# Beautiful Rising: Security & Privacy Options

Outlined in our [statement of values](statement-of-values-for-beautiful-rising.md) is the Beautiful Rising team's commitment to security & privacy:

The tools that we use in our communication and collaboration with contributors will respect and enhance their privacy to the greatest extent possible. If we are required to use systems or networks that we believe to be inherently insecure, we commit to providing clear guidance to our collaborators on how to protect themselves, their identity, and their location while working with us.

If you are collaborating with us -- as a workshop participant, as a contributor, as an advisor, as an ally -- we encourage you to read the following security considerations:

## Web sites & services

During the course of your involvement with Beautiful Rising you may be occasionally pointed to documents on web sites or services that routinely collect personal information. For example, you might be asked to view and complete a survey online. In this situation, we encourage you to protect your privacy by taking the following steps *before* visiting the survey link:

* Logging out of any web sites or services that you may be currently signed-in to, e.g., Facebook, Google, etc.
* Using the private browser feature of your web browser. Each web browser is different, but this feature is typically called "Incognito" or "Private browsing." You can learn more about this feature by using the "Help" menu in your browser and searching for privacy.

Where possible, we will work to ensure that we do not circulate links that may inadvertently compromise your personal information. We will typically do this by directing you to web sites that do not require you to sign-in, and by relying on sites where we have a reasonable belief that information collection is limited.

## Mobile applications & services

Similarly, during the course of your involvement with the project, you may hear about new and interesting mobile applications. We encourage you to approach these mobile applications with common sense and some basic scrutiny. Here are some common scenarios to be aware of:

* Some mobile applications, a good example is the popular messaging application Viber, will request access to the contacts on your phone. You should be aware that many of these applications will send your contacts (sometimes insecurely) from your phone to another location. This could result in inadvertently providing your entire address book of contacts to another party.
* Many popular mobile applications claim to be "secure," when in fact they offer very little in the way of protection at all. This can be difficult to assess, so we recommend that you attempt to undertake some basic research before installing and trusting new mobile applications (we provide some specific recommendations of tools that we believe to be more secure below).

## Communicating with us

During the course of collaborating with us, we may ask you to submit written material. If you would like to take steps to help ensure that this material is not easily read by others, we encourage you [research your options](https://ssd.eff.org/en/index) or ask us for assistance. Beautiful Rising is not resourced to provide digital security training at this time, but each team member has been briefed to be able to provide you with straightforward options for communicating with them security.

If communicating with the Beautiful Rising project would put you at risk in any way, please refrain from doing so directly and explore alternative, possibly indirect ways to contact us.

### Email

Each member of the [Beautiful Rising team](https://github.com/BeautifulTrouble/Beautiful-Rising-Research/blob/master/the-team-and-contributors.md) has a published public PGP key. That key can be used to secure your communication with that person, reducing the risk of the message being read by another party. Securing your communication in this way does not remove the evidence that you've communicated with us.

If you are not familiar with, or already set-up to use PGP, please contact the team member you want to communicate with and ask for alternative ways to transmit information to them.

## Chat

Most members of the [Beautiful Rising team](https://github.com/BeautifulTrouble/Beautiful-Rising-Research/blob/master/the-team-and-contributors.md) have published their indentity on the serivce [Chat Secure](https://chatsecure.org/). Chat Secure is an "Encrypted Messenger for iOS and Android" that enables you to send short messages securely to members of our team.

We are also investigating the [Telegram](https://telegram.org/) messenger at this time. If you are using Telegram already, please let us know.

## Phone calls

We may also ask to speak with you on the phone, or you may find that a voice call is the easiest way to convey some information. Most members of the team are set-up to initiate and receive calls using the encrypted voice application called [Redphone](https://whispersystems.org/) on Android or [Signal](https://whispersystems.org/blog/signal/) on iOS. If you have the option of commnicating with one of these mobile applications, we recommend it -- keep in mind, however, that these applications require a wifi or data connection.

## Video meetings

To facilitate one-on-one or multi-party video conferences, we have set-up an instance of Jitsi Meet. It is an equivalent to Google Hangouts and similar systems. In the course of collaborating with us, we will provide you with access to this tool and will encourage you to use it over other potentially less-secure alternatives.

If you have a question about this document, please contact us (securely if possible) using one of the methods above. Failing that, you can send an e-mail to phillip AT beautifultrouble DOT org.