contexts.

2023 Whistleblowing Solutions. Except where otherwise noted, this work is licensed under CC BY-ND 4.0 IT. Quotation permitted. Please contact Whistleblowing Solutions – info@whistleblowingsolutions.it – regarding derivatives requests.

¹ [Social Enterprise - Whistleblowing Solutions](https://www.whistleblowingsolutions.it/) (https://www.whistleblowingsolutions.it/)

WHAT IS THE PURPOSE OF THIS GUIDE?

This guidance has been developed to accompany the roll-out of the GlobaLeaks platform to interested organisations. It is a step-by-step guide created to explain how to access and use the platform in order to receive and manage whistleblowers' reports, as well as to communicate with whistleblowers by exchanging comments and/or messages. For the purpose of this guide, the organisation's staff authorized to securely access and manage whistleblowers' reports are called **Recipients**.

CONTENTS

Glossary	5
I. Getting started	6
First login	6
Access and save your Account Recovery Key	7
Enable Two-Factor-Authentication (2FA)	8
Change your password	9
Request support	10
<hr/>	
II. Accessing a New Report	11
Important notes before accessing whistleblowers' reports	11
How to access a new report	12
Important notes before opening files attached by whistleblowers	14
List of possible actions you could perform on a report	15

GLOSSARY

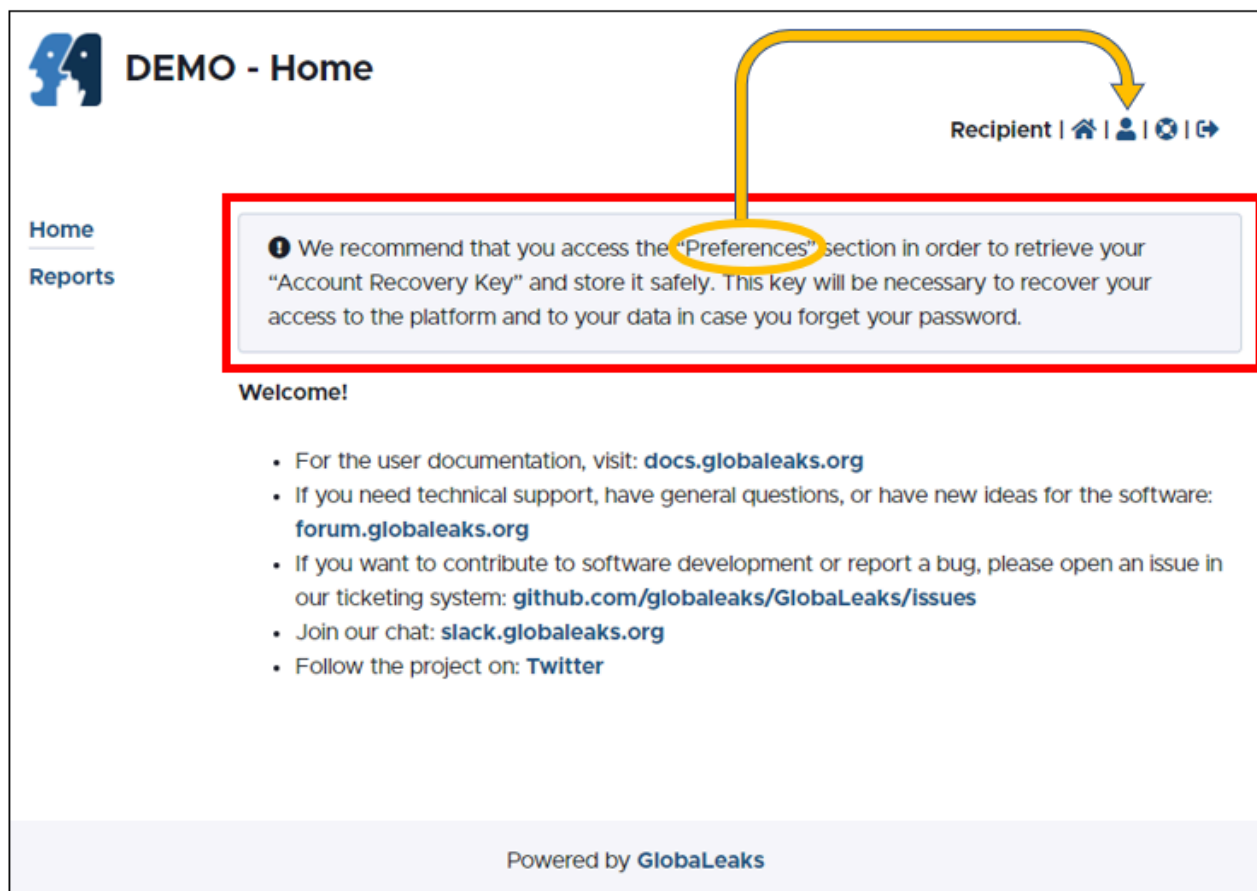
- **Administrator**
The user who is running the GlobaLeaks platform. Administrators perform the maintenance and overall management of the platform, and provide technical assistance to the organisation's staff managing the whistleblowers reports. Administrators do not have access to whistleblowers' reports.
- **Whistleblower/reporting person**
The user who submits a report through the GlobaLeaks platform.
- **Channel**
The platform's reporting channel; it can also be an area of issues addressed by the organisation (e.g., Corruption-related complaint). The platform offers the possibility for more than one reporting channels, offering the whistleblowers the option to select the topic of their report and submit through the appropriate reporting channel. Also, each reporting channel could be assigned to and managed by a different recipient.
- **Notification**
The email sent to inform a recipient of a new report, or an update relating to an existing report.
- **Platform**
The system running the GlobaLeaks software.
- **Questionnaire**
A set of questions that a whistleblower is asked to answer in order to file a report.
- **Receipt**
A random 16-digit code generated by the system and provided to whistleblowers upon the submission of their report, enabling them to access and update their report by adding comments and new files/evidence.
- **Recipient**
The user enabled to read, verify, and analyse whistleblowers' reports. Recipients may also communicate with whistleblowers via the platform to solicit additional information and evidence, by exchanging messages.
- **Report**
The object of a whistleblower's submission, including answers to a questionnaire and attached material.
- **Submission**
The action performed by the whistleblower when filing a report.

I. GETTING STARTED

FIRST LOGIN

Once the new user account is created, you will receive an “Account Activation” email, containing your Username and an activation link.

By clicking on the activation link the system will invite you to create your password, and then direct you to your homepage. There, you can find useful links for GlobaLeaks user guidance, software security, best practices and community support² – and an **important recommendation**:



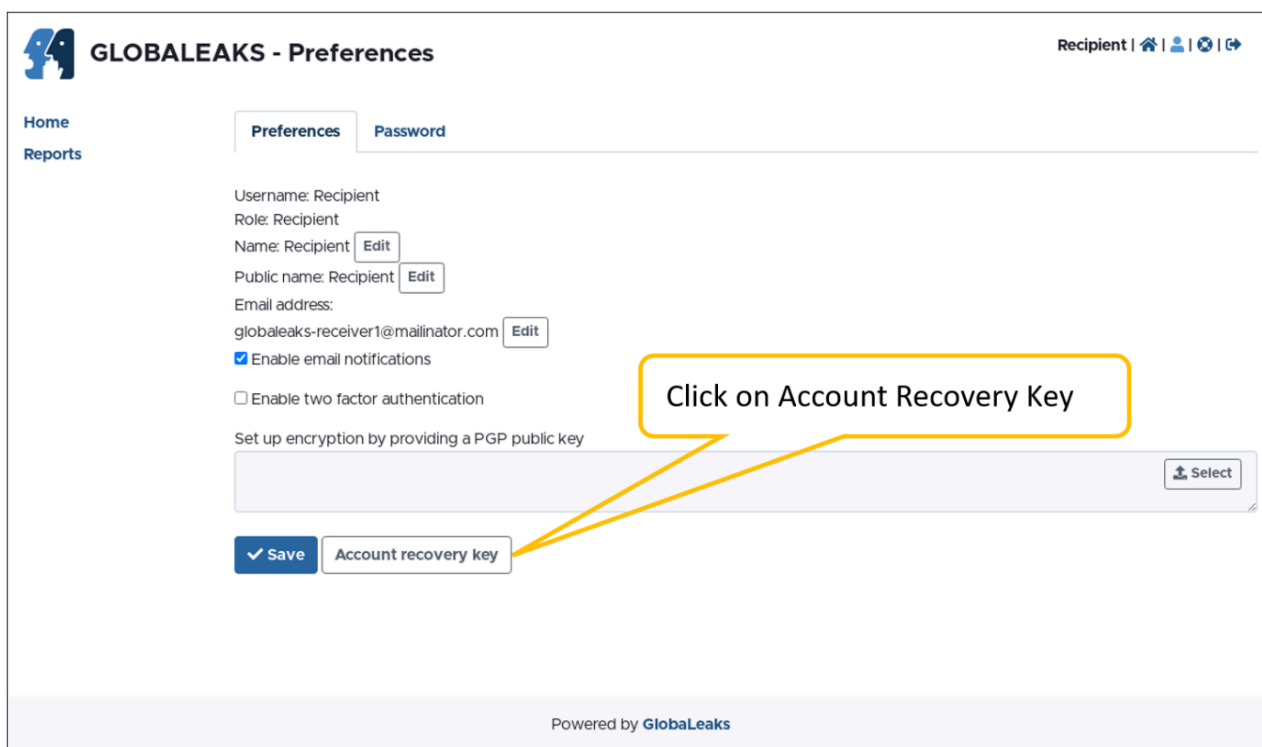
² if you encounter a problem using the platform, create an issue on the GlobaLeaks ticketing system [<https://github.com/globaleaks/GlobaLeaks/issues>] and help improve transparency worldwide!

ACCESS AND SAVE YOUR ACCOUNT RECOVERY KEY

After first login, you should access your [Account Recovery Key](#) on the [Preferences](#) page and save it in a secure location. You will be prompted to enter your password before the [Account Recovery Key](#) is made available.

IMPORTANT NOTE

This is a *fundamental step* that all Users should do at their first login after activating their account in order to back-up their own account recovery key. **Password loss will result in data loss**: any data received by a user will not be accessible after a password loss and reset without an account recovery key.



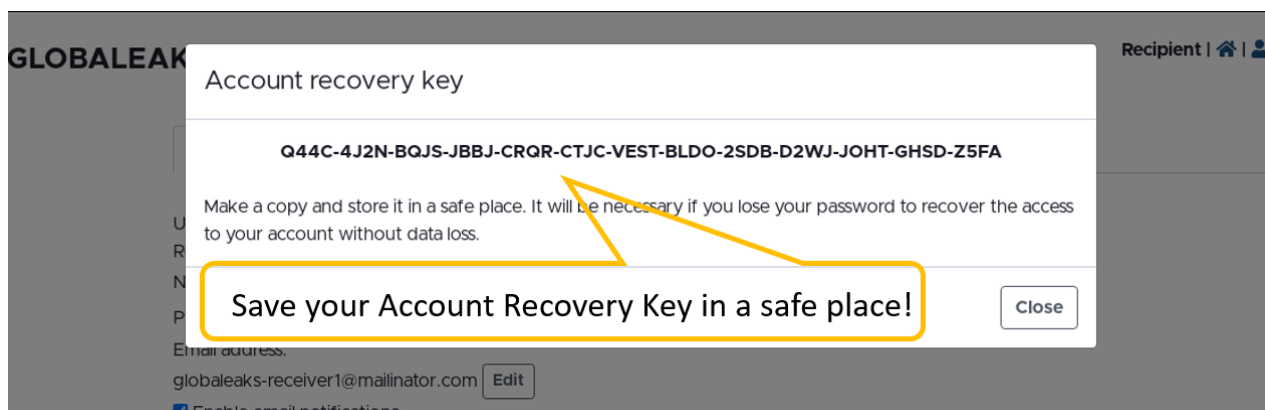
GLOBALEAKS - Preferences Recipient | Home | Profile | Logout

Home Reports

Preferences Password

Username: Recipient
Role: Recipient
Name: Recipient
Public name: Recipient
Email address: globaleaks-receiver1@mailinator.com
 Enable email notifications
 Enable two factor authentication
Set up encryption by providing a PGP public key

Powered by [Globleaks](#)



GLOBALEAKS Recipient | Home | Profile | Logout

Account recovery key

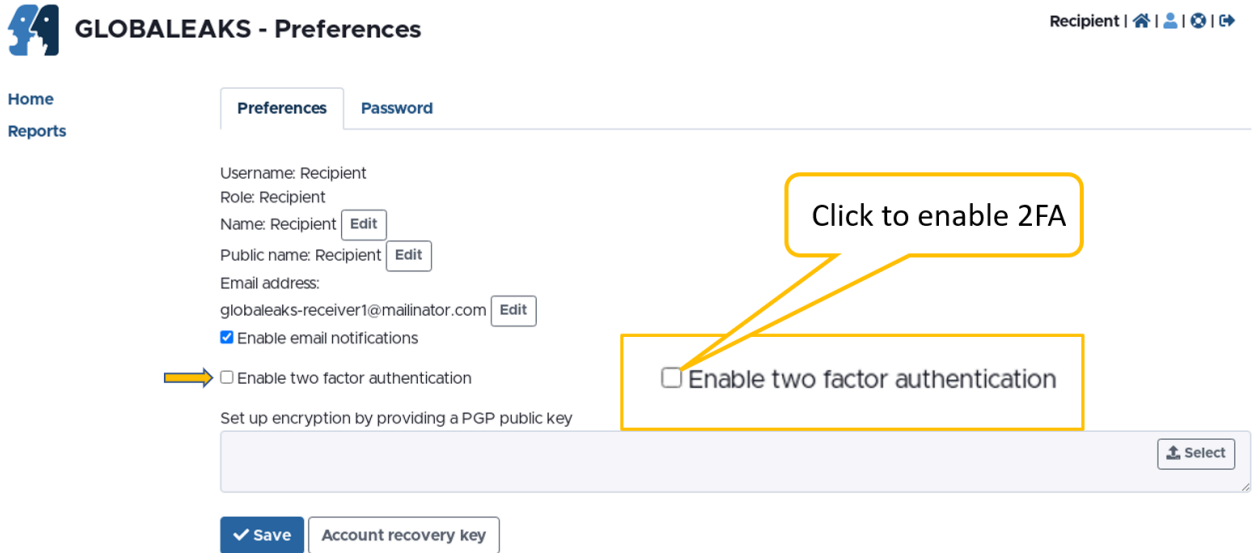
Q44C-4J2N-BQJS-JBBJ-CRQR-CTJC-VEST-BLDO-2SDB-D2WJ-JOHT-GHSD-Z5FA

Make a copy and store it in a safe place. It will be necessary if you lose your password to recover the access to your account without data loss.

U
R
N
P
Email address:
globaleaks-receiver1@mailinator.com
 Enable email notifications

ENABLE TWO-FACTOR-AUTHENTICATION (2FA)

After accessing your Account Recovery Key, you have to enable and configure **two factor authentication** (2FA) for extra security.



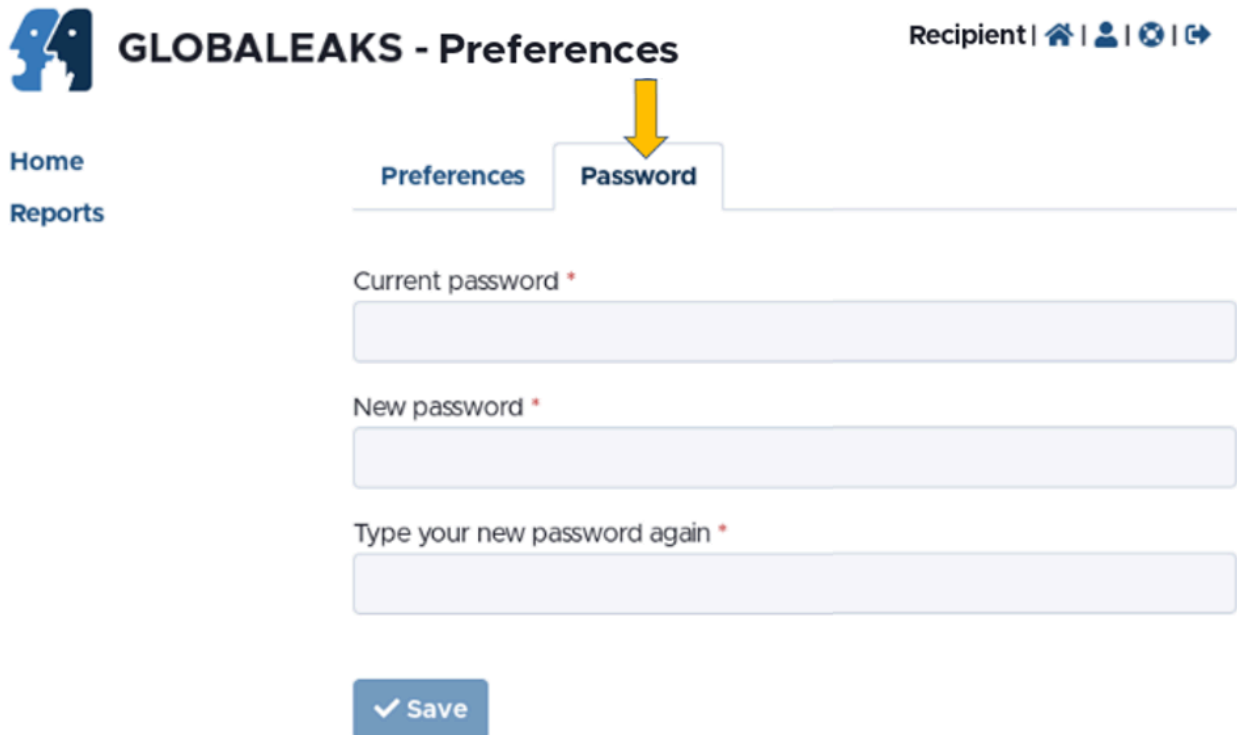
For this, you will also need to install an Authenticator App on your phone.³ Use the app to scan the code shown to set up a time-based code



³ You can download a commercial app like the Microsoft or the Google Authenticator Apps for Android phones on [Google Play](https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2) and for iOS phones on the [App Store](https://apps.apple.com/au/app/google-authenticator/id1450870919). Alternatively, you can download an opensource app like <https://freeotp.github.io/>.

CHANGE YOUR PASSWORD

You can change your password at any time by accessing the [Password](#) tab found on the [Preferences](#) page.



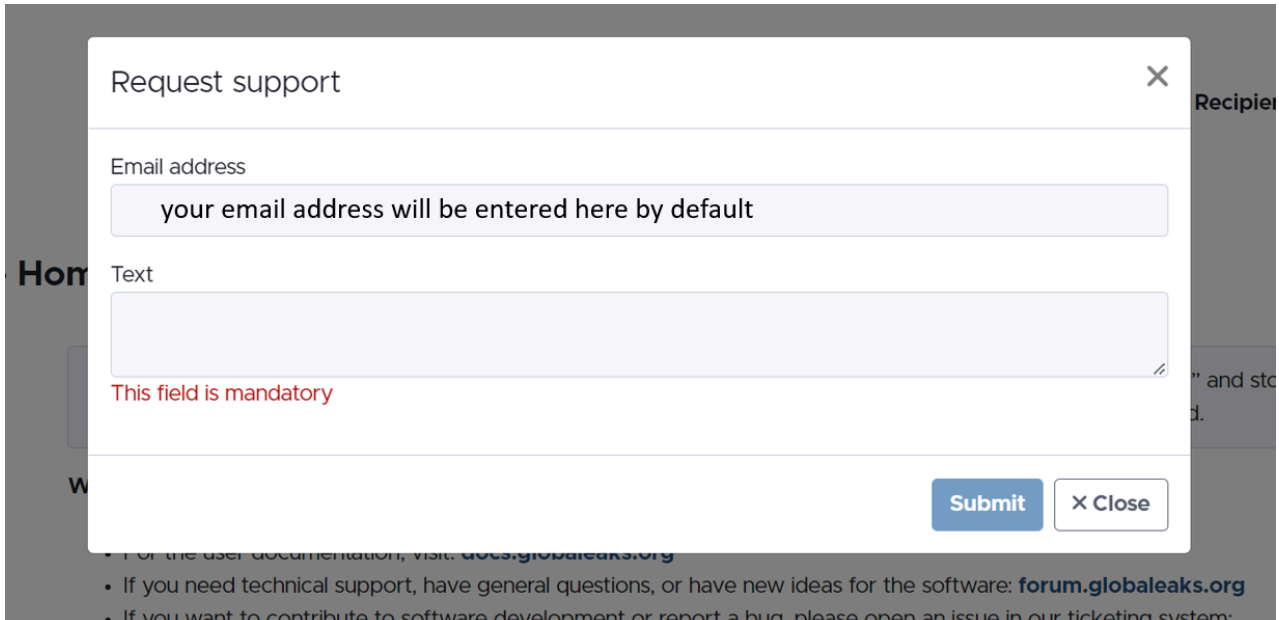
The screenshot shows the GLOBALEAKS - Preferences page. The page has a header with the GLOBALEAKS logo and the text "GLOBALEAKS - Preferences". In the top right corner, there is a user profile section labeled "Recipient" with icons for home, user, globe, and share. On the left side, there are navigation links for "Home" and "Reports". The main content area has two tabs: "Preferences" and "Password". A yellow arrow points to the "Password" tab, which is currently selected. Below the tabs, there are three input fields for password management: "Current password *", "New password *", and "Type your new password again *". At the bottom of the form is a blue button with a checkmark and the text "Save".

Please note that the system prompts users to change their password periodically for security purposes.⁴

⁴ Consider using an app like the [KeePassXC](#) to securely manage and store your passwords.

REQUEST SUPPORT

Whenever in doubt or in need of advice, you can ask for support from your platform Administrator; the relevant button can be found on the top right side of your screen:



The image shows a 'Request support' popup window. At the top left is the title 'Request support' and a close button 'X'. Below the title is an 'Email address' field with a light blue background and the placeholder text 'your email address will be entered here by default'. Underneath is a 'Text' field, also with a light blue background, which is currently empty. A red error message 'This field is mandatory' is positioned below the text field. At the bottom right of the popup are two buttons: a blue 'Submit' button and a white 'X Close' button. The background of the page is dimmed, showing parts of a navigation menu with 'Home', 'W', and 'Recipier' visible, and a list of links including 'docs.globaleaks.org', 'forum.globaleaks.org', and 'ticketing system'.

Use the popup to send a message, which the Administrator will receive via email:

II. ACCESSING A NEW REPORT

IMPORTANT NOTES BEFORE ACCESSING WHISTLEBLOWERS' REPORTS

Please be mindful that operating a system which allows you to communicate with whistleblowers may also attract viruses, malware, and other online threats. In case a virus attacks your computer, not only could it damage your computer, damage files, and result in data loss, but it could be transferred to your computer network and impact other computers and files.

Before accessing reports, please:

- Seek your Administrator's advice whenever there is doubt.
- Ensure that your computer's Antivirus software is enabled and updated. Use the Antivirus software to scan the files attached to reports.
- Encrypt your computer; if you are using Windows, ensure you have a Professional licence and enable the BitLocker feature. If you are using other operating systems, please follow your platform Administrator's advice on this topic. Hardware encryption can help prevent data breaches in case your computer is stolen or lost. Encrypting your computer's drive means that, to start up the PC, you need to use a password.
- Password-protect your computer by setting a strong password to secure your user account and data (this is an additional method of authentication, different from the encryption start-up password). Combine words that would not normally go together and replace some of the letters with numbers and similar-looking special characters to create a long and complicated password; store your password in a safe place without any indication of what it is; change your password regularly; consider using a password manager app to securely manage and store your passwords (e.g., [KeePassXC](https://keepassxc.org/))⁵

⁵ <https://keepassxc.org/>

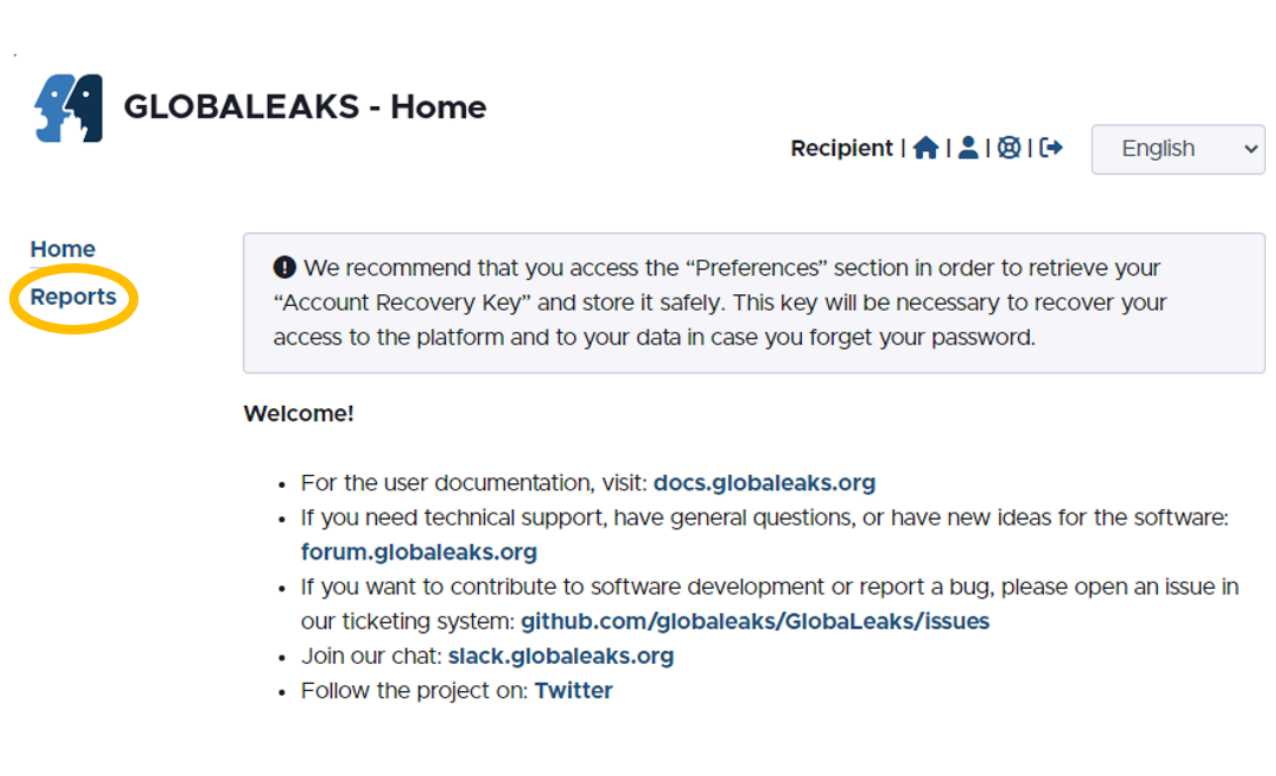
HOW TO ACCESS A NEW REPORT

When a whistleblower submits a report, you will receive an email notification. You can access the report:

- either by clicking the link provided in the email (you will be prompted to log into the system using your credentials, and you will be directed to the specific report page):



or by accessing the list of existing reports via the link [Reports](#) on the sidebar of your Homepage:



On the **Reports** page, you can access a report by clicking on it (as you would on a mailbox system). You can also search through the full reports list by entering keywords in the **Search bar**.

The screenshot shows the 'GLOBAL LEAKS - Reports' page. At the top left, there are navigation buttons: 'Back to Homepage', 'Select all', and 'Refresh Reports'. A search bar is located at the top center, with a callout 'Use keywords to look for Reports'. On the top right, there is a language dropdown set to 'English' and a 'Recipient' section with user icons. Below the navigation is a toolbar with a search bar and a refresh icon. The main content is a table of reports with columns: Status, Report date, Last update, Expiration date, and Preview. Callouts highlight that 'new Reports are in Bold' and that users can 'See when Reports are due to expire' and 'Preview for Attachments and Messages'.

★	#	Context	Label	Status	Report date	Last update	Expiration date	Preview
★	4	Default		New	25-02-2022 13:12	25-02-2022 13:12	27-05-2022 02:00	✓
★	3	Default		Opened	16-02-2022 16:40	16-02-2022 17:00	18-05-2022 02:00	✓ 1 1
★	2	Default	dirty money	Opened	16-02-2022 15:15	16-02-2022 15:15	18-05-2022 02:00	✓ 1
★	1	Default	corrupt transactions	Opened	16-02-2022 14:55	16-02-2022 14:55	18-05-2022 02:00	✓ 1

IMPORTANT NOTES BEFORE OPENING FILES ATTACHED BY WHISTLEBLOWERS

Opening attachments from unknown sources may carry an element of risk. Therefore, we urge you to follow the procedural safeguards your team has in place and be careful when opening files attached in reports.

Before opening files attached to reports, please:

- Firstly, read the whistleblower answers to the questionnaire carefully and assess the legitimacy of the report – and, therefore, assess the potential risk of opening the attached files. In case of doubt, make sure to reach out to your colleagues and/or team leader. Attachments in reports that do not seem plausible or legitimate could pose a threat; thus, the risks of opening them should be weighed in.
- When it comes to sharing information you received with colleagues, it is advisable not to forward the original attachment as received in the report, but rather to share a summary of the most relevant information. In case you need to share an entire attachment, make sure to check before sharing a potentially malicious file online and put your computer network at risk.
- On a relevant note, replicating documents by taking screenshots or copying text into a new document, printing and re-scanning it into your computer is considered a good practice to avoid sharing metadata; metadata is data hidden in data to characterize it. All digital files contain metadata about the who, what, when, where, why, and how about every aspect of the file and can expose information traceable to the source of the file.⁶

Did you know there is a way to remove hidden data and personal information from a document in Microsoft Word?

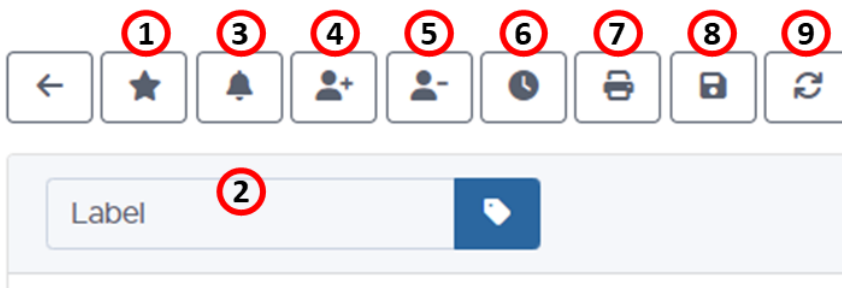
- 1. File > Info > Check for Issues > Inspect document**
- 2. Document Properties and Personal Information**
- 3. Remove All**

⁶ If you are comfortable using more advanced software tools, please find information about managing metadata here: <https://freedom.press/training/everything-you-wanted-know-about-media-metadata-were-afraid-ask/>

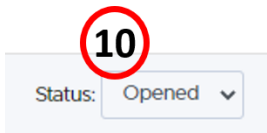
LIST OF POSSIBLE ACTIONS YOU COULD PERFORM ON A REPORT

(also see image below)

1. Mark a report as important in order to be able to filter reports by importance (star icon)
2. Label a report in order to be able to filter reports by labels
3. Silence email notifications regarding the update of a specific report
4. Grant access to another recipient for a specific report
5. Revoke the access from another recipient
6. Postpone the expiration date
7. Print the report
8. Download a copy of the report as an archive including file attachments
9. Refresh the page



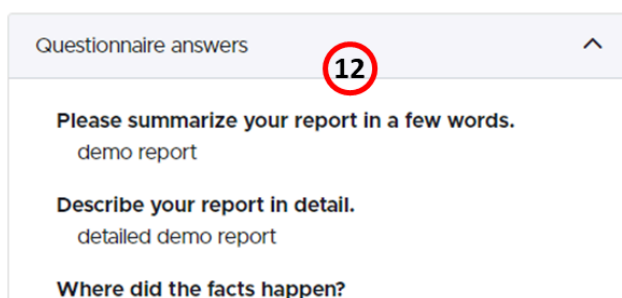
10. Change the status of a submission



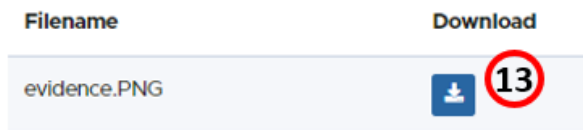
11. Access the whistleblower's identity (provided that they have agreed to share it)



12. Read the whistleblower's responses to the platform questionnaire



13. Download attachments



14. Leave comments to whistleblowers to ask for more information and/or send updates

15. Upload files to send to the whistleblower



16. Check whether the whistleblower has seen the recipient's comments

17. Check whether the whistleblower used the Tor browser to send the report



4 DEMO - Report

Recipient | | | |

1 3 4 5 6 7 8 9

Label Status: **10** Opened

#	Date	Last update	Expiration date	16	17 Tor	Status
3	16-02-2022 16:40	16-02-2022 17:00	18-05-2022 02:00	✓	×	Opened

Questionnaire answers **12**

Step 1: terms and conditions
privacy policy

Step 2: report
What sector does your concern relate to?
public

Identity

11

Attachments

Filename	Download	Upload date	Type	File size
evidence.PNG	13	16-02-2022 16:53	Image/png	28.19 KB

Files attached by recipients

evidence.PNG

From: Date: 16-02-2022 17:02 Size: 28.19 KB Number of downloads:

Upload a file: **15**

Description

Comments **14**

