Incognoto User Manual

Take control of your personal data with Incognoto, your secure incognito notes.

May 2018

Contents

Chapter 1

Introduction

1.1 Application Information

Corporations are constantly collecting your private, personal information. Many companies track your behavior and collect your data as part of their business model. User privacy continues to be a concern, but individuals do not have the right tools to take complete control of their data.

Welcome to Incognoto version 1.0. A free and open source application for Android in which you can securely store your personal notes, passwords, and task lists. This application is free of trackers, ads, and intrusive device permissions. Incognoto is a stand alone application that does not have access to your data; ensuring that your content will never be sold, traded, or shared. Take the first steps to regaining control of your privacy by encrypting your notes in a single file for exporting and easily storing backups of your data locally or on any cloud storage. Incognoto uses 256-bit encryption and offers the option of using a YubiKey for fast and secure authentication. We cannot, nor can your cloud storage provider or any other application installed on your device access or view the contents of your notes.

1.2 Terms of Service

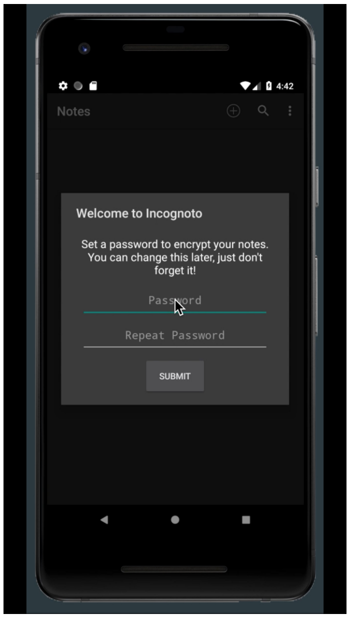
These terms of service govern your use of Incognoto, its website and services. Unless required by law or expressly agreed to in documented communication, this software is distributed under Public License and is distributed on an ”AS IS” basis, without warranties or conditions or guarantees, either express or implied. In no event shall the authors or copyright holders be liable for any claim, damages or other liability, whether in an action or contract, arising from, out of, or in connection with the software or the use of other dealings in the software. See the GNU General Public License V2.0 for the specific language governing permissions and limitations (https://www.gnu.org/licenses/old-licenses/gpl-2.0.en.html). By using Incognoto you agree to adhere to these terms and conditions.

Chapter 2

Getting Started

2.1 Creating a Password

In order to use Incognoto you must first create a password. You will be asked to retype your password in order to verify your input and after selecting enter you will receive a message at the bottom of the screen confirming that your password has been saved. You will have an opportunity to change this password later while logged into the application.



Welcome to Incognoto

Set a password to encrypt your notes. You can change this later, just don't forget it!

Figure 2.1: Password Prompt

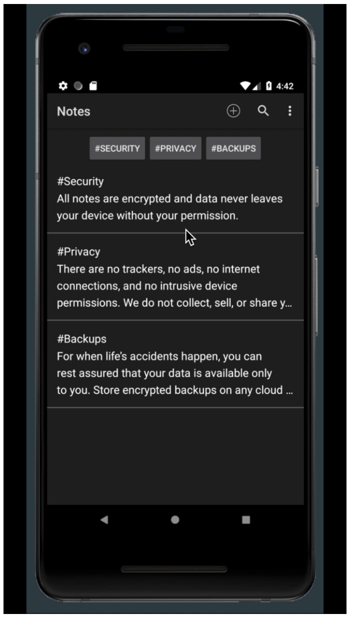
2.2 Default Notes

Please read the default display notes in order to familiarize yourself with the outline of the privacy and security policy and the secure storage feature.

- **Security**
  All notes are encrypted and data never leaves your device without your permission.

- **Privacy**
  There are no trackers, no ads, no Internet connections, and no intrusive device permissions. We do not collect, sell, or share your information since Incognoto is entirely free and open source.

- **Backups**
  For when life's accidents happen, you can rest assured that your data is available only to you. Store encrypted backups on any cloud while keeping your data locked behind your password.



#Security
All notes are encrypted and data never leaves your device without your permission.

#Privacy
There are no trackers, no ads, no internet connections, and no intrusive device permissions. We do not collect, sell, or share y...

#Backups
For when life's accidents happen, you can rest assured that your data is available only to you. Store encrypted backups on any cloud ...

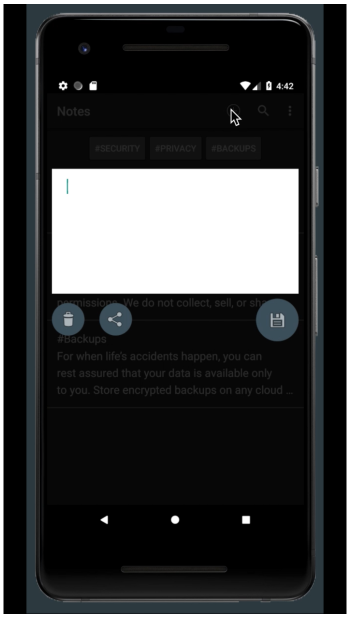
Figure 2.2: Default Notes

Chapter 3

Note Management

3.1 Create a Note

From the home screen within the Incognoto application where all currently saved notes are visible tap the addition sign surrounded by a circle at the top right of the screen and enter your content into the new note. Add a hashtag anywhere in the note to add a label for referencing and searching. The first three lines of the note will be visible from the home page of the application. Once you have finished adding content tap the save button on the lower right of the note. The note will save and close so that you can now view it from the home screen of the application.



permissions. We do not collect, sell, or sha

#Backups
For when life's accidents happen, you can rest assured that your data is available only to you. Store encrypted backups on any cloud ...

Figure 3.1: New Note

3.2 Edit a Note

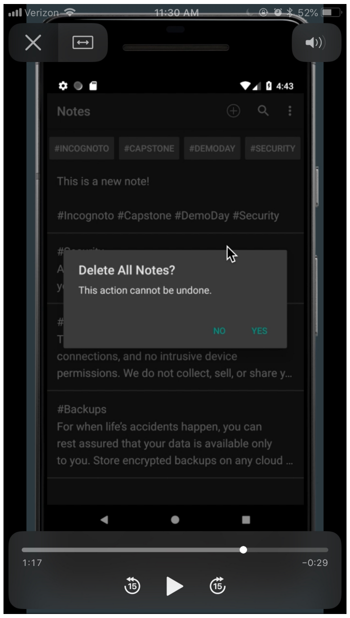
From the home screen within the Incognoto application tap the note that is to be edited, highlight or backspace over the existing text and type or paste new content. Click the save icon on the lower right of the note to save changes to the note. If you want to discard changes to the note click the the trash can icon and select no when asked if you want to delete the note.

3.3 Delete a Note

From the home screen within the Incognoto application tap the note that is to be deleted and select the trash can icon on the far bottom left of the note. When prompted ”Delete This Note? This action cannot be undone” select yes. Your note and its associated data and tag will be deleted and will no appear on the home screen or in search results.

3.4 Delete all Notes

From the home screen within the Incognoto application tap the menu icon at the far upper right of the screen. From the listed choices select Delete All. When prompted ”Delete All Notes? This action cannot be undone” select yes. All of your notes and their associated data and tags will be deleted and will no appear on the home screen or in search results.



This is a new note!

#Incognoto #Capstone #DemoDay #Security

Delete All Notes?

This action cannot be undone.

connections, and no intrusive device permissions. We do not collect, sell, or share y...

#Backups
For when life’s accidents happen, you can rest assured that your data is available only to you. Store encrypted backups on any cloud ...

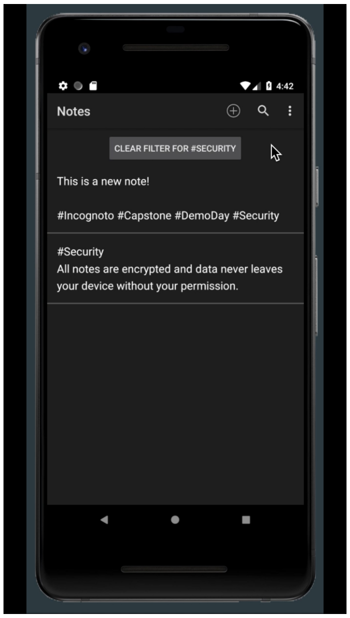
Figure 3.2: Delete all Notes

Chapter 4

Search for a Note

4.1 Search by Tag

From the home screen of the application all hashtags are visible at the top of the of the saved notes. Tap one of these tags to filter and view all currently saved notes that have been assigned this hashtag. The notes with the selected tag will be displayed chronologically from newest to oldest and you can select to view anyone of these filtered notes by tapping on it. After selecting the note from the list you can edit, delete, and import and export its content.



This is a new note!

#Incognoto #Capstone #DemoDay #Security

#Security
All notes are encrypted and data never leaves your device without your permission.

Figure 4.1: Search by Tag

4.2 Clear Search by Tag

Notes can have more than one hashtag so it may be necessary to search multiple tags to find the content that you are searching for. To clear the results of the current search select ”Clear Filter For.” This will remove the currently displayed notes and return you to the home screen of the application where all saved notes are visible. From this page you can now select a new hashtag to search by.

4.3 Search by Phrase

To search for specific notes using a phrase select the magnifying glass at the upper right of the application screen and type into the search bar a phrase or keyword. All notes containing that keyword or phrase will appear chronologically with the newest notes first.

4.4 Advanced Search Operations

4.4.1 And

In search phrases, enter a plus sign and another phrase after it to search for notes containing both the original phrase and the second phrase.

4.4.2 Or

In search phrases, enter a pipe and another phrase after it to search for notes containing either the original phrase or the second phrase.

4.4.3 Not

In search phrases, enter a tilde and another phrase after it to omit notes containing that phrase from the current search.

4.4.4 Compounding Operations

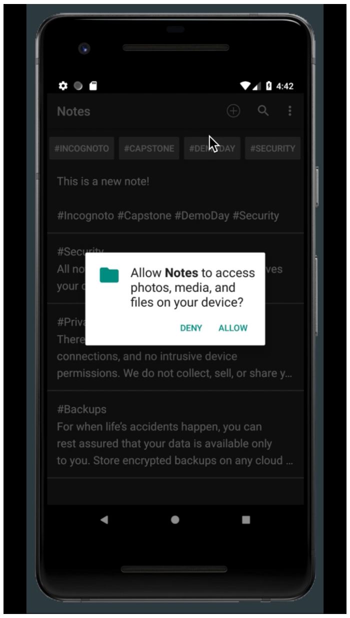
To use multiple of these operations in a single search, enter them one at a time. The search will conduct these operations from left to right.

Chapter 5

Content Management

5.1 Importing

In order to import a file you must have a file manager installed on your device.



This is a new note!

#Incognoto #Capstone #DemoDay #Security

#Secu
All no ves
your

Allow **Notes** to access photos, media, and files on your device?

#Priva
There
connections, and no intrusive device
permissions. We do not collect, sell, or share y…

#Backups
For when life's accidents happen, you can
rest assured that your data is available only
to you. Store encrypted backups on any cloud …

Figure 5.1: Application Permissions

5.1.1 Local Storage

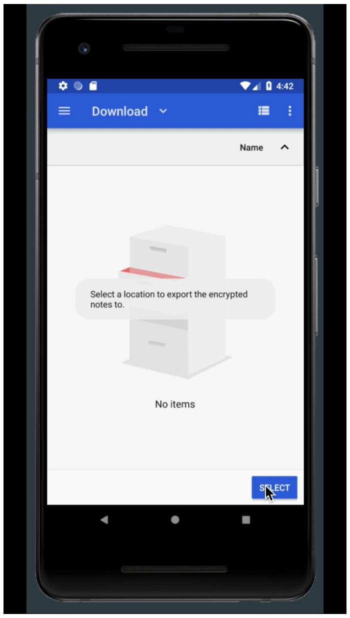
To import a file from local storage tap the menu icon at the far upper right of the application screen and select ”Import” from the list of available options. The device will ask you to grant permission to Incognoto to allow it to access your files if you have not imported a file before. Select yes and then select from the files stored locally on your device the file that you want to import. A copy of the selected file will now be available within Incognoto and can be accessed from the home screen where all notes are displayed and can be searched.

5.1.2 Cloud Storage

To import a file from cloud storage tap the menu icon at the far upper right of the application screen and select ”Import” from the list of available options. The device will ask you to grant permission to Incognoto to allow it to access your files if you have not imported a file before. Select yes and then select your cloud storage location from the listed storage locations in your file manager. Select the file from those that you have stored in cloud storage that you want to import. A copy of the selected file will now be available within Incognoto and can be accessed from the home screen where all notes are displayed and can be searched.

5.2 Exporting

In order to export you must have a file manager and a file decryption tool installed on your device.



Select a location to export the encrypted notes to.

Figure 5.2: Select File Export Location

5.2.1 Local Storage

To export a file to local storage tap the menu icon at the far upper right of the application screen and select ”Backup” from the list of available options. The device will ask you to grant permission to Incognoto to allow it to access your files if you have not exported a file before. Select yes and select the local location that you want to save the encrypted backup to. A single encrypted file will now be saved to your selected location.

5.2.2 Cloud Storage

To export a file to cloud storage tap the menu icon at the far upper right of the application screen and select ”Backup” from the list of available options. The device will ask you to grant permission to Incognoto to allow it to access your files if you have not exported a file before. Select yes and select the cloud storage location that you want to save the encrypted backup to. A single encrypted file will now be saved to your selected cloud storage location.

5.3 Sharing a Note

To share a unencrypted copy of a note tap the note that you want to share and select the share content button located at the lower left side of the note next to the delete button. A menu will appear of all available locations and methods where the content can be shared. Select your desired location to send the note to. You can now access the contents of the shared note from the selected application. The note will not contain information that identifies it as having been shared by Incognoto.

Chapter 6

Setting Up Advanced Authentication

6.1 Overview of YubiKey

The YubiKey is a hardware authentication device manufactured by Yubico that supports one-time passwords, public key encryption and authentication, and the Universal 2nd Factor (U2F) protocol. It allows a user to securely log into their accounts by emitting one-time passwords or using a FIDO-based public/private key pair generated by the device. YubiKey also allows for storing static passwords for use at sites and with applications that do not support one-time passwords. YubiKey strengthens the security of your Incognoto application by allowing you to create and use a very strong static password for encryption.

6.2 YubiKey Usage Instructions

Incognoto supports the use of YubiKey NEO as an authentication method. The YubiKey NEO contains a secure element (SE) that is accessible over both UBS and NFC. The SE offers a JavaCard 3.0/JCOP 2.4.2-compatible execution environment, an ISO14443A NFC interface, Mifare Classic emulation and an NDEF applet for interaction with Yubikey functionality.

Using a YubiKey NEO to unlock Incognoto requires that your device can authenticate using an NFC tag. This functionality is not supported by stock Android but is generally implemented in proprietary versions of the software. You may need to install and configure a RemoteAuthenticator application. Once installed, the application needs to be initialized with the same key and account name as the OATH applet on the YubiKey Neo.

Ensure that NFC is enabled before beginning configuration. To begin configuration for authentication of your Android device using the YubiKey NEO open the Android settings to the Location and Security screen, and configure your lock screen to be Secured with password. When asked to type it in, plug in the Yubikey with adapter, touch the disc, and the pre-configured static password spits out into the password field that is currently in focus on the device. Android has a limit of 17 characters for its disk encryption and screen unlock password so you will want to configure your static password with this in mind before beginning the configuration process. Once the YubiKey NEO has been configured to your Android device you can follow the same step to set up and store a static password specifically for Incognoto authentication.

Chapter 7

Security Features

7.1 AES-256

Incognoto implements AES-256 for encryption of your data. The security of this algorithm has been tested over many years of use in hundreds of different applications and ensures that your content will remain secure.

7.2 Screenshot Blocking

Screenshot blocking is a default security feature of Incognoto that disables the ability of your phone to take screen grabs of the content of the application. Should an unauthorized user gain access to an active session of Incognoto on your device they will be unable to take screenshots of your content. This security feature cannot be disabled within the application.

7.3 Blocking Application Screen Content

When switching between applications Incognoto will automatically hide the screen content with a plain gray screen. A header will still be available at the top of the application identifying it as Incognoto, but the current activity will be hidden and will not be viewable until the application is actively open. This default security feature cannot be disabled within the application.

7.4 Secure Storage

Incognoto offers users the ability to store your data in a single encrypted file locally or with any cloud storage provider. 256-bit encryption is a data/file encryption technique that uses a 256-bit key to encrypt and decrypt data or files and is used in most modern encryption algorithms, protocols and technologies. This affords you the ability to securely backup your content which ensures that you will always have access to your data without ever having to compromise the security of your application or system.

7.5 Small Application Size

With an a total application size of approximately 400kB Incognoto presents a small attack surface. This is accomplished by using only native libraries, a NoSQL database, and not using APIs. A small application ensures transparency in that it is easy to review the source code, should you be interested in doing so, and allows you to verify for yourself that Incognoto is not using any third party trackers, adds, and does not require intrusive device permissions.

A small application size means this application can be used on any device running Android 6 or later. Creating an application that is inclusive in terms of allowing older devices to be able to use it is one of the design features that Incognoto hopes will increase the usability for users of varying technical skill levels.

7.6 Responsible Disclosure

If you encounter a bug or a security vulnerability while using or researching Incognoto we ask that you kindly report it at https://github.com/Incognoto/incognoto.

7.7 Further Reading

Even the best security measures can fail if they are not used in combination with good security minded habits. Because there are not any limitations on password requirements you have the power to make the best possible password for keeping your information secure. This means when creating your password it is important to not make a weak password or reuse an existing password that you use for authentication for another application. The use of a password manager of a YubiKey can help ensure that you create and use the strongest possible password.

When you are finished using the application you should always close it. This will require you to reenter your password to decrypt the application upon restart and will prevent any unauthorized users from accessing your content.

Be mindful of the source that you import content from and only import from a known and trusted source. This ensures the vulnerability protection and security of not only your application but your entire system.

For further information regarding Incognoto's security features and policies refer to our Security Policy.

Chapter 8

Help

8.1 Security Questions

8.1.1 Forgotten Password

”I have forgotten my password. How can I reset it so I can decrypt my data?”

If you forget or lose access to your password for Incognoto it is not possible to reset your password without the application already being decrypted and active. As a security measure you must decrypt your application before you can access security features so your data is now unaccessible until a time that you remember or again have access to your password.

8.1.2 Screen Block

”I want to be able to view my notes when I am viewing all open applications currently open on my device. How do I disable the feature blocking application screen content when switching between applications?”

Blocking application content when switching between application is a default security feature of Incognoto and therefore cannot be disabled.

8.1.3 Screenshot Protection

”I want to be able to take screenshots of my notes while the application is open. How do I disable screenshot protection?”

Screenshot blocking is a default security feature of Incognoto and therefore cannot be disabled.

8.1.4 YubiKey

”I have lost the YubiKey that contains the password for my Incognoto data, can I still access my content?”

If you lose your registered YubiKey you can still manually enter in your password, copy and paste the password in from a password manager, or use an alternate YubiKey that has the same static password saved. If you lose access to your YubiKey that does not mean that you have lost access to your data.

8.2 Note Questions

8.2.1 Deleted Notes

”I accidentally deleted notes that contained data that I now need to access. Is there a way to recover them?”

If you have backed up you notes to local or cloud storage, then yes, simply access that backup, import it into Incognoto and your lost notes will be restored.

If you have not previously backed up your data that included the deleted notes, then no, they can not longer be accessed or restored.

8.2.2 Copying Notes

”Can I share more than one note at a time?”

At this time no, you can only share one note at a time. You will need to repeat the steps for sharing a note to share more than one.

Chapter 9

Glossary

9.1 Terms to Know

- **AES-256**
  The advanced encryption standard. An algorithm used for encryption.
- **Cloud Storage**
  Saving content to remote storage servers.
- **Exporting**
  To send data from one program to another.
- **File Manager**
  A program that provides a user interface to manage files and folders.
- **Hashtag**
  A word of phrase preceded by the pound symbol that is used to categorize content and track topics.
- **Importing**
  To receive data into one program from another.
- **Local Storage**
  Saving content directly to a device.
- **YubiKey**
  A hardware authentication device manufactured that supports public key encryption and authentication.