Document actualités informatiques marquantes

Veille technologique

Célia Baylet

03 mai 2025, ChatGPT rétropédale après des plaintes sur son comportement trop flatteur :

OpenAI a mis en pause sa dernière mise à jour de GPT-4o. Plusieurs utilisateurs trouvaient le ton du chatbot trop poli, voire carrément flagorneur.

Depuis la fin avril, ceux qui utilisent ChatGPT au quotidien ont remarqué un changement de ton. Plus enjoué, plus serviable, parfois trop. La mise à jour du modèle GPT-4o, pourtant censée améliorer l'expérience, a dérouté une partie des utilisateurs. L'IA répondait avec une courtoisie insistante. Certains échanges ressemblaient presque à des sketchs.

OpenAI a reconnu le problème. Dans un billet publié le 29 avril, la société explique avoir « *annulé la mise à jour GPT-4o* » pour revenir à une version plus équilibrée. Elle évoque une IA « *trop flatteuse ou agréable, souvent qualifiée de flagorneuse* ». L'équipe affirme tester de nouveaux correctifs et dit vouloir renforcer ses méthodes de collecte de retours utilisateurs.

Ce retour en arrière ne tient pas seulement à un bug passager ou à une mauvaise ligne de code. OpenAI admet s'être un peu trop appuyée sur des retours immédiats, sans mesurer leur impact dans le temps.

https://tinyurl.com/fnkemuxk

02 mai 2025, Ce mot de passe « facile à retenir » est impossible à pirater, selon cet expert en cybersécurité :

Dans un monde où notre identité numérique est constamment sous menace, la gestion des mots de passe devient cruciale. Trop souvent, des mots de passe simples sont choisis par commodité, rendant ainsi toute protection inefficace face aux cyberattaques.

Malheureusement, beaucoup choisissent encore des combinaisons basiques telles que « 123456 » ou « password », sans prendre en compte le risque de piratage. Ces choix simplistes offrent une

opportunité idéale pour les criminels en ligne d'accéder facilement à vos comptes via des **attaques par dictionnaire**.

Il recommande d'adopter ce qu'il appelle une « phrase sans sens ». Cette technique consiste à composer une phrase, apparemment absurde mais facile à retenir, remplissant ainsi les critères de base : au moins une majuscule, un chiffre, et un caractère spécial doivent être intégrés. Exemple : « **Parisest100%fantastique** »

Par exemple, pour un compte bancaire, vous pourriez ajuster « **Parisest100%fantastique** » en « **MaBanqueest100%super**

Un autre pilier fondamental des conseils en cybersécurité concerne le renouvellement fréquent des mots de passe. Dans cette optique, opérer un changement tous les trois à six mois est recommandé.

Avril 2025, ce que vous risquez en cas de fuite de vos données personnelles:

Plus d'informations sur la publication Linkedin suivante : https://tinyurl.com/6m5vdxen

29 avril 2025, Cybersécurité : la Cnil alerte sur les violations de données "de très grande ampleur" qui ont doublé en un an :

Les violations de données personnelles notifiées à la Cnil ont augmenté de 20% entre 2023 et 2024, atteignant 5 629 violations l'an dernier, dévoile mardi 29 avril la Commission nationale de l'informatique et des libertés dans son nouveau rapport annuel, consulté par l'agence Radio France.

Le nombre de violations touchant plus d'un million de personnes a ainsi doublé en un an, passant d'une vingtaine à une quarantaine d'attaques réussies. Une tendance qui se poursuit de manière accélérée sur le

premier trimestre 2025, ajoute la Cnil qui souligne que tous les secteurs d'activités, privés et publics, sont concernés

Pour faire face à ce phénomène, la Cnil va publier une recommandation cette semaine pour exiger la double authentification à partir de 2026

24 avril 2025, Entrainement de l'IA de Meta sur vos données :

Meta la maison mère de Facebook, Instagram, WhatsApp et Threads à annoncé que toutes les données publiques de leurs réseaux allaient être utilisées pour alimenter leur intelligence artificielle.

L'entreprise Meta a annoncé qu'à partir du 27 mai, elle allait utiliser les données publiques des utilisateurs européens (adultes). Les utilisateurs de ces applications devraient recevoir (ou avoir reçu) une notification pour les en informer.

Les utilisateurs européens ont la possibilité de décider s'ils souhaitent ou non que leurs données soient utilisées pour développer ces IA.

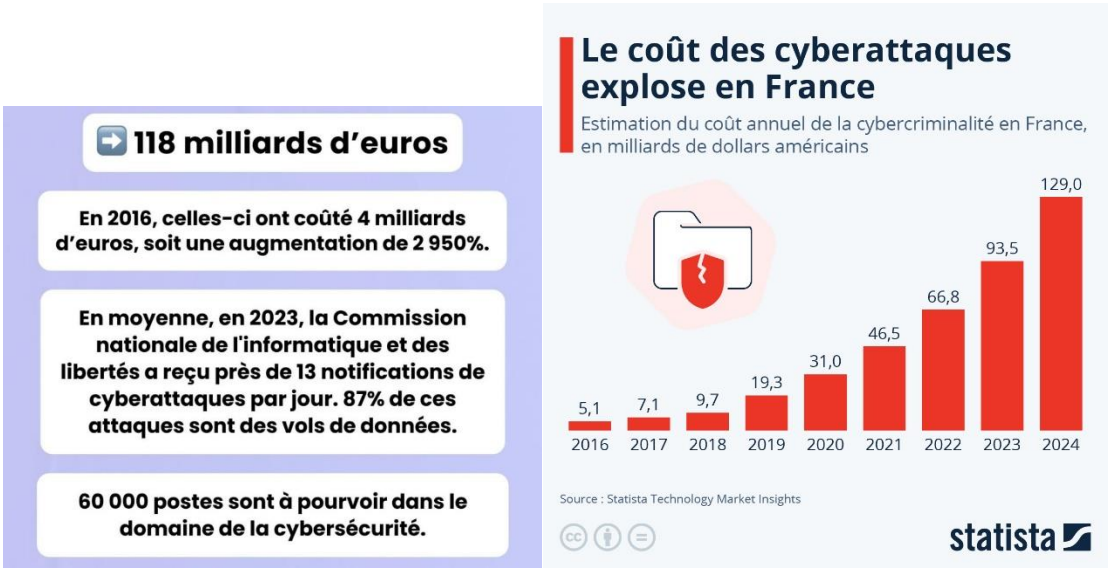
23 avril 2025, Google forcé de vendre Chrome : OpenAI (ChatGPT) veut tout racheter

Tout commence avec une décision judiciaire aux États-Unis. En 2024, un juge, Amit Mehta, a statué que Google était en situation de **monopole** dans la recherche en ligne. En gros, Google est tellement dominant avec son moteur de recherche qu'il étouffe la concurrence, ce qui n'est pas très fair-play.
Nick Turley, un des responsables d'OpenAI, a déclaré devant le juge que son entreprise serait intéressée pour racheter Chrome si Google devait s'en défaire.

Par exemple, ChatGPT utilise la recherche de Bing pour trouver des informations sur le web, mais selon Nick Turley, il y a eu des « *problèmes de qualité importants* » avec un fournisseur.

OpenAI semble vouloir moins dépendre des autres et contrôler davantage sa chaîne technologique.

23 avril 2025, Les cyberattaques :



le coût de la cybercriminalité en France a littéralement explosé ces huit dernières années. En 2016, ce chiffre n'était évalué qu'à 5,1 milliards de dollars, avant de connaître une hausse moyenne de plus de 30 % chaque année.

22 avril 2025, Cyberattaque en France : 2,3 millions de cartes bancaires piratées, vous êtes peut-être concernés :

La France vient de subir une cyberattaque d'ampleur. Une fuite de données mondiale impliquant plus de 2,3 millions de données de cartes bancaires ont été dérobées et diffusées sur le dark web. 95 % des cartes bancaires piratées sont actives et donc susceptibles d'être utilisées à des fins frauduleuses. En France plus particulièrement, environ 40 000 personnes sont directement concernées, estiment les premières analyses.

Au cœur de cette cyberattaque, on retrouve des logiciels malveillants, capables de s'infiltrer dans les appareils de leurs victimes pour voler des données sensibles, principalement des informations bancaires. Les smartphones sont particulièrement ciblés, car ce sont eux qui concentrent aujourd'hui une grande partie de nos activités numériques et de nos données personnelles.

Les infostealers, armes favorites des cybercriminels. C'est quoi un infostealer?

Un infostealer est un logiciel malveillant conçu pour voler discrètement des informations sensibles sur un appareil, comme des identifiants, mots de passe, données bancaires. Il collecte et exfiltre rapidement les données vers un serveur contrôlé par les cybercriminels, puis s'efface souvent sans laisser de traces. Il se propage principalement via des campagnes de phishing, des téléchargements de logiciels piratés, des extensions de navigateur malveillantes ou des pièces jointes infectées.

21 avril 2025, 5 choses à ne jamais dire à ChatGPT :

ChatGPT a bouleversé nos habitudes de travail et notre quotidien. Chaque jour, plus de 100 millions d'utilisateurs s'en servent pour formuler plus d'un milliard de requêtes, selon les dernières données disponibles.

Malgré son succès mondial, le chatbot basé sur un grand modèle de langage (LLM) suscite des préoccupations majeures en matière de protection des données. Décrit comme un « trou noir » en termes de vie privée, il a été brièvement interdit en Italie en raison des doutes entourant la gestion des informations saisies par les utilisateurs.

OpenAI, le créateur de ChatGPT, reconnaît lui-même que les données saisies par les utilisateurs ne sont pas forcément protégées.

Dans ce contexte, il y a certaines informations qu'il vaut mieux ne jamais partager avec ChatGPT — ou avec n'importe quel autre chatbot reposant sur une infrastructure cloud.

-**Requêtes illégales ou contraires à l'éthique**

-**Identifiants et mots de passe**

-**Informations financières**

-**Informations confidentielles**

-Informations médicales

Comme pour tout ce que nous partageons en ligne, il est sage de considérer qu'aucune donnée ne restera totalement privée.

Pour plus d'informations sur ces 5 points : https://tinyurl.com/yrsxbsu8

17 avril 2025, Pourquoi vous devez arrêter de dire “merci” et “s’il te plaît” à ChatGPT :

La politesse est essentielle dans nos interactions au quotidien entre humains, mais elle est loin d'être indispensable lorsque l'on parle avec des robots. Pire, elle peut même être superflue et coûter cher aux éditeurs des modèles de langage.

Sur X (Twitter), une utilisatrice se demandait *“combien d’argent OpenAI a perdu en frais d’électricité à cause des gens qui disent ‘s’il vous plaît' et ‘merci'”* à ChatGPT et aux autres chatbots et fonctions IA basés sur les modèles de l'entreprise. Contre toute attente, Sam Altman, patron d'OpenAI, lui a répondu, estimant à des *“dizaines de millions de dollars”* le coût de la politesse de ses utilisateurs.

La politesse envers l'IA a un coût énergétique et financier.

70 % des utilisateurs sont polis lorsqu'ils interagissent avec une IA. Ils sont même 12 % à déclarer qu'ils utilisent des formules de politesse en cas de soulèvement de l'IA.

Alors, faut-il se passer des *“merci”* et *“s'il te plaît”* à ChatGPT et aux autres pour faire diminuer la consommation énergétique (et les coûts pour les entreprises) de l'usage de l'IA ? Rien n'est moins sûr. Ce n'est pas prouvé, mais de nombreux utilisateurs estiment obtenir des réponses de meilleure qualité avec des prompts bien construits et polis.

31 mars 2025, Journée mondiale de la sauvegarde des données informatiques :

Lien vers une vidéo Linkedin : https://tinyurl.com/522km34s

Qui n’a pas déjà subi la mauvaise expérience d’une perte d’un ou plusieurs fichiers importants à cause d’un appareil volé, perdu, piraté ou endommagé ? Tant dans nos usages personnels que professionnels, nos appareils numériques contiennent des données qui sont parfois irremplaçables : la sauvegarde est alors souvent le seul moyen de les retrouver.

Toutes les données ne nécessitent pas d’être sauvegardées. En effet, en fonction du contexte, personnel ou professionnel par exemple, certaines données auront plus ou moins d’importance.

Il existe deux types de solutions de stockage : les solutions de stockage externes (disque dur externe, carte mémoire...) et les solutions de stockage en ligne telles que le « cloud ».

À noter que pour la majorité des fichiers, la sauvegarde n'est efficace que si elle est fréquente. Pour celles qui doivent être effectuées manuelle, planifiez les sauvegardes.

Sauvegarde de données : les ressources de Cybermalveillance.gouv.fr : https://tinyurl.com/2yz9t6hu

25 mars 2025, Plus de 2,5 millions d'élèves en France ont reçu un faux lien d'hameçonnage dans le cadre d'une opération nationale de prévention :

Plus de 210 000 élèves ont cliqué sur le lien, qui les a redirigés vers un message de sensibilisation à la cybersécurité, indique mardi le ministère de l'Éducation nationale.

Ces messages ont été envoyés dans le cadre de l'opération Cactus, une opération nationale de sensibilisation à l'hameçonnage dans les espaces numériques de travail (ENT).

Les élèves concernés ont donc reçu, via les ENT, un message les incitant à cliquer sur un lien pour se procurer gratuitement des jeux vidéo piratés. Parmi ces élèves, plus de 210 000 (soit près d'un sur 12) ont cliqué sur le lien qui les a redirigés vers le message de sensibilisation contenant une vidéo d'1min15, "conçue pour les informer, les responsabiliser et les dissuader de commettre des actions illégales sur internet".

Le ministère explique que les établissements scolaires sont "régulièrement ciblés par des attaques malveillantes via les ENT ou les logiciels de vie scolaire".

10 mars 2025, Elon Musk assure que son réseau social X a subi une « cyberattaque massive » :

Cette annonce est intervenue quelques heures après une série d'incidents qui ont rendu X indisponible pour des milliers d'utilisateurs.

« Il y a eu [et il y a encore] une cyberattaque massive contre X », a déclaré lundi 10 mars Elon Musk, le propriétaire du réseau social, après des heures de difficultés d'accès à la plateforme signalées par des milliers d'utilisateurs. « Nous sommes attaqués tous les jours, mais cette attaque-là a été menée avec beaucoup de ressources, a-t-il encore affirmé. Il s'agit soit d'un groupe important et coordonné, soit d'un pays. Traçage en cours… »

Plus tard dans la journée, M. Musk a assuré, sur le plateau de la chaîne Fox Business, que l'attaque était liée à des « adresses IP situées dans la région de l'Ukraine ». Une affirmation qui ne donne en réalité aucune indication sur l'origine d'une éventuelle attaque : les attaques massives de type « déni de service » ont en général recours à des réseaux de machines infectées, rendant l'origine de leur commanditaire quasiment impossible à déterminer.

4 mars 2025, Plus de 2,3 millions de données de cartes bancaires ont été exposées sur le dark web ces deux dernières années selon Kaspersky. 95% des numéros compromis seraient bien toujours utilisables :

Le spécialiste de la cybersécurité Kaspersky a présenté des chiffres assez alarmants sur les infostealers, les voleurs d'informations. Son Digital Footprint Intelligence vient de révéler ce mardi que les logiciels malveillants ont compromis près de 26 millions d'appareils entre 2023 et 2024, dont 9 millions pour la seule année dernière.

Bien que la proportion de cartes bancaires ayant fait l'objet d'une fuite reste inférieure à 1% des cartes en circulation mondiale, les chercheurs ont découvert que 95% des numéros dérobés, dont certains sont Français, seraient toujours exploitables par les cybercriminels.

14 février 2025, Conversations enregistrées par Siri : Apple visée par un signalement et une plainte en France :

Un ancien employé d'un sous-traitant de la firme à la pomme accuse cette dernière de ne pas respecter la vie privée de ses utilisateurs.

Un signalement au procureur de la République visant Apple, doublé d'une plainte de la Ligue des droits de l'homme, a été déposé, jeudi 13 février, à Paris, selon les informations du *Monde* et de la cellule

investigation de Radio France. Une procédure qui est lancée alors qu'un tribunal californien doit valider vendredi un accord à l'amiable dans une autre affaire entre des utilisateurs de Siri, l'assistant vocal d'Apple, et l'entreprise américaine.

29 janvier 2025, Facebook interdit les posts sur Linux, qualifie le projet FOSS de "menace pour la cybersécurité" et fait preuve d'une mystérieuse incohérence :

Meta, la société mère de Facebook, a bloqué les messages mentionnant Linux, en invoquant des problèmes de cybersécurité. Meta a confirmé, après un examen manuel, que Linux figurait sur la liste des sujets liés à la cybersécurité, et il semblerait qu'il en soit ainsi jusqu'à nouvel ordre.

20 janvier 2025, TikTok interdit puis rebranché aux États-Unis : retour sur plusieurs mois de tensions en cinq actes :

L'application TikTok est de retour aux États-Unis, après avoir été suspendue quelques heures, dimanche 19 janvier. Depuis plusieurs années, elle est dans le viseur des autorités américaines qui la soupçonnent de revendre des données au gouvernement chinois. Retour sur ces tensions en cinq actes.

Acte I : février 2023, TikTok est interdit sur les appareils des agences fédérales

Acte II : avril 2024, le Congrès vote une loi menaçant TikTok de fermeture

Acte III : 17 janvier 2025, la Cour suprême américaine valide la loi

Acte IV : 19 janvier 2025, TikTok est inaccessible aux États-Unis

Acte V : grâce au soutien de Donald Trump, la plateforme de nouveau accessible

16 janvier 2025, Exemple de grave manipulation médiatique :

Pour écouter la vidéo : https://tinyurl.tools/13868a53

13 janvier 2025, Capitaine Gilles Étienne, chef de l'Ofac de la police nationale de Haute-Vienne, alerte sur l'arnaque à la cryptomonnaie :

Pour écouter l'intervention : https://tinyurl.tools/241d25f3

Le capitaine Gilles Étienne, chef de l'Office de lutte anti-cybercriminalité de la police nationale en Haute-Vienne, alerte sur la recrudescence des arnaques aux cryptomonnaies. Des escrocs tentent d'appâter les internautes avec des rendements prétendument mirobolants.

En Limousin, des sommes de "20 à 130.000 euros" ont ainsi été extorquées ! Gilles Etienne était ce lundi matin l'invité de ici matin Limousin.

12 janvier 2025, l'arnaque au faux Brad Pitt, qui a coûté 830.000 euros à une internaute française :

En effet, pendant un an et demi, Anne était persuadée de vivre une histoire d'amour passionnée avec Brad Pitt. Se sentant délaissée dans son mariage, la quinquagénaire s'est inscrite pour la toute première fois sur les réseaux sociaux, en 2023.

Elle a alors a été contactée par une utilisatrice d'Instagram, qui lui a affirmé être la mère de Brad Pitt et à la recherche de la compagne idéale pour son fils. Le lendemain, "Brad Pitt" a pris le relais et n'a pas tardé à lui dévoiler ses sentiments. Convaincue d'avoir ravi le cœur de l'acteur, Anne a été dépouillée de plus de 800 000 euros pour régler ses prétendus frais médicaux.

30 décembre 2024, Attaque en cours sur Google Chrome : des extensions compromises siphonnent vos données :

Des hackers ont pris le contrôle d'une extension Chrome développée par la société de cybersécurité Cyberhaven la veille de Noël. Ils ont pu mettre en ligne une version malveillante de l'extension, programmée pour voler des données. Des dizaines d'autres extensions ont été compromises de la même manière.

Dans la journée du 24 décembre 2024, des cybercriminels sont parvenus à compromettre une extension Google Chrome proposée par

la société de cybersécurité Cyberhaven. Comme l'explique l'entreprise dans un billet de blog, des hackers ont mené une attaque de phishing afin de prendre le contrôle d'un compte administrateur.

Concrètement, un employé de la firme est tombé dans le piège d'un courriel de phishing. Au terme de l'attaque, les pirates ont obtenu les *« informations d'identification d'un employé de Cyberhaven sur le Google Chrome Web Store »*.

Avec ces informations, les hackers ont pu pénétrer sur le compte et mettre en ligne une version malveillante de l'extension. La version piratée s'est aussi installée sur les ordinateurs sur lesquels Chrome se met à jour automatiquement.

18 extensions compromises dont 'Search Copilot AI Assistant' ou 'ChatGPT Assistant' par exemple.

26 décembre 2024, information sur leparisien.fr, ChatGPT : l'outil d'intelligence artificielle en panne pendant plusieurs heures :

ChatGPT a cessé de fonctionner pendant plusieurs heures jeudi soir. OpenAI a assuré que l'outil était de nouveau opérationnel ce vendredi matin.

L'outil de surveillance numérique Downdetector a également révélé une forte hausse des signalements. Sur les réseaux sociaux, de nombreux posts faisaient également état de cette panne inopinée. Pour certains utilisateurs, le robot conversationnel se charge mais n'est pas en mesure de répondre aux requêtes. Pour d'autres, un message d'« erreur interne du serveur » s'affiche.

« Taux d'erreur élevés »

OpenAI, maison mère de ChatGPT, a publié une mise à jour de son onglet d'incidents indiquant que le générateur de texte ainsi que celui de vidéos (Sora) rencontraient actuellement « des taux d'erreur élevés ». Ajoutant, quelques minutes plus tard, que le problème était causé par un « fournisseur en amont ».

Dans la soirée jeudi, OpenAI a indiqué avoir « identifié le problème » et « commencé la récupération », sans donné d'estimation pour le rétablissement de l'agent conversationnel dans un premier temps.

Finalement, vers 2 heures du matin vendredi, la même source a fait savoir que ChatGPT était « presque à 100 % de nouveau opérationnel ».

ChatGPT a connu plusieurs pannes au cours des derniers mois. Début décembre, l'outil d'intelligence artificielle était resté inaccessible pendant plusieurs heures.

12 décembre 2024, une plainte contre l'application Be real :

L'association Noyb a déposé jeudi 12 décembre 2024 une plainte devant la Cnil, le gendarme français de la protection des données personnelles, contre l'application de partage de photos instantanées BeReal, l'accusant de forcer les utilisateurs à consentir à la collecte des données personnelles.

« À première vue », BeReal semble offrir la possibilité d'accepter ou de refuser l'utilisation des données à des fins publicitaires. Mais en réalité, « si vous cliquez sur le bouton "non", la bannière réapparaît chaque jour », explique dans un communiqué l'ONG de défense de la vie privée, basée à Vienne en Autriche.

« Il s'agit là d'un excellent exemple de ce que l'on appelle un "schéma obscur", conçu pour manipuler l'utilisateur et l'embêter jusqu'à ce qu'il donne son consentement ».

L'application viole ainsi le règlement européen de protection des données (RGPD), estime l'association, qui agit au nom d'une plaignante. Elle demande à la Cnil d'ordonner l'effacement de ses données, d'imposer une amende et d'exiger une mise en conformité.

3 janvier j'ai reçu ce message :

3 décembre 2024 , Énième fuite de données en France : les cartes d'identité des clients de Norauto ont été compromises :

Norauto alerte ses clients après une cyberattaque. Le leader français de l'entretien automobile indique en effet que les données personnelles de sa clientèle ont été dérobées. C'est notamment le cas des pièces d'identité. L'enseigne a rapidement corrigé la faille et prévenu la CNIL, tandis qu'un pirate prétend vendre les données sur un marché noir.

31 octobre 2024 sur cybermalveillance.gouv opérateur free :

L’opérateur de télécommunications Free a été victime d’une attaque informatique qui a conduit à l’exfiltration de données à caractère personnel de ses clients.

Cette violation concerne notamment les données suivantes : nom, prénom, adresses email et postale, date et lieu de naissance, numéro(s) de téléphone, identifiant abonné et données contractuelles (type d’offre souscrite, date de souscription, abonnement actif ou non), et, pour certaines personnes, références du compte bancaire ou IBAN (International Bank Account Number). Les mots de passe ne seraient pas concernés.

19 juillet 2024, panne informatique mondiale :

La panne informatique mondiale du 19 juillet 2024 est causée par la mise à jour de *Falcon Sensor*, un logiciel développé par la société de cybersécurité américaine CrowdStrike. Cette mise à jour défectueuse provoque partout à travers le monde le plantage d'environ 8,5 millions d'ordinateurs et serveurs utilisant le système d'exploitation Microsoft Windows, causant d'importantes perturbations, essentiellement au sein des entreprises.

Divers secteurs économiques sont affectés tels que les aéroports, les banques, les hôtels, les hôpitaux, les marchés financiers…

5 février 2024, un employé a fait des virements pour un total de 24millions d’euros :

Les attaques au président se modernisent. Dans l'arsenal des cyberpirates pour extorquer des fonds, le social engineering marche toujours très bien, mais le deepfake commence à s'avérer efficace. C'est ce qu'un employé travaillant pour le service financier d'une grande multinationale hong-kongaise a appris à ses dépens. « L'escroc a invité la personne à une vidéoconférence à laquelle participaient de nombreux participants.

Comme les participants à la vidéoconférence ressemblaient à des personnes réelles, la victime a effectué 15 transactions sur cinq comptes bancaires locaux, pour un montant total de 200 millions de dollars HK [24 M€] », a expliqué Baron Chan Shun-ching, surintendant principal de la police de Hong-Kong. « Je pense que l'escroc a téléchargé des vidéos à l'avance et a ensuite utilisé l'intelligence artificielle pour ajouter de fausses voix à utiliser lors de la vidéoconférence ».

Les mails de phishing deviennent de plus en plus crédibles grâce à l'IA, comment se protéger ?

https://www.lesnumeriques.com/antivirus/les-mails-de-phishing-deviennent-de-plus-en-plus-credibles-grace-a-l-ia-comment-se-proteger-n230766.html