



# Your First Training

First of all, you are awesome. If you are reading this, it means you want to help others, and you don't assume you know everything. By learning how to meet others where they're at and helping them find what they need, you are helping them improve their safety. You are also helping your communities learn more about crucial, complicated issues that affect all of us, so they can be more informed and engaged citizens.

The truth is that helping others learn about [surveillance self-defense](#) isn't easy. The good news is that you will definitely get better with experience as you learn and reflect on what doesn't work. Your first workshops may be stressful and you may feel self-conscious about how they went, but don't be too hard on yourself when you begin!

We've included some tips and links to information and tools that we wish we had when we started out. Remember that gaining experience and becoming skilled as a trainer is a process, much like learning about how to improve your own digital security and privacy. Similarly, it's highly rewarding the more you learn and the more skilled you get.

## Starting Out

Look into your local options for training education and practice. **If possible, find someone who's led digital security trainings before and co-train with them, or find someone interested in training to collaborate with.** This will make starting and gaining experience better and less stressful. To read more about this, see [Building your Superhero Team](#).

Then, we also recommend a few additional steps to set yourself up with the right participants, venues, and allies. Check out these additional steps from [Am I the Right Person?](#)

## Planning and Preparation:

**Craft an agenda.**

It's very common for first-time trainers to create The Completely Impossible Agenda. This is because we don't have a sense of how long certain things take during workshops. We also don't have deep experience teaching certain topics yet. If you come from a technical background, you might not have any event facilitation experience, and tend to focus on tools instead of concepts. It's also surprisingly common for us to think that our training will be the only time our participants will have access to an event like this, so we need to cover as many topics and tools as we can. Be aware of all of these tendencies in order to avoid them. For more on the fine art of agenda-crafting, see LevelUp's [Planning Your Event Agenda](#). For more on logistics, see our our piece on [Training Logistics](#).

### **It's better to do a few things well than many things poorly.**

Think about what will be the most useful thing a specific audience can learn with the time and resources available. If you try to include *all* the things they may need to know, you'll be setting the event up to fail. The concepts and tools are simply too complicated, and rushing through them doesn't mean you've taught them. People will forget what you say, you'll lose them early, and they won't know enough to actually use anything you've covered. It's much more effective to make sure they get a few things down well than a number of things poorly. That way they'll be able to build on what they did learn instead of walking away feeling overwhelmed. For more guidance on deciding what to cover and how, check out [Learning Objectives](#).

### **Think about the different ways people learn, and how to accommodate different types of participants.**

You may already be familiar with different learning styles if you don't learn well in a top-down lecture-style format that most of us have experienced. To learn more about learning styles, check out [Catering to Multiple Learning Preferences](#). This will also give you ideas for how you can make your events more dynamic and fun for participants. To be prepared for a wide range of participants, read [Cultural Sensitivity](#) and [Drawing from Inclusive Education](#). The latter will be particularly important if you are not personally familiar with different types of limitations and disabilities.

### **Be aware of how different types of privilege affect workshop dynamics.**

Learn more about how [technical privilege](#) is a real thing. In worst-case scenarios, it can alienate us from our audiences if we're not aware of it. And if you're completely new to

the concept of privilege, or hostile towards it as a word or concept, check out "[The Lowest Difficulty Setting](#)," by sci-fi author John Scalzi.

## **Prepare, prepare, prepare.**

The more you prepare, the better your event is likely to be. There's a huge gulf between you knowing a topic and others learning it from you. How long will it actually take to walk through an install and get some initial practice with a tool? Have you accounted for different operating systems and the very likely scenario that 1-2 people will need 1:1 help? Do you have some activities ready to go? Can you practice them with others before the event? If possible, see if you can have a friend who is unfamiliar with the topic stand in as your audience to practice certain sections, and ask them for constructive feedback. For more info on preparing, see [Training Prep](#).

## **Get familiar with all major operating systems.**

If you're not familiar with participants' technical operating environment, you won't be able to meet them where they're at and be prepared to troubleshoot issues during hands-on sessions. You'll also struggle to answer some essential 101 questions you'll receive. Also, if you look down upon people who use [this or that operating system or device](#), [your participants are likely to notice](#). This won't help build trust or respect for you and your work, and can work against you.

## **If you're covering specific tools, know them backwards and forwards on all major operating systems.**

This way you'll be prepared [when questions come up](#), you will already have the steps outlined, and you'll be better at troubleshooting any technical issues that arise. Additionally, if you are clearly unprepared, your participants might trust you less, or worry that you may not know enough about what you're teaching.

## **Find real-life examples to illustrate and clarify the material.**

Because digital security and surveillance is generally in the realm of things that people can't see or touch, it's common for people to struggle with how they can make a difference. Having real-life examples gives people meaningful stories they can use to comprehend what you're trying to convey. Try to identify current news or other stories that illustrate key concepts, gotchas, common mistakes, "teachable moments," or how certain tools work. Ideally, they should be contemporary and preferably [close to participants' daily lives and culture as possible](#).

## **Be prepared to manage wildly different expectations.**

This can play out in different ways. It might be that the convener of an event wants you to do way more than you have time and energy for. Or, they may exhibit "wishful technical thinking" and assume you can cover a wide range of topics for 100 participants within two hours, and you need to provide a gentle reality check about what the topics entail. Be aware that you may have to check your own expectations as well. Do you have enough time to prepare for an event? Are you going to have enough energy to lead to a specific workshop? For more on this, see LevelUp's [Setting Expectations for Participants, Organizers, and Yourself](#).

## **During Events:**

### **Don't forget to have fun!**

It's hard to feel like you're having fun if you're stressed out and nervous. Take a deep breath, tell yourself it's going to be okay, and try to have fun with it. If you have funny stories or great analogies, ham them up. During the activities, inject some life into what you're doing. Not only will training become easier the more you do it, but it'll also become more fun, which is better for you and the participants.

### **Meet people where they're at.**

It's common for novices to have a pre-set idea of who participants will be and what they'll need to learn without properly meeting and learning about them. Remember to "meet people where they're at" by keying your event to who they are, what they know, what they're afraid of, and what they're asking for. It probably won't be a good idea to teach them about a tool they say they don't need, or aren't convinced will benefit them. They may need to start at very basic first principles because they don't have accurate mental models of how the Internet works. If you have a mixed group of participants, think about how to handle [Different Devices and Operating Systems](#) and [Different Threat Models in the Same Room](#).

### **If you don't know something, don't say that you do.**

It's common to feel like we have to know all the answers, especially if we come from a more advanced technical background. No matter your background, [don't claim knowledge you don't have or give advice about contexts you're unfamiliar with](#). If you don't know the answer to a question, say "I don't know," and then offer to follow up if

they're willing to share their email or other contact information. Even though it may not feel like it, this will actually build trust between you and participants, because they see you as a peer who respects them enough to make sure they have the right information.

### **Collect feedback and reflect.**

One of the most valuable habits to develop is clear methods for gathering feedback and improving. In addition to collecting feedback from participants, do a debrief on your own or with your co-facilitator(s). What went well? What would you have changed? Don't be too hard on yourself when you get feedback! Acknowledge it, think about it, make a plan for how to address it in the future, and move on. We've all made mistakes and learned things the hard way.

### **There's a place here for you.**

Sometimes people try teaching digital security and realize it's not for them. This is okay! There is a huge need for your skills in other capacities in the world of activism. Some people end up working as sysadmins or IT support, or decide to contribute to open-source security and privacy tools. Others might go on to facilitate actions and events, and support digital security education by advocating for it in their community and bringing in trainers. Whatever it is, people need and will welcome your help. The ever-expanding number of issues related to digital security and privacy is mindblowing, and people need people they can trust to help them navigate all of this—be that person in whatever best way you are able.