When You Are Out of Scope

Just as important as sharing knowledge and skills at your training is knowing when to admit to yourself, "I don't know," or "I'm not prepared to go over that today." No single person knows everything about digital training, and there is always more to learn. It's better to identify when you are out of scope than to try to do something unfamiliar on the fly, which can lead to confusion and stray you off-topic.

This often comes up when someone in your training asks a question you may not have anticipated or heard before. Avoid the temptation to improvise an answer you are not sure of, and instead be ready to kindly say you don't know. You can say, for example, "That's a great question that falls out of my expertise," or "That's not in my wheelhouse, but that's definitely important to think about," or, "I haven't been following that issue closely." If appropriate, you can offer to investigate the question after the training, or connect the person with someone who may have an answer.

Knowing when to say "I don't know" is particularly important with legal questions. If you are not a lawyer, it is okay to simply say that and not answer any legal questions! This could include questions about whether or not certain activity is illegal, questions involving laws or legislation, or questions about legal rights when dealing with law enforcement or the government.

You can also run into tricky technical questions. You might be asked to give advice about a specific VPN, or about what anti-virus software to use. [Instead of giving a one-and-done recommendation, you can admit there is no one right answer and talking through your thought process instead.](#)

Just as trainers come with unique strengths as well as areas where they may be out of scope, so does this training resource. These guides are meant for one- to four-hour awareness raising and security education events. These guides are also best when used with one's friends, neighbors, and colleagues for discrete personal security topics and tasks like basic threat modeling, two-factor authentication, or installing Signal.

With all that in mind, if you find yourself considering leading a multi-day training for a frontline community interested in reconfiguring their systems or other complex tasks, then these guides are not the right resource. Similarly, these guides are not able to help with organization security, enterprise security, or other types of group security beyond personal digital security.

Everyone has areas of expertise, and areas they know less about. If you are not sure, it is okay to say you don't know and avoid giving shaky advice or inaccurate information.

Do you find yourself getting really into digital security awareness raising, and want to host a multi-day event?

LevelUp has great resources at https://level-up.cc/.

If you find yourself being asked to help an organization with deeper problems, and that you have the capacity to support them over time, you may want to look into the [SAFETAG auditing framework](#), as well as the organizational security approach at https://orgsec.community.