

Cybersecurity and Confidentiality

Protecting and securing data

MAYOLY
Taking your care to heart

Getting started: key notions



More targeted attacks

Cyberattacks are increasingly targeted and sophisticated.



Social engineering is diversifying

It no longer relies on emails alone, but also on QR codes, text messages and phone calls.



The human factor

A major risk for organisations, especially as the human factor plays a decisive role in their success.

Our vigilance, our best defence

Our vigilance remains our best defence!

On top of everything the IT teams put in place.

Know the risks

Knowing fraud attempts (phishing, vishing, smishing, quishing…) helps you spot risky situations and react better.

Adopt good practices

Data confidentiality and discretion on social media are an integral part of the shield we must build.

To start: a question

In your opinion, cybersecurity incidents originate from human error in:

- **A** 10% of cases
- **B** 38% of cases
- **C** 55% of cases
- **D** **80% of cases**

Correct answer: D – 80% of cases.

A few figures to start with

8,150

billion dollars: estimated worldwide cost of cybercrime in 2023

+70%

estimated increase in the worldwide cost of cybercrime by 2029

80%

of cybersecurity incidents worldwide originate from human error

45%

of companies are expected to face software supply chain attacks in 2025, 3 times more than in 2021

39 s

a cyberattack takes place somewhere in the world every 39 seconds

Human vigilance is our first line of defence.

Sources: statista.com; Le Monde Informatique

Growing data security challenges



Rising number of cyberattacks

Companies must strengthen their defences to counter the growing number of intrusion attempts and attacks.



Use of artificial intelligence

AI generates personalised, more convincing scams and can target organisations whose security is seen as weak.



Risk of losing trust

A successful attack can cause an irreversible loss of trust, damaging the company's reputation and credibility.

Five attack techniques to know



Phishing

EMAIL

Fraudulent email impersonating a third party



Vishing

PHONE

Call or voicemail from a fake advisor or support agent



Spear phishing

EMAIL / SMS

Targeted, personalised and highly credible message



Smishing

SMS

Text message urging you to click a link



Quishing

QR CODE

Booby-trapped QR code leading to a fake site

Phishing

DEFINITION

An email impersonates a third party (company, administration…) to push you to share personal, professional or banking information, or to open a link or an infected attachment.



EXAMPLE

You receive an email reminding you that a mandatory training (quality, safety or compliance) must be completed by the end of the week, with a link to log in to the platform

RULES TO FOLLOW

- Do not give in to “urgency”
- Check the sender's address by hovering over it
- Hover over the link before clicking; do not open the attachment
- Never share confidential information through the link

Vishing

DEFINITION

Voice phishing: scammers call or leave a voicemail posing as a bank advisor, IT support… to extract personal or banking information. They can display the phone number of the person or company they impersonate.



EXAMPLE

“Technical support” contacts you and asks for your Windows or business application password to “fix” a problem.

RULES TO FOLLOW

- Never give your password to anyone
- Do not trust the number or location of the call
- Call back through another channel to verify the request
- Real support never asks for confidential information

Spear phishing

MAYOLY

DEFINITION

An email or text impersonating a third party, but targeted: instead of aiming at a wide audience, scammers choose their target carefully and craft the message. It is personalised, credible and plays on trust or urgency.



EXAMPLE

You receive an email from your manager inviting you to join a Teams group.

RULES TO FOLLOW

- Do not give in to “urgency”
- Check the sender's address by hovering over it
- Contact the sender through another channel to verify the message
- Do not click the link or open the attachment

Smishing

DEFINITION

A method used by cybercriminals to deceive victims by text message, impersonating a known third party (administration, bank, delivery…). The short message urges you to click a link to hand over personal or banking information or credentials, or to install a malicious app.



EXAMPLE

You receive a text saying your parcel could not be delivered and inviting you to click a link to reschedule delivery.

RULES TO FOLLOW

- Always be wary of urgent messages
- Do not click the link: type the official site address in your browser (fake sites imitate real ones almost perfectly)
- Report the fraudulent text to the relevant authorities

What to do with a suspicious message?



Report via Outlook

From Outlook: “Report message” button or right-click, then phishing.



Security team

Forward the message to the security team: they will analyse and block the threat.



IT support

Contact IT support for help on what to do next.

More information on cybersecurity and data protection is available on the intranet.

Data confidentiality



Unsolicited access is prohibited

Accessing personal data not requested by a client is strictly prohibited. It notably constitutes:

- a violation of the right to privacy
- a breach of the information systems charter and the GDPR
- a breach of the duty of loyalty and confidentiality

Unauthorised disclosure

It is strictly forbidden to disclose or pass on client data to colleagues for non-work purposes, or outside the company, whatever the medium.

Confidentiality and discretion

Respecting these fundamentals protects the client, but also protects yourself and the company from any legal and/or financial penalty.

Special case: social media

Confidentiality requirement

Some partners entrust us with their customer relationship, but also their image and reputation, with a clear expectation: never publicly reveal the collaboration. This is a contractual requirement: breaching it exposes us to financial penalties and loss of the partnership.

Discretion is essential on social media

Do not mention or allude to your work for these brands on social media, especially LinkedIn. Even well-intentioned, such posts jeopardise our confidentiality commitment.

Quiz – Question 1 / 5

Spear phishing – You receive an email from your CEO urgently asking you to send a confidential file. What do you do?

A I send it immediately – it's the CEO after all!

B I reply to ask for more details

C **I check the email address and contact them through another channel to confirm**

Correct answer: Check the sender's address and contact the person through another channel before acting.

Quiz – Question 2 / 5

Vishing – You get a call from an IT technician asking for your password to “fix an urgent problem”. How do you react?

A. I offer to call back later

B. I give the password, they must need it

C. I note their number to call back later

D. I hang up immediately and report the call

Correct answer: No IT service or other organisation (bank, administration…) ever asks for a password by phone. Report the call to IT support immediately.

Quiz – Question 3 / 5

Smishing – You receive a text saying: “Your bank account will be suspended within 24h. To avoid this, click here”. What do you do?

A. I forward the text to a friend for advice

B. I check with my bank, then ignore and delete the message: it's smishing

C. I reply STOP to unsubscribe

D. I click to check

Correct answer: Do not click. Check through another channel. If it is not your bank, delete the text and report it if possible.

Quiz – Question 4 / 5

Phishing – What should you do if you receive an email asking you to verify your Microsoft 365 password?

- **A** I don't click, I report the email as phishing and forward it to the security team
- **B** I click to check, just in case
- **C** I reply to the message to ask a question
- **D** I forward it to a colleague to test

Correct answer: Do not click: report the email as phishing and forward it to the security team.

Quiz – Question 5 / 5

Quishing – You receive an email from Microsoft inviting you to scan a QR code for a security update. What do you do?

A. I just scan to look, but I don't confirm anything

B. I scan immediately and follow the instructions: it's Microsoft so it's safe

C. I check the sender's address and, at the slightest doubt, report the message

Correct answer: Always check the sender's address and use another channel. Even in a private setting, stay vigilant: malicious QR codes are increasingly used.

Key takeaways

1. Don't give in to urgency: a pressing message is a warning sign
2. Verify the sender or caller, through another channel if in doubt
3. Never share passwords or confidential information
4. Don't click a link, open an attachment or scan a suspicious QR code
5. Report: Outlook button, security team, IT support

Thank you for your attention



mayoly.com