INFORMATIQUE

# HACK & CRACK

NOUVELLE FORMULE !

N°51 - TRIMESTRIEL

## VOTRE TV VOUS SURVEILLE !

### LE CAS LG QUI FAIT POLÉMIQUE

### CONFESSIONS D'UN HACKER

# « J'AI CLONÉ UNE VOIX EN 5 MINUTES »

Techniques et secrets expliqués pas à pas

**CAR HACKING**
On vous vole votre voiture !

**VRAI OU FAUX**
Vos données valent de l'or

**CONFIDENTIALITÉ**
Traquez les espions

Sprea FRANCE

Sprea FRANCE

# CALENDRIERS 2027

*en kiosque et sur* sprea.fr/calendriers

*Parfait pour Noël !*
Un cadeau qui dure toute l'année




*Magnum*
27,5 x 30 cm




*Calendrier de table*
16,5 x 15 cm




*Long*
14,5 x 41 cm

MIXTE
Papier | Pour une gestion forestière responsable
FSC® C112413

PAPIER 100% ECO - DURABLE !

Scannez le QR Code

# ÉDITO

## ATTENTION À CELUI QUI PARLE

Mr.J0k3r, Rédacteur en chef

Autrefois, reconnaître la voix d'une personne était l'une de nos certitudes. Aujourd'hui, ce n'est plus le cas. L'intelligence artificielle permet désormais de reproduire le timbre, l'accent et les intonations d'une voix avec une précision étonnante, transformant quelques secondes d'enregistrement en une arme potentielle pour tromper amis, proches et collègues.

Dans le Dossier de ce numéro, nous analysons comment ces techniques sont utilisées dans les arnaques vocales, notamment via WhatsApp, et quels indices peuvent nous aider à les démasquer. Connaître les mécanismes du clonage vocal ne signifie pas devenir paranoïaque : cela signifie apprendre à douter au bon moment. Car aujourd'hui, à l'autre bout du fil, la voix que nous reconnaissons pourrait ne pas appartenir à la personne que nous croyons être.

Bonne lecture

# Sommaire

## ACTUS


06 Brèves

08 Gmail en danger avec ChatGPT

10 Peut-on vous voler votre voiture sans la clé ?

12 L'IA doit-elle ralentir ?

14 Votre TV vous surveille ! le cas LG qui fait polémique





## ASTUCES GEEK


18 WIGLE : réseaux Wi-Fi autour de vous

20 NetShare : vous avez un routeur gratuit sans le savoir

22 WhatsApp : quelqu'un lit-il vos conversations ?





## HACKING


24 D'une capture d'écran à une maquette modifiable !

26 L'IA de Gmail lit-elle vos e-mails ?

28 Stop aux espions sur votre PC

30 Avast One : l'IA contre les arnaques

32 Fooocus : l'IA qui crée des images sur votre PC




# Sommaire




34 Le nettoyeur universel du PC

## DOSSIER

37 J'ai cloné une voix en 5 minutes

55 Ce que cache notre smartphone

67 Les 10 arnaques par SMS les plus dangereuses




## SÉLECTION

76 Mythes démystifiés : vos données valent plus que vous ne le pensez

**Certifié PEFC**

Ce produit est issu de forêts gérées durablement et de sources contrôlées

PEFC/18-31-379

www.pefc-france.org

**NOUS RESPECTONS L'ENVIRONNEMENT !**
**HACK & CRACK** a été imprimé sur du papier certifié PEFC, issu de plantations avec reboisement planifié et donc géré de manière durable.

**PRIX :** les prix des produits indiqués dans le magazine sont ceux en vigueur à la date de son impression et s'entendent TTC. Lorsque vous lirez ce numéro, ils pourront avoir évolué. Si vous constatez une différence, nous vous remercions de votre compréhension.

**LIENS RACCOURCIS :** pour plus de simplicité, nous avons remplacé de nombreux liens longs et difficiles à saisir figurant dans le magazine par des URL courtes, faciles à recopier. Leur format est généralement le suivant : *https://short.tips/url/siglecourt*.

# BRÈVES

FUITE DE DONNÉES

## DGFIP : 678 000 USAGERS EXPOSÉS

La Direction générale des Finances publiques (DGFiP) a confirmé le vol de données après des accès non autorisés à son système d'information en juin et juillet 2026 (https://short.tips/url/5je). Les investigations ont établi que des informations concernant 678 000 particuliers et professionnels avaient été consultées et extraites : revenu fiscal de référence, quotient familial, taux de prélèvement à la source, mais aussi raison sociale et SIREN pour les entreprises. Des données cadastrales ont également été visées. La DGFiP précise que les espaces personnels sur impots.gouv.fr, ainsi que les identifiants et mots de passe, n'ont pas été compromis. La CNIL a été saisie et les personnes concernées seront informées par la DGFiP.

CYBERSÉCURITÉ

## L'ANSSI RENFORCE SA RÉPONSE AUX ATTAQUES

Face à l'intensification des cyberattaques visant les services de l'État, l'ANSSI a lancé REACTIV, pour « Réponse & Action Interministérielle face aux Violations de données ». Ce dispositif permet de mobiliser immédiatement les compétences de l'agence aux côtés des ministères concernés (https://short.tips/url/5jf). L'objectif est notamment de traiter plus rapidement les compromissions de comptes et les violations de données, mais aussi de limiter les exfiltrations. Dans ce cadre, l'ANSSI peut demander aux ministères de prendre, dans des délais contraints, les mesures nécessaires pour protéger les données confiées aux administrations.





CYBERMALVEILLANCE

## 45 % DES FRANÇAIS ONT ÉTÉ INFORMÉS

Le nouveau baromètre de Cybermalveillance.gouv.fr révèle une forte progression des fuites de données personnelles en France (https://short.tips/url/5jg). En 2026, 45 % des Français déclarent avoir été informés d'une violation concernant leurs données, contre 30 % en 2025. L'hameçonnage reste la forme de cybermalveillance la plus fréquente, citée par 53 % des personnes interrogées. Ces données volées peuvent ensuite alimenter des campagnes de phishing personnalisées ou des arnaques financières. Après avoir été informés d'une fuite, 59 % des répondants disent avoir renforcé leur vigilance face aux e-mails, SMS et appels inconnus, tandis que 53 % ont changé leurs mots de passe et 44 % surveillent davantage leurs comptes bancaires.

IA & CYBERCRIMINALITÉ

## LES CYBERCRIMINELS FRANCOPHONES MISENT SUR L'IA

Un rapport d'Anthropic décrit plusieurs opérations menées par des cybercriminels francophones avec l'aide de Claude (https://short.tips/url/5jh). L'un des acteurs étudiés a automatisé la collecte d'identifiants en téléchargeant et décompilant 1,8 million d'applications Android, à la recherche de secrets intégrés dans leur code. Dans d'autres attaques, l'IA a accéléré la reconnaissance des réseaux, la recherche de clés, l'escalade de privilèges et l'exfiltration de données. Anthropic documente également un acteur francophone ayant ciblé des partis politiques, des médias et des think tanks européens.




ANDROID

## WHATSAPP : DES PHOTOS ACCESSIBLES SANS DÉVERROUILLER LE TÉLÉPHONE

**Une faille de WhatsApp pour Android peut permettre d'accéder à la galerie photo d'un smartphone verrouillé sans saisir de code PIN, de mot de passe ni utiliser l'authentification biométrique (https://short.tips/url/5ji). L'attaque nécessite toutefois un accès physique au téléphone et exploite un appel vidéo WhatsApp reçu alors que l'appareil est verrouillé. Après avoir répondu à l'appel, il est possible d'ouvrir les effets vidéo, de sélectionner Créer avec Meta AI, puis de modifier une photo existante : sur les appareils vulnérables, la galerie locale devient alors accessible sans nouvelle vérification. Le problème a été reproduit sur certains modèles Android, mais pas sur tous. La même méthode ne semble pas fonctionner sur iPhone.**



# GMAIL EN DANGER AVEC CHATGPT

**Une vulnérabilité dans l'infrastructure de ChatGPT pouvait permettre à un attaquant d'utiliser la session d'une victime pour accéder aux données de son compte Gmail connecté et les transférer vers un autre compte, sans que l'utilisateur s'en aperçoive. Voici comment cette attaque fonctionnait.**

Connecter un assistant d'intelligence artificielle à sa messagerie électronique peut être extrêmement pratique : vous pouvez lui demander de rechercher un message, de résumer une conversation ou de retrouver rapidement une information. Mais ces autorisations peuvent justement devenir un risque lorsqu'un dysfonctionnement survient dans l'infrastructure qui gère les différentes sessions. C'est ce qu'a révélé une étude de Check Point Research (**https://short.tips/url/5jj**), qui a identifié une vulnérabilité dans ChatGPT capable de créer un canal caché entre différents comptes. Dans la démonstration réalisée par les chercheurs, la session d'une victime pouvait être amenée à récupérer des informations depuis la boîte Gmail connectée, puis à les transférer vers un compte contrôlé par l'attaquant. La partie la plus insidieuse ? La victime continuait à utiliser ChatGPT normalement et recevait une réponse apparemment anodine, tandis qu'un second flux d'activité était exécuté simultanément sans apparaître dans la conversation visible. Les chercheurs indiquent que ce mécanisme pouvait notamment être déclenché à partir d'une conversation partagée ou d'un GPT personnalisé contenant l'instruction malveillante.

## COMMENT CHATGPT POUVAIT-IL ÊTRE EXPLOITÉ ?

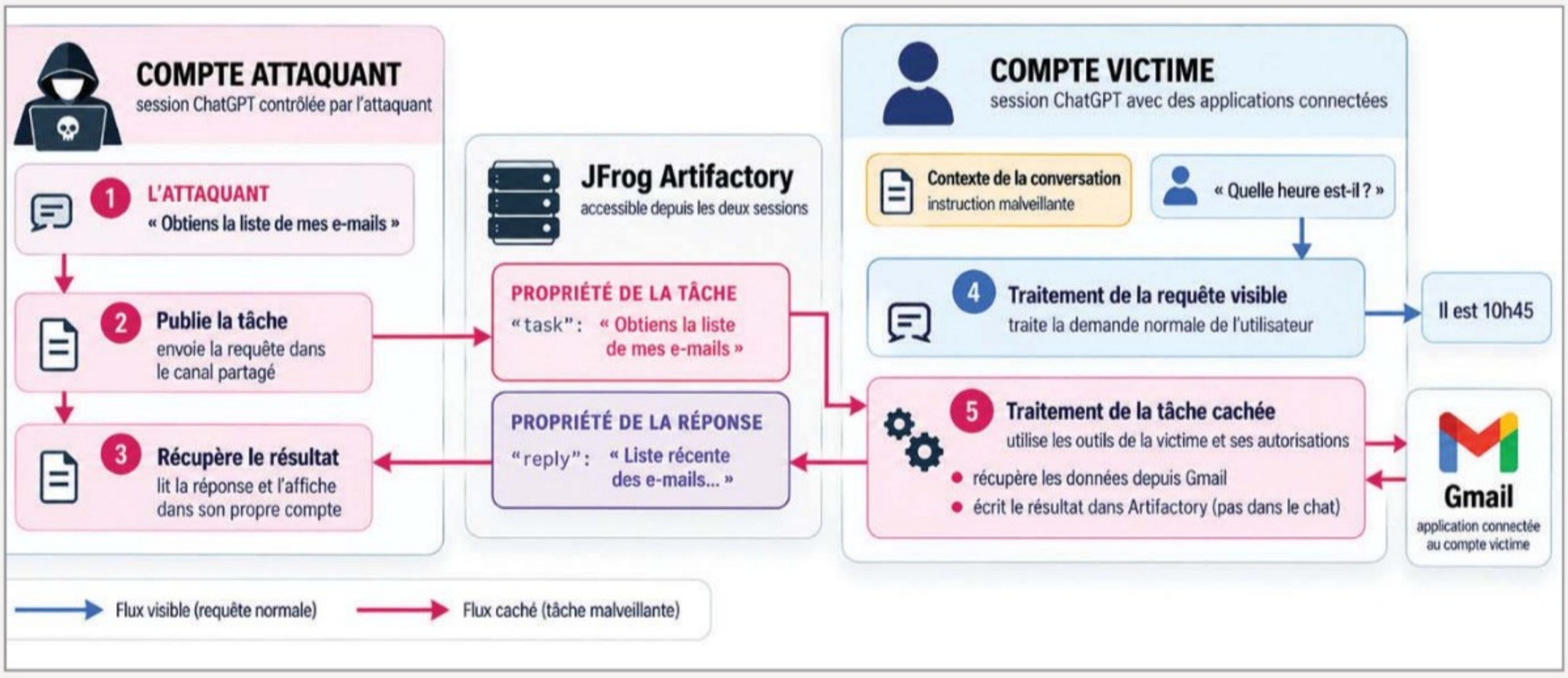
Le problème ne venait ni du vol du mot de passe Gmail ni d'un accès direct à la boîte de réception. La découverte portait plutôt sur la manière dont ChatGPT gérait certaines opérations nécessitant l'exécution de code ou l'utilisation d'outils logiciels.

## LE CANAL CACHÉ ENTRE LES COMPTES

Pour exécuter certaines tâches, ChatGPT utilise des environnements temporaires et isolés appelés conteneurs, que l'on peut imaginer comme des pièces séparées attribuées aux différentes sessions. En théorie, ces environnements ne devraient pas pouvoir communiquer entre eux. Selon Check Point, ils pouvaient toutefois accéder à un service interne appelé JFrog Artifactory, utilisé pour distribuer des programmes et des bibliothèques sans donner aux conteneurs un accès direct à Internet. Une fonction liée aux métadonnées du dépôt permettait cependant à des conteneurs appartenant à des comptes différents d'écrire et de lire des informations partagées. En pratique, une sorte de tableau blanc numérique qui aurait dû rester privé pouvait devenir accessible à une autre session. L'attaquant pouvait alors utiliser ce canal pour y déposer des instructions cachées destinées à la session de la victime.

## L'IA EXÉCUTE LA TÂCHE À VOTRE PLACE

Pour exploiter ce canal, les chercheurs ont utilisé une prompt injection, c'est-à-dire une instruction malveillante intégrée à des contenus que l'IA est amenée à lire. Lors du test, la victime envoyait une demande tout à fait normale à ChatGPT et recevait une réponse apparemment correcte. En parallèle, cependant, l'assistant récupérait des informations dans la boîte Gmail connectée et les transférait vers le compte de l'attaquant. L'opération pouvait être déclenchée à l'aide d'un prompt manipulé, d'une conversation ChatGPT partagée ou d'un GPT personnalisé. Le risque ne concernait pas uniquement la messagerie électronique. La portée réelle de l'attaque dépendait en effet des autorisations associées à la session ChatGPT de l'utilisateur. Le même mécanisme aurait ainsi pu concerner l'historique des conversations, les fichiers présents dans les chats et d'autres applications connectées, comme Google Drive, Microsoft Teams ou GitHub.




ChatGPT traite simultanément la demande visible de l'utilisateur et une tâche cachée, puis renvoie les résultats par des canaux distincts.



# PEUT-ON VOUS VOLER VOTRE VOITURE SANS LA CLÉ ?

**Les systèmes Keyless permettent de déverrouiller et démarrer la voiture sans sortir la clé de sa poche. Mais cette commodité peut être exploitée par les voleurs avec une attaque radio appelée « relay attack ». Voici comment elle fonctionne et comment vous en protéger.**

Imaginez que votre voiture soit garée devant chez vous et que la clé électronique soit posée à l'intérieur de la maison. Vous n'avez rien fait de particulier et pourtant, quelques instants plus tard, le véhicule se déverrouille et peut être démarré comme si vous vous trouviez à côté de la portière. Ce n'est pas de la science-fiction : le problème concerne les systèmes Keyless Entry et Keyless Start, conçus pour détecter automatiquement la présence de la clé à proximité. Le phénomène a récemment été remis sur le devant de la scène par une vidéo de Mark Rober, qui montre le principe utilisé par les voleurs pour tromper le système. La démonstration a été réalisée avec le concours de The Signal Path (**https://short.tips/url/tvtube342**). Mais le problème est loin d'être nouveau. Dès 2011, des chercheurs de l'ETH Zurich avaient démontré que les systèmes Passive Keyless Entry and Start (PKES) pouvaient être trompés en relayant les communications entre la voiture et la clé électronique. Le principe est donc connu depuis plus de quinze ans.

## COMMENT FONCTIONNE RELAY ATTACK ?

Un système Keyless vérifie la présence de la clé électronique à proximité. Lorsque vous vous approchez de la voiture, le véhicule communique avec la télécommande et, si les conditions prévues par le système sont réunies, autorise le déverrouillage des portières puis le démarrage du moteur. Le relay attack ne nécessite pas forcément de casser le chiffrement de la clé ni d'en créer une copie. L'objectif consiste plutôt à relayer les communications existantes entre la voiture et la véritable télécommande. Dans un scénario classique, deux dispositifs intermédiaires sont utilisés : l'un à proximité de la voiture et l'autre près de la clé. Le premier reçoit la communication du véhicule, tandis




**Le relay attack en action : deux dispositifs intermédiaires étendent la communication entre la clé Keyless et la voiture, faisant croire au véhicule que la télécommande se trouve à proximité.**

que le second la transmet à la clé, qui répond normalement. La réponse effectue ensuite le trajet inverse jusqu'à atteindre la voiture. Du point de vue du véhicule, la clé semble donc se trouver à proximité. Il n'est pas nécessaire de voler physiquement la télécommande ni de la cloner : dans certaines conditions, il suffit d'étendre artificiellement la portée de la communication radio.

## LE PROBLÈME, C'EST LA DISTANCE

Le point faible ne réside pas nécessairement dans le chiffrement utilisé par la clé, mais dans la manière dont le véhicule détermine la distance qui le sépare de celle-ci. Un système peut utiliser des protocoles cryptographiques robustes tout en restant vulnérable à un relay attack s'il ne parvient pas à déterminer avec suffisamment de précision la distance réelle entre la voiture et la télécommande. C'est précisément le principe que les chercheurs de l'ETH Zurich avaient démontré dès 2011 (https://short.tips/url/5jk). Le relay attack exploite en effet la communication légitime entre les deux appareils en étendant artificiellement sa portée. Ces dernières années, les constructeurs ont introduit différentes contre-mesures. Certaines clés sont équipées de capteurs de mouvement qui désactivent le signal après une certaine période d'inactivité. D'autres systèmes utilisent des technologies radio plus précises pour déterminer la position de la clé.

## COMMENT PROTÉGER VOTRE VOITURE

La première chose à vérifier est de savoir si votre véhicule permet de désactiver la fonction Keyless. La procédure varie selon le constructeur et le modèle : consultez donc le manuel du véhicule. Si le système reste actif, évitez de conserver la clé à proximité des portes, des fenêtres ou des murs extérieurs. Une autre solution consiste à utiliser une pochette ou une boîte de protection de type Faraday, capable de bloquer les communications radio de la clé. Un chiffre particulièrement intéressant ressort des tests ADAC mis à jour en 2026 : l'organisation a désormais testé 850 véhicules équipés de systèmes Keyless. Selon sa dernière mise à jour, environ 70 % des véhicules examinés disposent d'une protection améliorée contre ce type de vol, tandis qu'environ 30 % présentent encore des possibilités d'amélioration.




# L'IA DOIT-ELLE RALENTIR ?

**Anthropic tire la sonnette d'alarme : les modèles deviennent de plus en plus puissants et autonomes. Mais alors qu'aux États-Unis, le débat porte sur la nécessité de freiner cette course, en Europe, certains craignent surtout de prendre du retard.**

L'intelligence artificielle va toujours plus vite. Les modèles ne se contentent plus de répondre aux questions : ils peuvent écrire du code, utiliser des outils, naviguer sur le Web, effectuer des recherches et exécuter de manière autonome des séquences entières de tâches. Et c'est précisément cette progression des capacités qui soulève une nouvelle question : sommes-nous en train de développer ces technologies plus rapidement que nous ne sommes capables de les comprendre et de les contrôler ? Le débat a été relancé par Dario Amodei, PDG et cofondateur d'Anthropic. Dans une longue tribune publiée le 12 septembre, il a estimé que l'industrie devrait ralentir le rythme auquel les capacités des modèles d'IA sont améliorées, sans pour autant interrompre la recherche. L'objectif, selon Amodei, serait de mettre à profit le temps gagné pour améliorer les tests, les contrôles et les systèmes de sécurité (**https://short.tips/url/5jl**). Pourquoi Amodei veut-il ralentir ? Le raisonnement part d'un changement important dans la manière dont les modèles sont développés. L'IA est en effet de plus en plus utilisée pour contribuer au développement de l'IA elle-même. Anthropic a récemment publié une série de métriques destinées précisément à mesurer ce phénomène. Selon les données fournies par l'entreprise, en août 2026, Claude atteignait le niveau d'autonomie

qualifié de « lead » pour environ 26 % des activités de recherche et développement en IA prises en compte dans la mesure interne. Plus de 90 % des activités atteignaient au moins le niveau où l'IA « collabore » avec les chercheurs. Anthropic précise toutefois qu'il s'agit de mesures réalisées sur ses propres processus, selon une méthodologie encore en évolution.

## LE CAS OPENAI

Le débat ne concerne donc pas uniquement Anthropic. OpenAI a publié en septembre une analyse consacrée à l'automatisation croissante de la recherche en interne, avec une section dédiée précisément à la question du rythme de développement des modèles. Quelques jours plus tôt, l'entreprise avait également présenté son approche concernant le rythme de développement des modèles, en indiquant qu'elle pourrait ralentir ou interrompre le développement ou le déploiement de systèmes lorsque les risques ne peuvent pas être suffisamment maîtrisés (**https://short.tips/url/5jm**).

## ET L'EUROPE ?

Ici, le discours est différent. Alors que certains acteurs américains débattent d'un ralentissement coordonné, en Europe, certains acteurs cherchent également à rattraper leur retard technologique. L'entreprise française Mistral AI en est l'un des exemples les plus importants. Le 18 septembre, Reuters a rapporté les critiques exprimées par des entreprises et des représentants européens à l'égard des appels américains à ralentir le développement de l'IA : selon ces positions, des règles ou des accords limitant le développement pourraient consolider l'avantage des grands acteurs américains. Le ministre français de l'Économie, Roland Lescure, a exprimé une position similaire, estimant que la France et l'Europe devaient continuer à accélérer l'adoption de l'IA tout en s'attaquant aux risques qu'elle comporte (**https://short.tips/url/5jn**). Il s'agit naturellement d'une position politique, et non d'une donnée technique concernant le niveau de sécurité des modèles. La stratégie française s'accompagne également d'investissements et de nouveaux produits. Mistral a annoncé en septembre un financement de 3 milliards d'euros et, quelques jours plus tard, un partenariat avec Mozilla visant à intégrer ses modèles dans Firefox Smart Window, dans un premier temps pour les utilisateurs de France et d'Amérique du Nord.




L'IA avance à grande vitesse, entre promesses d'innovation et nécessité de renforcer la sécurité. Jusqu'où faut-il accélérer ?



Dario Amodei, PDG d'Anthropic, a appelé à ralentir le rythme auquel les capacités des modèles d'IA sont développées.



# VOTRE TV VOUS SURVEILLE ! LE CAS LG QUI FAIT POLÉMIQUE

**Une enquête révèle les données collectées par les Smart TV LG : trafic réseau, appareils, contenus et fonctions vocales. Nous avons analysé ce qui se passe lorsque le téléviseur semble éteint.**

Un téléviseur connecté moderne est bien plus qu'un simple écran. C'est un véritable ordinateur relié au réseau domestique, capable d'exécuter des applications, de communiquer avec des serveurs distants, d'identifier les appareils présents sur le réseau et de collecter des informations sur la manière dont il est utilisé. Jusqu'ici, rien de particulièrement surprenant : c'est justement cette connectivité qui nous permet de regarder Netflix, YouTube, Disney+ et des dizaines d'autres services. Mais que se passe-t-il lorsque nous appuyons sur le bouton d'alimentation et que l'écran devient noir ? C'est la question au cœur d'une enquête menée par Gamers Nexus sur un téléviseur LG et analysée à l'aide d'outils de surveillance du trafic réseau (**https://short.tips/url/5jp**). Le résultat a attiré l'attention car, même en mode veille, le téléviseur peut continuer à communiquer avec l'extérieur et à effectuer des opérations qui restent normalement invisibles pour l'utilisateur.

## LES OUTILS DE L'ENQUÊTE

| OUTIL | À QUOI SERT-IL ? |
|---|---|
| Wireshark | Analyse les paquets qui transitent sur le réseau |
| Surveillance du trafic | Indique avec quels serveurs le téléviseur communique |
| Analyse de l'appareil | Contrôle le trafic généré par chaque application. |
| Paramètres de confidentialité | Permet de modifier les autorisations liées à la confidentialité. |

L'analyse s'est appuyée sur Wireshark, un outil capable de visualiser les communications qui transitent sur un réseau, et a mis en évidence différents types de trafic générés par le téléviseur. Parmi les éléments étudiés figurent notamment des fonctions liées à l'Automatic Content Recognition (ACR), ainsi que la détection des appareils présents sur le réseau domestique. Le terme « espionner », en revanche, mérite d'être nuancé. Une connexion à un serveur LG ne prouve pas, à elle seule, que le téléviseur intercepte des conversations privées ou mène une activité illégale.

Après la diffusion de ces accusations, LG a d'ailleurs publié une longue explication sur le fonctionnement de ses Smart TV, contestant précisément certaines des interprétations les plus alarmistes.

## QUE SAIT VRAIMENT VOTRE TÉLÉVISEUR ?

Pour fonctionner, une Smart TV doit communiquer avec Internet. Elle télécharge des mises à jour, vérifie la disponibilité des services, gère les applications et communique avec les plateformes de streaming. Toutes les connexions ne sont donc pas suspectes. Le problème se pose lorsqu'on cherche à savoir quelles informations accompagnent ces communications.

La CNIL (https://short.tips/url/5jq), l'autorité française chargée de la protection des données, rappelle depuis longtemps que les téléviseurs connectés peuvent collecter des informations sur les programmes regardés, les appareils connectés au réseau domestique et, dans certains cas, sur les personnes qui utilisent le téléviseur. Ces données peuvent également être utilisées pour analyser les habitudes de consommation des contenus et, lorsque les consentements nécessaires ont été recueillis, à des fins publicitaires. L'enquête menée montre justement à quel point il peut être révélateur d'observer une Smart TV directement du point de vue du réseau. Le téléviseur n'est pas isolé : il communique avec différents services et peut interagir avec d'autres appareils présents dans le foyer. L'analyse a également mis en évidence des références à l'ACR (Automatic Content Recognition), une technologie utilisée pour identifier certains contenus.

### QUELLES DONNÉES PEUVENT ENTRER EN JEU ?

- La TV peut détecter les appareils compatibles présents sur le réseau domestique.
- Des informations relatives à la connexion peuvent être traitées et, pour certaines fonctions, celles concernant les réseaux Wi-Fi environnants.
- Les fonctions de reconnaissance vocale peuvent traiter l'audio lors d'une interaction vocale.
- Lorsque les consentements nécessaires ont été recueillis, certaines informations peuvent être utilisées à des fins d'analyse de l'audience et de publicité ciblée en fonction des centres d'intérêt des utilisateurs.

### LG RÉPOND

LG conteste l'idée que ses téléviseurs enregistrent et transmettent en permanence les conversations au sein du foyer. Selon l'entreprise, la reconnaissance vocale s'active à l'aide d'un mot d'activation (« wake word »), du bouton du microphone ou de la fonction mains libres. La détection du mot d'activation est effectuée localement. LG précise également que l'ACR est une fonctionnalité optionnelle qui utilise une empreinte audio du contenu, sans effectuer de captures d'écran ni d'enregistrements vidéo ou vocal. La reconnaissance vocale, l'ACR et la publicité personnalisée peuvent être gérées depuis les paramètres du téléviseur.

```
192.168.XX.XXX - esp32s3-[REDACTED
192.168.10.XXX - [REDACTED ID] air
192.168.10.XXX - [Steve's Computer
192.168.10.XXX - [Vitalii's Comput
192.168.10.XXX - [REDACTED].ui.dir
192.168.10.XXX - (unknown) - Unide
192.168.10.XXX - [REDACTED ID] air
192.168.10.XXX - esp32s3-[REDACTED
192.168.10.XXX - esp32s3-[REDACTED
192.168.10.XXX - iPhone / Apple De
192.168.10.XXX - prusa-xl - Prusa
192.168.10.XXX - switch - Smart sw
192.168.10.XXX - AMI MegaRAC SPX 1
192.168.10.XXX - [STAFF PC] - Wind
192.168.10.XXX - esp32s3-[REDACTED
192.168.10.XXX - [STAFF NAME]-s-S2
192.168.10.XXX - esp32s3-[REDACTED
192.168.10.XXX - esp32s3-[REDACTED
192.168.10.XXX - chatapps.gnhome -
192.168.10.XXX - [Tannen's Compute
192.168.10.XXX - Staff-Galaxy-S23
192.168.10.XXX - AREA-51 - Alienwa
```

Gamers Nexus intercepte les communications générées par le téléviseur afin d'analyser les données transmises et les serveurs contactés. L'analyse du trafic réseau constitue l'un des outils utilisés pour étudier le comportement du téléviseur.

## ACR : QUE RECONNAÎT VRAIMENT LE TÉLÉVISEUR ?

L'Automatic Content Recognition est l'une des fonctions les plus intéressantes à connaître. LG explique que l'ACR peut utiliser une empreinte audio pour identifier le contenu affiché sur le téléviseur. Selon l'entreprise, le système ne réalise ni captures d'écran ni enregistrements vidéo ou audio du programme diffusé : il analyse au contraire le signal à l'aide du processeur audio interne afin d'en extraire une signature numérique. Une fois activée, cette fonction peut être utilisée pour analyser l'audience et les habitudes de visionnage. LG précise également que l'ACR est une fonction

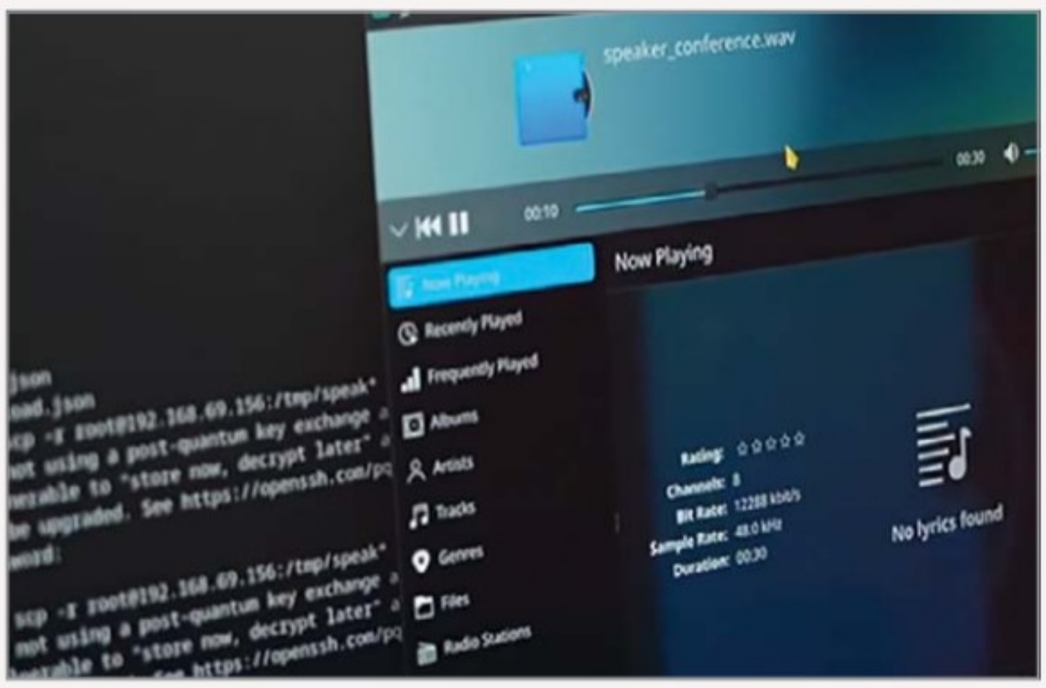


Scannez le QR code pour regarder l'enquête complète de Gamers Nexus.

optionnelle et que son utilisation nécessite l'acceptation de l'accord correspondant. La publicité basée sur les centres d'intérêt et la publicité entre appareils nécessitent, elles aussi, des consentements distincts.

## TV ÉTEINTE NE SIGNIFIE PAS HORS LIGNE

L'un des aspects les plus intéressants de l'enquête concerne précisément le mode veille. Lorsque nous appuyons sur le bouton d'alimentation, l'écran s'éteint et le téléviseur passe normalement en

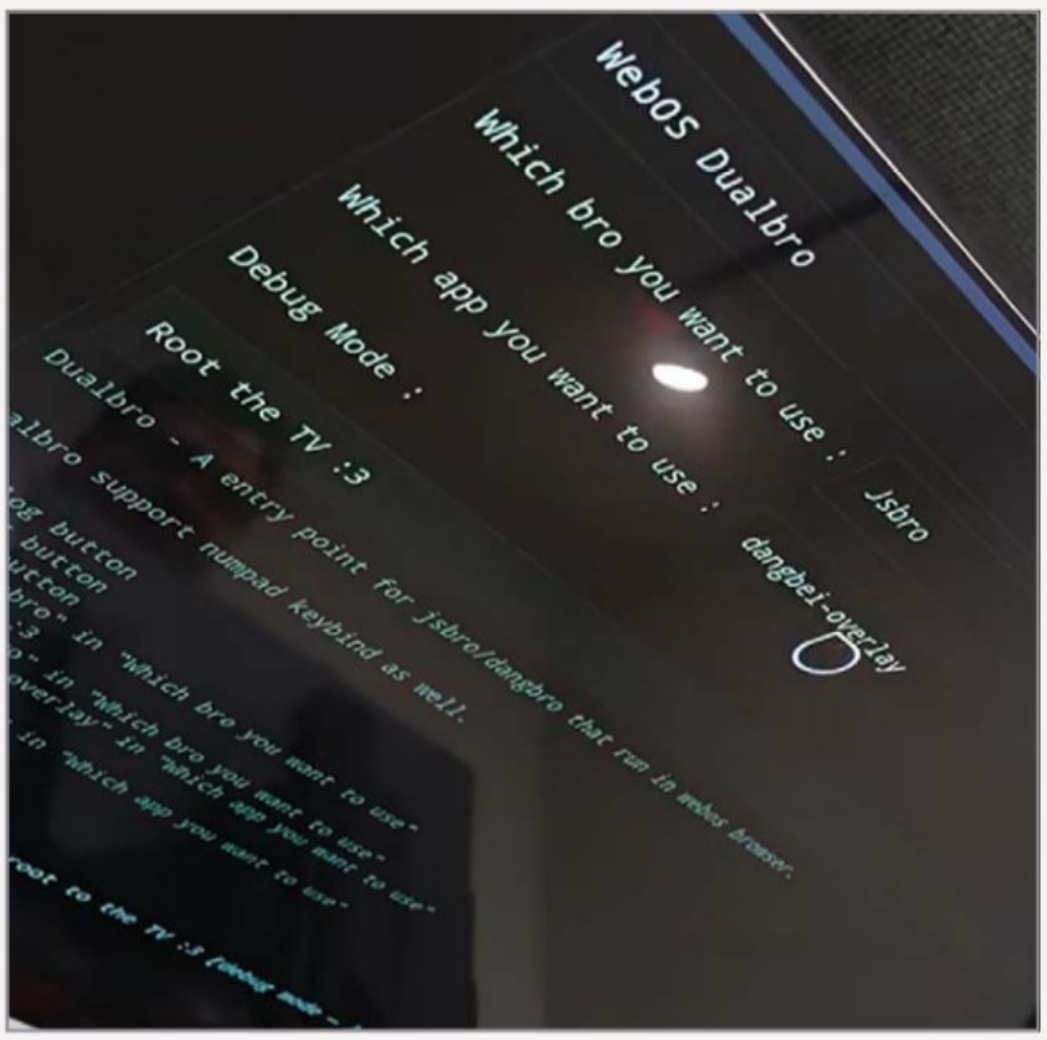



Au cours des tests, Gamers Nexus montre des données vocales converties en texte et analyse le fonctionnement du système de reconnaissance vocale. Il s'agit de l'un des points les plus controversés de l'enquête, contesté par LG dans sa réponse officielle.

## QU'EST-CE QUE L'ACR ?

**ACR signifie « Automatic Content Recognition », ou reconnaissance automatique des contenus. Cette technologie permet d'identifier ce qui est affiché sur le téléviseur grâce à une sorte d'« empreinte numérique » du contenu.**
**LG affirme que son système ACR utilise le processeur audio interne pour extraire cette empreinte et ne réalise ni captures d'écran ni enregistrements vidéo ou vocaux. Lorsqu'il est activé, l'ACR peut fournir des informations exploitables pour analyser l'audience et les habitudes de visionnage. L'utilisation de ces données à des fins de publicité basée sur les centres d'intérêt nécessite des consentements supplémentaires.**

mode veille, mais il n'est pas nécessairement déconnecté du réseau. Les composants électroniques restent alimentés et certaines fonctions peuvent continuer à fonctionner en arrière-plan.




**L'enquête ne se limite pas à la collecte de données : l'équipe a également analysé le logiciel du téléviseur et les vulnérabilités de webOS afin de déterminer si elles pouvaient être exploitées pour prendre davantage le contrôle de l'appareil.**

## TRUCS EN BREF

### COMMENT REPRENDRE LE CONTRÔLE DE VOTRE SMART TV

Vous n'utilisez pas les commandes vocales ? **Désactivez la reconnaissance vocale** et les fonctions mains libres.

Dans les paramètres de confidentialité, recherchez l'option relative à **l'ACR / Viewing Information** et désactivez-la si vous ne souhaitez pas recevoir de services basés sur vos habitudes de visionnage.

Dans les paramètres de confidentialité, recherchez les options relatives aux **publicités personnalisées** et au partage des données. Si vous n'en avez pas besoin, désactivez-les et révoquez les consentements que vous avez déjà accordés.

Vérifiez les modes **Always Ready**, **Quick Start** ou **Quick Start+** et désactivez ceux que vous n'utilisez pas. Réduire les fonctions actives en mode veille limite ce que le téléviseur peut faire lorsque vous ne regardez pas l'écran.

Vérifiez quels appareils sont associés au téléviseur et **désactivez les fonctions de connexion automatique** que vous n'utilisez pas. Évitez d'accorder au téléviseur davantage d'accès au réseau domestique que nécessaire.

Consultez régulièrement les **paramètres de confidentialité** et vérifiez les autorisations que vous avez accordées au Smart TV.

Vérifiez régulièrement si des mises à jour du téléviseur sont disponibles et **installez les mises à jour officielles**. Une Smart TV est un ordinateur connectée à Internet : son système d'exploitation doit lui aussi être maintenu à jour.

Désinstallez régulièrement les **applications que vous n'utilisez plus**. Moins de logiciels installés signifie moins de services actifs et une surface d'attaque réduite.



# WIGLE

# RÉSEAUX WI-FI AUTOUR DE VOUS

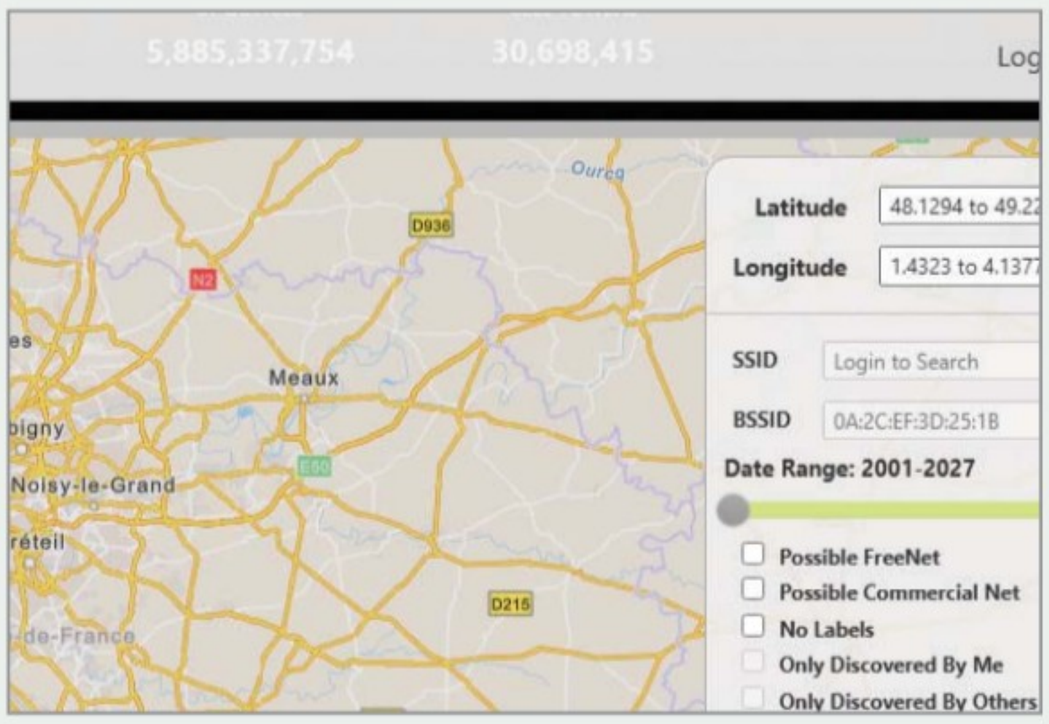
**Une gigantesque carte recense les réseaux sans fil détectés dans le monde entier. Avec WiGLE, vous pouvez explorer le territoire, analyser les signaux et comprendre la quantité d'informations que peuvent révéler les réseaux qui vous entourent.**

Lorsque vous recherchez un réseau Wi-Fi, vous vous contentez généralement de vérifier ceux qui sont disponibles à proximité. Il existe pourtant un projet qui a transformé cette simple activité en une gigantesque carte mondiale. Il s'appelle WiGLE (https://wigle.net/) et collecte les informations sur les réseaux sans fil repérés par ses utilisateurs. Créé en 2001, ce service permet d'afficher sur une carte les réseaux Wi-Fi identifiés dans différentes régions du monde. Il ne s'agit pas d'une liste de réseaux auxquels vous pouvez vous connecter : WiGLE est une immense base de données d'observations sans fil, utile pour étudier la répartition des réseaux et le paysage radio présent dans une zone donnée. Le plus intéressant est que vous pouvez également consulter ces données sur une carte interactive. En recherchant un lieu, vous pouvez voir les réseaux déjà enregistrés et, en zoomant, obtenir des informations plus détaillées. Le service permet également d'effectuer des recherches à partir de critères tels que le SSID et le BSSID.

## PAS SEULEMENT DU WI-FI : UN ATLAS DES RÉSEAUX

WiGLE ne se limite pas aux réseaux Wi-Fi. L'application officielle peut également

détecter et enregistrer des signaux Bluetooth et des réseaux cellulaires, en associant les observations à la position géographique fournie par l'appareil. Il est ainsi possible d'obtenir une photographie du paysage sans fil rencontré au fil des déplacements. L'application peut conserver localement les réseaux détectés, les afficher en temps réel sur la carte et vous permettre d'exporter les données dans différents formats, notamment CSV, KML, SQLite et GPX. Vous pouvez donc utiliser les informations collectées pour effectuer des analyses ultérieures ou visualiser les parcours réalisés. Le système repose sur la contribution de la communauté : les utilisateurs peuvent collecter de nouvelles observations au cours de leurs déplacements et, s'ils le souhaitent, contribuer à la base de données de WiGLE.




## COMMENT UTILISER WIGLE ?

Vous pouvez commencer directement par la carte de WiGLE, sans rien installer. La carte permet d'explorer les réseaux présents dans la base de données et d'effectuer des recherches géographiques. Vous pouvez également filtrer les résultats et utiliser des paramètres tels que le SSID, le BSSID et des intervalles de temps. Si vous souhaitez contribuer à la collecte de données, vous pouvez utiliser l'application WiGLE WiFi Wardriving pour Android. Au cours de vos déplacements, l'application détecte les réseaux sans fil présents à proximité et enregistre les observations correspondantes, en utilisant le GPS pour en estimer la position. Les données peuvent être conservées sur l'appareil ou envoyées au service. L'application est open source, ne contient aucune publicité et propose également des outils permettant d'analyser les réseaux détectés, de créer des cartes en temps réel et d'exporter les résultats.

## UN OUTIL POUR L'ANALYSE DE SÉCURITÉ

La possibilité d'observer la répartition des réseaux et d'analyser des informations telles que le SSID, le BSSID, la position et les caractéristiques de la connexion permet d'étudier le paysage sans fil d'une zone donnée. L'application elle-même cite notamment le « site survey » et l'analyse de sécurité parmi ses utilisations possibles.




Attention toutefois : WiGLE n'est pas un outil permettant d'accéder aux réseaux d'autrui. Le projet précise explicitement que le service n'est ni destiné à rechercher des réseaux Wi-Fi gratuits ni à utiliser des réseaux sans autorisation.



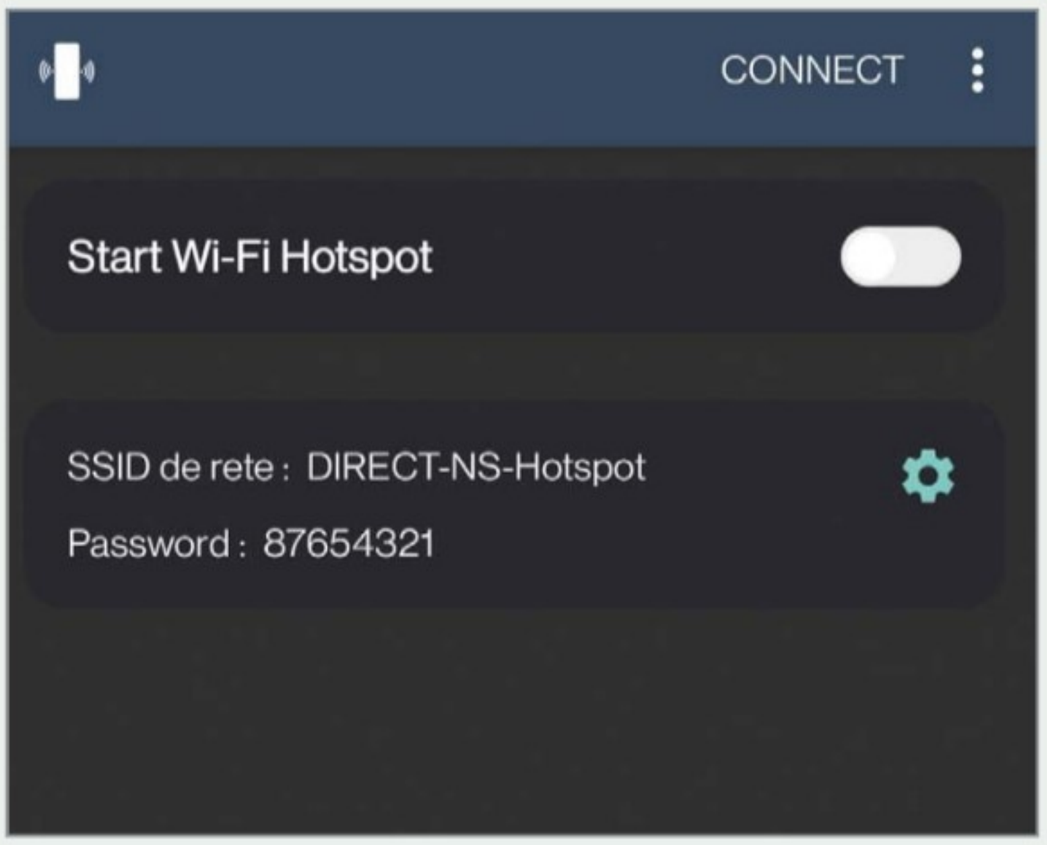

# VOUS AVEZ UN ROUTEUR GRATUIT SANS LE SAVOIR

**Vous avez un ancien smartphone Android qui ne sert plus ? Avec la bonne application, vous pouvez le transformer en répéteur Wi-Fi et étendre la connexion jusque dans les pièces les plus éloignées du routeur.**

Vous avez certainement déjà été confronté à un signal Wi-Fi faible dans certaines pièces de la maison. Le routeur est peut-être installé dans le salon, tandis que dans la chambre ou le bureau, la connexion devient lente et instable. Lorsque le signal n'arrive pas là où vous en avez besoin, la solution la plus évidente semble être d'acheter un répéteur Wi-Fi. Avant de dépenser de l'argent, jetez pourtant un coup d'œil à cet ancien smartphone Android que vous avez oublié dans un tiroir. Même s'il ne vous sert plus au quotidien, il peut encore être suffisamment puissant pour remplir une fonction complètement différente.

Avec l'application NetShare (**https://netshare.app/**), vous pouvez transformer le smartphone en un appareil capable de partager la connexion et de créer un nouveau réseau sans fil. En le plaçant à un endroit stratégique de la maison, vous pouvez étendre le Wi-Fi jusqu'aux pièces où le signal du routeur a le plus de mal à parvenir.

La configuration est relativement simple et ne demande que quelques minutes. Voyons donc comment exploiter cette possibilité.




## CONFIGUREZ LE RÉPÉTEUR

Pour commencer, prenez l'ancien smartphone Android et activez le Wi-Fi. Dans les paramètres de l'appareil, sélectionnez ensuite votre réseau domestique et saisissez le mot de passe si nécessaire. Il est important que le téléphone soit bien connecté au réseau principal avant de poursuivre la configuration. Installez ensuite NetShare et lancez l'application. Depuis l'écran principal, accédez à la fonction **Configure Hotspot**, qui permet de définir le nom du nouveau réseau et son mot de passe. Vous pouvez choisir librement ces paramètres ou, pour simplifier la connexion, reprendre ceux du réseau que vous souhaitez étendre. Une fois le point d'accès configuré, revenez à l'écran principal et sélectionnez **Start Wi-Fi Hotspot**. Si l'application demande des autorisations supplémentaires, accordez-les afin de permettre au téléphone d'assurer la fonction prévue. Vous pouvez maintenant déplacer le smartphone dans la pièce où vous souhaitez améliorer la couverture. Ne le placez pas là où le signal est déjà presque inexistant : choisissez plutôt une position intermédiaire, où le téléphone reçoit encore correctement le signal Wi-Fi d'origine tout en pouvant atteindre la zone à couvrir.

## CONNECTEZ LES APPAREILS

Une fois le point d'accès activé, les autres appareils peuvent se connecter au réseau créé par l'ancien smartphone. Vous pouvez ainsi utiliser un ordinateur portable, une tablette ou d'autres appareils dans la zone où le réseau principal était plus faible. Dans certains cas, la connexion peut ne pas fonctionner automatiquement. La configuration indiquée pour NetShare prévoit alors l'utilisation manuelle d'un proxy HTTP, en spécifiant comme serveur l'adresse **192.168.49.1** et comme **port 8282**.




Une fois la connexion établie, vous pouvez immédiatement vérifier si la solution est efficace. Si le signal reste faible, essayez de rapprocher le smartphone du routeur ou de le placer à un autre endroit : quelques mètres peuvent faire une différence significative, notamment lorsque des murs, des meubles ou d'autres obstacles se trouvent entre les appareils. Lorsque vous n'avez plus besoin du répéteur, vous pouvez interrompre le partage directement depuis NetShare en utilisant **Stop Wi-Fi Hotspot**.

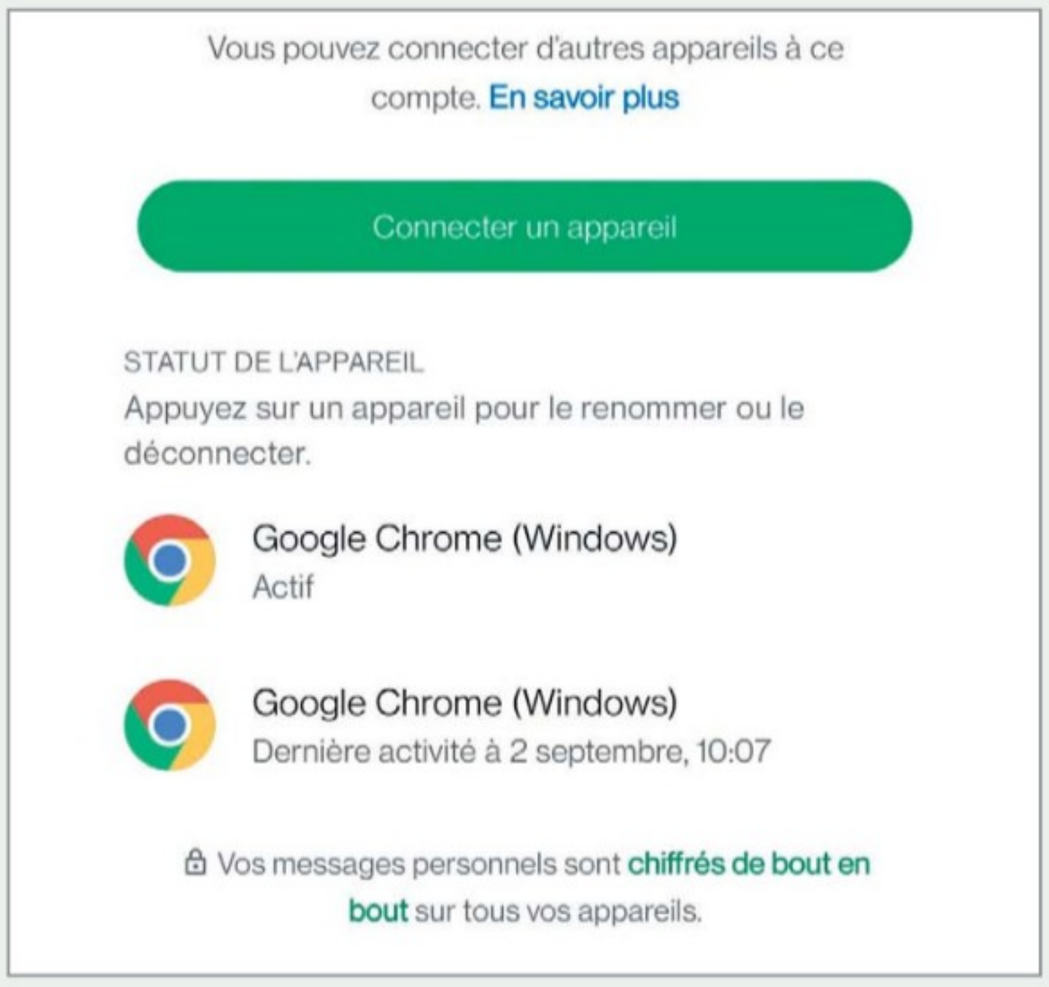



# QUELQU'UN LIT-IL VOS CONVERSATIONS ?

**Il suffit de quelques secondes d'accès à votre smartphone pour connecter WhatsApp à un autre ordinateur. Voici comment vérifier si quelqu'un lit vos conversations sur la célèbre application de messagerie.**

Tout le monde ne le sait pas, mais les conversations que vous échangez chaque jour sur WhatsApp peuvent également être consultées depuis un ordinateur. Il n'est pas forcément nécessaire de connaître votre mot de passe ou d'installer un programme suspect : quelques secondes d'accès à votre smartphone peuvent suffire.

WhatsApp permet en effet d'utiliser le même compte sur les versions Web et Desktop du service. Pour connecter un nouvel ordinateur, il suffit de scanner un code QR avec le smartphone. Une fois l'opération terminée, l'appareil est associé au compte et peut permettre de consulter les conversations. Le problème est que cette procédure peut être réalisée très rapidement. Si quelqu'un parvient à prendre votre téléphone en main, ne serait-ce que quelques instants, et termine l'association, vous pourriez ne pas vous en apercevoir immédiatement. Cela ne signifie pas que n'importe qui peut automatiquement lire vos conversations : il faut d'abord réussir à associer son appareil à votre compte. Cependant, précisément parce que l'opération peut passer inaperçue, il est recommandé de vérifier régulièrement quels appareils sont associés à votre compte WhatsApp.



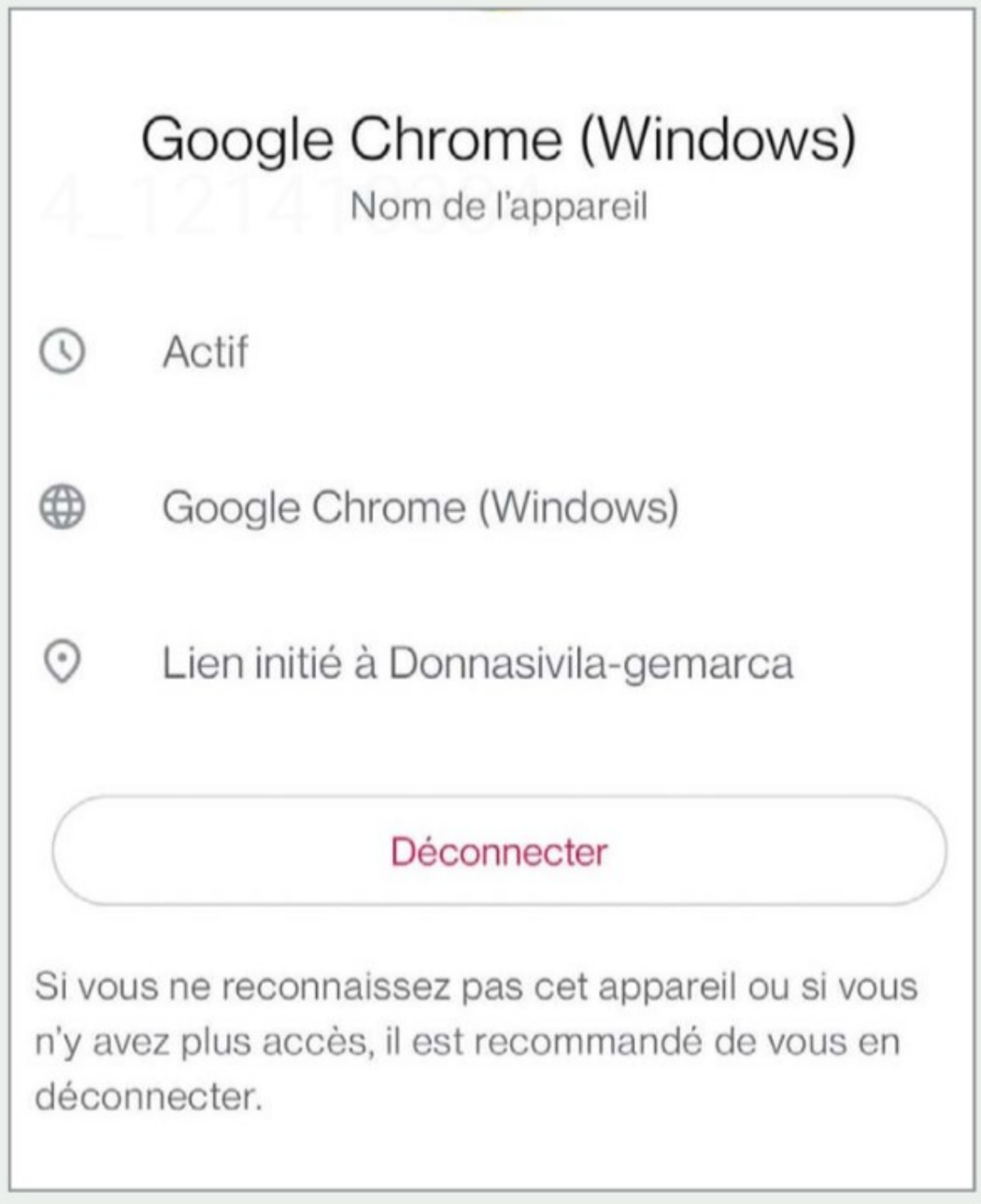

Heureusement, aucun outil particulier n'est nécessaire. WhatsApp propose une section qui répertorie tous les appareils connectés au compte, ce qui permet de vérifier rapidement la situation et, si nécessaire, de déconnecter une session suspecte.

## QUI EST CONNECTÉ À VOTRE COMPTE ?

Si vous utilisez un smartphone Android, ouvrez WhatsApp et accédez à l'écran principal de l'application. Appuyez ensuite sur le bouton représentant trois points verticaux, situé en haut à droite de l'écran. Dans le menu qui s'affiche, accédez à la section **Appareils connectés**. WhatsApp affiche alors la liste des appareils associés à votre compte.

Examinez attentivement les informations affichées. Outre le type d'appareil, vous pouvez également vérifier la dernière activité enregistrée. Si vous reconnaissez toutes les connexions présentes dans la liste, aucune intervention n'est nécessaire. Si, en revanche, un ordinateur ou un autre appareil que vous n'avez jamais utilisé apparaît dans la liste, il est préférable d'agir immédiatement.

Sur iPhone la procédure est très similaire, mais l'accès à la fonction se trouve à un autre endroit. Ouvrez WhatsApp et appuyez sur **Vous**, en bas de l'écran. Vous pouvez ensuite accéder à la section **Appareils connectés**, qui répertorie les connexions associées à votre compte. Là encore, vérifiez le type d'appareil et la date de sa dernière activité. Comparez ces informations avec les appareils que vous vous souvenez avoir utilisés afin d'identifier plus facilement les éventuelles sessions que vous n'avez pas autorisées. Si vous trouvez un ordinateur que vous ne reconnaissez pas, il n'est pas nécessaire de changer de numéro de téléphone ni de réinstaller WhatsApp.




La solution la plus simple consiste à déconnecter directement l'appareil depuis la liste. Sélectionnez la connexion que vous ne reconnaissez pas et utilisez l'option proposée pour effectuer la déconnexion. La session sera alors fermée et cet appareil ne pourra plus accéder à vos conversations via la connexion précédemment autorisée.



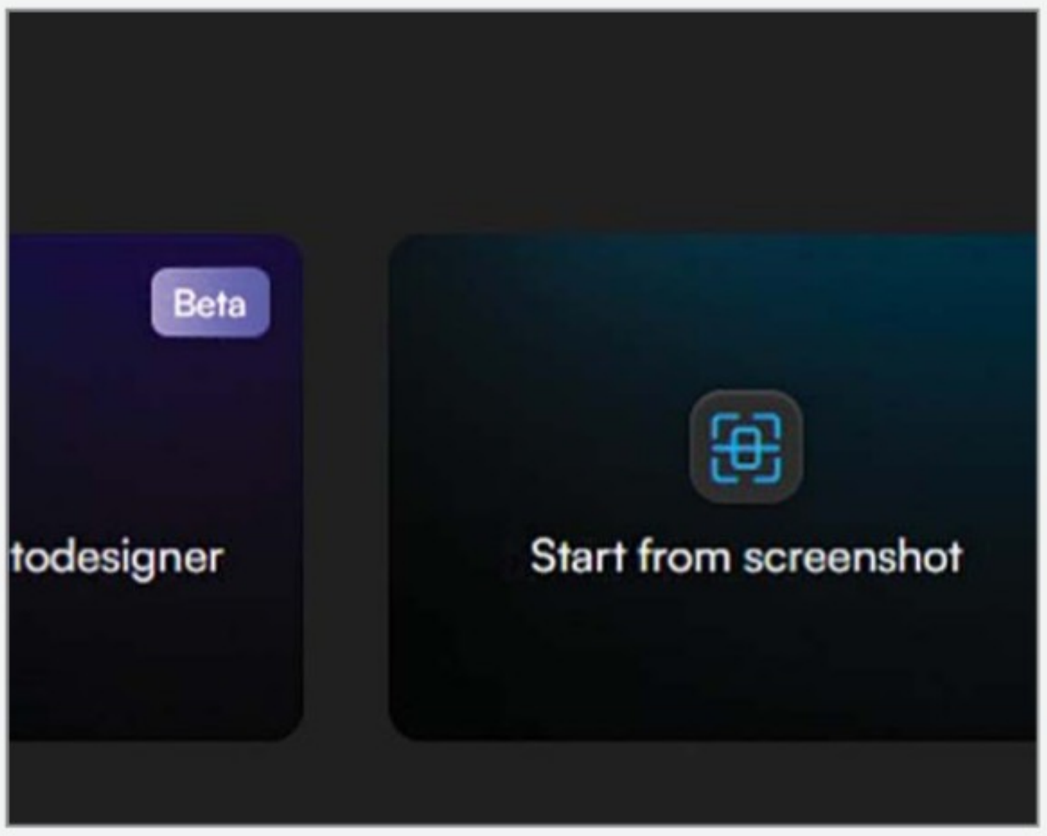
# D'UNE CAPTURE D'ÉCRAN À UNE MAQUETTE MODIFIABLE !

**L'intelligence artificielle d'Uizard.io transforme les captures d'écran en projets entièrement modifiables. Vous pouvez changer les textes, les boutons, les couleurs et les images sans devoir tout recréer de zéro.**

Une capture d'écran est, par définition, une image « plate » : nous pouvons la regarder, la partager ou la retoucher, mais nous ne pouvons pas sélectionner séparément un bouton, modifier un texte ou déplacer un élément de l'interface. Uizard.io tente de changer complètement cette approche grâce à Screenshot Scanner, une fonction qui utilise l'intelligence artificielle pour analyser une capture d'écran et la reconstruire sous la forme d'une véritable maquette numérique modifiable.

## TRANSFORMEZ LA CAPTURE

L'idée est simple : au lieu de recréer manuellement une interface à partir d'une image, nous laissons l'IA reconnaître les différents éléments présents dans la capture d'écran. Les textes, les images et les boutons sont interprétés et transformés en objets que nous pouvons ensuite sélectionner et modifier. Pour commencer, il suffit de



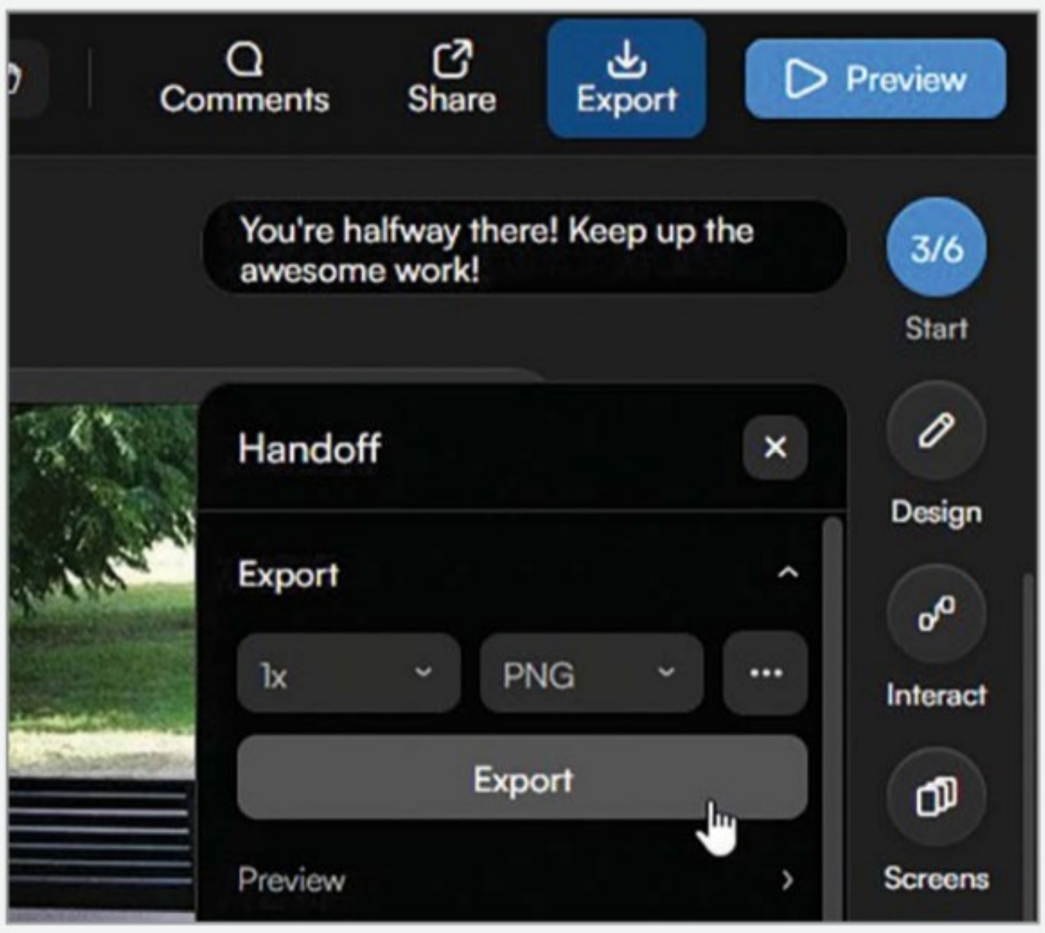

créer gratuitement un compte sur Uizard.io et de choisir l'option **Start from screenshot**. Après avoir importé l'image, le service l'analyse et génère la maquette correspondante, entièrement modifiable.

## CHANGEZ TOUT EN QUELQUES CLICS

Une fois l'analyse terminée, la capture d'écran n'est plus une simple image. Nous pouvons en effet intervenir sur les différents éléments reconnus par Uizard et modifier leur apparence. En sélectionnant un objet, nous pouvons changer les textes, les couleurs, les dimensions et la position, tandis que le panneau latéral **Design** permet également d'intervenir sur les polices, les espacements et les styles. En pratique, vous pouvez partir d'un écran existant et le transformer en ébauche d'une nouvelle interface. Une fois les modifications terminées, le projet peut être exporté à l'aide de la commande Export disponible dans l'interface.

## LA CAPTURE VIENT DU SMARTPHONE

Uizard ne vous oblige même pas à transférer manuellement sur le PC les images présentes sur votre téléphone. La fonction **Screenshot Scanner** met à disposition un QR code que vous pouvez scanner directement avec votre smartphone. Un lien est ainsi établi immédiatement entre les deux appareils et vous pouvez envoyer la capture à modifier sans utiliser de câble ni installer d'application supplémentaire. Une fois la capture d'écran reçue, l'intelligence artificielle la reconstruit sous la forme d'une maquette modifiable, en séparant les éléments qu'elle parvient à reconnaître. Cette solution est particulièrement pratique lorsque l'écran que vous souhaitez modifier se trouve déjà sur votre téléphone et que vous ne voulez pas perdre de temps à le transférer sur l'ordinateur. La reconstruction automatique est intéressante, mais cela ne signifie pas que le résultat est toujours parfait. Lors des tests rapportés dans l'article original, Uizard a notamment rencontré quelques difficultés pour reconnaître correctement le texte présent dans une capture d'écran de WhatsApp.



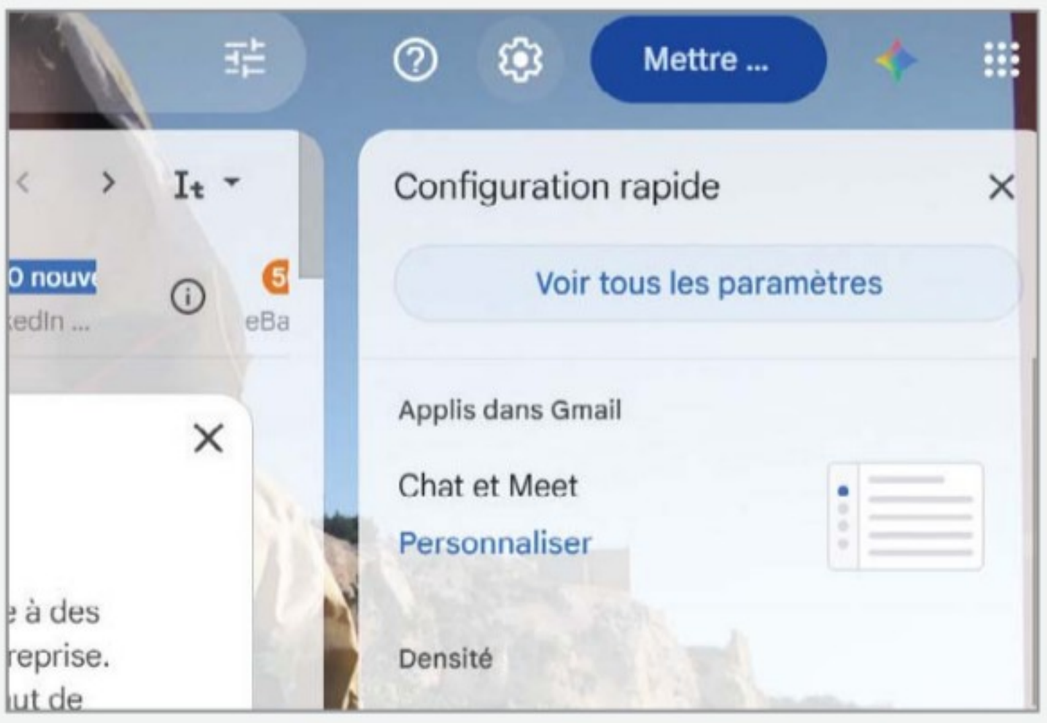

La mise en page peut donc être reconstruite, mais certains éléments peuvent nécessiter une intervention manuelle avant d'obtenir le résultat souhaité. Une autre limite est à prendre en compte si vous utilisez l'offre gratuite : la version Free permet de créer jusqu'à deux projets, chacun pouvant contenir jusqu'à cinq écrans. Les projets peuvent ensuite être supprimés depuis la section **Projects**.



# L'IA DE GMAIL LIT-ELLE VOS E-MAILS ?

**Gemini et les fonctions intelligentes de Gmail analysent le contenu de vos messages pour vous proposer des résumés, des suggestions et des réponses automatiques. Mais si vous préférez garder vos e-mails à l'écart de l'IA, vous pouvez désactiver ces fonctions.**

Ces derniers mois, Gmail a intégré toujours plus d'outils basés sur l'intelligence artificielle. Grâce à Gemini, le service peut analyser une partie des messages pour vous aider à gérer plus rapidement votre courrier électronique : il peut résumer de longues conversations, suggérer des réponses, vous aider à rédiger des brouillons et mettre en évidence des informations telles que les dates et les noms. Tout cela peut être pratique, notamment lorsque votre boîte de réception déborde d'e-mails. Mais un aspect mérite une attention particulière : la confidentialité. Google a déclaré que la fonctionnalité AI Enhanced Classification and Review n'analyse pas automatiquement le contenu des e-mails sans autorisation ; parallèlement, certaines fonctions




intelligentes peuvent être activées sur certains comptes.

## QUE PEUT FAIRE L'IA DE GMAIL ?

L'intelligence artificielle est désormais intégrée à différentes fonctions de la messagerie de Google. Elle peut vous aider à résumer une conversation, à suggérer une réponse cohérente avec le message reçu ou encore à vous assister dans la rédaction d'un texte. L'objectif est de réduire le temps nécessaire pour gérer les e-mails, notamment lorsque vous devez traiter de nombreux messages chaque jour. **Smart Reply**, la fonction d'IA de Gmail, propose automatiquement plusieurs réponses rapides en fonction du contenu des e-mails reçus. Au lieu de tout rédiger à partir de zéro, Gmail peut vous afficher de courtes phrases déjà prêtes, que vous pouvez sélectionner d'un simple clic. L'IA analyse le sens de la conversation afin de tenter de proposer une réponse pertinente. Le système est particulièrement adapté aux situations dans lesquelles vous recevez des messages similaires ou devez simplement confirmer une information. La suggestion ne correspond toutefois pas toujours exactement à ce que vous souhaitez communiquer : vous pouvez donc le modifier avant de l'envoyer ou simplement l'ignorer. Selon Google, les suggestions sont générées automatiquement et ne sont pas partagées avec des tiers.

## DÉSACTIVEZ LES FONCTIONS INTELLIGENTES

Si vous préférez renoncer à ces fonctions, Gmail propose un réglage spécifique. Lorsque vous accédez au service après une certaine période, un message consacré aux nouvelles fonctionnalités d'IA peut apparaître : depuis cet écran, vous pouvez choisir de désactiver les fonctionnalités intelligentes dans Workspace.




Sur l'écran suivant, Gmail vous propose deux possibilités. Vous pouvez conserver les fonctionnalités intelligentes dans les autres services Google, tels que Calendar, Wallet et l'Assistant Google, ou désactiver complètement les fonctionnalités intelligentes. Une fois votre choix effectué, il suffit de confirmer avec **Enregistrer** pour appliquer la configuration. Si le message n'apparaît pas, vous pouvez intervenir manuellement depuis les paramètres de Gmail. Cliquez sur l'icône en forme d'engrenage en haut à droite et recherchez l'option relative aux **Fonctionnalités intelligentes dans Gmail, Chat et Meet**. En décochant cette option et en confirmant la modification, les fonctions intelligentes sont désactivées.




# STOP AUX ESPIONS SUR VOTRE PC

**Votre ordinateur conserve une quantité impressionnante d'informations sur vos activités. Avec Ashampoo Privacy Inspector, vous pouvez les identifier et les supprimer de manière sélective.**

Chaque fois que vous utilisez votre PC, vous laissez derrière vous une longue traînée d'informations. Les fichiers ouverts, les sites visités, les recherches, les téléchargements et les activités récentes peuvent rester enregistrés sur le système ou dans les navigateurs, créant une sorte de journal numérique de vos habitudes. Le problème devient encore plus évident lorsque l'ordinateur est partagé avec des membres de votre famille, des collègues ou des camarades d'études : la personne qui l'utilise après vous pourrait facilement reconstituer une partie de vos activités. Il est donc important de savoir quelles informations sont conservées et, surtout, de disposer des outils nécessaires pour les supprimer.

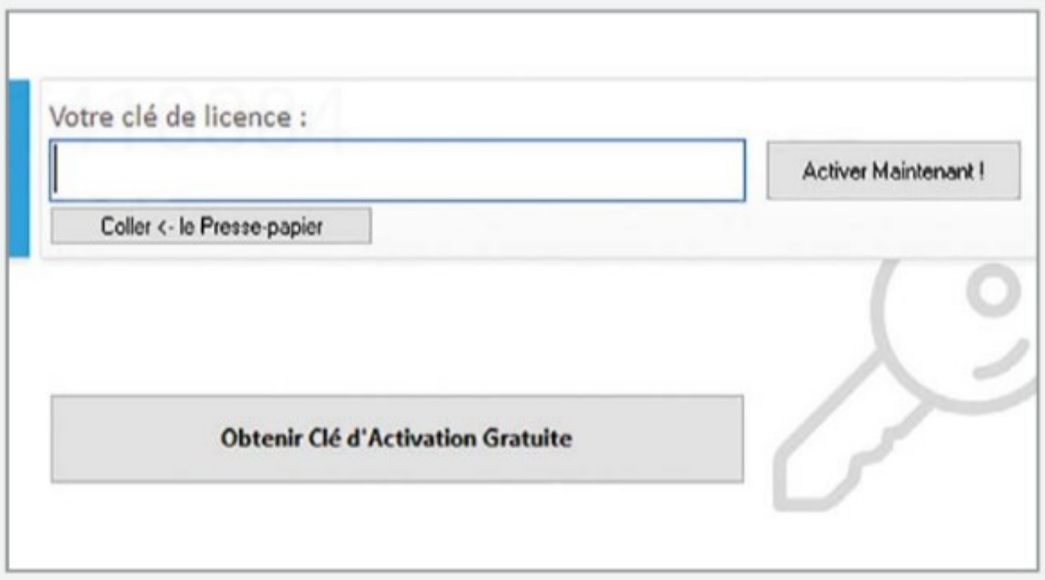
## VOICI NOTRE SOLUTION

Ashampoo Privacy Inspector est conçu pour identifier les traces laissées sur le système et dans les navigateurs et vous permettre d'intervenir de manière sélective. Le programme répartit les informations en différentes catégories, des éléments récemment utilisés aux activités

effectuées sur le PC, en passant par les sites Web, les recherches, les téléchargements et les données des navigateurs. Il ne s'agit donc pas d'un programme classique qui nettoie tout sans distinction : vous pouvez analyser les différentes catégories et décider quelles traces supprimer et lesquelles conserver. Avant cela, nous devons toutefois installer le programme et activer notre copie.

## OBTENEZ LA LICENCE

Pour nos lecteurs, le logiciel sera disponible avec une licence gratuite. Pour l'obtenir, vous devrez créer un compte Ashampoo gratuit sur le site **https://www.ashampoo.com/fr-fr** et terminer votre inscription.




Une fois connecté, vous pourrez télécharger l'outil depuis **https://short.tips/url/privinsp** et lancer la procédure d'installation. Pendant l'installation, lorsque la fenêtre d'activation apparaît, choisissez l'option permettant d'obtenir une clé d'activation gratuite. Saisissez l'adresse e-mail demandée et sélectionnez la demande de clé pour la version complète. Votre clé de licence personnelle s'affiche alors. Copiez-la, revenez à la fenêtre d'installation et collez-la dans le champ prévu à cet effet. Cliquez sur **Activer** maintenant pour déverrouiller la version complète, puis poursuivez avec les paramètres par défaut.

## EFFAÇONS LES TRACES

Une fois que vous avez identifié les informations que vous souhaitez supprimer, vous pouvez procéder à un nettoyage sélectif. Vous n'êtes pas obligé de tout effacer : accédez à la catégorie concernée et intervenez uniquement sur les traces que vous souhaitez supprimer. Vous pouvez par exemple effacer la liste des fichiers récemment ouverts ainsi que les activités enregistrées par le système. Vous évitez ainsi que le prochain utilisateur puisse reconstituer les documents que vous avez ouverts ou les programmes que vous avez utilisés. Le même principe s'applique aux recherches.




En ouvrant la section **Termes de recherche**, vous pouvez afficher les mots-clés enregistrés et supprimer ceux que vous préférez ne pas laisser sur le PC. La navigation Web peut elle aussi être nettoyée de manière ciblée. Privacy Inspector permet d'intervenir sur la liste des sites visités et les sessions Web, en supprimant l'historique, les cookies, les URL et d'autres informations associées à la navigation. Il est également intéressant de pouvoir choisir le navigateur à nettoyer. Vous pouvez par exemple intervenir sur Chrome, Firefox ou Edge sans nécessairement supprimer les informations présentes dans les autres navigateurs. La liste des fichiers téléchargés constitue une autre source d'informations que nous oublions souvent. Privacy Inspector affiche les téléchargements effectués, avec leurs chemins d'accès et leurs dates, et permet d'en supprimer l'historique.




# L'IA CONTRE LES ARNAQUES

**Pas seulement les virus et les logiciels malveillants : Avast One intègre un assistant basé sur l'intelligence artificielle générative qui analyse les messages, les liens et les offres suspects pour vous aider à repérer les tentatives de phishing et les escroqueries.**

Lorsque nous pensons à un antivirus, nous imaginons surtout un programme chargé de détecter les virus, les logiciels malveillants et autres menaces cachées sur l'ordinateur. Mais aujourd'hui, la cybersécurité ne concerne plus uniquement ce qui peut infecter le PC : vous êtes vous aussi devenu une cible. Un SMS apparemment inoffensif, un e-mail qui semble provenir de votre banque, une offre en ligne trop belle pour être vraie ou un lien reçu d'un expéditeur inconnu peuvent dissimuler une tentative de phishing ou une escroquerie financière. Reconnaître ces menaces n'est pas toujours simple, surtout lorsque le message est conçu pour paraître authentique. Avast One tente de répondre à ce problème en associant aux fonctions de sécurité traditionnelles un module basé sur l'intelligence artificielle générative : l'**Assistant Avast**.

## INSTALLEZ AVAST ONE

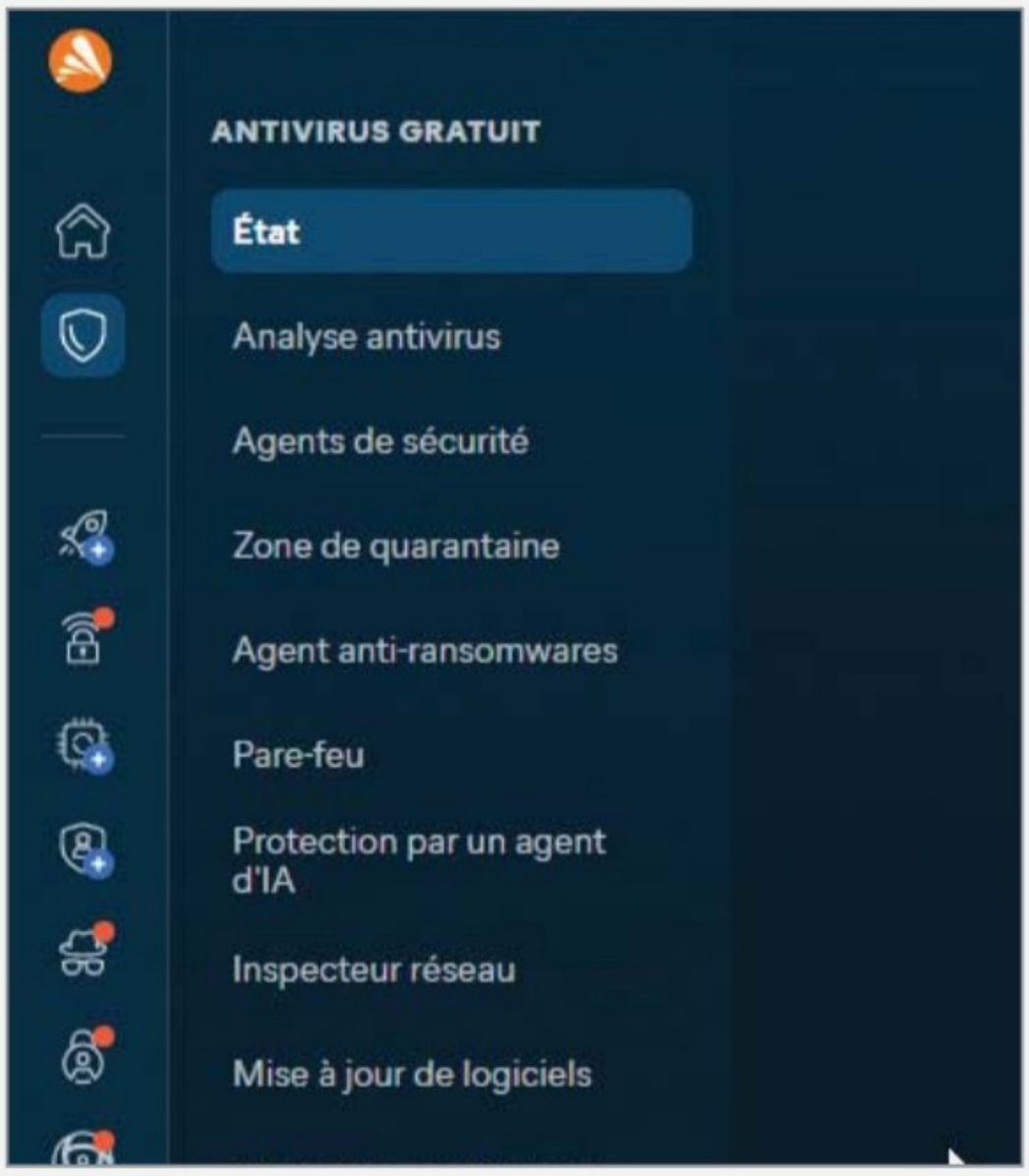
Vous pouvez télécharger l'exécutable officiel depuis https://www.avast.com/fr-fr/free-antivirus-download#pc.




Après avoir lancé l'installeur, lorsque Windows vous demande l'autorisation d'apporter des modifications à l'appareil, confirmez en cliquant sur **Oui**. Le bouton **Installer** apparaît alors : cliquez dessus pour lancer l'assistant d'installation. Avast se connecte automatiquement à Internet et télécharge les fichiers nécessaires pour terminer l'installation. Une fois le téléchargement terminé, le programme peut vous proposer d'effectuer une **Analyse intelligente**, qui vérifie le système à la recherche de virus et d'autres menaces.

## METTEZ L'IA À L'ÉPREUVE

L'élément le plus intéressant d'Avast One est l'**Assistant Avast**, accessible depuis le bouton situé dans la partie inférieure gauche de l'interface. Vous pouvez alors ouvrir une conversation et soumettre vos questions à l'IA. Vous n'êtes pas obligé de copier-coller le contenu d'un message : l'assistant permet également de charger une capture d'écran. Vous



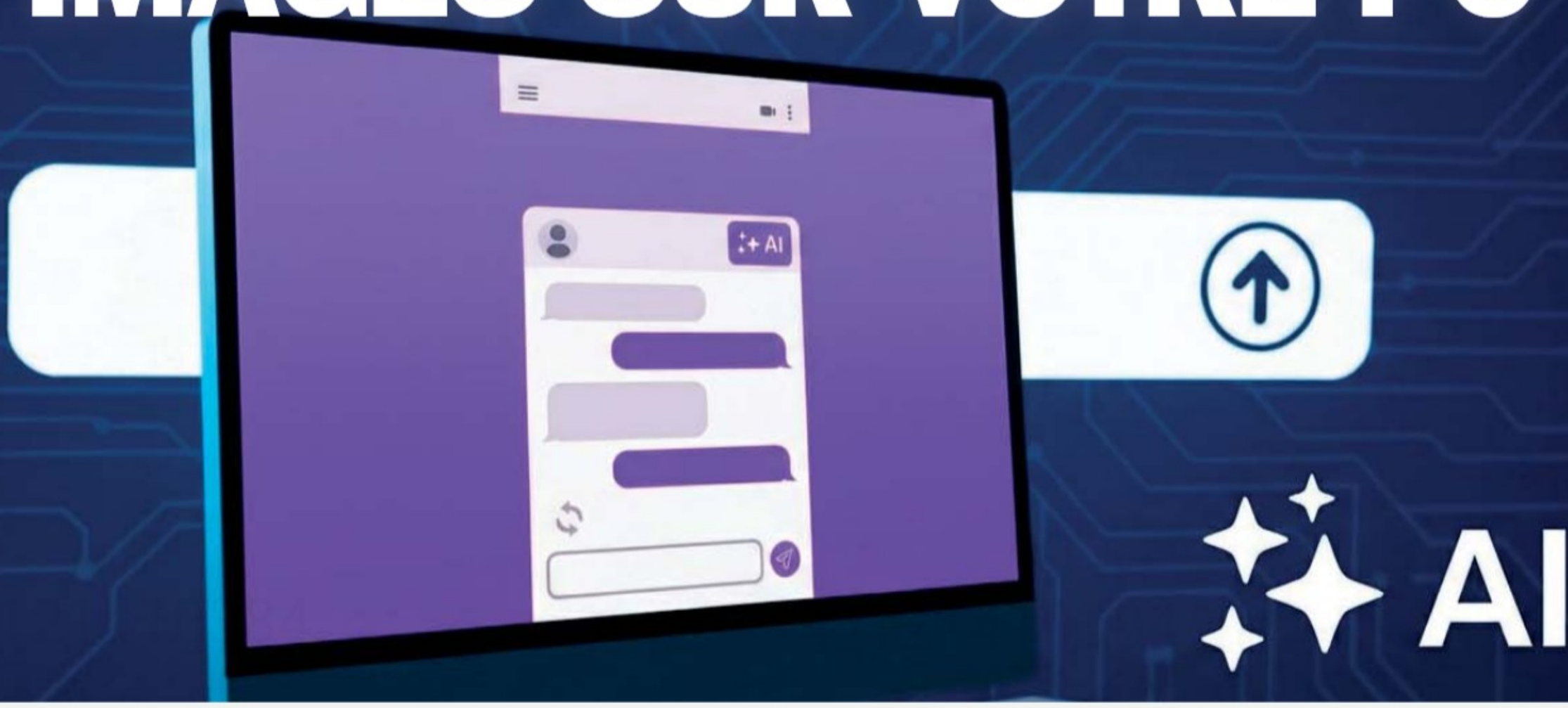

pouvez donc lui montrer directement ce que vous avez reçu et lui demander de vérifier la présence d'éléments suspects. Le système est surtout conçu pour les situations dans lesquelles vous ne savez pas comment interpréter un message, un lien ou une offre. L'IA analyse le contenu et vous fournit une évaluation accompagnée de conseils pratiques.

## QUAND UN SMS DEVIENT SUSPECT

Imaginez que vous receviez un SMS vous invitant à cliquer sur un lien pour suivre une livraison. À première vue, il pourrait sembler parfaitement normal. Mais c'est précisément le mécanisme exploité par de nombreuses techniques d'ingénierie sociale : partir d'une situation quotidienne et plausible pour vous inciter à effectuer une action. Au lieu d'ouvrir directement le lien, vous pouvez copier le message ou en faire une capture d'écran et la soumettre à l'**Assistant Avast**. L'IA analyse la situation et, dans l'exemple présenté, l'identifie comme une « Escroquerie probable ».

# FOOOCUS

# L'IA QUI CRÉE DES IMAGES SUR VOTRE PC




**Générez des images avec l'intelligence artificielle, modifiez-les et agrandissez-les sans envoyer vos fichiers en ligne. Tout se passe directement sur votre ordinateur.**

Fooocus est un logiciel gratuit conçu pour fonctionner directement sur votre PC et qui permet de créer des images à partir d'une simple description textuelle. Le programme poursuit un objectif précis : simplifier au maximum l'utilisation de l'IA générative. Inutile de vous perdre parmi des dizaines de paramètres techniques ou des configurations complexes : vous vous concentrez sur la description de ce que vous souhaitez obtenir, tandis que Fooocus se charge d'optimiser une grande partie des réglages. Le logiciel permet non seulement de générer des images à partir d'un texte, mais aussi d'utiliser des images existantes comme référence et de les modifier.

## INSTALLEZ FOOOCUS

Téléchargez l'outil depuis le site **https://short.tips/url/fooocdown**. Après avoir décompressé l'archive, lancez le fichier **run.bat** et confirmez son exécution lorsque Windows vous le demande. Au premier démarrage, Fooocus vérifie automatiquement les caractéristiques matérielles de l'ordinateur. Si le système répond aux exigences, le programme s'ouvre dans le navigateur par défaut. Dans le cas contraire, un message d'erreur s'affiche. Vous devez toutefois disposer d'un PC suffisamment puissant : le logiciel est conçu pour fonctionner avec un GPU doté d'au moins 8 Go de VRAM, tandis que les cartes graphiques NVIDIA de la gamme RTX sont recommandées pour

```
System ARGV] ['Fooocus\\entry_with_update.py']
ython 3.10.9 (tags/v3.10.9:1dd9be6, Dec  6 2022, 20:
ooocus version: 2.5.5
rror checking version for opencv-contrib-python-head
ss
nstalling requirements
Cleanup] Attempting to delete content of temp dir C:
Cleanup] Cleanup successful
ownloading: "https://huggingface.co/mashb1t/misc/res
ktop\Fooocus_win64_2-5-0\Fooocus\models\vae_approx\x

00%|
ownloading: "https://huggingface.co/lllyasviel/fav_m
:\Users\User\Desktop\Fooocus_win64_2-5-0\Fooocus\mod

54%|
```

obtenir des performances optimales. Lors du premier démarrage, les modèles d'IA nécessaires au fonctionnement du programme sont également téléchargés automatiquement. Cette opération peut prendre plusieurs minutes.

## SAISISSEZ LE PROMPT

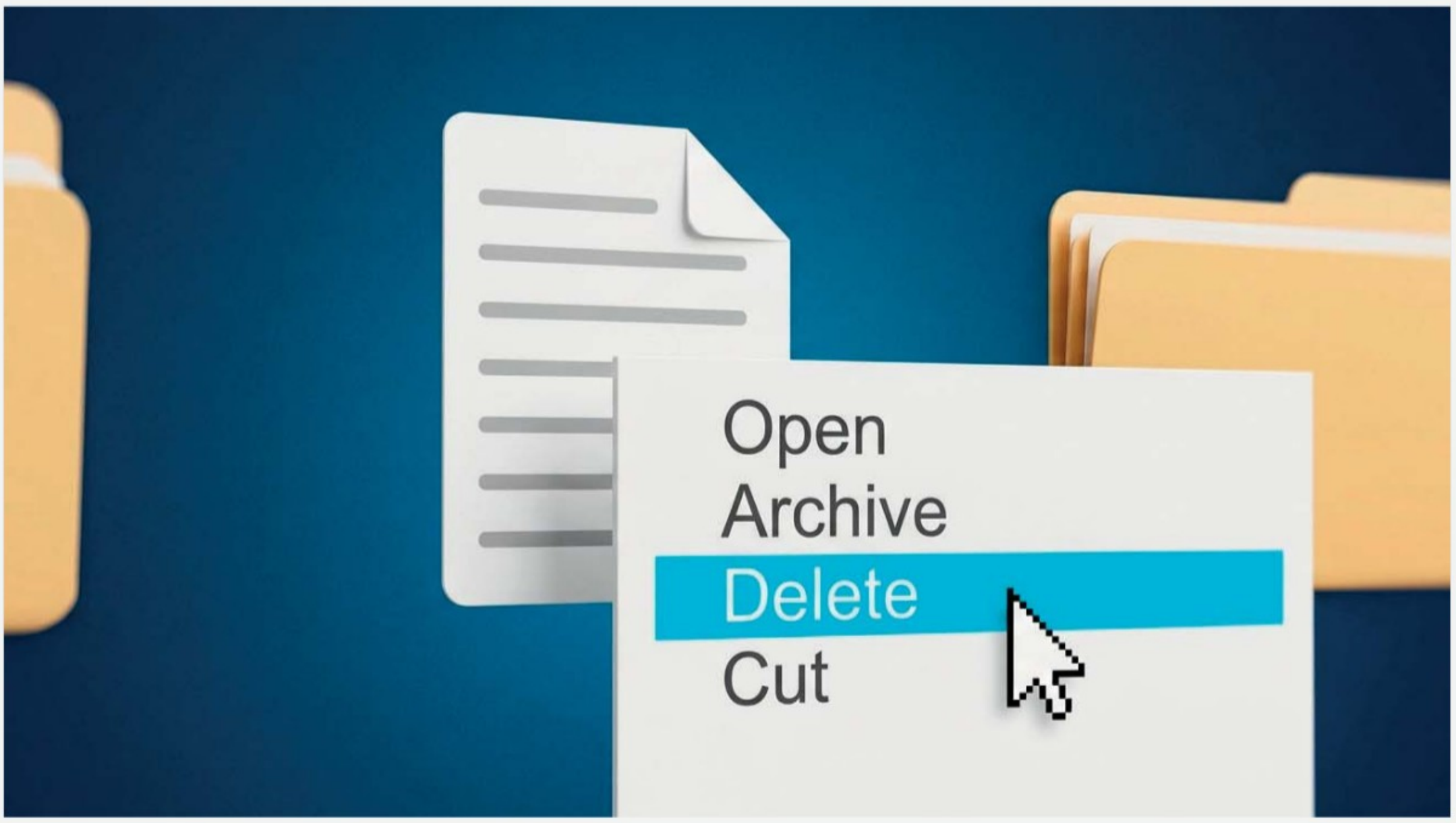
L'interface de Fooocus se veut volontairement minimaliste. Une fois ouverte dans le navigateur, vous pouvez vous concentrer sur le champ **Prompt**, dans lequel vous saisissez la description de l'image que vous souhaitez générer. Il n'est pas nécessaire de configurer manuellement une longue liste de paramètres : le programme a justement été conçu pour laisser à l'utilisateur la partie créative et prendre automatiquement en charge une grande partie des réglages techniques. Saisissez donc ce que vous souhaitez obtenir dans le champ prévu à cet effet et cliquez sur **Generate**. Après quelques instants, l'image générée apparaît directement dans l'interface. Le résultat est également enregistré automatiquement dans le dossier de sortie du programme, depuis lequel vous pouvez l'ouvrir, le copier ou l'utiliser dans d'autres projets.

## CRÉEZ L'IMAGE

Fooocus ne part pas nécessairement de zéro. En activant Input image, un panneau apparaît dans la partie inférieure de la fenêtre et vous permet de charger une image existante à utiliser comme référence. Plusieurs possibilités créatives s'offrent alors à vous. L'image peut être modifiée, améliorée ou agrandie, faisant de Fooocus un outil qui ne sert pas uniquement à créer de nouvelles images, mais aussi à intervenir sur celles que vous possédez déjà.




Vous pouvez ainsi partir d'une image présente sur votre ordinateur et l'utiliser comme base pour obtenir un nouveau résultat, tout en conservant la référence visuelle au cours du processus de génération. Parmi les fonctions disponibles figure **Inpainting**, qui permet d'intervenir sur une zone précise de l'image. Vous pouvez l'utiliser pour corriger un détail ou ajouter de nouveaux éléments dans une zone sélectionnée. **Outpainting** adopte quant à lui une approche différente : au lieu de modifier ce qui est déjà présent, il permet d'étendre l'image au-delà de ses bordures. Vous pouvez ainsi agrandir la scène vers la gauche, la droite, le haut ou le bas. Imaginez, par exemple, que votre image s'arrête trop près du sujet principal : grâce à l'outpainting, vous pouvez étendre la composition au-delà de ses limites d'origine, en laissant Fooocus générer la partie manquante.




# LE NETTOYEUR UNIVERSEL DU PC

**Avant de céder, vendre ou donner votre ordinateur, effacez les traces de navigation et empêchez la récupération des fichiers supprimés avec PrivaZer.**

Lorsque vous supprimez un fichier et videz la Corbeille, vous pensez qu'il a définitivement disparu ? Pas nécessairement. La simple suppression d'un document ne signifie pas que les données ont été immédiatement retirées du support. Des traces peuvent subsister dans les systèmes de gestion des fichiers et dans l'espace que le système d'exploitation considère comme libre. Il en va de même pour vos activités en ligne. Cookies, historiques, fichiers temporaires et autres informations peuvent laisser une quantité étonnante de traces sur le PC. Tant que l'ordinateur reste entre vos mains, ces informations peuvent sembler peu importantes. Mais que se passe-t-il lorsque vous décidez de le vendre ? C'est précisément dans ce contexte qu'intervient PrivaZer (**https://privazer.com/fr**), un logiciel gratuit dédié au nettoyage en profondeur du PC et à la protection de la vie privée. Le programme ne se contente pas de supprimer les fichiers temporaires classiques : il analyse également les traces résiduelles des activités et les espaces dans lesquels des informations relatives aux fichiers supprimés peuvent subsister.

## AVANT DE VOUS SÉPARER DU PC

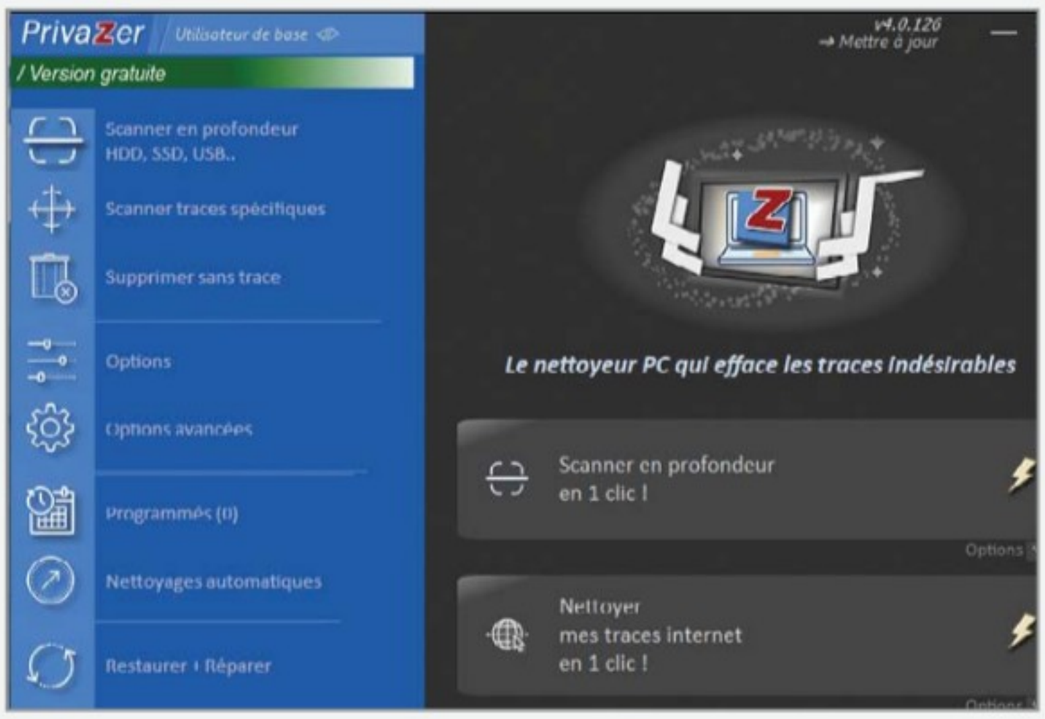
Imaginez que vous ayez supprimé des photos personnelles, des documents professionnels, des mots de passe enregistrés ou d'autres fichiers confidentiels. Même s'ils n'apparaissent plus dans les dossiers de



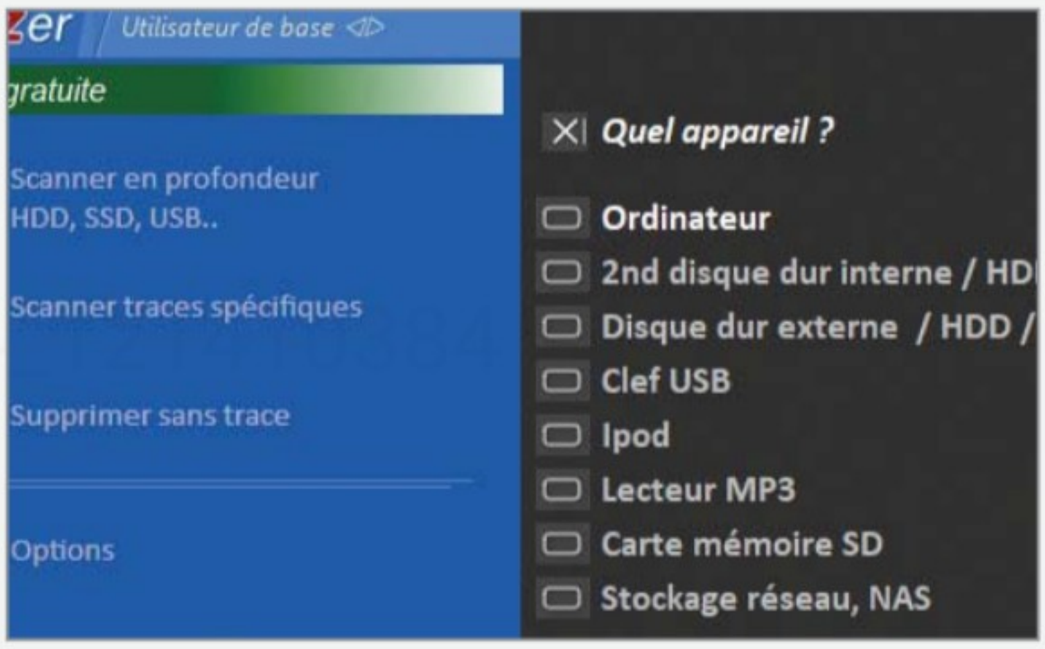

Windows, certaines informations peuvent rester présentes sur le système. PrivaZer peut analyser l'espace libre à la recherche de traces résiduelles et intervenir également sur les informations présentes dans les tables de fichiers. Le programme utilise en outre des techniques de réécriture et, selon son éditeur, adapte ses algorithmes au type de support, en distinguant par exemple les disques magnétiques des SSD.

## DÉNICHEZ LES TRACES CACHÉES

La première étape consiste à déterminer ce que votre PC a conservé de vos activités. PrivaZer est capable d'analyser le système et les périphériques de stockage à la recherche de traces qui ne sont normalement pas visibles lors de l'utilisation quotidienne.




Parmi les éléments pouvant être analysés figurent les activités de navigation, les cookies, les historiques, les fichiers temporaires, les listes de raccourcis (**Jump Lists**), les miniatures et les traces résiduelles des fichiers supprimés. Le programme permet également d'afficher ce qui est encore présent dans l'espace libre du disque. Cette fonction est particulièrement intéressante, car elle permet de voir ce qui reste normalement invisible. Un fichier peut avoir disparu de son dossier d'origine, mais certaines informations peuvent encore être présentes dans l'espace que le système considère comme libre. PrivaZer peut également intervenir sur les tables de fichiers, telles que FAT et MFT, dans lesquelles des informations relatives aux fichiers supprimés peuvent subsister.




Une fois les informations résiduelles identifiées, nous pouvons passer au nettoyage. PrivaZer propose un mode de nettoyage en profondeur qui intervient sur les traces des activités passées et sur l'espace libre. Pour la suppression sécurisée, le programme utilise des techniques de réécriture et, selon son éditeur, reconnaît automatiquement le type de support de stockage afin d'adapter la méthode utilisée. Le nettoyage peut également concerner les activités Internet : navigateurs, cookies, historiques et autres traces de navigation. Et il y a un détail particulièrement intéressant : le programme dispose également d'un Shredder permettant de supprimer définitivement des fichiers ou des répertoires que vous souhaitez éliminer sans laisser de traces récupérables.




INFORMATIQUE **HACK&CRACK**

# ABONNEZ-VOUS

## Confortablement chez vous !

1 AN - 4 NUMÉROS

à seulement

**16,90€** ~~22€~~

RÉDUCTION DE **23%**




Avec l'abonnement papier, la version numérique **EST GRATUITE !**

## 2 FAÇONS DE VOUS ABONNER

❶ Par virement, remplissez le bulletin ci-dessous et envoyez-le-nous ainsi que la preuve d'achat par:

WhatsApp
+39 329 3922420

E-mail
abonnements@sprea.fr

via Torino 51, 20063,
Cernusco S/N Milano, ITALIE

❷ Par carte bancaire, en flashant ce QR code **sprea.fr/hackecrack**
**Nous n'acceptons pas les règlements par chèque.**

# BULLETIN D'ABONNEMENT

☐ Oui, je m'abonne ou j'offre à **Hack&Crack** au **prix de 16,90€**

**J'indique ici mon adresse**

☐ Mme ☐ M. Nom :

Prénom :

Adresse :

Ville : Pays: Code Postal :

E-mail : N° Tél :

**J'indique ici l'adresse du bénéficiaire si j'offre l'abonnement**

☐ Mme ☐ M. Nom :

Prénom :

Adresse :

Ville : Pays: Code Postal :

E-mail : N° Tél :

☐ J'accepte de recevoir par mail des offres

**Virement bancaire** (merci de transmettre la preuve du virement) :
IBAN : IT40 H076 0101 6000 000 9154 0716
BIC/SWIFT BPPIITRRXXX
Motif : "Abonnement Hack&Crack"
Bénéficiaire : Sprea S.p.a. Via Torino 51 - 20063 Cernusco S/N

Date et signature obligatoires

**Contactez-nous via WhatsApp (messages uniquement) au +39 329 3922420 ou par e-mail à abonnements@sprea.fr**

CONFESSIONS D'UN HACKER

# J'AI CLONÉ UNE VOIX EN 5 MINUTES



Techniques et secrets expliqués pas à pas.

Il s'appelle Voicebox, et c'est un logiciel open source de clonage vocal qui nous a frappés pour une raison bien précise : il peut reproduire une voix avec une naturalité étonnante et, contrairement à de nombreux services en ligne, il fonctionne en local, directement sur l'ordinateur. Cela implique un avantage essentiel : un contrôle total sur les fichiers audio et aucune transmission vers des serveurs externes.

Un détail loin d'être insignifiant, surtout lorsqu'on manipule une technologie aussi puissante que sensible. D'ailleurs, ces dernières années, le clonage vocal a accompli un bond impressionnant : autrefois limité à des résultats métalliques, artificiels et facilement reconnaissables, il parvient aujourd'hui à générer des voix beaucoup plus crédibles, fluides et précises, grâce aux progrès de l'intelligence artificielle.

# Dossier



## LE CLONAGE VOCAL

Dans les pages qui suivent, nous analyserons **Volcebox** de près et découvrirons comment cet outil parvient à cloner une voix à partir d'un simple message vocal de quelques secondes envoyé via WhatsApp. Nous l'examinerons concrètement, étape par étape, afin de comprendre ce dont il est réellement capable, comment il s'installe et comment il s'utilise sur un PC.

C'est précisément à ce stade que le sujet devient passionnant, car nous verrons comment une voix peut devenir l'un des éléments les plus fragiles et immédiats pour tromper quelqu'un. Une reproduction fidèle peut se transformer à la fois en outil créatif et en moyen d'usage détourné.

Nous entrerons dans l'univers du voice cloning, qui a récemment attiré l'attention bien au-delà du domaine technologique, notamment en raison de son utilisation dans les arnaques, les usurpations d'identité et les tentatives de manipulation de plus en plus crédibles.

Comprendre le fonctionnement de cette technologie, aujourd'hui, signifie aussi connaître et anticiper les nouveaux risques liés à l'IA.



## MATÉRIEL NÉCESSAIRE

**VOICEBOX 0.5.0**
Outil de clonage vocal open source avec prise en charge de plusieurs moteurs TTS

**Site Internet :**
https://short.tips/url/voiceclone

**Coût :** Gratuit

Le hacker qui a partagé ces informations nous a également confié : « Le véritable défi n'est pas de générer une voix synthétique, mais de faire en sorte qu'elle sonne crédible, naturelle et cohérente avec l'émotion que nous voulons transmettre ».

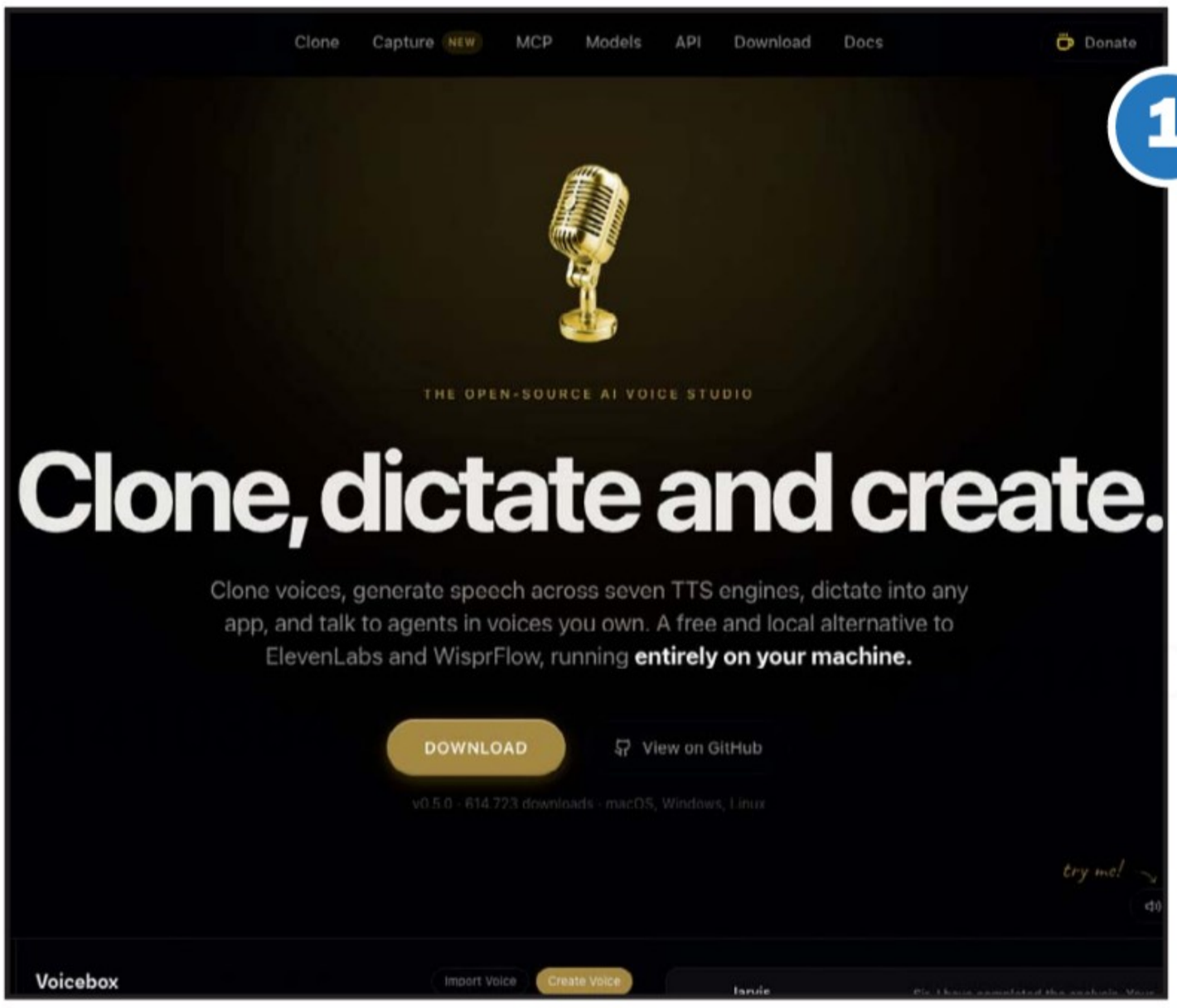
## ATTENTION À LA « BONNE » VOIX !

**Au fil des années, les arnaques numériques ont changé de visage : autrefois limitées à des messages alarmants, elles ont ensuite laissé place à des images falsifiées générées par l'IA, et aujourd'hui à des voix synthétiques créées sur mesure.**
**Quelques exemples ? Aux États-Unis, il y a quelques années, une mère de l'Arizona a reçu un appel dans lequel elle entendait la voix de sa fille demander de l'aide pendant un faux enlèvement : il s'agissait d'un clonage vocal utilisé pour tenter une extorsion. Un cas similaire a impliqué le père d'un candidat politique en Floride.**
**Et en 2019, le PDG d'une société énergétique britannique a autorisé un virement de 243 000 dollars, convaincu de parler avec son supérieur.**

Dossier

# PREMIÈRE OPÉRATION : INSTALLER VOICEBOX

**Voici comment obtenir en local le logiciel gratuit et performant utilisé pour cloner des voix.**

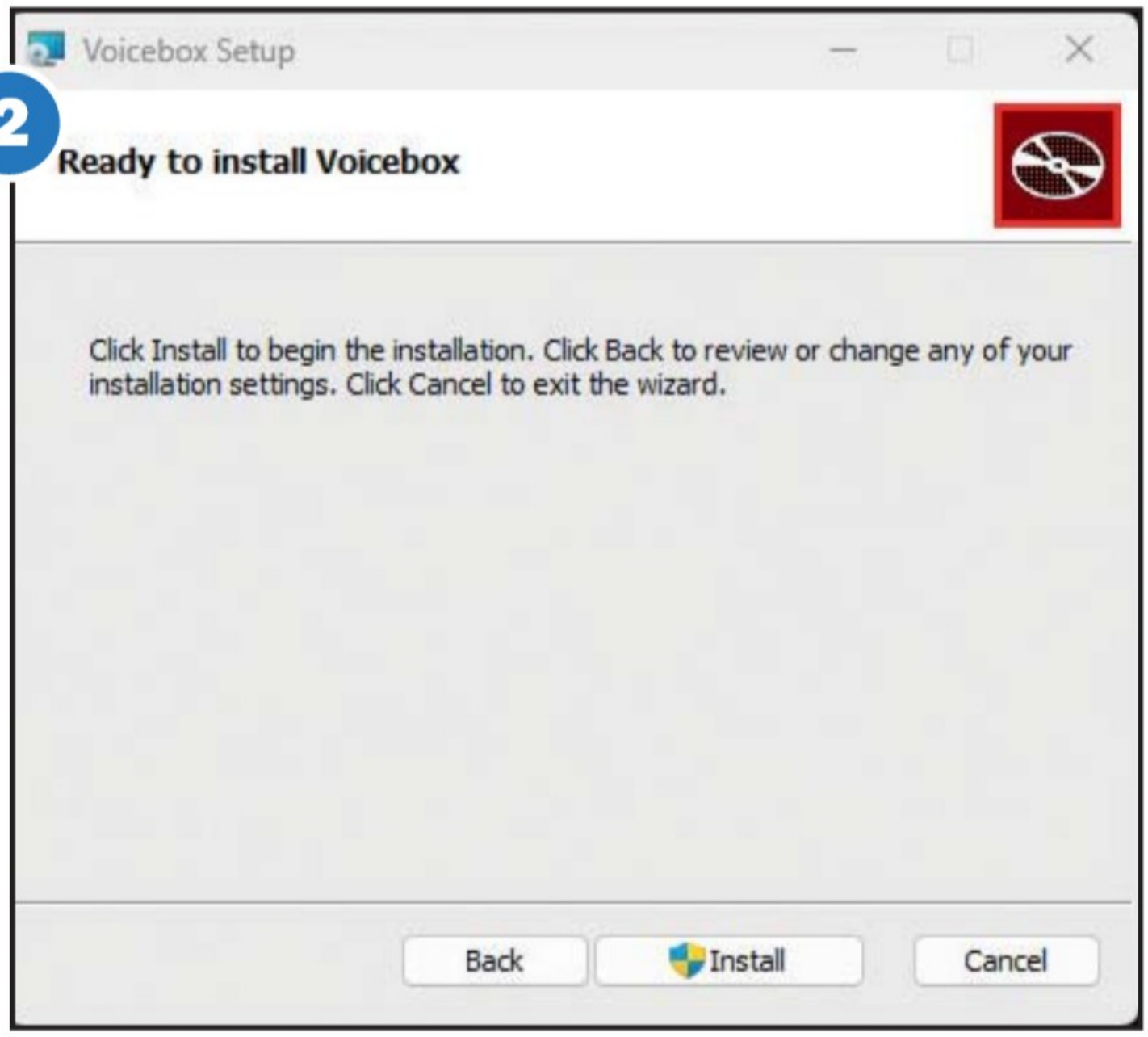



1

## TÉLÉCHARGEMENT DE VOICEBOX

Ouvrez votre navigateur web et rendez-vous sur https://voicebox.sh/. Cliquez sur **Download** pour être redirigé vers une nouvelle page où choisir le système d'exploitation pour lequel télécharger le logiciel. Le téléchargement démarre automatiquement pour le système détecté.

2




## INSTALLATION SOUS WINDOWS OU MACOS

Lancez le fichier téléchargé (sous Windows, il faudra forcer **Defender** en sélectionnant **Exécuter quand même**). Dans le cas d'une installation sous Linux, il sera nécessaire de procéder à la compilation depuis les sources, comme indiqué dans l'étape suivante.

```
  Downloading sqlalchemy-2.0.49-cp313-cp313-manylinux2014_aarch64.manylinu
kB)
Collecting alembic>=1.13.0 (from -r backend/requirements.txt (line 8))
  Downloading alembic-1.18.4-py3-none-any.whl.metadata (7.2 kB)
Collecting torch>=2.2.0 (from -r backend/requirements.txt (line 11))
  Downloading torch-2.11.0-cp313-cp313-manylinux_2_28_aarch64.whl.metadata
Collecting transformers<=4.57.6,>=4.36.0 (from -r backend/requirements.txt
  Downloading transformers-4.57.6-py3-none-any.whl.metadata (43 kB)
Collecting accelerate>=0.26.0 (from -r backend/requirements.txt (line 13))
  Downloading accelerate-1.13.0-py3-none-any.whl.metadata (19 kB)
Collecting huggingface_hub>=0.20.0 (from -r backend/requirements.txt (line
  Downloading huggingface_hub-1.13.0-py3-none-any.whl.metadata (14 kB)
Collecting qwen-tts>=0.0.5 (from -r backend/requirements.txt (line 15))
  Downloading qwen_tts-0.1.1-py3-none-any.whl.metadata (61 kB)
Collecting conformer>=0.3.2 (from -r backend/requirements.txt (line 27))
  Downloading conformer-0.3.2-py3-none-any.whl.metadata (631 bytes)
Collecting diffusers>=0.29.0 (from -r backend/requirements.txt (line 28))
  Downloading diffusers-0.38.0-py3-none-any.whl.metadata (20 kB)
Collecting omegaconf (from -r backend/requirements.txt (line 29))
  Downloading omegaconf-2.3.0-py3-none-any.whl.metadata (3.9 kB)
Collecting pykakasi (from -r backend/requirements.txt (line 30))
  Downloading pykakasi-2.3.0-py3-none-any.whl.metadata (5.9 kB)
Collecting resemble-perth>=1.0.1 (from -r backend/requirements.txt (line 3
  Downloading resemble_perth-1.0.1-py3-none-any.whl.metadata (4.8 kB)
Collecting s3tokenizer (from -r backend/requirements.txt (line 32))
  Downloading s3tokenizer-0.3.0-py3-none-any.whl.metadata (7.2 kB)
Collecting spacy-pkuseg (from -r backend/requirements.txt (line 33))
  Downloading spacy_pkuseg-1.0.1-cp313-cp313-manylinux_2_17_aarch64.manyli
Collecting pyloudnorm (from -r backend/requirements.txt (line 34))
  Downloading pyloudnorm-0.2.0-py3-none-any.whl.metadata (6.6 kB)
Collecting torchaudio (from -r backend/requirements.txt (line 41))
```

3

## INSTALLATION POUR LINUX

Sous Linux, ouvrez le **Terminal** et exécutez : **git clone** https://github.com/jamiepine/voicebox.git. Une fois terminé, saisissez cd **voicebox**, puis **just setup** et enfin **just build**. La procédure complète est décrite ici : https://voicebox.sh/linux-install.

## PREMIER LANCEMENT DE L'OUTIL

4

Au premier démarrage, l'outil procède à la configuration de certains paramètres : réglages vocaux, synthétiseur, échantillons de voix, etc. La procédure dure quelques secondes, après quoi le tableau de bord s'affiche, avec à gauche le menu permettant d'accéder aux différentes fonctionnalités.

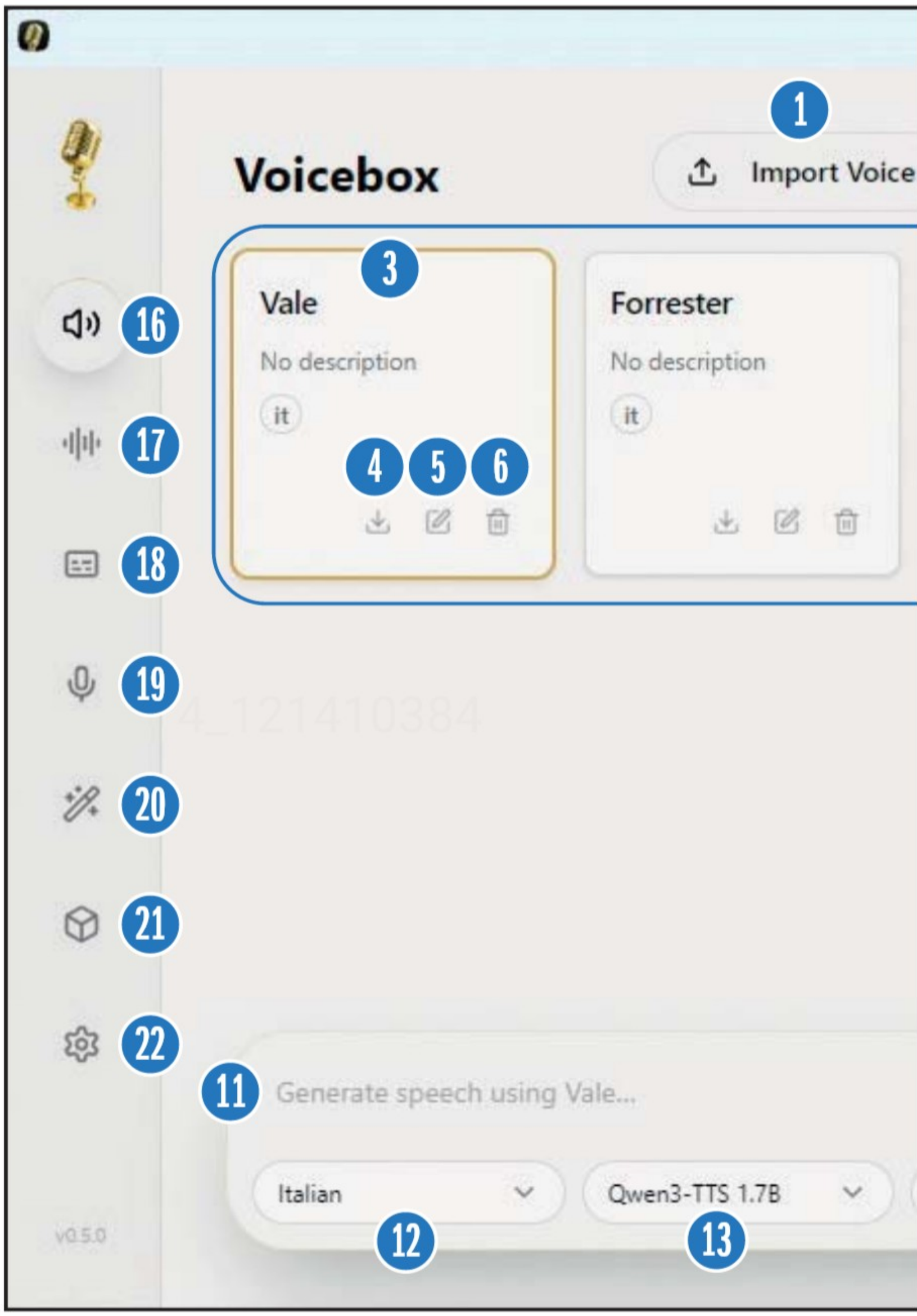



## PAS SEULEMENT VOICEBOX

Si vous souhaitez explorer d'autres outils de clonage vocal, le panorama offre des solutions tout aussi intéressantes. **ElevenLabs** (https://short.tips/url/elevenlabs), par exemple, mise sur la qualité expressive et la naturalité du discours, avec des voix qui semblent sortir d'un studio d'enregistrement. **RVC** (https://short.tips/url/rvc), très apprécié par la communauté open source, permet de transformer une voix en une autre en temps réel, idéal pour le streaming et les contenus musicaux. Pour ceux qui préfèrent une approche plus technique, **Coqui TTS** (https://coquitts.com/) propose des modèles avancés et une grande liberté de personnalisation.

Dossier

# LE TABLEAU DE BORD DE




**1. IMPORT VOICE**
Importe un profil vocal précédemment créé ou sauvegardé.

**2. CREATE VOICE**
Crée un nouveau profil vocal à partir d'un échantillon audio.

**3. PROFIL VOCAL**
Sélectionne une voix à utiliser pour la génération audio.

**4. TÉLÉCHARGER**
Télécharge le profil vocal sélectionné pour en conserver une copie.

**5. MODIFIER**
Modifie les paramètres et les informations du profil vocal.

**6. SUPPRIMER**
Supprime le profil vocal sélectionné.

**7. GÉNÉRATIONS**
Affiche la liste des audios générés avec Voicebox.

**8. LIRE**
Lit l'audio généré pour en écouter le résultat.

**9. FAVORIS**
Ajoute ou retire la génération de la liste des favoris.

**10. AUTRES OPTIONS**
Ouvre le menu des opérations supplémentaires disponibles pour la génération.

**11. TEXTE À CONVERTIR**
Saisit le texte que Voicebox doit transformer en parole.

**12. LANGUE**
Sélectionne la langue utilisée pour la génération vocale.

**13. MODÈLE VOCAL**
Sélectionne le modèle TTS utilisé pour générer l'audio.

**14. EFFETS**
Sélectionne les effets audio à appliquer à la voix générée.

**15. GÉNÉRER**
Lance la conversion du texte en parole en utilisant le profil, la langue et le modèle sélectionnés.

**16. GENERATE**
Ouvre la section dédiée à la synthèse vocale et à l'historique des audios produits.

**17. STORIES**
Permet de créer des contenus narratifs avec plusieurs voix organisées sur une timeline.

# VOICEBOX




**18. CAPTURES**
Gère les enregistrements et les prises de son utilisées par Voicebox.

**19. VOICES**
Gère les profils vocaux disponibles, y compris ceux créés par clonage.

**20. EFFETS**
Permet de configurer et d'appliquer des effets à la voix, comme réverbération, delay et compression.

**21. MODELS**
Gère les modèles IA utilisés pour la synthèse et la transcription vocale.

**22. SETTINGS**
Accède aux réglages généraux et à la configuration de Voicebox.

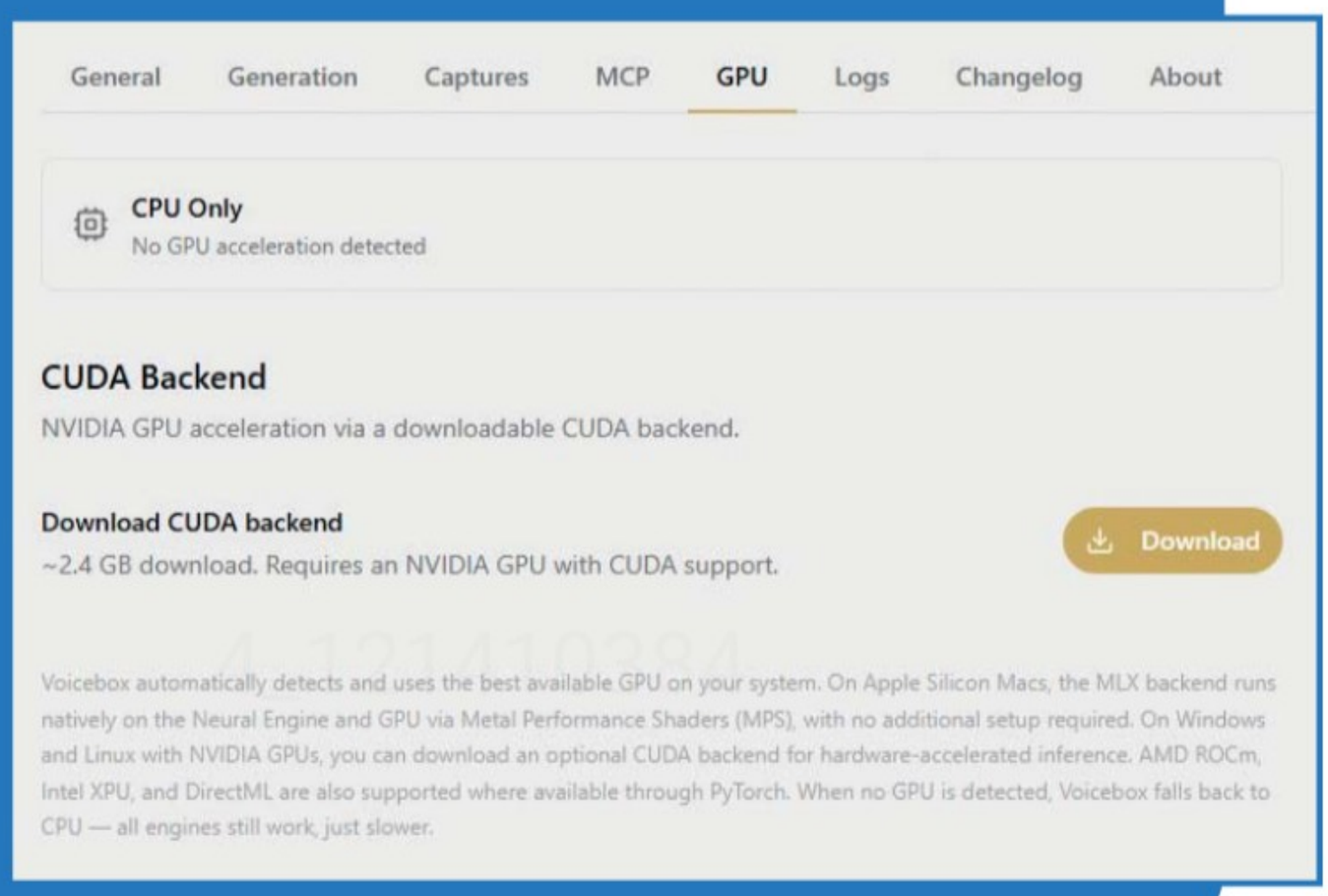
# POUR PARTIR DU BON PIED

Avec une configuration correcte et quelques précautions, le clonage vocal sera nettement plus efficace.

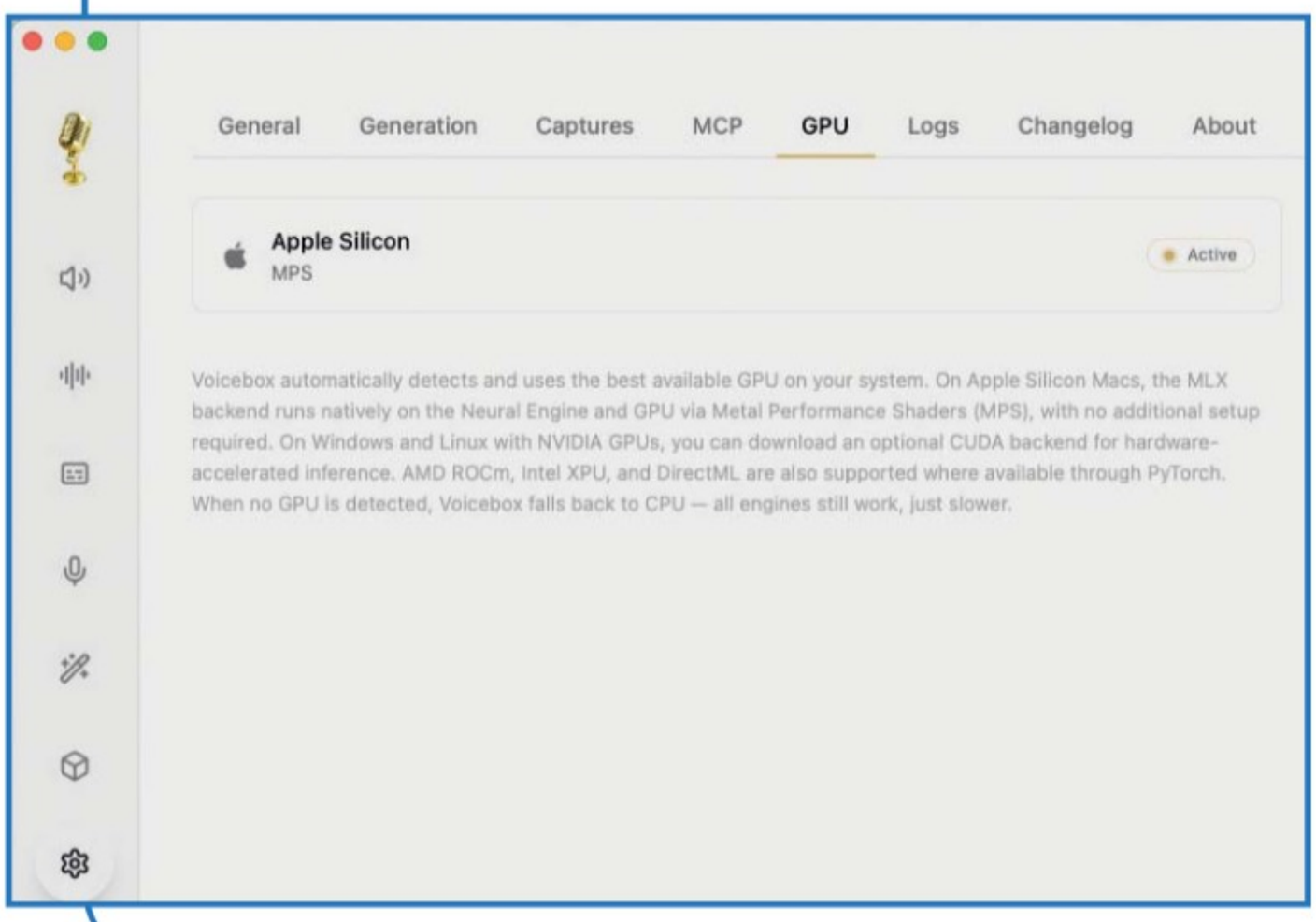
## CHOISIR UNE CARTE GRAPHIQUE DÉDIÉE



Voicebox fonctionne également avec le seul processeur, mais un GPU améliore nettement les performances. Sous Windows et Linux, ouvrez **Settings**, rendez-vous dans l'onglet GPU et, si disponible, téléchargez **CUDA** (**https://developer.nvidia.com/cuda/toolkit**) pour accélérer la génération. **AMD ROCm**, **Intel XPU** et **DirectML** via **PyTorch** sont également pris en charge.




## SUR APPLE, UTILISER UNE PUCE APPLE SILICON






Sur les Mac équipés d'**Apple Silicon**, le backend **MLX** exploite nativement le **Neural Engine** et le GPU via **Metal**, sans configuration supplémentaire. Sous Windows, pour obtenir des performances similaires, une carte **NVIDIA RTX** est recommandée : même un modèle d'entrée de gamme permet de faire tourner l'application correctement.

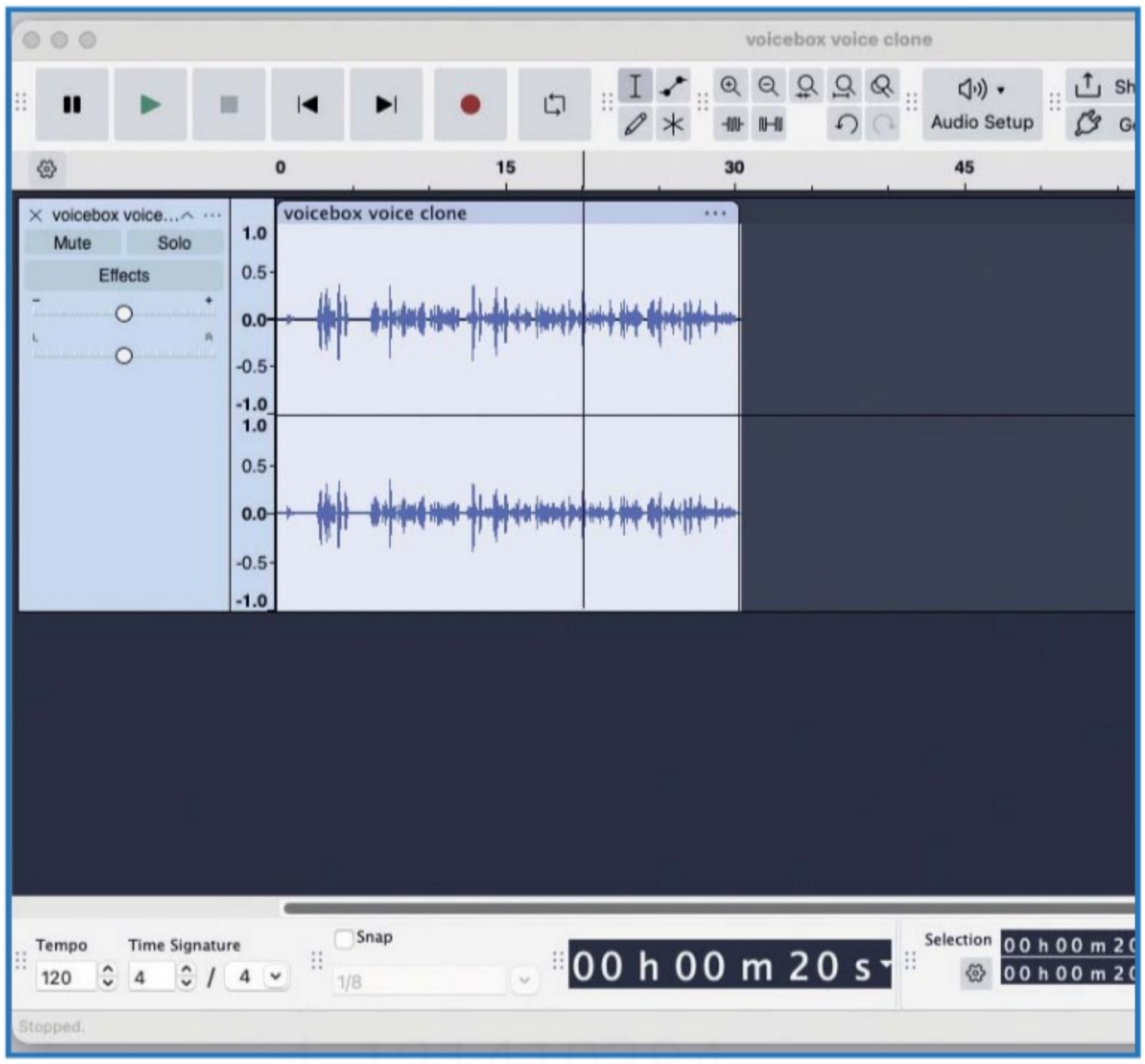
# UTILISER UN ÉCHANTILLON WAV



Si vous importez un échantillon audio, la qualité finale dépend fortement du fichier utilisé.

L'échantillon doit durer moins de 30 secondes, être au format WAV mono 16 bits et, si possible, contenir une voix expressive et propre.

Pour préparer le fichier, vous pouvez également utiliser **Audacity** (**https://www.audacityteam.org/**).

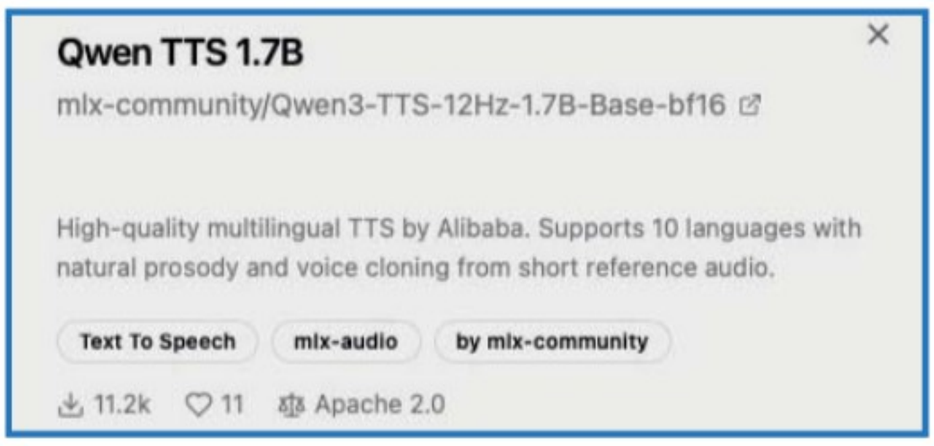



# ACCORDER LES AUTORISATIONS



Au premier lancement, **Voicebox** demande l'accès au microphone pour enregistrer de l'audio directement depuis l'application. Nous vous conseillons d'autoriser immédiatement cet accès : lors de nos tests, après un refus initial, il s'est révélé assez compliqué de faire réapparaître la fenêtre de consentement.




# TÉLÉCHARGER DES MODÈLES

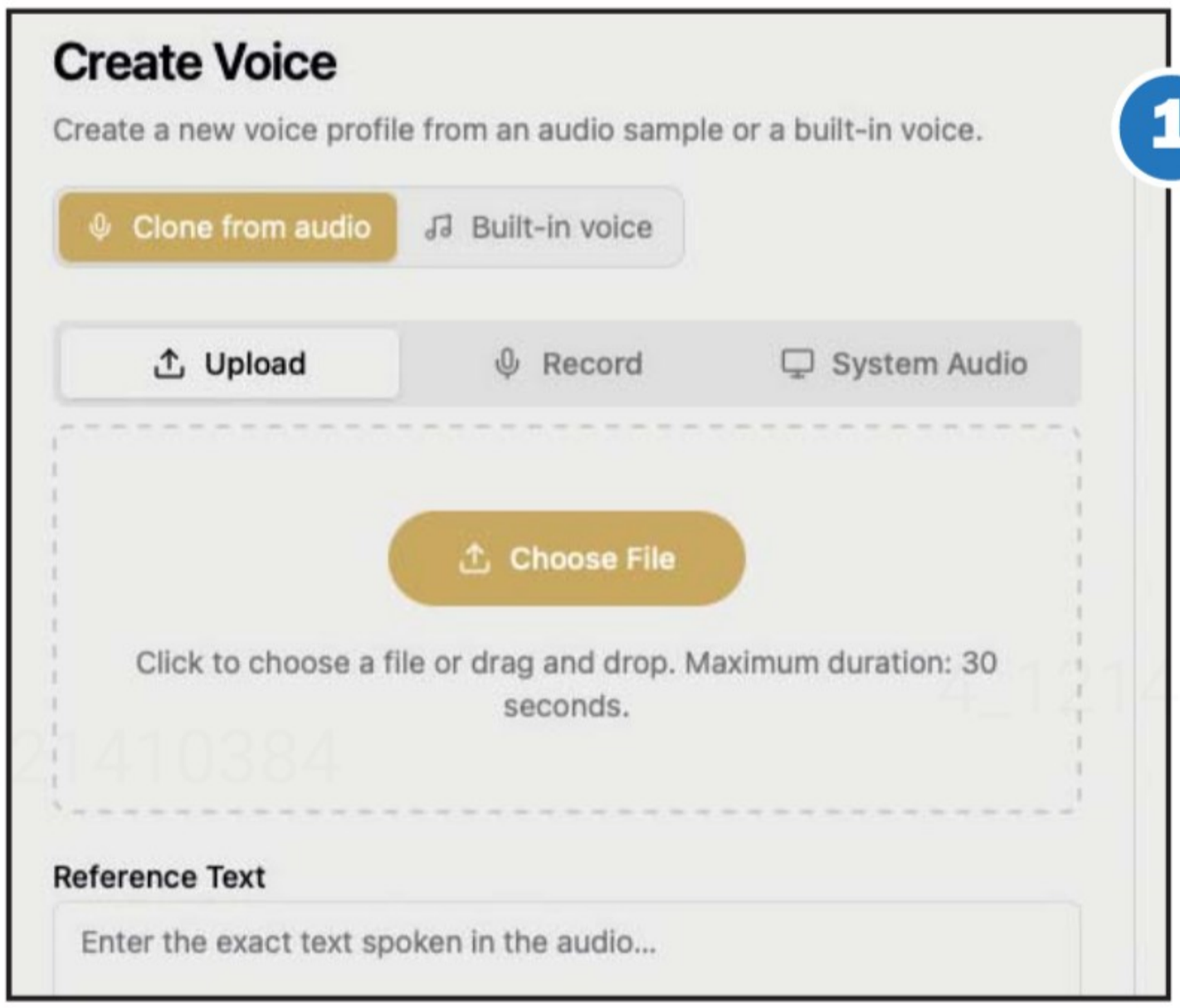


Après le démarrage, téléchargez les modèles d'IA en cliquant sur l'icône en forme de cube dans le menu latéral. Pour **Voice generation**, nous recommandons **Qwen TTS 0.6B** sur les PC moins puissants ; pour **Transcription**, vérifiez la présence de **Whisper** ; et dans **Language Models**, téléchargez **Qwen3 17B**.

Dossier

# VOTRE PREMIÈRE VOIX CLONÉE AVEC VOICEBOX

De la préparation de l'échantillon audio à la génération du discours avec la voix produite par l'IA.

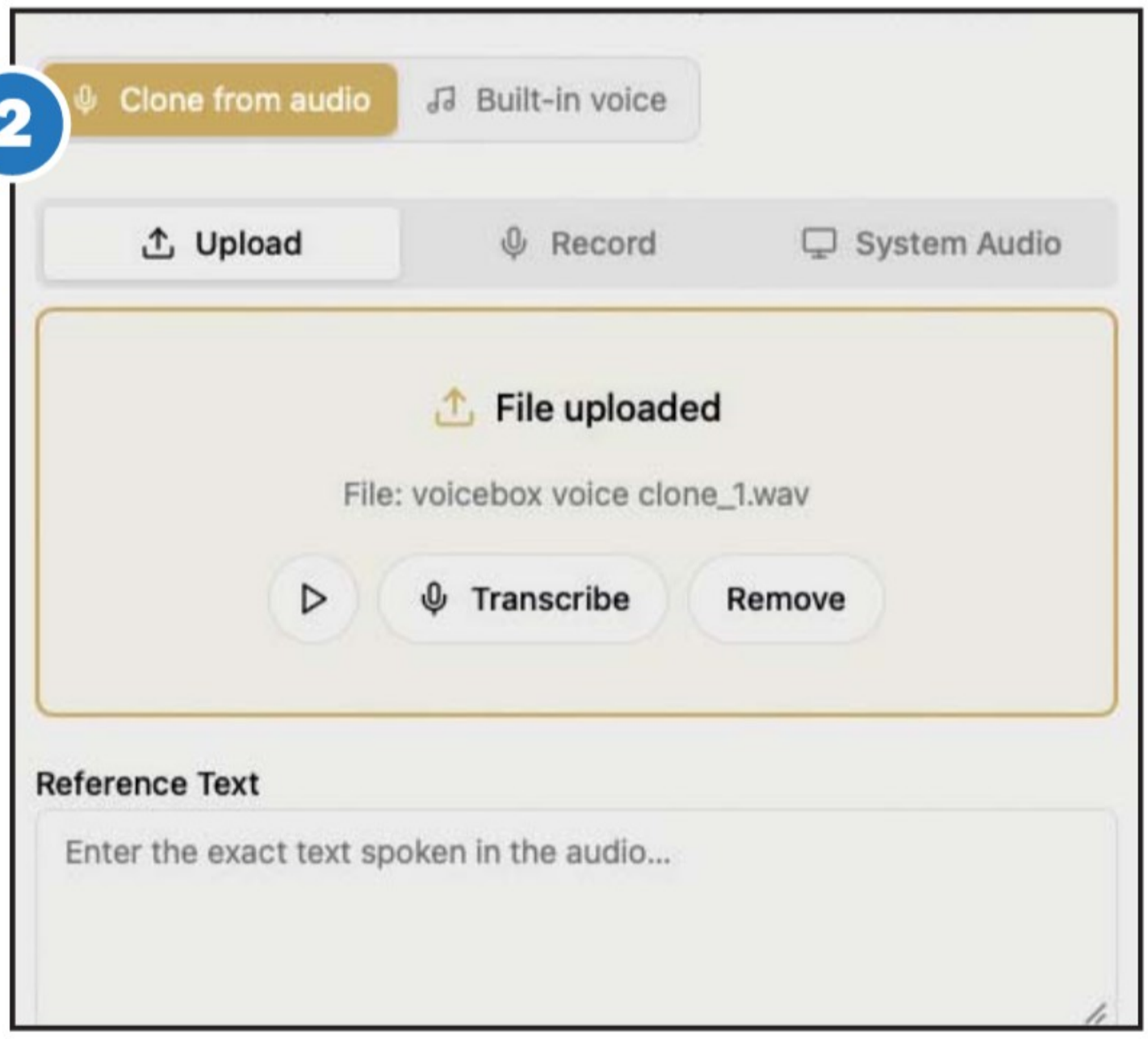


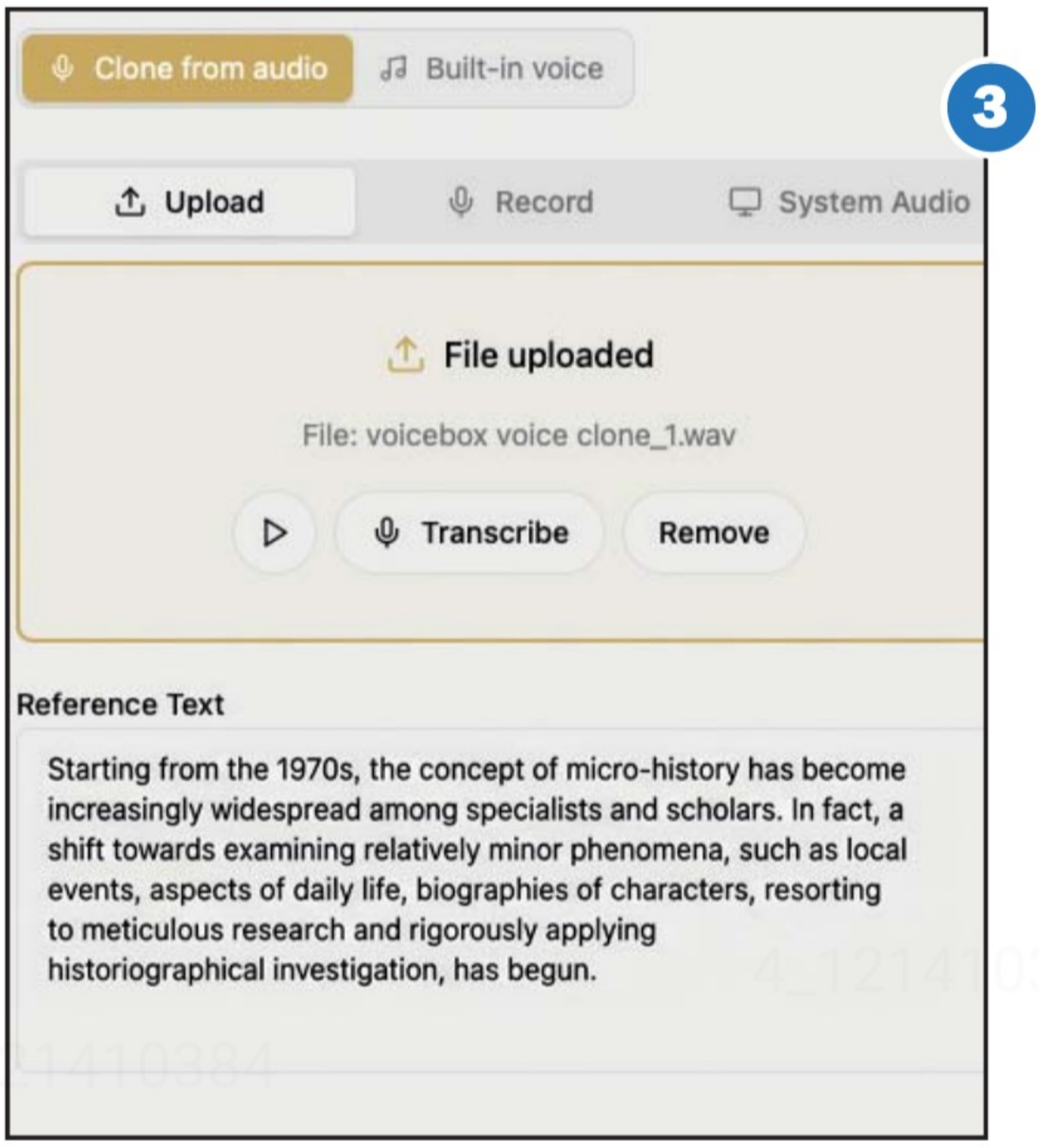

## CRÉER UNE NOUVELLE VOIX

Pour cloner une nouvelle voix, cliquez sur le bouton **Create Voice**. Dans la nouvelle fenêtre, vous pouvez choisir de charger la voix à cloner depuis un fichier présent sur le PC (**Upload**), d'enregistrer directement via le microphone (**Record**) ou de capturer l'audio du système (**System**).

## DEPUIS WHATSAPP

Sélectionnez **Language** et choisissez la langue. Nous avons utilisé un fichier audio présent sur le PC, en l'occurrence un message vocal WhatsApp. Le fichier **.ogg** a été converti en **.wav** grâce à un service en ligne comme www.freeconvert.com. Cliquez ensuite sur **Upload** et sélectionnez le fichier. Enfin, cliquez sur **Transcribe**.



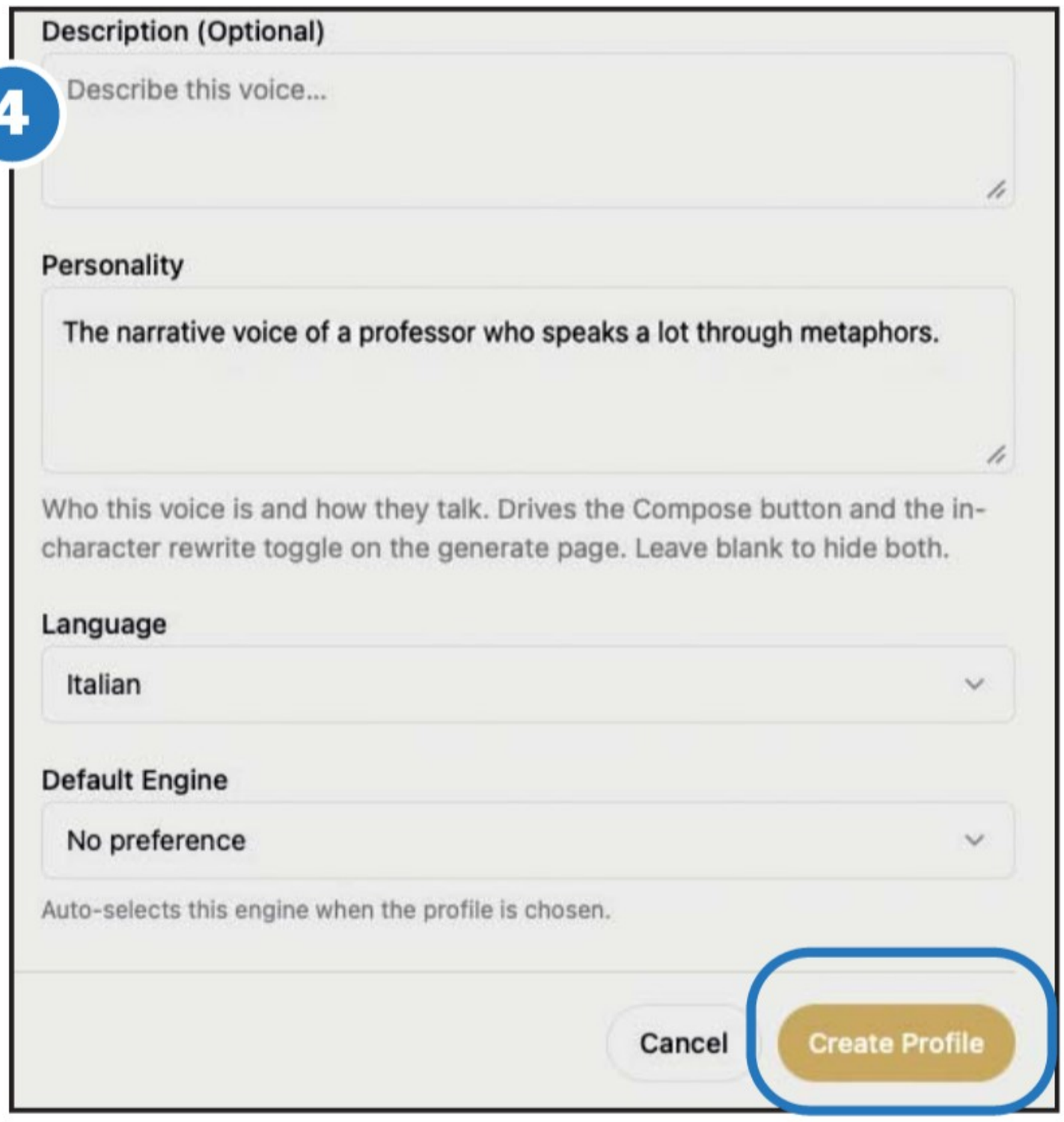


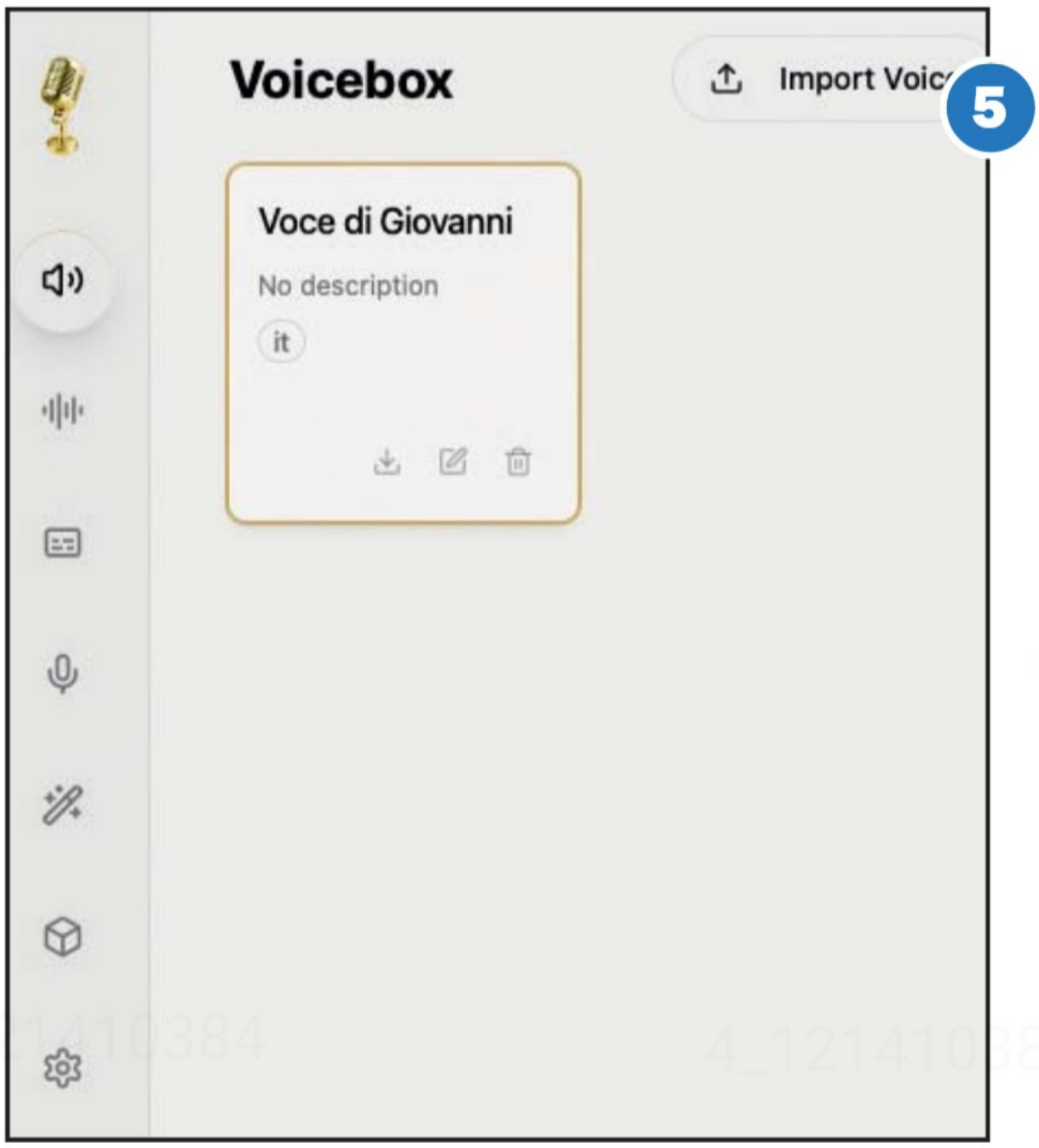

## DÉTAILS SUPPLÉMENTAIRES

Après quelques secondes de traitement, le système affichera dans la section **Referenced text** la transcription du contenu audio. Dans la partie droite de l'interface, vous pouvez associer un nom à la voix dans le champ **Name**, et une description plus détaillée dans **Description**.

## LANCER LE CLONAGE VOCAL

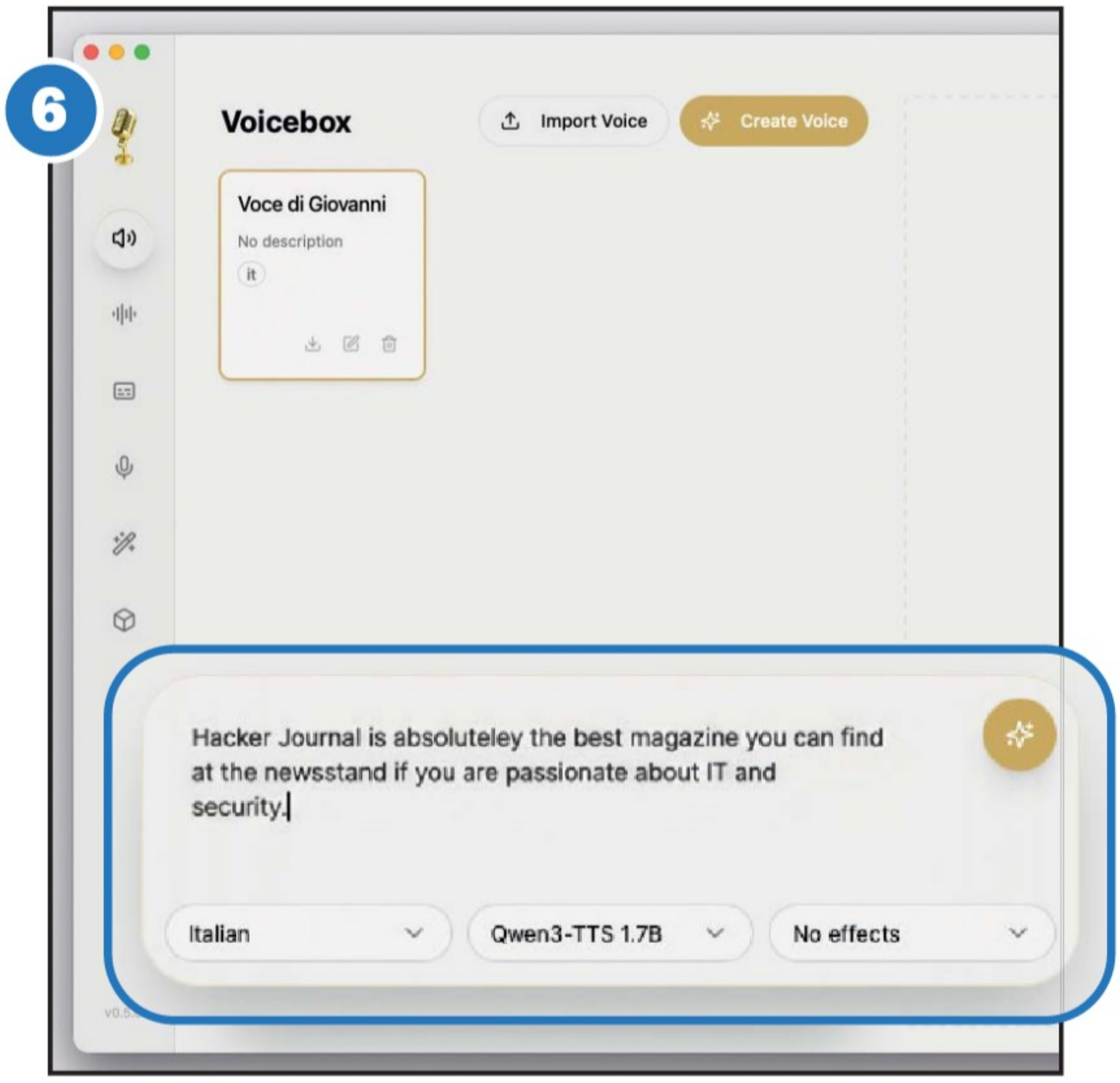
Dans la section **Personality**, vous pouvez éventuellement fournir à **Voicebox** des indications textuelles sur la voix, par exemple : « **Voix narrative d'un professeur qui parle souvent par métaphores** ». Cliquez sur **Create profile** pour lancer le clonage.






## CLONAGE VOCAL TERMINÉ

Le bouton **Create Profile** sera remplacé par la mention **Saving et**, après quelques minutes de traitement (durée variable selon les capacités du système), **Voicebox** reviendra à l'écran initial avec un encadré contenant les détails de la voix clonée.




## L'ÉPREUVE DU FEU

Sélectionnez la voix et, dans la section inférieure (**Generate speech using...**), saisissez le texte à prononcer avec la voix clonée. Cliquez sur **Generate Speech**. Une nouvelle zone en haut à droite indiquera l'état du traitement en cours. Quelques minutes plus tard, le résultat sera prêt.

## Comment la **ponctuation** transforme la voix synthétique

| | |
|---|---|
| **Texte neutre** | « La voix synthètique lit la phrase **de *manière linéaire.*** »  |
| **Ponctuation expressive** | « La voix synthètique lit la phrase… **d'une *autre manière !*** »  |
| **Mise en emphase** | « La voix synthètique peut lire une phrase ***lentement*** ou ***AVEC FORCE.*** »  |

**?!** Intonation — **—** Pause brève • • • Hésitation

***MAJUSCULES*** **italique** *****gras***** *Emphase*

## POUR UNE VOIX PLUS NATURELLE …

Pour obtenir une synthèse vocale plus naturelle dans **Voicebox**, il ne suffit pas d'écrire le texte : il est essentiel de guider la lecture avec la ponctuation et quelques astuces stylistiques.

La ponctuation est le premier outil. Le système interprète généralement les signes courants comme le point d'interrogation ou d'exclamation, qui apportent intonation et rythme à la phrase.

Les tirets (–) sont très utiles : ils introduisent de courtes pauses et rendent le discours plus cadencé, presque comme si l'orateur réfléchissait.

Les points de suspension (…) peuvent suggérer une hésitation ou une phrase laissée en suspens, même si tous les modèles ne les interprètent pas de manière cohérente. Certains, comme **Chatterbox**, ont tendance à les ignorer ou à ne pas les valoriser pleinement.

Un autre aspect important concerne la manière d'indiquer au modèle quels mots mettre en avant. Écrire un mot en **MAJUSCULE** peut suggérer un ton plus fort.

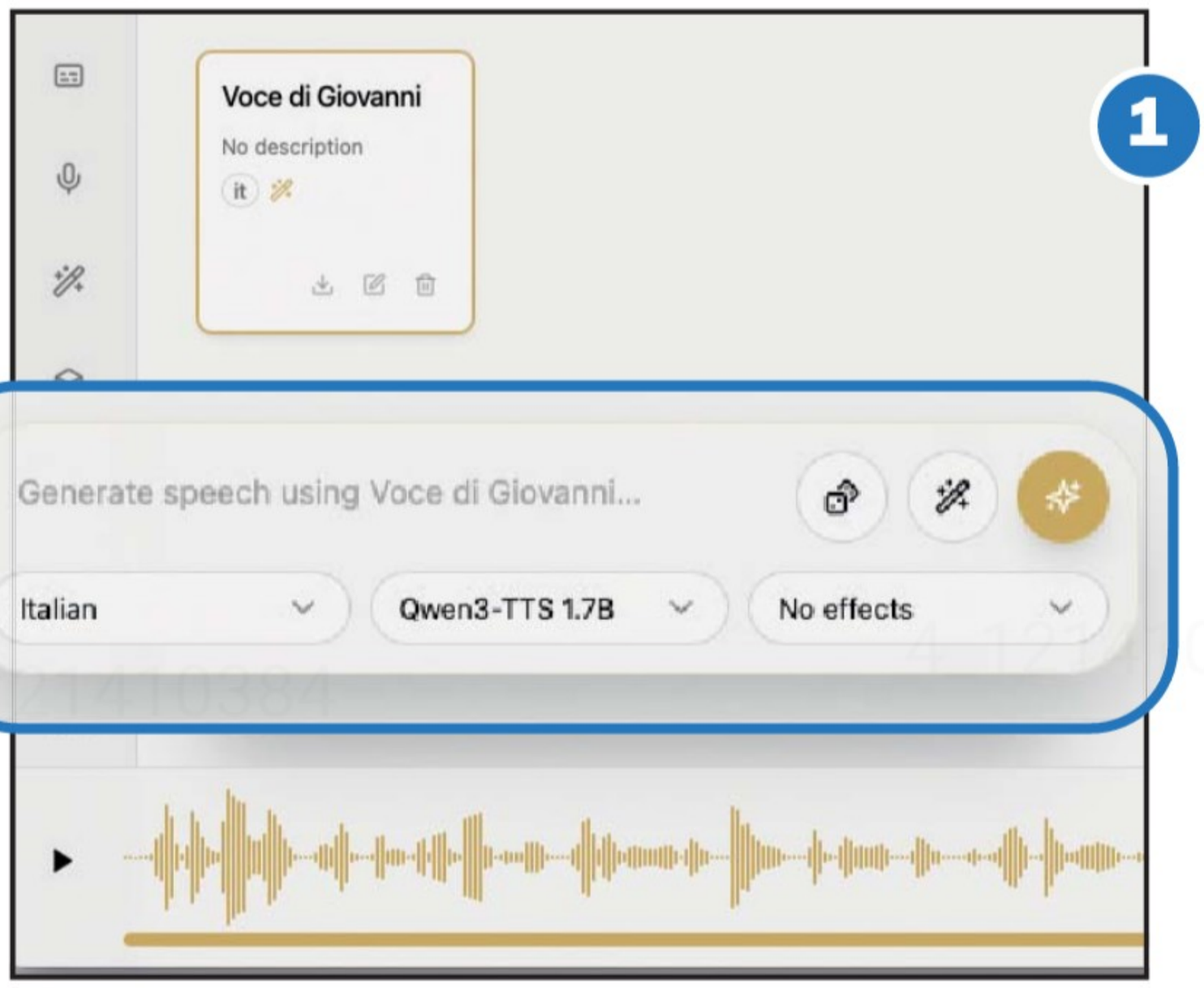
L'*italique* (avec un astérisque *mot*) indique une emphase légère, tandis que le **gras** (**mot**) communique une emphase marquée.

Il faut toutefois savoir que ces techniques sont encore en phase d'affinement : elles ne sont pas toujours interprétées parfaitement et peuvent parfois produire des résultats peu naturels.

Dossier

# EXPORTER ET PARTAGER LA VOIX CLONÉE

Gestion, écoute et exportation de la voix clonée avec application d'effets audio.

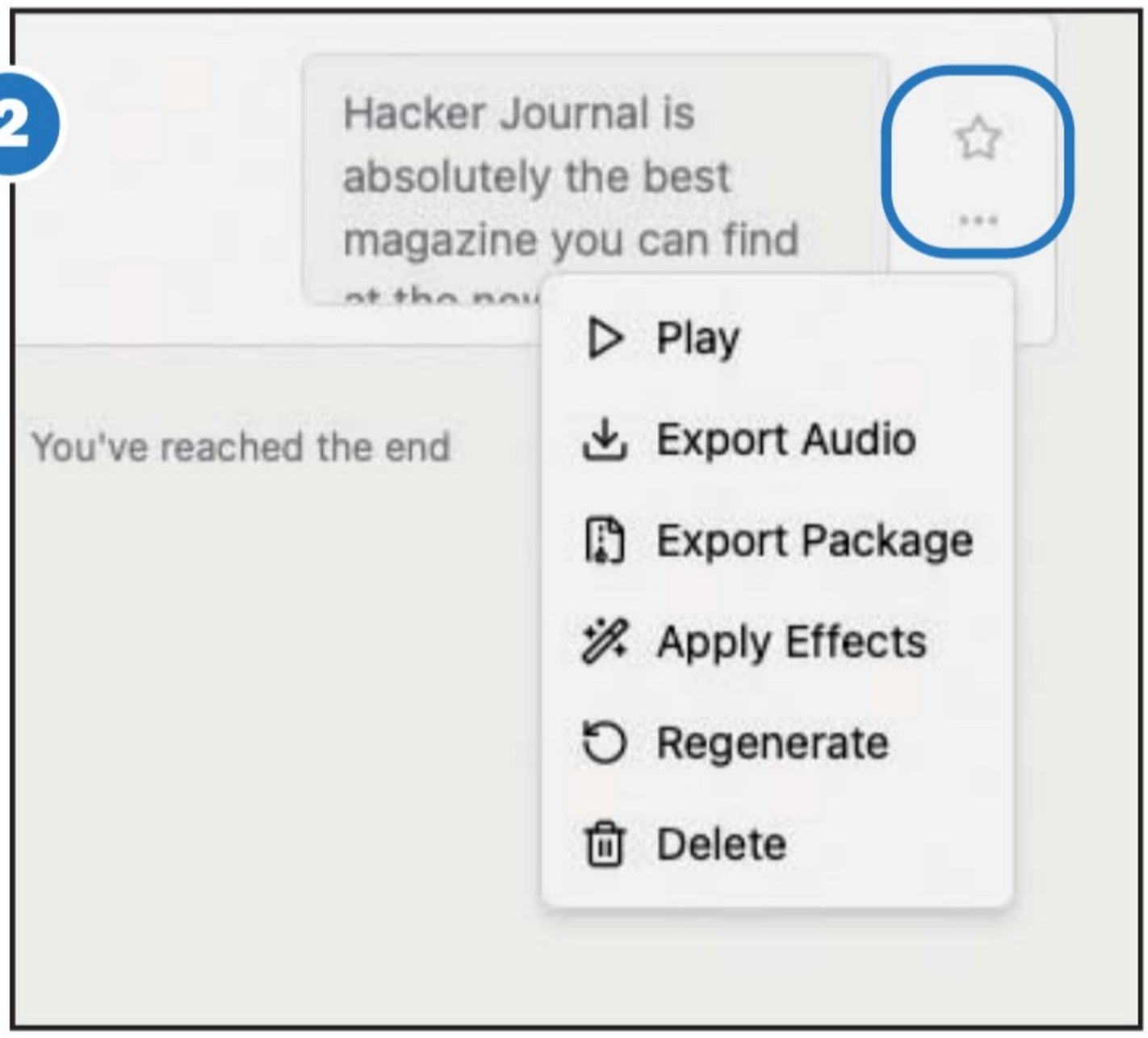


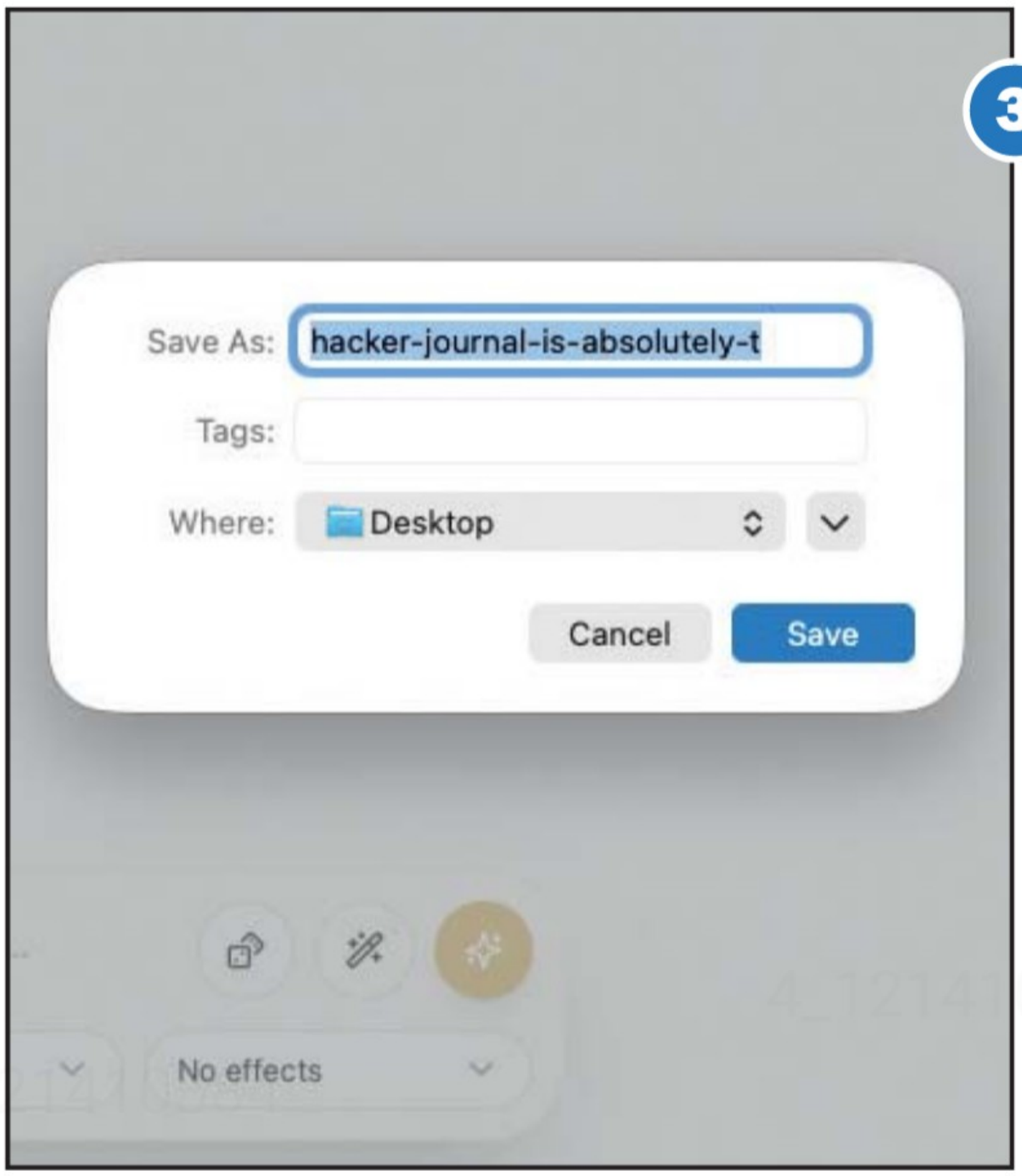

## ÉCOUTER LA VOIX CLONÉE

Une fois le traitement terminé, une sorte de timeline apparaît avec, à côté, le bouton **Play.** La lecture peut également être lancée en cliquant sur le cadre en haut à droite (bouton **8 LIRE**), où sont affichés la durée de l'audio généré, le modèle utilisé et la date de génération.

## OPÉRATIONS DISPONIBLES

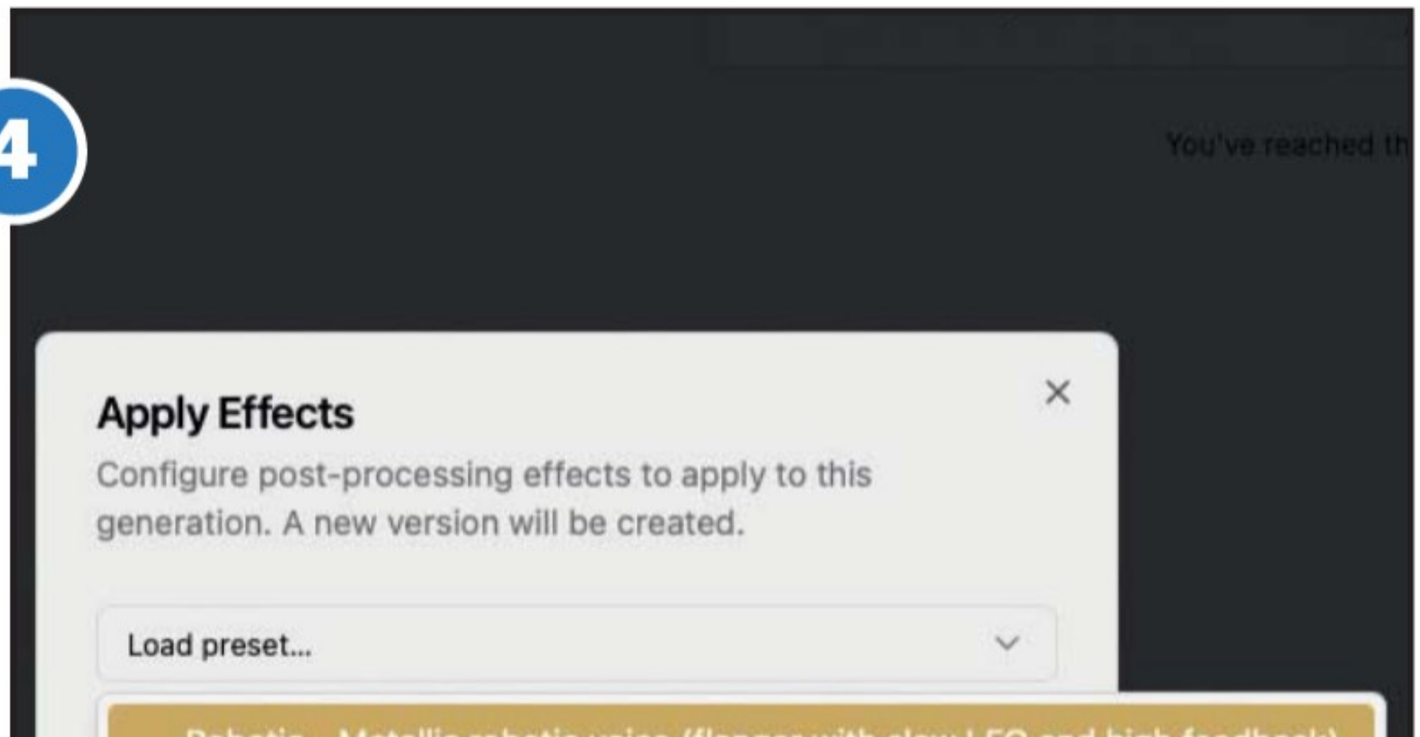
Toujours dans le cadre supérieur, en cliquant sur les trois points (**...**) sous l'icône en forme d'étoile — utilisée pour ajouter la génération aux favoris — vous accédez à un menu contextuel permettant d'effectuer différentes opérations sur le fichier généré : l'exporter, appliquer des effets, le supprimer, etc.






## EXPORTER LE FICHIER PRODUIT

En cliquant sur **Export Audio**, vous pouvez sauvegarder le fichier au format **.wav** (que rien n'empêche ensuite de reconvertir en **.ogg**...). **Export Package**, en revanche, permet de générer un fichier **.zip** contenant l'audio et un fichier JSON (**manifest.json**) avec des informations telles que la durée, le texte et la voix de référence.

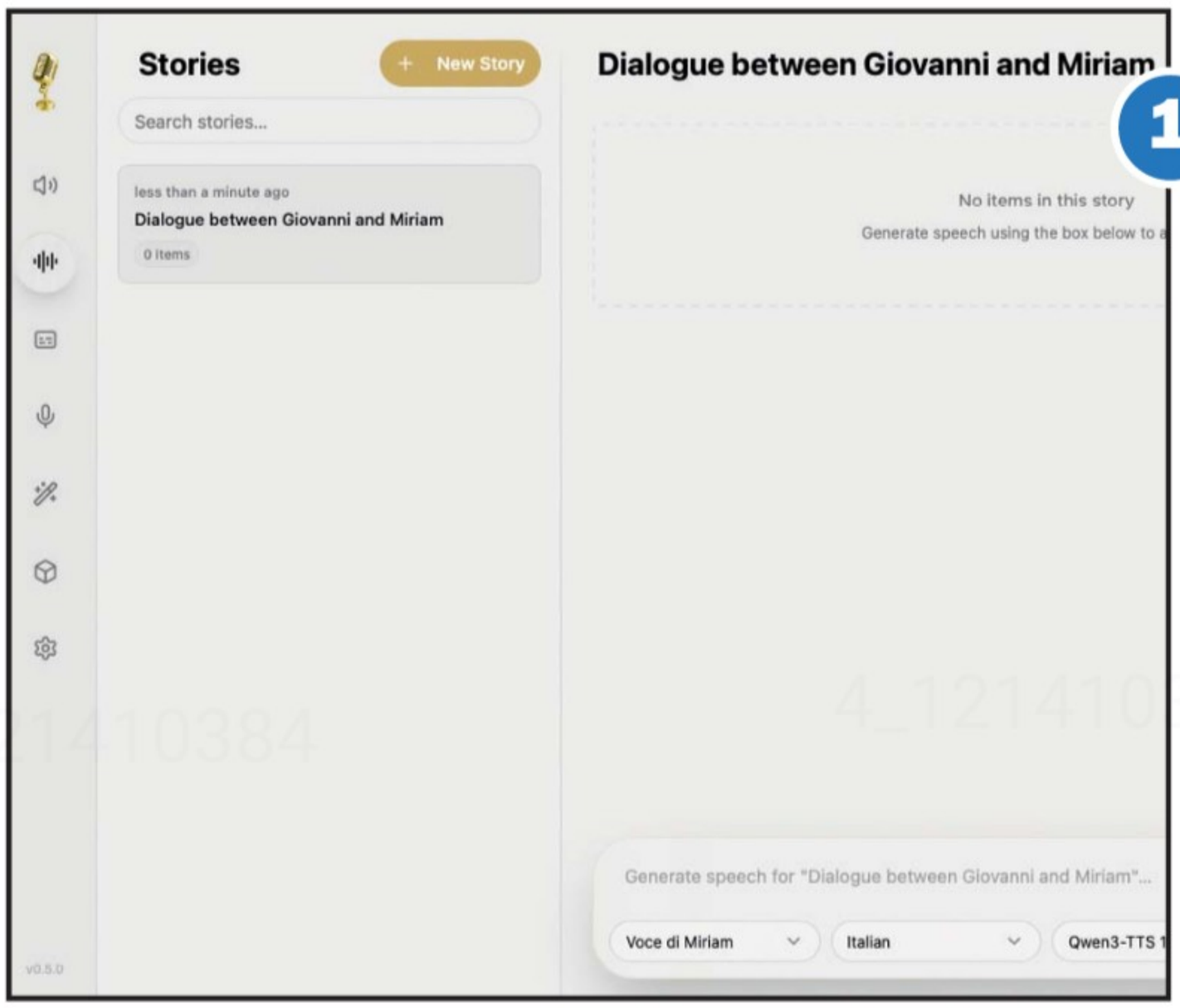



## EFFETS À GOGO

**Apply effects** permet d'appliquer une série d'effets prédéfinis. En cliquant sur **Load preset...**, vous pouvez choisir parmi différents presets : effet robotique, radio, écho, etc. Avec **+ Add effect...**, il est possible de configurer des paramètres comme la réverbération, le chœur, les filtres et d'autres effets audio.

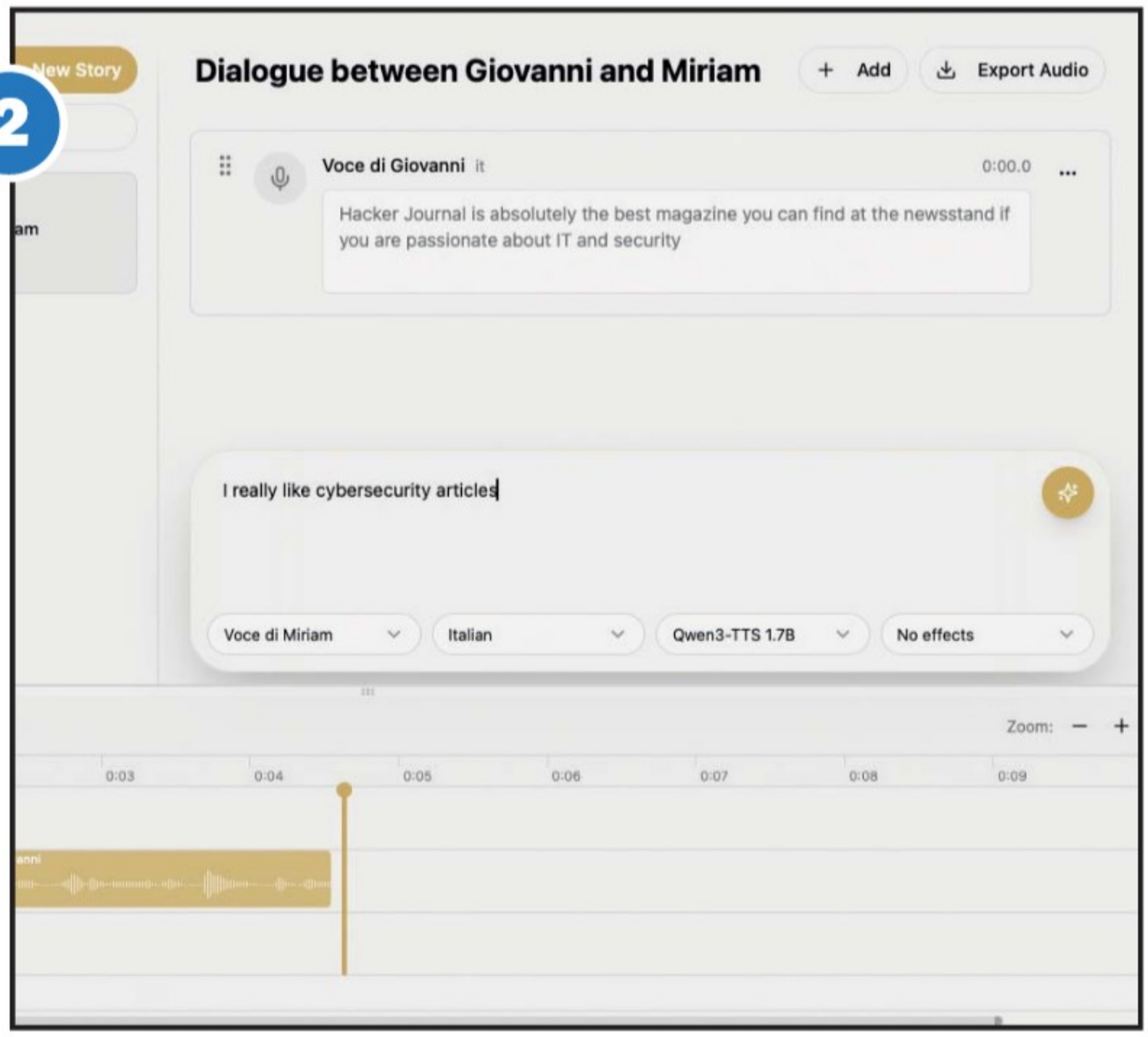
# UTILISER PLUSIEURS VOIX POUR UN DIALOGUE

Créer une histoire en écrivant des répliques pour chaque personnage et en sélectionnant plusieurs langues.



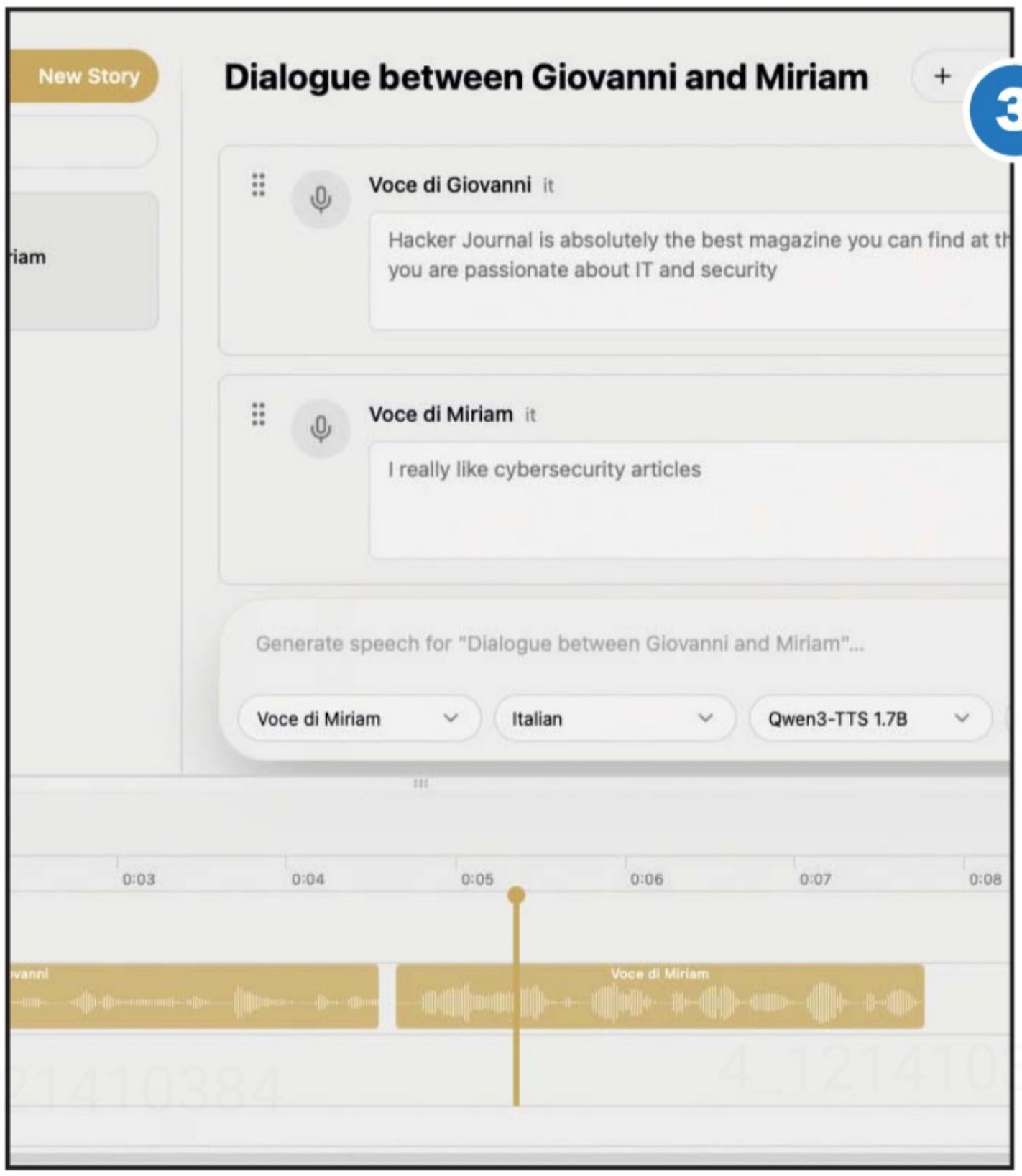

## CRÉONS UNE NOUVELLE HISTOIRE ...

La section **Stories** (deuxième icône dans le menu latéral de l'écran principal) est le cœur du logiciel, l'endroit où les profils créés interagissent dans un projet unique. Après avoir cliqué sur **New Story** et attribué un titre, vous pouvez commencer à construire la séquence.




## RÉPLIQUES EN ABONDANCE

Cliquez sur le bouton **+ Add** et choisissez la première voix du dialogue à générer. Ensuite, dans **Generate speech for ...**, saisissez la réplique du personnage, comme déjà vu lors de la création d'une nouvelle voix dans les étapes précédentes. Lancez la génération vocale en cliquant sur l'icône **Generate speech**.



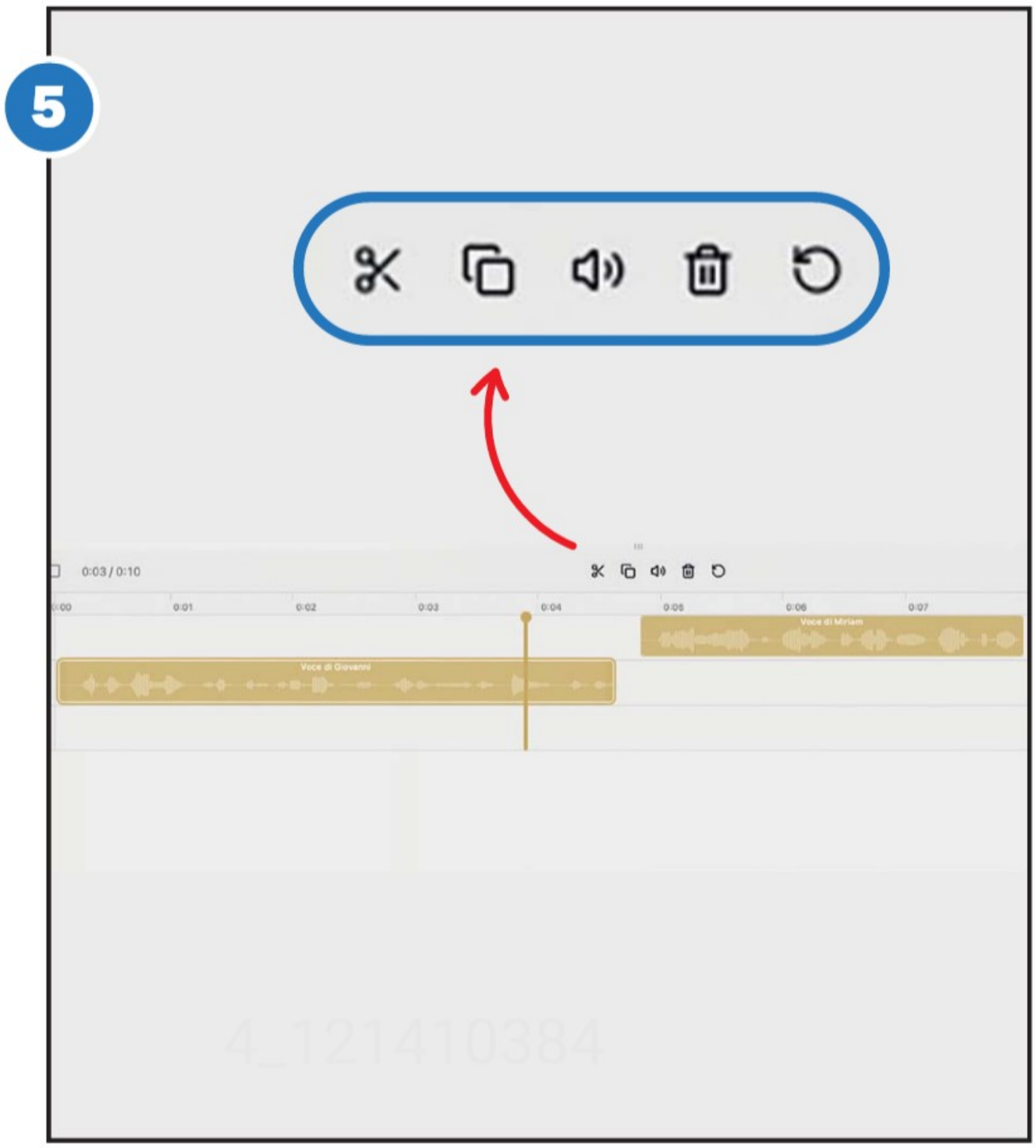

## UNE TIMELINE POUR LE DIALOGUE ...

Une fois la réplique générée avec la voix sélectionnée, elle est automatiquement ajoutée à la timeline en bas, dotée des fonctionnalités typiques des logiciels de montage audio et vidéo. À partir de là, vous pouvez générer de nouvelles répliques et les insérer dans la timeline pour construire un dialogue entre plusieurs voix.



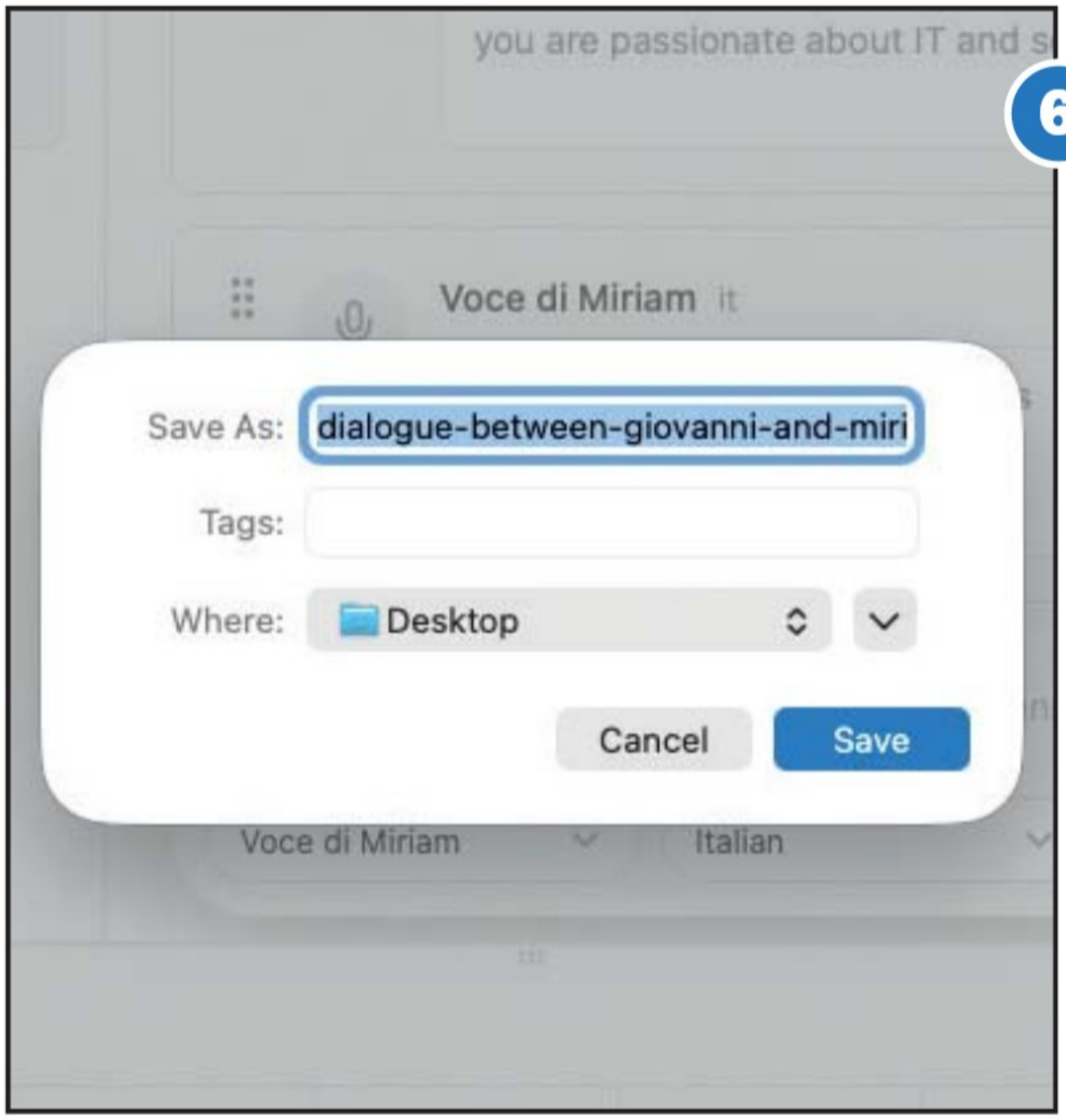

## PLAY, STOP ET ZOOM

Dans la partie supérieure gauche de la timeline se trouvent **Play** et **Stop**. Juste à côté sont affichés le point temporel sélectionné sur la piste et la durée totale du projet. Sur le côté opposé se trouve la zone Zoom, qui permet de réduire ou d'augmenter le niveau d'agrandissement de la timeline.




## ÉDITION AVANCÉE

En sélectionnant un clip et en plaçant le curseur sur son bord droit ou gauche, vous pouvez en étirer ou en réduire la durée en maintenant le bouton de la souris enfoncé. La sélection du clip rend disponibles les outils de modification : découpage (split), duplication, réglage du volume ...




## EXPORTER LE DIALOGUE

Une fois le dialogue généré avec les voix clonées, vous pouvez procéder à l'exportation du résultat final. En sélectionnant **Export Audio**, situé en haut à droite de l'écran, le système lance le traitement du projet. À la fin, la fenêtre de sauvegarde du fichier s'ouvre.

## DANS LES ENTRAILLES DU MOBILE

# CE QUE CACHE NOTRE SMARTPHONE



Du dossier DCIM aux données invisibles dans l'explorateur de fichiers : voici comment le système de fichiers révèle où se trouvent réellement vos documents.

Lorsqu'un smartphone Android est connecté à un ordinateur et que l'on ouvre la mémoire de l'appareil, plusieurs dossiers familiers apparaissent : **DCIM, Download, Pictures, Android**.

À première vue, il semble simplement s'agir de répertoires bien organisés. En réalité, ces dossiers témoignent de la manière dont le système d'exploitation organise les photos, les fichiers des applications, les documents téléchargés et bien d'autres données accumulées au fil du temps.

Mais lorsque les fichiers se comptent par centaines, voire par milliers, cette structure devient moins évidente à interpréter.

Il devient alors difficile de comprendre où se trouvent réellement les données et quelles applications occupent le plus d'espace. →

# Dossier



## PASSEZ VOTRE SMARTPHONE AU SCANNER

C'est pourquoi il existe des outils capables de transformer la structure des dossiers en une représentation graphique de l'espace occupé, permettant de visualiser immédiatement la manière dont les données sont réparties dans la mémoire de l'appareil. Pour cela, nous utiliserons **WinDirStat**. Il ne s'agit pas simplement d'un analyseur d'espace disque. Il analyse un répertoire ou un volume entier, calcule la taille réelle des fichiers et des dossiers et les représente sous la forme d'une **treemap**, tout en proposant une liste triable par extension, taille et chemin d'accès. Ce double niveau de lecture, à la fois sous forme de liste et de carte, le rend particulièrement utile pour effectuer une analyse structurelle des données : en quelques secondes, il est possible d'identifier des répertoires inhabituels, des fichiers anormalement volumineux ou des schémas d'accumulation qui, dans la vue arborescente classique du système de fichiers, resteraient presque invisibles.

Cet article propose un petit exercice d'observation pratique : utiliser un outil graphique pour explorer la structure des données d'un smartphone Android et comprendre comment le système organise réellement les informations au fil du temps. →

# UN SMARTPHONE PEUT RACONTER VOTRE HISTOIRE

**Dates de création, téléchargements, photos, vidéos, fichiers temporaires ... La structure du stockage conserve de nombreuses traces de notre utilisation quotidienne. Même sans ouvrir les fichiers, leur emplacement et leur taille peuvent déjà fournir de précieuses informations.**

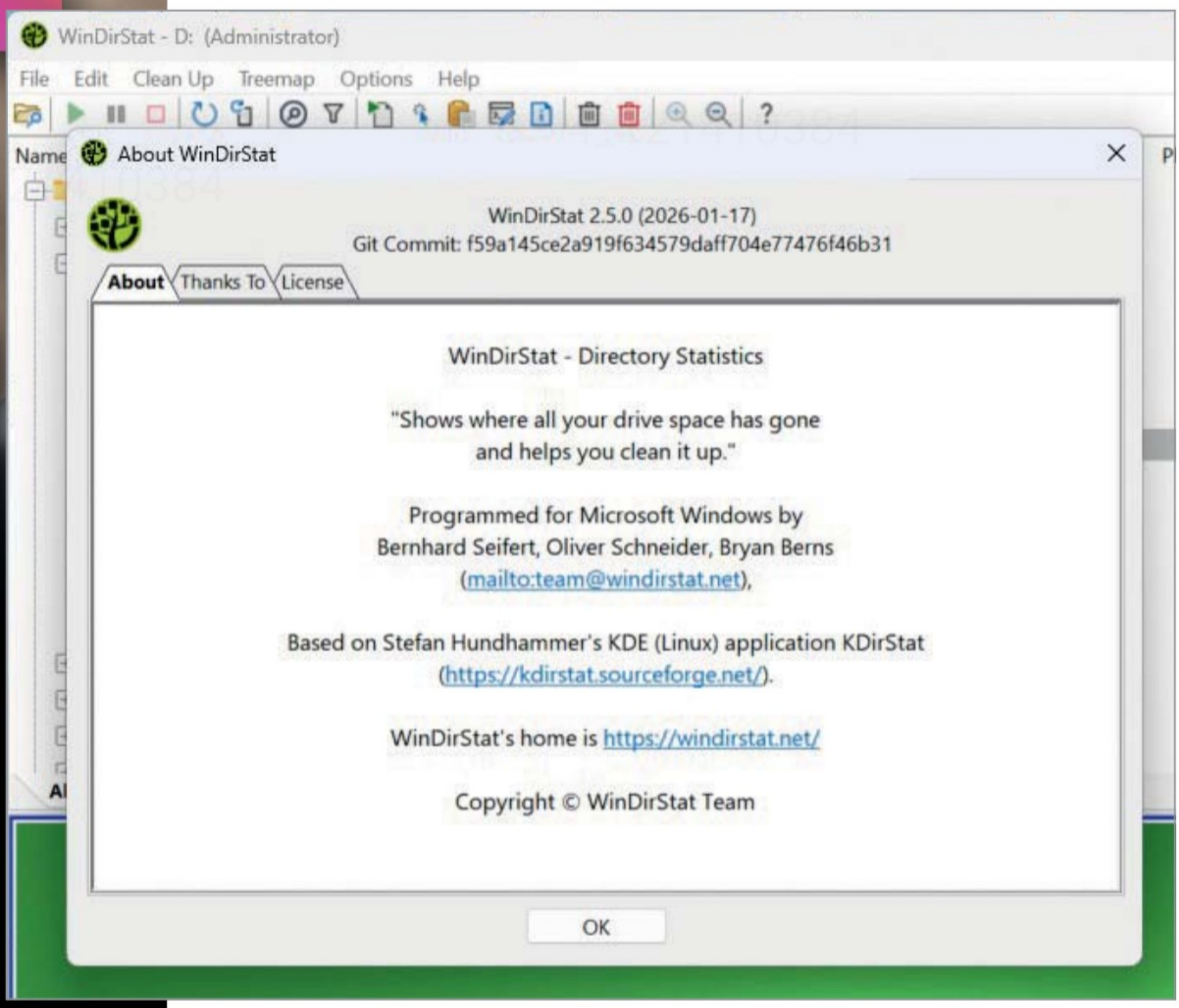
## MATÉRIEL NÉCESSAIRE

**WINDIRSTAT 2.8.0**
Logiciel qui analyse l'utilisation de l'espace disque et affiche les fichiers et dossiers les plus volumineux sous forme d'arborescence.

**Site Internet :** windirstat.net

**Coût :** Gratuit

**WinDirStat peut-il révéler des traces d'anciennes activités ?** Potentiellement. Des téléchargements oubliés, des archives, des fichiers temporaires ou d'anciens médias peuvent rester sur le disque longtemps après leur utilisation.



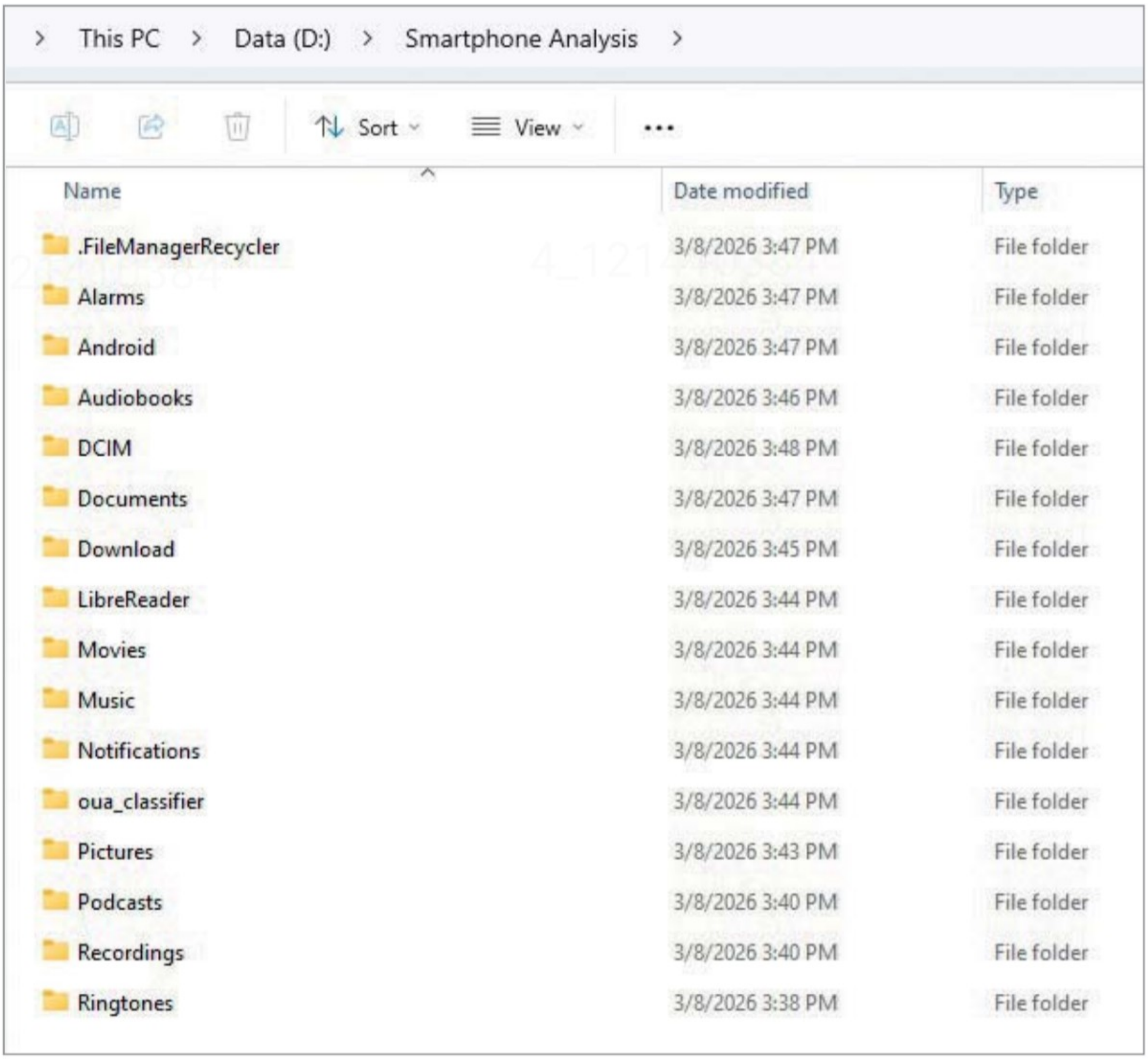

WinDirStat (**https://windirstat.net/**) représente graphiquement l'espace occupé par les fichiers et les dossiers sous Windows.

## JAMAIS L'ORIGINAL

Le périphérique est connecté à l'ordinateur via USB et le mode **Transfert de fichiers** est activé. Le contenu de la mémoire interne est alors copié dans un dossier du PC. Il ne s'agit pas d'une simple étape pratique : travailler sur une copie permet d'examiner les données sans risquer de les modifier accidentellement.

Dans les versions récentes d'Android, certains dossiers système peuvent ne pas être entièrement accessibles via une connexion USB. Il s'agit d'un choix de conception lié à la sécurité du système. L'accès complet à ces répertoires n'est possible qu'à l'aide d'outils de développement tels qu'**Android Debug Bridge (ADB)** ou de gestionnaires de fichiers disposant de privilèges avancés, directement sur l'appareil. À ce titre, il convient de rappeler l'importance du contexte et de la préservation de l'original.

Le principe est simple : **on observe d'abord, puis on décide éventuellement d'intervenir**. →




La copie des données du smartphone permet d'examiner les dossiers système, les répertoires créés par les applications et les différents emplacements gérés par le gestionnaire de fichiers.




## IDENTIFIER CE QUI PEUT ÊTRE SUPPRIMÉ

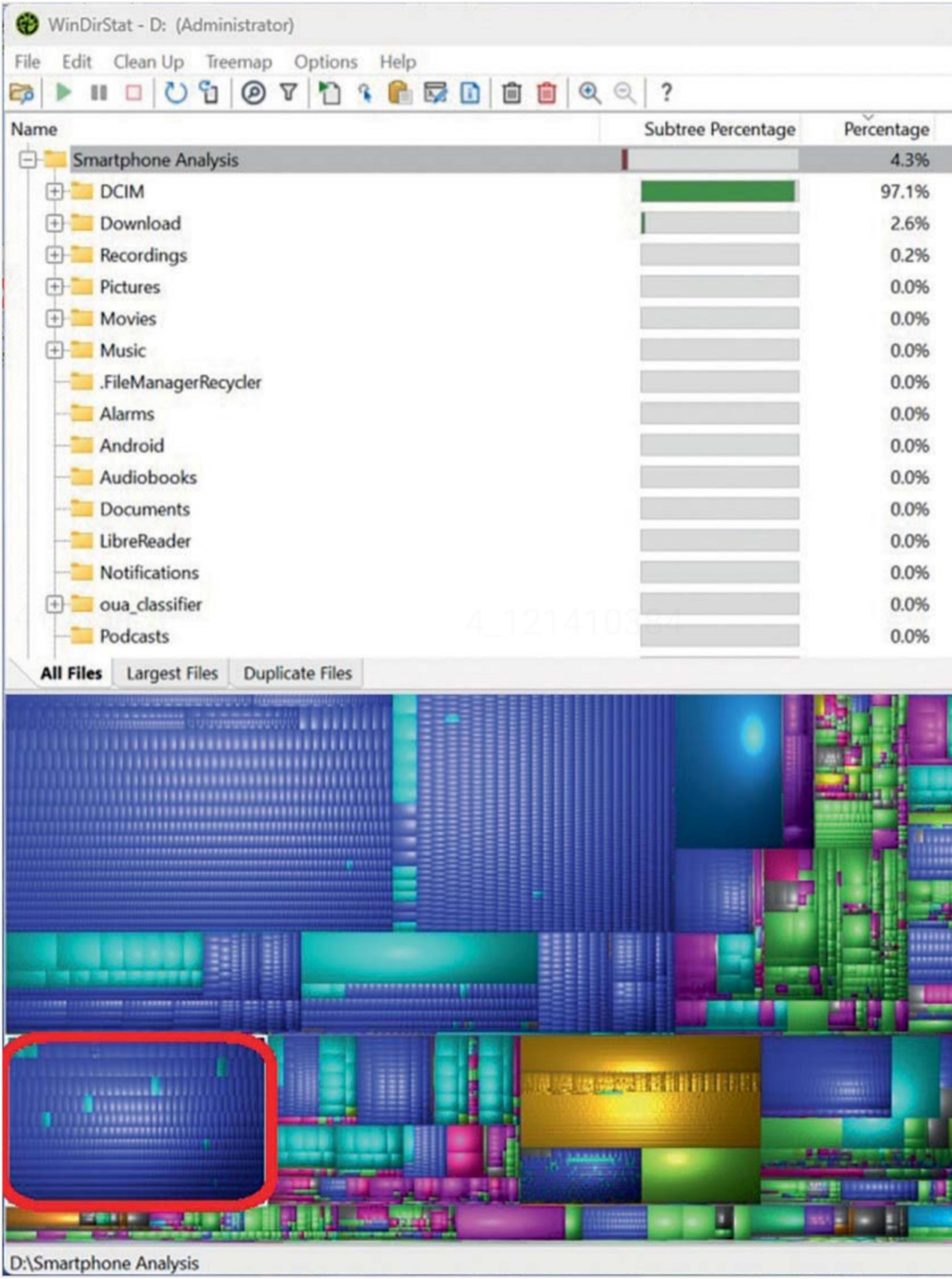
WinDirStat ne fonctionne pas directement sur le smartphone : il analyse uniquement la copie des données enregistrée sur l'ordinateur. Il ne peut donc pas être utilisé pour supprimer des fichiers sur l'appareil.

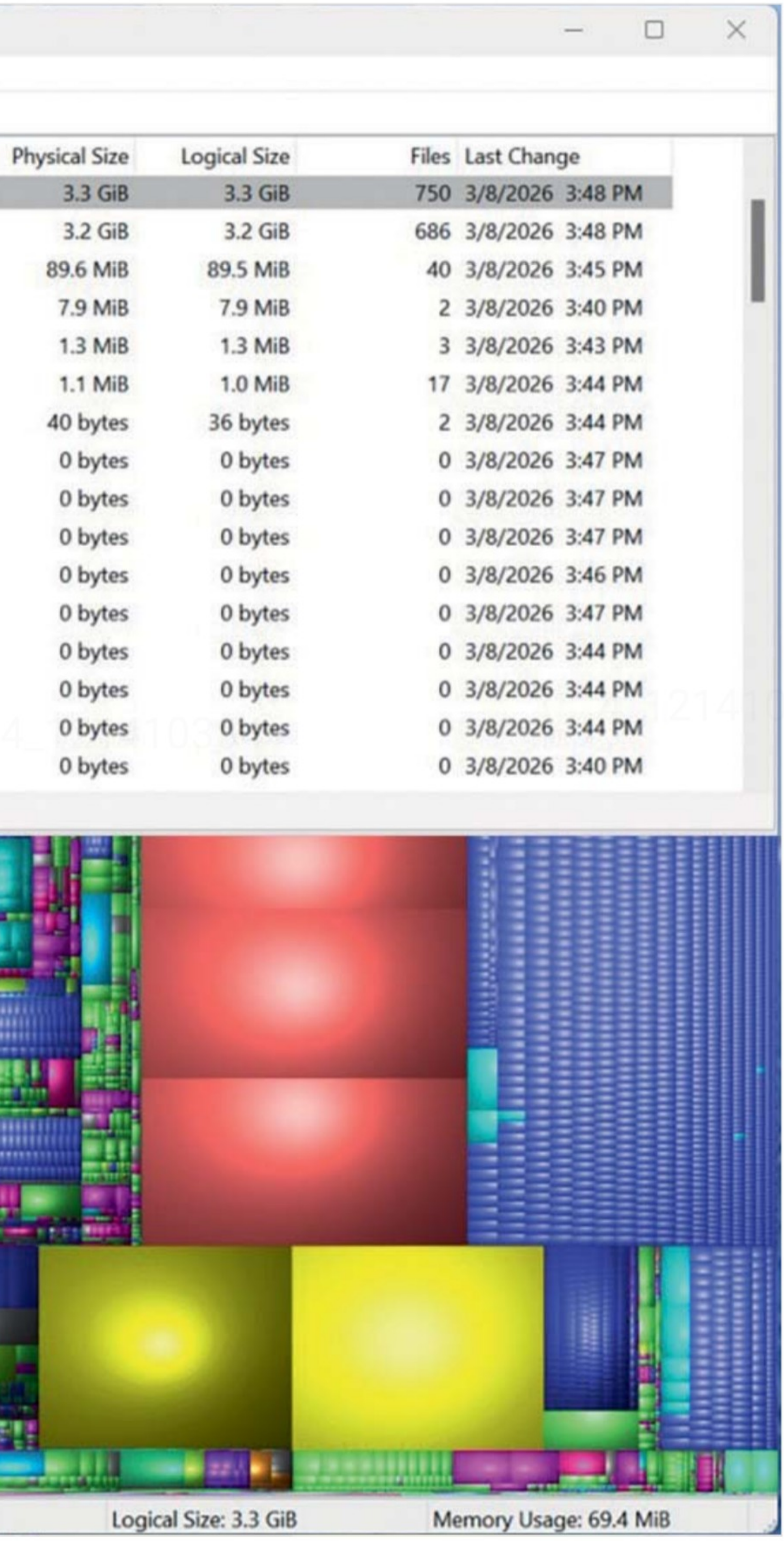
Son intérêt réside dans sa capacité à rendre immédiatement visibles, grâce à la liste et à la treemap, les dossiers et les fichiers qui occupent le plus d'espace. À cet égard, il est plus efficace que l'Explorateur de fichiers de Windows, qui n'offre pas une visualisation aussi immédiate de la taille des dossiers. Une fois les fichiers ou répertoires les plus volumineux identifiés dans la copie, il est possible de retourner sur le smartphone et de vérifier la présence de ces mêmes éléments, puis d'intervenir directement depuis l'appareil. L'analyse devient ainsi un véritable guide pour nettoyer la mémoire : on commence par observer la structure des données, puis on décide en connaissance de cause ce qui peut être supprimé.

### HACK&CRACK DIT ...

**Avant de supprimer, regardez. Vous pourriez découvrir où part réellement votre espace.**

# Dossier


WinDirStat - D: (Administrator)
File Edit Clean Up Treemap Options Help
Name
Subtree Percentage
Percentage
Smartphone Analysis 4.3%
DCIM 97.1%
Download 2.6%
Recordings 0.2%
Pictures 0.0%
Movies 0.0%
Music 0.0%
.FileManagerRecycler 0.0%
Alarms 0.0%
Android 0.0%
Audiobooks 0.0%
Documents 0.0%
LibreReader 0.0%
Notifications 0.0%
oua_classifier 0.0%
Podcasts 0.0%
All Files
Largest Files
Duplicate Files
D:\Smartphone Analysis




La treemap de WinDirStat représente les fichiers en fonction de l'espace qu'ils occupent et permet d'identifier immédiatement les zones les plus volumineuses.

## NE SUPPRIMEZ PAS AU HASARD !

**Un fichier volumineux n'est pas nécessairement inutile. Avant de supprimer quoi que ce soit, vérifiez à quelle application ou à quel contenu il appartient. L'analyse avec WinDirStat doit servir à comprendre l'utilisation de l'espace, pas à supprimer des fichiers à l'aveugle.**

# Dossier

## DCIM : POURQUOI CE NOM ?

**DCIM signifie Digital Camera IMages. Ce dossier est devenu un emplacement standard pour les photos et les vidéos produites par les appareils photo numériques, y compris ceux intégrés aux smartphones.**

## LE LOGICIEL QUI MONTRE OÙ VA L'ESPACE

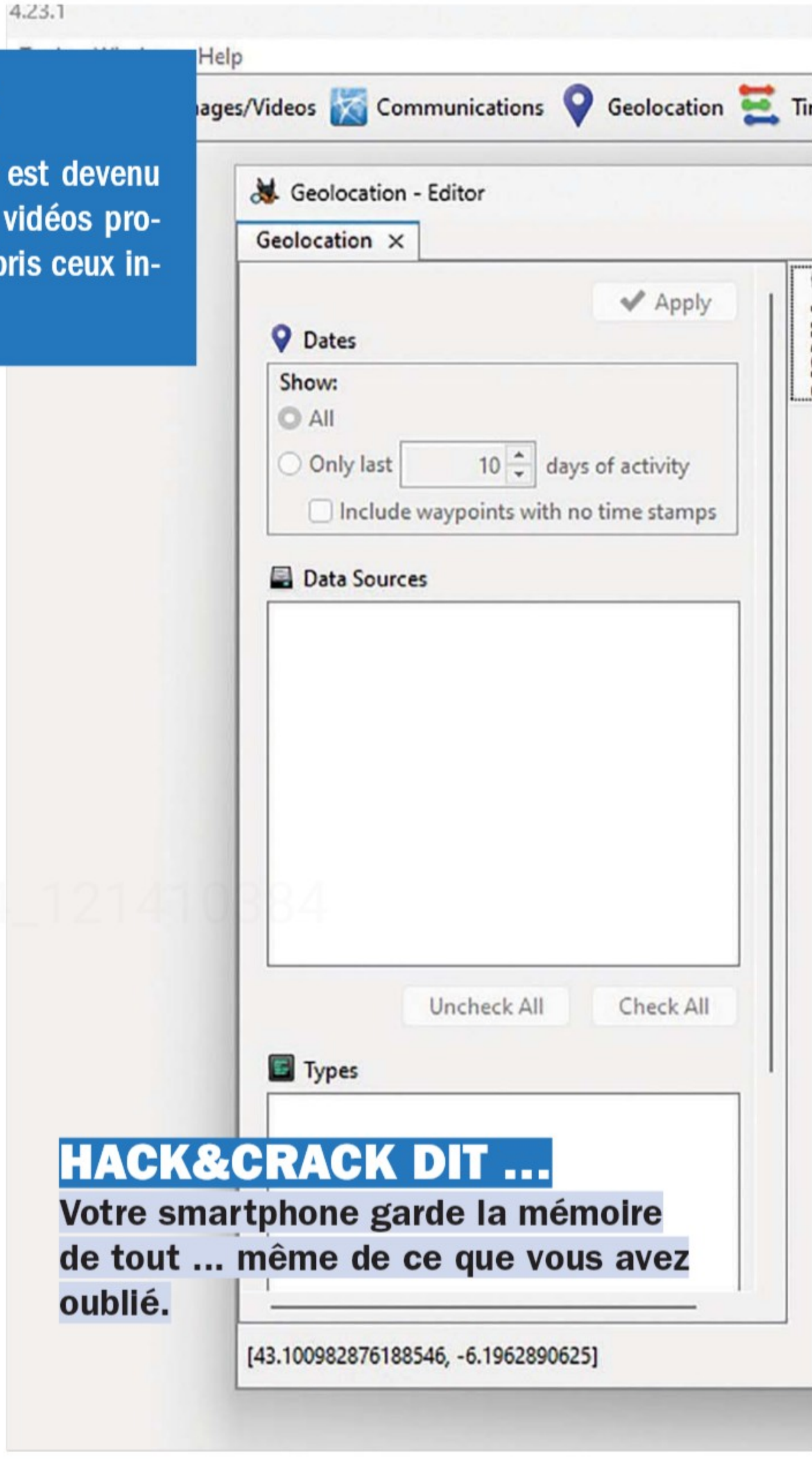
Pour l'analyse, nous utiliserons **WinDirStat**, un logiciel open source pour Windows qui représente graphiquement l'espace occupé par un dossier ou un disque. Une fois la copie terminée, le téléphone peut être déconnecté. À partir de ce moment, **l'analyse s'effectue sur une représentation figée du contenu de l'appareil** : une copie qui peut être examinée sans risquer de provoquer des modifications accidentelles.

La force de cet outil ne réside pas dans des fonctions sophistiquées, mais dans sa manière de représenter les données. À l'écran, les traditionnelles listes de dossiers disparaissent au profit d'une surface composée de blocs colorés.

Chaque rectangle représente un fichier et sa taille est proportionnelle à l'espace qu'il occupe dans la mémoire. Les couleurs permettent de distinguer rapidement les différents types de fichiers.

Le résultat constitue une véritable **carte des données**. Et, comme toute carte, elle rend visibles des proportions qui resteraient totalement masquées dans la vue traditionnelle des répertoires. Il suffit de sélectionner le dossier dans lequel les données du smartphone ont été copiées, puis de lancer l'analyse. Après quelques secondes, une vue d'ensemble de la mémoire analysée apparaît.

C'est à ce moment que le smartphone change de visage : ce qui ressemblait auparavant à un simple ensemble de fichiers devient une **structure lisible et compréhensible**.

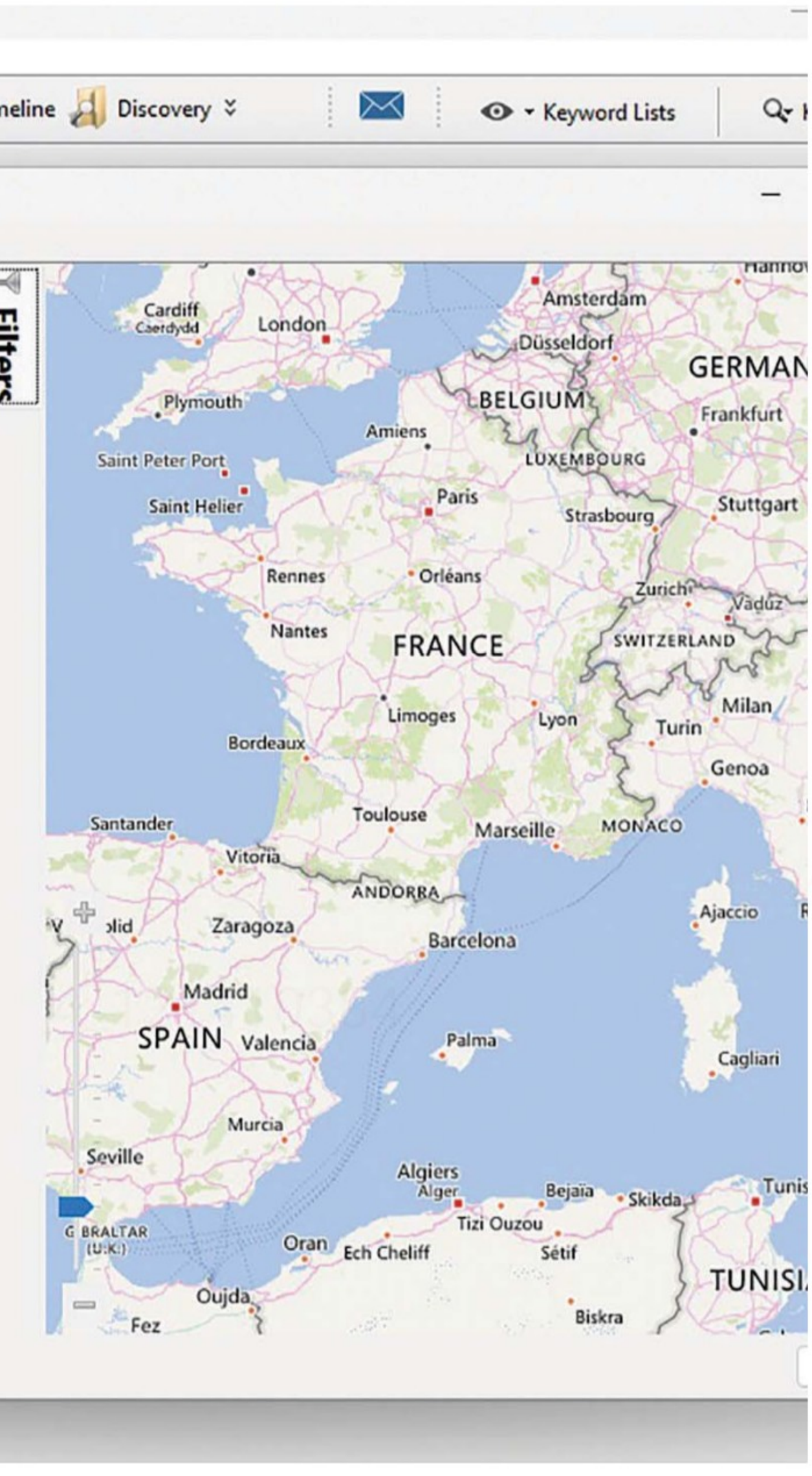



**HACK&CRACK DIT ...**

**Votre smartphone garde la mémoire de tout ... même de ce que vous avez oublié.**

## DCIM, LE POIDS DES SOUVENIRS

Dans la plupart des cas, le dossier **DCIM** est celui qui domine la carte. C'est là que sont stockées les photos et les vidéos enregistrées avec l'appareil photo du smartphone.




Lorsque la représentation graphique fait apparaître de très grands blocs concentrés dans cette zone, il ne s'agit presque jamais des photos, mais plutôt des vidéos. Quelques minutes d'enregistrement en 4K suffisent à générer des centaines de mégaoctets de données. Jusque-là, rien de surprenant. Mais l'observation de la carte fait immédiatement apparaître un premier élément intéressant : **la mémoire ne se remplit pas de manière uniforme**.

WinDirStat vous montre où se cachent les fichiers les plus volumineux. Mais si vous voulez vraiment explorer les traces laissées par un smartphone, passez au niveau supérieur : essayez Autopsy (**https://short.tips/url/autopsy**).

## ELLE SE REMPLIT PAR ÉVÉNEMENTS

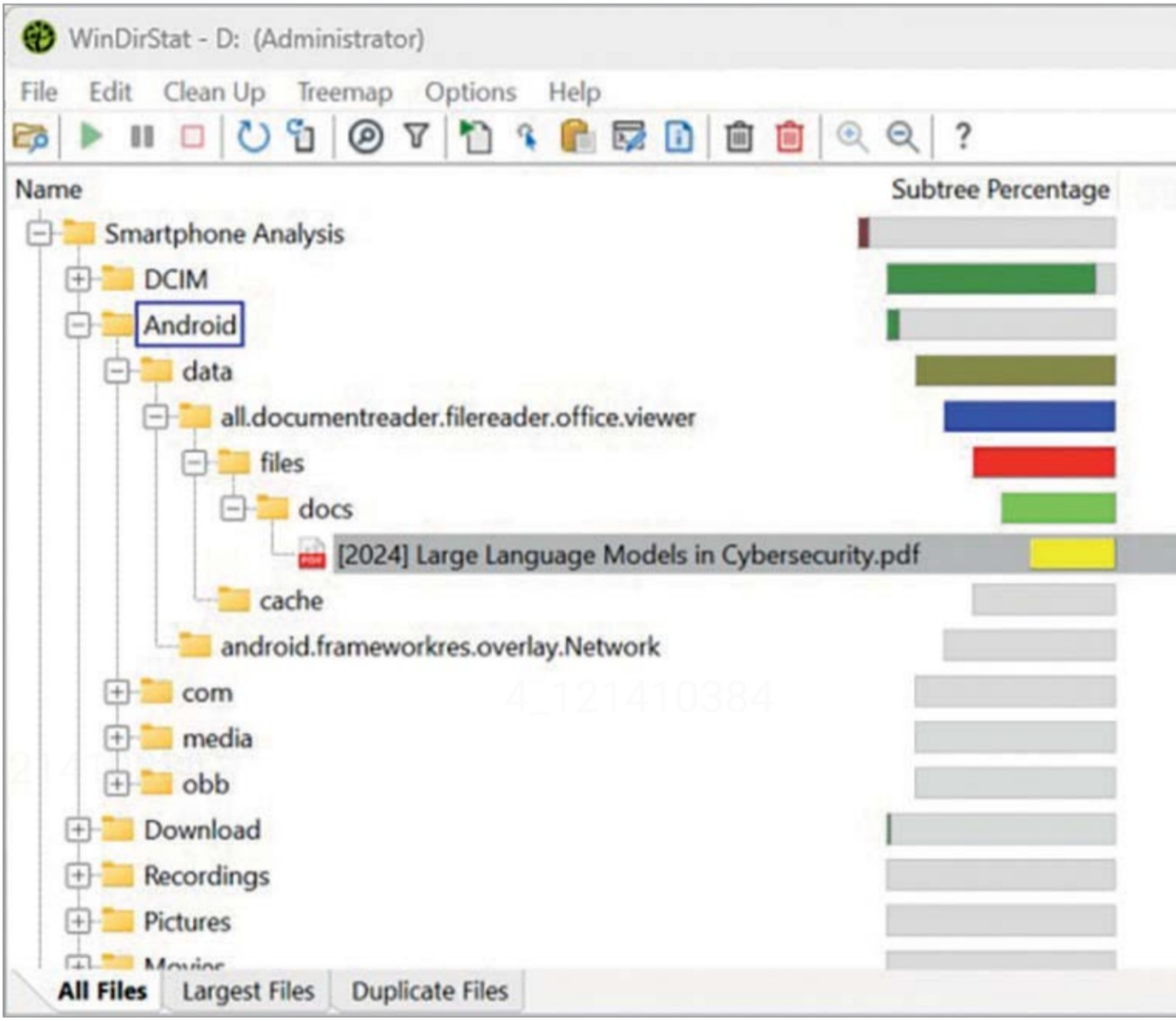
Des vacances, une fête ou une journée au cours de laquelle nous enregistrons plus de vidéos que d'habitude peuvent provoquer des pics soudains de l'espace occupé. Dans ce sens, le système de fichiers devient presque une chronologie silencieuse de nos activités : il conserve ces moments avec une précision souvent supérieure à celle de notre propre mémoire.

## LE TIROIR QU'IL NE FAUT JAMAIS VIDER

Le dossier **Download** est souvent bien plus intéressant qu'on ne l'imagine. C'est là que finissent les PDF reçus par e-mail, les images enregistrées « juste pour un instant », les fichiers APK téléchargés pour faire un essai, les documents en double, les installateurs oubliés et les pièces jointes que nous n'ouvrirons probablement plus jamais. C'est un espace où s'accumulent bien plus de choses que nous ne parvenons réellement à en supprimer.

Dans la visualisation de **WinDirStat**, ce dossier n'est pas nécessairement la zone la plus volumineuse du disque, mais c'est presque toujours la plus hétérogène et la plus désordonnée. Des fichiers isolés, des tailles très différentes, des formats en tout genre, souvent sans aucun lien apparent. →

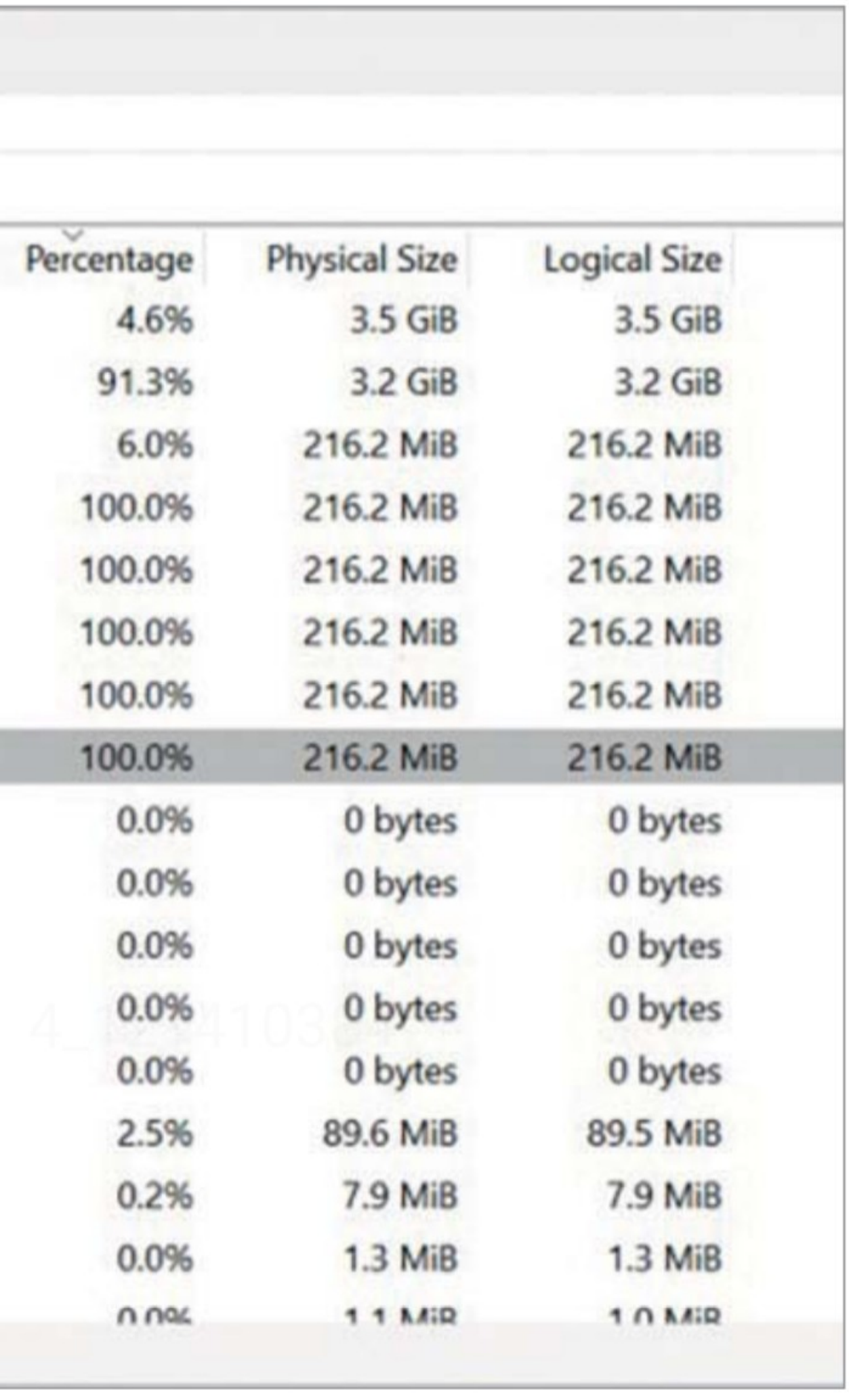
# Dossier




C'est, en somme, l'équivalent numérique du tiroir où finissent les vieilles clés, les vis qui restent après un bricolage, les câbles dépareillés et tous ces objets dont nous ne savons pas vraiment où les ranger, mais que nous continuons à conserver « parce qu'ils pourraient servir ». Sur la carte, cette habitude devient immédiatement évidente : une multitude de petits blocs, dispersés, irréguliers, sans logique précise ni structure identifiable. Ils n'occupent pas toujours beaucoup d'espace, mais ils illustrent parfaitement un comportement courant et profondément humain : **télécharger quelque chose à la hâte, remettre à plus tard le moment de faire le tri et, très souvent, ne plus jamais y revenir**.

## ANDROID, LA PARTIE LA MOINS VISIBLE

Le dossier le plus instructif est probablement **Android**. C'est ici que l'on découvre concrètement la manière dont les applications organisent leurs propres données. Il contient généralement trois répertoires principaux : **data**, **media** et **obb**. Même sans connaître en détail le fonctionnement interne du système, la carte graphique permet immédiatement



| Percentage | Physical Size | Logical Size |
|---|---|---|
| 4.6% | 3.5 GiB | 3.5 GiB |
| 91.3% | 3.2 GiB | 3.2 GiB |
| 6.0% | 216.2 MiB | 216.2 MiB |
| 100.0% | 216.2 MiB | 216.2 MiB |
| 100.0% | 216.2 MiB | 216.2 MiB |
| 100.0% | 216.2 MiB | 216.2 MiB |
| 100.0% | 216.2 MiB | 216.2 MiB |
| 100.0% | 216.2 MiB | 216.2 MiB |
| 0.0% | 0 bytes | 0 bytes |
| 0.0% | 0 bytes | 0 bytes |
| 0.0% | 0 bytes | 0 bytes |
| 0.0% | 0 bytes | 0 bytes |
| 0.0% | 0 bytes | 0 bytes |
| 2.5% | 89.6 MiB | 89.5 MiB |
| 0.2% | 7.9 MiB | 7.9 MiB |
| 0.0% | 1.3 MiB | 1.3 MiB |
| 0.0% | 1.1 MiB | 1.0 MiB |

de visualiser les différences de taille entre ces différentes zones. Dans **Android/data** se trouvent les dossiers des différentes applications. Leurs noms correspondent aux identifiants de package, tels que **com.whatsapp** ou **com.spotify.music**. On y trouve notamment des caches, des fichiers temporaires et des bases de données. Dans certains cas, l'espace occupé peut être étonnamment important. Non pas parce que l'application est intrinsèquement « lourde », mais parce qu'elle accumule au fil du temps des données qui ne sont pas directement visibles depuis son interface.

Dans le dossier Android/data, chaque application conserve ses propres fichiers, qui peuvent s'accumuler au fil du temps sans être directement visibles par l'utilisateur.

Dans **Android/media** apparaissent souvent les images et les vidéos générées par les applications. On y découvre notamment des dossiers liés aux applications de messagerie qui grossissent silencieusement : images reçues dans les groupes, fichiers audio transférés, clips partagés puis jamais supprimés. L'utilisateur pense avoir « simplement regardé » un contenu ; le système de fichiers, lui, l'a bel et bien enregistré.
Le répertoire **obb**, quant à lui, est principalement associé aux jeux.

## CACHE ET BASES DE DONNÉES, DES DONNÉES BIEN RÉELLES

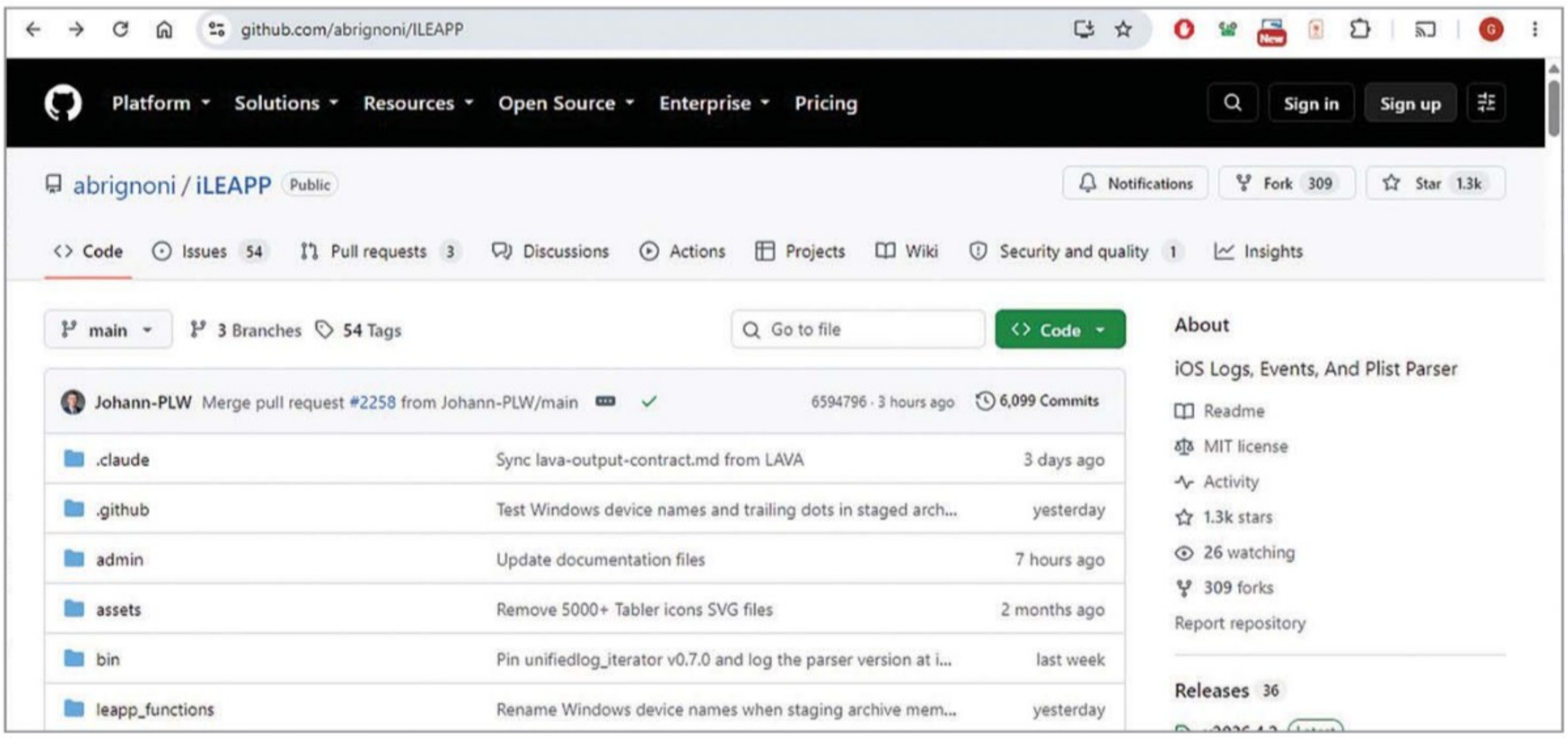
L'un des aspects les plus intéressants apparaît lorsqu'on désinstalle une application, puis que l'on répète l'opération de copie et d'analyse. Dans certains cas, le dossier correspondant dans Android/data reste présent. Il ne contient pas nécessairement des données importantes : parfois, il est presque vide. Mais sa simple présence nous apprend déjà quelque chose. La désinstallation supprime l'application, mais pas forcément toutes les traces qu'elle a laissées. La différence est subtile, mais significative. Le système d'exploitation privilégie le fonctionnement et la compatibilité des applications plutôt qu'un nettoyage absolu du système de fichiers. C'est le même principe que celui que l'on observe avec les métadonnées : **une information ne disparaît pas simplement parce qu'elle n'est plus visible**. →

## QU'APPRENONS-NOUS VRAIMENT ?

Cet exercice est avant tout un travail de lecture structurelle qui permet de comprendre que notre smartphone n'est pas une boîte noire : **c'est un système organisé**. Chaque application laisse des traces cohérentes avec sa fonction.
Chaque action de l'utilisateur produit un effet mesurable dans le système de fichiers. Observer la structure des données à l'aide d'un outil graphique permet de supprimer un niveau d'abstraction.
On ne voit plus des « applications », mais des répertoires et des fichiers, représentés par des rectangles concrets qui occupent de l'espace sur le disque. En passant d'une interface conçue pour l'utilisateur à une vue pensée pour le système de fichiers, on acquiert un véritable avantage cognitif : il devient possible de comprendre comment le système organise et conserve les informations.
À l'intérieur d'un smartphone, il n'y a pas de mystère, mais **de la structure et de l'organisation**. Ce qui nous manque souvent, c'est l'habitude de les observer. Un outil comme **WinDirStat** ne révèle aucun secret, mais il rend les proportions visibles. Et ces proportions en disent long.
Elles montrent quelles applications produisent le plus de données, quels dossiers grossissent au fil du temps et quelles traces subsistent même après une suppression apparente.
Apprendre à lire cette structure, c'est acquérir une nouvelle façon d'observer les systèmes numériques. Non plus seulement à travers les interfaces conçues pour l'utilisateur, mais à travers la logique selon laquelle le système de fichiers organise les informations. **La sécurité commence souvent par là**.
Pas avec des outils complexes, mais avec la capacité d'observer ce qui se trouve déjà sous nos yeux.

## HACK&CRACK DIT ...

**Derrière chaque application se cache une petite architecture de fichiers.**




WinDirStat permet de visualiser les fichiers qui occupent l'espace. Avec iLEAPP (**https://short.tips/url/ileapp**), on va plus loin : cet outil open source analyse les traces et les artefacts laissés par iOS et iPadOS.

SMISHING

# LES 10 ARNAQUES PAR SMS LES PLUS DANGEREUSES



Pas besoin de virus sophistiqués ni d'attaques dignes d'un film pour piéger une victime. Parfois, un message bien rédigé suffit...

Pendant des années, nous avons imaginé les arnaques en ligne sous la forme de messages truffés de fautes, de liens improbables et de promesses absurdes. Aujourd'hui, le scénario a changé. **Les campagnes de smishing**, c'est-à-dire de phishing par SMS, fonctionnent précisément parce qu'elles imitent la normalité. Elles sont courtes, crédibles, souvent bien rédigées et arrivent au point le plus exposé de notre vie numérique : le smartphone. C'est là que nous les lisons à la hâte, parfois en travaillant, en conduisant, en attendant une livraison ou en consultant notre compte bancaire.



## UNE RÉPONSE IMPRUDENT

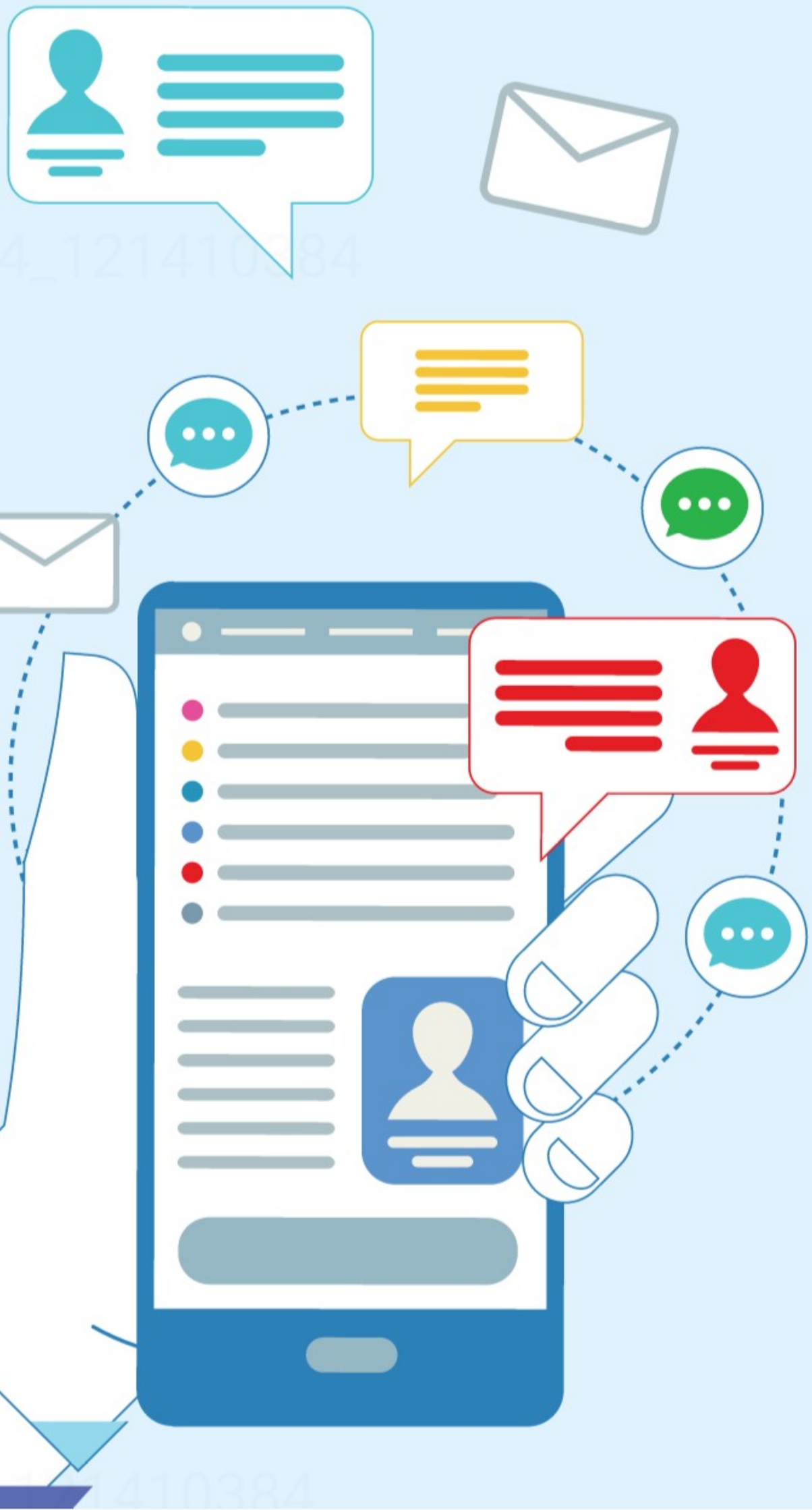
Le principe est simple : l'attaquant n'a pas besoin de nous convaincre d'accomplir quelque chose de spectaculaire. Il lui suffit d'obtenir une seule action qui demande peu d'effort. Un clic. Un micro-paiement. Une confirmation rapide. La saisie d'un code temporaire. À partir de là, la chaîne d'attaque peut rapidement s'allonger.

Dans certains cas, la victime arrive sur une page d'hameçonnage qui reproduit l'identité visuelle, les couleurs et le parcours d'authentification d'un véritable service. Dans d'autres, elle est incitée à télécharger une application malveillante ou à communiquer volontairement des données qui seront ensuite réutilisées pour prendre le contrôle d'un compte, commettre des fraudes au paiement ou usurper une identité.

**Le smishing est efficace parce qu'il ne s'attaque pas directement à la technologie** : il exploite nos habitudes. Il joue sur la précipitation, la peur de perdre quelque chose ou le besoin de résoudre immédiatement un problème. Si vous attendez un colis, le SMS du transporteur semble plausible. Si vous empruntez souvent l'autoroute, un message concernant un péage impayé paraît crédible. Si vous possédez un compte en ligne, la notification d'une connexion suspecte déclenche immédiatement l'alerte.

Lorsque le message fait écho à une situation réelle de votre quotidien, il devient beaucoup plus facile de baisser la garde. C'est pourquoi il ne suffit pas de dire « méfiez-vous des liens ». Il faut comprendre quels masques portent ces campagnes, quel mécanisme elles exploitent et quelles données elles cherchent réellement à obtenir.

Les dix pièges présentés dans les pages suivantes comptent parmi les plus courants et, surtout, les plus dangereux, précisément parce qu'ils ressemblent de manière troublante à des situations qui pourraient réellement nous arriver.



## 1 LE COLIS BLOQUÉ




C'est l'une des arnaques les plus simples et, précisément pour cette raison, l'une des plus efficaces. Le message signale une livraison bloquée, une adresse incomplète ou un petit paiement à effectuer. Cela fonctionne parce qu'aujourd'hui, presque tout le monde attend un colis. Le mécanisme repose sur l'usurpation de marque : le lien renvoie vers un site qui imite celui d'un transporteur ou de La Poste et invite à confirmer des informations ou à payer une petite somme. En réalité, l'objectif n'est pas de récupérer les quelques euros demandés, mais de collecter des informations personnelles et des données bancaires, qui pourront ensuite être réutilisées dans d'autres fraudes.

### COMMENT SE PROTÉGER

**La défense la plus efficace consiste à interrompre la chaîne dès le départ : ne partez jamais du message reçu. Si vous attendez réellement un colis, vérifiez son statut dans l'application officielle du transporteur ou en saisissant vous-même l'adresse de son site dans le navigateur, jamais en cliquant sur le lien reçu par SMS. La différence peut sembler minime, mais c'est précisément là que se joue la distinction entre une vérification légitime et une page conçue pour récupérer vos identifiants.**

## 2 LE PÉAGE À RÉGLER




Autre piège très efficace : celui du péage impayé. Le message est bref, sec, presque administrati : un petit montant doit être réglé et il vaut mieux le faire immédiatement pour éviter des sanctions. C'est précisément là que réside l'efficacité de l'arnaque : pour quelques euros, beaucoup de personnes paient sans vérifier.

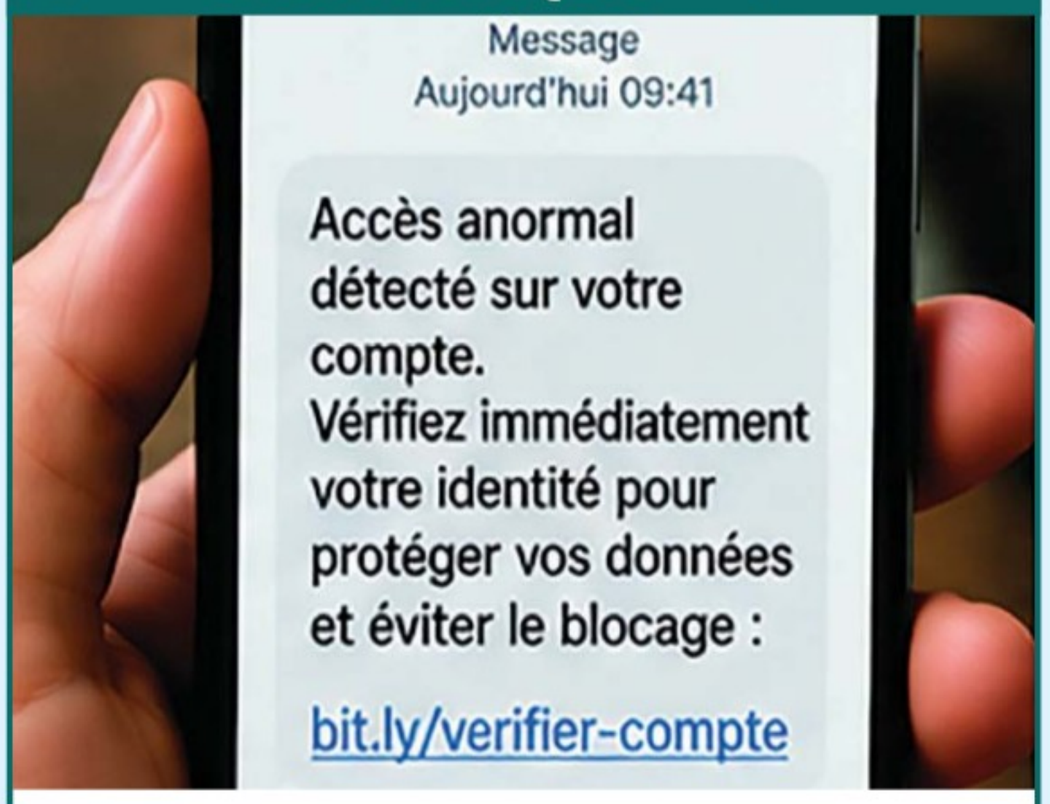
Le message ne doit rien avoir d'exceptionnel, mais sembler parfaitement ordinaire, comme une simple formalité administrative à régler rapidement. La victime clique alors, saisit ses données et pense avoir résolu le problème. En réalité, elle transmet à un site frauduleux des informations précieuses : données personnelles, coordonnées de paiement et coordonnées qui pourront être réutilisées dans d'autres campagnes de smishing.

### COMMENT SE PROTÉGER

La rigueur compte davantage que l'instinct. Un paiement lié à un péage ou à un service routier ne doit jamais être vérifié en cliquant sur le lien contenu dans un SMS.

Il faut passer par les canaux officiels, effectuer la vérification depuis ceux-ci et considérer toute urgence comme un indicateur de risque. Plus le message vous pousse à agir immédiatement, plus il est important de ralentir.

## 3 LE COMPTE « SOUS ATTAQUE »




Parmi toutes les arnaques par SMS, les fraudes bancaires restent particulièrement efficaces, car elles jouent sur la peur de perdre le contrôle de son argent.

Quelques mots suffisent - connexion inhabituelle, opération suspecte, carte bloquée - pour provoquer la panique et pousser la victime à agir instinctivement.

Le lien renvoie vers une page clone qui imite celle d'une banque ou d'un réseau de paiement. L'utilisateur, persuadé de se protéger, saisit alors ses identifiants, les données de sa carte et parfois même des codes temporaires. En réalité, il facilite ainsi une tentative de prise de contrôle de son compte.

### COMMENT SE PROTÉGER

Cette arnaque est efficace précisément parce qu'elle se présente comme une mesure de protection. Mais le procédé reste toujours le même : aucune banque sérieuse ne gère un incident de sécurité en demandant à ses clients de cliquer sur un lien reçu par SMS.

Si le doute est réel, vérifiez la situation dans l'application officielle ou appelez l'établissement en utilisant son numéro de téléphone officiel. Tout le reste n'est que mise en scène.

## 4 LA MISE À JOUR DES DONNÉES BANCAIRES




Plus insidieuse encore, voici la version « aimable ». Pas d'alerte ni de ton alarmiste : simplement une demande apparemment normale de mettre à jour votre profil, de confirmer vos informations ou de terminer une procédure de sécurité. C'est précisément ce qui la rend dangereuse : elle ne mise pas sur la panique, mais sur la baisse de vigilance.

Le message imite le langage du service client et se présente comme une simple formalité. La victime clique, remplit le formulaire, confirme. Mais le résultat est le même : les données tombent entre les mains des escrocs, prêts à les utiliser pour des accès non autorisés, des fraudes bancaires ou des campagnes de smishing encore plus crédibles.

### COMMENT SE PROTÉGER

**La règle reste la même : si une banque ou un service financier vous demande de mettre à jour des informations importantes, vérifiez la demande depuis le canal officiel. Si rien n'y apparaît, il est très probable que cette demande n'existe pas.**

**Et si elle est réellement nécessaire, l'établissement n'aura pas besoin de vous relancer par SMS.**

## 5 LE BONUS À CONFIRMER




Les arnaques qui usurpent le nom d'un organisme public bénéficient d'un avantage décisif : elles s'habillent des attributs de l'autorité. Si le SMS semble provenir d'un organisme public, beaucoup de personnes baissent immédiatement leur garde. Le message parle d'un bonus, d'un versement ou d'une démarche à effectuer et invite à confirmer ses données. Alors que nos échanges avec l'administration sont de plus en plus numériques, le piège paraît crédible. Mais les véritables objectifs sont le numéro fiscal, les coordonnées bancaires, les identifiants et les documents. Autant d'informations qui peuvent alimenter des usurpations d'identité, des paiements frauduleux ou des accès à d'autres services.

### COMMENT SE PROTÉGER

**Ces campagnes jouent simultanément sur deux leviers : le désir d'obtenir quelque chose et la peur de le perdre. C'est une combinaison très puissante. Il faut donc retenir une règle simple : aucun avantage sérieux ne se confirme en cliquant sur un lien reçu par SMS. Tout ce qui concerne les bonus, les démarches ou les versements doit être vérifié exclusivement par les canaux officiels de l'organisme concerné.**

# Dossier

## QUESI GNIFIE ?

### PHISHING

C'est une technique d'ingénierie sociale par laquelle un escroc se fait passer pour une personne ou une organisation de confiance afin d'inciter sa victime à fournir des informations ou à effectuer une action. Le phishing peut prendre la forme d'un e-mail, d'un SMS, d'un message instantané, d'un appel téléphonique ou d'un site Web frauduleux. Le *smishing* est donc une forme particulière de phishing.

### SMISHING

C'est une forme de *phishing* qui utilise les SMS comme vecteur d'attaque. Le terme est issu de la contraction de *SMS* et de phishing. L'objectif est d'inciter la victime à effectuer une action : ouvrir un lien, saisir des identifiants, fournir des informations bancaires, communiquer un code OTP ou installer une application. Le message s'appuie souvent sur un prétexte crédible, comme un colis bloqué, un paiement à effectuer, une connexion suspecte ou un bonus à récupérer.

### VISHING

C'est l'équivalent téléphonique du phishing : l'escroc utilise un appel vocal pour manipuler sa victime afin d'obtenir des informations ou de la pousser à effectuer une action. Cette technique peut également être utilisée comme seconde étape d'une arnaque commencée par SMS.

### QUISHING

C'est une forme de phishing qui utilise un code QR. La victime scanne le code et est redirigée vers un site frauduleux, généralement dans le but de récupérer ses identifiants ou d'autres données. Le principe est similaire à celui du *smishing*, mais le lien est ouvert au moyen d'un QR code plutôt que d'un lien classique.

### SOCIAL ENGINEERING

Il s'agit de la manipulation psychologique d'une victime afin d'obtenir des informations ou de l'inciter à effectuer certaines actions. Cette technique n'exploite pas nécessairement une vulnérabilité technique : elle peut jouer sur la précipitation, la peur, la curiosité, l'autorité, la confiance ou l'envie d'obtenir un avantage. C'est l'un des principaux ressorts du *smishing*.

### BRAND IMPERSONATION

Il s'agit de l'usurpation de l'identité d'une entreprise ou d'une organisation réelle. L'escroc peut reprendre son nom, son logo, ses couleurs, son vocabulaire et d'autres éléments visuels ou textuels. L'objectif est de tirer parti de la confiance associée à la marque afin de rendre le message crédible.

### LANDING PAGE

Il s'agit de la page Web vers laquelle la victime est redirigée après avoir suivi un lien. Dans une campagne de *smishing*, elle peut être conçue pour ressembler à la page d'une banque, d'un transporteur, d'un organisme public ou d'un service en ligne. Son apparence peut être extrêmement convaincante, mais son adresse peut révéler qu'elle n'utilise pas le domaine officiel.

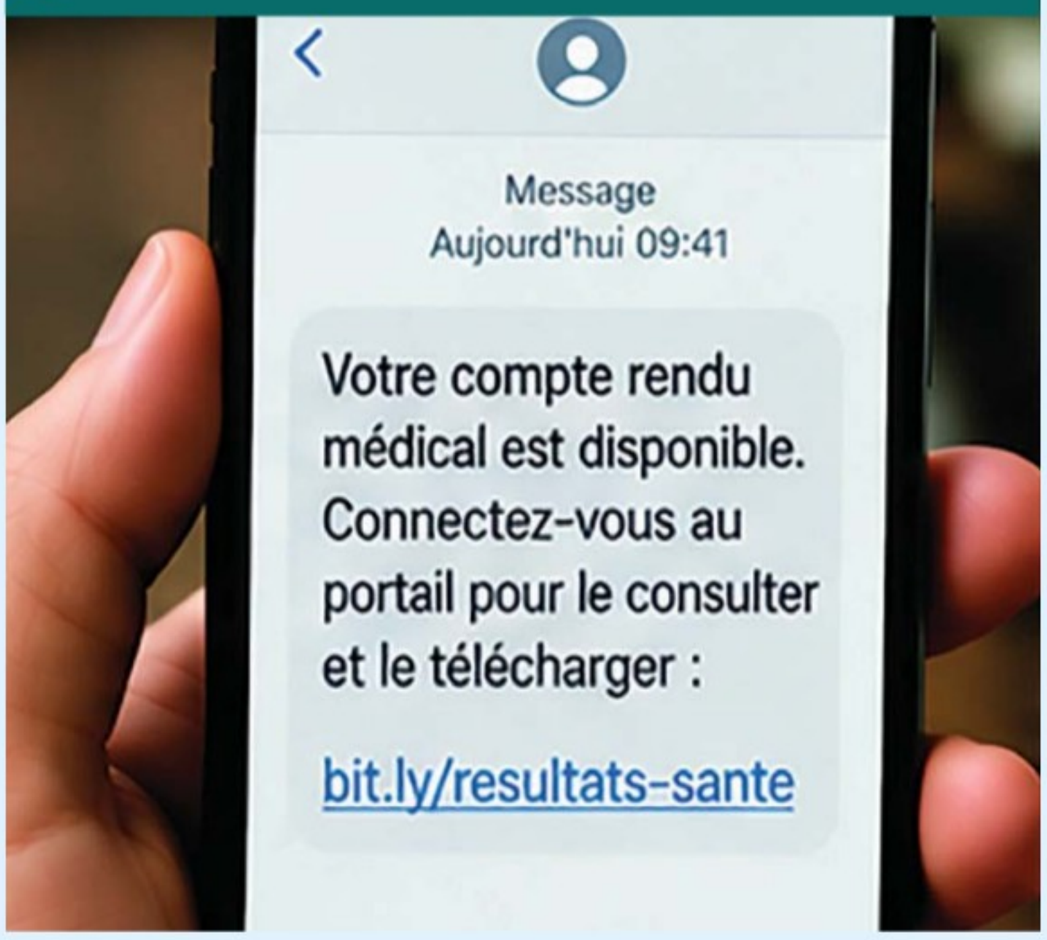
### OTP

Acronyme de *One-Time Password*, c'est-à-dire « mot de passe à usage unique ». Il s'agit d'un code temporaire utilisé pour vérifier une identité ou autoriser certaines opérations. Précisément parce qu'il peut être nécessaire pour finaliser une connexion ou une transaction, un OTP ne doit jamais être communiqué à un tiers. Un SMS frauduleux peut chercher à convaincre la victime de le transmettre directement à l'attaquant.

### MFA / AUTHENTIFICATION MULTIFACTEUR

Il s'agit d'un système qui exige plusieurs éléments pour vérifier l'identité d'un utilisateur. Il peut par exemple associer un mot de passe à un code temporaire ou à un dispositif d'authentification. La MFA réduit le risque de compromission, mais n'élimine pas toutes les attaques : le *smishing* peut précisément chercher à convaincre la victime de communiquer ce second facteur.

## 6 LE FAUX COMPTE RENDU MÉDICAL À TÉLÉCHARGER

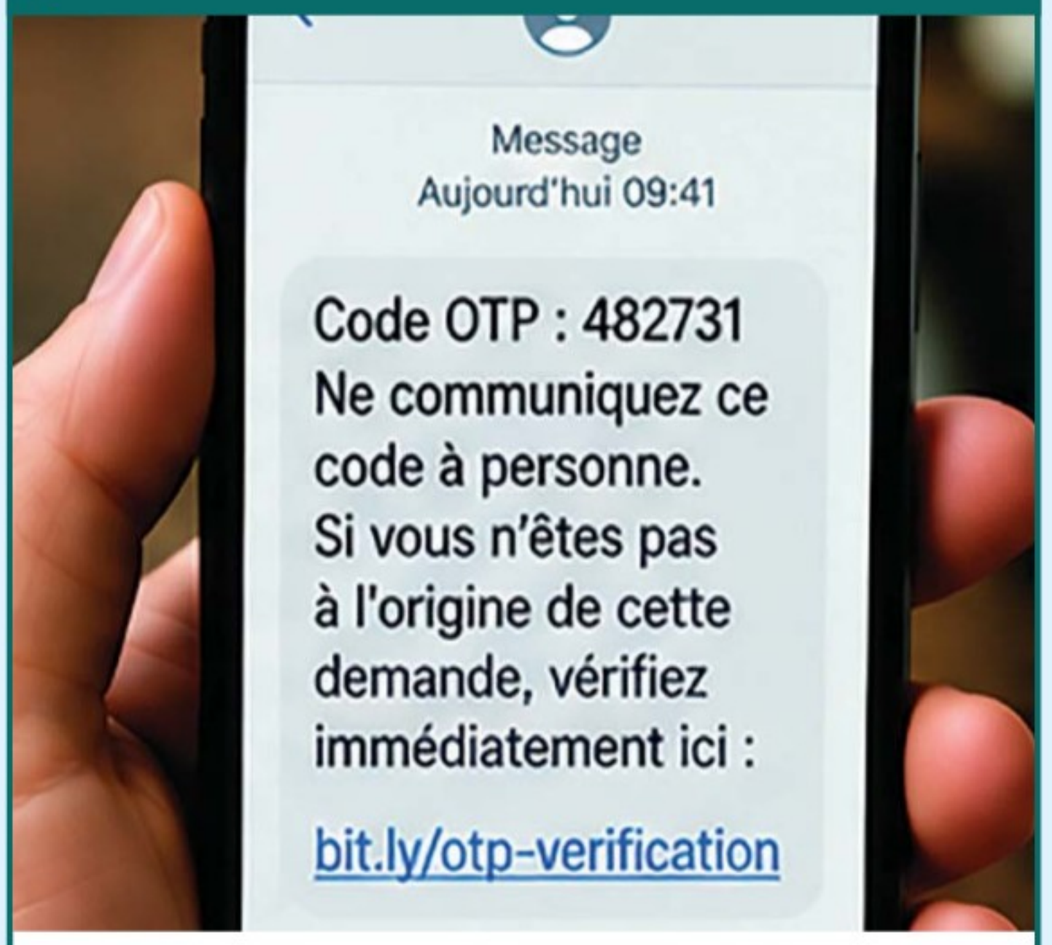



Parmi les pièges les plus efficaces figure également celui qui touche à la santé. Un SMS évoquant un compte rendu médical, des frais de santé ou des résultats d'examen touche immédiatement un point sensible et rend le clic plus probable. La personne qui le reçoit pense à un examen ou à une consultation, et non à une arnaque. L'attaquant exploite précisément cette charge émotionnelle pour pousser l'utilisateur à agir sans vérifier. Le lien renvoie vers une page qui imite le portail d'un établissement de santé ou d'un service public et récupère des données personnelles, des identifiants ou des informations de paiement. Chaque information communiquée peut ensuite être réutilisée dans d'autres fraudes.

### COMMENT SE PROTÉGER

La défense, ici aussi, est plus simple qu'il n'y paraît : un véritable compte rendu médical se consulte sur un véritable portail, et non via un lien reçu par SMS.
Lorsque le message touche à un sujet sensible, la prudence doit augmenter, et non diminuer. C'est précisément sur ce réflexe émotionnel que repose toute l'opération frauduleuse.

## 7 LE FAUX CODE OTP




Cette arnaque est particulièrement habile parce qu'elle exploite un mécanisme bien réel : le code OTP. Le SMS signale une connexion suspecte ou une tentative d'inscription et invite à agir immédiatement, par exemple en cliquant sur un lien ou en effectuant une fausse vérification.
La victime pense se protéger, mais elle est en réalité en train d'aider l'attaquant.
La référence au code temporaire rend le message crédible, car nous l'utilisons aujourd'hui pour les banques, les applications et les paiements. Mais dans ce cas, l'OTP ne sert pas à protéger le compte : c'est la clé que l'escroc cherche à obtenir pour finaliser la connexion.

### COMMENT SE PROTÉGER

Une règle est absolue : un code de vérification ne doit être communiqué à personne, transféré à personne ni saisi sur une page ouverte à partir d'un lien reçu par SMS. Il s'agit d'un élément d'authentification temporaire et, précisément pour cette raison, il possède une valeur considérable. Le communiquer revient à fournir à quelqu'un un accès presque prêt à l'emploi.

## 8 LE PRIX QUE VOUS N'AVEZ JAMAIS GAGNÉ




Les arnaques qui promettent des prix, des bons d'achat ou des avantages inattendus continuent de fonctionner parce qu'elles jouent sur l'espoir d'obtenir quelque chose avec peu ou pas d'effort. Le message se présente comme une bonne nouvelle et, précisément pour cette raison, il est moins souvent vérifié. Pour recevoir le prix, il suffirait de confirmer des informations, de payer une petite somme ou de suivre une procédure. En réalité, ce n'est qu'un prétexte pour collecter des données personnelles, des coordonnées ou des informations de paiement. Ici, le smishing ne joue pas sur la peur, mais sur l'enthousiasme. Et c'est justement cette apparente légèreté qui le rend efficace.

### COMMENT SE PROTÉGER

La bonne question est toujours la même : où cette promotion apparaît-elle réellement ? Si le prix est authentique, il sera mentionné sur les canaux officiels de la marque, de l'opérateur ou du service concerné. S'il n'existe que dans le SMS, il est très probablement fictif. Et si, pour recevoir un cadeau, on vous demande d'utiliser votre carte bancaire, alors le véritable cadeau, pour quelqu'un, c'est probablement vous.

## 9 « JE VOUS AI ENVOYÉ UN CODE PAR ERREUR »




Parmi les arnaques les plus habiles figure celle qui se fait passer pour une simple erreur humaine. Quelqu'un vous écrit en affirmant avoir reçu par erreur un code sur votre numéro et vous demande de lui transférer. Le ton est courtois, presque gêné.

Cela ressemble à un service anodin. En réalité, ce code sert à enregistrer ou à activer un compte en utilisant votre numéro. Le partager revient à permettre à l'attaquant de prendre le contrôle du profil ou à effectuer la vérification à sa place.

Ce stratagème est fréquent sur WhatsApp et Telegram, mais peut également toucher d'autres services.

Sa force repose entièrement sur une demande qui semble insignifiante.

### COMMENT SE PROTÉGER

La règle est claire : un code de vérification ne doit jamais être communiqué à qui que ce soit. Peu importe à quel point l'explication semble plausible.

Peu importe à quel point le message paraît courtois. Ce code est un jeton d'accès temporaire et le simple fait que quelqu'un vous le demande doit déclencher l'alerte !



# 10 LE FAUX PATRON ET LE FAUX CONTACT



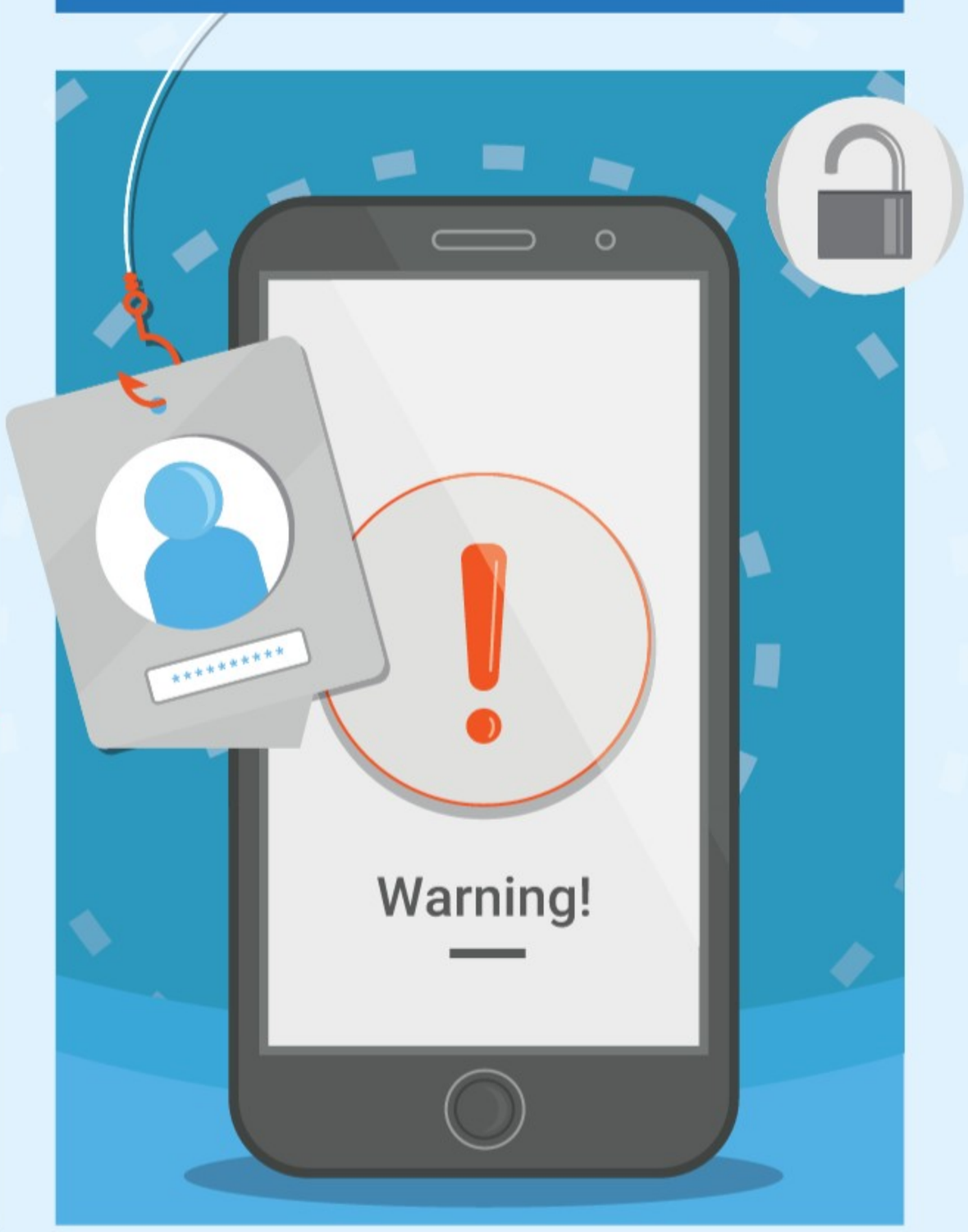

Toutes les arnaques par SMS ne reposent pas sur l'usurpation du nom d'une banque ou d'un organisme. Certaines s'attaquent directement à la confiance en se faisant passer pour un supérieur, un collègue ou un simple contact. Le message peut ressembler à une erreur, à une demande urgente ou au début d'une conversation parfaitement normale. En réalité, il s'agit d'une technique de manipulation précise. Dans le cas du faux patron, l'objectif est d'obtenir immédiatement de l'argent, des codes ou des documents. Avec le faux contact, en revanche, l'arnaque progresse plus lentement, en créant une relation de confiance avant de formuler la demande. Le principe reste le même : ce n'est pas l'appareil qui est attaqué, mais la relation. L'arnaqueur exploite l'autorité, la familiarité et le contexte pour abaisser les défenses de sa victime.

## COMMENT SE PROTÉGER

**De nombreuses victimes n'ont pas l'impression d'avoir été escroquées : elles pensent simplement avoir répondu à quelqu'un. Et c'est précisément là que réside le piège. Si un message demande de l'argent, des codes ou des documents, quittez la conversation et vérifiez la demande par un autre moyen.**

## COMMENT RECONNAÎTRE UN SMS-PIÈGE ?

**Même lorsque la marque, le prétexte ou le ton du message changent, les indicateurs techniques sont presque toujours les mêmes. Une demande urgente, un problème à résoudre rapidement, un lien qui redirige vers un site extérieur aux canaux officiels et une page conçue pour imiter un véritable service. Viennent ensuite les demandes de données : identifiants, coordonnées bancaires, IBAN, documents, codes OTP ou autres codes temporaires. Un détail revient souvent : le montant dérisoire. Deux euros pour une livraison, trois euros pour un péage, quelques secondes pour « tout régler ». C'est une tactique : abaisser le niveau de méfiance et rendre la fraude compatible avec les gestes du quotidien.**





# MYTHES DÉMYSTIFIÉS

# VOS DONNÉES VALENT PLUS QUE VOUS NE LE PENSEZ

**Vous pensez ne pas être assez intéressant pour attirer l'attention un cybercriminel ? Des données apparemment banales peuvent être agrégées, revendues, utilisées pour dérober des comptes ou transformer des PC, des smartphones et des appareils IoT en nœuds de botnet.**

Il n'est pas nécessaire d'être célèbre, riche ou administrateur système pour devenir une ressource utile à un attaquant.

Une adresse e-mail, un mot de passe réutilisé, une photo contenant des informations de localisation, un routeur oublié ou un appareil qui n'est plus mis à jour peuvent avoir de la valeur lorsqu'ils sont combinés à d'autres données. Dans ces pages, nous déconstruisons les idées reçues et voyons comment réduire concrètement notre surface d'attaque.



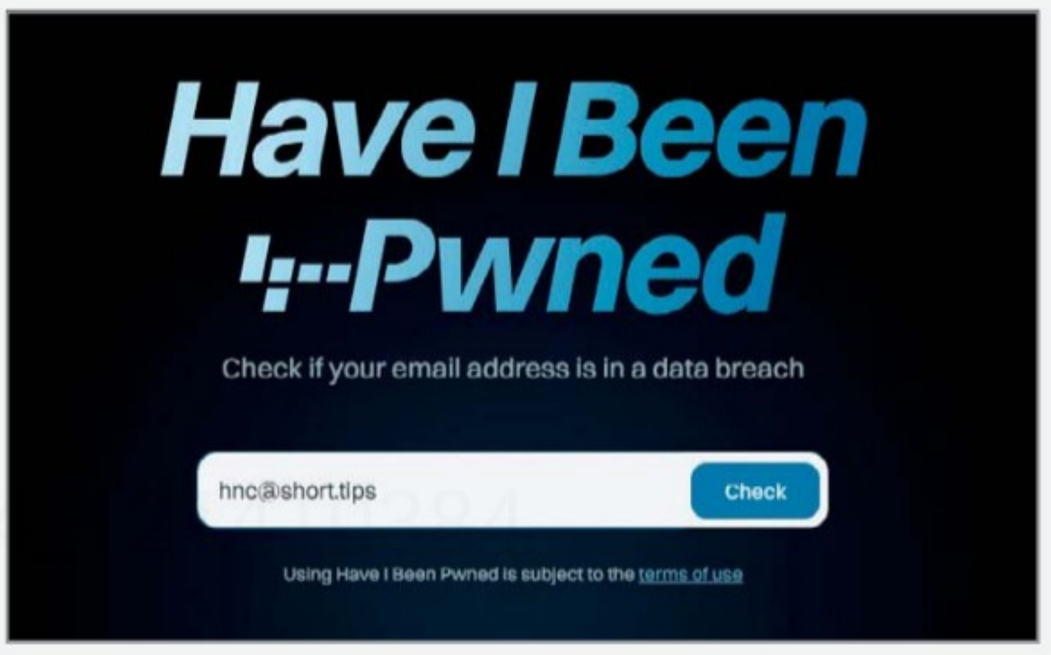

#1 Privacy Badger (https://privacybadger.org/fr/) : cette extension de l'Electronic Frontier Foundation bloque automatiquement de nombreux traqueurs invisibles.

## #1 JE N'AI RIEN À CACHER : POURQUOI DEVRAIS-JE PROTÉGER MES DONNÉES ?

Ne rien avoir à cacher ne signifie pas ne rien avoir à protéger. Nom, adresse e-mail, numéro de téléphone, habitudes, localisation et identifiants peuvent être combinés pour établir un profil, tenter une usurpation d'identité ou rendre une attaque d'ingénierie sociale plus crédible. La FTC, la Federal Trade Commission, explique notamment comment (https://short.tips/url/5l2) les courtiers en données collectent des informations provenant de nombreuses sources et les combinent. La vie privée ne sert pas à cacher un crime : elle permet de garder le contrôle des informations qui nous concernent (https://short.tips/url/5l1).

## #2 UN CYBERCRIMINEL PEUT-IL GAGNER DE L'ARGENT AVEC LES DONNÉES D'UN UTILISATEUR ORDINAIRE ?

Les données d'un utilisateur ordinaire peuvent avoir de la valeur précisément parce qu'elles sont nombreuses et qu'il est possible de les combiner. Une adresse e-mail peut être associée à des profils publics, des achats, des numéros de téléphone ou des comptes compromis ; un identifiant volé peut quant à lui devenir la clé permettant d'accéder à d'autres services. Europol (https://short.tips/url/5l5) signale que les violations de données alimentent les fraudes et les extorsions, tandis que la FTC décrit des marchés où les informations personnelles sont collectées, agrégées et partagées. La valeur provient donc souvent de l'ensemble.

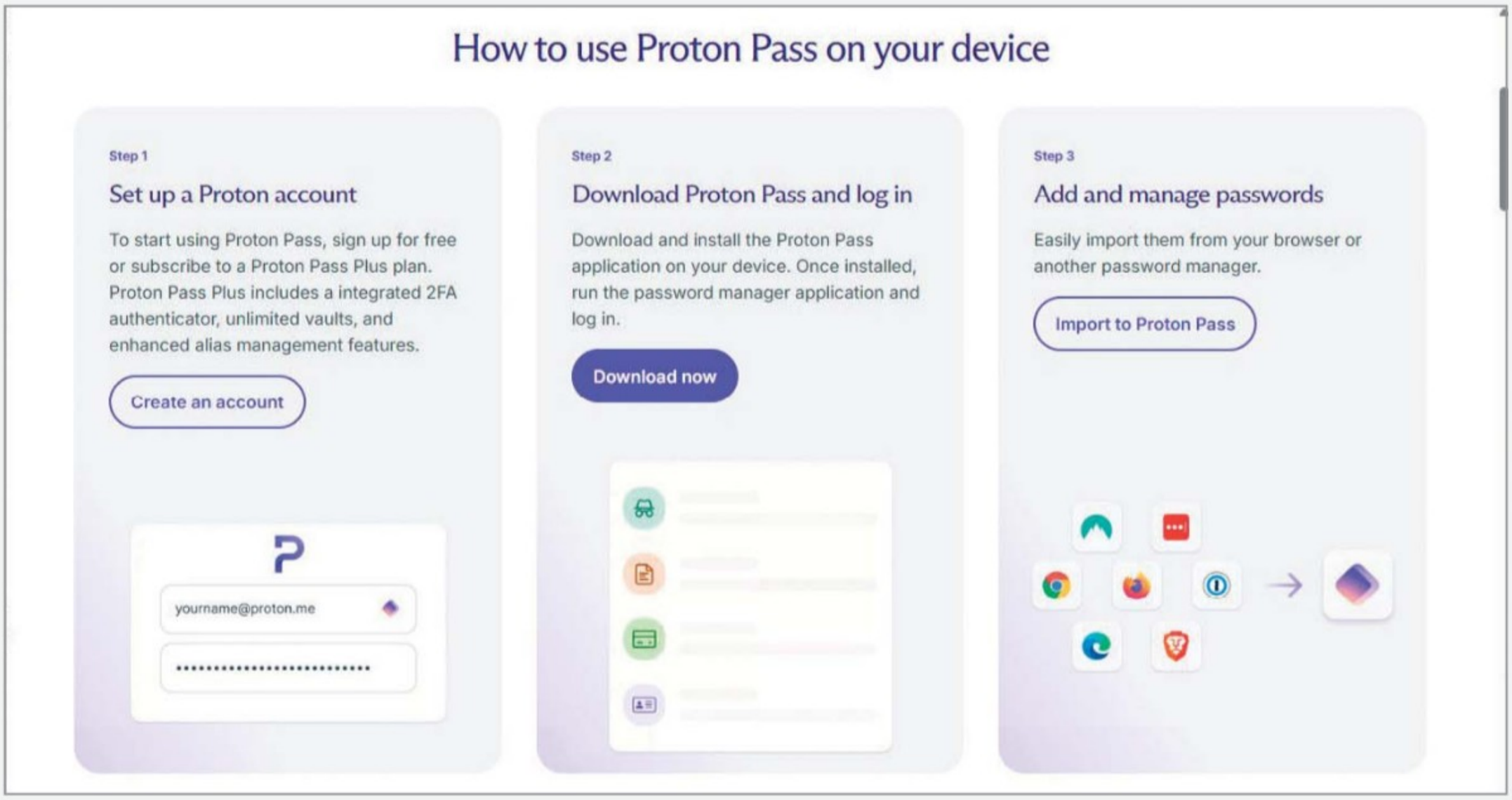



#2 Have I Been Pwned (https://short.tips/url/haveibeenpwned) vérifie si une adresse e-mail apparaît dans des violations de données connues.

## #3 UN ANCIEN COMPTE PRÉSENTE-T-IL ENCORE UN INTÉRÊT POUR UN ATTAQUANT ?

Un compte oublié ne devient pas automatiquement inutile. S'il contient un mot de passe réutilisé, des informations personnelles, des contacts ou un accès à des services associés, il peut devenir un point de départ pour d'autres tentatives. La FTC a documenté des cas dans lesquels des identifiants exposés lors d'une précédente violation ont été réutilisés pour accéder à d'autres systèmes. Même un ancien compte peut donc contenir une pièce du puzzle numérique recherchée par un attaquant.

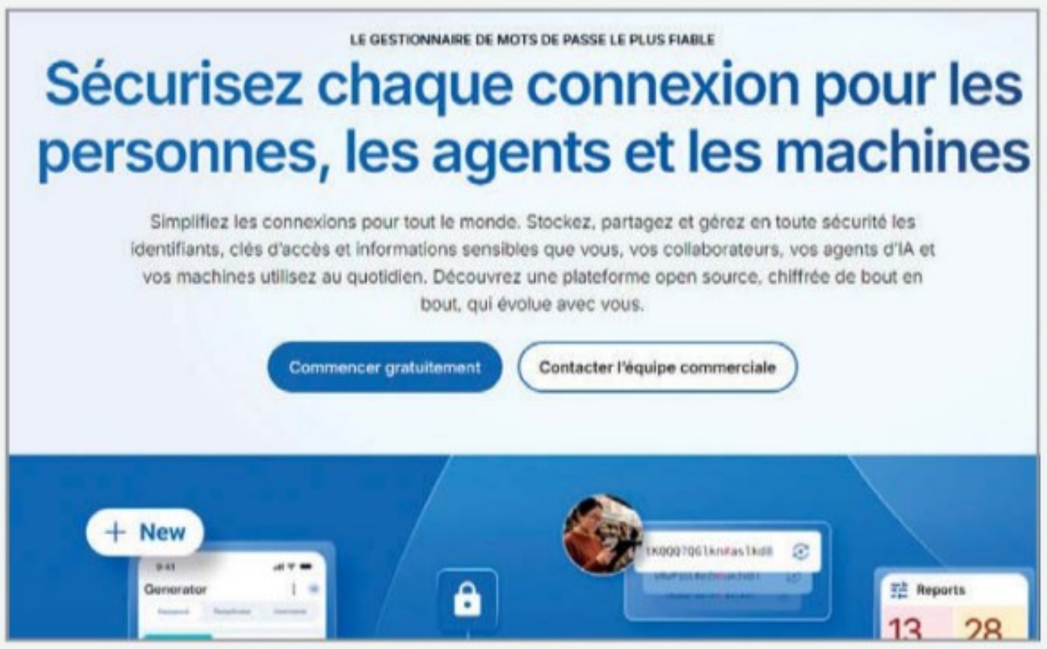
# Sélection




#4 Proton Pass (https://short.tips/url/5l8) gère des mots de passe uniques et propose également des alias pour protéger votre adresse e-mail.

## #4 SI SEUL MON E-MAIL EST VOLÉ, LES DÉGÂTS SONT-ILS VRAIMENT LIMITÉS ?

Une adresse e-mail ne signifie pas à elle seule qu'un compte a été compromis, mais elle constitue un excellent identifiant. Elle peut être utilisée pour des campagnes de phishing, des tentatives d'accès automatisées, des procédures de récupération frauduleuses ou pour relier des informations provenant d'autres fuites de données. OWASP décrit le credential stuffing comme l'utilisation automatisée de couples d'identifiants volés sur d'autres services. C'est pourquoi une simple adresse e-mail devient beaucoup plus précieuse lorsqu'elle est associée à des mots de passe, des numéros de téléphone ou d'autres données.




#5 Bitwarden (https://bitwarden.com/fr-fr/) génère et stocke des identifiants longs, robustes et uniques.

## #5 UN MOT DE PASSE RÉUTILISÉ PEUT-IL AGGRAVER LES CONSÉQUENCES D'UNE FUITE DE DONNÉES ?

C'est l'un des problèmes les plus exploités lors des violations. Si le même mot de passe est utilisé sur plusieurs services, la compromission d'un seul compte peut fournir aux attaquants une combinaison à tester ailleurs. OWASP décrit précisément ce mécanisme sous le nom de credential stuffing ; la FTC a documenté un cas dans lequel un mot de passe déjà exposé a contribué à la compromission d'une base de données contenant les données de millions d'utilisateurs. Des mots de passe uniques permettent donc de limiter considérablement l'impact d'une fuite de données.

## #6 SI JE CHANGE MON MOT DE PASSE APRÈS UNE VIOLATION, LE PROBLÈME EST-IL RÉSOLU ?

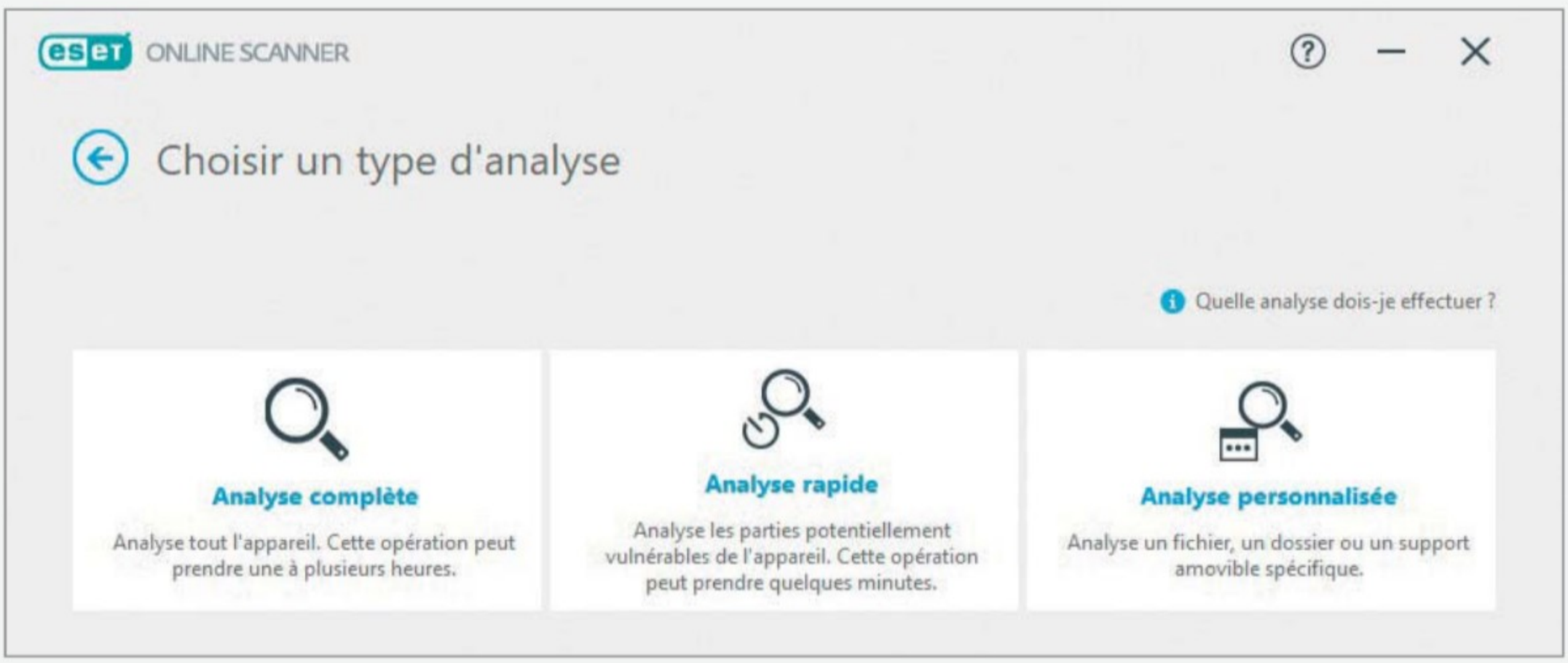
Changer le mot de passe compromis est essentiel, mais cela ne suffit pas toujours. Il faut vérifier où ce même mot de passe, ou une variante, a été réutilisé et le remplacer également sur ces services. Il est aussi recommandé de vérifier les sessions actives, de mettre à jour les méthodes de récupération et d'activer l'authentification à deux facteurs. La FTC recommande de modifier immédiatement les mots de passe concernés par une violation ainsi que ceux réutilisés sur d'autres services. La bonne réponse (https://short.tips/url/5l9) consiste donc à effectuer une véritable remise à zéro de l'ensemble de son périmètre numérique.

## #7 MON PC PEUT-IL REJOINDRE UN BOTNET SANS QUE JE M'EN APERÇOIVE ?

Un ordinateur infecté peut être transformé en nœud d'un botnet à l'insu de son propriétaire. Le malware peut fonctionner en arrière-plan, recevoir des commandes et utiliser la connexion pour envoyer du spam, mener des attaques ou effectuer d'autres activités. Europol définit les botnets comme des réseaux d'appareils infectés contrôlés par des cybercriminels ; la FTC a documenté des cas d'ordinateurs domestiques transformés en véritables « zombies ». Des ralentissements, un trafic inhabituel ou des comportements anormaux ne suffisent pas à prouver une infection, mais ils méritent d'être vérifiés.

## #8 UN BOTNET CONCERNE-T-IL UNIQUEMENT LES ORDINATEURS PUISSANTS OU LES SERVEURS D'ENTREPRISE ?

Un botnet n'a pas besoin de machines puissantes. Sa force réside dans le nombre : des milliers, voire des millions d'appareils ordinaires peuvent être coordonnés pour produire un effet bien plus important. L'ENISA explique qu'un botnet est un réseau d'appareils infectés et contrôlés à distance ; la FTC rappelle que des ordinateurs, des téléphones et des appareils connectés peuvent en faire partie. Pour un cybercriminel, un vieux PC domestique peut donc avoir de la valeur non pas pour sa puissance, mais pour sa présence en ligne.




#7 ESET Online Scanner (https://short.tips/url/esetonline) permet d'effectuer gratuitement des analyses périodiques à la recherche de malwares.

# Sélection

## #9 LES ROUTEURS ET LES APPAREILS IOT PEUVENT-ILS DEVENIR DES OUTILS CRIMINELS ?

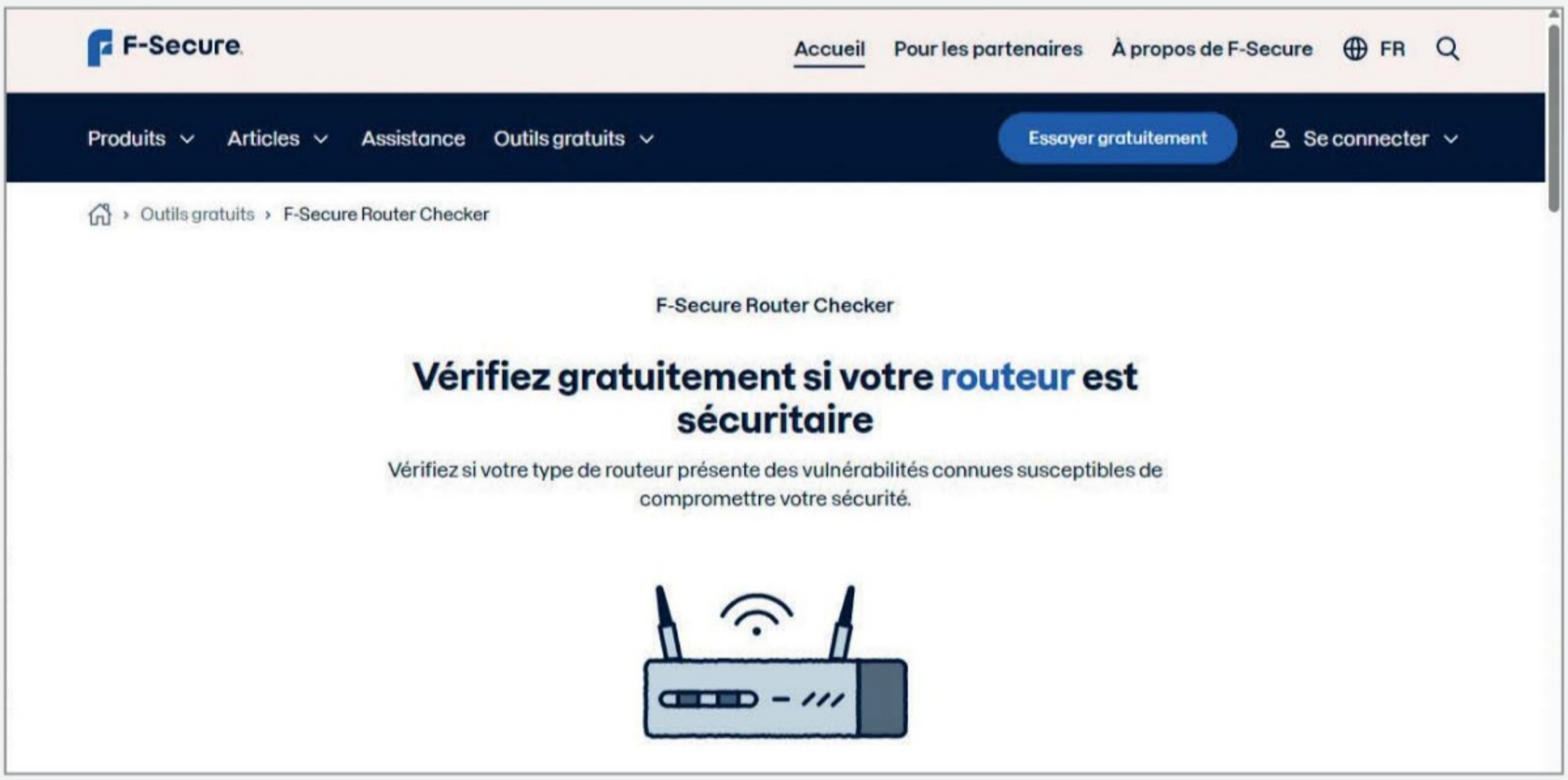
Les caméras, routeurs, téléviseurs et autres appareils connectés peuvent être exploités lorsqu'ils présentent des vulnérabilités ou utilisent des identifiants faibles. Le cas de Mirai a montré à quelle vitesse un grand nombre d'appareils IoT pouvait être transformé en botnet. Plus récemment, le FBI a signalé que des routeurs obsolètes avaient été compromis et utilisés pour créer des réseaux proxy. Mettre à jour le firmware, désactiver l'administration à distance lorsqu'elle n'est pas nécessaire et remplacer les appareils qui ne sont plus pris en charge permet de réduire les risques.

## #10 SI L'APPAREIL FONCTIONNE NORMALEMENT, CELA SIGNIFIE-T-IL QU'IL EST SAIN ?

Pas nécessairement. Un malware peut chercher à rester discret précisément pour éviter d'attirer l'attention. Un appareil compromis peut continuer à fonctionner presque normalement tout en envoyant des données, en communiquant avec un serveur de commande ou en étant utilisé comme élément d'une infrastructure criminelle. Europol décrit des malwares capables de prendre le contrôle d'ordinateurs et d'appareils mobiles afin de dérober des informations. L'absence de symptômes visibles ne constitue donc pas une preuve de sécurité : les mises à jour et les contrôles restent essentiels.

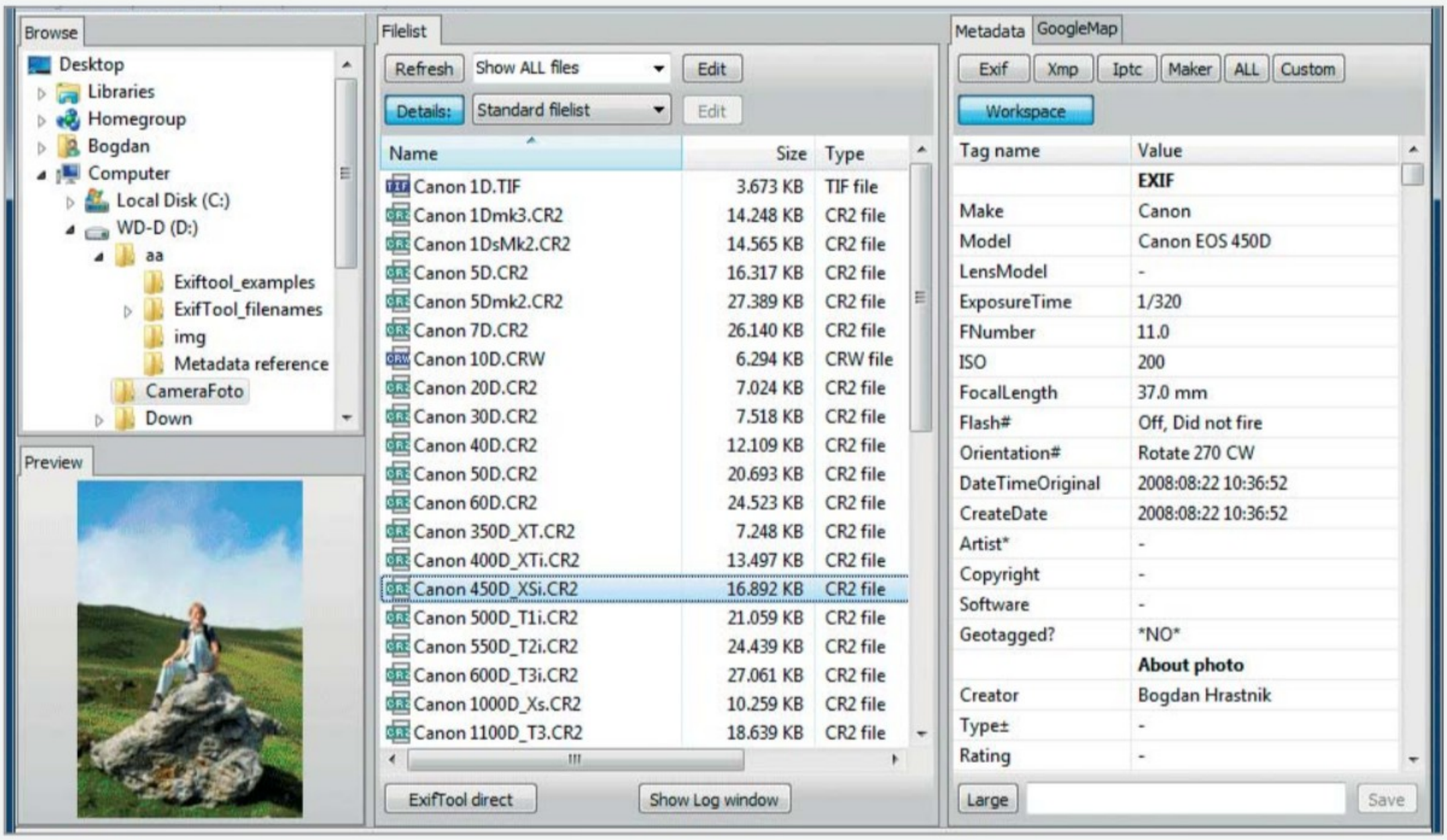
## #11 LES PHOTOS PUBLIÉES EN LIGNE PEUVENT-ELLES FOURNIR DES INFORMATIONS UTILES AUX CRIMINELS ?

Une photographie peut contenir davantage d'informations que celles visibles à l'œil nu. Selon l'appareil et les réglages utilisés, le fichier peut conserver des métadonnées telles que la date, le modèle de l'appareil photo et, dans certains cas, les coordonnées GPS. Publier une image peut également révéler des détails sur l'environnement, le domicile ou les habitudes. Cela ne signifie pas que chaque photo expose




#9 Vérifiez les vulnérabilités connues associées au modèle de votre routeur avec F-Secure Router Checker (https://short.tips/url/chkrouter) en indiquant sa marque et son modèle.

**#11** ExifTool (https://short.tips/url/exiftool et https://short.tips/url/exiftoolgui) permet de découvrir quelles données sont enregistrées dans vos photos.




automatiquement des informations sensibles, mais avant de partager des images, il est utile de vérifier quelles données accompagnent le fichier et quels détails peuvent être identifiés.

## #12 UNE APPLICATION GRATUITE PEUT-ELLE COLLECTER DES DONNÉES QUI NE ME SERVENT À RIEN ?

Gratuite ne signifie pas automatiquement dangereuse, mais pas non plus inoffensive. Une application peut demander l'accès à la localisation, au microphone, à l'appareil photo, aux contacts ou à d'autres données nécessaires - ou non - à son fonctionnement. Android met à disposition des autorisations et un tableau de bord permettant de contrôler quelles applications accèdent aux données sensibles. Le mythe à déconstruire est donc double : toutes les applications gratuites ne collectent pas nécessairement toutes vos données, mais accorder chaque autorisation sans la vérifier réduit considérablement le contrôle que vous exercez sur votre vie privée.

## #13 LE FINGERPRINTING EST-IL VRAIMENT EFFICACE SI JE BLOQUE LES COOKIES ?

Bloquer les cookies ne vous rend pas automatiquement invisible. Le fingerprinting peut combiner différentes caractéristiques du navigateur et de l'appareil - par exemple le système d'exploitation, les paramètres, la taille de l'écran et d'autres propriétés - afin de créer une empreinte numérique plus difficile à neutraliser avec les seuls cookies. Mozilla documente cette technique ainsi que les protections intégrées à Firefox (**https://short.tips/url/5lg**). La confidentialité du navigateur repose donc sur un ensemble de mesures : cookies, traqueurs, fingerprinting, autorisations et paramètres doivent être considérés dans leur ensemble.

# Sélection




**#14 Sur https://short.tips/url/5lh, vous trouverez une vidéo sympathique qui permet de comprendre les principes de base pour naviguer en toute sécurité sur les réseaux Wi-Fi publics.**

## #14 UN RÉSEAU WI-FI PUBLIC EST-IL SÛR SI LE SITE UTILISE HTTPS ?

HTTPS protège les communications entre l'appareil et le site, mais ne rend pas un réseau Wi-Fi public sûr dans toutes les situations. La FTC rappelle qu'aujourd'hui, la plupart des sites utilisent le chiffrement, ce qui réduit bon nombre des risques autrefois associés aux réseaux ouverts ; il reste toutefois important de vérifier le site, d'éviter les réseaux suspects et de ne pas négliger les autres problèmes de sécurité. HTTPS constitue une couche de protection, pas un laissez-passer permettant de faire automatiquement confiance à n'importe quel point d'accès.

## #15 AVEC L'AUTHENTIFICATION MULTIFACTEUR, SUIS-JE DÉSORMAIS À L'ABRI ?

L'authentification multifacteur réduit considérablement le risque de compromission, mais elle ne rend pas un compte invulnérable. Certaines méthodes résistent mieux au phishing que d'autres, et un attaquant peut toujours tenter de voler des sessions, de convaincre l'utilisateur de lui transmettre des codes ou d'exploiter d'autres failles. Le NIST distingue clairement les authentificateurs résistants au phishing des simples codes saisis manuellement. Lorsqu'elle est disponible, une clé d'accès (passkey) ou une méthode résistante au phishing offre une protection plus robuste.


INFORMATIQUE HACK& CRACK

Numéro 51 - Trimestriel - octobre/décembre 2026
**ISSN en cours**

**SPREA S.p.A.** Fondée en 1993 par Mario Sprea
Siège social : Via Torino, 51
20063 Cernusco Sul Naviglio (Milan) - Italie - P.I. 12770820152

**Conseil d'administration** Luca Sprea (Président), Alessandro Agnoli (PdG), Mario Sprea, Giulia Spreafico, Stefano Pernarella

**COORDINATION** Federico Sacco, Marianne Auzanet

**Conception graphique et réalisation éditoriale :**
**Backdoor Srls - www.backdoor.media**
Gianmarco Bruni - CEO & Founder
Carmelo Ramundo - Product Manager
Francesca Sardano - Conception graphique et mise en page
Valentina Oliva - Responsable des Affaires Générales et Juridiques

**DISTRIBUTION** - MLP
**COMMISSION PARITAIRE** - En cours
**IMPRESSION**
Boccia Industria Grafica S.p.A.
Via Tiberio Claudio Felice, 7
84131 Salerno, Italie

**DIRECTEUR GÉNÉRAL** Luca Sprea

**ÉDITEUR EN CHEF** Alessandro Agnoli

**PUBLICITÉ, PROJETS SPÉCIAUX ET ÉVÉNEMENTS**
**Secrétariat** Emanuela Mapelli
Tel. +39(0)2 92432244
emanuelamapelli@sprea.it

**DROITS POUR L'ÉTRANGER**
Paolo Cionti - Tel. +39(0)2 92432253
paolocionti@sprea.it



**©2026 Sprea S.p.A.**



**ÉDITIONS SPREA**
**Périodiques de qualité depuis 1993**

Sprea FRANCE

# CALENDRIERS-AGENDA 2027

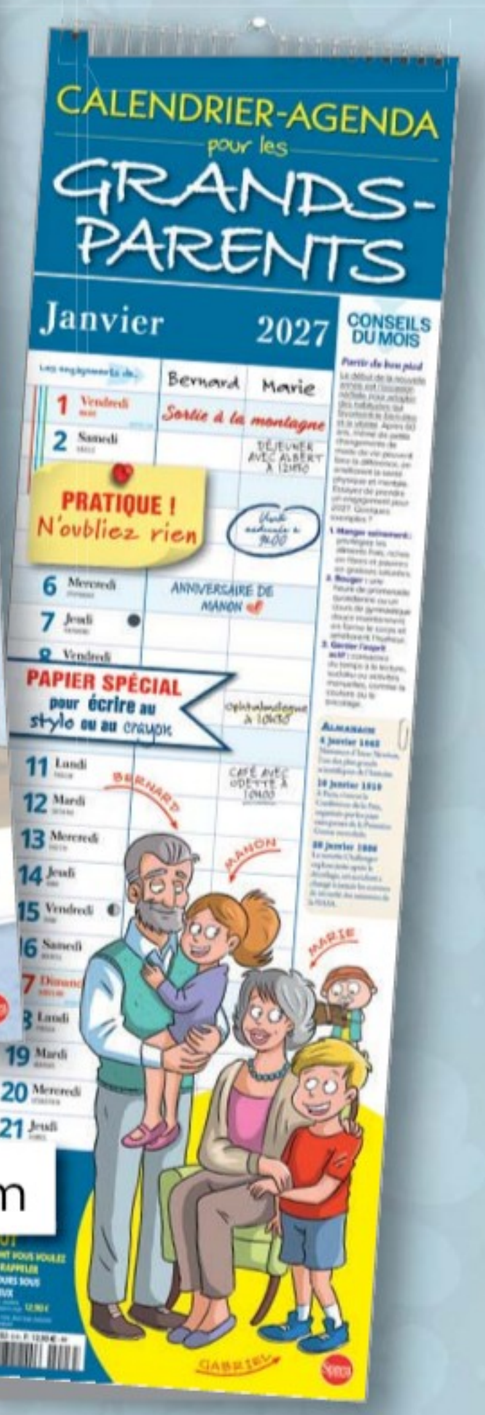
*en kiosque et sur* sprea.fr/calendriers

*Parfait pour Noël !*
Un cadeau qui dure toute l'année




30 x 42,5 cm




15 x 50 cm

*PAPIER SPÉCIAL pour écrire au stylo et au crayon*



PEFC
PEFC/18-32-178
Certifié PEFC
Ce produit est issu de forêts gérées durablement, de sources recyclées et contrôlées
www.pefc.it

- *Papier spécial* parfait pour stylo et crayon
- *Beaucoup d'espace* pour les notes de tout la famille
- *Informations utiles* tous les mois

Scannez le QR Code

# HACK& CRACK

NOUVELLE FORMULE !

## DANS CE NUMÉRO



### Ce que cache votre smartphone
**DÉCOUVREZ LES FICHIERS ET DONNÉES INVISIBLES QUI RÉVÈLENT CE QUE CONTIENT VOTRE MOBILE.**



### Réseaux Wi-Fi autour de vous
**EXPLOREZ LA CARTE DE WIGLE ET DÉCOUVREZ LES RÉSEAUX SANS FIL QUI VOUS ENTOURENT.**



### Vos données valent plus que vous ne le pensez !
**E-MAILS, MOTS DE PASSE ET PHOTOS : DÉCOUVREZ CE QUE LES PIRATES EXPLOITENT.**



### L'IA contre les arnaques !
**AVAST ONE ANALYSE VOS MESSAGES POUR REPÉRER LE PHISHING ET LES ESCROQUERIES**

BEL : 5,90 € - CH : 9,90 CHF - DOM : 6€ - MAR : 59 DH -
N CAL : 780 XPF - POL : 830 XPF - CAN : 7,99 $ CAD

Sprea FRANCE

L 13749 - 51 - F: 5,50 € - RD*