




# Conclusions

What you have learned and where to restart tomorrow

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



# Contents

How to use this handout ..... 3

1. The path in brief ..... 3

2. The conclusions ..... 5

3. The most common mistakes to avoid ..... 6

4. And now? ..... 7

4.1 The first week ..... 7

4.2 The first month ..... 8

4.3 How to keep learning ..... 8

Self-assessment ..... 9

Questions that come up in class ..... 10

Glossary ..... 10

Further reading ..... 11

## 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**
>
> Review the path lesson by lesson, fix the ideas that stay, avoid the most common mistakes and leave with a concrete action plan.

**What you will be able to do**

- Remember the key idea of each lesson.
- Recognise the most frequent mistakes and how to avoid them.
- Assess your own situation with a checklist.
- Plan the first steps: the first week and the first month.

## 1. The path in brief

You have made it to the end. Let us line up what you have learned.

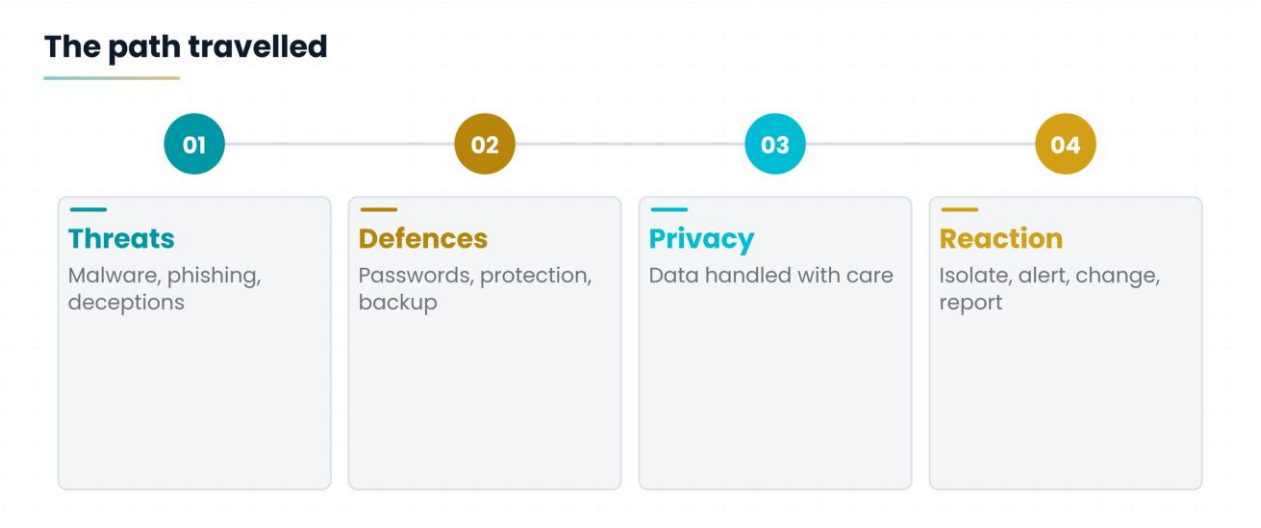



From threats to defences, all the way to incident response.

| Lesson | Key idea | What you can do now |
|---|---|---|
| **1. What is cybersecurity** | Confidentiality, integrity and availability are protected; the main risk is human error | Explain what you must protect and why |
| **2. Malware and ransomware** | You do not pay the ransom: the defence is the backup | Recognise the types of malware and how they arrive |
| **3. Phishing and its variants** | The channel changes, the goal does not: stop and check | Unmask scam e-mails, SMS, phone calls and QR codes |
| **4. Fake sites and social engineering** | The address matters more than how the page looks | Check a domain and recognise social engineering |
| **5. Passwords and two-step verification** | Long phrase, one per service, second check | Create solid passwords and turn on the check |
| **6. Protecting devices and networks** | Updates, Windows Security, screen lock, encryption | Secure your computer, USB sticks and Wi-Fi |
| **7. Backup and the 3-2-1 rule** | Three copies, two media, one off-site | Organise and test your backups |
| **8. Privacy and data protection** | Only the data you need; breaches reported in time | Apply good practice and handle a breach |
| **9. What to do when it happens** | Isolate, alert, change, report | React without improvising |

The path, lesson by lesson.

There is a single thread: the threats (lessons 1 to 4) almost always exploit a **distraction**, the defences (5 to 8) are there to limit the damage when the distraction has happened, and the last lesson tells you what to do when the defences are not enough.




The path travelled: from the threats to the defences, to the reaction

## 2. The conclusions

If you had to remember only four things, they would be these.

1. **Human error is the main risk, so training is the best defence** (lesson 1). You do not need to be technical, you need to stop for a moment.
2. **Stop and check** (lessons 3 and 4). Sender, rush, link and attachment: four questions are enough to stop most scams.
3. **Defences add up** (lessons 5, 6 and 7). Long passwords and two-step verification, updates, Windows Security, backups with the 3-2-1 rule: none is perfect, together they work.
4. **Data belongs to people** (lessons 8 and 9). Treat it with care and, if something goes wrong, tell someone at once: time matters.




Training, attention, complementary defences and care for people.

> **THE IDEA IN ONE LINE**
>
> Security is not a product you buy: it is a habit you build.




Stop, check, protect your data and report early.

## 3. The most common mistakes to avoid

These are the ones that come up most often in the questions of the lessons.

| Mistake | What to do instead |
|---|---|
| Clicking because the message rushes you | Stop, check the sender and call the organisation on its official number |
| Using the same password everywhere | A different long phrase for each service, in a password manager |
| Putting off updates | Leave them automatic |
| Having one backup, on the same computer | Apply the 3-2-1 rule and test the restore |
| Paying the ransomware ransom | Restore from your copies and report it |
| Trying to «fix it yourself» after an incident | Isolate the computer and tell the person in charge |

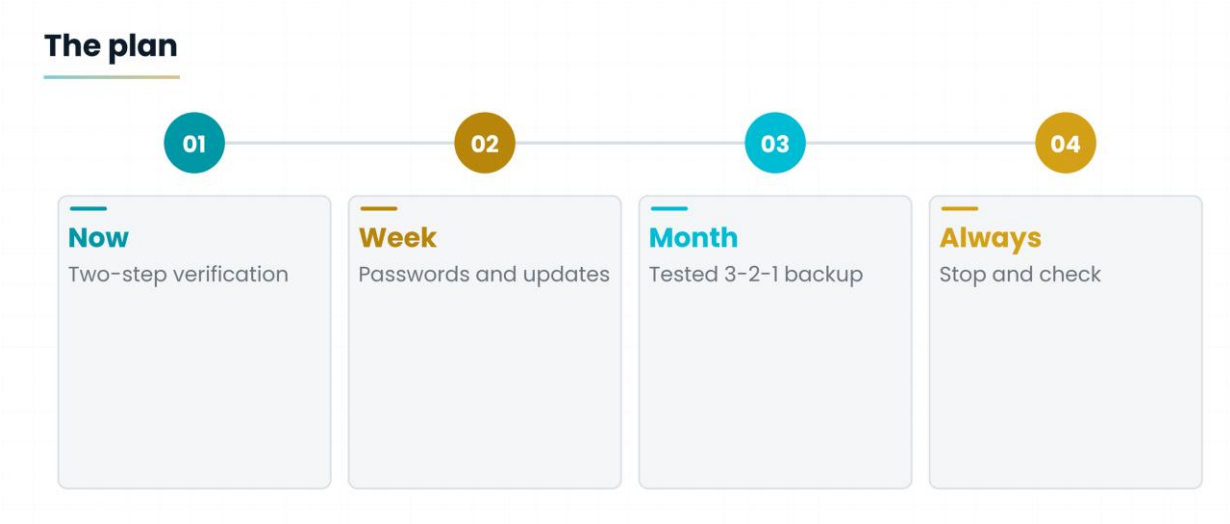
The most frequent mistakes.




Recognise the mistakes that can weaken your other defences.

## 4. And now?

A course is worth it if it changes what you do tomorrow. Here is a simple plan.




The action plan

### 4.1 The first week

- turn on two-step verification on your e-mail and cloud;
- change your most important passwords to long, different phrases;
- check that Windows Security and automatic updates are on;

- get into the habit of pressing Windows plus L when you leave your desk.

### 4.2 The first month

- set up your backup with the 3-2-1 rule and try restoring a file;
- review who can see which data in your work;
- write on a sheet of paper the four steps to follow if an incident happens and whom to call;
- tell your colleagues one thing you have learned.




This week secure your accounts and update; this month test your backup and your plan.

### 4.3 How to keep learning

Threats change, principles do not. Re-read the handouts now and then, look at the official sites of the Garante (the Italian Data Protection Authority, www.gpdp.it) and of the Polizia Postale e delle Comunicazioni (Italy's online-crime police unit, www.commissariatodips.it), and write to info@gianlu.it if you have doubts or want a course on a topic that is missing.

## Self-assessment

A checklist to see where you stand. Answer yes or no.

1. Have I turned on two-step verification on my e-mail?
2. Do I have a different, long password for important services?
3. Are Windows updates automatic and does Windows Security show green ticks?
4. Do I have at least three copies of my data, on two media, one off-site?
5. Have I tried restoring a file from the backup?
6. Do I know what to do and whom to tell if an incident happens?

> **WATCH OUT**
>
> Wherever you answered no, that is your priority for the first week.

## Questions that come up in class

**Where do I start if I have little time?**

With two-step verification on your e-mail and a long password for your most important service: they are the two moves that give the most protection for the least effort.

**Is it enough to have followed the course to be safe?**

No: total security does not exist. The course greatly reduces the risk and prepares you to react well when something happens.

**How often should I review?**

Re-read the handouts now and then, and check your backup and updates every month.

**Can I recommend the course to colleagues?**

Of course: the handouts are designed for that too. A team that follows the same rules is much harder to fool.

## Glossary

| Term | What it means |
|---|---|
| **3-2-1 rule** | Three copies of the data, on two different media, one off-site. |
| **Backup** | A safety copy of the data, to use in case of loss or fault. |
| **Cybersquatting** | Registering domain names similar to other people's trademarks to take advantage of them. |
| **Firewall** | A system that filters network traffic and blocks unauthorised connections. |
| **GDPR** | The European regulation on personal data protection. |
| **Malware** | Harmful software created to damage a computer or steal data. |
| **Phishing** | A deception to obtain data or to make people click dangerous links and attachments. |
| **Ransomware** | Malware that encrypts files and demands a ransom. |
| **Social engineering** | Manipulating people, rather than machines, to obtain data or access. |
| **Two-step verification** | A second check, besides the password, to log in to a service. |

## Further reading

**Garante per la protezione dei dati personali (Italian Data Protection Authority)** - www.gpdp.it

**Polizia Postale e delle Comunicazioni (Italy's online-crime police unit)** - www.commissariatodips.it

**Windows Security** - built-in guide in the app (Start, Windows Security)

> **WATCH OUT**
>
> This lesson recaps the course and introduces no new topics. For rules and procedures always refer to the official sites.