Association Loisirs et culture

Quand l'IA décuple le potentiel... des escrocs

Jean Marie Herbaux

Table des matières

1. Le phishing par Messagerie : 2
2. L'hameçonnage par téléphone : 2
3. L'intelligence artificielle s'en mêle : 2
   a. Scénario : 2
   b. La méthode : 2
      - Une première IA 2
      - Une seconde IA 2
      - Une troisième IA 3
      - La collaboration des 3 IA : 3
      - Pour parfaire : 3
4. Soyons plus que jamais prudents 3

Ces dernières années, les arnaques par l'ingénierie sociale se multiplient. Plutôt que de profiter d'une faille informatique, les criminels s'attaquent à un autre point faible l'utilisateur. L'Ingénierie sociale consiste à mettre sa victime en confiance en le faisant croire que l'escroc est une personne de confiance. L'une des formes les plus simples est le phishing, ou hameçonnage.

1. Le phishing par Messagerie :

Exemple : Vous recevez un mail de votre banque, vous cliquez sur le lien, vous ouvrez le site de votre banque et vous vous connectez. Le mail était un faux, et le site aussi... et vous venez de donner votre identifiant et votre mot de passe aux escrocs

2. L'hameçonnage par téléphone :

D'autres formes utilisent le téléphone, comme le numéro surtaxé qui vous appelle, laisse sonner et raccroche, espérant que vous allez le rappeler ou qui laisse un message indiquant que vous avez un colis/une amende/une facture en attente et de rappeler un numéro, là encore surtaxé. Toutefois, ce genre d'escroquerie peut aller beaucoup plus loin, puisque s'il s'agit d'une cible importante, les escrocs peuvent prendre le temps d'analyser toutes les données publiques sur la personne, puis la contacter et ainsi la mettre en confiance grâce à tout ce qu'ils savent sur la personne, par exemple en se faisant passer pour une connaissance. Une technique qui ne fonctionnait qu'à l'écrit jusqu'à présent, ou parfois au téléphone quand ils savent que leur victime est âgée.

3. L'intelligence artificielle s'en mêle :

Toutefois, tout ceci est en train de changer. L'intelligence artificielle va bouleverser nos vies dans quasiment tous les domaines, y compris pour les escroqueries.

a. Scénario :

Imaginez un instant ce scénario. Un proche part en vacances. Quelques jours plus tard, il vous appelle. Son numéro s'affiche et vous reconnaissez tout de suite sa voix lorsqu'il vous annonce qu'il vient de subir une catastrophe, et qu'il demande si vous pouvez le dépanner d'un peu d'argent qu'il vous remboursera en rentrant. Vous n'hésitez pas et transférez l'argent. Le lendemain, vous l'appelez pour lui demander s'il a bien reçu l'argent et si la situation s'améliore. Il n'a aucune idée de quoi vous parlez et vous indique qu'il est allongé sur la plage à se détendre, comme il l'a fait toute la journée d'hier et sans vous avoir appelé. Et pourtant, c'était bien sa voix, et c'était bien son numéro qui s'était affiché.

b. La méthode :

Grâce à l'intelligence artificielle, ce genre d'arnaque risque de devenir courante.

- Une première IA

Une première IA analyse les réseaux sociaux, à la recherche de potentielles victimes, en accédant aux informations publiées publiquement, ou même en créant de faux profils, afin de devenir amis avec ses victimes et voir tout ce qu'elles partagent. Dans ce scénario, votre proche avait informé ses amis sur Facebook qu'il partait en vacances, et donc l'IA savait que c'était le meilleur moment pour se faire passer pour lui. Elle analyse son style d'écriture et enregistre toutes les informations publiées en quelques instants, elle peut donc facilement l'imiter à l'écrit, et même connaître des détails très personnels.

- Une seconde IA

Une seconde IA analyse les quelques vidéos qu'il a pu publier, même plusieurs années en arrière. Il suffit d'un enregistrement de quelques secondes de sa voix pour pouvoir l'imiter. Ce 'est pas de la science-fiction, puisque l'IA Vall-E peut déjà faire à partir d'un enregistrement de trois secondes seulement.

- Une troisième IA

Avec une troisième IA pour reconnaître vos amies et qui les transcrit en texte pour les envoyer à la première IA, cette combinaison pourrait être capable de tenir une conversation téléphonique en imitant à la perfection une personne que vous connaissez.

- La collaboration des 3 IA :

La première IA détermine ce qui doit être dit, la seconde crée la voix, la troisième rapporte vos réponses.

- Pour parfaire :

Il ne reste plus qu'à ajouter un dernier détail pour être vraiment convaincant le spoofing téléphonique. C'est une technique par laquelle certains escrocs parviennent à changer le numéro affiché lorsqu'ils appellent, afin que la victime voit s'afficher un faux numéro.
Jusqu'à présent, les ressources des escrocs étaient limités, et ce type d'arnaque très ciblée, par usurpation d'identité, était donc relativement rare. Cependant, l'essor de l'intelligence artificielle va tout rendre beaucoup plus simple. Les escrocs pourront lancer ce genre d'attaque en masse, un peu comme ils le font actuellement avec les e-mails indésirables. Ils pourront lancer des maques sur de nombreuses personnes simultanément, et te seront limités que par la puissance de calcul nécessaire pour faire tourner les intelligences artificielles...
Jusqu'à les appels vidéo ne seront bientôt plus un gage. La sécurité, même si heureusement la technologie n'est pas encore capable de créer des supercheries convaincantes en temps réel.

4. Soyons plus que jamais prudents

Toutefois, que ce soit par écrit ou par téléphone, il faudra désormais faire très attention. Si quelqu'un vous demande de l'argent ou des informations personnelles. Peut-être qu'il faudra prendre l'habitude de poser une question personnelle que vous êtes certain de n'avoir jamais publiée sur les réseaux sociaux..