



Passwords and two-step verification

How to lock the door on your accounts properly, without memorising anything

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Contents

How to use this handout 3

1. Why the password is the weak spot 3

1.1 The case of Marta and the dance school 4

1.2 How passwords get stolen 5

2. How to build a good password 6

2.1 The long passphrase 6

2.2 What to avoid 7

2.3 Change it every three months? Not any more 8

3. One password per service: the manager 9

3.1 What it does, in practice 10

3.2 Which one to choose 11

3.3 The case of Luca's office 11

4. Two-step verification 12

4.1 The methods, from weakest to strongest 13

4.2 When requests arrive that you did not make 14

5. Where to turn it on first and how not to get locked out 15

5.1 A practical order 16

5.2 Plan B: recovery codes 16

5.3 The case of the lost phone 17

Practical exercise 19

Questions that come up in class 20

Glossary 21

Further reading 21

How to use this handout

This handout gathers, in written and ordered form, everything covered in the lesson. You do not need to memorise it: it is there so you can find things again calmly, later, when the lesson is over and a question is left hanging.

> **GOAL**
>
> Learn to build long passwords that are different for every service, keep them in a password manager, and turn on two-step verification for the accounts that really matter.

What you will be able to do

- Recognise why a short, predictable or reused password is a risk.
- Build a long passphrase that is easy to remember and hard to guess.
- Use a password manager to have a different password for every service.
- Turn on two-step verification and choose the method that fits best.
- Know how to get back into an account if you lose your phone.

1. Why the password is the weak spot

You can have the most up-to-date computer in the world: if your password is «office2024», the door is wide open.

A **password** is the key a service uses to work out that it really is you. Email, the school register, the invoicing software, online banking: every door has its own key. And the everyday problem is that there are many keys and only one memory.

So we do what almost everyone does: we pick an easy password and use it everywhere. Maybe with a number on the end, to satisfy the «at least one digit» rule. It is convenient. It is also the fastest way to get an account stolen.



A reused password links the security of different accounts.

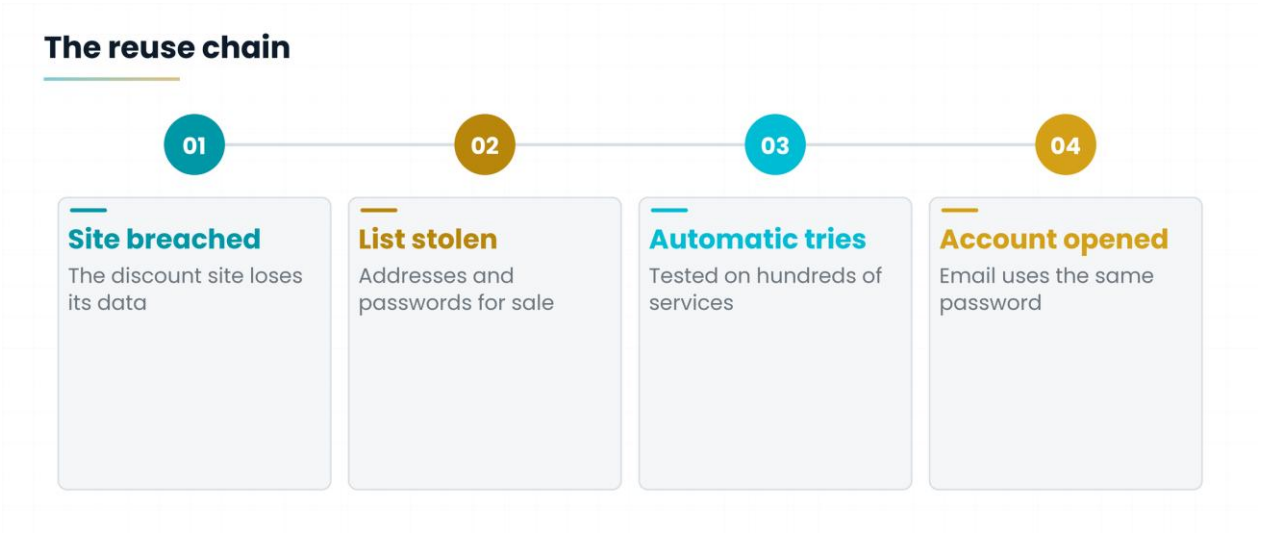
1.1 The case of Marta and the dance school

Marta works in the office of a small dance school. Years ago she signed up to a discount site for sportswear, using the same email address and the same password as the school's mailbox. One day that discount site is breached: thieves walk away with the list of subscribers' email addresses and passwords.



Credentials stolen from one site get tried on other services.

Nobody warns Marta. A few days later, though, an automated program tries that pair of details on hundreds of other services, one after another. On the school's mailbox the password works. From there, the thieves read the emails, see the lists of enrolled students and write to the parents pretending to be the school office.



How a reused password opens accounts that have nothing to do with it

THE IDEA IN ONE LINE

A reused password is only as strong as the **weakest site** you have used it on.

1.2 How passwords get stolen

You do not need a computer genius. There are only a few methods, all very common:

- **theft from a breached site:** lists of passwords end up for sale or online, and are tried on other services (this is called *credential stuffing*);
- **guessing at speed:** a program tries the most common passwords in the world, and dictionary words with a few digits added;
- **phishing and fake sites:** you type the password into a fake page yourself (lessons three and four of the course);
- **spy programs:** a keylogger records the keys you press (lesson two);
- **prying eyes and sticky notes:** the password written on a note under the keyboard, which anyone passing by can read.

Notice something: against four of these five methods, a more complicated password is not enough. That is why the second half of this lesson covers two-step verification.

2. How to build a good password

For years we were taught to write ugly, difficult passwords. The good news is that today the advice is the exact opposite.

A password like «Xk9#pL2!» is hard for you and fairly easy for a program, because it is short. What really counts is **length**: every extra character multiplies the work needed to guess it. So the practical rule is to reach at least **twelve to fourteen characters**, and better still to make it a phrase.

2.1 The long passphrase

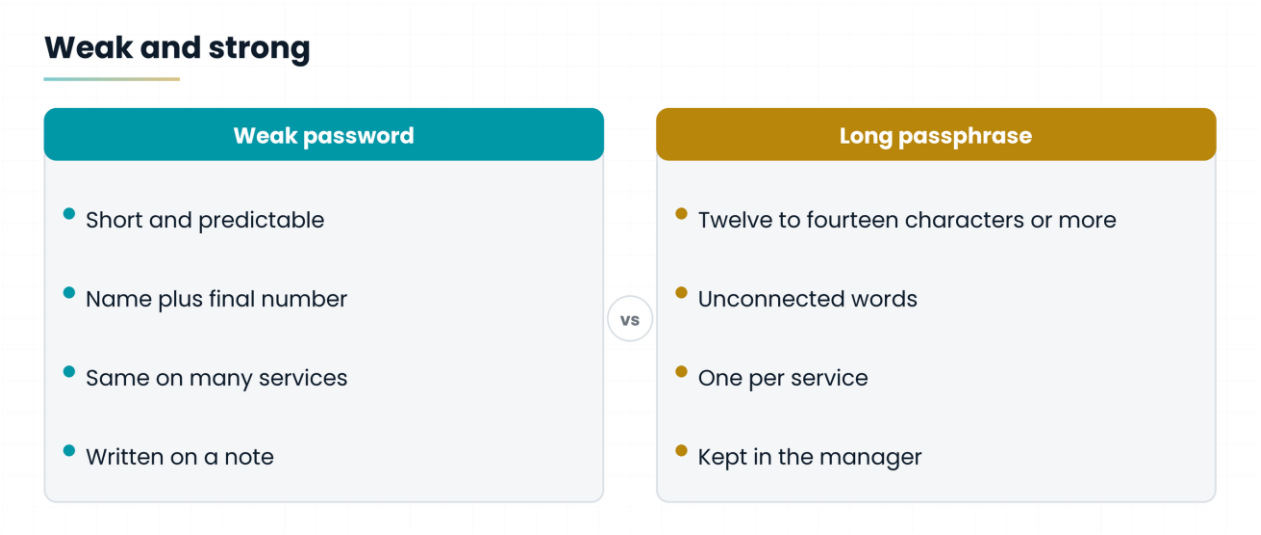
A long phrase is a password you can remember because it makes sense, but nobody can guess because it is yours. An example like «Il-giovedi-porto-il-caffe-in-ufficio!» (in English: «On-thursdays-i-bring-coffee-to-the-office!»): seven words, six hyphens, one exclamation mark. Easy to remember, long, and not a dictionary word.

> **DO NOT COPY THE EXAMPLE**
>
> A phrase printed in a handout, on a website or on a slide is a phrase that **everyone knows**. Use it only to understand the method, and invent your own, one you have never read anywhere.



Pick a long, unique phrase and do not copy the examples.

How do you invent one? Think of a vivid, slightly absurd picture and write it as words separated by hyphens or spaces. For example: «three-cats-eat-a-pizza-on-the-tram». It is not a saying, it is not connected to you, but you can picture it instantly.



A weak password and a long passphrase compared

2.2 What to avoid

Choice	Why it is a risk	What to do instead
Name, birthday, the dog's name	Found on social media or guessed with two questions	A phrase with no link to your life
A common word plus a number («Summer2026»)	It is the first thing programs try	Several unrelated words
Obvious swaps («p4ssw0rd»)	Programs know them and try them	Length, not disguises
The same password everywhere	One breached site opens all the others	A different password for every service
The note under the keyboard	Anyone passing the desk can read it	A password manager (see below)

The most common choices and why they do not work.



Names and public dates are predictable choices.

2.3 Change it every three months? Not any more

Maybe in some offices you are forced to change passwords all the time. The most recent digital identity guidelines from the US body NIST (National Institute of Standards and Technology, the institute that sets technical standards in the United States) no longer recommend this as a fixed rule: people forced to change often tend to make tiny changes («Summer1», «Summer2») that protect nothing.

The common-sense rule is this: **change the password at once** if you suspect it has been stolen, if a service warns you about a breach, or if you have given it to someone. Otherwise, a long and unique password can stay where it is.



Change it if it is compromised or the service reports a breach.

> **CHECK WHETHER YOU ARE ALREADY ON A LIST**
>
> There is a free and well-known service, *Have I Been Pwned* (haveibeenpwned.com), where you enter your email address and see whether it appears in data breaches that are already public. If it does, it is not a tragedy: change the password for that service and for every other one where you reused it.

3. One password per service: the manager

You have twenty accounts and one memory. Let something that never forgets do the work.

A different password for each service is the only way to break Marta's chain. But nobody can remember twenty long, different phrases. This is where the **password manager** comes in: a program, or a browser feature, that keeps all your passwords in an encrypted vault.

You remember **just one** password, the master password, which opens the vault. The manager picks and fills in all the others, and they can be long and random, because you do not have to learn them.



An encrypted vault keeps a different credential for every service.

3.1 What it does, in practice

- **creates** long, random passwords when you sign up to a service;
- **remembers** them and fills them in for you on the right site, on computer and phone;
- **warns you** if a password is weak, reused or appears in a known breach;
- **also stores** other sensitive items: recovery codes, notes, sometimes your card details.

There is a less obvious and very useful bonus: the manager fills in the password **only on the right site**. If you land on www.ente-esempl0.it, a fake site like those in lesson four, the manager does not recognise the address and offers nothing. That silence is an alarm bell.



If the expected autofill does not appear, check the domain.

3.2 Which one to choose

Type	Strengths	Limits
Browser manager (Edge, Chrome, Firefox)	Already installed, convenient, free	Works best inside that browser; protecting access to your profile matters a lot
Dedicated manager (app or extension)	Works everywhere, family or office sharing, fuller controls	Has to be installed and often costs money, especially for teams
System manager (phone, computer)	Integrated with fingerprint and face	May tie you to a single device maker

Three possible routes: the best is the one you will actually use.

I will not give you a product name, because offers keep changing. I will give you the **criterion**: look for a manager from a well-known provider, with an encrypted vault, that works on the devices you use and can turn on two-step verification for its own login.

3.3 The case of Luca's office

In a small accounting firm, four people shared the login for the deadlines portal, with a note stuck on the monitor. When a colleague left, nobody changed anything: she still had access, and nobody could say who had done what.

With a password manager that supports sharing, each person has their own login. You decide who sees which credentials, and when someone leaves you change the shared password in a moment. For an office with several people, it is far better than any note.

> **THE MANAGER'S LIMITS**
>
> If you lose the master password, in most managers **nobody can recover it for you**: it is a consequence of encryption. Write a reminder and keep it somewhere safe, for example in a sealed envelope in a safe. And protect access to the manager with two-step verification.

4. Two-step verification

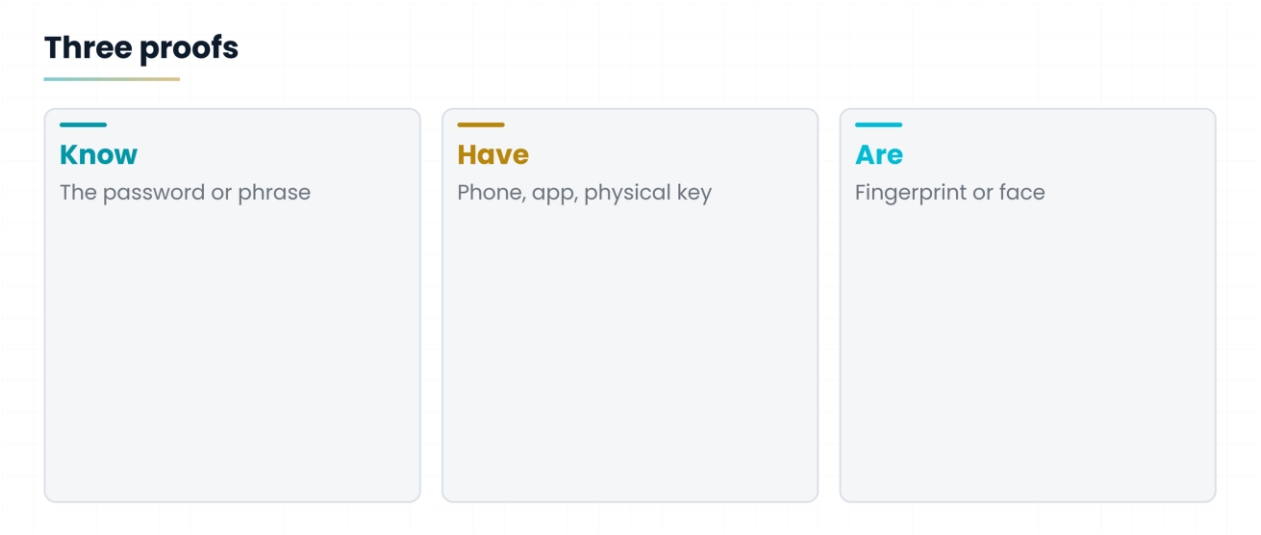
A password can be stolen. The second step makes it far less useful to whoever stole it.

Two-step verification (also called multi-factor authentication, abbreviated MFA) means that a password alone is not enough to get in: you need a second element, different from the first. Even if a thief knows your password, without the second element they stay out.



Something you know, something you have, something you are.

In practice you combine two things from different families, out of three: something you **know** (the password), something you **have** (the phone, a physical key), something you **are** (a fingerprint, your face).



The three kinds of proof that show who you are

4.1 The methods, from weakest to strongest

Method	How it works	Strengths and weaknesses
Code by text message	You get a code on your phone and type it in	Better than nothing. But a text can be intercepted, and a fraudster can talk you into reading out the code
Authenticator app	An app on your phone generates a code that keeps changing	Safer than text, works without a signal. If you change phone it must be moved carefully
«Approve» notification	Your phone asks you to confirm the login	Very convenient. Be careful not to press «approve» if it was not you
Fingerprint or face	The device recognises you	Fast. Usually unlocks one device, not the account everywhere
Physical key or passkey	A small USB key, or an identity saved on the device, proves it is you	The most robust method, because fake sites cannot trick it. Takes a little getting used to

Pick the most robust one the service offers.

A **passkey** is a credential that replaces the password: instead of typing something, you confirm with your fingerprint, face or the device's unlock code. A fake site cannot steal it, because it only works with the real site. More and more services offer it: if you see it, try it.



The methods do not all resist phishing equally.

NOBODY WILL EVER ASK YOU FOR THE CODE

A bank operator, a helpdesk colleague, a courier: **nobody** needs the code you receive on your phone. If someone asks for it, even in a friendly voice, they are a fraudster (*vishing*, the phone scam from lesson three). The code is not read out, not forwarded, not photographed.

4.2 When requests arrive that you did not make

If an approval request shows up on your phone when you did nothing, it means someone has your password and is trying to get in. Sometimes fraudsters send dozens, hoping you will press «approve» out of exhaustion. **Decline**, and change that account's password straight away.

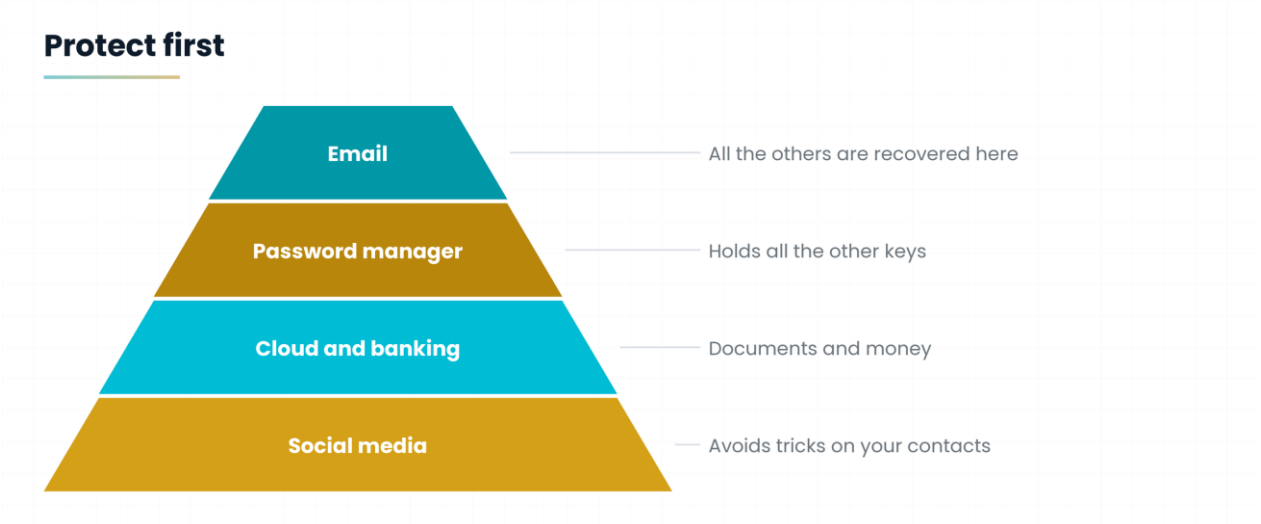


Do not share codes and do not approve unexpected requests.

5. Where to turn it on first and how not to get locked out

You do not need to turn on everything today. You need to turn on the right things, in the right order.

Fraudsters' first target is **email**. The reason is simple: almost every service, when you forget the password, sends the reset link to your email address. Whoever controls your email controls, in a cascade, everything else.



The order in which to protect your accounts

5.1 A practical order

1. **Email,** personal and work.
2. **The password manager.** If it is well protected, everything else is too.
3. **The cloud and your documents** (the online storage where you keep files and folders).
4. **Banking, payments and public portals,** such as the private area of the Agenzia delle Entrate (Italy's tax authority) or the services you use with your digital identity.
5. **Social media and the rest.** Even a stolen social profile helps fraudsters deceive your contacts.



Start with email, then protect your other important accounts.

The option is usually in the account settings, under an entry called «Security», «Two-step verification» or «Multi-factor authentication». The names vary from service to service, but the path is always similar: choose the method, scan a code with the app or confirm on your phone, and you are done.

5.2 Plan B: recovery codes

When you turn on two-step verification, the service almost always gives you **recovery codes**: a short series of single-use codes to use if you lose your phone. They matter more than they seem to.

- print them or write them by hand and **keep them away from the computer** (a safe, a locked drawer);
- or save them **in your password manager**, if you protect it with strong verification;
- do not leave them in a random file on the desktop, and do not photograph them on your phone, where they end up in the automatic backup of everything else.

5.3 The case of the lost phone

Giulia, a secretary at a middle school, loses her phone on the bus. It holds the app that generates the codes for the school's email. If Giulia kept her recovery codes, she logs in with those, removes the lost phone from the list of trusted devices and links a new one. If she did not, she has to go through support, with delays and documents to provide.



Keep recovery codes in a safe place.

The lesson: two-step verification protects you, but you must prepare plan B **beforehand**. A few seconds of organisation today, whole working days saved tomorrow.



Secure your accounts

IN SHORT

A long password, one per service, in a manager; two-step verification on email, cloud and banking; recovery codes somewhere safe.

Practical exercise

A short exercise to do at your own computer, with what you already have: your email and your phone.

1. On a sheet of paper, list (service names only, **never the passwords**) the five most important accounts you use: email, cloud, banking, work software, social media.
2. Open haveibeenpwned.com and check your email address. Note whether it appears in any breach.
3. Invent a new long phrase of your own, at least four words, and use it as the master password of a manager (the browser's one is perfectly fine to start with).
4. Go into your email settings, look for «Security» and turn on two-step verification, choosing the authenticator app if available.
5. When the service offers recovery codes, save them somewhere safe and away from the computer.
6. Pick a second account from your list and repeat: change the password to a long one and turn on the second step.

> **CHECK YOU DID IT LIKE THIS**
>
> Is the master password a phrase you have never read elsewhere?
>
> Are the recovery codes away from the computer?
>
> Have you turned on the second step at least on your email?
>
> Can you say what you do if you lose your phone?

Questions that come up in class

Isn't a password manager like putting all your eggs in one basket?

In part, yes, which is why the vault is encrypted and must be protected with a long master password and two-step verification. But the fair comparison is with the real alternative: weak, reused or handwritten passwords. For the vast majority of people, a manager is far safer than what they do today.

Is a text message useless as the second step?

No, it is much better than nothing. It is the weakest of the available methods, because it can be intercepted or talked out of you. If the service offers an authenticator app or a passkey, choose those. If only text is available, turn it on anyway.

How long should my password be?

At least twelve to fourteen characters; better, a phrase of four or five words. Passwords generated by the manager can be even longer, because you do not have to remember them.

Can I use the same phrase with a small variation for each site?

That is a bad idea: if a thief sees the variation on one site, they will guess it on the others. Every service deserves a different, independent password, and that is exactly the manager's job.

I lost the phone with the code app: am I locked out of everything?

If you saved the recovery codes, no: you use them to get in and link the new phone. If you did not, you must go through each service's recovery procedure, which can take time and checks. That is why it pays to prepare them right away.

Can I share my password with a colleague while I am on holiday?

Better not: a shared login no longer says who did what. If needed, use the sharing feature built into the manager, or ask your manager to create a dedicated login for her.

Glossary

Term	What it means
Credential stuffing	An automated attempt to use passwords stolen from one site on many other services.
Keylogger	A spy program that records the keys you press to steal passwords and card numbers.
MFA (two-step verification)	Besides the password you need a second element: an app code, a fingerprint, a physical key.
Passkey	A credential that replaces the password: you confirm with fingerprint, face or the device unlock.
Passphrase	A password made of several words, easy to remember and hard to guess.
Password	The secret key a service uses to work out that it really is you.
Password manager	A program that keeps all your passwords in an encrypted vault and fills them in for you.
Recovery codes	Single-use codes supplied by the service to get back into the account if you lose your phone.

Further reading

NIST, Digital Identity Guidelines (Special Publication 800-63B) - guidance on minimum length (at least 15 characters when the password is the only factor) and on changing only when necessary

Have I Been Pwned (haveibeenpwned.com) - free service to check whether an address appears in known breaches

FIDO Alliance, information on passkeys - description of how they work and their benefits

Agenzia per la cybersicurezza nazionale (acn.gov.it) - Italy's national cybersecurity agency: awareness materials on safe account use

> **WATCH OUT**
>
> Information up to date as of October 2026. Menu names and security settings in online services change often: if you cannot find an option, search for «security» in the account settings. Italian references: the Agenzia delle Entrate is Italy's tax authority; the Agenzia per la cybersicurezza nazionale is Italy's national cybersecurity authority. The US body NIST is cited for its widely used guidelines.