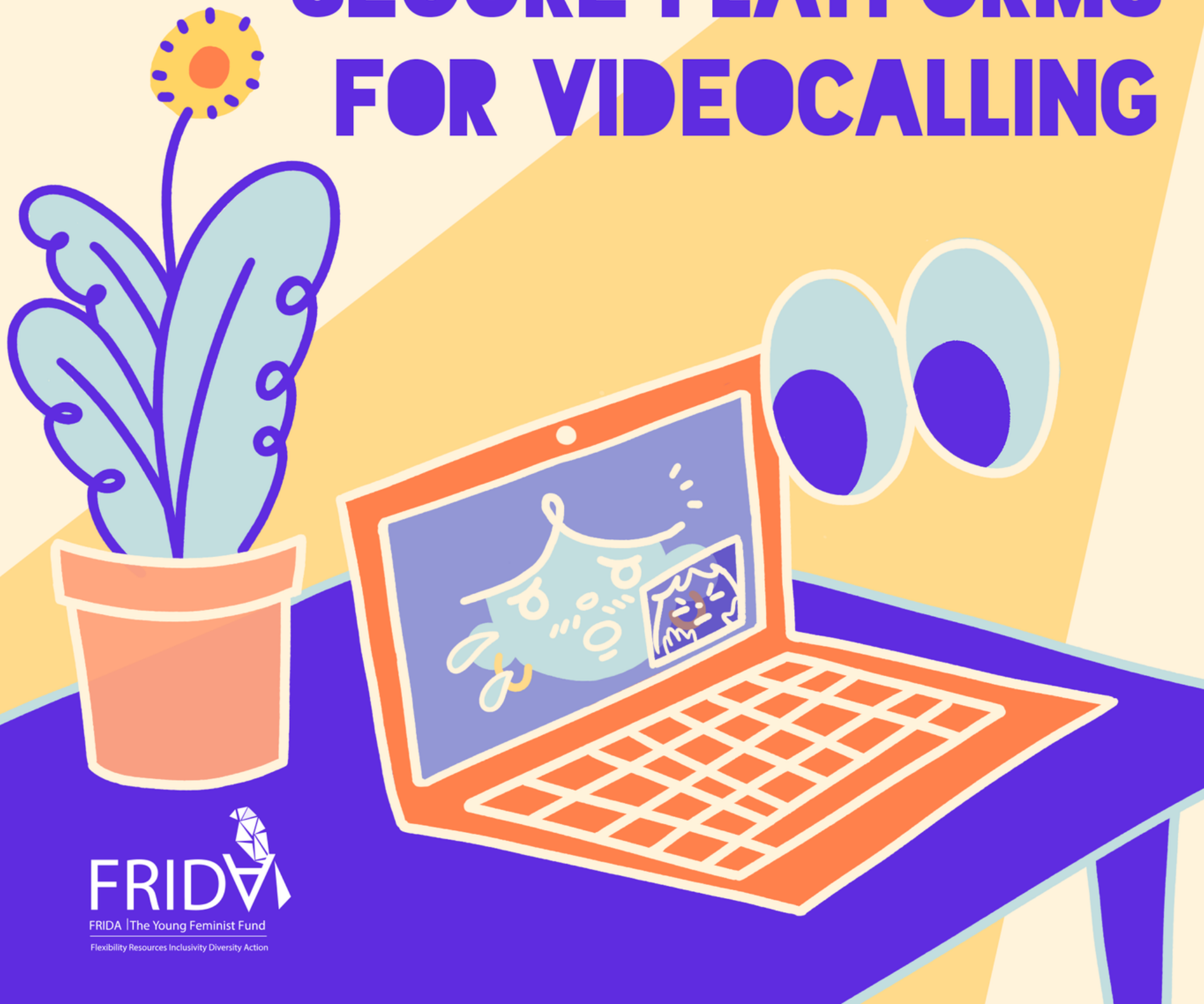
TALK WITH CONFIDENCE:

SECURE PLATFORMS FOR VIDEOCALLING



FRIDA

FRIDA | The Young Feminist Fund

Flexibility Resources Inclusivity Diversity Action

Due to the distancing measures that some countries have incorporated to reduce COVID-19 infections, we are experiencing **an increase in the use of video conferencing** applications to work, organize or connect with other people from a distance.

Unfortunately, sabotage and digital attacks are happening more often than before. An example are the **¨zoom bombings¨** which are usually **aggressive interruptions in Zoom video conferences of conservative and racist men** to meetings of feminist collectives or organizations that work in the defense of human rights.

With this context in mind, this guide takes up some video conferencing platforms that provide us with **the greatest possible security.** In addition to the brief characteristics that we present to you, it is important that you do some research about them and ask yourself the following questions: **What are their safety standards? Do they use encrypted messages for example? What information about us do they keep in files? In which country is our data stored? In which country are their servers located? What is their Data Privacy and Use policy?**

JITSI

You can share your screen, video, chat and voice. Depending on the server you use, you can stream or record the session.

Application based in USA

Free software and open source.

It can be used from your internet browser, either Firefox or Chrome. To use the application on your cell phone, you need to download the application.

It create rooms/links with long names, uses numbers and capital letters

Encryption in transit, but information is decrypted on servers. Because of this, it is recommended to use Jitsi on trusted servers like these or install it in your own server:

https://meet.greenhost.net
https://meet.mayfirst.org
https://talk.greenhost.net
https://framatalk.org/
https://calls.disroot.org

BIGBLUEBUTTON

To use this application
it is necessary to install
it on your own server,
or you can ask someone
you trust for an account;)

You can share screen, make
work rooms, use video, chat,
voice, and whiteboard.

It uses encryption in
transit, it means that it is
encrypted up to the server.

Free software
and open source

It is used through the browser
such as Firefox or Chrome

Remember that rooms/links
are created with long
names, use numbers
and capital letters

JAMI

You can use it without entering a phone or email, just by creating a user account. This gives us greater safety because you do not need to link your personal identity to the application.

Open source and free software

You receive or send messages only if you are online.

It has a distributed system. That is, there is no server that centralizes conversations or data.

End-to-end encryption for group video, audio and message calls.

Select a secure folder on your laptop/desktop to store your records.

WIRE

End-to-end encryption for calls

You can make voice and video calls, chats, make messages disappear, send photos and videos.

Open source

Video calls up to 4 people are free, for more people you must pay for the service.

Platform based in Switzerland

You can register just with an email address.

The application works for both cell phones and computers

WHEREBY

Company based in Norway

You can chat and use video, voice, share screen and record the call.

End-to-end encryption with a free account for meetings of up to 4 people.

It is used through an application or the internet browser

Meeting of more than 4 people is encrypted up to the server.

Two-step verification option is not supported.

The code is closed and that means that we cannot verify its operation.

IF YOU USE ZOOM, DO SO TAKING INTO ACCOUNT THESE SECURITY MEASURES:

1. Update Zoom constantly.

2. Use an access password for each call.

3. Use the option to manage participants that allows you to set the permissions that people will have during the session. For example, you can manage the way they share the screen, videos or links.

4. Avoid giving permission to record the session to all participants.

5. Remember! What happens in Zoom **is not private or anonymous.** Use measures to protect identities and avoid talking about controversial topics.

LAST MESSAGE:

In this time of pandemic, much of our lives and activism take place on digital platforms. **FRIDA | The Young Feminist Fund** knows the importance of having safe spaces to organize ourselves as young feminists, and for this reason we decided to bring out a series of contents focused on digital care practices and tools.
The content of this guide is based on the information developed by organizations that work in digital rights and by hackfeminist collectives.

We thank all of them for their efforts to make the internet and technologies safe spaces that can help us to continue conspiring together.

youngfeministfund.org
instagram.com/FRIDAFund
twitter.com/FRIDAFund
facebook.com/FRIDAFund

FRIDA
FRIDA |The Young Feminist Fund
Flexibility Resources Inclusivity Diversity Action

REFERENCES:

-Técnica Rudas, Tabla comparativa de plataformas para llamadas grupales: **www.tecnicasrudas.org**
- Front Line Defenders: **https://www.frontlinedefenders.org/en/resource-publication/guide-secure-group-chat-and-conferencing-tools**
- La Bekka, Vídeollamadas con Jitsi: la alternativa a las plataformas comerciales: **https://labekka.red/novedades/2020/04/21/jitsi.html**
Freedom of the Press Foundation, What we know about video conferencing with Whereby: **https://freedom.press/training/blog/what-we-know-whereby/**
- Sursiendo, ¿Qué está pasando con Jitsi?: **https://sursiendo.org/blog/2020/05/que-esta-pasando-con-jitsi/#more-10554**
- CheckPoint, Who's Zooming Who? Guidelines on How to use Zoom safely?: **https://blog.checkpoint.com/2020/03/26/whos-zooming-**