Sufyaan's Website

sufyaan.me/secure

Use Secure Messaging

Posted on: **23 January 2024**

Category: **Software** & **Technology**

In an era of uncomfortably intrusive tracking, the requirement for secure messaging has become crucial. With companies like Meta and Google intruding our privacy on a daily basis, we must take a stand, especially with the messaging applications, perhaps the most sensitive piece of software that people use. In this article, I will explain why it is urgent for you to take the stand by using secure messaging and explain how to get started.

Privacy: An Ignored Factor

Privacy is incredibly important in this modern day and age. This is why I will only speak about messaging software that is **both private and secure.** When choosing software, privacy and security should have equal importance.

Why?

Why would one use secure messaging if they have nothing to hide?

Protecting Your Privacy: Your privacy is incredibly important. However, it is ignored by most people, citing that they have nothing to hide. Everyone has something to hide, whether that be related to their money, reputation or even personal issues. Imagine your reaction if your current messages in their entirety got leaked, allowing anyone to read and go through them. You would be uncomfortable and also fear people taking advantage of your private messages. It is for this reason that it is important to safeguard your most personal conversations.

Avoiding Cyber Threats: Secure messaging uses end-to-end encryption. However, it is not wise to completely trust when companies advertise end-to-end encryption. It depends mostly on the algorithm that they use. For example, the Signal protocol is open-source and fully available to the public. This allows people to view and even contribute to improving its overall effectiveness. However, WhatsApp's encryption is proprietary. No one knows what encryption algorithm WhatsApp is running on their servers which makes it impossible to determine if it is secure. All in all, you should do your own research before proceeding.

Protecting Metadata: Your metadata is crucial to protecting your conversations. It can give context to your messages. Protecting your metadata helps mask your messages and protects it from being tampered.

Getting Started

I will be showcasing how to download and use secure messaging apps. As aforementioned, I will only show apps that are **both secure and private.**

1. Choose a secure app: Firstly, download one of the following:

1. Signal - It is free, open-source and is a great alternative for WhatsApp
2. Session - It is incredibly private. You do not get a phone number and have to backup a seed phrase, making it complicated for most users.
3. Threema - Threema is a **paid** option but also easy to use.

Next, open your app and set it up. Keep only the bare minimum data about you. For my name, I keep a dash (-) and no profile picture.

2. Enable two-factor authentication: Now, enable two-factor authentication if available. This allows you to prevent others from registering using your credentials without your consent.

3. Keep updating: Regularly check for updates. If an app has an update, update it. This prevents security and privacy breaches from occurring.

4. Use disappearing messages: Keep disappearing messages on by default. This ensures that sensitive messages are deleted within a period of time. For extremely sensitive chats, consider visiting the person you want to talk to physically. If that is not an option, turn on disappearing messages and set a time limit for 5 minutes and chat with them, so that the messages disappear after 5 minutes.

5. Educate your contacts: If your contacts are still on other messaging apps, convince them to join secure messaging apps as well. This allows you to have a secure option even if your main chats are on the other app.

Conclusion

In conclusion, it is important to employ secure messaging. Signal, Session and Threema are all viable applications that one can use. If only a few of your contacts are on Signal, do not worry. Talk to them on Signal and the others on the app you talk with them on. Remember, privacy is a journey, not a destination.