Fear is the Mind Killer: Rethinking Demos

Conducting digital security and privacy trainings for people who are sometimes not convinced that they need it can be a frustrating experience. It can be tempting to try to get participants to take security and privacy seriously by doing some type of “security demonstration” (or security demo) which often involves hacking your students in some way in order to demonstrate how vulnerable they are. Some examples of security demos include spying on your students’ unencrypted network traffic on a wifi network, sending your students a phishing email to convince them to enter their login credentials, covertly installing malware on your students’ devices using a USB stick, or conducting man-in-the-middle attacks to capture sensitive encrypted data.

These demonstrations are intended to show your students how vulnerable they are and to scare them into taking steps to protect their digital privacy and security. If you’re a hacker, you might think that it’s better for your students to experience this kind of attack from a “white hat” hacker in a classroom than a “black hat” hacker in the real world. But security demos can often backfire, are frequently conducted without the permission or awareness of participants, and—most importantly—do NOT help participants learn.

What’s So Bad About Security Demos?

Security demos are technically complicated. They often involve a lot of time or equipment and advanced preparation. Because they are so complicated, there is a lot that can go wrong. Your security demo may not even work.

Even if your security demo is technically successful, it can destroy the trust relationship you have built up with your students if you don’t do it in an ethical manner. Digital privacy and security trainings are built on trust. Your students may discuss extremely personal issues during the trainings, such as experiences with harassment, hacking, or abuse at the hands of their partners, family members, or law enforcement. If you are installing software, you may be trusted with access to their devices or email and social media accounts. Accessing their information without their consent, even if you think it’s for their own good, is a serious violation of that trust and can keep your students from effectively learning from you. Even worse, accessing that information and showing it to the entire classroom as an “example,” can embarrass them, inadvertently reveal highly sensitive information, and lead to *all* the participants distrusting and disliking you.

Security demos can even be a violation of the law. In some U.S. states, intercepting someone’s voice messages, or monitoring their unencrypted network traffic without their consent can be a violation of the Wiretapping Act. Logging into someone’s account without their permission can be a violation of the Computer Fraud and Abuse Act (CFAA) in the U.S.

But most importantly, humans don’t do their best learning when they’re afraid. Fear can be an effective motivator in some cases, but *feeling* afraid means your body goes into fight or flight mode and becomes doused with adrenaline. This can prevent people from learning, as scared participants often feel frozen or overwhelmed rather than encouraged and empowered to take action.

Even worse, when security demos are framed poorly, they can make the people you’re training feel that taking action to protect their privacy or security is pointless, because technically skilled attackers will always find a way in—a perspective we call **Security Nihilism**. The most common example of this is doing a scary security demo and then telling participants that it is extremely difficult or impossible to protect themselves from such an attack. In these situations, Security Nihilism is the worst way your security demo can backfire: It will lead participants to give up and do *nothing*, not just after your event, but into the future. You will have ended up leading a training that turned them off the topic completely.

If you’re someone who has done security demos this way, you may want to reflect on your motivations for doing so. In many cases, novice trainers may tend to rely on security demos because they aren’t yet skilled in other ways. Perhaps you’ve struggled with getting participants to care or be engaged, and extreme security demos have been the most effective approach you’ve had thus far. Or you’ve seen others do them and just assumed that it’s the way things are done. If this is the case, don’t beat yourself up. You can change how you deploy demos in your trainings. You’ll want to learn more about what makes an effective vs. ineffective security demo below. In other cases, there are trainers who do extreme security demos in unethical ways because it makes them feel powerful and cool in the eyes of their peers—not because it helps participants. If this is the case, you may want to reflect on your motivations for conducting trainings in general—are you there for the participants, or are you there for yourself?

What Can I Do Instead?

Showing demonstrations of traffic interception or account compromises to your students can still be a very powerful teaching tool, but you don’t need to trick your students or compromise their privacy in order to demonstrate it effectively. You can set up a demonstration using devices that you own and control, and collaborate with a co-trainer to do a live demo using these devices. For an even easier option, set up your demonstration in advance and record or take screenshots that you can show to your students during the training. This animated gif demonstrating what Google sees when two people chat using their Google Hangouts accounts and Tor Messenger, versus what Google sees once the users turn on Off-The-Record (OTR), is one such example.

Recording your demonstrations, using test accounts and devices you control, is an excellent way to show security and privacy concepts without risking a complicated setup, betraying your students’ trust, potentially breaking the law, or paralyzing your students with fear.

Do No Harm

Illustrating digital security and privacy concepts through demonstrations is absolutely worthwhile, but much like doctors, digital security trainers have an obligation to first do no harm. Insecurity demos may seem like a good idea at first, but they can be dangerous, off-putting, and ineffective. And you don’t want to undermine your work by frightening your participants out of learning what you’re there to share.