Don’t freeze, take action!

**What can you do to remain capable of acting and feel safe in a crisis situation?
And who takes on which tasks?**

Analogue security

What should you do?	What do you achieve and who is responsible?
Contact the local police station and request a security talk	Assessment of the hazardous situation by experts gives you control and the ability to act. **Security officer:** **In consultation with the observer of the attacks:**
Create legally compliant screenshots	Legally compliant screenshots document the progression of events and content permanently. This is important if you want to defend yourself legally, e.g. by filing a complaint with the police. **Community manager:**
Request address protection measure	You can find more information on this in the main section of the crisis plan. Please bear in mind that your address may be easily found out in other places and inform yourself and find out about protection options at an early stage. **Privacy guardian:**
Change routines and avoid being alone	Vary your daily routines to make it more difficult to find you and make sure you’re accompanied whenever possible, especially in public places. **Organise independently**
Change overnight accommodation at short notice	This allows you to create temporary protection and distance, as well as avoid analogue attacks in the event of acute threats. As a preventative measure, draw up a list of people who are close to you and with whom you can stay for a transitional period. **Organise independently**
Inform and sensitise your social environment	Make your social environment, e.g. family, friends and neighbours, aware of your situation and get emotional support if necessary. Sensitise your family members’ educational institutions to handle your personal data with particular care. **Inform your own neighbours independently.** **Office colleagues will be informed by the crisis coordinator:**
For events where you are invited as a guest: ask for a registration list, organise security staff and have house rules drawn up.	You get an overview of who is taking part in events and can prepare yourself and avert dangers if necessary. **Independently in consultation with the safeguard for netiquette:**
Consistently press criminal charges	The police will be informed about your situation through reports and can take security measures if necessary. In addition, unknown perpetrators can be identified through appropriate investigative measures and subsequently be brought to justice. **Security officer, if applicable, together with the person against whom the attacks are directed:**

Stand your ground

What should you do?	What do you achieve and who is responsible?
Publish a statement	You can present your own position clearly. **Press spokesperson:**
Get in touch with the local newspaper	You can disseminate your own position to different target groups and give the topic more credibility and importance. **Press spokesperson:**

Digital security

What should you do?	What do you achieve and who is responsible?
Change passwords	Strong passwords reduce the risk of hacking. A password manager can help you with this. This is a tool that generates secure passwords and stores them in a database for you. **Independently in consultation with the IT security officer:**
Set up two-factor authentication	Two-factor authentication impedes hacking attacks because you log in not just with your password, but with additional information. Authentication can be carried out using a code that is sent to you by email, for example. **Independently in consultation with the IT security officer:**
Search for and delete sensitive data on the internet	You protect your own privacy. **Privacy guardian:** (contact HateAid for support if necessary)
Involve external IT expertise if hacking is suspected	Hacking attacks can be dangerous on different levels. With external support, you can restore your own IT security and enhance the investigation of the incident. **IT security officer:**

Social media communication

What should you do?	What do you achieve and who is responsible?
Restrict the comment function on your own social media channels	You customise the comment settings in the comment function (e.g. ‘public’ → ‘private’, or a block list for specific terms). **Community manager:**
Deactivate social media accounts for a short time if necessary	Your account will not be deleted but made invisible for a period of time. If you want to use your account again after the crisis, you usually just have to log in again. This ends the deactivation. Deactivating the account temporarily can contribute to more relief and distancing. **Community manager:**
Report content on social media platforms	If legally compliant screenshots have already been created (see left), you can report the content. Ideally, reported content will be deleted by the platform. **Community manager:**
Block attackers on social media platforms	If you report the profiles of the attackers and block them for yourself, these people will not see what you publish in the future and will not be able to contact you. **Community manager:**
Consistently delete comments that contradict the netiquette	You create a safe place for people who want to interact respectfully with you and with others. **Community manager:** **In consultation with the safeguard for netiquette:**
Activate supporters	In this way, you can seek and activate support and solidarity on your channels, e.g. in the form of public encouragement from cooperation partners or counter-speech. **Crisis coordinator:**

HateAid