



What to do when it happens

Four steps to react calmly when the incident has already happened

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



Contents

How to use this handout 3

1. The moment you realise 3

1.1 Signs that something is wrong 4

2. The four steps, one at a time 5

2.1 Step one: isolate 5

2.2 Step two: alert 6

2.3 Step three: change passwords and two-step verification 7

2.4 Step four: keep the evidence and report 9

3. What not to do 10

3.1 The most frequent mistakes 11

4. Three practical cases 12

4.1 Case 1: the fake link in the school office 12

4.2 Case 2: the ransomware at the firm 13

4.3 Case 3: the email to the wrong recipient 13

5. After the incident 13

5.1 Understand and restore 14

5.2 When people's data are involved 15

5.3 Learn and improve 16

Practical exercise 17

Questions that come up in class 18

Glossary 18

Further reading 19

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**
>
> Know what to do, and in which order, when you suspect you have clicked a fake link, opened a dangerous file or lost data: isolate, alert, change passwords and two-step verification, keep the evidence and report.

What you will be able to do

- Recognise the signs of an incident and stop instead of panicking.
- Isolate a suspicious device from the network without losing evidence.
- Alert the right people in the right order, including the bank when needed.
- Change passwords and two-step verification from a clean device.
- Tell a report from a formal complaint to the Polizia Postale and understand when a notification to the Garante is required.

1. The moment you realise

Sooner or later it happens to everyone: one click too many, an attachment opened in a hurry, a screen that behaves strangely.

Picture Marta, who works in the office of a school. She receives an email that looks like it comes from the school's bank, clicks the link, types in her credentials and only then notices the address of the page looked odd. Her heart races. What does she do?

The most common reactions are these two: pretending nothing happened and hoping it goes away, or doing many things at once, in no order. Both are wrong. In the first case the problem grows in silence; in the second you risk deleting the very traces needed to understand what happened.

The good news is that there is a simple sequence you only need to learn once. Four steps, always the same, whatever the incident.



If it happens: isolate, alert, protect access, keep evidence and report

THE IDEA IN ONE LINE

First stop the damage, then alert people, then secure your access, and finally keep the evidence and report.

1.1 Signs that something is wrong

An incident does not always announce itself with a threatening screen. Often the signs are small, and you should take them seriously.

- you clicked a link or opened an attachment and something unusual happened right after;
- files have changed name or extension, or no longer open;
- a message demands a ransom;
- the computer is suddenly very slow or acts on its own;
- someone tells you that emails you never wrote are being sent from your address;
- you get an alert about a login to your account from a place or device you do not recognise;
- you see transactions on your account that you did not make.

DOUBT IS ENOUGH

You do not need to be one hundred percent sure to act. If you suspect an incident, behave as if it is real and speak up. A false alarm costs little; a hidden incident costs a lot.

2. The four steps, one at a time

Here is the full sequence. Then we go through it calmly, step by step.

Step	What you do	Why
1. Isolate	Disconnect the device from the network.	The problem cannot spread to other computers.
2. Alert	Immediately tell the person in charge what happened.	Those with the tools can step in and protect others.
3. Change passwords and verification	Change passwords and check two-step verification, from a clean device.	Whoever stole your credentials can no longer use them.
4. Keep and report	Keep the evidence and report to the Polizia Postale.	It helps to understand, to protect yourself and for investigations.

The four steps to follow every time, in this order.

2.1 Step one: isolate

To isolate means to take the device off the network. If the computer is connected with a cable, unplug it. If it uses Wi-Fi, switch Wi-Fi off from the Windows 11 quick settings or turn on airplane mode. This way a malicious program can neither spread to the other computers in the office nor talk to whoever created it.

If a USB stick or external drive is plugged in, unplug that as well: it could be the next target. And if you suspect ransomware (the program that locks your files and demands a ransom), disconnecting quickly can save backup copies that were plugged in.

Then leave the computer as it is. Do not reformat it, do not reinstall anything and do not delete files on your own initiative. If your office has an IT contact, they will decide how to proceed.



Disconnect the network and ask for help, without reformatting

2.2 Step two: alert

This is the step that costs most, because people feel embarrassed. Yet it is the most important. The longer you wait, the more the damage spreads: the attacker uses the access they obtained to move into other systems, write to your contacts or empty an account.

Alert people in the right order. First the office manager or the IT contact. Then, if an account or card is involved, the bank, using the official number from its website or the back of the card (not the one written in the suspicious email). If your mailbox was used to scam others, also warn your key contacts with a short message: «Ignore any strange emails that came from my address».



Alert your manager; if money is involved, call the bank on its official number

> **IT IS NOT YOUR FAULT**
>
> A good office rewards those who report at once and does not punish those who make a mistake. The real fault is staying silent.

2.3 Step three: change passwords and two-step verification

If you typed a password into a suspicious page, treat that password as compromised. Change it right away on the real site (by typing the address yourself or using a bookmark, never a link you received). Then change every other password that was the same or similar: whoever has one will immediately try it on other services.

Do this from a clean device, meaning one that is not the suspicious one: your phone, if it is not involved, or a colleague's computer. If spyware (a program that spies on you) is still on the computer, changing passwords from there would hand them over again to whoever is watching.



Change credentials from a trusted device and on the real site

Then check two-step verification (the second proof of identity, such as the code in an app). Make sure it is on for your important accounts: email, bank, the organisation's services. Also check that no unknown devices appear among the authorised ones and, if the service allows it, sign out of all open sessions.



Check two-step verification, authorised devices and suspicious forwarding

2.4 Step four: keep the evidence and report

Before deleting the scam email, the message or the screen, keep a copy: save the email as a file, photograph the screen with your phone, note the day, the time and what you did. These are your own notes, written while it is fresh: a week later you will remember nothing.



Keep the message, a photo of the screen, and the date and time

Then report. In Italy the reference for computer crime is the **Polizia Postale e delle Comunicazioni**, the part of the State Police that deals with crimes committed online (roughly the equivalent of the FBI's IC3 in the US). Its portal, the online police station (commissariatodips.it), lets you choose between several routes.



A report is not the same as a formal complaint

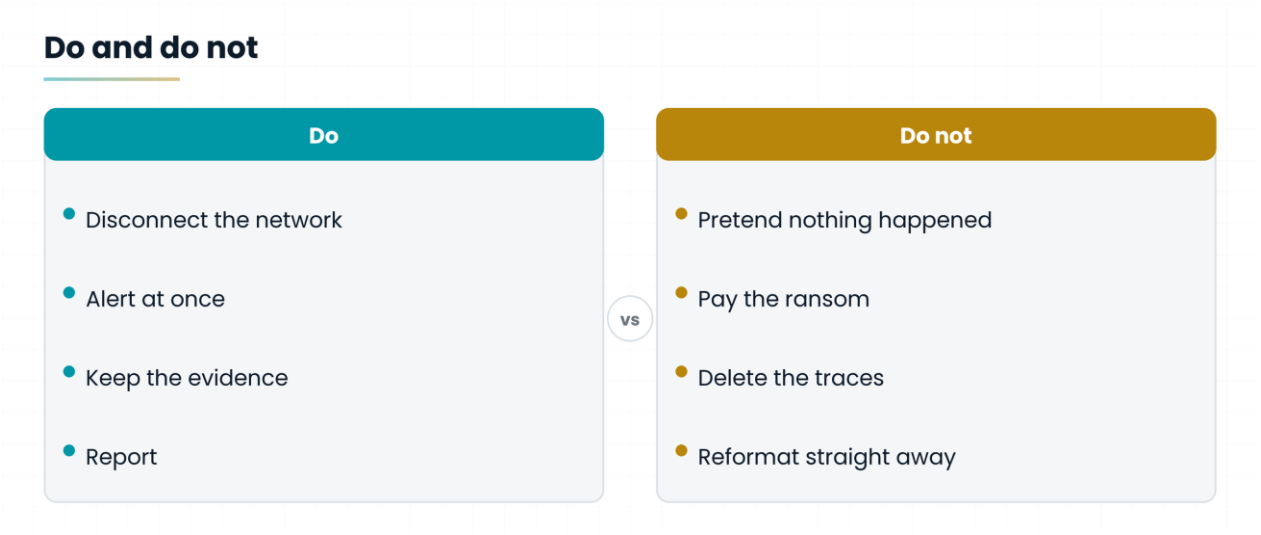
Route	What it is for
Online report (segnalazione)	You bring to the police's attention conduct you think is unlawful so they can check it. It is not a formal complaint.
Formal complaint (denuncia)	The formal act in which you state the facts. For computer crimes the portal offers a dedicated service; you can also file in person at a police office.
Information request	If you only have a doubt, you can ask the experts for advice through the portal.

The three routes on the Polizia Postale portal.

> **A REPORT IS NOT ENOUGH IF YOU LOST MONEY**
>
> The online report does not replace a formal complaint and is not an emergency service. If there is immediate danger call 112 or 113 (Italy's emergency numbers). If you lost money, call the bank first and then file a complaint.

3. What not to do

In a panic people do things that seem helpful and only make matters worse.



What to do and what not to do

3.1 The most frequent mistakes

- **Pretending nothing happened.** Silence is the costliest mistake, because it gives the attacker time.
- **Paying a ransom.** There is no guarantee the files will come back, and the payment funds more attacks and marks you as a willing customer.
- **Replying to blackmailers or calling the number in the message.** Every reply confirms that your address is active.
- **Deleting emails, files or history** to «clean up». You destroy the evidence.
- **Reformatting the computer straight away.** If you do it before understanding what happened, you will not know what was stolen.
- **Changing passwords from the infected computer.** You hand them over again to whoever is spying on you.
- **Calling the number written in the email or message** to «verify». Always look up the official number yourself.



Do not stay silent, pay, delete evidence or reformat on your own

BEWARE OF FAKE RESCUERS

After an incident someone may offer to «recover everything» for money, often contacting you first. If you did not look for them, be suspicious.

4. Three practical cases

The theory is simple. Let us apply it to three office situations. The names are invented.

4.1 Case 1: the fake link in the school office

Marta, in the office of Istituto Esempio, clicks a link received by email and types in her mailbox credentials. She notices the domain was wrong: ente-esempio.it had become ente-esempio.com.

- **Isolate:** she closes the page and disconnects the computer from Wi-Fi.
- **Alert:** she immediately tells the head teacher and the IT contact, without waiting.
- **Change:** from her phone she changes the mailbox password and checks that two-step verification is on; she also checks the forwarding rules, which attackers use to receive a copy of your mail.

- **Keep and report:** she saves the scam email and notes the time; the school files a report with the Polizia Postale.

Result: the access is closed before the attacker uses it. Marta is not punished; on the contrary, the school warns the other colleagues that this email is going around.

4.2 Case 2: the ransomware at the firm

At the small consulting firm Rossi e Soci, one Monday morning the shared files no longer open and a message demands a payment. Giulia, the secretary, touches nothing and does not try to «fix it» herself.

- **Isolate:** she unplugs the network cable and asks everyone to do the same; she also unplugs the external backup drive.
- **Alert:** she calls the owner and the trusted technician.
- **Change:** from a clean device, the email and online service passwords are changed.
- **Keep and report:** the ransom message is photographed and a complaint is filed with the Polizia Postale.

The firm does not pay. The backup drive had been unplugged since the previous week, so the technician restores the data from the last healthy copy. A few days of work are lost, not everything. This is why the lesson on backup is the real insurance.

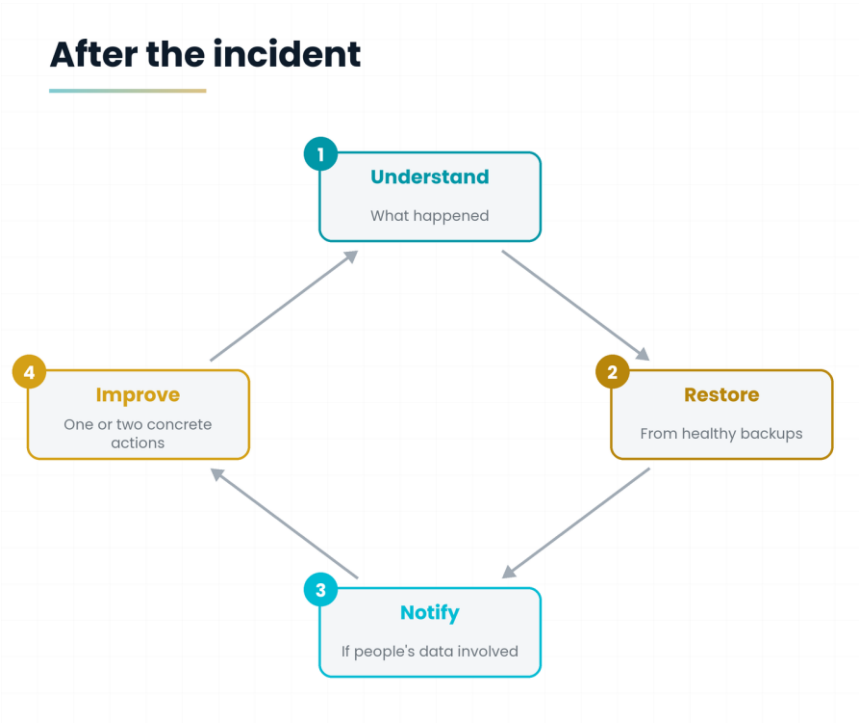
4.3 Case 3: the email to the wrong recipient

In an office, Luca mistakenly sends an outside address a list with names, tax codes and contact details of several people. There is no attacker, but it is still a personal data breach.

What does he do? He immediately tells the data controller (the person who decides how the organisation's data are used). He tries to recall the message and asks the recipient, in writing, to delete it without opening it. He notes what happened. It will be up to the controller to assess whether the breach must be notified to the Garante, as we see in the last section.

5. After the incident

When the emergency is over, the most useful work remains: understanding and improving. An incident handled well is a lesson that costs less than the one the next time would bring.



After the incident: from restoring to improving

5.1 Understand and restore

Together with the IT contact you reconstruct the facts: what was hit, what was seen or taken, where the attacker got in. Only then do you restore, from backups and onto a cleaned system. Restoring before you have closed the front door means being attacked the same way a second time.



Understand the cause, close the access, restore on a clean system, improve

5.2 When people's data are involved

When the incident concerns personal data, the GDPR (the European data protection regulation) comes into play, and there is a duty to assess the breach. The one who does it is the **data controller**, not the individual employee: you alert at once, they decide.

- the breach must be notified to the Garante per la protezione dei dati personali (the Italian Data Protection Authority) **without undue delay and, where feasible, within 72 hours** of the controller becoming aware of it;
- notification is not needed if the breach is unlikely to result in a risk to people's rights and freedoms;
- a notification after 72 hours is possible, but the reasons for the delay must be explained;
- today the notification is made through the online procedure on the Garante's website;
- if the risk to people is high, the data subjects, meaning the people the data refer to, must be informed too;
- every breach must in any case be recorded in an internal register, even when it is not notified.



The data controller assesses the risk, notifies and informs people when needed

THE CLOCK STARTS AT ONCE

The 72 hours run from when the controller became aware. That is why it is so important that you alert them immediately: if you keep the problem to yourself, you waste precious time for the whole organisation.

5.3 Learn and improve

Close with a short discussion, without looking for culprits. What made the incident possible? A weak password, a postponed update, a backup never tested? Choose one or two concrete actions and decide who will do them. Then tell your colleagues what happened: an incident well told is worth more than a thousand generic warnings.

AFTER THE SCHOOL CASE

After the fake email, Istituto Esempio turns on two-step verification for all the office mailboxes and prepares a sheet with the four steps to pin beside the phone.



Write the checklist and the contacts before you need them

Practical exercise

A short exercise to prepare, now and calmly, the plan you will need if one day you are in trouble.

1. Take a sheet of paper and write «If it happens» at the top. Below, list the four steps in your own words.
2. Next to the step «Alert», write the name and number of the person to call in your office or family.
3. On your bank's official website find the number to block cards and accounts and write it on the sheet.
4. Open commissariatodips.it and see where the online report and the complaint for computer crimes are; note the address.
5. In the Windows 11 quick settings, find the button to turn Wi-Fi off or enable airplane mode.
6. Pin the sheet near your desk or keep it in a safe place.

CHECK THAT YOU DID THIS

Does the sheet have at least one name and number to call?

Do you know how to disconnect your computer from the network?

Does the bank's number come from the official website and not from an email?

Questions that come up in class

I clicked a link but nothing happened. Do I need to do anything?

Yes, at least alert and check. Some malicious programs are invisible. Disconnect the device, tell your IT contact, change the password if you typed it, and check recent logins to the account.

Can I switch the computer off straight away?

Disconnecting it from the network is the first thing. Switching it off depends on the case: ask your IT contact. The important thing is not to reformat or reinstall anything before understanding what happened.

Do I have to file a complaint with the Polizia Postale?

If you suffered damage, for example a scam with loss of money or identity theft, filing a complaint is advisable. In other cases you can send an online report. If in doubt, the portal lets you ask for information.

Is notifying the Garante my job?

No, it belongs to the data controller, the one who decides how the organisation's data are used. Your job is to alert them immediately, because the deadlines start from when they become aware.

Can I pay the ransom if I have no backup?

It is not recommended. There is no guarantee you will get the files back, and you fund further attacks. Before deciding, have a technician assess the case and consider filing a complaint.

How do I know whether my data were stolen?

You cannot always know at once. Check recent logins to your accounts, bank alerts and the forwarding rules of your mailbox. If in doubt, ask a technician for help.

Glossary

Term	What it means
Data controller	Whoever decides why and how personal data are used, for example the organisation, firm or company.
Evidence	Emails, screenshots and notes that document what happened and help to understand it and to report it.

Term	What it means
Formal complaint (denuncia)	The formal act of telling the authorities about a crime.
Garante per la protezione dei dati personali	The Italian independent authority that supervises compliance with privacy law.
Isolate	Disconnect a device from the network, by cable or by turning off Wi-Fi, to stop a problem spreading.
Personal data breach	An incident leading to the loss, alteration, disclosure of or unauthorised access to people's data.
Polizia Postale e delle Comunicazioni	The part of the Italian State Police that deals with computer crime. Its portal is commissariatodips.it.
Report (segnalazione)	A communication to the police about a fact that seems unlawful, so they can check it. It does not replace a formal complaint.
Security incident	An event that endangers the confidentiality, integrity or availability of data.

Further reading

Commissariato di Polizia di Stato online (Polizia Postale e delle Comunicazioni), commissariatodips.it - online report, complaint for computer crimes, information; consulted in October 2026

Garante per la protezione dei dati personali, page on personal data breaches (data breach) - 72-hour deadline, online procedure, internal register; consulted in October 2026

Regulation (EU) 2016/679 (GDPR), Articles 33 and 34 - notification to the supervisory authority and communication to data subjects

WATCH OUT

Information up to date as of October 2026. This lesson refers to Italian bodies: the Polizia Postale e delle Comunicazioni (Italy's online-crime police unit, comparable to the FBI's IC3 in the US) and the Garante (the Italian Data Protection Authority). The services on their websites may change, so always check the official pages. This lesson is a general guide and does not replace the advice of a technician or a lawyer.