Our Guidelines may sometimes make your internet use more complicated, but with regards to online campaigning against racism and discrimination, always keep in mind that you are facing people committed to ideologies connected to all forms of violence and crimes. They are not gentlemen so being careful can never be paranoia.
YOUR ONLINE ACCOUNTS ARE PART OF YOUR PRIVACY AND PROPERTY

If you do not want to put them at risk, please read our simple tips.
For our mutual benefit, we list some of the most commonly made mistakes and share some technical advice about how to avoid them.

Imagine > You lost your phone with all those contacts not being backed up, or you lost your keys and someone finds them, and breaks into your home.
This happens in the virtual world when someone breaks into your email account and takes over your data and contacts.

Imagine > That after going to a demonstration, some nazis follow you back home and harass you.
This happens online when you post something on social media using your own name, and you are targeted by right-wing extremists.

Imagine > That you plan a private party in your backyard, and your worst enemies show up before it starts to trash it, and then harass your friends for coming, and even the police show up.
This can happen if you make your events and conferences completely open and let everybody know what are you doing.

Privacy

Make a clear distinction between your private life (and its presence on the internet) and your online activism. To effectively do so leave no personal traces behind:

• It’s clever to create a separate account and aliases for engaging and reacting on hate speech. Another effect of an alias is that nobody actually knows how many people are involved in maintaining that alias and who is doing precisely what. Choosing a good name can bring extra benefits.

• It is important to keep the information and people connected to your activity safe. This should be a primary concern which all team members understand and agree. Just one wrong email sent is enough to compromise it.

• It is important to consider that if someone is threatened, this can have the impact of scaring everybody - which can destroy all the effort you have already put in.

• If creating events on Facebook, keep other organisations protected too, hide the list of participants and do not publish the location. Be careful with media presence by asking journalists or photographers to register for the event beforehand - this gives you time to check if they are reliable or not.

• Address participants with the topic of privacy, explain it in detail or share this guide to make them understand the repercussions of not safeguarding your data.

Password

• Set a strong and different password for each service, otherwise, you will eventually get hacked.
• Change between cases, use numbers and special characters, at least 12 characters long.
• If you use one password across different accounts, the person that cracks it gains access everywhere.
• Take extra care with your email password – all password recovery links are sent there.
• Use password management software such as “1password” (Mac and Windows).

Communication

• Use accounts from activists for activists, such as riseup.net.
• Use GPG-Mail to encrypt mail communication.
• Use encrypted Jabber communication such as systemli.org.

Consider

• Use a proper and updated Anti-Virus software.
• If you use public computers use the virtual keyboard to enter your passwords, because public computers might have a key logger or other malware (malicious software) which will steal your login info.
• If you work with personal information, encrypt your hard drive. It might actually be illegal to store personal information unencrypted and you can risk your privacy and, in extreme cases, you can put your family, friends and colleagues in danger and you can even face legal consequences if they are leaked. To encrypt your hard disk use programs such as PGP Hole Disk, FileVault (MAC) or TrueCrypt (especially for encrypted data containers). You will always find guidelines and How to Dos on the website of the providers.
• If using free products like Facebook or Gmail, do not forget that sometimes you are the product - your behavioral data is being sold.

The action of extreme groups is always going to be extreme - ideological opinions are more emotional than reasonable and tend to be violent in nature.
If you do not want to put them at risk, please read our simple tips. For our mutual benefit, we list some of the most commonly made mistakes and share some technical advice about how to avoid them.

Imagine > You lost your phone with all those contacts not being backed up, or you lost your keys and someone finds them, and breaks into your home.

This happens in the virtual world when someone breaks into your email account and takes over your data and contacts.

Imagine > That after going to a demonstration, some nazis follow you back home and harass you.

This happens online when you post something on social media using your own name, and you are targeted by right-wing extremists.

Imagine > That you plan a private party in your backyard, and your worst enemies show up before it starts to trash it, and then harass your friends for coming, and even the police show up.

This can happen if you make your events and conferences completely open and let everybody know what are you doing.

Make a clear distinction between your private life (and its presence on the internet) and your (online) activism. To effectively do so leave no personal traces behind:

• It’s clever to create a separate account and aliases for engaging and reacting on hate speech. Another effect of an alias is that nobody actually knows how many people are involved in maintaining that alias and who is doing precisely what. Choosing a good name can bring extra benefits.

• It is important to keep the information and people connected to your activity safe. This should be a primary concern which all team members understand and agree. Just one wrong email sent is enough to compromise it.

• It is important to consider that if someone is threatened, this can have the impact of scaring everybody - which can destroy all the effort you have already put in.

• If creating events on Facebook, keep other organisations protected too, hide the list of participants and do not publish the location. Be careful with media presence by asking journalists or photographers to register for the event beforehand - this gives you time to check if they are reliable or not.

• Address participants with the topic of privacy, explain it in detail or share this guide to make them understand the repercussions of not safeguarding your data.

YOUR ONLINE ACCOUNTS ARE PART OF YOUR PRIVACY AND PROPERTY

Imagine > You lost your phone with all those contacts not being backed up, or you lost your keys and someone finds them, and breaks into your home.

This happens in the virtual world when someone breaks into your email account and takes over your data and contacts.

Imagine > That after going to a demonstration, some nazis follow you back home and harass you.

This happens online when you post something on social media using your own name, and you are targeted by right-wing extremists.

Imagine > That you plan a private party in your backyard, and your worst enemies show up before it starts to trash it, and then harass your friends for coming, and even the police show up.

This can happen if you make your events and conferences completely open and let everybody know what are you doing.

Privacy

Password

• Set a strong and different password for each service, otherwise, you will eventually get hacked.

• Change between cases, use numbers and special characters, at least 12 characters long.

• If you use one password across different accounts, the person that cracks it gains access everywhere.

• Take extra care with your email password – all password recovery links are sent there.

• Use password management software such as “1password” (Mac and Windows).

Communication

• Use accounts from activists for activists, such as riseup.net.

• Use GPG-Mail to encrypt mail communication.

• Use encrypted Jabber communication such as systemli.org.

Consider

• Use a proper and updated Anti-Virus software.

• If you use public computers use the virtual keyboard to enter your passwords, because public computers might have a key logger or other malware (malicious software) which will steal your login info.

• If you work with personal information, encrypt your hard drive. It might actually be illegal to store personal information unencrypted and you can risk your privacy and, in extreme cases, you can put your family, friends and colleagues in danger and you can even face legal consequences if they are leaked. To encrypt your hard disk use programs such as PGP Hole Disk, FileVault (MAC) or TrueCrypt (especially for encrypted data containers). You will always find guidelines and How to Dos on the website of the providers.

• If using free products like Facebook or Gmail, do not forget that sometimes you are the product - your behavioral data is being sold.

The action of extreme groups is always going to be extreme - ideological opinions are more emotional than reasonable and tend to be violent in nature.
Online Privacy for DUMMIES

by the (H)ACKTIVIST group*

Our Guidelines may sometimes make your internet use more complicated, but with regards to online campaigning against racism and discrimination, always keep in mind that you are facing people committed to ideologies connected to all forms of violence and crimes. They are not gentlemen so being careful can never be paranoia.