When Different Threat Models Are in the Same Room

Digital security trainings have a better chance of succeeding if all of the people in the room have a similar threat model. This can mean training a room full of people who all work for the same organization, or a room full of freelance journalists, or a room full of activists who are from the same region or who work on the same issues. But sometimes trainers are asked to work with broad audiences with diverse threat models, or conduct trainings that are open to everyone. Here are some tips for what to do when that happens:

Set expectations:

Talking to a group of people with dissimilar threat models means that you may not have enough time to go in-depth on each person's specific concerns. If it's just you, you probably won't have enough time to to speak to multiple threat models, and going into great detail about one particular person's concerns may mean losing the rest of your audience. This may be a better fit for an "awareness raising" event rather than a security training.

Find common denominators:

Try to focus on content that will be relevant to as many of the people you are training as possible. You can find this out by asking people to complete a survey in advance. If you do not have the option of having attendees fill out a survey, try to keep your content as broadly applicable as possible and tailor your teaching plan based on feedback you receive during the training. This can be as simple as giving your students a range of potential topics and periodically asking them what they would be interested in exploring next.

Some topics that are likely to be relevant to most people in a training include threat modeling, strong passwords, password managers, encrypting the data on your device,

two-factor authentication, phishing, and using an end-to-end encrypted messaging application.

Don’t get bogged down in a single person’s threat model:

When people with many threat models are in the room, sometimes one or two people will dominate the conversation with a set of specific problems or concerns that are not relevant to the rest of the people at the training. It may take a few questions before you identify these people, but it’s usually a good idea to offer to talk to them one-on-one during a break or after the training rather than allowing them to take up training time in a way that is not useful to the rest of the group.

Divide and conquer:

If you have a co-facilitator(s), assign one to each group to lead a discussion about their specific concerns or (if you have enough time) go in-depth on each group’s needs. You can then regroup and share debriefs on how it went for each group and what next steps might be for them. Or, if you don’t have multiple co-facilitators, you can cover the topics that are broadly applicable to everyone, then divide participants up into groups that have broadly similar threat models. You can then ask for a volunteer from each group to facilitate their group discussion.

Since learning the process and habit of assessing risk is something that’s developed over time, remember to be reasonable in what you can achieve given your time and resources. Depending on the amount of time you have, the needs and skill levels of your participants, and the number of facilitators you have, you will have to adjust what you can achieve. You may only have time to go over how to assess risk and then apply it to a few examples. Or you may be fortunate enough to have enough time to do some amazing in-depth work over a longer period of time with multiple facilitators, resulting in a comprehensive assessment of participants’ risks and a plan for what they should do next. Whatever your situation is, remember to manage expectations, not try to cover more than you can, and focus on getting a few things down well rather than than covering a large number of things poorly.