



Phishing and its variants

How to spot a scam that arrives by email, text message, phone call or QR code

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



Contents

How to use this handout 3

1. A scam that looks real 3

1.1 Why it works, even on careful people 4

1.2 What an office really stands to lose 5

2. The variants: same goal, different channels 6

2.1 Spear phishing: the message made to measure 7

2.2 Smishing: the bait lands on your phone 7

2.3 Vishing: the voice that sounds sure 8

2.4 Quishing: the QR code that hides the link 8

3. The warning signs 8

3.1 Case study: the fake tax office email 10

4. The "stop and check" list 10

4.1 The official number: where to find it for real 11

4.2 Rules that apply to everyone 12

5. Three cases from everyday work 13

5.1 Case 1: the invoice you were not expecting 13

5.2 Case 2: the QR code on the car park notice 14

5.3 Case 3: the "technician" who calls 14

Practical exercise 16

Questions that come up in class 17

Glossary 18

Further reading 18

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 phishing and its variants (spear phishing, smishing, vishing, quishing) and apply the "stop and check" list every time before you click, open or reply.

What you will be able to do

- Explain what phishing is and why it works even on careful people.
- Tell phishing, spear phishing, smishing, vishing and quishing apart by the channel they use.
- Recognise the warning signs of a suspicious message.
- Apply the "stop and check" list: sender, urgency, link, expected attachment.
- Verify a doubtful request by calling the organisation's official number.

1. A scam that looks real

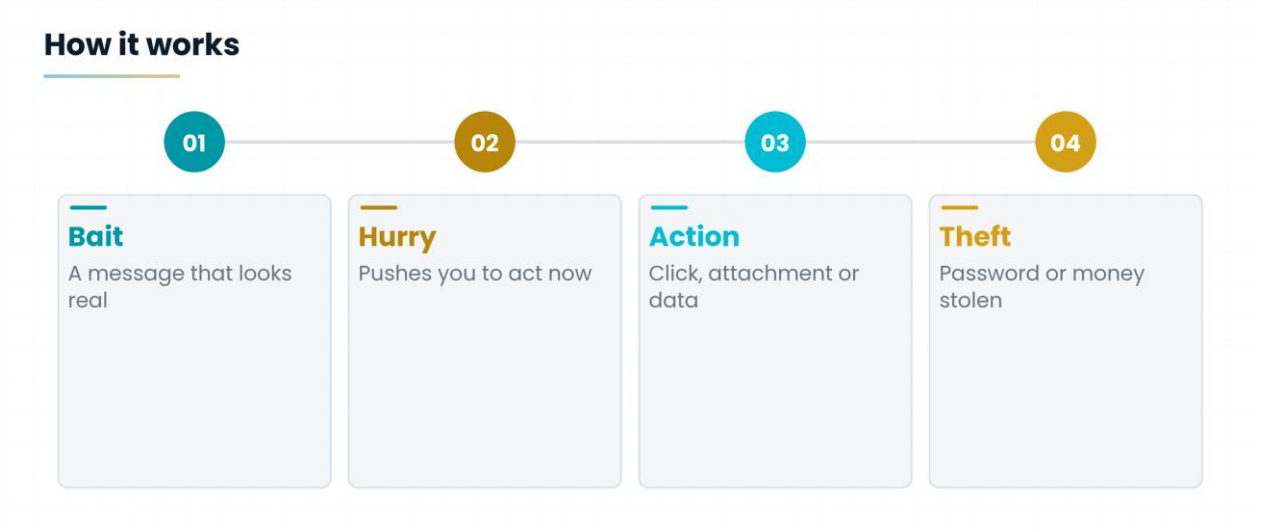
A criminal does not need to break into your computer if they can talk you into opening the door.

It is Monday morning in the office of Studio Esempio. Marta opens her mail and finds what looks like a message from a courier: "Your parcel is on hold, confirm your details today". She really was expecting a parcel. The logo is right, the tone is polite but firm. Her finger is already on the link.



An expected message can become bait.

That message is **phishing**. The word comes from *fishing*: the scammer throws out some bait and waits for someone to bite. They pretend to be a person or organisation you trust (a bank, a courier, the tax office, a colleague, the director) to get you to do one of three things: click a link, open an attachment, or hand over confidential information.



How a phishing attack works, from bait to theft

1.1 Why it works, even on careful people

Phishing does not attack machines, it attacks people. There is no flaw to exploit in the computer: the flaw is hurry, trust, and the distraction of a Monday morning. That is why even skilled people fall for it.

Scammers almost always pull the same levers. They play on **urgency** ("by today"), **fear** ("your account will be suspended"), **authority** ("this is the director"), **curiosity** ("a photo of you") or your wish to be **helpful** ("I need a hand"). If a message pushes you to act without thinking, that is already a warning sign.



Spotting the pressure helps you slow down.

> **THE IDEA IN ONE LINE**
>
> Phishing changes channel and disguise, but the goal is always the same: to make you act before you think.

1.2 What an office really stands to lose

If Marta types her password into a fake page, the scammer can get into the office mailbox, read clients' messages, download lists with names and tax codes, and send more messages in Marta's name. One stolen password opens the door to everything else. That is why this lesson comes right after the one on malware: many attacks begin with a message just like this.



A stolen password can expose the mailbox and the contacts.

2. The variants: same goal, different channels

When fake emails became easier to spot, scammers did not give up: they changed route. Today the same trick can arrive by email, text message, phone call or QR code. The channel changes, the purpose does not.

Variant	Channel	Example
Phishing	Email	"Your account is suspended, log in now"
Spear phishing	Email aimed at one person	A fake message from the director to the office assistant: "Make this bank transfer right away"
Smishing	Text message (SMS)	"Parcel held, pay 1.99 euros handling fee"
Vishing	Phone call	A fake bank operator asking for the code you just received by text
Quishing	QR code	A fake QR code on a parking meter or leaflet that leads to a trap site

Phishing changes channel, not goal.



The channel changes, the trick stays the same.

2.1 Spear phishing: the message made to measure

A *spear* is a fishing harpoon: you do not cast a net at random, you aim at one particular fish. The scammer studies the victim. They look at the office website, public social media profiles, colleagues' names. Then they write a believable message with the right name and the right tone.

> **CASE STUDY: THE DIRECTOR'S BANK TRANSFER**
>
> A message that seems to come from the director, Mr Rossi, reaches the office of a small organisation: "I'm in a meeting, can't call. Make an urgent transfer to a new supplier right now, I'm sending the IBAN. I'll explain later".
>
> The name is right and so is the tone. But the sender address is not the organisation's: it is a free email address with a similar name. And the request ticks every scam box: hurry, secrecy, money, no chance to phone.
>
> **What to do:** do not reply. Call the director on the number you already know, or ask in person or through a colleague. For payments, adopt a simple office rule: no new bank transfer without a second confirmation on a different channel.

2.2 Smishing: the bait lands on your phone

The name joins *SMS* and *phishing*. The message seems to come from the courier, the bank, the post office or the phone company: "Parcel on hold, pay 1.99 euros delivery fee".

The amount is small on purpose, so it does not make you suspicious. But the link leads to a page asking for your card details, and those details are worth far more than 1.99 euros.

On a phone it is harder to check the address, and we tend to trust more because a text feels personal. The advice is the same: do not tap the link, open the courier's official app or website yourself and check whether there really is a parcel.

2.3 Vishing: the voice that sounds sure

Vishing uses the voice (*voice* plus *phishing*). Someone calls and says they are from your bank: "We have spotted a suspicious transaction. To block it, please read me the code you are about to receive by text". The tone is professional and reassuring. The code, in fact, lets the scammer authorise an operation in your name.

> **GOLDEN RULE**
>
> A real bank never asks you by phone for passwords, codes received by text, or your PIN. If someone asks for a code, you are talking to a scammer. Hang up and call back yourself, on the number printed on the official website or on your card.

Sometimes the number on your display looks right, because scammers can fake it. So who is calling is not enough: what they ask for is what counts.

2.4 Quishing: the QR code that hides the link

A QR code is a square of dots that, when you point a camera at it, opens a web address. The problem is that you cannot read by eye where it leads. A scammer sticks a fake QR code on a parking meter, a car park post, a poster or a leaflet. Whoever scans it lands on a page that imitates the real one and asks for a card number.

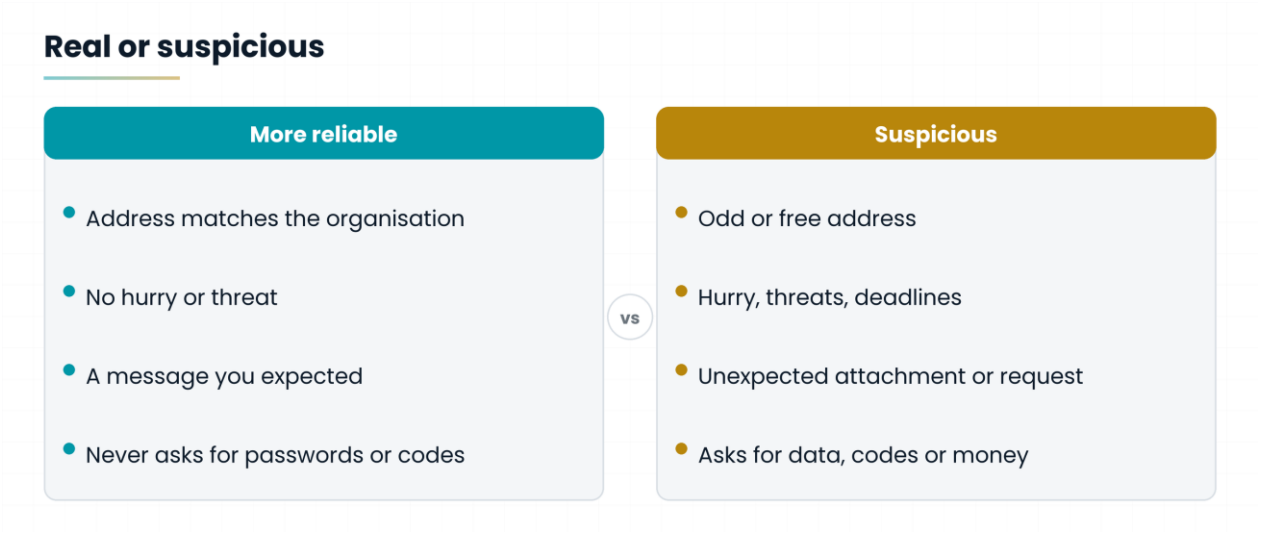
The QR code can also arrive inside an email or a PDF. Often it is a way to move the attack onto your phone, where there are fewer controls. Before opening the address, read the preview your phone shows: if the domain is not the one you expect, close it. On stickers, check they have not been glued over something else.

3. The warning signs

No single sign proves a message is fake, and no fake message has them all. But the more you find, the more careful you should be. Here are the main ones, with what to look at.

Sign	What to look at
Odd sender	Read the address, not just the name. A name can be fake, the address tells you where the message really comes from. "Tax Office" written from a free address or a strange domain is a red flag.
Hurry or threat	"By today", "final notice", "your account will be closed". A serious organisation gives you time to check.
Generic greeting	"Dear customer" instead of your name. It is not decisive, but an organisation that knows you usually uses your name.
Suspicious link	The link text says one thing, the real address another. Hover the mouse over it, without clicking, and look at the bottom of the window.
Unexpected attachment	An invoice you were not waiting for, a "scanned document" from an unknown sender. Attachments with a double extension (such as .pdf.exe) are a classic.
Request for data	Passwords, PINs, codes, card numbers: no serious organisation asks for them by email, text or phone.
Mistakes and oddities	Clumsy sentences, blurry logo, odd translations. Useful, but not decisive: many fake messages today are written perfectly.

The most common signs of a suspicious message.



A reliable message and a suspicious one compared

DO NOT TRUST "IT LOOKS WELL WRITTEN"

Grammar mistakes used to give fake messages away. Today scammers can use translation and automatic writing tools, and the texts come out polished. A well-written message is not therefore a real one: look at the sender, the link and the request.

3.1 Case study: the fake tax office email

An email arrives with the header of the Agenzia delle Entrate (the Italian tax authority): "A refund in your favour has been found. Click here to enter your card details". The logo is right. But the sender's address is some random domain, the greeting is generic and the request is about a credit card.

A public body does not ask for your card details like this, and does not send you to outside pages through a link in a message. If you think there may be something real in it, log in yourself to the official site by typing the address by hand, or phone the office.

4. The "stop and check" list

Recognising every trick is impossible, because they keep changing. A habit, on the other hand, can be learned. Before you click, open or reply, stop for a moment and make four checks. Then, if you still have a doubt, one fifth move.



Sender, pressure, link, attachments and a check on another channel.

1. **Who is the sender, really?** Read the address, not just the name. On a phone, tap the name to see the full address.
2. **Is it rushing or threatening me?** If so, slow down on purpose. Hurry is the scammer's weapon.

3. **Where does the link go?** Hover the mouse over it, without clicking, and read the address shown at the bottom. On a phone, press and hold the link to see the preview.
4. **Was I expecting it?** If you get an attachment or a request you were not waiting for, looking real is not enough.
5. **When in doubt, check.** Call the organisation on its official number, or ask whoever looks after IT.



The visible text can hide a different destination.

4.1 The official number: where to find it for real

The number to call is not the one written in the suspicious message: that would be like asking the scammer whether they are a scammer. Look it up from a source of your own: the organisation's website typed by hand into the address bar, a bill, a contract, the bank card, a statement.



Call back using a number found from an independent source.

4.2 Rules that apply to everyone

- **No new payment and no change of IBAN (bank account number) without a second confirmation** on a channel different from the one the request came through, for example a call to a number you already know.
- **No password, no code** is shared with anyone. Not with a colleague, not with the "technician". A real technician does not need them.
- **When in doubt, show it to someone.** A second person looks with fresh eyes and does not have the hurry on their back.



A new transfer or a change of IBAN needs independent confirmation.

> **IN PLAIN WORDS**
>
> Stopping is not wasting time. It is the one move scammers cannot exploit.

5. Three cases from everyday work

Let us put it into practice. For each case, try first to decide what you would do, then read the answer.

5.1 Case 1: the invoice you were not expecting

At a school an email arrives: "Attached is the overdue invoice, please settle it". The sender is unknown, the attachment is called *invoice.pdf.exe*. The school secretary has not ordered anything from that supplier.

What to do: do not open the attachment. A double extension reveals a program pretending to be a document: it could be malware, as you saw in the previous lesson. Check the order records to see whether that supplier really exists, tell the IT contact, and delete the message.



An unexpected attachment does not become safe because it looks like an invoice.

5.2 Case 2: the QR code on the car park notice

Outside a shop there is a notice: "Pay for parking, scan the QR code". It looks a bit crooked, stuck over the original notice. The QR code opens a site with a card payment form.

What to do: do not scan it. If the car park has an official app or a meter, use those. A sticker glued over the original notice is a warning sign. If you have already typed in your card, call the bank right away to block it and go to the lesson on what to do when it happens.

5.3 Case 3: the "technician" who calls

The phone rings: "Good morning, I am from your mail provider's support. We noticed an unusual login and I need the code that is about to reach your phone, to block it". The tone is polite and confident, and the code really does arrive while you are talking.

What to do: end the call. The code that arrives is exactly what the scammer needs, because at that very moment they are trying to get into your account. No serious service asks you for that code by voice. Then tell your IT contact and change your password from the real site, as you will see in the next lessons.



A code that has just arrived must not be given to whoever calls.

IF YOU HAVE ALREADY CLICKED

Do not be embarrassed and do not hide it: speed matters more than awkwardness. Isolate the computer, tell the person in charge right away and change your passwords from the real site. The complete four steps are in the lesson "What to do when it happens".



Clicked by mistake? Tell someone straight away. To practise, observe without opening links or attachments.

Practical exercise

A short exercise, alone or in pairs, using the latest emails and messages you have really received.

1. Open your spam (junk mail) folder and pick three messages. If you have none, use an email from the last few days that seemed odd to you.
2. For each one write on a sheet: who the sender is (full address), what they ask for, which lever they use (hurry, fear, authority, curiosity).
3. Hover the mouse over each link, without clicking, and note the address that appears at the bottom: does it match what the text claims?
4. Apply the "stop and check" list and decide for each: delete, report, or check with the official number.
5. If you work in pairs, swap sheets and discuss the differences. Then write together your office rule for new bank transfers.

> **SELF-CHECK**
>
> What is the difference between phishing and spear phishing?
>
> Why does a real bank never ask you for a code over the phone?
>
> What are the four checks of the "stop and check" list?
>
> Where do you find the official number to call when in doubt?

Questions that come up in class

Can I spot phishing from grammar mistakes?

Not any more. It used to be a good clue, but many fake messages today are carefully written. Trust the tone less and the facts more: sender, link, request for data or money.

If I hover over the link and it looks normal, can I click?

If the address matches what you expect, that is a good sign, but not a guarantee. If you have doubts about the message, still do not click: open the site by typing the address by hand or from the official app.

I clicked a suspicious link but typed nothing. Am I at risk?

Usually the main risk is in typing in data or downloading something. Close the page, download nothing and tell your IT contact. If you downloaded or opened a file, or entered data, go straight to the steps in the dedicated lesson.

The message seems to come from a colleague I know. Can I trust it?

Not always: the address can be forged or the colleague's account may have been stolen. If the request is unusual (money, passwords, confidential files), confirm with a phone call or in person.

Can I scan a QR code safely?

Scanning on its own will not harm you, but it takes you to a page you do not know. Look at the address in the preview before opening it, and never type passwords or card details into a page reached this way unless you are sure.

How do I report a phishing attempt?

Tell the IT contact of your office or school. If money or other people's data are involved, keep the messages and contact the Polizia Postale e delle Comunicazioni (Italy's online-crime police unit; in the US the nearest equivalent is the FBI's IC3), through commissariatodips.it.

Glossary

Term	What it means
IBAN	The code that identifies a bank account and to which a bank transfer is addressed.
Phishing	A scam in which a criminal pretends to be a trusted organisation or person to make you click, open an attachment or give confidential data.
QR code	A square of dots that a camera reads and turns into a web address or text.
Quishing	Phishing through a fake QR code, for example on a sticker or leaflet.
Sender	Whoever sends the message; the real address matters more than the displayed name.
Smishing	Phishing by text message, often with fake alerts from couriers or banks.
Spear phishing	Targeted phishing: the message is made to measure for one specific person, using information about them.
Vishing	Phishing by phone: the caller pretends to be, for example, a bank operator.

Further reading

Polizia Postale e delle Comunicazioni, online police station - commissariatodips.it, for reports and advice on online scams

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

Garante per la protezione dei dati personali (the Italian Data Protection Authority) - garanteprivacy.it, information sheets on phishing and data security

> **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; if you live elsewhere, use your country's equivalent (your national police cybercrime unit, tax office and data protection authority). Techniques change fast: the checking method matters more than any single example.