In 2025, the digital world is changing fast. Artificial Intelligence (AI) helps companies improve services and create new tools. But it also gives criminals new, powerful ways to attack computers, networks and people.

Security experts warn that cyber-attacks are becoming more frequent and more difficult to detect. One major trend is "ransomware": this is a kind of malicious software (malware) that locks a computer or steals data, then demands money to unlock or return it. In recent years, hundreds of new ransomware types have appeared.

At the same time, many businesses and organizations use cloud services (remote data storage and software over the internet), but often without strong security measures. This makes them vulnerable. Security specialists recommend a model called Zero Trust: each user or device must "prove" who they are every time they access data — nothing is automatically trusted.

AI itself is now a double-edged sword. On one hand, companies use AI to detect attacks more quickly and analyse huge volumes of data — this helps improve cybersecurity. On the other hand, attackers also use AI to build more advanced malware, create convincing fake messages (phishing), or manipulate people online.

Another concern for the near future is that powerful computers — called quantum computers — might break today's encryption (the locks that protect our data). Experts advise companies to prepare now by adopting "quantum-safe" encryption methods.

In conclusion: while technology offers many opportunities, it also creates serious risks. The balance depends on how we use new tools and protect ourselves. Strong security practices, regular software updates, and awareness are more important than ever.

- 🔎 Vocabulaire utile (à connaître avant de répondre)
- ransomware — logiciel malveillant qui bloque un ordinateur ou vole des données pour demander une rançon
- malware — logiciel malveillant / virus informatique
- to detect — détecter
- cloud services — services hébergés "dans le cloud" (stockage, applications en ligne)
- to access — accéder à (des données, un service…)
- encryption — cryptage / chiffrement (protection des données)
- quantum computer — ordinateur quantique
- security measures — mesures de sécurité
- phishing — hameçonnage (messages frauduleux pour tromper quelqu'un)

- ❓ Questions directes (5 — "find in the text")
- What kind of malware is described as demanding money to unlock or return data?
- What does the "Zero Trust" model require from users or devices when they access data?
- According to the text, what two opposite roles can AI play in cybersecurity?
- Why are cloud services considered risky, according to the text?
- What future technological threat could break today's encryption?

- Questions personnelles / implicites (5)
- Do you think individuals (private people) should do more to protect their online data? If yes — what could they do?
- If you were manager of a small company, what security steps from the text would you implement first — and why?
- Do you believe that new technologies (like AI) help more than they harm, or the opposite? Explain.
- How do you feel about the idea of "Zero Trust"? Does it make sense for daily life (not only companies)?
- Do you think governments should regulate AI and cybersecurity more strictly? What might be the advantages or disadvantages?