COVID-19 and digital security: How LGBTI activists can safely work online

Blog, Communications, Community Organising, Security

> While the opponents of LGBTI equality might also be overwhelmed with COVID-19 and focus their attention less on LGBTI groups right now, the digital footprints we leave today will still be around for a long time to come, which could make us more vulnerable after the crisis is over. So, now that most of our activities have moved online, how do we stay safe and secure? Here are tools and tips from the ILGA-Europe Programmes & Policy team.

As the coronavirus pandemic has taken us all by surprise, and we've all found ourselves isolating and working from our homes, the ways in which we communicate have drastically changed and we have to adapt quickly. Although many of us were already acclimatised to communicating digitally, moving 100 per cent of our daily work to the online sphere has been challenging in already complicated contexts.

For LGBTI activist organisiations, it is important to keep in mind that safety comes first. While our opponents might also be overwhelmed with Covid-19, the digital footprints we leave today will still be around for a long time to come. The following tips and tools on how your activist organisation and work can move its communication online are lead by the principle of online safety

Here's how to **quickly and safely reshape the work with your team** without losing time and resources.

1. Group Communication

For group chats, one-to-one video and audio quick calls, you can use various apps on your cell phone. The following apps facilitate group meetings and here are the safety elements you need to bear in mind:

App	Security	Features	What can be shared	Pro's and Con's
Signal	Encryption (end to end), password	Audio, videocalls, file transmission, group chats and calls	Sensitive info	Less used – safest so far!
Wire	Encryption (end to end), password	Audio, videocalls, file transmission, group chats and calls	Sensitive info	Less used, user friendly, easy
Whatsapp	Encryption (end to end), owned by Facebook	Audio, videocalls, file transmission, group chats and calls	General communication, nothing sensitive	Frequently used, you'll find most of your contact there
Viber	Encryption (end to end), password (PIN)	Audio, videocalls, file transmission, group chats and calls	General communication, nothing sensitive	Less used than whatsapp, might be an advantage currently
Telegram	Encryption, unclear	Audio, videocalls, file transmission, Channels (mass messaging)	General communication, nothing sensitive	Less used, but we're not entirely sure how secure it is

Remember that some of these apps are linked to your cellphone number. When you have sensitive conversations, you may want to be able to delete conversations for everyone in the app. Signal, WhatsApp, Viber allow you to do that, while Wire also allows you to write self-destructing messages.

You can find detailed information here on these and additional apps.

For longer conversations with your teams, it is probably easier to use apps that are available on your computer or tablet. Most of the following are also available on your phone, but generally harder to operate there.

Tool	Security	Features	What can be shared	Pro's and Con's
Zoom.us	Encryption (end to end), passwords can be set	Audio, videocalls, chat, file transmission, group chats and calls, screen sharing. Supports laptop and mobile use.	Webinars Meetings with no sensitive content	Zoom is extensively used by workplaces around the world, so the connection might not be perfect all the time. Needs, registration and software installation (both easy) and has limited free options. Can be used for large teams. Security concerns have been signaled.
Wire	Encryption (end to end), password	Audio, videocalls, chat, file transmission, group chats and calls	Sensitive info	Less used, user-friendly, easy
Microsoft Team Meeting	Encryption (end to end), passwords can be set	Audio, videocalls, chat, file transmission, group chats and calls, screen sharing	General communication, nothing sensitive	Frequently used
Meet.jit.si	Generates a unique link and the meeting can be password protected.	Audio, videocalls, chat, group chats and screen sharing. Laptop and mobile use.	General communication, including sensitive aspects	Less used than WhatsApp, so might be an advantage currently. Some connectivity issues might be experienced.

In case you plan video calls and sensitive aspects may or may not come into discussion, please follow some simple rules:

I. Always set a password to the meeting.

II. Avoid sharing a the link to the meeting in a public online space as anyone who has the link can join the meeting.

III. Ask participants to introduce themselves verbally, preferably with video (later you can mute and/or turn the cameras off).

IV. If you see suspicious participants joining (not responding to questions, sharing unsolicited content, etc.) close the meeting for everyone and start a new one.

For those using zoom, besides the above rules, there are some specific technical aspects that can improve the safety of your calls:

I. Change screensharing to “Host Only”.

II. Disable “Join Before Host”.

III. Disable “File Transfer” so there’s no digital virus sharing.

IV. Disable “Allow Removed Participants to Rejoin” so booted attendees can’t slip back in.

V. Also try to avoid using your personal meeting room for public meetings. If someone gets access to your personal meeting ID and the personal link, they could potentially then join any meeting in the room at any time.

Long, but as we say, better informed than hacked.

2. Project Management Tools

To work collaboratively with your teams on multiple projects with mixed requirements and deadlines, you could try one of these **project management tools**:

Slack — A virtual office which works well for prompt communication on various work projects with separate channels that can be encrypted or password protected.

Asana — Good for a growing team, it offers calendars, joint and individual task management, file sharing, workload indicator, etc. This is probably useful if your team is used to working online already, a bit harder to get used to quickly than Slack.

Trello — A good tool for planning and keeping track of steps in project implementation, good with deadlines and good for small teams!

Wrike — Similar to Asana, this is good for complex projects with long timelines, conditionality of tasks and timeframe.

Keep in mind that these tools are cloud-based. This means that they are quite secure unless at least one person has their password breached. **Two-factor authentication and regular changing of strong passwords are a must.**

The second consideration is that these tools are not free of charge, but this period is a good opportunity to explore their fee offerings. Then you can decide if you want to continue using some of them.

3. Collaborative and Cloud-storage Tools

If you plan to work together with your colleagues on documents, these collaborative work and cloud storage tools may be handy. We do not recommend Dropbox as it is not a safe tool to use for permanent storage. Remember always that safety comes first!

Google Drive — Well known and understood, Google Drive works well, but is not the safest option. If you have security concerns, consider two-factor authentication. Here's how to set it.

The Box — Similar to Google Drive and Dropbox, but considerably safer.

4. Password Changing

Changing passwords is a good safety tool, but constantly changing and saving them, especially with all the current anxiety, might be challenging. Here are some tools to generate and safely store your passwords:

1password.com — Features cloud-based database storage, meaning it is less likely that it will be hacked on your computer, and can be accessed around the world (if you have a good Internet connection).

Keypass.com — A software-based database of passwords. Can be used offline, but it will be stored on your laptop and/or smartphone.

You can find here more general tips on how to set your workspace at home, and security considerations in a report produced by Frontline Defenders here.