Hitting the Sweet Spot of Engaged Learning

It’s common to feel frustrated when participants are clearly not engaged in a workshop. Why is one person passionately engaged in learning more, while another is checked out, or even upset?

One of the most useful concepts to internalize when teaching others about security is a “pressure gauge” of engagement. This was developed by Craig Higson-Smith, of the Center for Victims of Torture, to help trainers understand how common human reactions to learning about security affects our ability to learn.

This Anxiety-O-Meter image is adapted from Craig Higson-Smith's original graphic.

Too Cold: This doesn’t relate to me

It’s helpful to think of a gauge ranging from “cold” on the left to “extremely hot” on the right. “Cold” represents how someone feels or responds to something—in this case, to the topic of surveillance and digital security. When people remain “cold” towards the topic of surveillance and digital security, they might be unaware of it, don’t understand its significance, or don’t consider it important enough to spend their time and energy on. When they think about these issues, they personally feel safe as they are. When participants are “cold” towards a topic, they tend to ignore or tune out conversations about it and believe that something or someone will protect them from harm.

Getting Hot: I’m afraid and uncomfortable

In the other direction, many people react to discussions of digital “threats,” “risks,” and “surveillance,” with some level of anxiety or “increased emotional pressure.” People may react with a sense of fear and try to escape or avoid what they identify as a threat. One person may be thinking about having their emails read by a stranger, another person may be afraid of how embarrassing it would be for their personal details to be stolen and revealed. Another person may be afraid of being arrested, detained, or deported. Higson-Smith asks trainers to “remember that healthy participants will act automatically, unconsciously, and immediately to make themselves safer.” Trainers should be aware that some participants could find that a topic threatens their sense of safety and well-being, and may feel some anxiety, fear, and even panic.

These reactions often exist on a physical level, with sweaty palms or an increased heart rate. They can also be behavioral or emotional reactions as we try to regain a sense of safety and avoid danger. We may not even be conscious of physical responses while they are happening. Behavioral reactions may appear unrelated to one’s anxiety or fear about the topic of surveillance and digital threats. For example, participants who react with anxiety or fear may try to soothe their anxiety by focusing on their cell phones and ignoring the presenter completely. Others may aggressively challenge a facilitator. Others may try to divert their attention and calm themselves by starting conversations with a neighbor. Some may even get up and leave.

Runaway Adrenaline: Overwhelmed

It’s important to realize that some participants may react with more anxiety, stress, and fear than others, and they will not be in a “zone” where they are able to learn. In these cases, participants may respond even more strongly than others. Some may have been stalked or abused, or experienced types of trauma. It’s possible to have participants like this at events, and participating may be too challenging for them. They may benefit from other types of assistance, or a far more tailored type of event for participants with similar experiences. To read more about this, see the links at the bottom.

"Just Right": Concerned, anxious, but comfortable enough to learn

The ideal experience is when participants react with a little bit of anxiety, but not too much. This helps them reach a level of engagement ("I should really take this seriously!") while still feeling comfortable enough to actively learn new things ("Ok, tell me what I need to do"). Participants in this zone have been exposed to enough information and context to understand how the topic relates to them, believe learning about it is worth their time, and that they can take steps to meaningfully improve the security of their data and communications. Participants in this zone are concerned, but they are *engaged*. They will listen and follow along, they will probably ask questions, and they will participate.

A note about "security demos" and "scare tactics": You may feel frustrated when you're running a training and participants appear "cool" towards the topic. They aren't listening to you, and they don't appear to care. In this situation—especially if you're new to teaching and have a technical background—it is common to use different types of "scare tactics" to get participants to react and care. Scare tactics may be horror stories you've picked up where people lose everything, get arrested, or worse. You might also use different "security demos" where you directly demonstrate a type of hacking or attack on participants' devices and accounts. There are ethical or unethical ways to use scare tactics and security demos, which you can read about in Fear is the Mind Killer.

Remember that if you use scare tactics and security demos unwisely, unethically, or inappropriately, you can make your participants *so* anxious and fearful that they automatically and unconsciously focus on how they can immediately regain a sense of safety. This often means diminishing or diverting themselves from the source of their discomfort: *you* and your presentation on surveillance and digital security.

Don't forget to clearly communicate that they *can* do something about the threats and attacks you talk about, and highlight that they are *not powerless*. This is particularly important because of how the media often covers digital attacks. It is common to encounter a sense of "digital nihilism," or a fatalistic attitude towards digital threats because the media often focuses on advanced attacks by highly skilled adversaries. When describing specific threats, pair them with tools and tactics participants can use to protect themselves from those same threats. This helps people feel like they are clearly making progress and protecting themselves, even if they aren't technical experts.

This piece was adapted from Higson-Smith's writing on "The psychosocial underpinnings of security training". For more details on how emotional responses to safety are at play in digital security trainings, and how to use this knowledge in your work, we highly recommend reading more of Craig Higson-Smith's piece on LevelUp. If you're interested in learning more about how to take a "holistic" approach to training that integrates physical and digital security with wellbeing, you may also want to check out this end-user manual and trainers' guide on holistic security.