Threat Modeling (beginning)

Learning Objectives

Learners will:

- Define what a threat model is.
- Understand that they use threat modeling already in their day-to-day lives.
- Understand the five questions and concepts at the heart of threat modeling.
- Understand the five terms learners should be aware of to apply threat modeling.
- Have thought about the various points an email can be intercepted.

Prerequisites

- None! This is an excellent first module for starting your training.

Ratio

Instructor: Learners
Flexible

Suggested Materials

Threat Modeling Activity Handout

Post-its or notecards

Pens

GOTCHAS AND PROBLEMS YOU MIGHT HIT:

- It’s best to have a group of people who share the same general risks, concerns, and threats. If not, you’ll want to prepare for when different threat models are in the same room.

- People might be intimidated by the term “threat model” and associate it with military terms. (Actually, it historically comes from software development!) Some trainers prefer to call this activity “assessing your risks” for this reason.
- People might feel overwhelmed as they consider the five threat modeling questions.

Recommended Reading

Assessing Your Risks

Lesson Content

WARMUPS

Ask learners, “What are the things you think about when…”

- You are driving your car somewhere and deciding where to park it?
- You are choosing locks or security systems for your apartment or house?
- You are deciding on a route to walk or bike somewhere?

The takeaway is that *everyone in the audience already does threat modeling in their everyday life.* The task during this module is to apply that kind of thinking to your digital security and privacy.

Alternatively, you can try this activity, inspired by Lucy Parsons Labs' training approach: Give each participant something to write on (sticky notes work well) and a pen to write with. Ask them to write down the things they are most concerned about when they think about their digital privacy and security. Questions to start them off could include:

- What made you want to come to this workshop today?
- What questions do you want answered?

Depending on the setting, you can go around the group and have participants share one or two things they wrote down, or collect the sticky notes and review them yourself.

KNOWLEDGE SHARE

Start with presenting the five questions:

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

Go through each of the questions one at a time, with pauses to define the terms learners will need to be familiar with to answer each of the questions.

- What do I want to protect? These are **assets**.
- Who do I want to protect it from? These are **adversaries**.
- How bad are the consequences if I fail? These are potential **threats**.
- How likely is it that I will need to protect it? This depends on your adversary's **capabilities**.

For each of these four questions, encourage learners to name examples of the bolded terms. For example, what are some assets that you have? Who are some adversaries you can imagine? And so on for each of the questions and terms.

- How much trouble am I willing to go through to try to prevent potential consequences? This is your appetite for **risk**.

Now take a step back to talk about why, even though each of these seem like very straightforward concepts, they are actually very complicated, especially when it comes to digital security.

- When you threat model about, for example, where you want to park your car, you are dealing with known variables, places, and things.
- In the digital space, there's more uncertainty. It's harder to know exactly where different pieces of information are, or exactly what different adversaries are

capable of.

ACTIVITY

“Imagine you’re sending an email to a friend. How does that email get from you to them? Where does that email go before it arrives in your friend’s inbox?”

In a small group, you might have time to have everyone tell you their thoughts. In larger groups, you can divide learners up into break-out groups to discuss, or call on people randomly to encourage them to share.

If you have the materials—post-its, pens, etc—you can also ask learners to draw a diagram as well as tell you what they think.

After learners have had a chance to share, show them the slides that demonstrate all the places your email goes, and all the places adversaries with different capabilities can read it.