

OUCH!

Votre bulletin mensuel sur la sensibilisation à la sécurité

# Intelligence artificielle : Ce qu'il faut savoir

## Que puis-je faire ?

L'intelligence artificielle (IA) décrit des systèmes programmés pour penser et réagir comme des humains. En fait, nous avons posé cette question à la solution d'IA ChatGPT et nous avons obtenu la réponse suivante.

### *Qu'est-ce que l'intelligence artificielle ?*

*L'intelligence artificielle (IA) désigne la simulation de l'intelligence humaine dans des machines programmées pour penser et apprendre comme des humains. Elle implique le développement d'algorithmes et de programmes informatiques capables d'effectuer des tâches qui requièrent généralement l'intelligence humaine, telles que la reconnaissance de la parole, la compréhension du langage naturel, la prise de décisions et les jeux. Il existe plusieurs types d'IA, notamment l'IA basée sur des règles, les systèmes experts et l'apprentissage automatique.*

Ce qui rend l'IA si puissante, c'est qu'elle peut simuler l'intelligence et la capacité de raisonnement de l'esprit humain, mais elle peut analyser exponentiellement beaucoup plus d'informations que n'importe quel humain et le faire exponentiellement plus vite.

Le concept d'IA n'est pas nouveau. D'abord abordée dans les romans de science-fiction, l'IA est en cours de développement depuis des décennies. Si l'on en entend autant parler aujourd'hui, c'est parce que, pour la première fois, tout le monde a la possibilité d'interagir avec l'IA et d'en voir les véritables fonctionnalités.

ChatGPT, un robot de conversation en ligne doté d'une intelligence artificielle, est l'une des premières solutions accessibles au public capable de répondre comme un véritable humain, en réussissant ce que l'on appelle le test de Turing. Ce test détermine la capacité d'une machine à faire preuve d'un comportement intelligent en faisant interagir un véritable humain avec la machine par l'intermédiaire d'un canal de discussion textuel. Si l'homme ne peut pas dire s'il interagit avec une machine ou une personne, on considère que la machine a réussi le test. Les solutions d'IA sont aujourd'hui les premières disponibles publiquement à faire cela.

Cependant, les conversations en ligne ne sont que le début de ce que l'IA peut faire. Il existe aujourd'hui des solutions d'IA capables de créer une vidéo d'une personne donnant un cours dans n'importe quelle langue ou d'analyser des dossiers médicaux et de déterminer rapidement qui est le plus susceptible d'avoir un cancer. Elles peuvent aussi créer des articles de presse ou des essais sur le sujet de votre choix, générer des images pour des livres d'enfants ou créer du code pour de nouveaux programmes informatiques. Si l'IA n'est pas nécessairement à craindre, il existe néanmoins certains dangers dont il faut être conscient.

## Les dangers de l'intelligence artificielle

1. **Vous recréer** : Les solutions d'IA peuvent prendre un enregistrement de la voix d'une personne - votre voix - et l'utiliser pour créer un son en temps réel qui vous ressemble et qui dit ce qu'il veut pour se faire passer pour vous. Ainsi, un cyber-attaquant pourrait enregistrer un message vocal qui vous ressemble et faire croire à vos collègues, à votre banque ou à un membre de votre famille que vous les avez appelés pour leur demander d'effectuer une action. L'IA peut également le faire avec des images ou des vidéos. Parfois appelée "Deep Fakes » ou « hypertrucage », une solution d'IA peut prendre une photo ou une vidéo existante de vous et l'utiliser pour recréer des photos ou des vidéos entièrement nouvelles (y compris votre voix) où vous être en train de faire des choses que vous n'avez jamais faites.
2. **Mauvaises réponses** : En ce qui concerne les données ou les réponses fournies par l'IA, les solutions peuvent être erronées. L'IA utilise souvent des informations publiques provenant d'Internet, et ses réponses peuvent être influencées par les préjugés de ses développeurs. Alors que les moteurs de recherche classiques sont conçus pour vous fournir la "meilleure" réponse ou la plus correcte à vos requêtes, des solutions telles que l'IA peuvent être conçues pour vous donner la réponse la plus humaine possible. Le choix de la meilleure solution dépend de l'objectif que vous souhaitez atteindre.
3. **Pas tous égaux** : L'IA étant devenue la dernière technologie en vogue, des centaines de startups proposent aujourd'hui différents services liés à l'IA. Beaucoup d'entre eux demandent vos informations ou votre carte de crédit pour un essai. Attention, tous les services d'IA ne sont pas dignes de confiance. Faites vos recherches avant de vous inscrire et d'utiliser un service d'IA.
4. **Votre vie privée** : Lorsque vous utilisez ou interagissez avec un système d'intelligence artificielle, comme lors d'un chat en ligne avec ChatGPT, sachez que toute information que vous entrez dans le système peut non seulement être traitée par celui-ci, mais aussi conservée et utilisée pour donner des réponses à d'autres personnes. Cela signifie que si vous saisissez des informations personnelles vous concernant ou des informations confidentielles relatives à votre travail, ces informations seront stockées et potentiellement partagées ou vendues à d'autres personnes. Ne partagez pas et ne saisissez pas d'informations que vous considérez comme sensibles, personnelles ou confidentielles au travail.

## The Future of AI

L'intelligence artificielle en est encore à ses balbutiements, comme l'internet il y a vingt ou trente ans. Si l'on peut s'attendre à une évolution et à une adoption rapides de l'IA, il est très difficile de prédire quel sera son impact. Soyez simplement conscient que ces capacités existent et, lorsque vous utilisez l'IA, soyez très prudent quant aux informations que vous saisissez et partagez.

## Ressources

**ChatGPT** : <https://chat.openai.com/chat>

**Le test Turing** : [https://fr.wikipedia.org/wiki/Test\\_de\\_Turing](https://fr.wikipedia.org/wiki/Test_de_Turing)

**Traduit pour la communauté par : Juliette Busson**

OUCH! Est publié par SANS Security Awareness et est distribué sous la licence [Creative Commons BY-NC-ND 4.0.](https://creativecommons.org/licenses/by-nc-nd/4.0/) . Vous êtes libre de partager ou de distribuer ce bulletin d'information, à condition de ne pas le vendre ou le modifier. Comité de rédaction : Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.