Why Your Audience Should Care—And Act

Even the best planned, most expert training will be hard to conduct if your audience is not motivated to engage and learn. Sometimes, as a trainer, you will have to explain not just the what and the how of digital security, but the *why*. Why should your learners care about digital security? And, why should they take action to develop their personal security?

In addition to general tips and tricks, there are several types of learners you might encounter who need extra motivation to care and act.

General Tips

The best way to motivate your audience is to be genuine and empathetic. Have some of your own real-life stories ready to go. Have you ever accidentally clicked on a phishing link? Was there ever a time in your life where you used less-than-strong passwords? What motivated you to learn more or change your habits? Stories about your own mistakes and learning can build trust with your audience and encourage them to think about their own motivations.

Avoid making your stories sound too scary or intimidating, however. Fear is the motivation killer, and can lead to "security paralysis" or other kinds of disengagement from learning. Motivated learners should ideally feel capable and empowered, not helpless.

Finally, be attentive to how learners are approaching concepts and tasks throughout your training. A single person can cycle through several of the attitudes below (and more!) in a single training. The better you are at spotting and responding to learners' motivational hangups, the more they will get out of the session.

Nothing-to-Hide Apathy

> "I have nothing to hide, so why do I need to protect privacy?"

Learners with this attitude typically do not feel a personal stake in their digital privacy and security, and therefore do not feel compelled to act. They may associate digital security concepts with high-profile state actors, whistleblowers, and public figures—not with "normal" people like themselves.

Talking through the first step of threat modeling—the question "What do you want to protect?"—can also be helpful to guide this type of learner towards finding their own stake in digital security. One common motivator can be to remind this learner about the importance of keeping their credit card and bank account information safe, both on the associated websites and on any commerce websites like Amazon, PayPal, or Venmo. The information often found on "people finder" sites—like full names, home addresses, and family connections—can also be motivating.

It's also common for the "nothing to hide argument" to become so dominant that we forget what's at play when we talk about privacy. If you're going to cover topics related to privacy, or if you think this will be a common reaction among participants, you may want to plan to include a conversation or activity that explores what privacy is and what it means to people.

Finally, sometimes a learner with this attitude is making a logical decision based on their own threat model. Having identified what they want to protect, who may come after it, and what their risk is, they may have simply decided that a certain privacy

protection is not worth them expending significant time, resources, or energy. Your job as a trainer is not to “convince” them that they “should” take certain actions, but to help them make an informed decision.

Security Paralysis

> “I am worried about my digital security to the point of being overwhelmed. I don’t know where to start.”

This kind of learner cares deeply about digital security, but is frightened and paralyzed. Often, learners with this attitude are overwhelmed with the task of locking down their personal information. Perhaps they have been bombarded with news stories about leaks and data breaches, or have close friends who have experienced personal harassment or doxxing. They may have even been exposed to intimidation-based trainings in the past that left them feeling overwhelmed and helpless in the face of various digital threats.

In this case, it can be helpful to emphasize one’s personal agency. At the same time, acknowledge the reality that it may very well be impossible to control all the information about one person online—and *that’s okay*. Instead, we can shift the goal from erasing all our information to just minimizing our information. First steps to take could include Googling oneself (perhaps with the support of a trusted friend to help alleviate any fear associated with doing so), investigating social media settings, or looking into opt-out options on people finder sites. The mission is to get the best idea possible of the information available about ourselves online, and then reduce it according to what we care about and are worried about. If we can minimize the information that we have control over, then we are in a much more powerful position if and when a company we use has a data breach or a social media platform we’re on changes its default settings.

Technical Confusion

> *“I’m ready to take action, but not until I have a perfect handle on how all of these technical concepts fit together.”*

This kind of learner may be technically overwhelmed. They are hearing about different kinds of devices, operating systems, apps, software, browser extensions, and encryption. While they have abundant information, they have no idea where to start or exactly how all these things are connected. Often, these learners have less experience with technology than the average trainer, but they are detail-oriented and cautious. They may be senior citizens, or come from a low-resource background that has not given them consistent access to cutting-edge devices and software. Just like security paralysis, this learner typically does not know where to start.

As a trainer, you can help them focus on the security principles behind the technology. Technology changes quickly and can be confusing, but fundamental security principles—threat modeling/risk assessment, tradeoffs, and deciding who and what to trust—can all act as steadfast guides as technology changes and evolves. Also emphasize that security is more than just tools. It’s about adopting a “security mindset” over time.

Security Nihilism

> *“There’s no such thing as perfect security, so why even bother? If someone wants to hack me, they’ll figure out a way to do it.”*

Learners with this attitude are at your training because they care, but also because they don’t know what to do. Or, perhaps more accurately, they do not think they have the power to do much.

One commonly useful concept with this kind of learner is “**door lock security**.” Ask your learner to think about the lock on the door of their home. It’s likely a normal deadbolt with a doorknob lock. Point out that that lock can be compromised in any number of ways: keys can be stolen or forged, locks can be picked, doors can be kicked down. If someone was determined to breach that door, they probably could. But your learner probably still locks their door regularly and finds some assurance in that level of security.

You can even extend the analogy to extra layers of security. Perhaps you can imagine someone with particularly expensive items in their home having a security system protecting the perimeter of their house. Or, maybe they’d have a safe inside the house for valuables and important documents.

Encourage your learners to approach their digital security in the same way. The digital security equivalent of a “door lock” can be reliable, reasonable, and worth using, even if it is imperfect and incomplete. For higher-value assets, added layers of security (analogous to safes or home security systems) can also be put in place.

Emphasize throughout that the entirely achievable goal is to make it *harder* or *more inconvenient* or *more expensive* to hack you, not to make it impossible.