Encouraging Ongoing Learning and Engagement

In teaching digital security skills, it's important to let participants take pride in what they've accomplished in a session while also showing them that digital security is an ongoing process. You want participants to leave feeling encouraged that they've learned a specific skill and excited to take the next step on their own or with a group.

It's a subtle balance to strike. You don't want to give participants a false sense of security after taking one step, but you also don't want to leave them feeling hopelessly overwhelmed. A participant might leave a training believing that now that she's learned how to use Signal, she'll never have to worry about the security of her communications again. Or conversely, the first time a participant gets frustrated trying to open an encrypted email, he may decide that there's no hope and that he's simply not smart enough to protect himself online. (Some educators refer to this way of thinking as the "**growth mindset**.")

For each topic in the Security Education Companion, we've created learning objectives ranging from beginning to advanced. You can use these accomplishments to help give participants an idea of where they stand within a longer development process. Let's use the example of passwords and avoiding phishing. Here's a range of achievements that someone might attain in their password security:

1. Using a password that is not "password"
2. Using a strong passphrase
3. Enabling two-factor authentication on any services that offer it
4. Switching to a time-based two-factor authentication app rather than receiving SMS messages for two-factor authentication
5. Using a different password for every service that requires one
6. Using a password manager and replacing every password you have with a randomly generated one
7. Using a strong passphrase to secure your password database
8. Using multiple factors to secure your password database

In a short, two-hour session, participants simply won't be able to complete all eight of these items (and trying to do so without understanding what they're doing could likely

result in a big mess). But they can likely do two or three. Meanwhile, a participant who successfully completes three or four of these items shouldn't get a false sense of security simply because she's ahead of the less experienced participants. She should be encouraged to push herself to the next level as well.

It’s also useful to keep this balance in mind when discussing participants’ current security strategies. Let’s say that a participant says that he keeps his email address and password in his wallet because his password is too long to remember. Rather than telling him that that’s the wrong way to protect his account, you could say something like: “That’s a great point. A long password that’s harder to remember is harder for a hacker to guess too. The next step is to hide that password a little more effectively. Have you ever heard of password managers?”