




# Fake sites and social engineering

Almost-identical addresses, convincing calls and stolen identities

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



# Contents

How to use this handout ..... 3

1. The site that looks right ..... 3

1.1 What a domain name is ..... 4

1.2 Cybersquatting and typosquatting ..... 4

2. Reading an address without being fooled ..... 5

2.1 The rule for finding the real domain ..... 7

2.2 Characters that look alike ..... 7

2.3 Shortened links ..... 8

3. How to check and how to defend yourself ..... 8

3.1 Five habits that save the day ..... 9

3.2 An unknown online shop: how to tell if it is serious ..... 10

4. Social engineering: manipulating people ..... 11

4.1 The levers it uses ..... 12

4.2 A few techniques, with examples ..... 13

4.3 A procedure beats good will ..... 14

5. Identity theft ..... 14

5.1 Where the data comes from ..... 14

5.2 How to reduce the risk ..... 15

5.3 If you think you have been hit ..... 16

Practical exercise ..... 18

Questions that come up in class ..... 19

Glossary ..... 19

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**
>
> Recognise a fake site by reading its domain, defend yourself with bookmarks and checks, and understand how social engineering and identity theft exploit people more than machines.

**What you will be able to do**

- Explain what cybersquatting and typosquatting are.
- Read a web address and find the real domain.
- Check a site before entering passwords or payment details.
- Recognise the levers of social engineering and answer with a procedure.
- Reduce the risk of identity theft and know how to react.

## 1. The site that looks right

A single wrong character in an address can take you to a page identical to the real one, but run by someone else.

Giulia works in the office of a public body. She needs to open the services portal, whose address is www.ente-esempio.it. She is in a hurry, types the address from memory and presses enter. A page appears that looks identical: same logo, same colours, same password box. She enters her credentials. Then she notices that the address was www.ente-esenpio.it, with an "n" instead of an "m".

That page was a trap site. Whoever built it did not hack anything: they simply registered an almost identical name and waited for someone to make a typing mistake.




A page's look can be copied: check the address.

## 1.1 What a domain name is

The **domain name** is the part of the address that identifies a site, for example *ente-esempio.it*. It is registered through authorised companies, and anyone can register a free name. There is no check on whether the name resembles someone else's.

## 1.2 Cybersquatting and typosquatting

**Cybersquatting** means registering a domain name that is identical or very similar to the name of a company, an organisation or a well-known person, to resell it at a high price or exploit its fame. The term comes from *to squat*, to occupy a place without permission.

**Typosquatting** is a variant: you register domains with likely typing mistakes (a *typo* is a slip of the fingers), hoping the user will mistype. No need to trick anyone with an email: just wait.

| Real site | Examples of trap sites |
|---|---|
| www.ente-esempio.it | www.ente-esempio.com (different ending) |
| www.ente-esempio.it | www.ente-esemp1o.it (the "i" replaced by the number one) |
| www.ente-esempio.it | www.ente-esempio-it.net (the dot turned into a hyphen) |
| www.ente-esempio.it | www.ente-esenpio.it (one letter changed) |

Similar domains that fool the eye (invented examples).



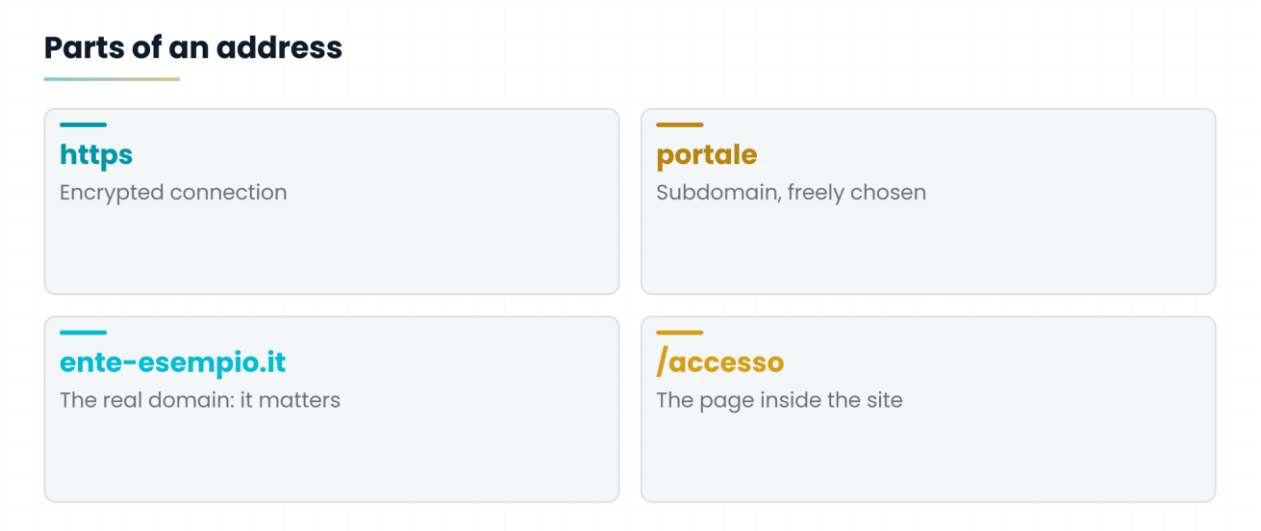

Similar names and typing mistakes can be exploited to deceive.

What do these sites host? Pages that imitate the real ones to **steal credentials**, shops selling counterfeit goods or goods never shipped, sometimes pages that spread **malware**, the harmful software from the lesson on ransomware.

> **THE IDEA IN ONE LINE**
>
> The trap site does not attack you: it waits for you to slip, or sends you a link that looks right.

## 2. Reading an address without being fooled

To spot a fake address you need to know how a real one is built. Take an invented one: **https://portale.ente-esempio.it/accesso**. It reads in pieces.




The parts of a web address

- **https://** is the protocol: it means the connection is encrypted, that is, data on the way is made unreadable to anyone who intercepts it;
- **portale** is the subdomain, a section chosen by whoever runs the site (it can be any word);
- **ente-esempio.it** is the real domain, the part that matters, made of the name and the ending (.it, .com, .net...);
- **/accesso** is the path, that is, the page inside the site.




Protocol, subdomain, domain and path each have a different job.

## 2.1 The rule for finding the real domain

Find the first slash (/) after https:// and look at **the two words just before it, separated by a dot**. Those are the real domain. Everything further to the left can be freely chosen by whoever owns the domain.

> **THE SUBDOMAIN TRICK**
>
> Look at this address: **https://ente-esempio.it.accesso-sicuro.net/login**
>
> At first glance it seems to belong to the organisation, because "ente-esempio.it" comes first. But the real domain is **accesso-sicuro.net**: everything before it is just a subdomain chosen by the scammer.
>
> Compare with **https://servizi.ente-esempio.it/login**: here the real domain is ente-esempio.it and "servizi" is a subdomain of the organisation. This address is trustworthy.




The organisation's name at the start does not prove the site belongs to it.

## 2.2 Characters that look alike

Some characters are easily confused by eye. The number zero and the letter "o". The number one and a lowercase "l". Two letters side by side, like "r" and "n", that look like an "m". In some cases scammers also use letters from other alphabets that look identical to ours. The browser, the program you use to surf, sometimes shows such addresses in a different form to warn you, but you cannot count on it.

**THE PADLOCK DOES NOT MEAN "HONEST SITE"**

The padlock next to the address (in Chrome, the settings icon to the left of the address) only shows that the connection is encrypted. A trap site can have one too. It says nobody is spying on the data while it travels, not that the site is what it claims to be.



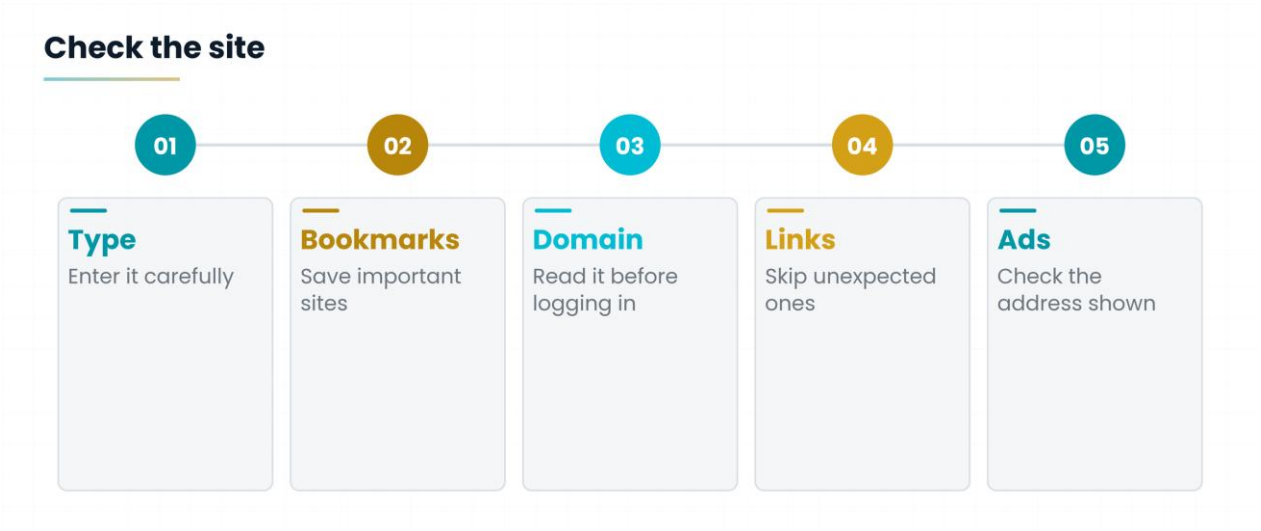

HTTPS protects the connection; it does not certify the site's honesty.

### 2.3 Shortened links

Sometimes a link is "shortened" by a dedicated service and you cannot see where it goes. It is handy, but in an unexpected message it is one more reason for suspicion. Better not to open it: go directly to the official site yourself.

## 3. How to check and how to defend yourself

The defences are few and simple. The hard part is turning them into a habit, especially when you are working in a hurry.




Five habits to avoid the trap site

### 3.1 Five habits that save the day

1. **Type carefully** the addresses you enter by hand and reread them before pressing enter.
2. **Bookmark** important sites (bank, mail, the organisation's portals): you reach them with one click, with no risk of a typing slip.
3. **Always check the domain** in the address bar before entering a password: read from the ending towards the left.
4. **Do not follow links in unexpected messages**: open the site from your bookmarks or by typing the address.
5. **Distrust ads at the top of search results**: they can be sponsored. Before clicking, check that the address shown is the right one.




Reread, use bookmarks and check before entering credentials.

One more help: a password manager (you will see it in the lesson on passwords) usually offers your credentials only on the site they were saved for. If it does not offer them, you may be on a different site from the real one. It is not infallible, but it is a good alarm bell.

### 3.2 An unknown online shop: how to tell if it is serious

Trap sites are not only for stealing passwords. Many are fake shops, with prices that look like a bargain. Before buying from a site you do not know, look at a few signs.

| Sign | What it may mean |
|---|---|
| Prices far lower than everyone else | An offer too good to be true often is. |
| No company details (name, address, VAT number) | A serious shop shows them and you can check them. |
| Only payments you cannot reverse (bank transfer, top-up) | If something goes wrong, you cannot go back. |
| Reviews all alike and all enthusiastic | They may have been written by a single person. |
| Strange address or unusual ending | Check how long it has existed and what others say about it. |

Signs that make you suspect a fake online shop.




Clues to check before buying.

**CASE STUDY: HALF-PRICE TONER**

The office of a small practice is looking for printer toner and finds a site with prices cut in half. The address is very close to that of a well-known big retailer, with one extra hyphen.

The site shows no company name, accepts only bank transfer and promises discounts "today only".

**What to do:** do not pay. Open the known retailer's site from your bookmarks, compare, and report the suspicious address to your IT contact.

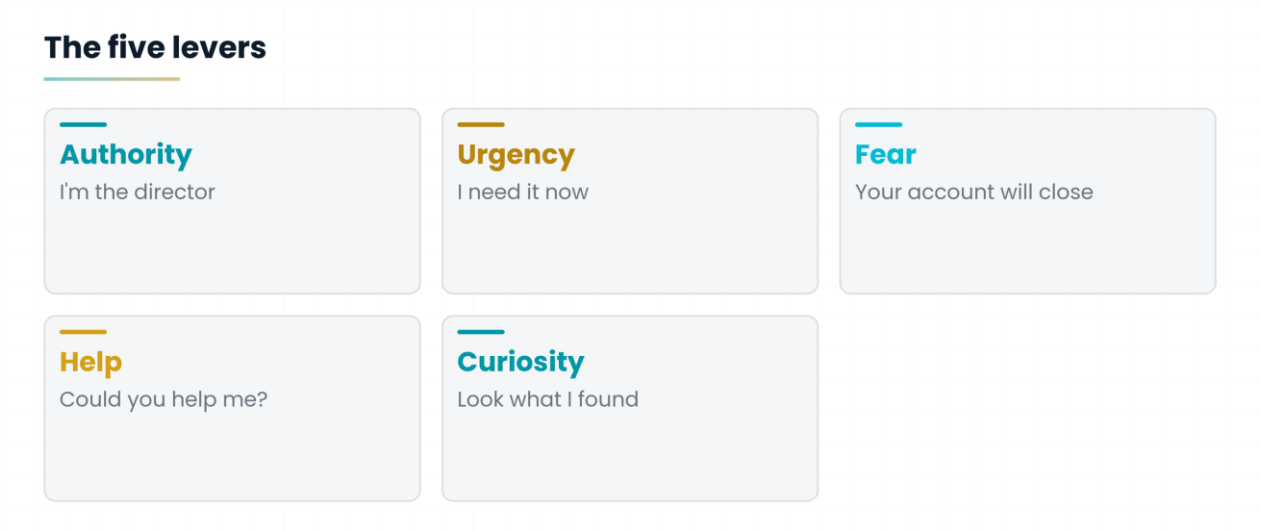
## 4. Social engineering: manipulating people

Breaking into a computer is hard. Persuading a kind person to give you the password is much easier.

**Social engineering** is the art of manipulating people, more than machines, to obtain information or access. The phishing from the previous lesson is one form of it. But social engineering is wider: it can be a phone call, a fake badge, a person in a smart suit who walks in behind you.

## 4.1 The levers it uses

The stories change, the levers do not. Whoever is trying to fool you aims at one of these sensitive spots.




The five levers of social engineering

| Lever | How it sounds | What to do |
|---|---|---|
| **Authority** | "This is the director" or "this is the police" | Verify with a number you already know. |
| **Urgency** | "I need it now, it's an emergency" | Slow down: urgency is designed to stop you thinking. |
| **Fear** | "Your account will be closed" | Check from the real site, not from the message. |
| **Help and likeability** | "Could you help? I can't find the password" | Being kind does not mean handing out access. |
| **Curiosity** | A found USB stick, a "confidential" file | It is not yours and you do not know what is on it. |

The five levers most used by social engineering.




Authority, urgency, fear, help and curiosity can become levers of deception.

## 4.2 A few techniques, with examples

- **Pretext (pretexting):** the scammer invents a believable story. Example: phones pretending to be technical support to get your password.
- **Bait (baiting):** leaves a tempting object. Example: a USB stick labelled "Salaries" dropped in the car park. Whoever plugs it into a computer may install malware.
- **Physical access (tailgating):** slips into an office behind you, perhaps with arms full of boxes, and you hold the door.
- **Information gathering:** before attacking, the scammer looks at organisation charts, social media and sites to know who you are and who you work with.

> **CASE STUDY: THE FAKE TECHNICIAN**
>
> A polite man phones: "I'm from IT support, we're updating the organisation's computers. I need your password to finish quickly; otherwise we risk locking your mail".
>
> He knows your colleague's name and your manager's, which makes him believable. But he asks for the password, the mark of a scammer: a real technician does not need one.
>
> **What to do:** refuse politely, ask for name and number, hang up and call the IT contact on the usual number. Then report the attempt, because the same man might phone another colleague.




A familiar name does not authorise a request for your password.

### 4.3 A procedure beats good will

Saying no to a kind person who says they need help is hard. That is why you need a written rule, valid for everyone, even the director: that way the "no" is not personal, it is the procedure. For example: **no password is ever shared with anyone**; **every visitor has an escort**; **every strange request is checked on another channel**.

## 5. Identity theft

**Identity theft** means using someone's data to open accounts, make purchases, sign contracts or apply for loans in their name. Victims may notice only months later, when a payment demand arrives for something they never bought.

### 5.1 Where the data comes from

Data can come from many routes, and you have met many of them in these lessons: a password stolen through phishing, a trap site, a data breach at a service, a document left in view, a public social media profile full of information (date of birth, town, pet names, places you visit).

Put together, these fragments say a lot. For a scammer, name, date of birth and address are already a good start to sound credible on the phone or to guess a security answer.




Stolen data can be used to impersonate a person.

## 5.2 How to reduce the risk

- **Share the minimum.** Do not post documents, tax codes, photos of tickets, cards or passes on social media.
- **Do not leave documents lying around.** Photocopies of ID cards and passes must not stay on the desk or in the printer.
- **Check your passwords and accounts.** A password reused on several services opens every door when one of them is breached (we cover this in the lesson on passwords).
- **Look at your statements.** An unknown charge should be raised with the bank at once.
- **Destroy documents before throwing them away.** A sheet with personal data does not belong in the bin as it is.




Share the minimum and look after other people's documents too.

**OTHER PEOPLE'S DOCUMENTS**

In an office, ID cards, tax codes and documents of members and clients pass through your hands. Identity theft can hit them too, and you are responsible for how you keep them. If you lose one, tell the person in charge at once (we cover this in the lesson on privacy and data protection).

### 5.3 If you think you have been hit

If you find that someone is using your data or a client's, do not wait. Tell the bank if there are payments, change the passwords of the accounts involved, keep the evidence and contact the Polizia Postale e delle Comunicazioni (Italy's online-crime police unit; commissariatodips.it). The complete steps are in the lesson "What to do when it happens".




Warn, protect your access, keep the evidence and contact the authorities.

## Practical exercise

A short exercise using the browser you use every day, with nothing to install.

1. Open the browser and type by hand the address of a site you use often (your bank, your mail, the organisation's portal). Check that it is the right one and bookmark it.
2. Take four invented addresses and write down the real domain of each: https:*servizi.ente-esempio.it/login, https:*ente-esempio.it.accesso-sicuro.net/login, https:*www.ente-esempl0.it, https:*ente-esempio-it.net/accesso.
3. Search for the name of your bank or an organisation. See whether the first result is an ad, and compare its address with your bookmark.
4. Write on a sheet the office procedure for suspicious phone calls: what to answer, who to call, where to report.
5. Make an inventory of what is publicly known about you on social media: date of birth, workplace, family names. What would you remove?

> **SELF-CHECK**
>
> Why is www.ente-esempl0.it dangerous?
>
> What is the real domain of https://ente-esempio.it.accesso-sicuro.net/login?
>
> What is the difference between cybersquatting and typosquatting?
>
> What do you do if a "technician" phones and asks for your password?

## Questions that come up in class

**If the site has the padlock, is it safe?**

Not necessarily. The padlock says the connection is encrypted, not that the site is honest. A trap site can have it too: always check the domain.

**Is typing the address by hand enough to be safe?**

It reduces the risk, but a typing slip can take you straight to a trap site. For important sites, bookmarks are safer than typing every time.

**How do I know if an online shop is reliable?**

Look at the company details (name, address, VAT number), the payment methods, prices that are too low, and look for opinions outside the site. If in doubt, pay with a method that lets you dispute the charge, not with a bank transfer.

**How do I behave with someone who asks me for help and seems sincere?**

Kindly, but following the procedure. A real colleague understands a check: "I'll call you back on a number I know" offends nobody.

**Can I find out whether my data is already out there?**

There are services that warn you if an email address appears in a known breach. They do not give a full guarantee, and you should use only reliable, official ones. In any case: a different password for every service.

**Can I register a domain similar to mine to protect myself?**

Yes, many organisations register the likeliest variants, such as the .com ending or the commonest typo. It does not protect against everything, but it lowers the risk. Owners of a trademark can also start procedures to recover a domain registered in bad faith, with a lawyer's help.

## Glossary

| Term | What it means |
|---|---|
| **Browser** | The program used to surf websites. |
| **Cybersquatting** | Registering a domain name identical or similar to that of a company or well-known person, to resell it or exploit its fame. |
| **Domain name** | The part of the address that identifies a site, for example ente-esempio.it. |

| Term | What it means |
|---|---|
| **Identity theft** | Using someone's data to open accounts, make purchases or sign contracts in their name. |
| **Malware** | Harmful software created to damage a computer or steal data. |
| **Social engineering** | Manipulating people, more than machines, to obtain information or access. |
| **Subdomain** | The part of the address to the left of the real domain, which the owner chooses freely. |
| **Typosquatting** | Registering domains with likely typing mistakes, hoping the user will mistype. |

## Further reading

**Registro .it** - the registry of Italian domain names, with rules and information on registration

**Polizia Postale e delle Comunicazioni** - commissariatodips.it, for reports and advice on online scams and identity theft

**National Cybersecurity Agency (ACN) and CSIRT Italia** - alerts and guides on cyber threats

**Garante per la protezione dei dati personali (the Italian Data Protection Authority)** - garanteprivacy.it, guidance on identity theft and data protection

> **WATCH OUT**
>
> Information up to date as of October 2026. Examples, names and domains (such as ente-esempio.it) are invented. Italian bodies are explained in brackets; elsewhere use your national equivalents (the police cybercrime unit, the domain registry of your country, the data protection authority). Domain registration rules and reporting procedures can change: always check the official channels listed.