Two-Factor Authentication (intermediate)

Two-factor authentication (also called “2FA”) is one of the simplest things users can do to protect their accounts. Teaching 2FA can sometimes be tricky, though. For different services, you’ll encounter different language and workflows enabling 2FA, and not all apps work for all services. We’ll help you navigate this tricky landscape in a way that won’t confuse your learners or cause them to lose interest.

Recommended Reading

How to: Enable Two-Factor Authentication

https://2fa.directory

A Guide to Common Types of Two-Factor Authentication on the Web

The 12 Days of 2FA: How to Enable Two-Factor Authentication for Your Online Accounts

Gotchas And Problems You Might Hit

The biggest challenge with two-factor authentication is that, while the idea and practice both seem straightforward, there are lots of distracting side issues.

- When teaching the concept, there are plenty of systems that seem like 2FA to a learning user, but aren’t—including account recovery, **password** resets, out-of-band messaging, and security questions.
- Many services have a different name for “two-factor authentication,” which means identifying and finding it can be hard. Some of these include “multi-factor authentication,” “two-step verification,” and “login approvals.”
- Services often bury how to turn on 2FA and it’s not in a consistent place.
- 2FA can fail in ways that block you from accessing your account, for instance, if you don’t have your phone.

- 2FA can be implemented in ways that don't protect you against certain attackers—for example, when authentication codes are sent via text message and your attacker has control of the phone system.
- 2FA apps can be interchangeable, so there is often not a "right" one to choose.

It's better to emphasize strategies that empower the learner, rather than tell them about problems they will have no control over.

- Concentrate on how to spot "two-factor-y" terms, not a particular process.
- Emphasise 2FA as "an extra step"—not perfect (because pretty much all 2FA systems have some workaround), and not absolutely required, but still an improvement on just using passwords.

- Guide the learners to resources they can use as a reference for enabling 2FA on their accounts—such as https://2fa.directory.

You don't have to talk about all the failure modes of 2FA. Talk about what it stops, not what it fails to do.

Anticipated Questions and Answers

Q: How do I turn on two-factor authentication for [insert service here]?

A: "Let's take a look at https://2fa.directory … " (either walk them through it or offer to help afterwards, depending on the structure of your training.)

Q: What happens if I'm travelling / lose my phone / don't have the module?

A: If you have your phone but no service, you will still be able to use your authenticator app. Otherwise, many websites will let you save and print out "backup codes." When you don't have your phone or can't receive texts, you can use one of the hard-copy codes instead of the code you would usually get texted to you or grab from your authenticator app. Each code is for one-time use only. Whether you print them out or save them to your computer, make sure you keep them in a safe place where you won't lose them, forget them, or risk them being found and stolen by someone else.

Q: I hate doing this every time! (*Not technically a question, but we hear it a lot.)*

A: You can usually set up two-factor so that it will only ask you every so often. Look for the check box next time you log in.

Q: I've heard that two-factor authentication was bypassed in [this incident].

A: This is almost always a story of either the phone system being hacked (redirecting or intercepting text messages via the SS7 system) or an attacker calling customer support at a carrier and tricking their way into accessing someone else's text messages. Or, the account recovery process was less secure and used to bypass the usual login system.

If you don't use text messages and use an authenticator app or hardware token instead, you don't have to worry about this!

If you do use text messages, you may still be okay. For someone to successfully bypass your text message-based 2FA, they would have to 1) know your password and 2) spend significant amount of time and energy targeting you specifically. If you are worried about being targeted individually, then text message-based 2FA may not be right for you. But, if the chance of that kind of targeted **attack** is small enough, text message-based 2FA may still be a perfectly reasonable choice.

Remember: no security is perfect, and text message-based 2FA is no exception! Rather than focusing on its imperfections, think about its benefits and drawbacks and how those tradeoffs matter to your own specific situation.

Q: Why don't services just ask for a second password instead of having to use your phone? That's two-factor, right?

A: Explain that this doesn't fall into the "something you know, something you have" framing, and that it poses similar risks to someone stealing a password.

Q: Why would I trust a service like Google Authenticator? I don't want them to see my two-factor codes.

A: It's true that Google could, in theory, put out a new version of their tool that gives them the ability to generate your two-factor codes, but it's unlikely they would. These companies built authenticators specifically to protect their own services, so they would be undermining their own security by doing this. It's also not enough—remember: they'd need to know your password too. There are also open-source alternatives to Google Authenticator that you can use if you *really* don't want to use Google Authenticator, such as FreeOTP.

Q: How does a service like an authentication app work? Or, how does TOTP (time-based one time password) work?

A: This is an advanced question that may best be answered separately, rather than to the whole group. You can refer the asker to this discussion thread.

Learning Objectives

Learners will:

- Be able to find the **two-factor authentication** settings page for a service they use.
- Turn on two-factor authentication for one of their services.

Understanding two-factor authentication is potentially a lecture-format discussion.

Finding the two-factor authentication settings page for each individual service can be difficult, so benefits from having helpers to assist learners (1 helper to 5 students) is helpful.

Turning on two-factor authentication will require closer pairing, similar to installing an app (1 helper to 1-2 students).

Recommended Reading

How to: Enable Two-Factor Authentication

https://twofactorauth.org/

A Guide to Common Types of Two-Factor Authentication on the Web

The 12 Days of 2FA: How to Enable Two-Factor Authentication for Your Online Accounts

Lesson Content

Activity: Turning on 2FA

Point the group to EFF's “12 Days of 2FA” post.

The learners should be able to choose an account from the list and visit the page of instructions to turn 2FA on for that account. If they do not have any account with a

company/platform listed on the page, it may be worth guiding them through the 2FA instructions manually for an account they do have.

Optional Closing Activity

Go on a two-factor authentication adventure! Go to Facebook, or some other site, and try to find the 2FA option.