



Protecting devices and networks

Updates, Windows Security, screen lock, encryption and Wi-Fi

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



Contents

How to use this handout 3

1. Updates: closing the known holes 3

1.1 The case everyone remembers: WannaCry 4

1.2 How to keep everything updated 5

2. Windows Security: antivirus and firewall already included 6

2.1 How to open it 7

2.2 The sections to know 8

2.3 Do you need a paid antivirus? 8

3. Protecting the computer when you are away: lock and encryption 9

3.1 Locking the screen: a gesture to repeat 10

3.2 Prying eyes and sticky notes 10

3.3 A standard account for everyday work 11

3.4 Encryption: if the computer is lost or stolen 11

4. Public Wi-Fi and home and office networks 12

4.1 What is sensible to do, in practice 13

4.2 Good habits when you are out 14

4.3 And your office network? 14

5. USB sticks and unknown media 15

5.1 The case of the stick in the waiting room 16

5.2 When you need to use your own sticks 16

Practical exercise 18

Questions that come up in class 19

Glossary 20

Further reading 20

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 keep your computer updated and protected with the tools already built into Windows 11, to protect your data if a device is left unattended or lost, and to be careful on public Wi-Fi and with unknown USB sticks.

What you will be able to do

- Check that Windows and program updates are switched on.
- Open Windows Security and check antivirus and firewall.
- Lock the screen and set up the computer so it is not left open by mistake.
- Understand what disk encryption is for and how BitLocker works.
- Behave carefully on public Wi-Fi networks and with unknown USB sticks.

1. Updates: closing the known holes

The doors attackers use most are not the new ones: they are the ones already known, which someone has not yet closed.

Every program, from the operating system to the PDF reader, is written by people, so it contains mistakes. Some are **security vulnerabilities**: weak points an attacker can exploit to get into the computer. When one is discovered, the maker of the program publishes a fix, which reaches you as an **update**.



Updates close known vulnerabilities.

From that moment something unsettling happens: the vulnerability becomes public. Attackers know where to look, and hunt for computers that have not yet installed the fix. The risk is not so much the flaw itself as the time it stays open.



The risk lies in the time between the fix and your update

1.1 The case everyone remembers: WannaCry

In May 2017 a ransomware called WannaCry hit hundreds of thousands of computers worldwide, even stopping hospitals and companies. It exploited a Windows flaw for which Microsoft had already published the fix almost two months earlier (March 2017). The computers hit were, to a large extent, those that had not been updated.

The same applies on a small scale. Imagine an office where an old computer in the front desk «must not be touched because it works». It works, sure. But every month that passes without updates, the list of known flaws grows.

1.2 How to keep everything updated

- **Windows Update:** open Settings, choose **Windows Update** and leave automatic updates on. If you see «Check for updates» you can click it to check straight away;
- **really restart:** many updates finish only on restart. A computer left on for weeks with a «restart pending» is not protected yet;
- **programs:** browsers, PDF readers, video-conferencing and office programs usually update themselves. Let them, and do not ignore the notices;
- **phones and tablets:** the same rules apply, from the system settings menu.



Update the system and programs; complete the restarts they ask for.

WHEN THE SYSTEM IS TOO OLD

Every version of Windows has a date after which it no longer receives security fixes. For Windows 10 that date has passed (14 October 2025): computers still using it without additional support programs remain exposed to new flaws, unless they are enrolled in Microsoft's Extended Security Updates (ESU) programme, which for consumers runs until 12 October 2027. It is a temporary bridge: plan the move to Windows 11. If you still have some in the office, talk to whoever looks after IT and plan the move to a supported version.

There is a related habit: install only programs you need, and remove the ones you no longer use. Every extra program is one more door to keep updated.

2. Windows Security: antivirus and firewall already included

In Windows 11 you need less than you think: the basic protection is already inside, you just have to check it is on.

Windows 11 includes **Windows Security**, which uses the engine called Microsoft Defender. It contains two essential tools. The **antivirus** checks files and programs looking for harmful software (the malware of lesson two). The **firewall** controls network traffic going into and out of the computer, and blocks unauthorised connections.



Antivirus and firewall check for different risks.

2.1 How to open it

1. Open the Start menu and choose **Settings**.
2. Go to **Privacy & security** and then **Windows Security**.
3. Click **Open Windows Security**. Alternatively, type «Windows Security» in the search box and open the program from the result.

The first screen shows an overview called «Security at a glance». Each area has an icon: a **green tick** means you need do nothing. A yellow exclamation mark or a red cross means something needs your attention.

Windows Security areas

Viruses and threats Antivirus and scans	**Firewall and network** The wall towards the network
Apps and browser Suspicious programs and sites	**Device** Hardware security

The four main areas of Windows Security

2.2 The sections to know

Section	What it is for	What to check
Virus & threat protection	Antivirus and scans	That real-time protection is on; now and then run a scan
Account protection	Windows sign-in, Windows Hello, dynamic lock	That sign-in is protected by PIN, fingerprint or face
Firewall & network protection	The wall between the computer and the network	That the firewall is on for all networks
App & browser control	Protection against suspicious programs and sites	That reputation checks are on
Device security	Hardware security features	That no yellow warnings appear

The main areas of Windows Security.

The antivirus works by itself in the background: it analyses files as you download or open them. You can also start a **quick scan** by hand from the «Virus & threat protection» section, for example after opening an attachment you were not sure about.



Check the protections and pay attention to the warnings.

2.3 Do you need a paid antivirus?

For normal use in an office or at home, the protection included in Windows 11 is a solid base, provided you keep it on and updated. Paid products can add features (central management, protection for more devices), and larger companies choose them for that.

It is not compulsory, and it does not fix human error: no antivirus stops someone typing a password into a fake page.

> **ONLY ONE ANTIVIRUS AT A TIME**
>
> If you install an antivirus from another maker, Windows usually switches its own off automatically. Do not install two together: they get in each other's way. And distrust fake alerts that pop up in the browser saying «Your computer is infected, download this program»: they are scams, not Windows alarms.



A warning inside a web page can be bait.

3. Protecting the computer when you are away: lock and encryption

The safest computer in the world, left on and unlocked, is a computer open to anyone passing by.

So far we have talked about attacks from the network. But in an office plenty of risks are much more physical: a client walking behind the desk, a cleaner, a supplier left alone for a moment, a laptop forgotten on the train.

3.1 Locking the screen: a gesture to repeat

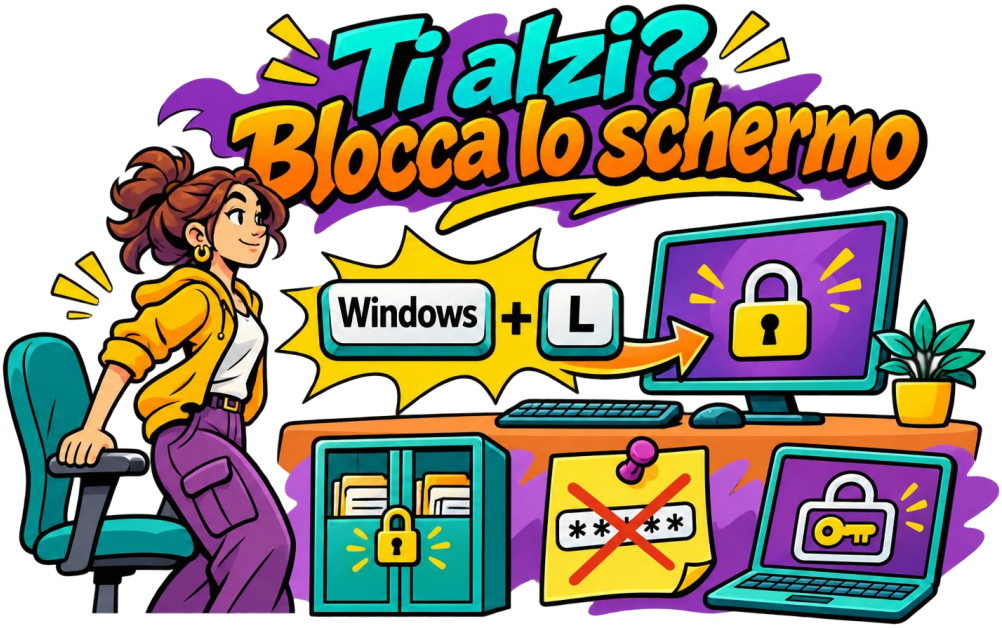
Every time you leave your desk, press the **Windows** key and the **L** key together. The screen locks and to get back in you need your password, PIN or fingerprint. It is a one-second gesture. Do it even if you are only stepping away briefly, because a few steps are enough for someone to read a screen.

Let automation help: in Windows sign-in settings you can make the computer ask for the password again after a period of inactivity, and set the screen saver to ask for sign-in on return. Windows Hello also offers **dynamic lock**: the computer locks when your phone, paired by Bluetooth, moves away.

3.2 Prying eyes and sticky notes

The sticky note with the password on the monitor is a classic. But the list of enrolments left next to the keyboard, or a screen facing the waiting room, are security holes too. A few simple measures:

- turn the screen so that it cannot be seen by people coming in or waiting;
- lock away documents with personal data when you do not need them;
- use a password manager instead of notes (lesson five);
- if you work on the train or in a café, consider a «privacy» film for the screen, which narrows the viewing angle.



Lock the screen and keep papers and credentials safe.

3.3 A standard account for everyday work

Windows distinguishes between **administrator** accounts (which can install programs and change system settings) and **standard** accounts. For daily work a standard account is better: if malware sneaks in, it has fewer powers to do damage. When you need to install something, Windows asks for confirmation with the administrator password, and that moment of pause is precisely the advantage.

3.4 Encryption: if the computer is lost or stolen

Imagine a colleague's laptop, with lists of course participants, stolen from a car. If the disk is **not encrypted**, whoever steals it can remove it, connect it to another computer and read everything, even though Windows had a password. The sign-in password protects Windows, not the files on the disk.

Encryption turns data into an unreadable code that unlocks only with the right key. Whoever does not have the key sees only meaningless characters. In Windows the tool is called **BitLocker** and is available in **Windows Pro** (and higher) editions. Home editions have a similar feature, called device encryption, which depends on the computer's hardware.



Encryption protects the data on a stolen disk.

DO NOT LOSE THE RECOVERY KEY

When you turn on encryption, Windows gives you a **recovery key**: it is needed to unlock the disk if something goes wrong. Save it somewhere safe **outside the computer** (for example in your account, or printed and kept safe). Without the key and without access, encrypted data is lost even to you. That is why backup (lesson seven) remains essential.



Keep the recovery key separate from the computer.

To find out whether your computer is already encrypted, look in the settings for the relevant entry (on Windows Pro, type «BitLocker» in search; on Home, check the device encryption section under Privacy & security). If you are not sure, ask whoever looks after IT: it is a decision to take calmly, because it changes how data is organised.

4. Public Wi-Fi and home and office networks

A free Wi-Fi network at the station is very handy. It is also a waiting room where you do not know who is sitting next to you.

When you connect to a public Wi-Fi network, your data travels on the same network as strangers. If the network is open, or badly managed, someone connected can try to intercept traffic or lure you onto a fake network with a name almost identical to the real one: for example «Station_Free_WiFi» in place of the official one.

4.1 What is sensible to do, in practice

Situation	What is reasonable	What to avoid
Reading the news, checking a timetable	Fine	Nothing in particular
Accessing email or work software	Better to use your phone as the access point (personal hotspot)	Signing in with passwords on an unknown network
Banking or payments	Your phone's mobile data or a trusted network	Any public Wi-Fi
Downloading or sending documents with people's data	Only from a trusted network, with a VPN if your organisation provides one	Doing it from a café on free Wi-Fi

A simple rule: the more sensitive the data, the less you trust the network.



Choose a trusted network for sensitive work.

Two honest clarifications. Today most sites use an encrypted connection (the padlock next to the address, *HTTPS*), which makes it much harder to read traffic even on public networks. It is not, however, a guarantee against fake networks or fake sites. And a **VPN** (*virtual private network*: an encrypted tunnel between your device and a trusted server) helps, but only if it comes from a serious provider and you actually use it.



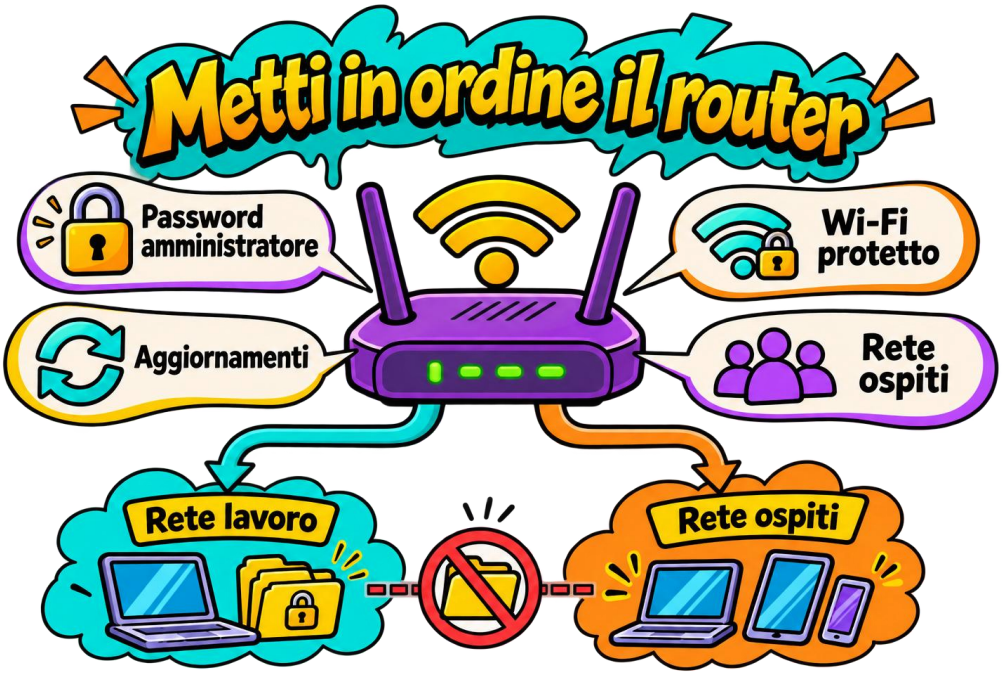
Encryption helps, but you still need to check the network and the destination.

4.2 Good habits when you are out

- if Windows asks what type of network it is, choose **public** for any network that is not your home or office: the firewall will be stricter;
- turn off automatic file and printer sharing on public networks;
- ask staff for the **exact** name of the network and do not trust similar names;
- after use, disconnect and «forget the network», so you do not reconnect on your own in future;
- prefer your phone's data when you need to work on confidential things.

4.3 And your office network?

The router, the box that brings the internet into the office, is the front door of your network. Three checks that apply to both office and home: change the default administration password (the one printed on the label); set up the Wi-Fi with the latest encryption available (WPA3, or WPA2 if the device supports nothing else) and a long password; keep the router's software updated, asking your connection provider if you do not know how.



Secure the router and keep guests apart from the work network.

If you host clients or suppliers, use the router's **guest network**: it gives them internet without opening the door to the office computers.

5. USB sticks and unknown media

A USB stick found in the car park is a gift. The trouble is that nobody knows from whom.

A **USB stick** is a small memory device you plug into the computer. Precisely because it is so handy, it is also a classic vehicle for malware. People who want to attack an organisation sometimes leave sticks lying around, with tempting labels («Salaries», «Party photos»), counting on curiosity.

Some devices, moreover, look like sticks but behave like keyboards: as soon as you plug them in, they **type fast commands by themselves** on the computer. There is nothing to click. That is why the only safe rule is not to plug in media of unknown origin.



What to do if you find an unknown USB stick

5.1 The case of the stick in the waiting room

In a small clinic, a nurse finds a stick in the waiting room. On the key ring it says «Reports». With the best intentions (to return it to the owner!) she plugs it into the reception computer to find out whose it is. That is exactly what the attacker hoped for.

The right behaviour is simple: do not plug it in, hand it to the person in charge, who sets it aside or has it analysed by someone who knows how, on a separate computer with no data and no network connection.

5.2 When you need to use your own sticks

- use only sticks you know, bought by you or supplied by the organisation, not giveaways from fairs or promotions;
- if you put people's data on them, **encrypt the stick** (BitLocker To Go, in Windows Pro, also protects USB media) and use a long password;
- do not leave them lying around, and do not use the same stick between your home computer and the office one without a good reason;
- a stick is not a backup: it gets lost and breaks easily (lesson seven);
- to exchange a file with a client, prefer a password-protected sharing service.



Do not plug in unknown media; protect the ones you are authorised to use.

IN SHORT

Update, check Windows Security, lock the screen with Windows plus L, encrypt the disk, distrust public Wi-Fi and found USB sticks.

Practical exercise

A short exercise to do on the computer you use most: a small security check-up, with what Windows 11 already gives you.

1. Open Settings, go to Windows Update and check there are no updates waiting. If needed, restart the computer.
2. Go to Privacy & security, then Windows Security, and open the program.
3. Look at the «Security at a glance» screen: note which areas have a green tick and which do not.
4. In «Virus & threat protection» check that real-time protection is on and start a quick scan.
5. In «Firewall & network protection» check that the firewall is on.
6. Try the Windows plus L shortcut: lock the screen, then sign back in with your PIN or password.
7. Search for «BitLocker» or device encryption and note whether your disk appears encrypted or not, without changing anything until you have asked whoever looks after IT.
8. Write three lines of rules for your workstation: where you keep documents, when you lock the screen, what you do with an unknown USB stick.

> **CHECK YOU DID IT LIKE THIS**
>
> Does Windows Update have no updates waiting?
>
> Do antivirus and firewall show as on?
>
> Can you lock the screen with one hand, without thinking?
>
> Have you noted the encryption status, without touching anything unnecessary?

Questions that come up in class

Is Microsoft Defender enough or do I need to buy another antivirus?

For normal use the protection included in Windows 11 is a valid base, if it stays on and updated. A paid product can add features (central management, more devices) that mainly help larger organisations. No antivirus, in any case, replaces caution with links and attachments.

Updates slow down the computer: can I postpone them?

You can choose when, for example letting the restart happen at the end of the day. Postponing them for long is risky, though, because every uncorrected flaw stays open. A scheduled restart is better than weeks of exposure.

Does Windows Home have BitLocker?

BitLocker in its full form is in Windows Pro and higher. Many Home computers have device encryption, if the hardware allows it. Check in the settings or ask whoever looks after IT: it depends on the model.

Can I use the hotel Wi-Fi for work email?

Better to avoid it, or use your phone's mobile data. If you have no alternative, visit only sites with the padlock (HTTPS), turn on two-step verification and, if your organisation provides one, use the VPN.

I plugged in an unknown USB stick: what do I do?

Do not panic, but act at once: disconnect the computer from the network (unplug the cable or turn off Wi-Fi), tell the IT contact and do not keep working. See lesson nine for the steps to follow.

Is the screen lock enough, why encrypt the disk too?

They are two different protections. The lock stops whoever sits at your desk. Encryption stops whoever takes away the computer or the disk. For laptops, which get lost and stolen, both are recommended.

Glossary

Term	What it means
Antivirus	A program that finds and blocks harmful software (malware).
BitLocker	The disk encryption tool included in Windows Pro and higher.
Encryption	Turning data into an unreadable code, unlockable only with the right key.
Firewall	The «wall» that controls network traffic into and out of the computer.
Public Wi-Fi	A wireless network open to anyone, like those in stations, cafés and hotels.
Update	A corrected version of a program that closes known flaws.
VPN	Virtual private network: an encrypted tunnel between your device and a trusted server.
Vulnerability	A mistake in a program that an attacker can exploit to get into the computer.
Windows Security	The Windows 11 application that gathers antivirus, firewall and other checks, based on Microsoft Defender.

Further reading

Microsoft, documentation on Windows Security and Microsoft Defender - features and areas of the application

Microsoft, documentation on BitLocker and device encryption - Windows editions and the recovery key

Microsoft, Windows 10 lifecycle - end-of-support date of 14 October 2025

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

> **WATCH OUT**
>
> Information up to date as of October 2026. Menu names are those of Windows 11 and may change slightly with updates: if you cannot find an option, use the Windows search box. Features (BitLocker, device encryption) depend on the Windows edition and the computer. The Agenzia per la cybersicurezza nazionale is Italy's national cybersecurity authority.