# Two-Factor Authentication (beginning)

## Learning Objectives

Learners will:

- Understand what two-factor authentication is and how it helps protect accounts from unauthorized access.
- Know the various ways two-factor authentication is referred to.
- Be able to tell the difference between a two-factor authentication app and receiving codes via text message, and will be able to describe the pros and cons of each.

## Ratio

Instructor: Learners
Varies

The knowledge share is potentially a lecture-format discussion.

Finding a two-factor authentication page benefits from having helpers (1 helper to 5 students).

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

### GOTCHAS AND PROBLEMS YOU MIGHT HIT

The biggest challenge with two-factor authentication (also called “2FA”) 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 two-factor authentication, 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 defend you against certain attackers. For example, when authentication codes are sent via text message and your attacker has control of the phone system.

It's better to emphasize strategies that empower the user, 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.

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

### 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

#### KNOWLEDGE SHARE

Some services offer "two-factor authentication," which is to say they can be set up to ask for something else other than a password.

Usually, they ask for a number or code that they've texted separately, or ask you to use a separate app that helps to verify your identity. It demonstrates that not only do you know your password, but you also have access to something—like your phone with the right phone number, or an app you set up previously.

This protects you against passwords getting stolen. Even if someone gets your password, they won't be able to get into your account without also having your phone.

**CAUTION!** If you use the kind of 2FA that texts a code to your phone, you will need to give the service or platform your phone number—or, at least, a phone number at which you can reliably receive texts. For some people, this may not be the right choice. For example, Twitter only supports 2FA by text. Twitter is also a popular platform for anonymous accounts. If you want to protect the anonymity of your account, or if you want to prevent several different accounts being linked together with common information, you may not be comfortable giving Twitter your phone number.

**ACTIVITY: "The Annoying Security Guard"**

Ask the attendees, "Has anyone been in a situation where they are supposed to be let into a party, or an office, or an event, but there's a bouncer or security guard or official who is really demanding and doesn't believe you?

Pick someone to be the "anoying security guard," or, if you have a small group, encourage everyone to be the "guard."

"I'm going to try and prove that I should be allowed past you. Whatever I say, you should come up with a reason why that isn't enough and you can't let me in. My name really is on the guest list though!

"Hello, my name is XXX, and I've come here to teach people about digital security. Do you see my name on the list?"

The guard should make up a reason like "I don't see your name," or "How do I know it's really you?" Go through, in turn, other possible identifications, each more ridiculous: "Well, here's my credit card, it's got my name on it," or "Here's my passport, there's a photo of me," or "If you ask anyone who knows me, they know I'm a really good dancer, so here's my signature dance," or "Here's an Instagram photo of me with your boss," etc.)

What this shows is that there is no single perfect way to prove your identity, but the more ways in which you can prove you are who you say you are, the more likely it is to

be true. The security guard isn't wrong to be skeptical. Eventually, the weight of the evidence reasonably proves someone is who they claim to be.

Once you're done with the "annoying security guard" activity, explain how this relates to the lesson:

"Now apply this to logging into an account. Most log-ins only ask users to prove their identity in one way: passwords. The problem with passwords is that someone else might get ahold of them. That's what the annoying security guard would say.

"You've all run into this in other parts of life. An ATM is a great example: you need both your pin number and your card to be allowed to withdraw or deposit money. Someone else could find out your pin or they could steal your card, but it's less likely that they will be able to do both.

"So two-factor just means 'something other than the password, as well as the password.' Your password is your first 'factor' of identification, and then you need to provide one more to be let in."

Ask: "What other things could a website ask you for when you log in?" Emphasize that it has to be in addition to a password.

**ANTICIPATED Q&A'S AND HOW TO NAVIGATE THEM**

**Q:** How do I turn on two-factor authentication for [insert service here]?
**A:** "Let's take a look at https://twofactorauth.org/ … " (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, 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:** Some services recommend having a second password. 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.

**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.