Loose Leaf Security

presents

Two-factor authentication

A zine about making
good computer security
for everyone

by Liz Denys &
Geoffrey Thomas

version 1.0.xoxo
updated 2018.08.31

In summary, when evaluating the 2FA methods available for your accounts, ask the following questions:

1. Which two-factor methods are available?
   - Phone-based? ↓ ***weaker***
   - Email-based?
   - Push notifications?
   - Authenticator apps?
   - U2F/WebAuthn security keys? ***stronger***

2. If I have multiple accounts with this service and need to use phone-based 2FA methods, will I be able to use my phone number for all of them?

3. Can I use multiple types of strong second factors? *e.g. authenticator app on phone + security keys*

4. Do I have a backup 2FA method available to me? *e.g. an authenticator app on an old phone or a second security key*

5. Are there backup codes and how do I get them? How do I re-generate backup codes? How do I invalidate old ones?

6. What if I lose access to my account? Can customer service reset it? *Do I want them to be able to?*

This zine just scratches the surface of two-factor authentication. To learn more about two-factor authentication and other personal security topics, check out https://looseleafsecurity.com/2fa   <3 Liz & Geoffrey *getting just your password, but if someone gets into your password manager, they'd have both factors. If you're more worried about losing access than someone breaking in, it's better than no 2FA but not by much.*

Also, *sometimes* customer service will let you back into your accounts, but you can't always count on it!

The best solution, though, is to not have to deal with backup codes and have multiple forms of 2FA available to you. ✨

- An **old phone with an authenticator app** makes a handy backup. Scan the QR codes at the same time with both your current and old phones when setting up 2FA, and they'll generate the same codes! Then, leave it somewhere safe.

- If you want to be using only hardware security keys for some accounts, **get a second backup security key**, set it up, and leave it somewhere safe.

Pro tip: this is also great for setting up 2FA when you're collaborating. Meet up with your project partners, and scan the QR codes together! :)

Why use 2FA?

When you use two-factor authentication (2FA for short), anyone trying to get into your account has to go through two layers, instead of just the single layer of your password, to gain access to your account.

This is especially helpful since lots of modern attacks aren't from a **specific** person trying to get in **your** account, but an attacker with a list of passwords from a breach - they'll try them on the site from the breach and try your credentials on other sites, too, because lots of people reuse passwords.

But...

If an attacker can't get in with just your password, you're a little more protected ~~if~~ when your information is leaked.

Shoutout to password managers, which make it easy for you to have unique, strong passwords for everything.

What is 2FA anyway?

That extra security layer needed is another factor! So... **what's a factor?** A way of demonstrating who you are. In high security environments, people consider three types of factors:

Something you know

- e.g. PINs, passwords*
- Pain to remember so humans are tempted to pick passwords that can be guessed easily, can be leaked/breached

Something you have

- e.g. a badge, your house key
- Can get lost or stolen, but you'll likely notice it's missing

Something you are

- e.g. fingerprints, Touch ID, Face ID, retina scans
- Hard to duplicate, expensive, impossible to change, *technically* gets leaked all the time (you leave your fingerprints everywhere)

But most of us aren’t walking into top-secret buildings daily, so we probs don’t need all three types of factors. However, **we can pretty easily use 2FA:**

something we know: our password
+
something we have: usually, our cell phone or a special security key

This all sounds great but...

What if I lose access to my 2FA? 😱 😱 😱

Typically when you enable 2FA, you'll get a list of **backup codes** to use that will bypass 2FA, should you ever lose access to your second factor. Since these codes bypass your second factor, they're *really powerful* and should be kept in a safe place. Unfortunately, there's not a perfect answer to where that safe place is. Some common places to keep them:

- a physically safe place at home
  e.g. with your birth certificate & passport

- your wallet
  Your wallet could get stolen, but you'll probably notice when it does so you can get new codes/invalidate the old ones fast.

  Be careful if you carry your phone with an authenticator app or your security key in the same place so you don't lose both your 2FA and its backup codes at once.

- your password manager
  Reduces the level of security you have: you are still protected from someone

*If you're using a password manager, then this isn't *exactly* something you know. The something you know is your password manager's master password to unlock the specific password.

BTW, we're really stoked about initiatives to *replace* passwords w/WebAuthn security keys in certain situations bc security keys as your only factor is more secure than a password as your only factor! \o/

So I should just use security keys all the time because they're the most secure 2FA method, *right?*

Unfortuntely, not all accounts/services support all these options, so it's not quite that simple. But **you should use the strongest form of two-factor available that works in your workflow.**

There's two super handy resources you can use to figure out what 2FA methods are available for your accounts:

- **twofactorauth.org**
  a crowd-sourced resource of who supports which types of second factors
- **your password manager, possibly!**
  1Password's Watchtower has a section called "Inactive 2FA" which shows you accounts you have stored passwords for but don't have 2FA on. Or maybe you have 2FA on but 1Password doesn't know you do,* in which case you can tag the account "2FA" to let 1Password know!

*1Password doesn't know about your 2FA unless you have its 2FA configured in 1Password. It is more secure to use a separate authenticator app in case 1Password is breached.

2FA methods, tag yourself!

Very insecure, but probs better than nothing … maybe.

SMS texts

*A code is texted to your phone to use to complete login. Convenient, but your phone number is **pretty vulnerable** to attacks**

- kind of insecure
- excited about meeting new people
- hasn't talked to most of their friends in years, but cares about them v. deeply

*SMS is *not* an encrypted protocol and can be snooped on; also SIMjacking is always a threat

Phone call

You get a call that has a code to enter. Similar level of security to texts, but also works on non-cell phones. Also, really interruptive.

- never wears white after Labor Day
- taxes done by February 1
- tried to get a millennial to explain Snapchat to them once, but didn't get it

Authenticator app on desktop

*See Authenticator app on phone for how this works. Your desktop/laptop/PC is **substantially** less secure than your phone in general.*

- still runs Windows XP bc it's the best OS
- cleverly hides a spare house key under the front door mat
- writes "Check ID" instead of signing their credit card

more secure methods on the next page

More secure methods to use:

increasingly secure as you go down the page

Email

A code is emailed to you to use to complete login. Easy, but not really adding security as most accounts can be reset over email.

- hip to the latest trends… from 5 years ago
- knows all the best gossip
- doesn't bother to lift their sunglasses off their eyes when they get on the subway

Push notifications

An app on your phone alerts you to approve or deny it, usually with a some info about where the request is coming from. Easy to use, not widely available. Need to be careful not to accidentally tap accept when it's not you.

- really outgoing
- feeds your fomo
- gets mad when you don't reply on group chat

Authenticator app on phone

e.g. Duo Mobile, Google Authenticator (Maybe your password manager has one, but then it's not technically a separate factor.)

Scans a QR code to set up. When you login, click to generate a changing 6-digit value to use.

- pan
- stares at art in a museum for at least 10 minutes but can't distill their feelings about it into more than one word at a time
- always knows about the hip, new restaurant in your neighborhood

even *more* secure methods on the next page!!

The *most* secure methods to use:

hardware security tokens!

increasing levels of security

Hardware code generator

No potential malware risk like with authenticator apps, but each device can only work with one login so it's not the most practical for personal use since you probs have lots of accounts. Most commonly used by businesses.

- my job is to deliver business value
- nothing gets past my hard shell
- when I die, they'll just replace me :(:(:(

Security key

e.g. Yubico's YubiKeys*, Feitian MultiPass FIDO Security Key.

Uses the U2F/WebAuthn key standard with a supported web browser to do a handshake with the website you're authenticating to.

✦ **You're protected from phishing sites because they can't do the handshake.** ✦

Not all phones support these right now, and you need to think about what USB inputs you have across all devices.

- knows that black is always in fashion
- has a small group of core friends that are extremely good at keeping each other's secrets
- has a skincare routine and sticks to it

*A brief warning that some YubiKey Nanos have an OTP function that can accidentally make it look like you just got a cat! Some models default to generating an OTP whenever you touch it and it's not doing a handshake with something - yikes! Yubico recommends using the YubiKey Personalization Tool to swap it to Slot 2 or using their command line tool to disable it.