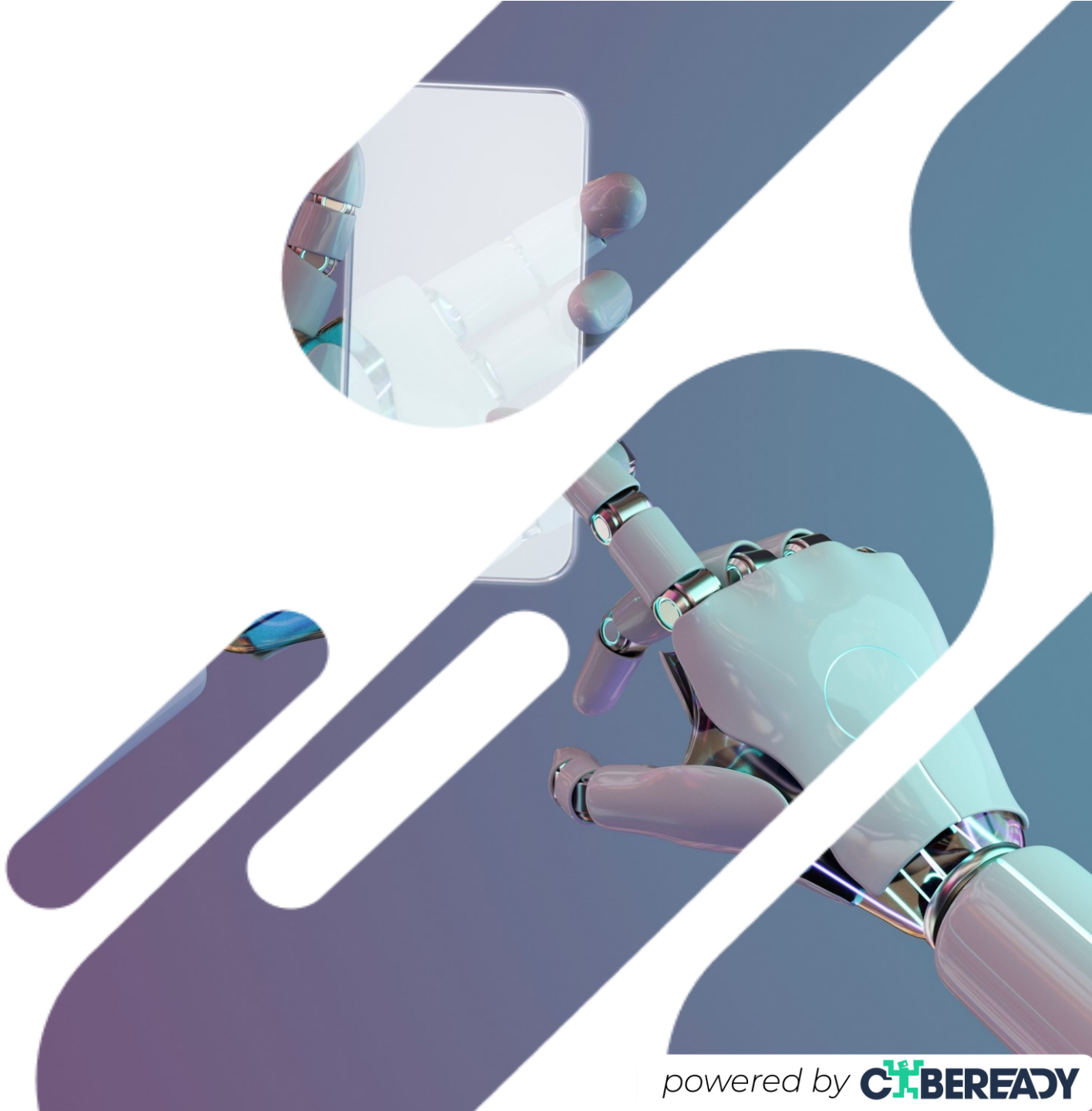
CYBEREADY

# Les outils d'IA changent la donne pour les pirates informatiques.

## Êtes-vous prêt ?



# Précédemment...

Les attaques très trompeuses nécessitaient beaucoup de temps et d'efforts et ne pouvaient être créées que par des pirates informatiques compétents.

}Par conséquent, **les tentatives d'hameçonnage les plus fréquentes sur le site**étaient d'un niveau débutant (avec des fautes d'orthographe, des dessins suspects, des erreurs de langage, etc.

# De nos jours...

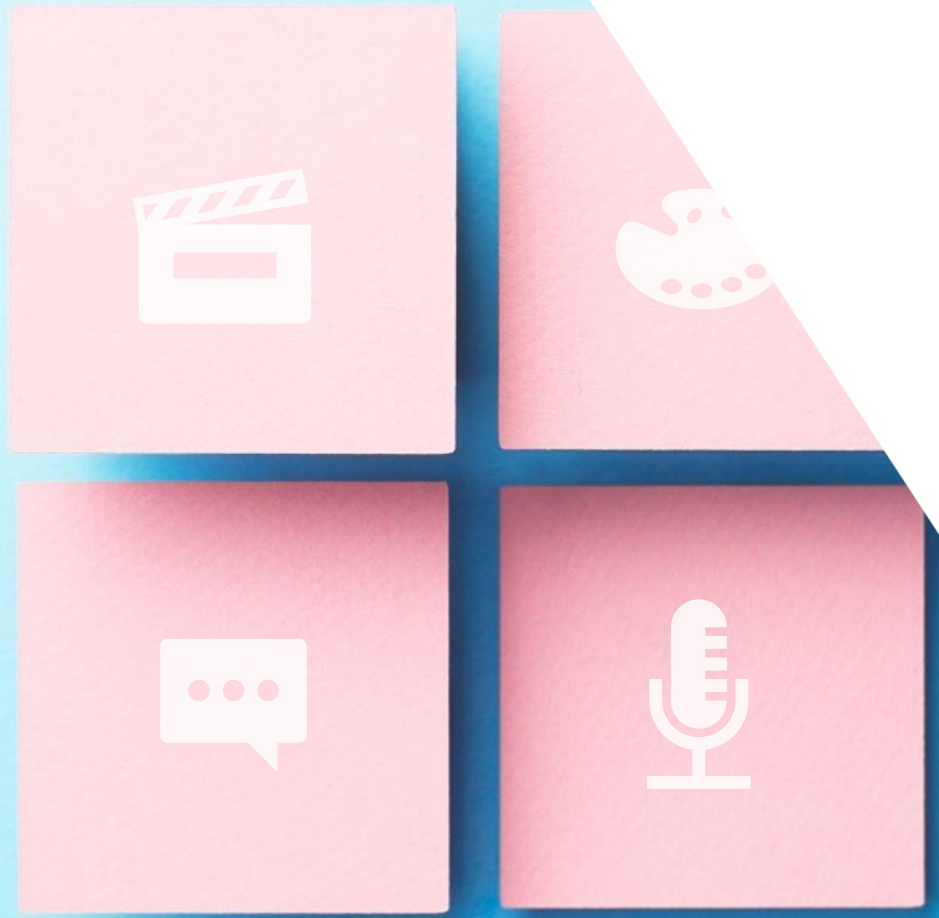
Les outils d'IA permettent aux pirates de créer rapidement et facilement des courriels et des contenus d'apparence très professionnelle.

C'est pourquoi **des attaques de plus en plus sophistiquées ont commencé à atteindre nos boîtes aux lettres électroniques.** Ces attaques très trompeuses sont plus difficiles à identifier comme des menaces, ce qui augmente le risque que nous tombions dans le panneau.

# Comment repérer les tentatives d'hameçonnage de nos jours ?

- Dans les courriels, veillez à ce que **l'adresse de l'expéditeur** apparaisse exactement comme prévu. Les pirates ne peuvent pas truquer ce détail.

- Survolez **les liens** avant de cliquer pour vous assurer qu'ils sont légitimes. Les pirates peuvent imiter le design d'entreprises célèbres, mais ils ne peuvent pas utiliser leurs domaines authentiques.



# Qu'est-ce qui n'est plus un signe fiable d'authenticité ?

- Modèles professionnels
- Texte bien écrit
- Enregistrement de la voix d'une personne que vous connaissez
- Vidéos de haute qualité

CYBEREADY

# **Rappel :** Notre sécurité est entre nos mains.

Prenez l'habitude d'examiner chaque courriel avant de cliquer sur un lien et ne consultez jamais vos courriels lorsque vous êtes distrait.