



Introduction to the course

Who it is for, what you will learn and how to follow it

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



Contents

How to use this handout 3

1. Why this course 3

2. Who it is for and what you need 4

2.1 What you need 5

3. What you will learn 5

4. The programme, lesson by lesson 5

4.1 The threats, in brief 6

4.2 The defences, in brief 8

4.3 If it happens 10

5. How to follow the course 10

6. Who is telling you all this 11

Getting ready 13

Questions that come up in class 14

Glossary 14

Further reading 14

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 whether the course is right for you, know what each lesson contains and in which order to follow them, and get your tools ready to start.

What you will be able to do

- Know who the course is for and what you need to follow it.
- Know the programme, lesson by lesson.
- Choose a way of studying that suits you.
- Prepare your working folder and the tools for the exercises.

1. Why this course

Monday morning, at the office, an e-mail arrives from the director: «Make this transfer right now, I'll explain later». What do you do?

It is a situation that really happens, and it is a scam with a name: spear phishing. Whoever recognises it in time avoids the damage. Whoever does not, pays, sometimes with money, sometimes with other people's data.



An urgent request deserves a second look.

An office computer holds names, addresses, tax codes, sometimes medical or financial documents of many people. Protecting them is a legal duty, but first of all it is a matter of **trust**: whoever handed you their data expects you to treat it with care.

> **THE IDEA IN ONE LINE**
>
> Almost all incidents come from human error: that is why the best defence is you, and it can be learned.

2. Who it is for and what you need

The course starts from zero. You need no technical skills: curiosity and the habit of using a computer, e-mail and a phone are enough. It is designed for people working in an office, a small firm, a school, a small shop, but it works at home too.

It is for you if	It may not be for you if
You use a computer, e-mail and phone every day for work	You are already a security technician looking for details of an attack
You handle data of customers, members, colleagues	You want a course on defending a large company network

It is for you if	It may not be for you if
You want to understand what to do, without jargon	You never use digital tools

Who the course is for.

2.1 What you need

- a computer with **Windows 11** (the examples use it);
- an e-mail account and a phone;
- a folder on your computer to save your notes;
- pen and paper for the exercises.

> **WARNING**
>
> In the exercises always use invented data or your own. Never use real data of customers, colleagues or members to practise.

3. What you will learn

By the end of the course you will be able to do these things, and they are not theory: you will use them the very next day.

- **Recognise** malware, ransomware, phishing and trap sites before falling for them;
- **Choose** solid passwords and turn on two-step verification;
- **Protect** your computer with updates, Windows Security, screen lock and encryption;
- **Organise** backups that really work, with the 3-2-1 rule;
- **Handle** personal data as the law requires, from blind copy to reporting a breach;
- **React** in the right way when something happens.

4. The programme, lesson by lesson

There are nine lessons and they should be followed in order. The first four explain **what** we defend ourselves from, the next four **how** we defend ourselves, the last one **what to do** when the defences are not enough.

Lesson	Title	What you will be able to do afterwards
1	What is cybersecurity	Explain what is being protected and why human error is the main risk
2	Malware and ransomware	Recognise the types of harmful software and know why you do not pay the ransom
3	Phishing and its variants	Unmask scam e-mails, SMS, phone calls and QR codes
4	Fake sites and social engineering	Check a web address and recognise social engineering
5	Passwords and two-step verification	Create solid passwords and turn on the second check
6	Protecting devices and networks	Secure your computer, USB sticks and Wi-Fi
7	Backup and the 3-2-1 rule	Organise backups and test the restore
8	Privacy and data protection	Apply good practice on personal data and handle a breach
9	What to do when it happens	Follow the right steps after an incident

The course programme.

4.1 The threats, in brief

The first four lessons teach you to recognise the enemy. We start with harmful software: **ransomware** locks your files and demands a ransom to give them back.



Ransomware locks your files and demands a ransom.

Then come the scams that reach you from outside: **phishing** does not travel only by e-mail, but also by messages, phone calls and QR codes.



Phishing can arrive through different channels.

Finally trap sites and social engineering, the scams that aim at people rather than at machines.



Scams play on people, not on machines.

4.2 The defences, in brief

The next four lessons teach you how to defend yourself. For your accounts you need two complementary defences: solid passwords and two-step verification.



Protect your accounts with solid passwords and two-step verification.

Then come the everyday tools: the computer, USB sticks and Wi-Fi are protected with a few clear rules.



Security also covers the tools you use every day.

Backups follow the 3-2-1 rule, so that you always have copies that work when you need them.



The 3-2-1 rule: different copies, available when you need them.

Finally privacy: other people's personal data must be handled with care, as the law requires.



Handle personal data with care.

4.3 If it happens

The last lesson is the most practical: what to do if it happens, even when the defences are not enough.



Being prepared helps you know what to do.

Here is the whole course path at a glance.



The course path: what we defend ourselves from, how, and what to do when it happens

5. How to follow the course

Every lesson comes with four materials that say the same things in different ways: choose the one that suits you best.

- **The handout** (PDF): to read calmly and to keep;
- **The slides**: to review or to explain to others;
- **The video**: to grasp the main points quickly;
- **The exercise**: the most important part, to do with what you already have.

The advice is simple: read the handout, watch the video, then do the exercise. One lesson at a time, without rushing. If a week later you remember the method but not the details, that is perfectly fine: the details are in the handout.



Nine lessons, one at a time: read, watch and try.

When you feel you have understood the method, download the free handout on gianlu.it and move on to the next lesson.

> **A RHYTHM THAT WORKS**
>
> One lesson at a time, with a pause between them to try things on your own computer. Whoever puts lesson 5 (passwords) into practice the same day remembers it for years.

6. Who is telling you all this

I am Gianluca Bonomo, an IT consultant and trainer. For years I have been explaining digital matters to non-technical people, in simple words and with examples from

everyday work. You will find more courses and articles at www.gianlu.it; for questions or suggestions write to info@gianlu.it.

Getting ready

Before you start, get what you need ready.

1. Create a folder on your computer called «Security course» and inside it one folder per lesson.
2. Open a text file and write one sentence: «I want to protect…». Complete it with the data or service that matters most to you.
3. Check that you have an up-to-date Windows 11 and a phone to receive codes.
4. Download the handout of lesson 1.

> **WATCH OUT**
>
> Do you have one folder per lesson?
>
> Do you know what you want to protect first?

Questions that come up in class

Do I need to be a computer expert?

No. The course starts from zero and explains every technical term the first time it appears.

Can I skip some lessons?

Better not: each lesson builds on the previous ones. If you already know a topic, read the handout and go straight to the exercise.

Does it work if I use a Mac or a phone?

The concepts do, because phishing, passwords and backups are the same everywhere. The menu paths and practical examples are those of Windows 11.

Do I have to pay for anything or install programs?

No: the course uses what you already have, in particular Windows Security. Where something else would be needed, I tell you in the lesson.

Glossary

Term	What it means
Backup	A safety copy of the data, to use in case of loss or fault.
Malware	Harmful software created to damage a computer or steal data.
Personal data	Any information relating to an identified or identifiable person.
Phishing	A deception to make you click a link, open an attachment or give confidential data.
Two-step verification	A second check, besides the password, to log in to a service.

Further reading

Gianluca Bonomo, www.gianlu.it - course materials

> **WATCH OUT**
>
> Examples, names and domains in the course are invented. The practical examples refer to Windows 11.