



Backup and the 3-2-1 rule

How to never lose your data, whatever happens

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



Contents

How to use this handout 3

1. Why a backup, and what it really is 3

1.1 Four ways to lose your data 4

1.2 Copy, synchronisation, backup: not the same thing 5

2. The 3-2-1 rule 6

2.1 An example for a school office 6

2.2 The drive left plugged in is a common mistake 7

3. Where to keep your copies: drive, network, cloud 8

3.1 External drive 8

3.2 Network drive 8

3.3 Cloud 8

3.4 The copy built into Windows 11 10

4. What to save and how often 10

4.1 How often 11

4.2 Full, incremental, versions 11

5. Testing a restore, and the link with ransomware 13

5.1 A backup is the real defence against ransomware 14

5.2 Backup and availability 14

Practical exercise 16

Questions that come up in class 17

Glossary 17

Further reading 18

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**
>
> Understand what a real backup is, apply the 3-2-1 rule with tools you already have, and check that your copies really work, even after a ransomware attack.

What you will be able to do

- Tell a real backup apart from a simple copy or a synchronisation.
- Apply the 3-2-1 rule to an office or home computer.
- Choose between an external drive, a local network drive and the cloud, depending on the data.
- Decide what to save and how often.
- Test a restore of a file to be sure the copy is usable.

1. Why a backup, and what it really is

Sooner or later a computer breaks, a file gets deleted or someone locks your data. The question is not if it will happen, but whether you will have a copy that day.

Picture the front office of a small firm, Studio Esempio. One morning the computer that holds the clients' files will not start. Ten years of work are inside: contracts, invoices, scans. With no copy, that work is gone.

A **backup** is a copy of your data kept in a place different from the original, with one purpose: letting you start again after a failure, a mistake or an attack.



The four most common causes of data loss

1.1 Four ways to lose your data

- **A failure**: the disk breaks, often with no warning;
- **A mistake**: you delete or overwrite a file by accident;
- **Theft or fire**: the computer disappears with everything on it;
- **Ransomware**: malicious software encrypts your files and demands a ransom.

None of these gives notice. That is why the copy must be made **before** you need it, not after.



Failure, mistakes, theft or attacks can all cause data loss.

1.2 Copy, synchronisation, backup: not the same thing

Many people think they have a backup because their files are also in the cloud or on a USB stick. That is not always true. **Synchronisation** keeps two places identical: if you delete a file in one, it disappears from the other. If ransomware encrypts your files, the encryption is synchronised too.



Syncing is not enough when deletions and changes are replicated.

What you do	Protects from a failure?	Protects from a mistake or ransomware?
Keep files only on the computer	No	No
Synchronise a folder with the cloud	Partly	Often no: the mistake is copied there too
Copy to a USB stick that stays plugged in	Partly	No: ransomware encrypts that too
Make a backup with previous versions and a disconnected copy	Yes	Yes

Having files in two places is not enough: what counts is whether the attacker can reach the copy.

> **THE IDEA IN ONE LINE**
>
> A backup only helps if it is separate from the original and if, on that day, you can really open it.

2. The 3-2-1 rule

Three numbers to remember: 3 copies, 2 different media, 1 copy far away.

The 3-2-1 rule is the scheme technicians have used for years because it is simple and survives almost anything. Let us take it one piece at a time.



Three copies in total: the original and two backups, on two media, one off site.

- **3 copies of your data**: the original on the computer plus two backup copies. If one goes wrong, two are left;
- **2 different media**: for example the computer's internal disk and an external drive, or an external drive and the cloud. Different media fail for different reasons;
- **1 off-site copy**: at least one copy away from the office, for example in the cloud or in another building. A fire, a flood or a theft cannot take everything.

2.1 An example for a school office

The office of Istituto Esempio, a fictional school, works on registers and enrolments. It applies the rule like this.

Copy	Where it is	Medium
Copy 1	The working files on the office computer	Internal disk
Copy 2	An external drive, plugged in only while copying and then locked in a drawer	External drive

Copy	Where it is	Medium
Copy 3	An encrypted cloud service, in another location	Cloud, off-site

Three copies, two different media, one off-site.



The computer, the unplugged disk and the off-site copy each play a different role.

> **WHEN THE RULE SAVED THE DAY**
>
> On a Monday a virus encrypts the computer's files. The external drive was unplugged in the drawer, so it is intact. The office cleans the computer, reloads the data from the copy and starts again. The cloud copy, in addition, kept the earlier versions of the documents safe.

2.2 The drive left plugged in is a common mistake

An external drive that is always connected can be reached by ransomware, which encrypts it along with the rest. The copy that is truly safe is the one that is **disconnected**, or the one the attack cannot modify.

> **WARNING**
>
> If all your copies are connected to the computer, then for ransomware they are a single thing. At least one copy must stay physically disconnected or protected by previous versions.

3. Where to keep your copies: drive, network, cloud

There is no perfect medium: each has strengths and weaknesses, which is why you use two.



Each destination has strengths and limits to consider.

3.1 External drive

It is the simplest and cheapest choice: you plug it into the USB port (the standard socket on computers), copy, and unplug it. It works without Internet. The limit is that it is physical: it can break, get lost or stolen, and you have to remember to connect it.

3.2 Network drive

A small firm can use a **NAS**, a device with one or more disks connected to the office network, to which the computers send their copies automatically. It is handy, but if it stays on and reachable all the time it can be hit by ransomware like the computers. Ask your technician to set it up with copies that cannot be modified.

3.3 Cloud

The **cloud** means keeping files on a provider's computers, reachable over the Internet. It is the most convenient off-site copy: you do not have to carry it anywhere. Choose a service that keeps **previous versions** of files, so you can go back to yesterday if today everything was encrypted.

Drive or cloud

External drive	Cloud
Cheap and simple	Off-site by nature
Works without Internet	Previous versions
Can break or be stolen	Needs Internet access
Must be plugged in	Account to protect

vs

External drive and cloud compared

OTHER PEOPLE'S DATA IN THE CLOUD

If the copies contain personal data of clients, pupils or patients, the cloud provider handles that data on your behalf. Choose a service that states it processes data in the European Union and have the head of your organisation assess the choice, as we will see in the lesson on privacy.



The cloud must keep recoverable copies and have protected access.

3.4 The copy built into Windows 11

Windows 11 has ready-made tools. Search for **Windows Backup** in the taskbar search box: it lets you save folders and settings to Microsoft's cloud service (OneDrive). To save to an external drive you can use **File History**, if it is available on your version. Exact menu names can change with updates: look for the feature by name.

> **IN PLAIN WORDS**
>
> An unplugged external drive plus a cloud with previous versions: two media, one off-site copy. For an office, that is already an excellent start.

4. What to save and how often

You do not need to save everything: you need to save what you cannot redo.

Windows and programs can be reinstalled. Your documents, photos, databases and emails cannot. Start from a list of what would land you in trouble if it vanished tomorrow.



Start from what you cannot easily recreate.

Always save	Save if needed	Usually can be redone
Documents, spreadsheets, contracts	Program settings	Windows
Mail archive and address book	List of installed programs	Programs you can download again
Photos and scans	Browser bookmarks	Temporary files
Management or accounting database	Custom templates	Downloads already archived

Start with the first column.

4.1 How often

The practical rule is one question: **how much work can I afford to redo?** If redoing one day is acceptable, copy every day. If losing a week would be a disaster, copy more often. For data that changes every day, such as accounting, a daily automatic copy is the safest choice.



How often you copy depends on how much work you can afford to redo.

4.2 Full, incremental, versions

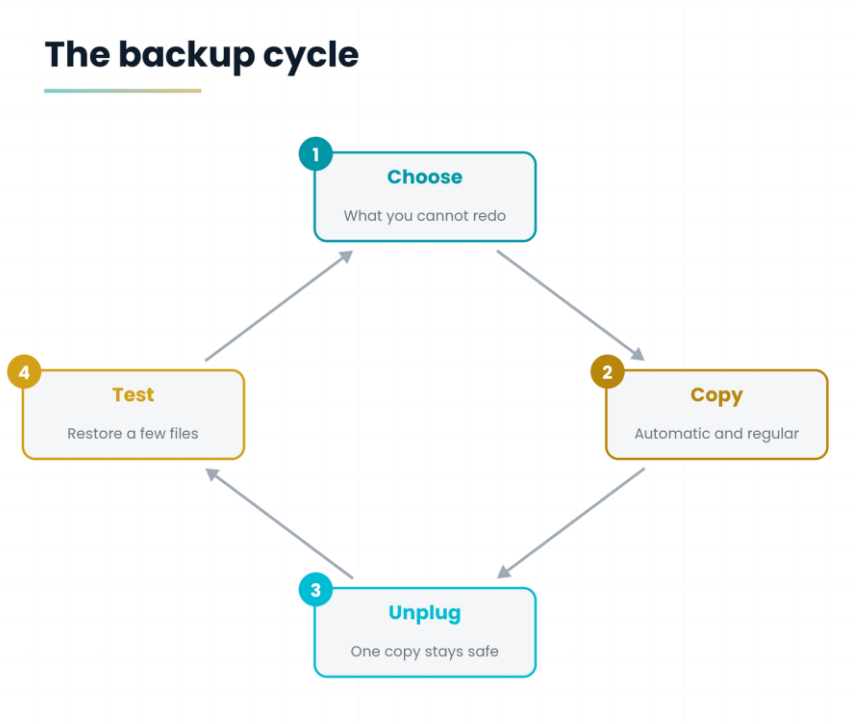
- **Full copy**: copies everything again. It is the simplest to use but needs more space and time;
- **Incremental copy**: saves only what has changed since the last copy. It is lighter;

- **Previous versions**: the program remembers several versions of the same file, so you can recover the one from before a mistake or an attack.



A full copy saves everything; an incremental one saves the changes.

> **A PRACTICAL CASE: THE SHOP**
>
> At Negozio Esempio, the till sends its data every evening to a computer. The owner leaves the automatic copy on the external drive and, on Fridays, takes a second drive home in rotation. If the shop is burgled, the last week of data is still safe.



The cycle of a backup that works

> **AUTOMATE IT**
>
> A backup that depends on your memory will eventually be skipped. Schedule it, and check now and then that it is running.

5. Testing a restore, and the link with ransomware

A copy you have never tried to open is just a hope.

It happens that on the day of need you find the copy was empty, damaged or incomplete. That is why every so often you must **test a restore**: pick a few files at random from the copy and check that they open and are up to date.

1. pick three important files of different types (a document, a spreadsheet, a photo);
2. recover them from the copy into a test folder, not over the originals;
3. open them and check the content is right;
4. note the date of the test and what you checked.



Restore three files into a test folder and open them.

5.1 A backup is the real defence against ransomware

In the lesson on malware and ransomware we saw that whoever encrypts your files asks for a ransom. Paying gives no guarantee: you cannot be sure to get your data back, and you fund the attackers. With a recent, disconnected copy the blackmail loses its force: you do not need criminals to get your files back.

5.2 Backup and availability

Remember the three properties of security from the first lesson? Backup defends **availability**: having your data when you need it. But careful: copies contain the same personal data as the originals and must be protected in the same way.

- **encrypt** the external drive and the copies (Windows Pro includes BitLocker, which we covered in the lesson on devices);
- keep the drive in a **locked place**, not lying on the desk;
- protect cloud access with a **long password and two-step verification**;
- when you dispose of an old drive, **wipe it securely or destroy it**, do not throw it away.



The copies hold people's data too.

THE HONEST LIMIT

A backup does not stop the attack and does not prevent stolen data from being published: it only lets you start again. That is why all the other defences in this course remain necessary: updates, caution with emails, passwords.

Practical exercise

A short exercise with your computer and an external drive or cloud account you already have.

1. List on a sheet the folders you would never want to lose: documents, photos, mail.
2. Check where they are today: only on the computer, or elsewhere too?
3. Draw your own 3-2-1 rule: which is copy 1, 2 and 3, and which is off-site.
4. Make a manual copy of the important folders on an external drive, then unplug it.
5. Recover three files from the copy into a test folder and open them.
6. Note the date and set a reminder to repeat the test.

FINAL CHECK

Do you have at least one copy disconnected from the computer?

Do you have an off-site copy?

Did the recovered files open correctly?

Is the external drive kept in a locked place?

Questions that come up in class

Is it enough to save files on OneDrive or Google Drive?

Not on its own. A synchronised cloud also copies your mistakes and, in some cases, files encrypted by ransomware. It works as an off-site copy if it keeps previous versions, but you also need another copy on a different medium.

Is the cloud safe?

It depends on the service and on how you use it. A serious provider protects its systems, but an account with a weak password and no two-step verification remains the weak point. Always turn it on.

How much space do I need?

Check how much the folders to save take up and choose a drive at least twice that size, so you have room for versions over time. A medium-sized external drive is enough for most offices.

Can I leave the external drive connected for convenience?

Better not. If it is always connected, ransomware reaches it and encrypts it. Connect it for the copy, then unplug it.

How often should I test a restore?

More often at the start, to be sure everything works, then at regular intervals you decide. What matters is doing it and writing it down.

Does the personal data in a backup fall under privacy rules?

Yes. Copies hold the same personal data as the originals, so they need the same protection: limited access, encryption and secure disposal.

Glossary

Term	What it means
3-2-1 rule	A security scheme: 3 copies of the data, on 2 different media, 1 of them off-site.
Backup	A safety copy of your data, kept in a place different from the original, to use after a loss or failure.
Cloud	Storing files on a provider's computers, reachable over the Internet.

Term	What it means
Incremental copy	A copy that saves only what has changed since the last backup.
NAS	A small device with disks connected to the office network, used to store files and copies.
Previous versions	Successive copies of the same file, which let you go back to an earlier one.
Ransomware	Malicious software that encrypts files and demands a ransom to return them.
Restore	The operation of recovering data from the backup.
Synchronisation	A feature that keeps two places identical: every change or deletion is repeated in the other. It is not a backup.

Further reading

Agenzia per la Cybersicurezza Nazionale (ACN, Italy's National Cybersecurity Agency) - guidance and good practice on backups and defence from ransomware

Microsoft, Windows 11 documentation - Windows Backup, File History and Windows Security

Polizia Postale e delle Comunicazioni (Italy's online-crime police unit) - advice on data security

> **WATCH OUT**
>
> Information up to date as of October 2026. Windows 11 menu names can change with updates: if you cannot find an item, search for it by name in the search box. Italian bodies are explained in brackets; in the US, similar guidance comes from CISA.