Office Security Series: Entrapment Prevention and Preparation

Office Security and Safety Series

This document is part of RoadMap's Weathering the Storms--Office Security and Safety Series for social justice organizations, done in collaboration with Vision Change Win. The series seeks to equip organizations like yours with the resources and tools to manage different types of situations and/or crises your organization may face. This series currently includes several webinars and the following documents:

- De-escalation Methods and Tactics
- Event Safety Plans
- Entrapment Prevention and Preparation.
- Office Safety Assessment
- References to other resources such as "Know Your Rights" are offered in these documents

Disclaimer: The information provided in the Office Security and Safety Series are for informational and resource purposes only and not for the purpose of providing legal advice.

Entrapment Protection

Entrapment and entrapment attempts of social justice organizations/leaders is on the rise and can have serious consequences.

> **Always exercise awareness and caution to what is said aloud or sent via email. Do not say anything that you would not want to be public or end up in the news!**

Every nonprofit organization should have a list of protocols that clearly outline how to manage everyday walk-ins and phone calls to their office(s) that fit in line with the organization's values. This includes policies and procedures on how to track messages and field calls from important stakeholders. This particular document acts as a supplement to those protocols and solely focuses on how to manage individuals whose intent is entrapment.

In this document, entrapment refers to someone pretending to represent an entity falsely, the act of an individual trying to induce a member of your organization to make a statement or

commit an act that can be used against the organization. For example, this could be the case when an individual takes a statement out of context and uses it in a smear campaign against your organization. Another example includes paid informants trying to encourage a member of your organization to commit a crime. Please note, RoadMap sometimes also refers to entrappers as "posers." For the purposes of consistency in this document, we will be using the word entrappers.

The same groups that seek to entrap members of your organization may also be working to entrap members of the community your organization serves. There are separate protocols your organization can take to identify these cases and help educate your community on how to handle those situations. Although this is an important topic to discuss, handling this type of situation is not covered in this document. For additional information, please refer to RoadMap's document entitled, "Event Security Plans."

Role of the Receptionist/Office Administer

The front staff of your organization, usually the receptionist or office administrator, will often the first one to encounter a walk-in or a call-in. This staff member should be empowered with the necessary training and support to execute the protocols you create. At the same time, dealing with office security and safety are big tasks to tackle and it should not be the expectation that the receptionist or office administer manage it by themselves. There should be an expectation that other staff will be involved to assist with the de-escalation of different scenarios that may come up and decision-making when needed.

Keys to Success: Important ways to Proactively Prepare

To be fully prepared to respond to cases of entrapment or posers, we suggest that your organization have clear messaging that can be used in various types of cases. This messaging would clearly outline your organization's mission, values, and the work it does. This messaging should be designed in a way so it can be used in any type of situation (media requests, fundraising, managing crises, and so on). This messaging is often created as part of a crisis communication plan.

Additionally, it would be helpful to have a clear emergency plan to implement when there is a case of entrapment. This plan would include identifying which key members of staff would be notified and tasked with creating and implementing a strategy to manage the case. This is often called a crisis management team and they would implement the protocols outlined in a crisis management plan.

For support in this area, RoadMap has additional resources that can guide your organization to create both a crisis communication and crisis management plans.

What to Look For?

When dealing with callers or walk-ins you want to look for specific signs that indicate that extra precautions should be taken when communicating with this individual. However, not all callers or walk-ins will carry these characteristics and you should assume that any conversation you have with someone could lead to a possible entrapment case. Therefore, stay on message and be mindful of what you say at all times. With that being said, the signs listed below may help flag possible scenarios. The protocols in this document should always be implemented and followed to protect your organization.

Signs to look for:

- Refuse to give their name or contact information.
- Not clear on the purpose of their call or visit.
- Make statements that appear to be intended to incite a reaction (i.e. they support some type of violence or marginalization of a community).
- Ask leading questions or make inflammatory or provocative statements.
- If you are a client-based organization, their case may seem not plausible.

Structure of Reception Area

- Decide who from the organization will greet walk-ins and answer the phone calls. If you do not have a designated reception or office administrator, it is recommended that not everyone answer the phone or be tasked with greeting walk-ins. Rather, have a few selected staff members who are trained in these protocols. Whoever is tasked with managing walk-ins and answering the phone calls, should also be capable of handling stressful situations and there should be a protocol, a system, special code or alert mechanism to alert other staff or higher ups to step in and handle the situation when needed (i.e. a crisis management team). Alternatively, you can train these staff on de-escalation tactics.
- Consider adopting a policy for how walk-in requests will be responded to. We strongly suggest requiring all walk-ins to sign in. Other policies may include:
    - Ensure the sign-in sheet is reviewed immediately when filled out.
    - The organization only meets with community members by appointment.
    - For organizations that are client-oriented, ask them to fill out an intake form that can be reviewed before a staff member meets with them.
    - Ask for guests to show identification.
    - *Note: These are only examples and may need to be catered to fit your organization.*
- If they are requesting to meet with a staff member and you do not know the person, take the following steps:
    - Do not immediately inform them that the person is present or available.
    - See if you can do a quick search on the person and if any red flags (research elaborated on below).

    - The safest step to take is to tell the person the employee they requested to see is not available and you will call them back to set up an appointment. This gives you more time to research the person properly. To help, consider placing some type of barrier between the reception desk and the rest of the office so an individual who walks in cannot easily get through. The trick is to make sure that the employee who the individual wants to see doesn't come to the reception area during this time.
    - If the team feels like the meeting should take place immediately, meet in a conference room or a room that does not have any papers, filing cabinets, etc. with sensitive information and have at least two people in the meeting. You can also consider recording if the team feels it is necessary (recording is elaborated on later).
- For some communities, entrapment tactics are used by law enforcement, particularly when they are searching for specific information. As you should know, anything you say or do in front of law enforcement can be used against you or your organization, and therefore, any visits need to be handled properly. In instances where law enforcement appears without being called or Immigrant & Customs Enforcement (ICE) officials appear there should be clear protocols for who and how this is handled. These types of unexpected visits can be frightening. We strongly recommend that your policy does not place the responsibility for managing police relations or receiving or evaluating warrants to reception staff. Consider having protocol that front office staff are tasked with saying they are not authorized to evaluate a warrant or grant access and that they will call on someone who is to speak to them. These interactions are covered in more detail in other RoadMap materials and webinars.

How to Communicate with the Caller or Guest:

- For phone calls, always ask the full name of the caller, their contact information, and the purpose of the call. Consider having an intake form that creates an official way to document 'suspicious' conversations. Report these "suspicious" calls to your Crisis Management Team.
- For walk-ins, always have sign-in sheets that require listing their name, contact information, and purpose of their visit.
- Be extremely cautious about what you say or write to the person and never give information out that cannot already be found on your website or a recent publication (i.e. press release).
- If they insist on additional information, refer them to your website.
- Never send any information over email that is outside of your official messaging (as we explained in 'Keys to Success' section).
- Always document and record any interactions with suspicious guests and keep for record keeping.

Researching

We have suggested a few times to do some research on the person in question. This research can primarily be done through a basic web search. Here are some things to look for:

- Quotation in other articles that share more information about who they are and what their views are.
- Verify their credentials are accurate.
- If you are a client-based organization, create a process to verify claims as part of the in-take process.
- Look for public posts on social media that may be concerning (i.e. strong statements that are against the community your organization serves or the cause your organization supports).
- Find ways to verify their name is real. One way would be to find social media and take the following steps:
    1. Find a picture of them on social media platforms and download it if you find one.
    2. Open a search engine on a browser and find the option to search for images. Follow the steps it provides.
    3. See if pictures of the same person come up with a different name.

What to do post research?

If the research indicates that this person may not be who they claim to be, find ways to decline their requests. For example, you may tell the person that someone will get back to them and never follow up. In most cases, the entrapper will not follow through.

If for any reason you believe this person may also approach organizations that are your partners or allies, consider telling them about this incident so they can be prepared as well.

Interview Requests

If they are asking for an interview, always take a message and communicate that someone from the organization will get back to them. This will give you a chance to research the person and find any flags that may indicate what their intent is. Make sure to always ask for credentials and what their deadline is. In the event that they do represent a media entity, you always want to help them meet their deadline. It is possible to help them reach deadlines and still follow the protocols outlined in this document.

If they say they are an independent reporter or a freelancer, ask them for samples of their work in addition to researching them.

If you do not find anything that confirms the person's claim or your suspicions after research, always trust your gut and be very cautious about what you say or write to that person. If you still do not feel comfortable giving an interview, ask the person to email the questions and

answer over email. This is where clear messaging comes in hand as you can repeat the organization's messaging over and over again. There is no harm in sticking to this messaging and you won't lose an opportunity if it is a legitimate media request.

If you proceed with this option, keep a copy of the email for your record keeping.

If you decide to move forward with an in-person interview, you can still use the strategy of repeating the organization's message over and over again.

Lastly, one or two staff members who are trained to deal with different types of interview scenarios should handle all interviews.

Issues around Recording

When protecting your organization from potential cases of entrapment, your organization should adopt policies that indicate when it is okay to record and how to handle situations when you are being recorded.

When to record?

When in doubt, always record a conversation so you have a copy of the conversation for your own records. This can help clarify any statements that may be taken out of context and proof against any accusations that may be made against your organization.

However, you must be familiar with your state's laws on what consent is needed when recording. Currently (as of 1/1/2018), 12 states forbid the recording of private conversations without the consent of all parties. This includes California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. Make sure to continuously check the laws for any changes.

If you live in a state that needs the consent of all parties, try documenting the conversation that is happening by taking detailed notes via pen and paper or typing. If that is not possible, document the conversation after the conversation has concluded. It may even be a good idea to create a template form that staff fill out (aka an in-take form) so all details are documented correctly and thoroughly.

When they are recording you

If they are recording openly with you, you have the right to decline to be recorded or ask them to not record.

If you feel you are being recorded secretly in your office, you can also ask them if they are recording or indicate they do not have permission to record. Even if they deny they are not recording, repeat that they do not have permission to record and make no other comments.

If you feel you are being recorded in a public space, you can decline to make any comments or make comments that are short and concise and match the organization's messaging or already

found on your website. For example, a short response that may already be part of your messaging is 'The tax bill favors the wealthy over the rest of us.'

This may be an opportune time to record any comments so you have proof of what you said. Or consider asking another staff member to join you and witness you making comments.

For these situations, it would be helpful to have clear policies that outline when people can or cannot record within the office. For example, you can have a policy that you only allow individuals with verified credentials to record. Alternatively, you can have a protocol that states no one is allow to record. It could also be a good idea to post these policies somewhere where it is visible in the reception area of the office.

If you are a target of entrapment, know your legal rights and push back, when possible. There should be consequences for entrapment and entrappers.

Advocacy Statements

Make sure all staff are trained on the statements the organization can or cannot make regarding policies, elected officials, or candidates. Make sure all staff know they can never express their personal views when representing their organization. This includes views social media. (For more information check out the sample "social media policy" in RoadMap's 'Weathering the Storms' Tool Kit). Make sure all staff are clear on what messaging exists on advocacy issues the organization is currently engaged with.

Seeking Legal Assistance

If you feel your organization may be threatened with an entrapment case, you should contact an attorney for legal support and advice. It is important to establish relationships with attorneys ahead of time so you know who you can approach. Your organization can also look at social justice organizations who may provide legal services pro-bono such as the National Lawyers' Guild or the Lawyers' Committee on Civil Rights.