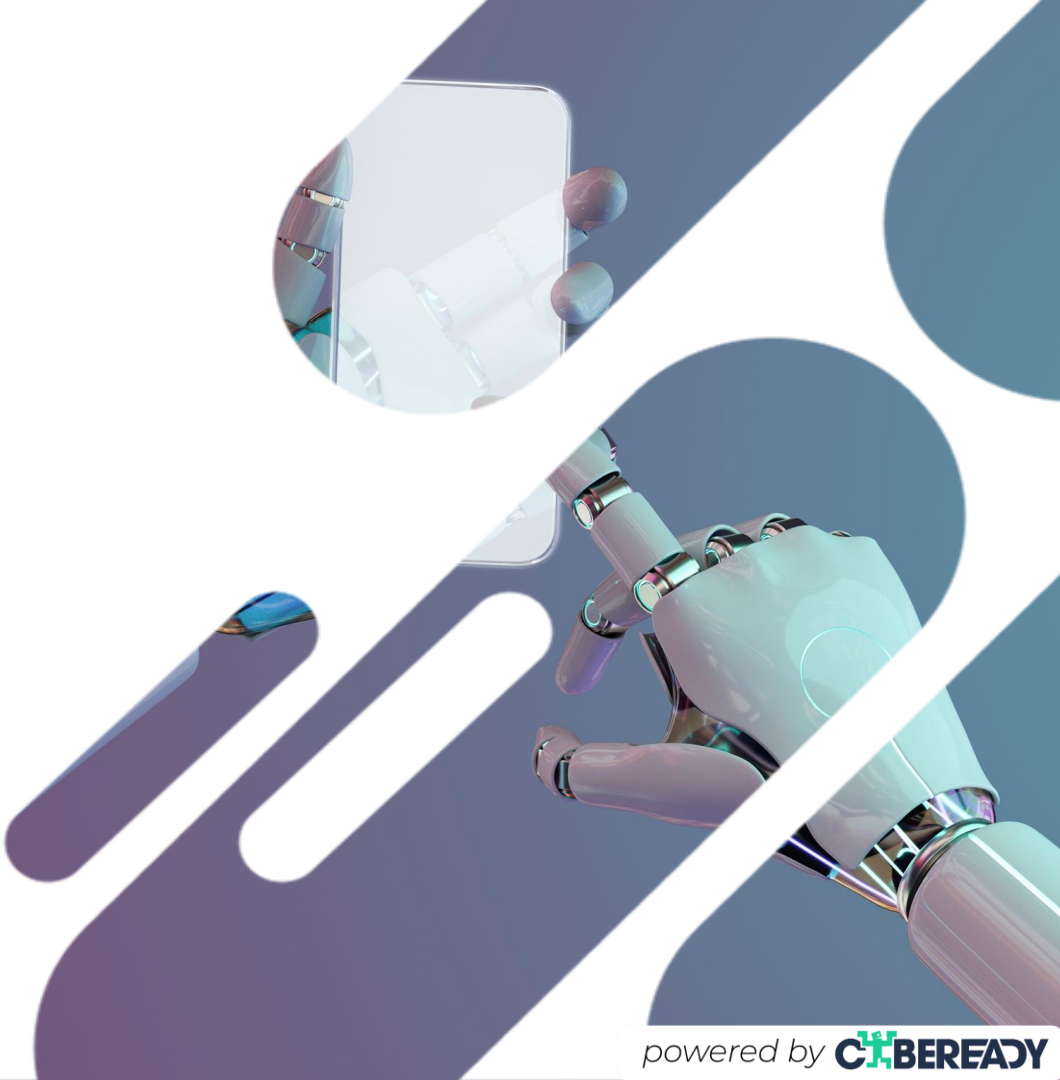
factis®

AI tools are changing the game for hackers.

Are you prepared?



powered by CYBEREADY

factis®

Previously...

Highly deceptive attacks required a lot of time and effort and could only be created by skilled hackers.

As a result, **most phishing attempts were at a novice level** (e.g. with spelling errors, suspicious designs, broken language, etc.), so spotting a fake was pretty easy.

Nowadays...

AI tools enable hackers to quickly and easily create highly professional-looking emails and content.

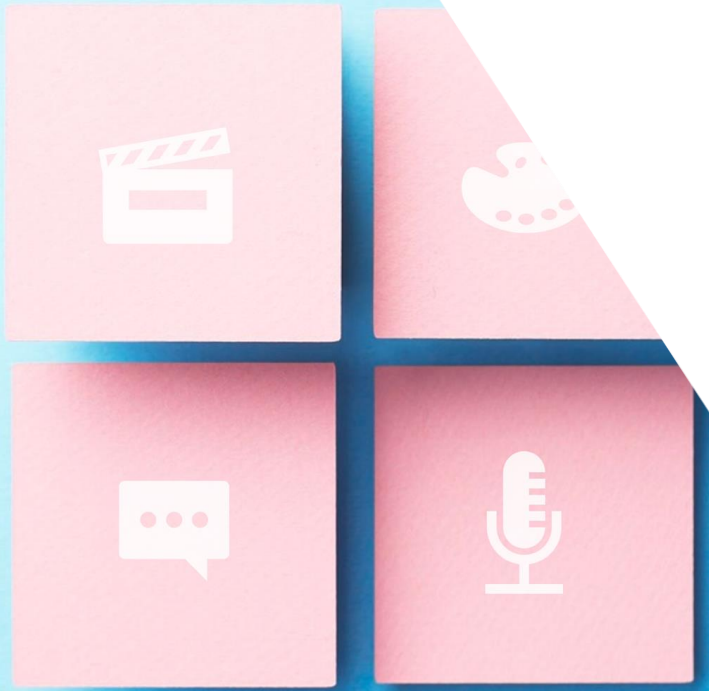
Because of this, **more sophisticated attacks have begun to reach our mailboxes.** These highly deceptive attacks are harder to identify as threats, increasing the risk that we'll fall for them.

factis®

How can you spot phishing now?

- In emails, ensure that **sender's address** appears exactly as expected. Hackers cannot fake this detail.
- Hover over **links** before clicking to ensure they look legitimate. Hackers can mimic famous company designs, but they cannot use their genuine domains.

powered by CYBERREADY



What's no longer a Reliable sign of authenticity?

- Professional designs
- Well-written texto
- Voice recording of someone you know
- High-quality videos

factis®

Remember:
Our safety is in our hands.

Make it a habit to examine every email before clicking on any links, and never check emails when you're distracted.