

AU SOMMAIRE

5 actus · 1 Skill

- 01 De faux robots d'IA fouillent les sites d'entreprises à la recherche de mots de passe
- 02 Le Pentagone ouvre son IA à trois millions de personnes et laisse Claude à la porte
- 03 Perplexity fait traiter vos données confidentielles sur votre Mac, sans les envoyer sur internet
- 04 L'outil qui remplit les fichiers de prospection vaut désormais 7 milliards de dollars
- 05 Une entreprise de logiciel interdit l'IA à ses équipes tous les vendredis

LE SKILL

claude-persona : un panel de faux clients pour tester une idée avant de dépenser.



01

De faux robots d'IA fouillent les sites d'entreprises à la recherche de mots de passe

Ils se présentent comme les robots de ChatGPT ou de Claude. En réalité, ils cherchent les fichiers où dorment vos identifiants.

Les grandes sociétés d'IA envoient sur le web des robots, des programmes qui parcourent automatiquement les pages pour les lire. Elles publient le nom de ces robots afin que les propriétaires de sites puissent les autoriser, et la liste des adresses internet d'où ils partent afin qu'on puisse les vérifier. Des attaquants ont simplement recopié les noms. Entre le 28 juillet et le 23 août, treize identités de robots d'IA ont été usurpées, dont celles de ChatGPT, de Claude, de Google et de Perplexity.

Le trafic venait de 824 adresses internet différentes, réparties sur 795 réseaux distincts, ce qui rend le blocage adresse par adresse à peu près inutile. Ces faux robots ne demandaient ni articles ni fiches produits. Ils réclamaient des fichiers précis : celui où beaucoup de sites rangent les mots de passe de leur base de données et leurs clés d'accès, celui des identifiants du service d'hébergement, et les traces laissées par l'outil de gestion du code. Un détail les trahit. Un vrai robot commence toujours par lire le fichier qui liste ce qu'il a le droit de visiter : sous les six noms usurpés, ce fichier n'a jamais été demandé une seule fois.

La leçon est vérifiable en une matinée. Le nom que déclare un visiteur n'est qu'une étiquette qu'il écrit lui-même : autoriser un robot sur son nom sans vérifier l'adresse d'où il vient, c'est laisser entrer n'importe qui muni d'un badge photocopié. Si votre site a été installé par un prestataire, une seule question suffit pour ouvrir le sujet : est-ce que nos fichiers de configuration sont accessibles depuis le web, et nos clés d'accès ont-elles été changées récemment ?



02

Le Pentagone ouvre son IA à trois millions de personnes et laisse Claude à la porte

ChatGPT et Grok rejoignent Gemini sur le portail interne de l'armée américaine. Quelques jours plus tôt, une juge fédérale avait déclaré illégale la mise à l'écart d'Anthropic.

Le ministère américain de la Défense a mis en service GenAI.mil, un portail unique qui donne accès à des assistants d'IA à plus de trois millions de militaires, fonctionnaires et sous-traitants. 1,7 million de comptes sont déjà ouverts. Gemini, l'IA de Google, était arrivée la première ; ChatGPT et Grok, l'IA de xAI, viennent d'être ajoutés. Les trois ont obtenu le niveau d'habilitation le plus élevé prévu pour les données sensibles mais non classées secrètes.

Claude, l'IA d'Anthropic, n'y est pas. Anthropic voulait deux interdictions écrites noir sur blanc dans le contrat : pas de surveillance de masse des citoyens américains, pas d'armes qui décident seules de tirer. Le ministère a refusé, puis a désigné l'entreprise comme un risque pour sa chaîne d'approvisionnement, ce qui revient à la bannir de ses achats. La semaine dernière, une juge fédérale a qualifié cette décision d'illégale et sans fondement. Le ministère poursuit malgré tout son retrait de Claude, qu'il compte terminer fin septembre.

L'épisode dépasse largement l'armée américaine. Il montre qu'un fournisseur d'IA peut être écarté du jour au lendemain par un client immense, pour des raisons qui n'ont rien à voir avec la qualité de son produit, et qu'un client peut continuer à débrancher un outil même après avoir perdu au tribunal. À votre échelle, la question est la même que pour n'importe quel logiciel devenu central : que faites-vous si l'assistant sur lequel vous avez bâti un process n'est plus disponible dans six mois, et combien de jours vous faudrait-il pour en changer ?



03

Perplexity fait traiter vos données confidentielles sur votre Mac, sans les envoyer sur internet

Un même travail commence sur les serveurs de l'éditeur et bascule sur votre ordinateur dès qu'un nom de client ou un numéro de compte apparaît.

Quand vous posez une question à un assistant d'IA, votre texte part sur les serveurs de l'éditeur. C'est le premier frein dans les entreprises : personne n'a envie d'envoyer un fichier de paie, un contrat ou une liste de clients chez un prestataire installé à l'autre bout du monde. Perplexity propose un compromis, sur les Mac équipés des puces conçues par Apple.

Un petit programme installé sur la machine relit chaque demande avant l'envoi. S'il repère une donnée personnelle, un nom, une adresse, un numéro de compte, il vous prévient et vous propose de traiter cette partie sur votre ordinateur, avec un modèle plus petit installé chez vous. Les informations sensibles sont remplacées par des étiquettes le temps du trajet, puis remises en place dans la réponse ; le reste du travail, celui qui demande de la puissance, continue sur les serveurs. Il faut macOS 15 ou plus récent et 24 gigaoctets de mémoire, 32 pour que ce soit confortable.

L'intérêt n'est pas la vitesse, c'est la conformité. Beaucoup de dirigeants ont interdit l'IA sur les dossiers clients faute de pouvoir répondre à une question simple : où partent les données ? Un découpage automatique entre ce qui sort de l'entreprise et ce qui reste dedans est la première réponse crédible à cette question. La même mécanique va arriver chez les concurrents, et elle devient un argument à réclamer aux prestataires qui vous vendent de l'IA.

1	US	Furhaven Pet Dog Bed	654345678X	8074F2G	X474F2G	FBA	+ 26.99	124
2	US	New Obsession by Dala	47321	8071T79	X471T79	FBA	+ 21.99	341
3	US	GoTags Stainless Steel	789055	80141QV	X4141QV	FBA	+ 29.99	36
4	US	Milk-Bone Flavor Snac	789064	800182	X04082	FBA	+ 24.50	382
5	US	Adventure II & Cross I	88330790	804048	X04048	FBA	+ 18.99	774
6	US	Taste of the Wild High	9967	8074F2G	X474F2G	FBA	+ 24.50	382
7	US	Earth Rated Dog WipeWipe100-GROOM-UP	8074F2G	X474F2G	FBA	+ 18.99	292	
8	US	Hertzko Self-Cleaning	FBA_881314701702	8032DPH	X042DPH	FBA	+ 23.50	374
9	US	Portable Cordless Leash	GL-CHC-F-GLV	8000SEI	X040SEI	FBA	+ 18.99	224
10	US	Dog Training Collar - J	LO404	X474F2G	X474F2G	FBA	+ 29.99	1102
11	US	Rachael Ray Nutrish S	TC01	8083JND	X483JND	FBA	+ 26.99	121
12	US	Dog Chew Toy	TC02	8083JND	X483JND	FBA	+ 21.99	710
13	US	Orthopedic Dog Bed	GB-0M-01	8083JND	X483JND	FBA	+ 21.99	710
14	US	Adjustable Dog Harness	OC-ERD-02	8074F2G	X474F2G	FBA	+ 29.99	100
15	US	Reflective Dog Leash	WB-ES-22	8044QQT	X044QQT	FBA	+ 18.99	100
16	US	Dog Water Dispenser	YM-AJ-04	8084TQT	X084TQT	FBA	+ 24.99	100
17	US	Slow Feeder Dog Bowl	LB-0M-04	8084TQT	X084TQT	FBA	+ 22.00	80
18	US	Dog Poop Bags	DB-ADJ-07	8074F2G	X474F2G	FBA	+ 34.99	28
19	US	Dog Grooming Brush	RB-MC-06	8084TQT	X084TQT	FBA	+ 18.00	110
20	US	Dog Nail Clippers	CP-WL-09	8084TQT	X084TQT	FBA	+ 16.00	278
21	US	Dog Shampoo	RB-SET-10	8074F2G	X474F2G	FBA	+ 15.99	460
22	US	Dog Training Pads	GB-AR-11	8084TQT	X084TQT	FBA	+ 12.99	46
23	US	Interactive Dog Puzzle	PB-10K-12	8074F2G	X474F2G	FBA	+ 22.99	150
24	US	Squeaky Dog Toy Set	GL-8L-13	8074F2G	X474F2G	FBA	+ 21.99	500
25	US	Dog Dental Chews	AT-EL-14	8084TQT	X084TQT	FBA	+ 14.99	200
26	US	Grain-Free Dog Treats	PL-AM-15	8074F2G	X474F2G	FBA	+ 40.99	86
27	US	Dog Car Seat Cover	FT-WY-18	8074F2G	X474F2G	FBA	+ 18.99	180
28	US	Portable Dog Water B	MG-CA-17	8074F2G	X474F2G	FBA	+ 39.99	120
29	US	Reflective Dog Collar	LS-AJ-19	8074F2G	X474F2G	FBA	+ 11.99	400
30	US					FBA	+ 27.99	180

04

L'outil qui remplit les fichiers de prospection vaut désormais 7 milliards de dollars

Clay est passé de 3,1 à 7 milliards de dollars en un an. Ce que ses clients achètent : des listes de prospects complétées et triées sans personne pour les remplir.

Clay lève de nouveaux fonds, menés par le gestionnaire d'actifs Wellington, sur une valorisation de 7 milliards de dollars avant l'opération. L'entreprise valait 3,1 milliards en août 2025 et 5 milliards en janvier. Le produit mérite plus d'attention que le montant.

Clay réunit en un seul endroit plus de deux cents fournisseurs de données d'entreprises, puis lance des assistants d'IA qui vont chercher eux-mêmes ce qui manque : la fonction exacte d'un contact, les outils utilisés par une société, un changement de poste récent, un signal qui indique qu'une boîte cherche à acheter. Le résultat est un fichier de prospection rempli et trié automatiquement, branché sur votre logiciel de suivi commercial, avec l'envoi des messages derrière. Plus de 500 000 équipes commerciales s'en servent, dont celles d'OpenAI, de Stripe et de Figma.

Le travail que Clay supprime existe dans toutes les petites entreprises : quelqu'un passe ses soirées à compléter un tableur de contacts avant de pouvoir décrocher son téléphone. Ce que le marché valorise 7 milliards de dollars, ce n'est pas l'IA qui écrit les e-mails, c'est celle qui prépare la liste. Si votre prospection cale, comptez d'abord les heures que vous payez pour constituer le fichier : c'est souvent là que se trouve le gain, pas dans un nouveau modèle d'e-mail.



05

Une entreprise de logiciel interdit l'IA à ses équipes tous les vendredis

Un jour par semaine sans assistant. L'idée vient de circuler très vite dans le milieu du développement, avec un argument que les dirigeants connaissent bien.

L'équipe derrière htmx, une brique logicielle très utilisée pour construire des sites web, a instauré chez elle une règle simple : le vendredi, les assistants d'IA restent éteints. On écrit soi-même, on lit la documentation, on réfléchit au problème jusqu'au bout. Le texte qui explique la démarche a été publié en ligne et est monté en quelques heures parmi les discussions les plus lues du milieu, avec plusieurs centaines de réactions.

L'argument n'est pas moral, il est professionnel. À force de déléguer chaque décision à un assistant, on perd la trace des compromis qui ont été faits, et la compétence qui permettait de les juger s'émousse. Les auteurs parlent de dette cognitive : un gain de vitesse immédiat, payé plus tard par une équipe qui ne sait plus vérifier ce qu'elle livre. La règle admet une exception révélatrice : les outils qui relisent le travail et expliquent leurs remarques restent autorisés, parce que la personne, elle, apprend quelque chose au passage.

Une seule entreprise applique officiellement la règle pour l'instant, et ce n'est pas l'essentiel. L'essentiel, c'est la question posée à tous ceux qui ont déployé l'IA dans leurs équipes cette année : vos collaborateurs sauraient-ils encore faire le travail sans elle, et le sauriez-vous avant le jour où l'outil tombe en panne ou change de prix ? Une journée par mois suffit généralement à obtenir la réponse.

LE SKILL

claude-persona

Open source · takechanman1228 · MIT

Un panel de faux clients pour éprouver une idée avant de dépenser. Vous décrivez la cible en une phrase, le Skill fabrique une dizaine de profils différents, les interroge un par un, puis vous rend un rapport avec leurs réponses et le classement de vos options.

C'EST QUOI UN SKILL ?

Un Skill, c'est un mode d'emploi écrit par quelqu'un d'autre et donné à votre IA. Vous l'installez une fois sur votre ordinateur, dans Claude Code (la version de Claude qui tourne chez vous). Ensuite, au lieu de réexpliquer chaque fois ce que vous attendez, vous demandez la tâche en une phrase et l'IA suit la méthode déjà écrite dans le Skill. C'est gratuit, ce sont de simples fichiers texte, et vous pouvez les lire avant de vous en servir.

En quoi c'est utile : avant de lancer une offre, un nom, un prix ou une nouvelle formule, on aimerait savoir ce qu'en penseront les clients. Une étude qualitative se commande, coûte plusieurs milliers d'euros et met des semaines à revenir, ce qui explique que la plupart des dirigeants tranchent à l'instinct. Ici, en quelques minutes, vous obtenez une dizaine de profils contrastés, leurs objections formulées avec leurs mots, et un classement de vos options avec l'intention d'achat de chacun. Soyons clairs : ce ne sont pas de vrais clients et cela ne remplace pas un appel. C'est un premier filtre, fait pour éliminer les mauvaises idées et pour arriver avec de meilleures questions devant de vraies personnes.

Ce que ça fait concrètement : fabriquer un panel à partir d'une description en français, par exemple dix primo-abonnés à un service de paniers repas en France. Poser une question ouverte à tout le panel et remonter les thèmes qui reviennent, avec les citations. Comparer deux ou trois concepts en parallèle et voir lequel arrive premier, et pourquoi. Chaque profil répond dans une session isolée, sans voir les réponses des autres ni vos propres documents, et le coût de chaque passage est indiqué à la fin.

Pour qui : dirigeants, indépendants, responsables marketing ou produit qui doivent choisir entre plusieurs offres, plusieurs noms ou plusieurs prix sans budget d'étude. Aucune clé d'accès à acheter : le Skill se sert de votre abonnement Claude existant. Seuls les graphiques du rapport demandent Python installé sur la machine, le reste fonctionne sans.

INSTALLER EN 2 MINUTES

1. Ouvrez le Terminal, la fenêtre où l'on tape des commandes (Mac : Applications → Utilitaires → Terminal. Windows : menu Démarrer, tapez « Terminal »), puis lancez Claude Code en tapant **claude** et Entrée.

2. Copiez ces deux lignes, collez-les l'une après l'autre, appuyez sur Entrée :

```
/plugin marketplace add takechanman1228/claude-persona
/plugin install claude-persona@claude-persona
```

Mot à mot : la première ligne indique à Claude Code où trouver le dépôt de l'auteur sur GitHub, la seconde y prend le Skill. Fermez puis relancez Claude Code pour qu'il en tienne compte. Rien ne passe par KLEAA. Plus tard, pour rester à jour : `/plugin marketplace update claude-persona`.

3. Lancez une première étude : tapez `/persona generate` suivi de votre cible décrite en français, par exemple dix dirigeants de très petites entreprises françaises qui cherchent un logiciel de facturation. Puis `/persona concept-test` suivi de vos deux ou trois offres, décrites en une ligne chacune.

Sélection KLEAA · le code et la licence restent chez l'auteur · licence MIT vérifiée sur le dépôt