Locking Down Social Media (beginning)

Learning Objectives

Learners will:

- Be able to identify what information they want to protect on social media and from whom.
- Know the various ways that commonly used social media platforms describe important privacy settings (privacy, security, or safety settings).
- Abstractly explain the kind of changes they need to protect that information.
- Be able to explain why they may want to keep accounts on different networks separate.
- Understand why using two-factor authentication on an account could be potentially identifying.

Ratio

Instructor: Learners
1:5 (One instructor to five students)

A ratio of at least 1 trainer to 5 learners is ideal. While this module does not necessarily involve installing tools, it does involve a lot of individual questions and individual threat model considerations. Consider splitting learners into groups based on similar concerns or situations.

GOTCHAS AND PROBLEMS YOU MIGHT HIT

Different platforms: There are countless social media platforms out there, and your learners may use lots of them. If possible, try to survey your learners before the session or otherwise get a sense of what kinds of social media they use. Depending on what kind of information you can gather from your participants, give yourself a refresher on the security and privacy settings of major platforms like Facebook, Twitter, Instagram, and LinkedIn. If you have time and think your audience will be interested in it, it also

doesn’t hurt to review online dating networks like OKCupid, Tinder, and Bumble. This kind of general knowledge will help with unexpected questions and troubleshooting!

Sensitive information and identity: Sometimes, people are motivated to lock down their social media security after experiencing scary harassment, doxxing, or stalking, or after having watched a friend go through it. These stories can be hard to tell others, and going over these fears can put people into an anxious, worried place. Also keep in mind that social media, like any environment, can pose different risks depending on your gender, race, or sexuality. Women, people of color, and LGBTQ people bear the majority of online harassment. Some specific concerns to be mindful of include locational privacy, the risk of sharing a phone number, maintaining multiple accounts and identities, and online dating security and privacy.

The buddy system: Coming face-to-face with one’s online presence can be a scary undertaking. Many people very reasonably would rather not know what information of theirs is out there rather than the painful process of confronting it. If possible, encourage participants before the workshop to bring a trusted friend or family member with them. Learning that your phone number has been public this whole time, or finding a public photo you thought was private, can be intense experiences, and they can be less overwhelming with personal support nearby**.**

Recommended Reading

SSD's Protecting Yourself On Social Networks

The Smart Girl’s Guide to Privacy by Violet Blue

Hack*Blossom

https://resist.space/

Lesson Content

ICE BREAKER

“Raise your hand if you’ve used a social media platform once today. How about twice? How about three times?” Hopefully this will generate some laughs and drive home the point that it’s normal for social media platforms to be essential to people’s daily lives.

WARMUP

Have participants split into pairs or small groups and talk about their favorite use of social media. Examples could include: sharing pictures, organizing events, staying in touch with long-distance family and friends, participating in online communities, spreading their art/work/activism, etc.

KNOWLEDGE SHARE

Learning about so many different platforms with so many different settings can overwhelm your learners (and you!). Before diving into nitty-gritty settings tutorials and questions, be sure to go over more general concepts that apply regardless of platform or settings scheme. This might include:

What is personally Identifying Information (PII)?
PII, sometimes called “Sensitive Personal Information” or “Potentially Identifying Information,” is information that can be used to identify a person. It might be combined with other information to figure out someone’s location, to contact them, or to gather additional information about their life. Lots of companies collect this information for many purposes, including advertising, medical documentation, or billing. While it is difficult to control the information and data that companies collect on someone, learners can take control of the information they put out into the world on social media.

"Don’t blame yourself."
Sometimes, learners can feel shameful or embarrassed when they take the first step of identifying what they want to protect on social media. They may feel like it’s their fault, that they should have been more careful, or that they made mistakes when sharing information. As a trainer, you can reassure them that it’s not their fault. You might say something like, “I don’t want you to blame yourself for what big tech companies and social media platforms have done to your privacy.” Instead, you can help them focus on small but powerful actions they can take to reclaim their privacy.

Security and privacy “check-ups”
Facebook, Google, and other major websites offer “security check-up” features. These tutorial-style guides walk you through common privacy and security settings in plain language and are an excellent feature to take advantage of.

Privacy vs. security; safety vs. account settings
Even though every social media platform has its own unique settings, you can find some patterns.

Privacy settings tend to answer the question: “Who can see what?” Here you’ll probably find settings concerning audience defaults (“public,” “friends of friends,” “friends only,” etc.), location, in photos, contact information, tagging, and if/how people can find your profile in searches.

Security (sometimes called “safety”) settings will probably have more to do with blocking/muting other accounts, and if/how you want to be notified if there is an unauthorized attempt to authorize your account. Sometimes, you’ll find login settings--like two-factor authentication and a backup email/phone number--in this section. Other times, these login settings will be in an account settings or login settings section, along with options to change your password.

Phone numbers

When you give your phone number to a website—perhaps to send two-factor authentication codes, or to reset your account—some websites have a tendency to fill in your phone number in other places. On Facebook, this could mean others can look you up in search by your phone number. On other sites, it could mean your phone number is public without you knowing it. It’s easy to overlook, but since your phone number is a potentially identifying piece of information, this is one of the first things to lock down.

Location

Location settings help you make sure that you don’t accidentally share where you are. Some sites will include your approximate location by default when you post things. Location information can paint a detailed picture of your habits, home, and workplace, so it’s important to turn off if it’s leaking information that you feel uncomfortable with.

Photos

Photos can share more information than meets the eye. In addition to metadata that might include the time and place a photo was taken, the image itself can provide some information. Before you post a picture, ask: Was it taken outside your home or workplace? Are there any addresses or street signs visible in it? If you post photos often at certain times of day, does it make it easy to figure out what your routines and habits might be?

Photos can also link accounts you intend to keep separate. This is a surprisingly common issue with dating sites and professional profiles. If you want to maintain your anonymity or keep a certain account’s identity separate from others, be sure to use a photo or image that you don’t use anywhere else online. To check, you can use Google reverse image-search function.

Making sure different profiles don’t get linked together

For a lot of us, it’s critical to keep different account’s identities separate. This can apply on dating websites, professional profiles, anonymous accounts, and accounts in various communities. In addition to phone numbers and pictures, other potentially linking variables to watch out for include your name (including nicknames) and your email. If you discover that one of these pieces of information is in a place you didn’t expect it, it can be easy to get scared or panic. It can be useful to think in baby steps: instead of trying to wipe all information about you off the entire Internet, just focus on specific pieces of information, where they are, and what you can do about them.

Group settings

Facebook groups are increasingly places for social action, advocacy, and other potentially sensitive activities, and group settings can be confusing. If participants are interested in learning more about group settings, refer to this guide for more information.

ANTICIPATED QUESTIONS & ANSWERS

When you ask learners to think about what they protect on social media, they can very quickly fall into “security paralysis” or “security nihilism.” A learner might say something like, “It’s impossible to lock everything down and I have no idea where to start. I can’t even think of what to do next.” or “What’s the point of even trying? Privacy settings will change, information will leak, and it’s all outside my control.”

One good response is to manage expectations. It’s impossible, whether in a phonebook world or a social media world, to lock down every single piece of information about us, and that’s okay. Lots of things are outside our control online, and that’s okay too. It’s not about bringing the amount of information about us online to zero; it’s about minimizing the most important information. 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 public information that we have control over, then we are in a much more powerful position if and when settings change or we make a small slip.