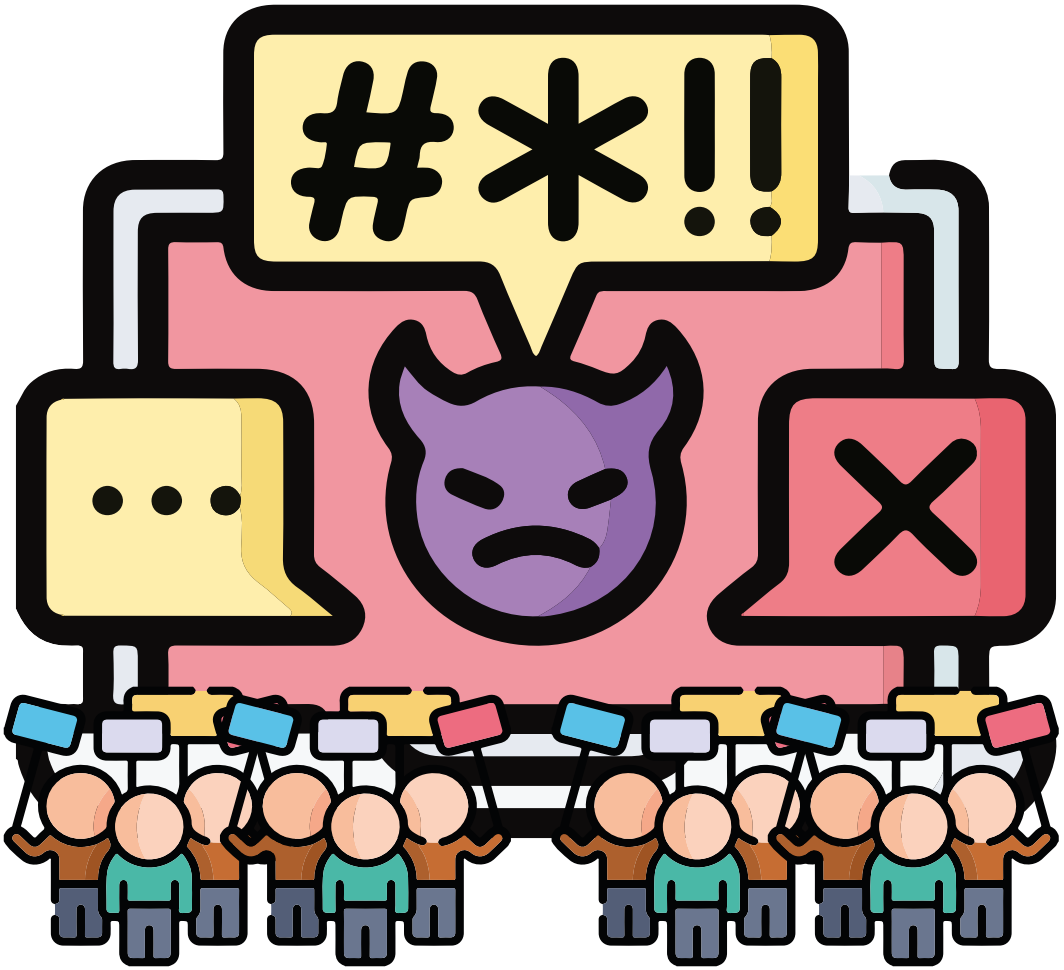
FAR-RIGHT ATTACKS ON ORGANISATIONS



HOPE NOT HATE

A SAFETY AND SECURITY GUIDE FROM HOPE NOT HATE

CONTENTS

INTRODUCTION

In the last few years, HOPE not hate has recorded numerous incidents of organisations being targeted by the far right online, in the media or even in person because they are supporting people that the far right do not deem worthy of support. As well as incidents which take place, threats of attacks also have a negative impact on organisations.

Organisations vulnerable to attack might be those who directly support people seeking asylum and refugees, or organisations who indirectly support these groups whilst also supporting the wider community. We also see organisations being attacked who work on LGBTQ+ rights, gender-based violence and child sexual exploitation.

The aim of this resource is to provide a basic overview of in-person and online personal security, as well as information and examples of how the far right think about violence. We also try to provide some practical tips, however personalised advice from security experts is advisable in addition to the content in this resource.

Security is highly contextual and constantly changing. This resource aims to provide basic information but does not constitute legal guidance, nor does it provide a one-size-fits-all solution. Please consult with relevant security, legal, or safeguarding experts for help and advice.

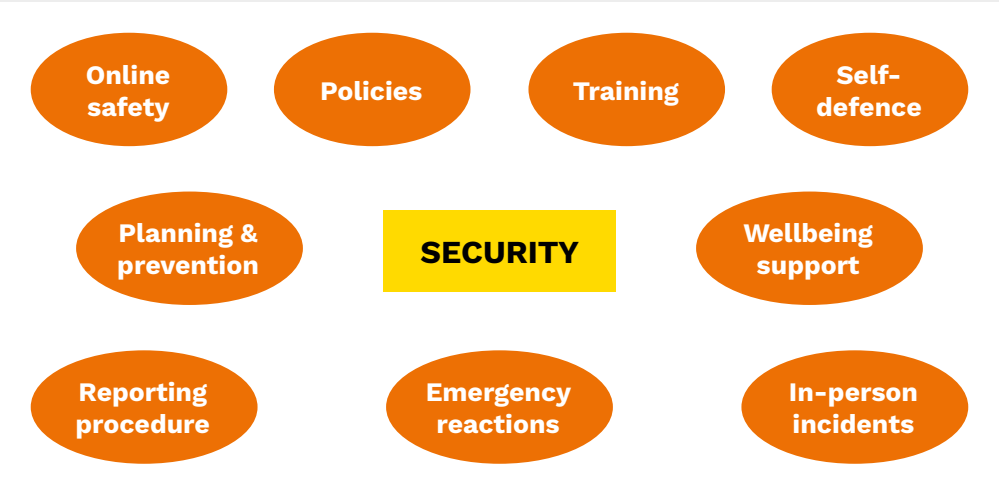
WHAT IS SECURITY?

In many respects, security is an abstract concept. It is an umbrella term and can comprise many things, but in this resource we address personal security which may be compromised as a result of the work or reputation of an organisation with which a person is affiliated.

Personal security consists mostly of situational awareness and risk assessment. It is also vital to understand that even if all of the advice in this resource is followed to the letter, situations occur which are uncontrollable and could not have been predicted.

You can try to keep yourself secure by making sure you have the most up to date knowledge of the tactics used by organisations and individuals who target you and your organisation. This will go some way to ensuring you use the correct counter measures to keep you as safe as possible.

There is no one solution to day-to-day security as the situation and threat changes depending on the location, media attention, organisation you work for and current public opinion.



THE SECURITY COMPROMISE

Lowest risk of negative interactions, but reduced stakeholder reach	Lowered risk, maintaining usability and engagement	Highest risk of negative interactions and compromise of safety

We use the term “security compromise” to describe the balance people need to find between being ultra-secure and relaxed around security. Different organisations will require a different balance, and this can change over time.

Organisations who need to be discoverable by service users, donors, volunteers or even just the public cannot afford to reduce their public visibility. However, risk of attack can be reduced through careful consideration of what and how information needs to be released.

A compromise also needs to be found psychologically between paranoia and laxity. Worrying about the threat of attack can have a toll on staff wellbeing and lead to burnout and stress. Hiding important information such as volunteering opportunities or event dates and times can compromise the efficacy of these efforts.

The aim of this resource is to provide people with as much information as possible so they can make informed decisions. You might not need to implement every recommendation in the resource. Safety is highly contextual, and some people will want or require a higher level of security than others due to their work, needs and previous experience.

THE FAR-RIGHT THREAT

The organised far right share hateful views about their own superiority; they also often demonise and target the same minority groups. For various reasons, including belief in white supremacy, Nazism, the Great Replacement conspiracy theory or Cultural Marxism, the far right have focused their attention on non-white people who choose to live in the UK. They view these people as a direct threat to a White British way of life.

THE ANTI-MIGRANT FAR RIGHT

Far-right groups speak explicitly about wanting to put a stop to all "illegal migration". The majority do not recognise the right to seek asylum. Beyond asylum, many do not approve of migration for finding work or family reunification.

Alongside this rejection of immigration, many far right groups talk about wanting a return to "British values". This is a thinly veiled way of saying that they are against the advancement of social justice, for example trans rights and racial equality. They rail against organisations they perceive to be "lefty", even those that do not work explicitly on migration, because they view them as aiding and advancing a system which has the wrong priorities. This could be foodbanks, legal advice services, housing services and more.

Many of those who follow the far right would prefer to see homelessness and veterans rights as a focus, but this is because they mistakenly see these as issues only for white British people, as opposed to being complex and intersectional. They often see organisations who help people of all backgrounds as favouring "foreigners" or "illegals" over indigenous

British people, and will use this as an excuse to abuse or attack these organisations.

A lot of far-right activity, both within the organised far right and in community groups online, centres around calls for violence and ideation of violence. The difficulty can be in assessing how likely it is that threats will spill out into real life: in some cases, far-right trolls are content to cause psychological damage from the comfort of their own homes. In other cases, people decide to act in person.

As well as a focus on migration and Islam and race more generally, the far right also focus their hatred on organisations who support the Jewish community, LGBTQ+ rights, child sexual exploitation and more.

EXAMPLES OF BEHAVIOURS

We see a range of behaviour from far-right actors who choose to attack organisations. This includes:

- **Online abuse.** Trolls might reply to everything an organisation posts with hateful comments, or go out of their way to create dedicated "investigations" or posts about the organisation. Sometimes this will be done by an individual, but at other times groups of people pile on together and encourage others to all post about the same organisation or person. This can take place on the organisation's social media or website, or the accounts of staff of the organisation.
- **Online activism.** This can take many forms, including creating a petition, clogging up an organisation's social media, mailbox or phone line with spam requests, or repeatedly reporting an organisation on social media in an attempt to get the account suspended. In any case, the aim is to intimidate and inconvenience the organisation.
- **"Citizen journalism" filming.** Far-right actors position themselves as journalists investigating an issue and film themselves walking up to or even entering organisational premises. They are often careful to stay within the limits of the law, and then post their created content to social media. The most prolific "citizen journalists" will post multiple times a week, encouraging followers to also visit the same locations.
- **Visits to organisations.** Similar to "citizen journalism", but without a camera, individuals might protest inside or outside the premises of an organisation in order to intimidate or draw attention to their hatred of the organisation.
- **Following staff.** Rarer and similar to the above, someone might identify someone as working for an organisation and choose to intimidate them by following or shouting at them. This can take place outside of the organisational premises.
- **Physical attacks.** Although rare, in some cases someone will attack someone representing an organisation because of their work.

CASE STUDY: ANDREW LEAK

In November 2022, Andrew Leak attacked a migrant centre in Dover with two or three petrol bombs, before killing himself. HOPE not hate subsequently discovered that Leak had a history of engaging with the far right online, including anti-migrant, transphobic and conspiracy theory content. He had even been retweeted by anti-migrant activist Amanda Smith (Yorkshire Rose) on a couple of occasions.

Leak's online activity suggested risk of an attack, but his level of engagement online was not drastically different to others. He frequently posted angry, violent and desperate messages – both his own and resharing from other people. With no dedicated resources or skills for monitoring social media, it is hard to see how organisations like the migrant centre attacked by Leak could have predicted the attack.

It is important to remember that security provision cannot always prevent attacks from happening. However, it can prevent attacks from causing damage and injury. In the case of Leak, no one could really have predicted he would act in that way. However, the effects of his actions could be mitigated by preventing access and "locking down" the site he attacked.

Alan Leggett or "Active Patriot", a migrant hunter.

ORGANISATIONAL SECURITY

RISK ASSESSMENTS

There are two types of risk assessment: organisational and personal.

1. **Organisational risk assessment**

   These fall into the risk assessments carried out under health and safety legislation and include many aspects including but not limited to: fire risk, trips and hazards and risks to the safety of any person employed, contracted, or visiting your place of employment. It also covers any off-site visits that you engage in in the line of your work.

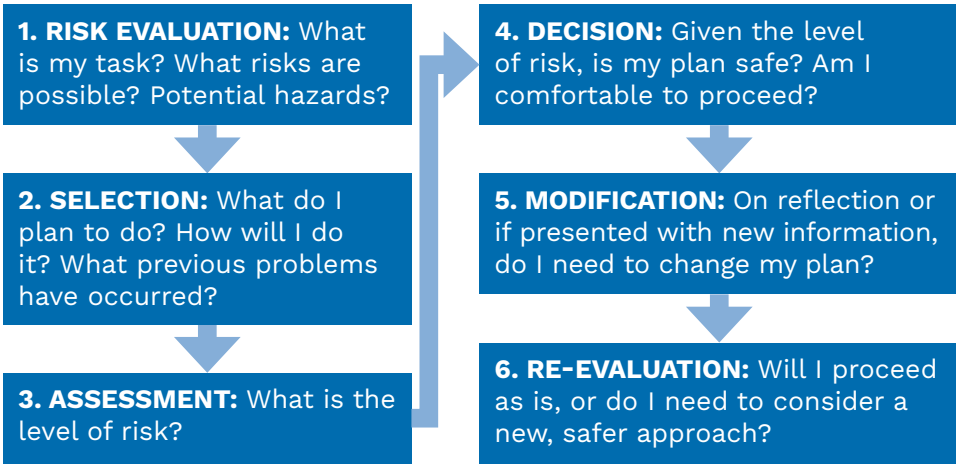
   These will be carried out by the organisation, not by staff (the health and safety lead or line managers will be responsible). Health and safety legislation and policies should be available to staff and need to be followed especially where staff are lone workers. Always refer to the lone worker policy of your organisation.

   The Health and Safety at Work Act 1974 (HASWA) lays down wide-ranging duties on employers. Employers must protect the 'health, safety and welfare' at work of all their employees, as well as others on their premises, including temps, casual workers, the self-employed, clients, visitors, and the general public.

2. Personal risk assessment.

Any risk assessment carried out by you is a personal risk assessment. This is based on a cycle of risk and can be based on a six-point plan. It is often called a **dynamic risk assessment** due to the changing nature of a situation.

THE SIX-POINT PLAN FOR PERSONAL RISK ASSESSMENT



Risk assessment is a cyclical approach to keeping safe and we do it every day, with every decision. This is simply a more formalised approach to one of our most common decision-making processes.

Being situationally aware is vital, this comes from knowing how a situation can change. This may be a change in a person's demeanour, tone of voice or their physical stance.

COMMUNICATING SECURITY

Keeping staff and volunteers informed about security is crucial, but a heavy handed approach can compromise wellbeing and morale.

The following tips might help you navigate conversations with staff sensitively:

- **Be clear about the risk level.** Are you addressing security now because you want to be prepared, or because there is existing risk? If there is an existing risk, what are non-negotiable measures that need to be taken, and what else could staff be made aware of?
- **Be clear about what the risk is.** What is it about the organisation's work that people are focusing on? Are volunteers also at risk? Note that the risk is unfortunately likely to be higher for Muslim, racialised or LGBTQ+ staff.
- **Offer regular updates and reassessments.** Following an announcement about security, offer updates of what the organisation is doing to address the situation and how you are monitoring risk. If you have recommended that staff take security precautions, let them know if they should continue to follow this advice.
- **Offer proactive support.** Acknowledge that security concerns have an effect on staff wellbeing and be clear about what the organisation can provide to assist with this, for example through group conversations, specialist support or training – see below.

PREPARING FOR SECURITY INCIDENTS

As well as managing a crisis situation itself, thought needs to be given to what happens next. Business continuity refers to a plan for how the organisation will work following an emergency. For example, will staff still come into the office? Will they work from home, or if they have to be on site what measures will be taken to provide security and reassurance?

Crisis management

- Up-to-date crisis management plan?
- Do you have a business continuity plan?
- Insurance?
- Media support to deal with enquiries if the incident is publicised?
- Timeline plan – how long will it take to return to business as usual?

First Aid training

- How many of your staff are first aid trained?
- Is a member of staff (or more) trained in trauma care?
- Do you have a trauma pack?
- Do non first aid trained staff know the basics?

PUBLIC ORDER OFFENCES

⚠ **Please seek legal advice before making claims about Public Order Offences.**

Some of the most likely offences you will face will be offences under the Public Order Act 1986. These are a range of offences which cover harassing, abusive or offensive language or conduct directed in public, or at individuals or threats made to an individual. Sections 5, 4A and 4 are the most common.

Section 5 is the lowest offence. This is using any language, or having/displaying signs or writing which can be viewed by a reasonable third party to be abusive or offensive in a public place. It cannot be committed by two or more parties in a private place.

Section 4A is committed when any abusive, offensive language causes alarm or distress to an individual.

Section 4 is committed when any abusive, offensive language causes fear of or provocation of violence.

POLICE

It is worth noting that criminal investigations will generally go via a local police service. While there are third party reporting mechanisms such as Crimestoppers, and specific centres for hate crime such as the Community Security Trust (CST) for antisemitic hate crime, Tell MAMA for anti-Muslim hate crime and Gallop for LGBTQ+ hate crime, it will be a specific police service who will ultimately be the investigating body if you decide to report an incident.

Not everyone is comfortable reporting to the police. You can report online via that police service's web address or, if hate related, report via any third-party reporting centre. These may be found in locations such as council offices, housing associations, etc.

ALTERNATIVES TO THE POLICE

Some organisations or groups of people will have difficult relationships with the police and other institutions, and for valid reasons. The presence of institutional racism and misogyny in the police is widely accepted. However, the police retain certain powers in society that are currently unique to them. For this reason, they are often the main authority in these matters. It can be worth trying to engage with community police liaisons and trying to gauge their willingness to be flexible and work with you, as well as their understanding of the contexts and experiences of asylum seekers.

Organisations that don't work with the police manage this by having strong relationships and links to other organisations who can share skills, especially to do with technology and security. Having local networks of similar organisations can be helpful in general, but in particular for organisations who might want extra help with keeping safe or sharing experiences of working in a traumatic or difficult environment. The organisation Vision Change Win has a toolkit explaining a community safety approach and how to embed it in organisations.

However, wherever possible the one form of engagement with the police that can be extremely helpful is reporting hate crimes. When there is no clear picture of what is playing out in communities, allocation of budget, time and skills spent on tackling far-right hatred cannot accurately reflect the situation. In some cases, allegations of crimes purported to have been perpetrated by vulnerable marginalised groups outnumber allegations made against far-right actors, even if this is not an accurate reflection of the situation.

REPORTING ISSUES INTERNALLY

Even if security issues do not meet the threshold of legal action, it can be useful to record information about incidents in case they form a wider pattern of activity or need to be referred to in the future. However, some organisations find themselves inundated with possible threats online, and keeping track of this would become a full time job that could be distressing for the person forced to do it.

Organisations should make an internal decision on content that meets the threshold worth storing – for example content that compromises staff safety, names specific staff members or contains sensitive content, or meets legal thresholds for action. A decision also needs to be made on how this information is stored and filed. It is hard to search through screenshots but copied messages are hard to prove if they are later deleted.

WELLBEING SUPPORT

Concerns about security can have a real toll on staff wellbeing. Even if no attack ever materialises or a situation does not appear to be grave, staff are

likely to experience ongoing paranoia and anxiety which can take its toll. This can particularly affect staff who are personally affected by the hate because of their ethnicity, religion, gender or sexuality.

Consider expanding your employee care packages to include trauma counselling or consider running courses on mental health in the workplace to equip staff with the tools to assist and recognise post emergency stress. Beyond specialist support, being able to share anxieties and fears about security within the organisation can be a helpful way of keeping people grounded.

Other forms of support include legal assistance and advice on communicating with the media, as well as advice on how to talk to family and friends about workplace risk.

IN-PERSON SECURITY

BUILDING SECURITY

It is impossible to give specific advice on building security as every location will have different requirements, but there is some general advice below.

OFFICE SECURITY

Shared offices can mean security is easier to compromise. Fostering good working relationships with your neighbours is vital. Security personnel can be expensive, and other forms may need to be considered such as video doorbells, which are low cost and don't need fully technical support. Some basic security advice should include a functioning CCTV system covering locations accessible to the public. This needs clear signage to be visible to the public visiting your location that CCTV is in use. Be aware of GDPR regulations surrounding CCTV. All forward facing staff must be aware of the policy and protocols regarding requirement to freedom of information under GDPR rulings.

ALARMS

Consider a personal alarm system for front facing staff, if this is not possible then a direct line with code words will be effective. Code phrases such as "Can you ask (name of someone not working at the organisation) to come to the front desk please" can be effective. Every individual will react differently to an emergency so consider drills to reinforce emergency

procedures such as evacuation and locking down as necessary. You might also wish to consider security and alarm procedures around post and parcels, including possible “white powder” incidents.

ENTRY AND EXIT

Coming in and out of the venue can be two vulnerable points, as this is where staff can be distracted and feel safe but are still often in public. These precautions are particularly important for lone workers, and you should consider including them in your lone worker policy. This policy should be regularly reviewed and risk assessed.

Be aware of tailgating. Even if your building is secure, be mindful of those who may gain access behind you or view entry codes. Challenge, identify and report any attempts to secure entry via this means.

DO:	DON’T
✔ Be aware of the emergency exits in the buildings you work in. ✔ Try to minimise the walk between your car and the entrance of the building you are visiting. ✔ Try to stay in well-lit areas and in plain sight. ✔ Text a colleague or friend once you leave with an ETA of when you might arrive, and then update on arrival.	✘ Have unnecessary distractions such as phone calls or music when entering a building. ✘ Have documents/lanyards/ ID badges which show your organisation prominently on your public transport commute. ✘ Forget to text upon arrival – your colleague should follow procedure even if they think you have forgotten.

IN-PERSON EVENTS

Hosting events such as community conversations, drop-ins or talks can be an excellent way of engaging the community and spreading news of your organisation and its work. However, in some cases these events can be targeted by individuals who disagree with the premise and who might become a risk to the event. These cases are rare, and so it is important for you to assess the risk well in advance and decide which, if any, safety measures you need to take. Bear in mind that sometimes introducing safety measures means compromising on aspects of the event, so you will need to decide how to strike this balance.

- You should do a **risk assessment** of events considering the venue and who will be in attendance. It might be helpful to have a guest list of known attendees in advance of the event, or security on the door if the event is open to the public. If vulnerable people will be in attendance, you should consider informing them of the assessment.

- Consider your **event publicity**: does it need to be publicly advertised on social media or on your website, or could you reach your desired audience through closed groups or mailing lists? When will you disclose the location of the event to your audience?
- **Avoid live social media posts** – it may be safer to wait until after you and all other staff and volunteers have left the area, so your location will not be revealed.
- **Exit strategy** – When using a venue, check the room where you set up, and work out a plan for how you and attendees will be able to leave safely. Of course, most of the time this will not be necessary, but it can be reassuring to know just in case.
- If you are out and about it can be a good idea to have a **buddy support system**. Let your buddy know what time your meeting or event is likely to end, and text them to say you are home safe. If your buddy does not contact you to say they are home when you expect them to, and you cannot get hold of them, you should have the contact details of who they would like you to contact to raise the alarm.

"CITIZEN JOURNALISTS"

Is "citizen journalist" filming illegal?

It is not illegal to photograph, video or otherwise record locations or individuals in public. It is generally not illegal to record someone in a public setting without their consent in the UK. Nor is it illegal to take photographs of someone in a public setting without their consent, even children.

However, private locations require the permission of the owner, registered user or those who have a legal claim to the title of the location used. That permission can be revoked. Recording someone with the intent to harass, intimidate, or stalk them can be illegal. Similarly, recording someone in a private setting where they have a reasonable expectation of privacy, may be considered intrusive and potentially illegal.

The difficulty arises as the claim of reasonable expectations of privacy may not apply to the locations and work you are conducting. Places such as hotels, shared office buildings and conference or event venues will have both public areas (e.g. the foyer/ reception and grounds) and private areas (e.g. guest rooms, areas marked private, staff rooms).

Many protests are held close to, but not on grounds owned by the location you are visiting and the right to protest is a significant part of UK law.

Citizen journalists are careful to ensure they do not cross the line into criminality. They have been coached in understanding the laws which will have an impact on them. This is not to say that sometimes they may overstep the line and commit some offences under the public order act,

but this is generally rare.

A common tactic is to force the conversation towards “strawman” arguments. It is designed to undermine any point that you may be trying to make. Strawman arguments simplify and twist what someone is saying. For example, if a schoolteacher says many accidents involving children happen when they are playing, a strawman argument could be “the schoolteacher wants to ban everything fun”.

Amanda Smith with “The Bulldog” at a Yorkshire Patriots-organised protest in Leeds, 10 June 2023. Photo: HOPE not hate

WHAT TO DO WHEN “CITIZEN JOURNALISTS” ARE FILMING

It is important that all personnel remain polite and professional if responding to a situation where someone is recording premises and/or staff. When engaging, remember that your first words will often dictate the tone of the interaction. It is vital that you never volunteer information, and never attempt to change their mind by engaging with them.

Stick to a scripted reply and always be polite. Despite some individual’s façade of polite enquiry, it is wise to remember that everything you say can be re-edited to have the meaning that they require. Every question will be designed to mislead or trick you into feeding their agenda. The citizen journalist is well versed in legality.

While it may seem a good approach, saying “Don’t know” or “Can’t comment” will fuel the citizen journalist, as these statements can be easily manipulated to show either incompetence or naivety. It is easier to stick to a scripted statement such as “I am not in a position to answer your questions, please look at our website or speak to our press officer”

or if these are not available in your organisation, “I am not in a position to answer your questions, thank you.”

Remember that the goal is often to generate controversial content. The best defence is to make their interactions with you forgettable. Even the most innocent of statements can be turned and any hint of annoyance, aggression or impoliteness will be used to discredit not only you but your organisation as well.

If you are not comfortable engaging with the person filming, and it would not further endanger others, consider simply walking away or returning to the last place of safety. These individuals can be intimidating and ultimately it is your safety which takes precedence.

If the questioning becomes threatening and aggressive, return to your last safe location, and call for help.

CONFLICT MANAGEMENT

When interacting with suspected citizen journalists/auditors, we recommend a **CALM** approach – Chat, Assess, Limit, Monitor.

C **hat** in a friendly manner. (polite but not forthcoming with information)

A **ssess** for hostile intent. (be mindful of their agenda)

L **imit** interactions beyond what’s necessary. (do you have to interact?)

M **onitor** risk of escalation. (be situationally aware)

ONLINE SECURITY

The three tips below are general good practice for being online, and could be used by anyone to keep safe.

- **Passwords**: To avoid the threat of hacking, we suggest you have a different password for every online account, especially social media accounts. Password vaults, which are apps that securely store your various passwords, are helpful for this.
- **Two-factor authentication:** Using two-factor authentication, where you need to use more than one device to log into an account, makes your accounts less vulnerable to hacking. For example, you could receive a text message or email to confirm it's actually you logging into the account. If you receive these messages but have not tried to log in, someone else might be trying to access your account.
- **Check for hacks:** the website Have I been pwned? helps you to check whether your email address and passwords have been breached online. You should change all passwords associated with the email account if it has been breached.

DIGITAL FOOTPRINT

Although accounts being hacked into does happen, the most common way for bad actors to find out about you online is through your digital footprint: the collection of information that exists about you online as a result of your and others' online activity.

Anyone seeking to find information about you online will act like a detective: they will start with a few clues and then use this to gain more information. For this reason, it is important to consider what you put online: both what is public and who has access to what you put out privately. Bear in mind that you are only as strong as your weakest link – if friends, family or partners have information about you on their public profiles this can also be used.

Common starting points for looking into someone's personal information include names, email addresses (including old ones), relationship status, photos, employment status, location of work, the area you live in and phone numbers.

DOXING

Doxing is a slang term for hacking and publishing other people's private information online. While it can be a genuine error, it is normally done with malicious intent.

The information obtained by the “doxer” can be anything that you have left behind on the internet. This is generally your full name, address, phone numbers, photographs, email addresses, social networking accounts, passwords and banking details. However, some doxers will go beyond this and obtain as much information about your life as they can. This can include information about family, friends and associates.

The far right often use doxing to punish, publicly shame or harrass organisations, as well as what they see as “taking revenge” for what organisations do. In one example, a group who were frequently attending demonstrations doxed a group of counter protesters in an effort to dissuade them from continuing in their efforts.

There is no specific legal offence covering doxing. Depending on the circumstances, it may constitute an offence under a number of UK laws:

Section 1 Protection from Harassment Act 1997: a person must not pursue a course of conduct which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. To do so is an offence.

Section 127 Communications Act 2003: a person is guilty of an offence if he sends by means of a public electronic communications network (includes the internet) a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or causes any such message or matter to be so sent.

Section 1 Computer Misuse Act 1990: Unauthorised access to computer material. Causing a computer to perform any function with intent to secure access to any program or data held in any computer.

ONLINE ABUSE

Receiving online abuse, whether on a personal or organisational account, can be scary and exhausting. The main thing to remember is that in most cases, the onslaught dies down eventually, and in the meantime it is important to consider how you can look after your wellbeing, and find support for and from colleagues. Even if the account receiving abuse is not named, the person who checks it most frequently is still likely to be affected.

Sometimes, people want to speak up on their abuse in defiance of trolls. Sharing online can often result in further attention landing on a person, which can end up defeating the point of the exercise. Private, closed groups on secure social media apps like WhatsApp or Signal are best for sharing safely with a wider community. It might be worth reaching out to other local activist groups, even if they are in a different sector. People can offer solidarity and share their experiences of trolling or abuse and how they followed up. Remember that the context and circumstances will be different for different people, so there will not be a one-size-fits-all solution.

CASE STUDY: ONLINE ATTACKS


Jeremy Davis
Photo: YouTube

Far-right anti-migrant activist "Little Boats" (real name Jeremy Davis) posted on Twitter that he planned to galvanise his followers to attack "Quisling institutions" who worked with refugees, people seeking asylum and migrants more broadly. Many organisations in the sector were concerned about the impact of this. However, in the end the action involved attacking a single law firm by getting followers to consistently ring the phone line so that it was blocked, although this lasted for about an hour.

The impact on the law firm was minimal, although it gave them pause to reconsider the security measures they took in their office. For example, they made the office address less easily findable, as well as making it harder for people to get past the reception desk and into the main office in the case of escalation. They also blocked Little Boats and any associated accounts on social media, so that they are no longer disturbed by them.

SOCIAL MEDIA SECURITY

People engage with social media in different ways, and some people are comfortable having information shared publicly that others will be more cautious about.

However, consider the following if you are concerned about online security:

1. **Limit location information** – people can figure out patterns of where you live, work or spend time from location tagging settings on social media – which can be switched off – or from recognisable features in the background of photos. If you are posting whilst at a location or live streaming, anyone able to view that post will know where you are. Consider avoiding public posts which make the locations of the office and people's homes clear, and only posting tagged locations after you have left.
2. **Privacy settings for posts and tagged photos** – ensure that what you post on your own profile is only visible to the audience you want. For example, you can choose for content to be seen by anyone, friends of friends or only your friends. Tagging people in photos or allowing yourself to be tagged on profiles, groups and pages means that people can access posts about you through other people's profiles, which may be less secure than yours. Privacy settings change from time to time on platforms, so it can be helpful to regularly check for changes to your profile(s).

3. **Limit who can access your profile** – your privacy settings do not guarantee that anything you post online will remain private. For example, a Facebook "friend" may pass your comments on. Consider whether you might benefit from having separate accounts for your personal social media use with more restrictive privacy settings if you have to be more public for work purposes.

4. **Audit friends and followers –** it can be helpful for organisations and individuals who are at higher risk of trolling and online abuse to regularly check through follower lists. If a follower/subscriber/friend seems suspicious or does not align with yours or your organisation's values, consider blocking or removing them.

HOW CAN I PROTECT MYSELF ONLINE?

Doing a regular search for what information about you is available online is a good way of taking precautions before that information falls into the wrong hands.

Choosing to have no online presence is not a viable option for most people – sharing with friends and family and professional networking are just some reasons why people enjoy being online. That said, you may want to consider the following:

1. **What do you put online?** Think about what you might not want to be exposed publicly before you sign up, post and share.
2. **App permissions and privacy settings.** Ensure that you check permissions on your phone and other devices. This includes how your name, phone number and email address are shared, and what is shared publicly and with friends.
3. **Email.** Having separate email accounts for personal use and using to register with online accounts can be helpful as this prevents access to one leading to access to the other. Some online accounts have low security and are easy to hack.

ONLINE EVENTS

It is important for you to consider how to strike a balance between security needs and the needs of the event. Some of these tips will not be feasible if you want to use certain video call functions, and they might be overly cautious if you are not sending out public invitations to your event.

- If you are concerned about infiltrators taking over the meeting, use a **webinar format**, which means that only the speaking panel can speak and show video. You have to sign up for webinars with a name and email, so you will have a list of participants.

- In webinar mode, it is possible to **check the sign up list** and exclude suspicious names from receiving joining information. Closing sign ups a few hours before the event can help too.
- Ensure **screen sharing is set to "host only"** to ensure participants do not share harmful content or derail the event. If someone else needs to share their screen, the host can share permission during the call.

- It can be helpful to have a **moderator** (or two!) if you suspect that your event may be at risk. The role of a moderator is to monitor the meeting including the chat, screen sharing and breakout rooms. They can also block people quickly during the call if needed.
- You may want to **"lock" the call** after it's started or a few minutes in to avoid lots of people joining the call halfway through, which can be derailing. This can be particularly helpful if you do not have a moderator, although it prevents late joiners.
- In some cases, calls are recorded or participants could be recording their screens. It is best to **avoid directly quoting harmful material** as this can be clipped and misedited to make it appear as though you are saying it. If in doubt, paraphrase the harmful language.
- **Keep alert to the chat box** in the last two minutes of the conversation, this is when spamming and abuse are most common. If you have had issues with spamming previously, you might consider turning off the chat altogether, although obviously this will affect engagement with your event.

CASE STUDY: ZOOM BOMBING

An organisation in the migration sector was holding an open event to discuss their work with prospective volunteers and members. About five minutes before the event ended, one of the participants in the call changed their name and display picture to something profane and then proceeded to unmute themself and interrupt the talk.

The interloper was swiftly removed from the call and blocked from re-entry. Following the incident, the organisation made sure to always have one person "working" the event who was not busy talking or participating so they could remove participants quickly as needed.

CHEAT SHEET: IN AN EMERGENCY

⚠️ **Always remove yourself from the area of danger.**

⚠️ **Return to a location where you can safely call the police or your organisation.**

⚠️ **Remain in a safe space until help arrives. A safe place is somewhere public with other people around, with lots of exits you can easily leave from.**

⚠️ **In an emergency always call 999 and ask for the police. If you can't, ask someone nearby to do so.**

SHARE YOUR STRENGTH AND RESILIENCE WITH US!

HOPE not hate are always looking to champion communities who put up a fight against harmful far-right narratives. If you would like to share news about acts of solidarity happening in your community and be the hope for someone else, email us at towns@hopenothate.org.uk

HOPE not hate Ltd
Registered office:
167-169 Great Portland Street, 5th Floor
London W1W 5PF