N°60

Casser les codes et décrypter l'info

Mai / Juillet 2024

PIRATE INFORMATIQUE

ANONYMAT

TAILS 6.0 : L'ARME ANTI-SURVEILLANCE N°1

HACKING

USURPATION DE TÉLÉPHONE : QUI M'APPELLE ?!

LE GUIDE PRATIQUE DU PIRATE

REDLINE

LE VOLEUR DE MOTS DE PASSE QUI SÉVIT SUR YOUTUBE

PROTECTION

BLINDEZ VOTRE PC CONTRE LES RANSOMWARES

BLACK DOSSIER

HACKS & CRACKS

LES 30 MEILLEURS OUTILS GRATUITS

SOMMAIRE

BLACK DOSSIER

13–23

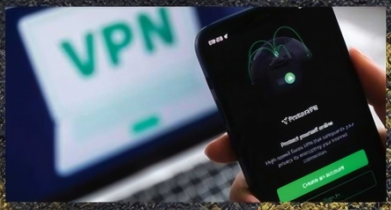
LA TROUSSE À OUTILS DU HACKER

Les 30 MEILLEURS LOGICIELS **100% GRATUITS**

ÉDITION 2024

HACKING

ANONYMAT



SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'ayant téléchargé illégalement ? C'est de bonne guerre, nous sommes pour le partage ! Merci de l'intérêt que vous portez à nos articles, mais pour que nous puissions continuer l'aventure, pensez à acheter le magazine : offrez-le, parlez-en autour de vous ! *Pirate Informatique* existe depuis plus de 10 ans, sans publicité et sans hausse de prix !

PROTECTION

MULTIMÉDIA

PIRATE INFORMATIQUE
N°60
Mai – Juillet 2024

Une publication du groupe ID Presse
Impasse de l'Espéron - Villa Miramar
13960 Sausset Les Pins

Directeur de la publication :
David Côme

Directeur artistique :
Sergei Afanasiuk

Service Abonnement :
Indiquez la référence *Pirate Informatique* dans vos échanges
Tél. : 03 44 51 97 21
Email : abonnement.bii@gmail.com

Imprimé en France par / Printed in France by :
Mordacq Impression
Rue de Constantinople
62120 Aire-sur-la-Lys
France

Distribution : MLP
Dépôt légal : à parution
Commission paritaire : en cours
ISSN : 1969 - 8631

«Pirate Informatique» est édité par SARL ID Presse, RCS Aix-En-Provence 491 497 665

Parution : 4 numéros par an.

ÉDITO

LA POLITIQUE DES PETITS PAS EN MARCHE

Le gouvernement français vient de faire adopter la loi SREN (Sécurisation et Régulation de l'Espace Numérique) au parlement. Sur le papier, les politiques français sont censés reprendre le contrôle d'Internet, territoire perdu de la République. En vrai, puisque ce n'est pas possible, l'État lance simplement quelques jalons, définit quelques armes et stratégies de reconquête... Il réfléchira à l'effectivité incertaine des mesures ensuite. Certains disent que c'est mieux que rien, d'autres que les nombreuses imprécisions et flous que sous-tend le texte sont le signe d'une reprise en main autoritaire à venir. Et personne ne veut voir l'éléphant au milieu de la pièce : l'anonymat des échanges sera sacrifié à court terme. Parce qu'Internet n'est pas qu'un espace de libertés et de belles utopies. Mais qu'il est aussi devenu le terrain de jeu de tous les médiocres en mal de victimes. Les citoyens ont merdé. L'État en profite.

Bonne lecture !

La rédaction

BITTORRENT

QUEL EST LE FICHIER LE PLUS ANCIEN SUR THE PIRATE BAY ?

The Pirate Bay a fait mieux que survivre aux années 2000. Plus de vingt ans après sa création, en septembre 2003, la plateforme Torrent reste aujourd'hui l'une des principales sources de partage et de piratage dans le monde. Même si la majorité des utilisateurs de The Pirate Bay téléchargent du contenu récent, certains torrents plus anciens parviennent quand même à rester actifs. Il faut pour cela que le lien magnet ou torrent d'origine continue d'être « seedé », c'est-à-dire qu'au moins une copie complète du fichier soit à disposition des autres utilisateurs. L'épisode 2 de la saison 2 de la série télévisée suédoise "High Chaparral" a ainsi récemment célébré son vingtième anniversaire. Selon TorrebntFreak, le fichier de 357,91 MiB a été initialement téléchargé le 25 mars 2004 et plusieurs personnes continuent de le partager aujourd'hui.

Un torrent devenu culte

La capture d'écran contre ne répertorie qu'un seul seeder, mais selon les informations transmises par OpenTrackr.org, il existe quatre seeders avec une copie complète. Au fil des années, le torrent « High Chaparral » est devenu culte parmi un petit groupe de personnes qui continuent probablement à le partager, simplement parce qu'il s'agit du torrent le plus ancien encore existant.

D'autres torrents restent également actifs après deux décennies. Le 31 mars 2004, quelqu'un a par exemple mis en ligne sur The Pirate Bay une copie piratée du documentaire « Revolution OS ». « Revolution OS » couvre l'histoire de Linux, de GNU et du mouvement du logiciel libre, ce qui convenait bien aux premiers fans de Pirate Bay.

C'EST QUI LE CHAMPION ?!

Il existe désormais un "World Cybercrime Index", soit un classement mondial des pays les plus actifs en matière de cyberattaques. Cette première édition a été structurée et compilée par l'Université d'Oxford, sous la houlette du Dr. Miranda Bruce. Cet outil est donc destiné à mesurer l'impact de la cybercriminalité à travers les différentes nations. Il faut noter tout de suite

CYBERCRIME INDEX

Ranking countries by cybercrime threat level

Ranking	Country	WCI score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	United States	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	United Kingdom	9.01
9	Brazil	8.93
10	India	6.13
11	Iran	4.78
12	Belarus	3.87
13	Ghana	3.58
14	South Africa	2.58
15	Moldova	2.57
16	Israel	2.51
17	Poland	2.22
18	Germany	2.17
19	Netherlands	1.92
20	Latvia	1.68

CE QUI VA CHANGER POUR L'INTERNET FRANÇAIS

La loi SREN adoptée, mais pas sereine

La loi SREN (Sécurisation et Régulation de l'Espace Numérique), malgré son adoption début avril, soulève des controverses significatives quant à sa mise en œuvre technique et son impact sur les libertés individuelles. Concoctée pour favoriser « un espace numérique plus sûr et plus protecteur » selon Marina Ferrari, la secrétaire d'État chargée du numérique, cette loi entend redonner de l'autorité au politique face aux grandes plateformes mondialisées. Mais entre autorité et accusations d'autoritarisme, responsabilité et atteintes possibles à la vie privée, marges de manœuvre et flous juridiques, le texte continue de faire débat en dehors de l'hémicycle.

Identification sur les réseaux sociaux : Le projet initial visait à lier les comptes des réseaux sociaux à une identité physique vérifiable, par exemple en utilisant un système de certification de «personne physique». Toutefois, cela pose des problèmes de faisabilité et de respect de la vie privée, car tous les citoyens français ne sont pas obligés de posséder une carte d'identité numérique.

Bannissement des réseaux sociaux : La loi propose des sanctions telles que le bannissement temporaire des réseaux sociaux pour les auteurs d'infractions en ligne (de six mois à un an). Cependant, la mise en œuvre de cette mesure est compliquée, notamment en termes de lier efficacement et équitablement un individu à ses actions en ligne sans empiéter sur les droits individuels.

Contrôle de l'accès aux sites pornographiques : Bien que la loi prescrive un contrôle renforcé de l'accès des mineurs aux sites pornographiques par des systèmes de vérification d'âge, la mise en œuvre pratique reste complexe. Les difficultés incluent la création d'un référentiel technique fiable et respectueux de la vie privée, ainsi que le fait que la responsabilité de l'implémentation est laissée aux plateformes, souvent basées hors de France.

Filtre anti-arnaque : Le projet de loi envisage un système d'alerte pour prévenir l'accès à des sites frauduleux. Cela nécessiterait que les opérateurs télécoms établissent une liste noire de sites, mais la CNIL, l'Arcep et l'Arcom ont émis des réserves sur les risques de restrictions abusives des libertés de communication.

VPN et anonymat : Des amendements proposés pour limiter l'usage des VPN afin de combattre l'anonymat en ligne ont suscité une forte opposition. Bien que certains de ces amendements aient été rejetés, ils reflètent une tendance à vouloir réguler de manière plus stricte l'accès à Internet, ce qui a été comparé au «Grand Firewall» de Chine.

Définitions floues et délits vagues : Le texte inclut des infractions telles que l'outrage en ligne, avec des sanctions pour des contenus jugés offensants ou intimidants. Les critiques arguent que ces définitions sont trop larges et ouvrent la porte à des interprétations subjectives, potentiellement dangereuses pour la liberté d'expression.

que ce n'est pas l'activité cybercriminelle des États qui est classée, mais celle de toutes les composantes d'une nation (secteur public, secteur privé, particuliers).

REFLET DE L'ACTUALITÉ

La Russie, en tête de classement, est suivie de près par l'Ukraine, reflétant ainsi les tensions géopolitiques actuelles et soulignant la guerre informationnelle en cours. La Chine et les États-Unis ne sont pas loin derrière, assumant leur rôle de superpuissances... y compris à l'échelle cybercriminelle. Surprenant pour certains, le Nigeria, souvent associé aux fameuses escroqueries aux "princes nigérians", confirme sa réputation en se plaçant en cinquième position. L'Europe n'est pas en reste, avec la Roumanie menant la danse en se positionnant comme le premier pays européen du classement, suivi par la Pologne, l'Allemagne, et les Pays-Bas. Le Royaume-Uni figure

également en bonne place, nous n'en attendions pas moins de la perfide Albion. La France, conformément à la charte de la Fédération Française de la Loose, n'es bien sûr pas parmi les 20 premières nations du classement. De bon augure avant les JO.

FIND MY DEVICE DE GOOGLE :

LOCALISER SON APPAREIL PLUS PRÉCISÉMENT QUE JAMAIS

Google déploie en ce moment son service Find My Device (Localiser mon appareil). Destiné à localiser beaucoup plus précisément son appareil Android perdu ou volé, il implique aussi un maillage massif de géolocalisations et devra faire la preuve de son innocuité, notamment en matière de stalking.

Find my Device promet de révolutionner la façon dont les utilisateurs d'Android retrouvent leurs appareils perdus ou égarés. Officiellement lancé le 8 avril 2024, le service de géolocalisation de Google étend depuis son maillage sur l'ensemble du globe. Il augmente considérablement les capacités de localisation des appareils Android, les transformant en un réseau de balises de géolocalisation mondial.

UN MAILLAGE INÉGALÉ

Avec plus de trois milliards d'appareils Android à travers le monde, le réseau Find My Device se positionne comme le plus vaste réseau de localisation, dépassant même les capacités du réseau Localiser d'Apple et de Tile (Samsung). Le principe de fonctionnement est simple : utiliser la technologie Bluetooth présente sur la majorité des appareils Android pour permettre à ces derniers de servir de relais dans la localisation des smartphones perdus, des écouteurs, ou même des appareils éteints, comme les Pixel 8, les rendant repérables même sans connexion Internet.

SMARTPHONE ET TRACKERS : ANTIVOLS OU ESPIONS ?

En parallèle de la localisation d'appareils, Google entend bien s'imposer sur le marché des traqueurs Bluetooth, en annonçant des partenariats avec des marques comme Chipolo, Pebblebee, Eufy, et Motorola pour lancer des dispositifs compatibles avec son réseau. Ces traqueurs permettront aux utilisateurs de retrouver non seulement leurs appareils, mais aussi des objets du quotidien comme des clés ou des portefeuilles, grâce à une intégration directe dans l'écosystème Android.
Ces traqueurs inquiètent, car les Airtags de Apple, par exemple, ont souvent été détournés par leurs propriétaires pour surveiller à distance les déplacements d'un proche. Désormais, Apple envoie des notifications sur l'iPhone d'un utilisateur si un airtag est placé à proximité de façon régulière ou prolongée. Google procèdera de même et a même noué un partenariat avec la firme à la pomme pour assurer une meilleure sécurité et prévenir les utilisations malveillantes des traqueurs, telles que le stalking. Grâce à des notifications automatiques alertant les utilisateurs de la présence de traqueurs inconnus à leur proximité, les deux géants technologiques mettent en place un système de sécurité interplateforme.

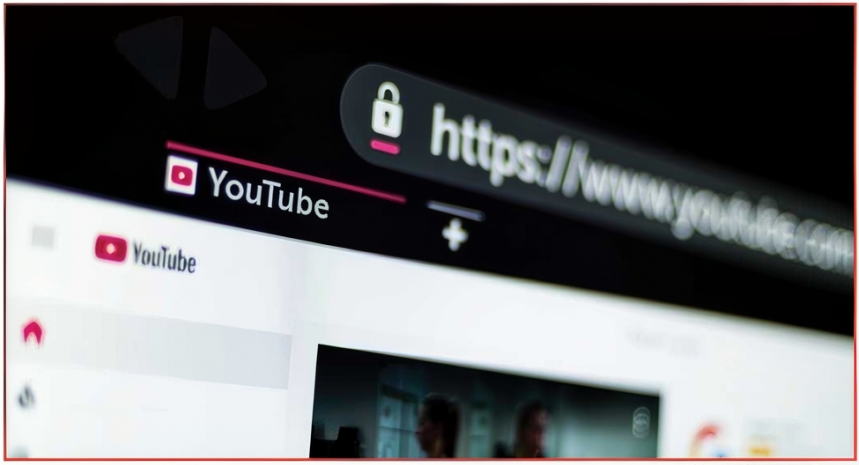
Des balises de type Airtag seront compatibles avec le réseau Find My Device de Google. Utile pour ne plus rien perdre, mais inquiétant quant aux risques de géolocalisation malveillante.

TILE DE SAMSUNG MENACÉ ?

L'arrivée de Find My Device de Google soulève des questions quant à l'avenir des acteurs déjà établis tels que Tile et Samsung. Bien que Tile possède son propre réseau d'accessoires, et que Samsung occupe une part importante du marché Android, l'intégration native de Find My Device dans les appareils Android pose la question de la redondance de leurs services respectifs.

REDLINE, VOLEUR DE MOTS DE PASSE N°1

Une récente étude de Specops met en lumière une augmentation continue du vol de mots de passe (comptes et services en ligne), avec plus de 359 millions de mots de passe volés au cours des six derniers mois. Le principal responsable de cette hécatombe est RedLine, un malware si populaire et efficace qu'il est responsable du vol de près de la moitié de ces mots de passe, soit environ 170 millions d'identifiants. Suivent les malwares Vidar (65 millions d'identifiants), Raccoon Stealer (42 millions), Meta (38 millions) et Cryptbot (16 millions).



RedLine serait responsable de la moitié des vols de mots de passe. YouTube est l'un de ses terrains de jeu favoris.

COMMENT FONCTIONNE-T-IL ?

RedLine a été détecté en mars 2020. Il récupère souvent les données volées vers son infrastructure C2 et peut inclure un mineur de crypto-monnaie, ciblant donc prioritairement les utilisateurs PC avec des GPU élevés (comme les joueurs). Les méthodes de distribution varient, les campagnes d'hameçonnage étant prédominantes, exploitant notamment des plateformes comme YouTube.

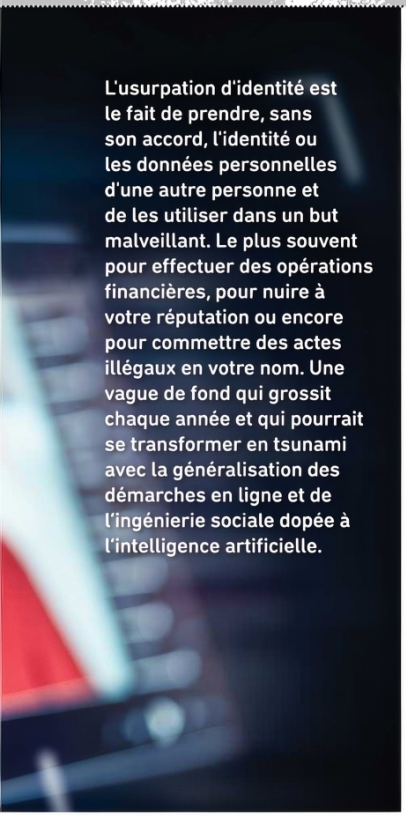
Nous utiliserons ici cet exemple : RedLine compromet par exemple un compte Google/YouTube pour en prendre possession. Le pirate crée différentes chaînes ou y publie directement des vidéos (qui font la promotion de techniques de triche ou de cracks de jeux, fournissant des instructions sur le piratage de jeux ou de logiciels populaires). Dans ses descriptions, le hackeur inclut un lien malveillant censé être en rapport avec le thème de la vidéo. Les utilisateurs qui cliqueraient sur le lien téléchargent en fait RedLine sur leur appareil, ce qui entraîne le vol de leurs mots de passe et d'autres informations privées.

USURPATION D'IDENTITÉ

LA FRAUDE QUI N'ARRIVE PAS QU'AUX AUTRES

200 000. Ce serait, selon France Victimes, le nombre de personnes victimes d'une usurpation d'identité chaque année en France. Avec la généralisation des démarches dématérialisées, ce chiffre atteint des proportions industrielles. C'est presque autant que le nombre de cambriolages et bien plus que celui de vols de voitures. Nous sommes tous susceptibles d'être, un jour ou l'autre, victimes d'une usurpation d'identité. Nos données personnelles nous sont demandées pour opérer de très nombreuses démarches, y compris anodines. Nous envoyons régulièrement des copies de documents officiels (justificatifs de domicile, pièces d'identité, etc.) sans être toujours certains de la sécurisation des organismes destinataires. Des identifiants, des documents et des bases de données sont volés et collectés frauduleusement,

PHISHING



L'usurpation d'identité est le fait de prendre, sans son accord, l'identité ou les données personnelles d'une autre personne et de les utiliser dans un but malveillant. Le plus souvent pour effectuer des opérations financières, pour nuire à votre réputation ou encore pour commettre des actes illégaux en votre nom. Une vague de fond qui grossit chaque année et qui pourrait se transformer en tsunami avec la généralisation des démarches en ligne et de l'ingénierie sociale dopée à l'intelligence artificielle.

chaque jour, sur le Web… ou à domicile (poubelle, boîte aux lettres). Et de nombreux escrocs vous appelleront directement ou viendront même à votre porte pour obtenir ces informations, en se faisant passer pour telle ou telle autorité.

QUELLES CONSÉQUENCES POSSIBLES ?

Les cybercriminels, armés de ces données personnelles et éventuellement de documents officiels ou copies, peuvent orchestrer une variété de délits en leur nom, incluant l'ouverture de comptes bancaires, la souscription à des abonnements téléphoniques, l'obtention de prêts, la

QUELS SONT LES TYPES DE DONNÉES OU DE DOCUMENTS NÉCESSAIRES À UNE USURPATION D'IDENTITÉ ?

L'usurpation d'identité par des cybercriminels peut se faire de différentes manières et nécessiter divers types d'informations ou de documents. En général, voici les informations, types de données personnelles et documents les plus couramment recherchés par les cybercriminels pour réussir une usurpation d'identité :

1# DONNÉES PERSONNELLES

- **Nom complet :** Souvent le point de départ pour d'autres recherches.
- **Date de naissance :** Utilisée en combinaison avec d'autres données.
- **Adresse postale :** Peut être utilisée pour des fraudes par correspondance ou pour obtenir d'autres informations personnelles.
- **Numéro de Sécurité sociale**: Permet l'accès à une multitude de services et informations financières.
- **Numéros de téléphone :** Utilisés pour la récupération de compte ou la vérification d'identité.
- **Adresses email :** Peuvent être utilisées pour le phishing ou l'accès à d'autres comptes via la récupération de mot de passe.
- **Mots de passe et identifiants de connexion :** Donnent un accès direct à des comptes personnels et financiers.
- **Données bancaires et financières :** Numéros de compte, numéros de carte de crédit, PIN, etc.
- **Questions et réponses de sécurité :** Souvent utilisées pour réinitialiser les accès aux comptes.
- **Photographies et informations biométriques :** Utilisées pour créer de faux documents ou contourner certaines sécurités basées sur la reconnaissance faciale.

2# DOCUMENTS OU COPIES DE DOCUMENTS

- **Carte d'identité nationale ou passeport :** Permettent une usurpation d'identité complète.
- **Permis de conduire :** Peut être utilisé comme pièce d'identité dans de nombreux contextes.
- **Relevés bancaires ou factures :** Contiennent des informations financières précises.
- **Justificatifs de domicile :** Utilisés pour prouver une adresse lors de la création de comptes ou la souscription de services.
- **Cartes de sécurité sociale ou d'assurance santé :** Donnent accès à des services et prestations.
- **Documents officiels signés :** Contrats, actes notariés, etc., peuvent être falsifiés ou modifiés.
- **Correspondance officielle :** Lettres de l'administration, décisions judiciaires, peuvent être détournées pour obtenir d'autres documents ou informations.

LES ARNAQUES DEVIENNENT DE PLUS EN PLUS SOPHISTIQUÉES ET CRÉDIBLES, NOTAMMENT GRÂCE À L'AIDE D'OUTILS BASÉS SUR L'INTELLIGENCE ARTIFICIELLE. ICI, LA DGCCRF MET EN GARDE CONTRE DES ESCROCS SE FAISANT PASSER CETTE ANNÉE POUR CERTAINS DE SES AGENTS ET TENTANT D'OBTENIR DES INFORMATIONS SENSIBLES.

« Prouver son innocence relève du parcours du combattant pour les victimes.

création de profils sur les réseaux sociaux, la location de véhicules, le non-paiement d'amendes (infractions routières, transports, etc.), la publication d'annonces frauduleuses, l'arnaque de proches, etc.
Sous couvert d'une fausse identité, ils peuvent aussi se faire passer pour un autre dans des cas de harcèlement en ligne,

À SAVOIR
L'usurpation d'identité est punissable par la loi, entraînant jusqu'à un an d'emprisonnement et 15 000 euros d'amende pour utilisation frauduleuse des données identifiant une personne dans l'intention de nuire.

RÉAGIR À UNE USURPATION D'IDENTITÉ : GUIDE D'ACTION

1) COLLECTE DE PREUVES
Amassez toutes les preuves attestant de l'usurpation (messages, URL, documents justificatifs, captures d'écran) et contactez immédiatement les plateformes impliquées pour signaler le délit et demander la suppression de vos informations personnelles.

2) DÉPÔT DE PLAINTE
Portez plainte auprès de la police, de la gendarmerie, ou par courrier adressé au procureur de la République. Conservez une copie de chaque plainte, qui vous sera utile dans vos démarches ultérieures.

3) ALERTEZ VOTRE BANQUE ET VOS ORGANISMES FINANCIERS
Informez sans délai vos institutions bancaires de la situation pour surveiller toute activité suspecte sur vos comptes et, en cas de vol de données bancaires, faites opposition.

4) RENOUVELLEMENT DES PIÈCES D'IDENTITÉ
C'est essentiel pour que d'autres documents en libre circulation soient considérés comme caducs. Faites annuler et renouveler vos documents d'identité volés.

5) ATTESTATION SUR L'HONNEUR
Pour les démarches auprès des différents organismes, fournissez une attestation sur l'honneur accompagnée d'une copie de votre plainte.

6) CONTACTEZ LA BANQUE DE FRANCE
Signalez l'usurpation à la Banque de France pour vérifier l'ouverture frauduleuse de comptes ou de crédits en votre nom, et pour vous assurer de ne pas être inscrit sur des fichiers d'incidents bancaires.

7) FAITES-VOUS AIDER
Pour toute assistance, contactez France Victime au 116 006 et la plateforme Info Escroquerie au 0 805 805 817, services gratuits offrant conseils et accompagnement. En cas de besoin, un avocat peut également vous aider à défendre vos droits.

CONSEIL
Pour l'envoi de copies de documents (RIB, justificatif de domicile, pièces d'identité, etc.), pensez à apposer un filigrane sur ceux-ci. Voir notre tuto page 44.

de chantage, de diffamation ou d'extorsion. Ces agissements placent les victimes dans une position précaire, les forçant à prouver leur innocence face à des infractions, délits ou crimes qu'elles n'ont pas commis. Et cela est un véritable parcours du combattant.

UN BUSINESS QUI A DE L'AVENIR

Aux États-Unis, des sociétés spécialisées offrent leurs services pour répondre aux besoins de victimes de plus en plus nombreuses ou pour prévenir les risques d'usurpation. Et oui, au pays de l'Oncle Sam, quand un nouveau marché se développe, il y a toujours une entreprise privée qui se crée immédiatement au coin de la rue ! Lifelock, IdentityForce et Experian IdentityWorks par exemple offrent une surveillance des données personnelles et financières, alertes en cas d'activité suspecte, et apportent leur assistance en cas d'usurpation. Lifelock se distingue par son service de compensation en cas de vol d'identité. IdentityForce offre une surveillance étendue incluant les médias sociaux. Experian IdentityWorks combine la surveillance de l'identité avec des rapports de crédit détaillés. Les prix varient selon le niveau de service, généralement de quelques euros à plusieurs dizaines d'euros par mois.

TROIS EXEMPLES D'USURPATION D'IDENTITÉ

> PRÊT DE 500 000 EUROS

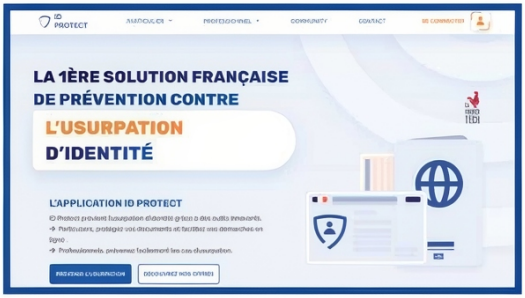
Virginie, une Normande, a vécu un cauchemar financier après que sa carte d'identité a été volée, menant à son usurpation d'identité. Comme le raconte Capital, des escrocs ont acheté un immeuble en son nom, engendrant une dette de 500 000 euros. Elle s'est retrouvée contrainte de vivre dans sa voiture, même en étant employée. La situation est devenue si critique que la banque, face aux impayés, s'est retournée contre elle, la laissant avec la responsabilité de rembourser les frais liés à l'immeuble. Un procès est prévu en 2025 pour résoudre cette affaire.

> 7300 EUROS D'AMENDES À SON NOM

Charly Acosta, étudiant en odontologie à Montpellier, subit depuis trois ans les conséquences d'une usurpation d'identité. Comme le raconte Le Parisien, des fraudeurs voyageant sans billet ont utilisé son identité, accumulant plus de 7 300 euros d'amendes à la SNCF en son nom. Charly doit désormais prouver qu'il n'était pas sur les trajets incriminés, une procédure chronophage qui impacte ses études et finances. Malgré ses efforts, les courriers de recouvrement et les saisies directes sur son compte bancaire continuent, aggravant sa situation financière et psychologique.

> 25 ANS DE CAUCHEMAR

Présentée dans Envoyé Spécial fin 2023, l'histoire de José illustre la difficulté à faire réparer une usurpation d'identité. Il a vécu un véritable cauchemar après le vol de ses papiers, en 2000, empêchant des événements importants comme la reconnaissance de ses enfants. La plainte déposée n'a pas empêché l'escroc de s'accrocher à cette fausse identité, puisque José apprend qu'il est « marié », à Londres, avec une femme qu'il ne connaît pas. Sous son nom, l'usurpateur a un emploi, des enfants... et a maille à partir avec la justice. José se voit réclamer des impôts impayés, des remboursements de prêts, etc. L'usurpation de son identité lui a coûté cher, l'impliquant même dans des affaires de viol et séquestration dont il était innocent, et l'a privé de ses droits sociaux et professionnels. Même après la condamnation de l'escroc, José continue de subir les conséquences de cette longue période d'usurpation.



EN FRANCE, C'EST LA SOCIÉTÉ ID PROTECT QUI FAIT FIGURE DE PIONNIÈRE EN LA MATIÈRE. ELLE SE PROPOSE D'ENQUÊTER ET DE VOUS ACCOMPAGNER DANS VOS DÉMARCHES, SOUS LA FORME DE FORFAITS ALLANT DE 79 À 489 EUROS. CÔTÉ PRÉVENTION, UN SYSTÈME DE SURVEILLANCE EN CONTINU ET D'ALERTES EST PROPOSÉ SOUS FORME D'ABONNEMENTS MENSUELS.


FREE JULIAN
ASSANGE

LE **BLACK** DOSSIER

ÉDITION 2024

LA TROUSSE À OUTILS DU HACKER

Les 30 MEILLEURS LOGICIELS 100% GRATUITS

Réseaux - Cloud - Contrôle à distance
Intrusion - Surveillance - Wi-Fi

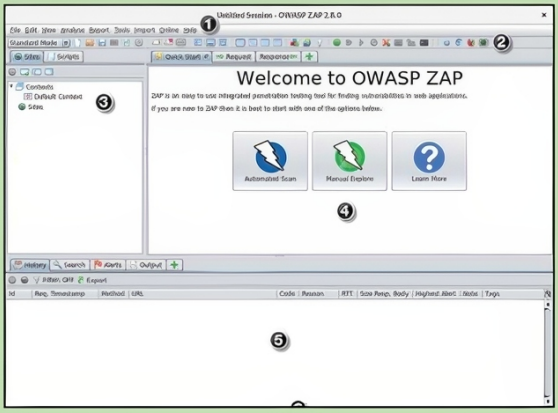
TOP 20 LOGICIELS POUR TOUT HACKER FACILEMENT

ZAP

> Analyse des vulnérabilité d'un service

ZAP (Zed Attack Proxy) est un outil de test de sécurité d'application Web polyvalent qui analyse les réponses reçues d'une application Web cible. Il peut identifier les vulnérabilités potentielles, notamment les attaques par injection SQL, cross-site scripting (XSS) et par débordement de tampon. Il prend en charge les analyses passives et actives. De plus, il dispose d'une interface graphique facile à utiliser, d'un proxy d'interception, de scanners automatisés et d'une variété de plug-ins. Comme Nmap, ZAP fonctionne sur plusieurs plateformes.

Lien : www.zaproxy.org

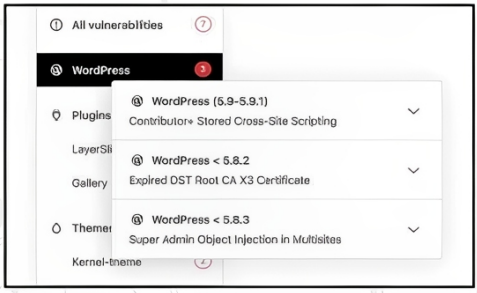


WPSCAN

> Cible WordPress

WPScan, conçu spécifiquement pour WordPress, contient une vaste base de données de vulnérabilités et de faiblesses connues. Ses capacités d'analyse incluent la détection des noms d'utilisateur, des mots de passe faibles, des versions de plugins non sécurisées et des thèmes vulnérables. WPScan est un outil de ligne de commande doté d'un potentiel d'automatisation utilisant des scripts pour des tests à grande échelle. Il est régulièrement mis à jour pour inclure les dernières vulnérabilités connues.

Lien : wpscan.com/wordpress-security-scanner

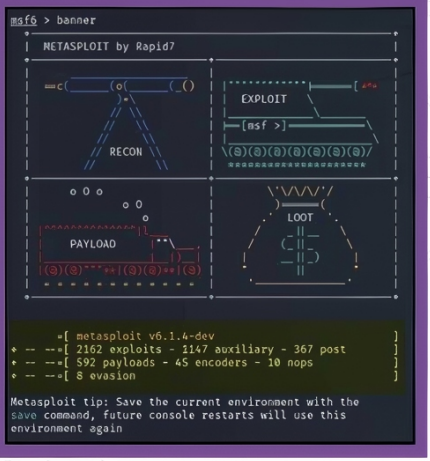


METASPLOIT

> Multi-intrusion

Metasploit fournit une suite complète d'outils. Cela inclut une vaste base de données d'exploits et de vulnérabilités connus pour aider à identifier les faiblesses d'un système cible. Son interface conviviale est idéale pour développer et exécuter des exploits. Idéal également pour les modules auxiliaires qui effectuent des tâches telles que la prise d'empreintes digitales, la reconnaissance et l'analyse des vulnérabilités. Metasploit s'intègre à d'autres outils et frameworks, tels que Nmap et Burp Suite. Il fournit une suite complète de fonctionnalités de test d'intrusion.

Lien : www.metasploit.com

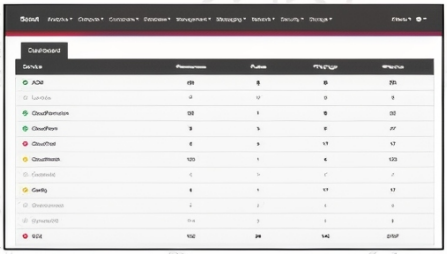


SCOUTSUITE

> Pour le cloud

ScoutSuite est un outil populaire qui analyse les environnements cloud à la recherche de vulnérabilités et de mauvaises configurations. L'outil fonctionne sur AWS, Azure et GCP. Il fournit une analyse détaillée des ressources cloud, telles que les machines virtuelles, les bases de données et les compartiments de stockage. Il évalue également leur conformité aux meilleures pratiques de sécurité standards du secteur.

Lien : sourceforge.net/projects/scout-suite.mirror

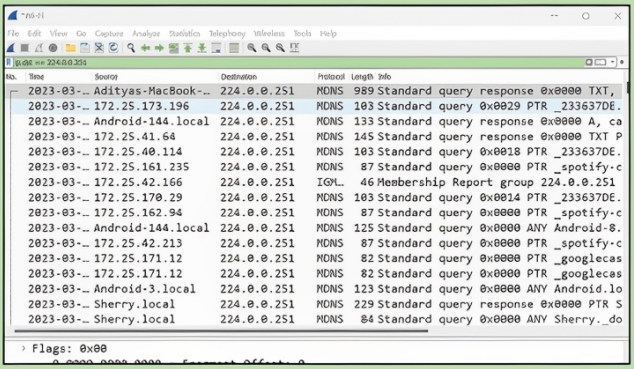


WIRESHARK

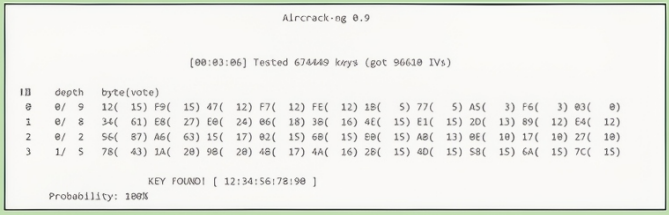
> Analyse les vulnérabilités d'un réseau

Wireshark est un analyseur de protocole réseau open source populaire. Il peut être utilisé sur plusieurs systèmes d'exploitation pour capturer et analyser le trafic réseau. Les capacités d'inspection et de filtrage des paquets réseau en temps réel facilitent l'investigation ciblée d'un trafic réseau spécifique.

Lien : www.wireshark.org



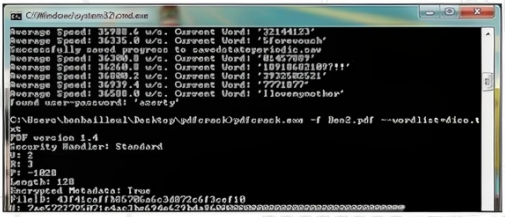
AIRCRACK-NG
> Cible les réseaux Wi-Fi



Aircrack-ng fournit une suite complète d'outils pour surveiller et analyser le trafic réseau. Il prend également en charge le piratage des mots de passe pour les réseaux wifi qui utilisent des méthodes de cryptage faibles. Il est open source et peut aider à identifier les points d'accès vulnérables, à surveiller le trafic réseau et à tester la sécurité du réseau.

Lien : www.aircrack-ng.org

PDFCRACK > 100%PDF



PDFCrack est un logiciel destiné à fonctionner sur système Linux, mais il existe une version pour Windows. Il permet de tirer profit des processeurs multicœurs et de la puissance de plusieurs ordinateurs (cluster) pour attaquer les mots de passe d'ouverture et d'autorisation du format PDF.

Lien : **http://andi.flowrider.ch/research/pdfcrack.html**

NMAP > Analyse les vulnérabilités d'un réseau

Nmap, communément appelé mappeur de réseau, « cartographie » un réseau en analysant les réponses reçues des paquets envoyés au réseau cible. Avec Nmap, les utilisateurs peuvent déterminer quels hôtes et services sont disponibles. Nmap permet également aux testeurs d'identifier les détails du système d'exploitation, les ports ouverts, les numéros de version des services en cours d'exécution, les pare-feu et les vulnérabilités potentielles du réseau.Nmap peut être utilisé sur divers systèmes d'exploitation, notamment Linux, Windows et macOS. Il prend également en charge différents types d'analyse, depuis les analyses de ports simples jusqu'aux analyses avancées qui détectent des vulnérabilités spécifiques. Il peut être utilisé avec d'autres outils comme Metasploit pour une exploitation automatisée des vulnérabilités.

Lien : github.com/nmap/nmap

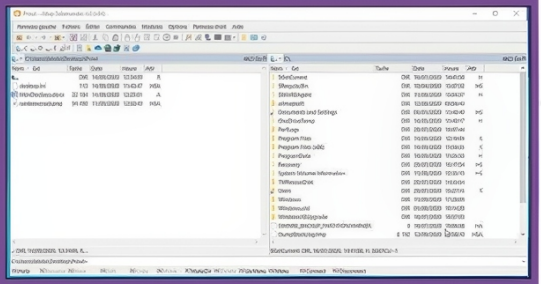
```
Nmap scan report for 10.0.0.71
Host is up (0.0095s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
2869/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
MAC Address: B0:6E:BF:30:AD:33 (ASUSTek Computer)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 10.0.0.89
Host is up (0.14s latency).
Not shown: 999 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
7000/tcp open  rtsp    AirTunes rtspd 377.40.00
MAC Address: 10:3D:0A:90:A1:B5 (Hui Zhou Gaoshengda Technology)

Nmap scan report for 10.0.0.138
Host is up (0.17s latency).
All 1000 scanned ports on 10.0.0.138 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 44:61:32:52:EA:8D (ecobee)
```

ALTAP SALAMANDER

> Révéler l'invisible

Vous avez masqué, un peu trop consciencieusement, des fichiers sensibles sur votre partition Windows (avec par exemple les commandes attrib +s +h) et vous ne vous souvenez plus où ils se trouvent ? L'utilitaire gratuit Altap Salamander va vous aider à les dénicher. Il suffit de lui indiquer l'emplacement qu'il doit scruter et, au bout de quelques minutes, les fichiers cachés ressurgissent. À garder sous la main.

Lien : **altap.cz/salamander/downloads**



PROXMARK3

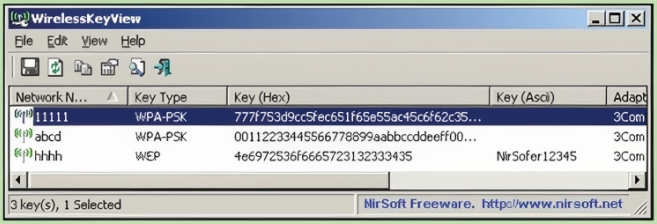
> Intrusion matérielle

Proxmark3 est un outil matériel opensource utilisé pour la recherche et les tests RFID. Il peut lire et émuler différents types de cartes et d'étiquettes RFID, effectuer des analyses sans fil et cloner des appareils RFID. Cet outil permet aux pentesters de simuler diverses attaques, telles que des attaques par rejeu et des attaques de type man-in-the-middle, sur les systèmes RFID afin d'évaluer leur niveau de sécurité.

Lien : proxmark.com

WIRELESSKEYVIEW

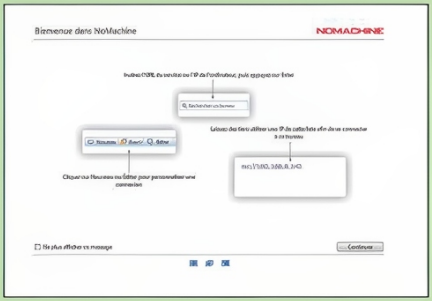
> Cible les réseaux Wi-Fi



Cette fois-ci, ce logiciel se spécialise uniquement dans la récupération des identifiants de votre réseau Wi-Fi. Installé sur votre PC, il va analyser le signal et tentera de vous livrer le nom du réseau (SSID), le type de protection (WEP/WPA), le mot de passe complet (Hex, Ascii) et le nom du routeur Wi-Fi.

Lien : **www.nirsoft.net**

NO MACHINE > Prise de contrôle à distance



Pas vraiment connu, NoMachine est pourtant une excellente solution de contrôle à distance. Gratuit et multi-plateforme, il permet de se connecter grâce à un identifiant, et de gérer plusieurs ordinateurs. Le top ? La fluidité garantie par le protocole NX, et la sécurité assurée grâce au SSH. L'utilisateur est guidé étape par étape, et peut configurer NoMachine en finesse. Un logiciel à découvrir !

Lien : **www.nomachine.com**

OFFICE2JOHN

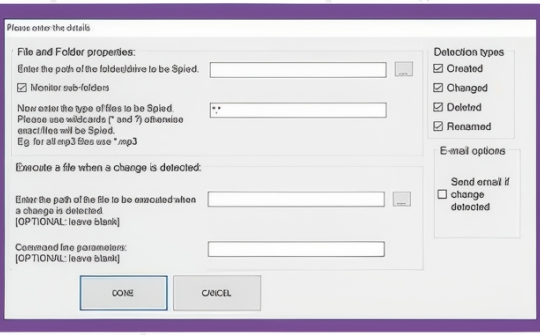
> Un puissant cracker de docs

Les documents Word, Excel ou PowerPoint peuvent aussi profiter d'une protection par mot de passe. Si votre mémoire vous joue des tours, pas de panique. Office2John va vous donner un sérieux coup de main. Ce programme gratuit, écrit en Python, se charge d'extraire le hash du fichier issu de diverses versions d'Office (de 97 à 2013). Le hash en main, ne reste plus qu'à se remettre à Johnny ou Hashcat pour révéler le sésame. Vous pouvez pour cela suivre ce tutoriel en anglais mais très détaillé : **tinyurl.com/y4n6cvws**.

Lien : **tinyurl.com/y5as3b87**

THE FOLDER SPY

> Monitoring pour tout surveiller

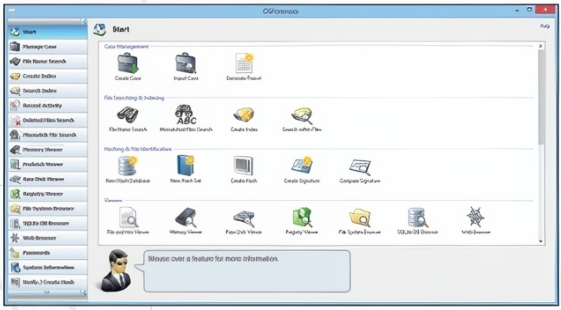


Cet outil de monitoring peut se transporter sur une clé USB et s'installer en mode incognito sur un appareil. Très léger, il surveille toutes les modifications de fichiers et dossiers et est entièrement automatisé. Une fois en place, vous n'avez plus qu'à regarder les journaux pour savoir ce qu'il s'est passé en votre absence.

Lien : **bit.ly/3KhMQZI**

OSFORENSIC

> Intrusion matérielle



Ce puissant outil de recherche et d'investigation est utilisé par la police, les services de renseignement et les professionnels de restauration de fichiers. OSForensics va scanner votre ordinateur (ou celui que vous voudrez) en vue d'extraire les informations pertinentes : mot de passe (site ou documents), activité récente, fichiers supprimés ou avec une extension ne correspondant pas, etc. En plus de toutes ces fonctionnalités, le logiciel permet de créer un index des fichiers et des e-mails pour retrouver en un instant les éléments en rapport avec tel ou tel sujet. Il analyse le contenu du disque par secteur et fouille même dans la mémoire. Notons aussi la possibilité de faire un cliché des partitions du disque pour observer les changements dans le temps ou créer une image du disque pour l'exporter et l'analyser tranquillement plus tard. La version 8 dispose d'un essai gratuit mais de plus anciennes versions sont, elles, disponibles gratuitement.

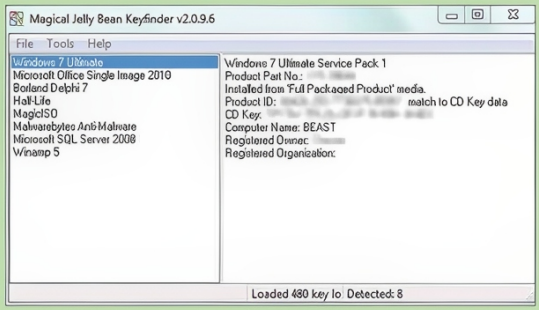
Lien : **www.osforensics.com**

KEYFINDER

> Retrouvez sa clé Windows

Sur le site de KeyFinder, cliquez sur **Download** en dessous de **Free** pour télécharger la version gratuite du logiciel. Ne vous inquiétez pas : pour ce qui nous intéresse ici, elle est amplement suffisante. Après avoir installé KeyFinder, il vous suffit de lancer le programme pour voir s'afficher votre clé Windows, à droite de **CD KEY**. Notez-la précieusement et conservez-la dans un endroit sûr en cas de besoin.

Lien : **www.magicaljellybean.com/keyfinder**

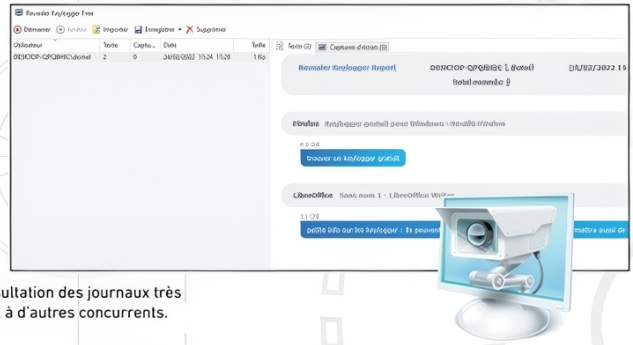


REVEALER KEYLOGGER >

Enregistreur de frappes

Un outil précieux pour surveiller tout ce qui est écrit sur votre PC, sur un document ou une messagerie : tout ce qui est frappé sur le clavier est enregistré. Dans sa version gratuite, Revealer Keylogger ne peut être masqué à l'insu d'un utilisateur curieux, ce qui le réserve heureusement à des usages légaux. L'ergonomie du logiciel permet la consultation des journaux très clairs et bien organisés, contrairement à d'autres concurrents.

Lien : **logixoft.com**

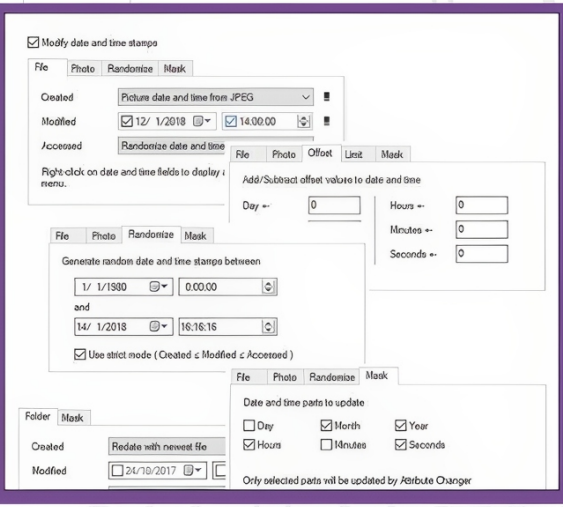


ATTRIBUTE CHANGER

> Changer les attribut d'un fichier

Attribute Changer vous donne la main sur les attributs d'un fichier ou d'un dossier (date et heure de création ou modification, lecture seule, système, caché, archive et indexé, etc.). Il vous permet de les modifier et donc de leur donner une nouvelle identité pour, par exemple, masquer ses origines. Une fois Attribute Changer installé, ce programme gratuit sera accessible via le clic droit de votre souris sur le fichier ou dossier cible. Vous avez la possibilité de modifier les attributs de fichiers un par un ou par lot. Un mode **Simulation** vous permet de vérifier le résultat avant toute modification.

Lien : **www.petges.lu**



ROUTERPASSWORDS

> Mots de passe WiFi

RouterPasswords.com est un site qui répertorie les mots de passe par défauts de centaines de routeurs différents. Il suffit de sélectionner la marque et le modèle pour accéder au couple identifiant/mot de passe ainsi qu'au protocole d'échange de donnée. Si vous êtes un administrateur ou que vous dépannez souvent vos amis étourdis, vous aurez donc accès aux réglages à condition que les utilisateurs n'aient pas changé les identifiants. Si vous ne trouvez pas le modèle exact du routeur que vous recherchez, essayez un mot de passe à partir d'un modèle alternatif du même fabricant !

Lien : **www.routerpasswords.com**

SOCIAL ENGINEER TOOLKIT

> Boîte à arnaques

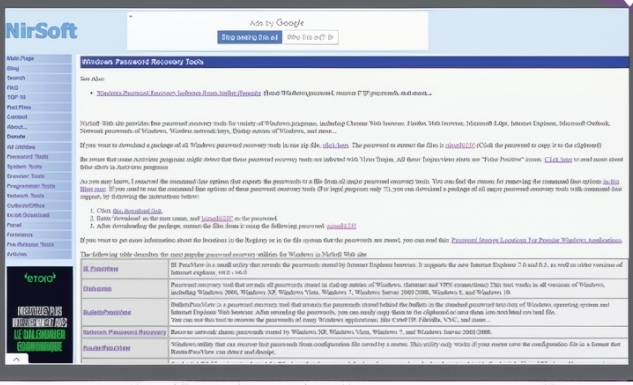
Le Social Engineer Toolkit (SET) est un outil open source utilisé pour générer diverses attaques d'ingénierie sociale telles que le phishing et la récolte d'informations d'identification. De plus, il inclut des fonctionnalités d'usurpation d'e-mails, d'usurpation de SMS et d'usurpation de géolocalisation. Il peut même s'intégrer au framework Metasploit pour permettre aux testeurs de fournir des charges utiles et d'exploiter les vulnérabilités.

Lien : www.trustedsec.com/tools/the-social-engineer-toolkit-set

NIRSOFT > LA TROUSSE À OUTILS

Pour ceux qui ne le connaisse pas, Nirsoft est un site web qui propose une collection unique de petits utilitaires freeware utiles, tous développés par Nir Sofer. Vous y trouverez des outils de récupération de mot de passe, de surveillance réseau, de ligne de commande, pour retrouver des clés de licence, etc. Certains outils sont un peu datés mais d'autres continue d'être mis à jour.

Lien : **www.nirsoft.net**

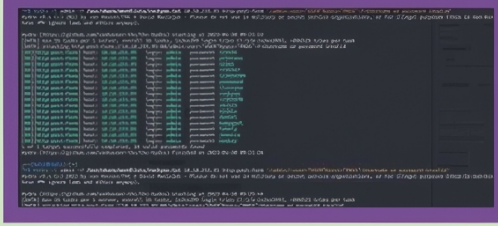


TOP 3 CRACK DE MOTS DE PASSE

HYDRA

Hydra est un outil populaire de piratage de mots de passe qui effectue des attaques par force brute sur divers protocoles et services tels que SSH, FTP et Telnet. Il prend en charge les mécanismes d'authentification tels que HTTP, FTP et SMB, ce qui en fait un outil polyvalent.

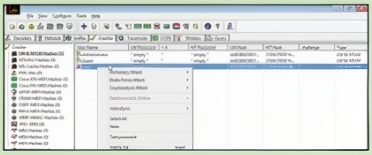
Lien : github.com/vanhauser-thc/thc-hydra



CAIN & ABEL

Connu pour sa capacité à cracker des mots de passe, Cain & Abel possède dans sa besace de nombreux autres outils d'analyse et de sniff. L'interface est riche et « assez » intuitive si vous n'êtes pas rebuté par les dizaines de sous-menus disponibles. Il prend en charge les attaques par rainbow tables, comme les attaques plus classiques (brute, dictionnaire, etc.), que ce soit en local ou en ligne. Gratuit, Cain & Abel ne fournit cependant pas son code source.

Lien : **tinyurl.com/y3zb2tqv**



JOHN THE RIPPER

John the Ripper est un outil largement utilisé pour déchiffrer les mots de passe cryptés avec des algorithmes de cryptage populaires tels que MD5 et SHA. Il peut également effectuer des attaques par dictionnaire et tester la force des mots de passe.

Lien : www.openwall.com/john/

HASHCAT

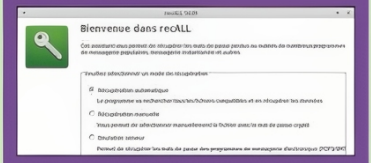
Hashcat est un outil populaire capable de déchiffrer plus de 300 types de hachage différents à l'aide d'attaques par dictionnaire, par force brute et hybrides. Il prend en charge le cracking distribué afin que plusieurs ordinateurs puissent travailler ensemble pour cracker un mot de passe lors d'enquêtes forensic.

Lien : hashcat.net

RECALL

Vous devrez installer recALL sur le PC cible et laisser le programme travailler pour vous. Il n'est pas là pour cracker un fichier ou un service en ligne mais pour chercher des mots de passe, des codes d'accès ou des numéros de licence dans des endroits de votre Windows dont vous ne soupçonniez même pas l'existence (dossier d'installation, base de registre, etc.). Ces emplacements sont préenregistrés et toutes sortes de logiciels sont passés au crible : Windows, Office, antivirus, client mail, navigateurs, client FTP, messagerie instantanée, logiciels commerciaux, jeux vidéo, etc. Avec presque 3 000 références, ce serait bien le diable si recALL ne trouvait pas ce que vous cherchez.

Lien : **keit.co/p/recall**

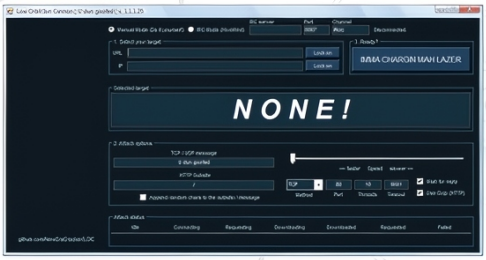


TOP 3 LOGICIELS POUR LANCER UNE ATTAQUE DDOS

LOIC (LOW ORBIT ION CANNON)

> Pour les débutants et les tests de sécurité

Toujours utilisé mais plutôt destiné aux débutants grâce à son interface accessible) et aux cibles mal protégées. LOIC a été conçu avec l'intention de permettre aux administrateurs de réseau de tester la résistance de leur propre infrastructure aux attaques DDoS. L'idée était de fournir un moyen simple et accessible pour simuler des attaques réalistes, permettant ainsi d'identifier et de renforcer les points faibles. Cependant, en raison de sa facilité d'utilisation et de sa disponibilité en open-source, LOIC a rapidement été adopté par des hackers et des collectifs tels que Anonymous. Mais il se trouve aujourd'hui de plus en plus délaissé au profit d'alternatives plus puissantes. Car les attaques menées avec LOIC sont relativement faciles à détecter et à atténuer par les défenseurs modernes de cybersécurité.



Les systèmes de protection contre les DDoS ont évolué pour identifier et filtrer le trafic malveillant généré par des outils comme LOIC. Le programme n'offre qui plus est pas d'anonymat pour ses utilisateurs, rendant les attaquants facilement traçables par les autorités. L'utilisation de VPN ou autre solution de routage proxy s'impose donc.

Lien : sourceforge.net/projects/loic/

ET POUR LES RÉSEAUX DE BOTNETS ?

Pour l'utilisation de PC zombies et de botnets, voici les principaux malwares utilisés :

- Mirai : Comme indiqué ci-contre, Mirai est un tout-en-un qui peut préparer et lancer une attaque DDoS en ayant la capacité à mobiliser son réseau de botnets infectés pour se faire.

- Trickbot : Originellement un cheval de Troie bancaire, Trickbot a évolué pour inclure des fonctionnalités permettant la création de botnets. Il est souvent distribué via des campagnes de phishing.

- Emotet : Bien qu'il soit principalement un logiciel malveillant de vol d'informations, Emotet a été utilisé pour distribuer d'autres types de malwares, y compris ceux qui créent des botnets.

- Qbot (ou Qakbot) : Ce malware polymorphe est connu pour sa capacité à infecter des réseaux d'entreprises et à recruter des machines infectées dans des botnets.

- DDoS-for-hire Services : Ces services, également connus sous le nom de «booters» ou «stressers», offrent à des individus la capacité de lancer des attaques DDoS sans avoir besoin de créer leur propre botnet. Ils louent l'accès à des réseaux de machines infectées.

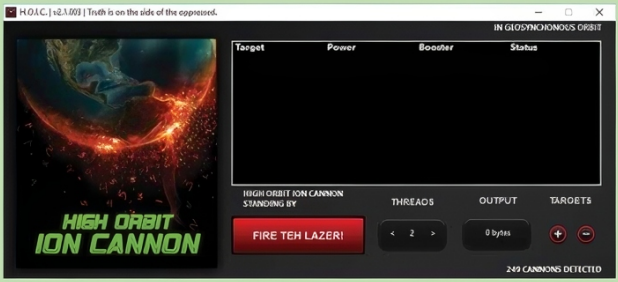
LES HACKERS EN HERBE TROUVE FACILEMENT DES SITES LEUR PROPOSANT POUR QUELQUES DIZAINES D'EUROS PAR MOI DES SERVICES « DDOS-FOR-HIRE ». C'EST-À-DIRE QUE PROGRAMMES D'ATTAQUES ET BOTNETS SONT FOURNIS POUR AUTOMATISER AU MAXIMUM LES ATTAQUES.

HOIC (HIGH ORBIT ION CANNON)

> LOIC... MAIS EN MIEUX.

À la différence de LOIC, qui se concentre sur une seule cible à la fois, HOIC peut attaquer plusieurs cibles simultanément grâce à sa capacité à gérer jusqu'à 256 adresses URL ou IP différentes en une seule instance. Il utilise des scripts personnalisables, appelés «boosters», pour varier le type de trafic généré, rendant ainsi les attaques plus difficiles à détecter et à bloquer par les mécanismes de défense traditionnels. Ces scripts permettent également d'imiter les comportements des utilisateurs légitimes, augmentant d'autant plus la complexité de la détection des attaques.

Comme LOIC, HOIC présente une interface utilisateur graphique (GUI) simple, rendant les attaques DDoS accessibles même aux utilisateurs ayant des connaissances techniques limitées.

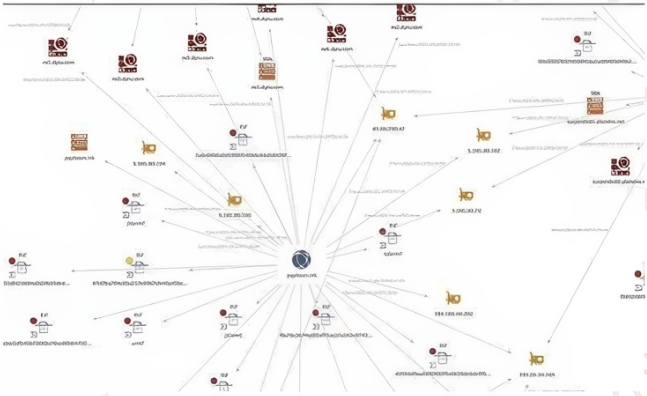


Bien que l'utilisation de HOIC puisse être tracée jusqu'à l'IP de l'attaquant si des précautions supplémentaires ne sont pas prises, l'outil est souvent utilisé en conjonction avec des réseaux privés virtuels (VPN) ou des réseaux de botnets pour masquer l'identité de l'attaquant.

Lien : sourceforge.net/projects/high-orbit-ion-cannon

MIRAI BOTNET

> MYRIADES D'OBJETS CONNECTÉS



Bien que plus connu comme un botnet, Mirai est également associé à un outil pour lancer des attaques DDoS. Mirai fonctionne en infectant des appareils IoT vulnérables, tels que des caméras IP, des routeurs et d'autres dispositifs connectés, en utilisant une table de mots de passe par défaut largement répandus et rarement modifiés par les utilisateurs finaux. Une fois un appareil infecté, il est ajouté à un réseau de bots (botnet) contrôlé à distance par l'attaquant. Ce réseau peut ensuite être utilisé pour lancer des attaques DDoS. Mirai peut automatiquement scanner Internet à la recherche de nouveaux appareils vulnérables à infecter, augmentant rapidement la taille de son botnet. Le botnet Mirai peut être utilisé pour lancer plusieurs types d'attaques DDoS, y compris les attaques par inondation SYN, UDP, et DNS, rendant ses attaques difficiles à atténuer.

L'impact et la facilité d'utilisation de Mirai ont rapidement conduit à sa notoriété. Après l'attaque contre Dyn, le code source de Mirai a été publié en ligne, permettant à d'autres cybercriminels de créer leurs propres variantes du botnet. Le dernier en date ayant impressionné les spécialistes en cybersécurité est baptisé « V3G4 de Mirai ».

7 BONNES RAISONS DE CRÉER DES PARTITIONS SUR SON PC

Utiliser le disque dur d'un PC sans créer de partitions, c'est un peu comme ranger ses affaires dans une armoire sans étagère ou penderie : tout s'entasse au même endroit et une chatte n'y retrouverait pas ses petits ! En créant, organisant et en gérant vos partitions, vous optimisez l'usage du système et sécurisez même vos données.

1# ORGANISATION DES DONNÉES

Le partitionnement permet de séparer les données selon leur usage ou leur importance. Par exemple, on peut avoir une partition pour le système d'exploitation, une autre pour les documents personnels, et une troisième pour les applications. Cela facilite la gestion et l'accès aux fichiers.

2# SÉCURITÉ ET SAUVEGARDE

En séparant les données importantes sur différentes partitions, il est plus facile de les protéger. En cas de problème sur une partition (par exemple, une corruption due à un virus), les autres partitions peuvent rester intactes. De plus, cela simplifie les processus de sauvegarde et de récupération de données, car on peut cibler les partitions les plus importantes.

3# PERFORMANCE DU SYSTÈME

Certaines configurations de partitionnement peuvent améliorer les performances du système. Par exemple, séparer les fichiers système des fichiers utilisateurs peut réduire le temps d'accès aux données et améliorer la vitesse de démarrage du système.

4# MULTI-BOOT

La gestion des partitions permet d'installer et de démarrer plusieurs systèmes d'exploitation sur le même ordinateur (par exemple, Windows et Linux). Chaque système d'exploitation peut être installé sur sa propre partition, ce qui permet à l'utilisateur de choisir quel système démarrer au moment du boot.

5# OPTIMISATION DE L'ESPACE DISQUE

Le partitionnement peut aider à utiliser l'espace disque de manière plus efficace. Par exemple, on peut allouer de l'espace disque en fonction des besoins réels de chaque type de données ou application, en évitant le gaspillage d'espace.

6# GESTION DES TYPES DE FICHIERS SYSTÈME

Différents systèmes d'exploitation peuvent nécessiter différents systèmes de fichiers (par exemple, NTFS pour Windows, EXT4 pour Linux). Les partitions permettent de formater chaque section du disque avec le système de fichiers approprié à chaque OS.

7# ISOLATION ET CONFINEMENT DES ERREURS

En séparant les données en différentes partitions, il est possible de limiter l'impact des erreurs de disque ou des défaillances à une seule partition, facilitant ainsi la détection des problèmes et la réparation.

C'EST QUOI EXACTEMENT UNE PARTITION ?

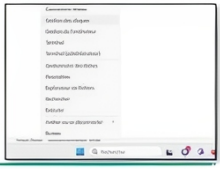
Une partition est une division logique d'un disque dur ou d'un autre support de stockage. Elle fonctionne comme une section indépendante du disque, permettant au système d'exploitation de gérer et d'organiser les données de manière plus efficace. Chaque partition peut être utilisée comme si elle était un disque dur distinct, et on peut lui attribuer un système de fichiers (comme NTFS pour Windows ou EXT4 pour Linux) et un point de montage (comme une lettre de lecteur sous Windows, par exemple C:).

COMMENT CRÉER UNE PARTITION AVEC WINDOWS ?

PRATIQUE

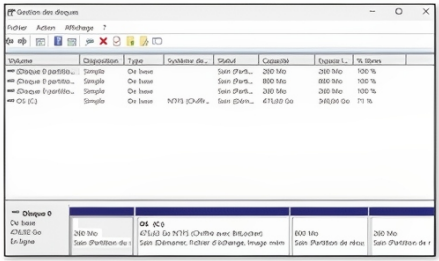
01 › OUVRIR LA GESTION DES DISQUES

Faites un clic droit sur le bouton **Démarrer (icône Windows)** et choisissez **Gestion des disques.**



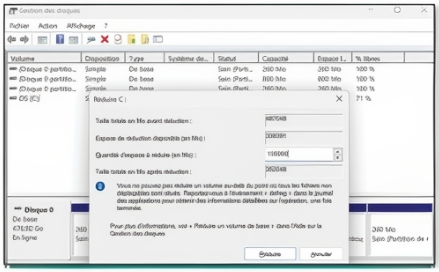
02 › TROUVER LE VOLUME À RÉDUIRE

Cet outil vous permet de voir toutes les partitions existantes sur vos disques durs et d'en créer de nouvelles. Si votre disque dur est entièrement alloué à une seule partition, vous devrez d'abord réduire cette partition pour libérer de l'espace non alloué.



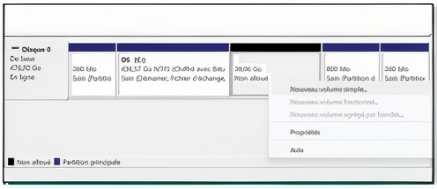
03 › CHOISIR L'ESPACE ALLOUÉ

Faites un clic droit sur la partition que vous souhaitez réduire (ici **C:**) et sélectionnez **Réduire le volume**. Windows analyse l'espace de stockage total et disponible (**Requête de l'espace de stockage**). Suivez les instructions pour spécifier combien d'espace libérer.



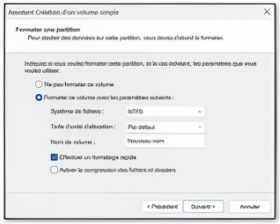
04 › CRÉER UNE NOUVELLE PARTITION

Vous aurez ainsi une partition disponible de XX Go **« Non alloué »**. Faites un clic droit dessus et choisissez **Nouveau volume simple**. Un assistant de création de partition se lancera.



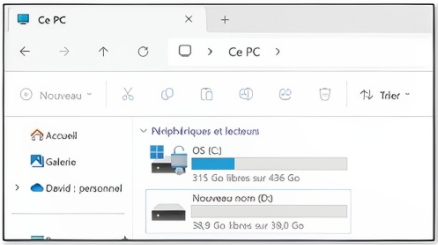
05 › ASSISTANT DE CRÉATION

Suivez l'assistant pour choisir la taille de la partition, lui attribuer une lettre de lecteur, et formater la partition avec un système de fichiers. Les réglages par défaut sont cohérents mais, selon vos besoins, vous pourrez agir durant ce process sur certaines valeurs clés. Suivez les instructions jusqu'à la fin de l'assistant pour terminer la création de votre nouvelle partition.



06 › VOTRE NOUVEAU VOLUME

Vous retrouverez maintenant votre partition à la racine de votre PC. Elle apparait bien dans la **Gestion des disques** comme un nouveau volume. Cet espace de stockage indépendant sera au nom que vous lui aurez donné à l'étape précédente.



ATTENTION

Modifier les partitions d'un disque dur peut entraîner une perte de données. Il est crucial de sauvegarder toutes les données importantes avant de procéder à la création, à la suppression, ou à la modification de partitions.

SÉLECTION

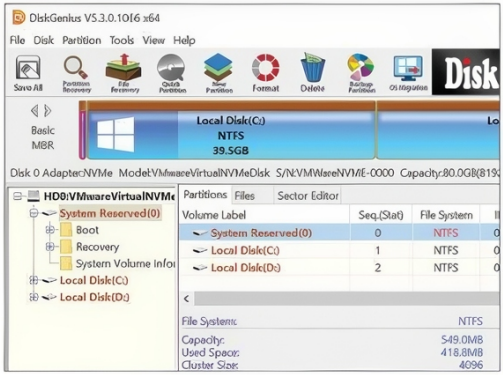
TOP 3 OUTILS POUR GÉRER ET OPTIMISER VOS PARTITIONS

L'outil Windows que nous vous avons présenté page précédente est suffisant pour créer votre partition. Mais d'autres solutions gratuites existent pour en tirer tout le potentiel au quotidien.

DISKGENIUS FREE : LE COUTEAU SUISSE

Une solution tout-en-un destinée à la gestion de partitions, à la récupération de données et au clonage de disque. Outre ses capacités à créer, supprimer et formater des partitions, il excelle dans la restauration de fichiers perdus ou supprimés, même sur des partitions endommagées. Sa spécificité réside dans ses outils avancés tels que le support du RAID et la capacité de booter depuis un USB, offrant ainsi une flexibilité inégalée pour les professionnels et les utilisateurs avancés.

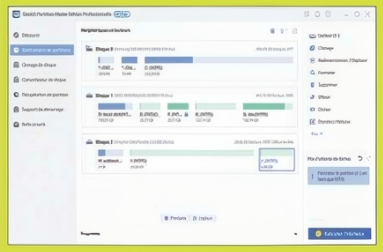
Lien : partitionguru-free.fr.softonic.com



EASEUS PARTITION MASTER FREE : CLAIR ET EFFICACE

EaseUS Partition Master Free simplifie la gestion des partitions de disque sans risque de perte de données. Ce logiciel gratuit permet de redimensionner, déplacer, fusionner, et cloner les partitions ainsi que de convertir des disques ou des formats de fichier sans effort. Avec une interface claire et des instructions pas à pas, ce spécialiste des partitions rend la gestion des espaces de stockage accessible à tous. Son avantage réside dans sa capacité à maximiser les performances du disque et à optimiser l'utilisation de l'espace.

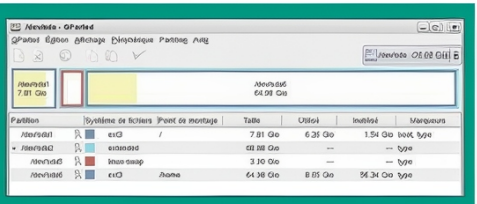
Lien : www.easeus.fr



GPARTED : TOUT POUR LINUX !

GParted est le spécialiste du partitionnement sur Linux. Ce logiciel libre permet de créer, supprimer, redimensionner, déplacer, vérifier et copier des partitions et des systèmes de fichiers sur disques durs, SSD et même des clés USB. Il peut gérer les partitions sans avoir à démarrer le système d'exploitation, parfait pour les administrateurs système et les utilisateurs avancés. Son interface graphique est conviviale (si, si) et vous pouvez aussi l'utiliser de façon portable (live CD/USB).

Lien : gparted.org

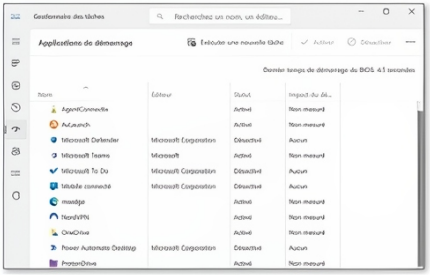


DÉSACTIVEZ ONEDRIVE AU DÉMARRAGE

PRATIQUE

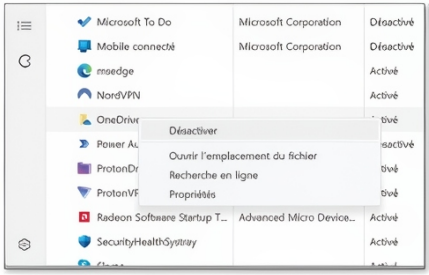
OneDrive, le système de stockage de fichiers sur le cloud de Microsoft, se lance de lui-même lors de l'ouverture de Windows 11… même si vous ne l'utilisez pas ! Voici la marche à suivre pour désactiver ce lancement intempestif.

INFOS
[Onedrive]
Difficulté :



01 › APPLICATIONS AU DÉMARRAGE

Allez dans Gestionnaire des tâches puis, dans le menu à gauche, sélectionnez **Applications au démarrage** (icône compteur de vitesse).



02 › DÉSACTIVER

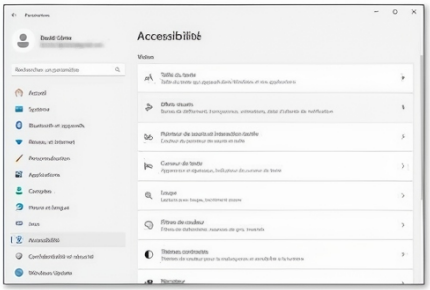
Trouvez maintenant l'application Ondrive dans la liste présentée. Faites un clic droit sur elle puis choisissez **Désactiver**. Il vous suffira de le réactiver en cas de besoin.

WINDOWS 11 PLUS RÉACTIF !

PRATIQUE

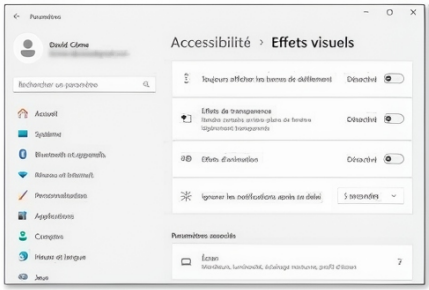
Sur certains PC d'entrée de gamme, ou un peu fatigués, l'expérience Windows 11 n'est pas optimale, avec beaucoup de ralentissements. Testez cette astuce pour redonner du peps à votre PC.

INFOS
[Windows 11]
Difficulté :



01 › EFFETS VISUELS

Allez dans **Paramètres** et cliquez sur **Accessibilité** dans la colonne de gauche. Ouvrez maintenant **Effets visuels.**



02 › DÉSACTIVER

Vous pouvez maintenant désactiver les **Effets d'animation**, très gourmands. Si cela n'est pas suffisant, vous pouvez également désactiver les **Effets de transparence**, même s'ils sont appréciables.

3 QUESTIONS SUR Usurpation de NUMÉRO DE TÉLÉPHONE

1 QU'EST-CE QUE LE « SPOOFING » ?

Cette pratique malveillante, connue sous le terme d'ID spoofing, consiste à masquer l'identité réelle de l'appelant en falsifiant le numéro de téléphone affiché par le destinataire de l'appel. L'usurpation de numéro de téléphone implique l'utilisation de logiciels ou de services spécialisés pour modifier les informations d'identification de l'appelant affichées sur le téléphone du destinataire. Ainsi, l'usurpateur peut se faire passer pour une autre personne, une entreprise de confiance, ou même un organisme gouvernemental.

Les motifs derrière ces actes d'usurpation sont divers et varient de la simple plaisanterie de mauvais goût à des objectifs beaucoup plus sinistres, tels que :

- **L'escroquerie et la fraude**: en se faisant passer pour des banques ou des services publics, les escrocs tentent d'obtenir des informations personnelles ou financières. Un numéro précis (y compris mobiles en 06 ou 07) peut même être utilisé. Il est ainsi possible d'usurper l'identité d'un proche ou d'un contact connu.

- **Le spam téléphonique** : diffuser en masse des appels indésirables, souvent pour vendre des produits ou services. L'utilisation de préfixe téléphonique correspondant à votre région fait partie des arnaques les plus simples pour vous convaincre de décrocher.

- **Le cyberharcèlement**: masquer son identité pour harceler ou intimider une personne en changeant régulièrement de numéro.

LE SPOOFING

2 COMMENT FONT LES PIRATES ?

L'usurpation d'identité via VoIP repose sur la manipulation des en-têtes SIP (Session Initiation Protocol). Le protocole SIP est utilisé pour initier, maintenir et terminer des sessions de communication interactive, telles que des appels vidéo et vocaux sur Internet. Ce protocole intègre des failles connues que les pirates peuvent exploiter.

TECHNIQUES D'USURPATION

- Modification du SIP Header: Le SIP (Session Initiation Protocol) est un protocole utilisé pour initier, maintenir, modifier et terminer des sessions de communication en temps réel. L'usurpateur peut manipuler le «From» header du paquet SIP pour afficher un numéro différent auprès du destinataire.

- Utilisation de Proxy VoIP: Certains services VoIP permettent aux utilisateurs de passer par un proxy qui peut modifier les informations d'identification de l'appelant avant de les transmettre au destinataire.

- Exploitation de failles dans les PBX d'Entreprise: Les systèmes téléphoniques privés (PBX) mal sécurisés peuvent être exploités pour effectuer des appels qui semblent provenir de numéros légitimes de l'entreprise.

EXEMPLES D'OUTILS PIRATES

a# Services VoIP Spécialisés

- **SpoofCard** : Un des services les plus connus pour l'usurpation d'appels téléphoniques, via PC ou mobile. SpoofCard permet aux utilisateurs de choisir le numéro qui s'affiche sur le téléphone du destinataire, d'ajouter des effets de voix et même d'enregistrer les appels. Le service est proposé via une tarification à la carte, avec des packages allant de 10 $ pour 60 minutes à des options plus coûteuses pour des besoins plus élevés.

b# Applications Mobiles

- **Bluff My Call** : Application disponible pour iOS et Android hors des stores officiels, Bluff My Call offre des fonctionnalités similaires à SpoofCard, y compris la modification du numéro de l'appelant, la modification de la voix, et l'enregistrement des appels. Les prix varient selon les minutes d'appel achetées.

c# Plateformes en Ligne

- **SpoofTel** : Exemple de plateforme qui offre des services d'usurpation, permettant aux utilisateurs de réaliser des appels et des messages textes avec un numéro d'identification falsifié. Ces services sont souvent payants, basés sur un système de crédits.

③ COMMENT SE PROTÉGER ?

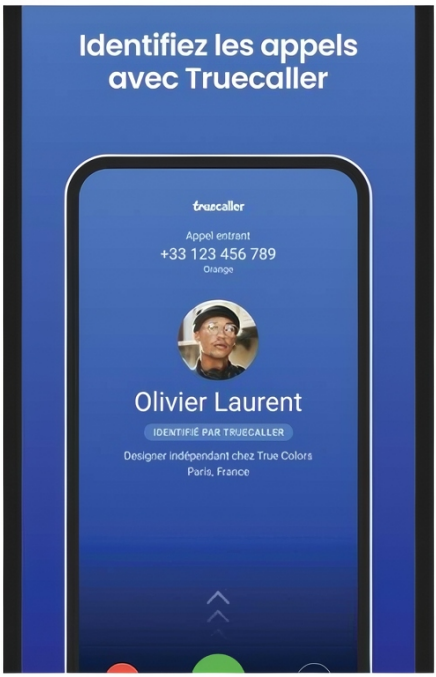
Pour se prémunir contre l'usurpation de numéro de téléphone, plusieurs mesures peuvent être adoptées :

a# **Vérification systématique** : Ne jamais prendre pour acquis l'identité de l'appelant et vérifier auprès de l'entité supposée. En cas de doute, il est conseillé de raccrocher et de rappeler l'organisation ou la personne via un numéro vérifié.

b# **Utilisation de services intégrés d'identification des appelants** : Certains opérateurs proposent des services avancés pour détecter et bloquer les appels usurpés. L'adoption de standards comme STIR/SHAKEN par les opérateurs téléphoniques aide à authentifier et à vérifier l'origine des appels, réduisant ainsi la capacité des attaquants à mener des attaques d'usurpation

c# **Utilisation de services tiers d'Identification des appelants :**

- **Truecaller**: Une application qui identifie les appels entrants et bloque ceux qui sont connus pour être des spams ou des usurpations. Truecaller repose



sur une vaste base de données d'identifiants téléphoniques collectés auprès de ses utilisateurs.

- **Hiya**: Comme Truecaller, Hiya utilise une base de données pour identifier les appels frauduleux et les bloquer avant qu'ils n'atteignent l'utilisateur. Les deux services offrent des versions gratuites et payantes, ces dernières proposant des fonctionnalités avancées de blocage et d'identification.

d# **Prudence avec les informations personnelles** : Ne jamais divulguer d'informations sensibles par téléphone sans vérification préalable.

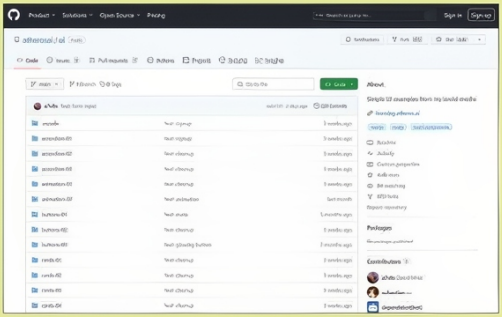
SÉLECTION

TOP 3 SITES POUR TROUVER DES PROGRAMMES OPEN SOURCE

GITHUB > La référence pour les experts

GitHub est la plus grande plateforme de collaboration pour le développement de logiciels dans le monde, permettant aux développeurs de stocker, gérer, suivre et collaborer sur des projets. Une mine d'informations et de logiciels à tester ! Bien qu'il ne soit pas le plus intuitif pour les utilisateurs novices, c'est le lieu de prédilection pour trouver de nouveaux logiciels incroyables mais aussi les dernières mises à jour et tutos de certains programmes stars.

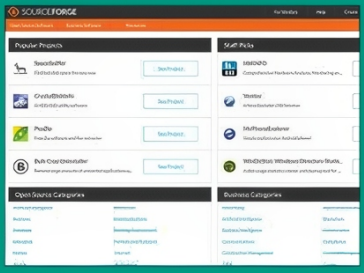
Lien : github.com



SOURCEFORGE

> Le libre pour tous !

À la fois destiné aux utilisateurs et aux développeurs, Sourceforge est plus accessible que GitHub. Cette plateforme de distribution de logiciels libres et open source offre une



grande variété de logiciels pour différents systèmes d'exploitation et des index de recherche qui facilitent grandement la vie.

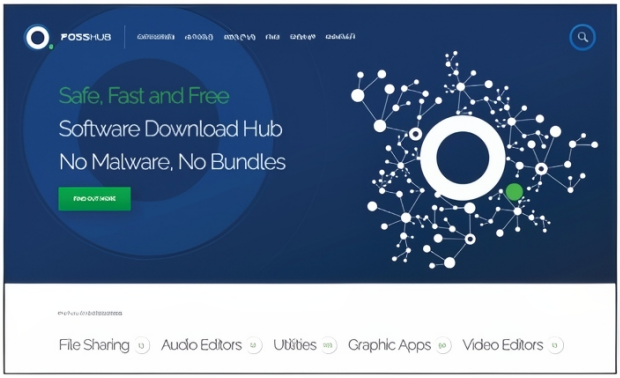
Lien : sourceforge.net

FOSSHUB

> Vérifiés sans malwares

Ce site propose un téléchargement sécurisé de logiciels gratuits et open source, couvrant une large gamme de catégories logicielles. Il est connu pour son engagement envers la sécurité des programmes qu'il héberge. Fosshub s'engage à offrir des téléchargements sans logiciels malveillants, adwares, ou spywares.

Lien : www.fosshub.com



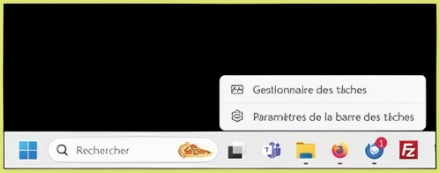
NE PLUS REGROUPER LES FENÊTRES OUVERTES

INFOS
[Barre des tâches]
Difficulté :

Sur Windows 10 et 11, les fenêtres d'une même application sont regroupées sous une seule icône dans votre barre des tâches. Pratique… sauf si vous possédez un grand écran voire plusieurs écrans pour jongler de l'un à l'autre. Voici comment dissocier ces fenêtres pour avoir un accès direct à chacune d'entre-elles.

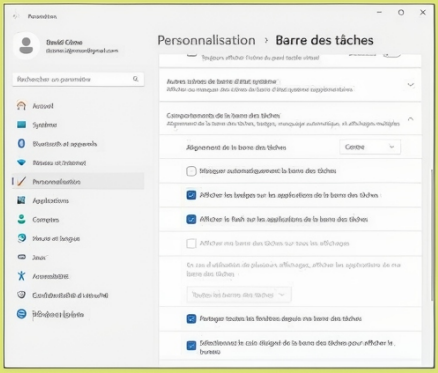
01 PARAMÈTRES

Faites un clic droit sur un espace vide de votre barre des tâches. Cliquez maintenant sur **Paramètres de la barre des tâches.**



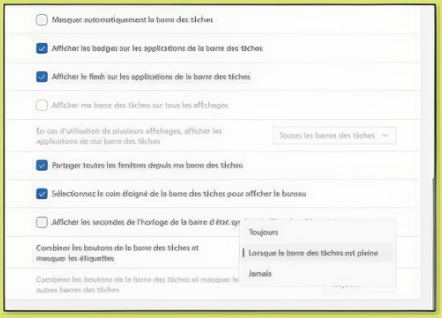
02 RÉGLAGES

Dans la fenêtre qui s'est ouverte, sélectionnez en bas **Comportement de la barre des tâches.**



03 DISSOCIER

En bas de ce menu, trouvez **Combiner les boutons de la barre des tâches et masquer les étiquettes**. Ouvrez ce menu et choisissez **Lorsque la barre des tâches est pleine.**



04 RÉSULTAT

Ainsi, tant que l'espace de votre barre des tâches ne sera pas entièrement rempli de boutons d'applications, vous aurez accès à chacune des fenêtres ouvertes individuellement.

L'INFORMATIQUE FACILE
POUR TOUS !

CHEZ VOTRE MARCHAND DE JOURNAUX

DECRYPTAGE

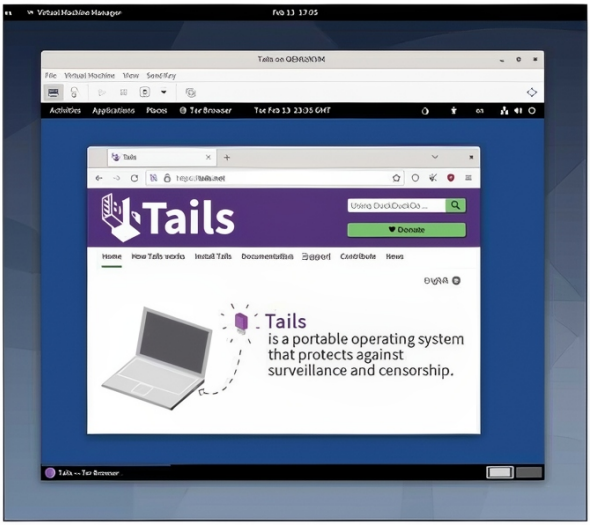
TAILS

ANONYMISE VOTRE PC

Tails, "The Amnesic Incognito Live System", est un système d'exploitation dédié à la sécurité et à la protection de la vie privée. Il s'agit d'un système live, ce qui signifie qu'il peut être démarré à partir d'une clé USB ou d'un DVD sans laisser de traces sur l'ordinateur utilisé après son redémarrage.

Quel que soit votre ordinateur et son système d'exploitation (Windows, Mac, Linux…), vous pouvez avoir besoin de lancer une session vraiment sécurisée sans craindre la présence d'un espion installé sur votre terminal ou qui surveille vos données transitant sur le Web. C'est la promesse de Tails, un système d'opération qui se lance à la demande via un port USB et qui fonctionne comme un container inviolable. Cet OS se base sur Debian GNU/Linux et route l'ensemble du trafic Internet à travers le réseau Tor, masquant ainsi l'identité et la localisation de l'utilisateur.

Depuis son lancement en 2009, Tails a constamment évolué, intégrant de nouvelles technologies de chiffrement et



> Un système entier sur un simple support USB qui fonctionne comme un container inviolable. Tails est utilisable à la demande, avec n'importe quel PC

UN OUTIL ANTI-SURVEILLANCE OU MAFIEUX ?

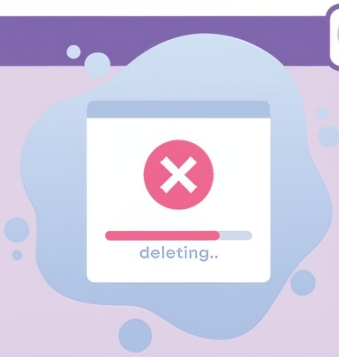
Tails continue de faire l'actualité, avec des mises à jour régulières qui améliorent ses fonctionnalités et sa sécurité. Toutefois, comme tout outil de protection de la vie privée, Tails fait l'objet de controverses. Certains gouvernements et organisations le voient d'un mauvais œil, arguant qu'il pourrait faciliter des activités illégales en offrant un anonymat presque parfait. Ces critiques sont régulièrement balayées par la communauté Tails, qui souligne l'importance de la vie privée et de la liberté d'expression dans un monde numérique.

MODE LIVE AVEC AMNÉSIE

Tails est principalement conçu pour être utilisé comme un système live, ce qui signifie qu'il peut être démarré à partir d'une clé USB ou d'un DVD sans avoir à être installé sur l'ordinateur. Plus important encore, il ne laisse aucune trace sur l'ordinateur une fois qu'il est éteint, grâce à sa fonctionnalité d'amnésie. Cela empêche la récupération de l'activité ou des données après utilisation.

CHIFFRER CE QUI DOIT ÊTRE CONSERVÉ

Pour ceux qui souhaitent conserver des documents ou des réglages entre différentes sessions d'utilisation, Tails offre la possibilité de créer un volume chiffré persistant sur la clé USB. Ce volume est chiffré avec une forte cryptographie, protégeant les données en cas de perte ou de vol de la clé USB.



LA NOUVELLE VERSION 6.0 DE TAILS EST SORTIE EN FÉVRIER DERNIER.

TAILS : UN PACK « TOUT-EN-UN »

Voici une liste non exhaustive de certaines des fonctionnalités et programmes préinstallés sur Tails. Ces programmes permettent aux utilisateurs de naviguer sur Internet, de communiquer, de gérer des fichiers et d'effectuer des tâches bureautiques tout en minimisant les risques de surveillance et d'analyse de leur activité en ligne.

- **Tor Browser :** un navigateur web modifié à partir de Mozilla Firefox, conçu pour une navigation anonyme via le réseau Tor.

- **Thunderbird :** un client de messagerie électronique pour envoyer et recevoir des emails de manière sécurisée.

- **KeePassXC :** un gestionnaire de mots de passe pour stocker de manière sécurisée tous vos mots de passe.

- **LibreOffice :** une suite bureautique complète pour créer et éditer des documents texte, des feuilles de calcul, des présentations, etc.

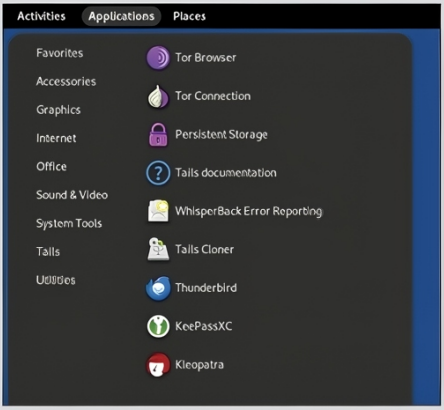
- **GIMP :** un programme de manipulation d'images pour l'édition et la création d'images numériques.

- **Audacity :** un logiciel d'édition audio permettant d'enregistrer et de modifier des fichiers audio.

- **Electrum :** un portefeuille Bitcoin pour effectuer des transactions en Bitcoin de manière anonyme.

- **OnionShare :** un outil pour partager des fichiers de manière anonyme et sécurisée à travers le réseau Tor.

- **GNOME Sound Recorder :** un enregistreur de son simple pour enregistrer de l'audio avec un microphone.



- **Pidgin** : un client de messagerie instantanée qui supporte plusieurs protocoles, configuré pour une utilisation anonyme avec OTR (Off-the-Record Messaging) pour le chiffrement des conversations.

- **MAT (Metadata Anonymisation Toolkit) :** un outil pour supprimer les métadonnées des fichiers, réduisant ainsi les risques de fuites d'informations personnelles.

- **Tails Installer :** un outil pour installer Tails sur une clé USB ou un disque dur externe.

PEUT-ON INSTALLER CE QUE L'ON VEUT SUR TAILS ?

Tails est basé sur Debian GNU/Linux, ce qui signifie que les applications doivent être compatibles avec Linux pour fonctionner. De nombreux programmes populaires sur Windows ou macOS, comme Microsoft Office ou les logiciels Adobe, n'ont pas de versions natives pour Linux. Bien qu'il existe des alternatives Linux pour presque toutes les applications Windows, l'installation de logiciels non pris en charge nativement par Tails peut compromettre les fonctionnalités de sécurité intégrées de Tails. Par exemple, installer et utiliser Google Chrome au lieu du Tor Browser serait une erreur critique : autant jeter Tails à la poubelle !

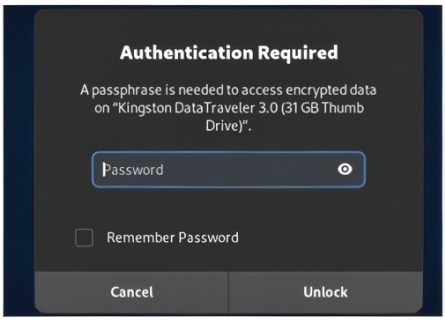
de sécurité pour rester à la pointe de la protection des données. Son but premier est de permettre à ses utilisateurs de contrer la surveillance de masse et les attaques informatiques, offrant ainsi un havre de paix dans un monde numérique de plus en plus sous surveillance.

OBJECTIF ANONYMAT !

Tails s'appuie donc sur le réseau Tor pour chiffrer et anonymiser l'ensemble du trafic Internet de ses utilisateurs, rendant ainsi leur navigation véritablement privée. Outre l'accès à un Internet anonyme, Tails comprend une suite d'outils de sécurité préinstallés, parmi laquelle figurent des applications de messagerie chiffrée, de gestion de mots de passe et de cryptage de fichiers. Tails ne laisse aucune trace sur l'ordinateur utilisé après redémarrage, grâce à son système d'exploitation amnésique, assurant ainsi une couche supplémentaire de sécurité.

SÉCURITÉ PAR DÉFAUT

Tails est conçu avec une approche de sécurité par défaut. Cela inclut l'utilisation de logiciels open source largement audités, la désactivation de composants logiciels potentiellement vulnérables et la configuration par défaut de ses applications pour maximiser la confidentialité et la sécurité. De plus, étant basé sur Debian GNU/Linux, il bénéficie des mises à jour de sécurité régulières et des pratiques de sécurisation du système d'exploitation Linux. En utilisant des outils et des configurations qui minimisent l'empreinte numérique, Tails rend plus difficile pour les sites web et les services en ligne de suivre ou d'identifier ses utilisateurs.



VOS DOSSIERS CHIFFRÉS SONT ACCESSIBLES VIA MOTS DE PASSE.

QUEL SUPPORT USB CHOISIR ?

La taille de l'image ISO de Tails varie légèrement avec chaque version, mais elle est généralement autour de 1.1 à 1.2 Go. Cette taille est importante, car elle doit être prise en compte lors du choix du média sur lequel Tails sera installé ou gravé.

Pour installer Tails sur une clé USB ou un disque dur externe, il est recommandé d'utiliser un périphérique d'au moins 8 Go de capacité. Cette recommandation prend en compte non seulement l'espace nécessaire pour l'image ISO elle-même, mais aussi pour le volume de persistance optionnel qui permet de sauvegarder des données entre les sessions d'utilisation. Un périphérique de plus grande capacité pourrait être nécessaire si vous prévoyez de stocker une grande quantité de données de manière persistante.

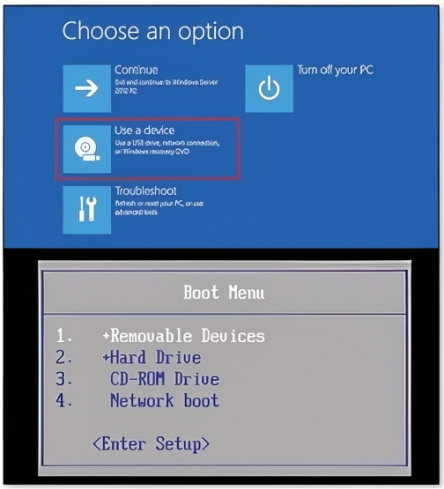
> Tails est conçu avec une approche de sécurité par défaut. Rien de ce que vous ferez ne doit pouvoir être tracé ou récupéré.

COMMENT LANCER TAILS ?

PRATIQUE

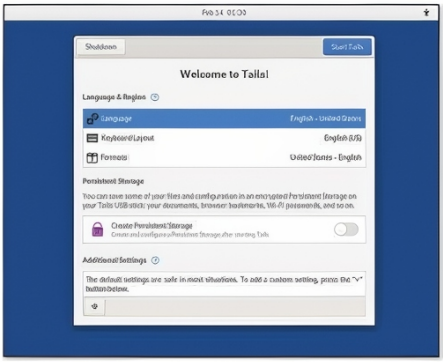
01 › BOOT USB

Pour démarrer Tails, insérez la clé USB dans un port USB de l'ordinateur, puis redémarrez-le. Vous devrez peut-être accéder au menu de démarrage de l'ordinateur ou modifier l'ordre de démarrage dans le BIOS/UEFI pour permettre le démarrage depuis la clé USB.



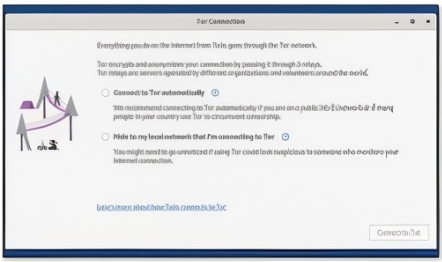
02 › CONFIGURER

Une fois que Tails démarre, vous serez accueilli par un écran de bienvenue où vous pouvez configurer des options telles que la langue et le clavier avant d'entrer dans l'environnement de bureau.



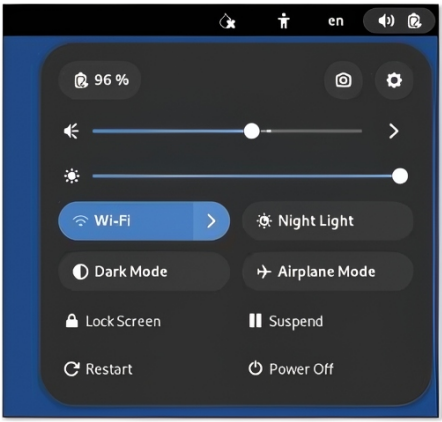
03 › INTERNET

Vous serez bien sûr amené à configurer votre accès Internet et votre connexion à Tor.



04 › ÉTEINDRE

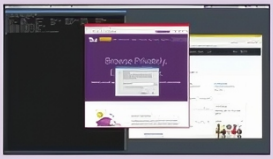
Pour éteindre Tails, cliquez sur le menu d'application en haut à gauche, sélectionnez le bouton d'arrêt, puis choisissez **Éteindre**. Tails se fermera et vous indiquera quand il est sûr de retirer la clé USB.
Il est crucial de suivre cette procédure pour s'assurer que toutes les données temporaires sont effacées et que le volume de persistance (si utilisé) est correctement démonté, préservant l'intégrité des données et la sécurité du système.



TOP 5 ALTERNATIVES À TAILS

Plusieurs systèmes d'exploitation alternatifs à Tails offrent des niveaux élevés de sécurité informatique, de protection de la vie privée, et d'anonymat. Chacun a ses propres caractéristiques et cas d'utilisation spécifiques. Voici quelques-unes des alternatives les plus notables :

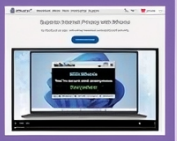
QUBES OS > Je cloisonne !



Qubes OS base sa résistance aux intrusions et à la surveillance sur la virtualisation. Il partitionne les différentes parties de l'activité quotidienne de l'utilisateur, comme naviguer sur Internet, travailler sur des documents, ou vérifier les emails, en domaines isolés exécutés dans des machines virtuelles séparées. Cette séparation permet de limiter les dommages potentiels en cas d'attaque logicielle.

Lien : www.qubes-os.org

WHONIX > IP à double tour



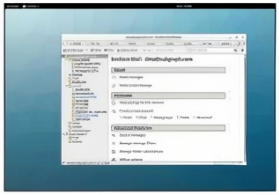
Whonix est un système d'exploitation axé sur l'anonymat, qui utilise également Tor pour tout le trafic Internet et fonctionne sur le principe de la sécurité par l'isolement. Il se compose de deux parties : une «Workstation» où l'utilisateur effectue toutes ses activités, qui est isolée et ne peut pas voir l'IP réelle de l'utilisateur, et une «Gateway» qui route tout le trafic à travers le réseau Tor.

Lien : www.whonix.org

SUBGRAPH OS > Tout terrain

Subgraph OS est un système d'exploitation conçu pour être résistant aux attaques logicielles et à la surveillance en ligne. Il intègre des technologies de sécurité avancées comme le sandboxing des applications, le système de fichiers chiffré, et la communication anonyme via Tor.

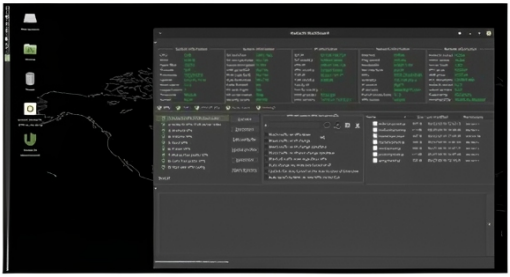
Lien : subgraph.com



KODACHI LINUX > Internet blindé

Linux Kodachi route également tout le trafic Internet à travers le réseau Tor et utilise un VPN et des DNS sécurisés pour une couche supplémentaire de protection en ligne. Convient aux utilisateurs qui cherchent une solution tout-en-un pour la navigation sécurisée et anonyme sur Internet.

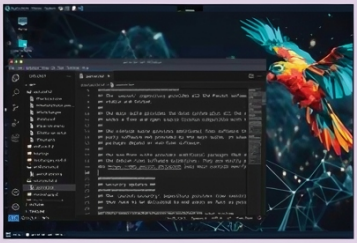
Lien : sourceforge.net/projects/linuxkodachi/



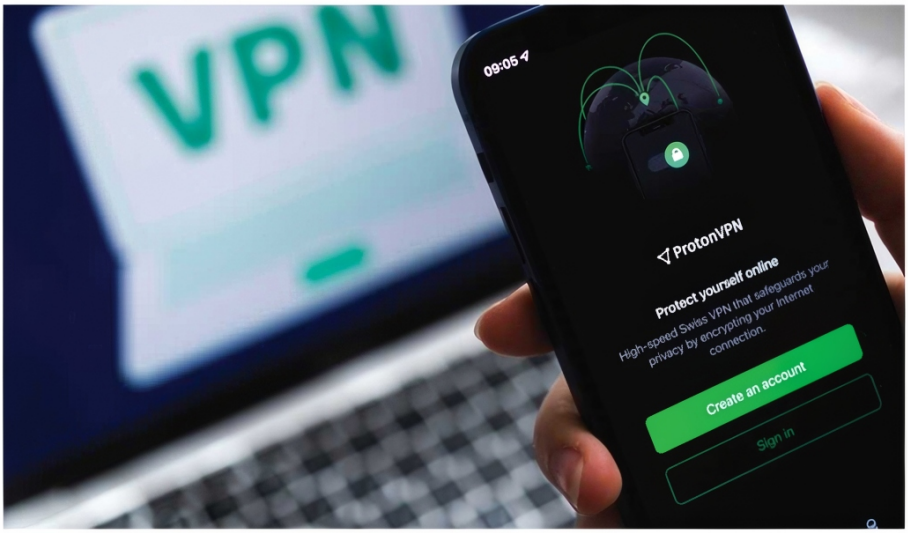
PARROT SECURITY OS > Pro et accessible

Parrot Security OS est une distribution basée sur Debian conçue pour les tests de sécurité, l'analyse médico-légale numérique, le piratage éthique, et la protection de la vie privée. Tout en offrant des dizaines d'outils pour les professionnels de la sécurité et les hackers, Parrot OS propose également une édition Home pour une utilisation quotidienne avec un accent sur la confidentialité.

Lien : www.parrotsec.org



LE MEILLEUR VPN GRATUIT DU MARCHÉ



Parmi toutes les offres de VPN gratuits, difficile de trouver un service qui ne soit pas limité en termes de datas ou alors manquant cruellement de sécurité (un comble !). ProtonVPN Free offre un Internet illimité et l'un des anonymats les plus puissants du marché.

La version Premium de ProtonVPN est l'une des plus abouties et des plus sûres au monde. Le sérieux et la transparence dont fait montre la société helvétique lui confèrent une aura de confiance et de sécurité unique. Côté performances, là encore, les utilisateurs louent la qualité et la puissance de ses services même si les vitesses d'uploads et de downloads restent, en moyenne, inférieures à celles de services comme NordVPN, ExpressVPN ou Surfshark. Si ProtonVPN ne trône pas parmi les leaders du secteur, c'est surtout à cause de ses prix, nettement plus élevés que la concurrence (comptez 6 euros par mois pour un abonnement d'un an).

UNE VERSION GRATUITE GÉNÉREUSE ET SANS COMPROMIS

Mais une bonne surprise attend les internautes qui souhaiteraient tester ProtonVPN : sa version gratuite offre sans doute le meilleur rapport qualité/performances/sécurité du marché. Vous accédez à un VPN sans limitation de datas, bénéficiant de la même architecture sécurisée que la version Premium et bien sûr avec la garantie que vos données ne seront pas monétisées d'une façon ou d'une autre grâce à une politique no-log toujours aussi stricte. Les bémols viennent de la limitation géographique : ProtonVPN Free ne donne accès qu'à 100 serveurs situés dans 3 pays

(Japon, Pays-Bas et USA) et à des débits réduits par rapport à la version Premium. Le visionnage de contenus en streaming peut être compromis selon les jours et horaires de connexion. Malgré ces contraintes, ce VPN gratuit reste incroyablement généreux et fiable face à d'autres offres, soit plus limitées, soit plus inquiétantes, en matière de protection des données utilisateurs.

PROTECTION « SWISS QUALITAT »

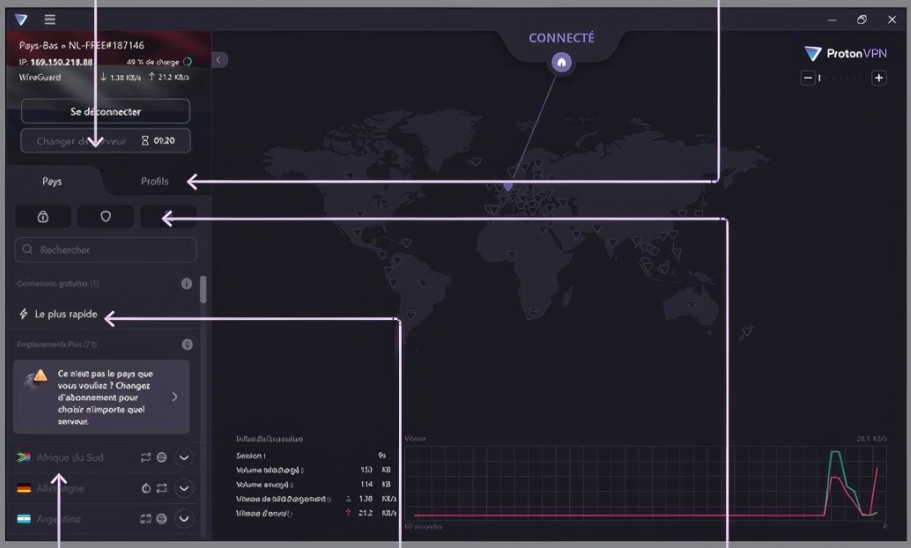
Contrairement à de nombreux autres services VPN, Proton VPN applique une politique stricte de non-conservation des logs, garantissant ainsi que les activités en ligne de ses utilisateurs ne sont jamais enregistrées, surveillées, ni partagées avec des tiers. Cette politique est cruciale pour les utilisateurs qui cherchent à protéger

> La version gratuite de ProtonVPN vous offre la puissance d'un VPN Pro malgré ses limitations en termes de géolocalisation et de vitesses de connexions.

L'INTERFACE DE PROTON VPN FREE

Changer de serveur > Vous pouvez demander à être basculé sur un autre serveur pour tester sa stabilité et rapidité. Attention, un temps de latence est nécessaire avant de changer à nouveau de serveur.

Profils > Enregistrez vos paramètres et serveurs préférés pour une utilisation future. Cette fonction n'est disponible que dans la version payante.



Pays > La version gratuite ne vous permet pas de choisir librement mais vous connectera à l'un des quelques serveurs disponibles (États-Unis, Japon, Pays-Bas, Roumanie).

Le plus rapide > Se connecter automatiquement au serveur qui vous fournira la connexion la plus rapide

Kill switch > Disponible dans la version gratuite, cette fonction vous permet d'être déconnecté immédiatement d'Internet si le VPN se trouve malencontreusement désactivé.

leur vie privée en ligne contre les regards indiscrets des annonceurs, des fournisseurs de services Internet et des gouvernements.
En outre, ProtonVPN utilise un cryptage de pointe pour sécuriser les données des utilisateurs. En s'appuyant sur des protocoles sécurisés tels que IKEv2/IPSec et OpenVPN, le service assure que toutes les données transitant par ses serveurs sont entièrement cryptées et à l'abri des interceptions.

SECURE CORE AU CŒUR DU DISPOSITIF

Une autre caractéristique qui fait de ProtonVPN un choix de prédilection est son réseau Secure Core. Cette fonctionnalité route le trafic des utilisateurs à travers plusieurs serveurs avant de quitter le réseau de ProtonVPN, augmentant ainsi significativement l'anonymat et la sécurité. Les serveurs Secure Core sont situés dans des pays réputés pour la protection de la vie privée, comme la Suisse, l'Islande et la Suède, offrant une couche supplémentaire de sécurité.
ProtonVPN offre également une protection contre les fuites DNS et WebRTC, s'assurant que les requêtes DNS des utilisateurs passent uniquement à travers le tunnel sécurisé du VPN et empêchant toute fuite d'adresse IP via WebRTC. Ces mesures renforcent davantage l'anonymat en ligne et protègent contre les expositions accidentelles de données.
Avec une interface utilisateur intuitive et un support client réactif, ProtonVPN est accessible même pour les novices de la sécurité en ligne. Les utilisateurs peuvent facilement sélectionner des serveurs optimisés pour différents usages, tels que le streaming ou le partage de fichiers en P2P, rendant ProtonVPN non seulement sécurisé, mais aussi adaptatif selon vos besoins.

LA SUISSE, PARADIS DE LA DATA ?

La Suisse est reconnue pour sa neutralité politique et ses lois strictes en matière de protection de la vie privée, héritage de ses spécificités bancaires et géopolitiques. Être basé en Suisse offre plusieurs avantages significatifs à ProtonVPN et à ses utilisateurs.

① Loi fédérale stricte
La législation suisse sur la protection des données est l'une des plus strictes au monde. La Loi fédérale sur la protection des données (LPD) protège efficacement les informations personnelles et limite la surveillance gouvernementale. ProtonVPN peut ainsi s'engager à ne pas conserver de journaux d'activité (no-logs policy) avec une plus grande légitimité juridique.

② Pas de coopération internationale par défaut
En étant basé en Suisse, ProtonVPN bénéficie d'une position sécurisée en termes de demandes d'informations par des gouvernements étrangers. La Suisse n'étant membre ni de l'Union européenne ni des alliances de surveillance des «Five Eyes» ou «Fourteen Eyes» (accords de partage de renseignements entre certains pays), elle est moins susceptible de soumettre ses entreprises à des demandes de données étrangères. Les transferts internationaux ne sont autorisés que vers des pays offrant un niveau de protection des données équivalent à celui de la Suisse. Cette disposition garantit que les données des individus restent protégées selon les standards suisses, même lorsqu'elles sont transférées à l'étranger.

③ Serveurs bénéficiant d'une sécurisation de type militaire
La Suisse est enfin un gruyère militarisé et ultrasécurisé. Des centaines de structures jalonnent le territoire, sous terre, creusées au cœur de certaines montagnes, etc. ProtonVPN a pu par exemple récupérer d'anciens bunkers pour ses serveurs Secure Core. Ils bénéficient toujours des protocoles et standards d'accès et de protection les plus élevés.

PREMIÈRE CONNEXION AVEC PROTON VPN FREE

PRATIQUE

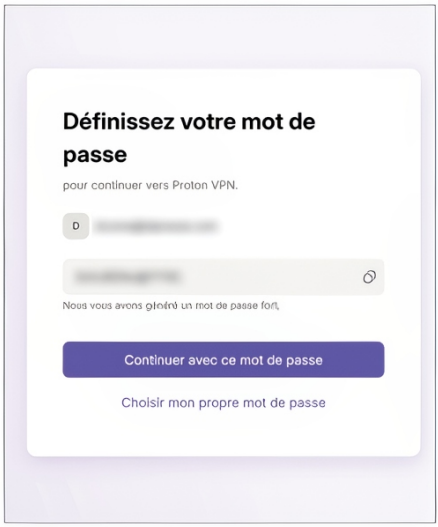
01 › CRÉATION DE COMPTE

Sur le site, passez par **Obtenir Proton VPN Free > Je choisis free**. Renseignez votre adresse email et choisissez un mot de passe ou conservez celui

proposé par Proton VPN. Attention, copiez bien ce mot de passe, vous en aurez besoin dès l'étape 3.

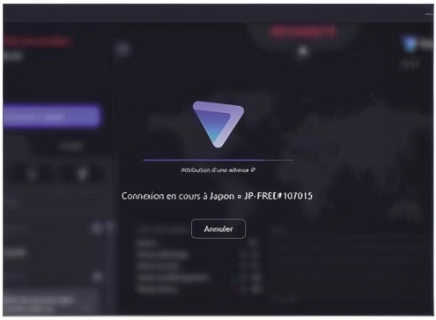
02 › TÉLÉCHARGER

Cliquez sur **Télécharger** puis confirmez dans la page Web suivante l'application qui vous convient (ici **Télécharger Proton VPN** pour Windows).



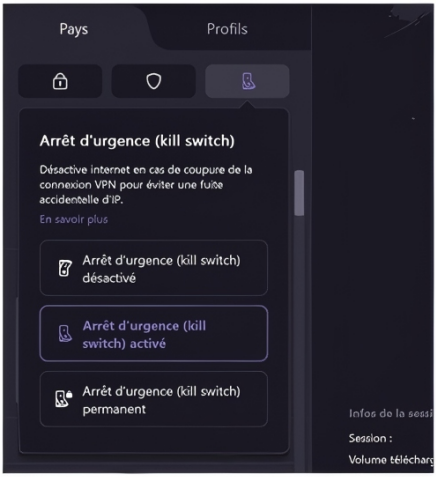
03 › PREMIÈRE CONNEXION

Lancez l'exécutable et choisissez la langue française. Finalisez l'installation puis une fois le VPN lancé, renseignez vos identifiants. Cliquez sur **Connexion rapide**. Proton VPN cherche un serveur disponible. Vous êtes connectés !



04 › KILL SWITCH

Pour activer le Kill switch (« Arrêt d'urgence »), cliquez sur l'icône d'interrupteur à gauche de l'interface puis sélectionnez **Arrêt d'urgence activé** (il durera le temps de votre session) ou **Arrêt d'urgence permanent** (il sera activé par défaut à chaque lancement de Proton VPN).



TUTO

AJOUTEZ UN FILIGRANE À UN DOCUMENT IMPORTANT

Filigrane Facile est un service en ligne gratuit proposé par l'État. Il se destine aussi bien aux particuliers qu'aux entreprises.

Protégez vos documents et images les plus sensibles en leur apposant un filigrane personnalisé avant tout envoi. Accessible gratuitement par tous, ce service ne requiert aucun téléchargement et est compatible avec une vaste gamme d'appareils connectés, du smartphone à l'ordinateur de bureau. Vous pourrez ainsi marquer cartes d'identité, passeports, vos photos ou encore des chèques, afin de prévenir toute tentative de fraude ou d'usurpation d'identité lors de leur transmission.

GRATUIT ET RAPIDE

L'utilisation de Filigrane Facile est un jeu d'enfant : après avoir chargé le document à sécuriser sur la plateforme, les utilisateurs peuvent y apposer un filigrane de leur choix en quelques clics. Seule la raison d'envoi du document doit être précisée pour prévenir les futures utilisations malveillantes. Une fois le processus terminé, le document est disponible au téléchargement au format PDF, avant d'être automatiquement supprimé du serveur pour garantir la confidentialité.

Malgré son efficacité, il est important de rappeler que la présence d'un filigrane ne rend pas un document inviolable. Ici, ce service gouvernemental ne propose pas une signature électronique infalsifiable, mais bien un simple filigrane. Des logiciels spécialisés peuvent, dans certains cas, retirer ces marques.

PAS INNOVANT, MAIS PRATIQUE !

Au-delà de Filigrane Facile, plusieurs alternatives existent pour ceux à la recherche d'options plus personnalisées. Make Watermark, par exemple, cible spécifiquement les images. Mais des services plus poussés comme Canva et bien sûr Photoshop se distinguent par leur polyvalence et leurs nombreuses fonctionnalités, permettant une manipulation poussée des images et filigranes.

FILIGRANE FACILE EN 2 CLICS !

PRATIQUE

01 GÉNÉRER

Sur le site, commencez par télécharger votre fichier via **Parcourir** puis indiquez le texte qui servira de marquage dans le champ **Indiquez le filigrane à insérer**. Cliquez enfin sur **Ajouter le filigrane**.

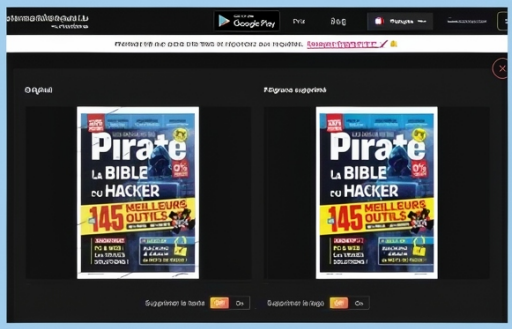
02 RÉCUPÉRER

Une fois votre document généré, vous pouvez le récupérer via **Télécharger le document. filigrané**.

03 RENDU

Malheureusement, l'orientation, la taille et l'emplacement du filigrane ne peuvent être choisis. Par défaut, Filigrane Facile appose un filigrane en diagonale répété sur l'ensemble du document. L'avantage est qu'il s'agit d'un filigrane fastidieux à retirer pour celui qui voudrait s'y attaquer.

PEUX-TON RETIRER UN FILIGRANE ?



La réponse est immédiatement oui. N'importe quel bon graphiste, avec un peu de temps, pourra effacer plus ou moins facilement un filigrane. Mais tout le monde n'est pas graphiste. Il existe aussi des éditeurs de photos qui proposent de simplifier ce travail pour monsieur Tout-le-Monde ainsi que des services spécialisés. Nous avons par exemple testé trois d'entre eux : Watermark Remover (watermarkremover.io), PicWish (picwish.com) et Vidmore (vidmore.com). Les deux derniers restent laborieux et finalement assez décevants (beaucoup d'autres détails sont perdus). Par contre, le résultat de Water Marker est tout à fait satisfaisant avec notre document protégé par Filigrane Facile. La seule contrainte (hormis l'inscription) est de téléverser un fichier image (png, jpeg, etc.) plutôt qu'un PDF. Une conversion préalable s'impose donc.

DECRYPTAGE

ACTIVEZ LA PROTECTION ANTI RANSOMWARES DE WINDOWS 11

Windows 11 possède un dispositif anti-ransomware qui n'est pas activé par défaut. Son objectif est de prévenir toute infection. Microsoft Defender devra devenir votre antivirus par défaut pour que cette protection fonctionne en temps réel.

Microsoft intègre un outil anti ransomware baptisé « Dispositif d'accès contrôlé aux dossiers ». L'idée n'est pas de supprimer un rançongiciel puis de libérer vos fichiers en cas d'attaque : non, l'objectif est qu'aucun malware ne puisse chiffrer les dossiers cibles que vous aurez choisis de protéger par ce dispositif. L'accès contrôlé aux dossiers désigne ainsi des dossiers spécifiques auxquels seules les applications jugées inoffensives ou approuvées par

vos soins seront autorisées à accéder. Cela empêchera donc le contenu des dossiers d'être modifié ou chiffré par des malwares tels que les rançongiciels. En cas de fichier ou de programme suspect, Windows les bloquera tout simplement et les empêchera d'agir sur vos répertoires ou fichiers protégés.

RAPPEL SUR LES RANSOMWARES

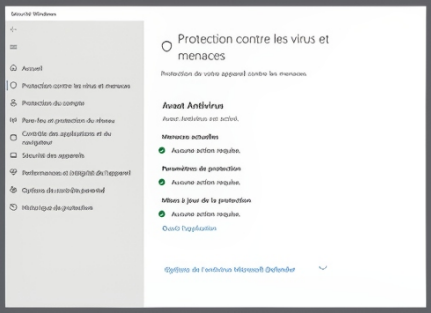
Un rançongiciel est un logiciel malveillant qui chiffre vos fichiers ou vous empêche d'utiliser votre ordinateur jusqu'à ce que vous payiez une somme d'argent (rançon) pour les déverrouiller. Si votre ordinateur est connecté à un réseau, le rançongiciel peut également se propager vers d'autres ordinateurs ou périphériques de stockage sur le réseau. Les attaques par ransomware se multiplient ces dernières années car

UN RANÇONGICIEL PREND LE CONTRÔLE SUR DES FICHIERS OU DES DOSSIERS ENTIERS DE VOTRE PC, EN LES CHIFFRANT ET EN LES RENDANT INACCESSIBLES. POUR LES DÉVERROUILLER, UN PROCESSUS DE DÉCHIFFREMENT EST NÉCESSAIRE, PROCESSUS QUE LES PIRATES PEUVENT VOUS FOURNIR... MOYENNANT LE PAIEMENT D'UNE RANÇON.

Mieux vaut prévenir que guérir : la solution gratuite de Microsoft vise à éviter l'infection, pas à la réparer

ATTENTION : PROBLÈMES DE COMPATIBILITÉ AVEC D'AUTRES ANTIVIRUS !

Si vous utilisez un logiciel antivirus (Avast!, McAfee, ...), celui-ci supplante la solution de protection en temps réel de Microsoft Defender. Or, cette protection doit être activée pour que vous puissiez utiliser le « Dispositif d'accès contrôlé aux Dossiers ». Dans votre barre de recherche, tapez **Protection contre les virus et les menaces** puis validez. Si vous n'accédez pas à toutes les fonctions

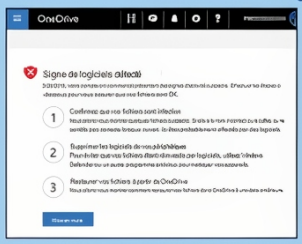


Windows, c'est que votre antivirus gère par défaut tous les outils de sécurité qui protègent votre PC. Vous devrez donc le désinstaller pour profiter par exemple de l'outil anti-ransomwares de Microsoft !
Microsoft Defender prendra alors automatiquement le relais de votre protection. Le choix est donc cornélien si vous êtes habitué à tel ou tel antimalware. Mais sachez que Microsoft Defender est plébiscité pour la qualité de ses défenses et services associés, qu'il est gratuit et qu'il ne vous inondera pas de pop-ups commerciaux comme les autres antivirus gratuits.

ICI, LE LOGICIEL AVAST! GÈRE LES DÉFENSES PRINCIPALES DU PC. MAIS CELA EMPÊCHE L'UTILISATEUR D'ACCÉDER À CERTAINES FONCTIONS SÉDUISANTES DE MICROSOFT DEFENDER. DÉSINSTALLER AVAST! EST NÉCESSAIRE POUR RETROUVER TOUTES LES OPTIONS DE CE DERNIER, NOTAMMENT SON OUTIL CONTRE LES RANÇOGICIELS.

très lucratives pour les pirates et assez faciles à mettre en place.
Dans son dernier « Panorama de la Cybermenace », l'Agence nationale de sécurité des systèmes d'information (Anssi) constatait pour 2023 que le nombre total d'attaques par rançongiciel portées à sa connaissance est supérieur de 30 % à celui constaté en 2022. De grandes entreprises ou institutions (hôpitaux, administrations, ...) sont visés car les sommes demandées sont importantes. Mais les particuliers sont aussi ciblés avec des rançons de quelques dizaines ou centaines de dollars réclamées à des personnes pour la plupart incapables de déjouer le piège dans lequel elles sont tombées.

MICROSOFT 365 : LE CLOUD POUR RESTAURER EN CAS D'ATTAQUE



Pour les utilisateurs qui possèdent une licence Microsoft 365 (Office, OneDrive), une seconde solution de sécurité anti-ransomwares est également inclue. Cette fois-ci, l'objectif est de vous protéger d'une attaque mais aussi de restaurer des fichiers et dossiers bloqués grâce au cloud. Quand Microsoft 365 détecte une attaque par rançongiciel, vous recevez une notification sur votre appareil et recevez un e-mail de Microsoft 365. Si vous n'êtes pas abonné, votre première notification et votre première récupération sont gratuites. Vous aurez la possibilité de supprimer un fichier ou programme que Microsoft juge potentiellement infecté par un rançongiciel. En cas de blocage de tout ou partie de votre PC, une option de restauration à partir du cloud est également proposée. Vous pourrez choisir un jour et un horaire antérieurs à l'infection pour retrouver votre contenu sauvegardé. Pour rappel, les versions premium de Onedrive proposent effectivement une copie systématique de vos contenus PC sur le cloud (jusqu'à 1To).

DISPOSITIF D'ACCÈS CONTRÔLÉ AUX DOSSIERS : COMMENT ÇA MARCHE ?

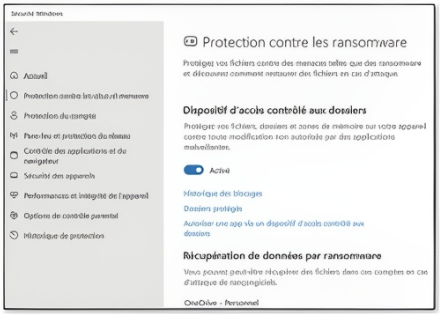
PRATIQUE

01› PROTECTION EN TEMPS RÉEL

Vérifiez que la protection en temps réel de Microsoft Defender soit bien activée. Allez dans **Paramètres de protection contre les menaces et les virus > Gérer les paramètres**. Passez le bouton **Protection en temps réel** sur **Activé** s'il ne l'était pas déjà.

02› ACTIVER LE DISPOSITIF

En bas de la page, allez dans **Dispositif d'accès contrôlé aux dossiers > Gérer l'accès contrôlé aux dossiers.** En activant **Dispositif d'accès contrôlé aux dossiers**, vous activez la protection de vos fichiers,



dossiers et zones de mémoire de votre PC contre toute modification non autorisée par des applications malveillantes.

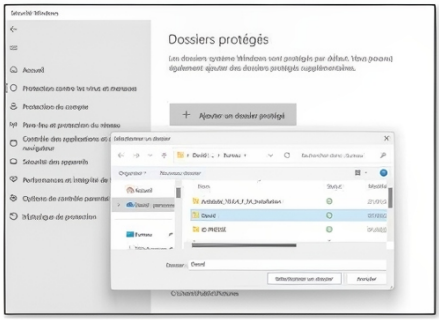
03 OPTIONS

Des options essentielles sont apparues suite à l'activation. **Dossiers** protégés vous permettra de définir les dossiers à sécuriser. Par défaut, le module

anti-rançongiciel de Microsoft protège vos répertoires *Documents*, *Images*, *Vidéos*, *Musique* et *Favoris*.

04 CHOISIR QUOI PROTÉGER

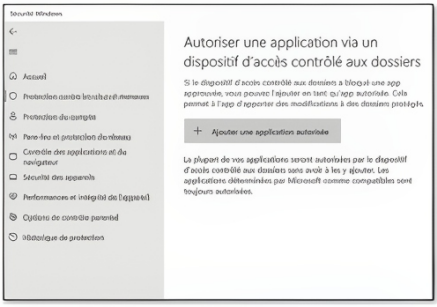
En cliquant sur **Ajouter un dossier protégé**, vous pourrez choisir sur votre disque dur le ou les dossiers à sécuriser. Il peut s'agir de petits dossiers



comme des répertoires racine ! Prenez le temps de réfléchir à vos besoins pour ne rien oublier de sensible.

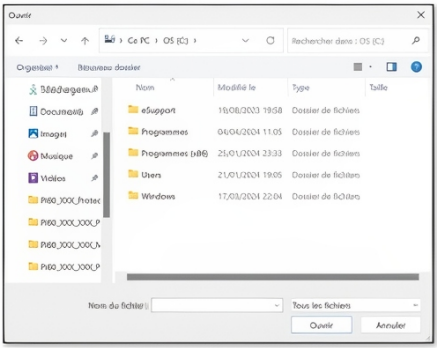
05 DÉTECTIONS ERRONÉES

Il est possible que certains programmes utilisés régulièrement ne soient plus permis d'accéder aux dossiers sécurisés. L'outil de Windows peut, par erreur, classer des applications inoffensives comme menaçantes pour vos informations. Pour contourner ces détections erronées, cliquez sur **Autorisez une app via un dispositif d'accès contrôlé aux dossiers**.



06 LISTE BLANCHE

Via **Ajouter une application autorisée**, vous pouvez soit débloquer l'accès de programme bloqués récemment par Microsoft, soit aller chercher ceux à



inclure dans cette liste « approuvée » par vos soins. Dans ce dernier cas, parcourez votre répertoire jusqu'au dossier d'installation de vos logiciels (habituellement situé dans **C:Programmes** ou **C:Programmes (x86)**).

CONSEIL

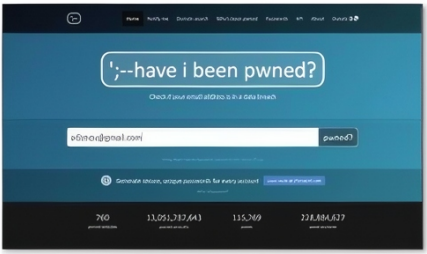
Si vous essayez d'enregistrer un fichier dans un dossier et que celui-ci est bloqué, cela signifie que l'application que vous utilisez est empêchée d'effectuer un enregistrement à cet emplacement. Si cela se produit, enregistrez le fichier dans un autre emplacement de votre appareil. Ensuite, suivez les étapes 5 et 6 pour débloquer l'application. Vous serez en mesure d'enregistrer vos fichiers à l'emplacement souhaité.

MES IDENTIFIANTS ONT-ILS ÉTÉ VOLÉS ?

PRATIQUE

«Have I Been Pwned?» est un service qui permet aux utilisateurs de vérifier si leurs emails et certains comptes personnels associés ont été compromis.

INFOS [Have I Been Pwned ?]
Où le trouver ? [haveibeenpwned.com]
Difficulté :



01› CHOISIR LE MAIL À SCANNER

Saisissez l'adresse e-mail que vous voulez vérifier et cliquez sur **pwned?**. Le service scanne sa base de données de compromission et de vols de données connus.

02› ALORS, ALORS ?

Si l'email ou les identifiants d'un compte associé ont été volés puis diffusés, vous aurez le message **Oh no — pwned!**. Plus bas sur la page, vous aurez le détail des différents services Web dont les identifiants ont été compromis : changez immédiatement les mots de passe de chacun !

BLOCTEL, VOTRE BOUCLIER CONTRE LE DÉMARCHAGE TÉLÉPHONIQUE

PRATIQUE

Ce service gouvernemental vous permet de vous inscrire sur une liste d'opposition au démarchage téléphonique.

INFOS Bloctel
Où le trouver ? [www.bloctel.gouv.fr]
Difficulté :

01› S'INSCRIRE À BLOCTEL

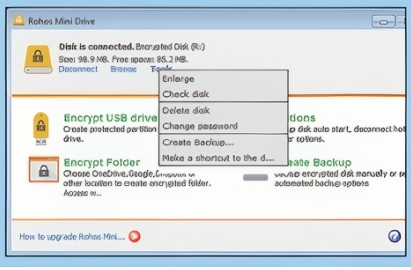
Une fois sur le site, cliquez sur le bouton **Créer son compte**. Remplissez le formulaire avec les informations requises, y compris votre numéro de téléphone (vous pouvez en ajouter plusieurs sur le même compte). Cliquez sur **Validez le formulaire** puis confirmez via le mail reçu.

02› SIGNALER UN ABUS

Si vous recevez malgré tout un appel de démarchage après votre inscription à Bloctel, connectez-vous à votre compte sur le site, choisissez par exemple l'option **Signaler un démarchage abusif**. Remplissez le formulaire et envoyez.

Chiffrer vos clés USB
> avec Rohos Mini Drive

Rohos crée une partition sécurisée protégée par mot de passe sur votre clé. Ainsi, l'autre partie, non chiffrée, peut encore servir à d'autres usages. Le chiffrement est en AES 256 bits. La zone cryptée est paramétrable, mais ne peut pas dépasser 2 Go dans la version d'essai. Rohos est portable, c'est l'une de ses forces.
Lien : rohos.com



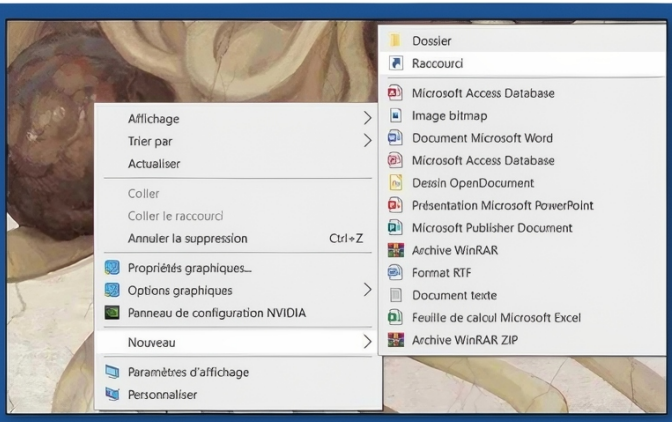
Cryptez vos frappes au clavier
> avec KeyScrambler

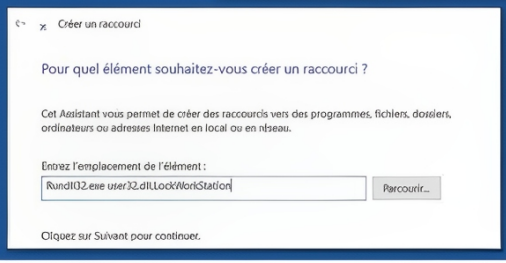
Nous vous avons parlé plusieurs fois des keyloggers, ces logiciels malveillants qui, une fois installés sur vos PC, vont récupérer tout ce que vous saisissez au clavier : mots de passe, informations bancaires, etc. Même si un antivirus est la meilleure arme contre ces malwares, il arrive que certains passent au travers du filet. Pour lutter contre cette menace, nous vous conseillons KeyScrambler un logiciel qui va crypter toutes les frappes directement au niveau du pilote de votre clavier pour ne le décrypter que dans votre navigateur Web (IE, Firefox ou Flock). Si un pirate essaye de lire vos frappes, il se retrouvera avec du texte inexploitable...

Lien : **www.qfxsoftware.com**

Créer un icone de verrouillage
> Avec Windows

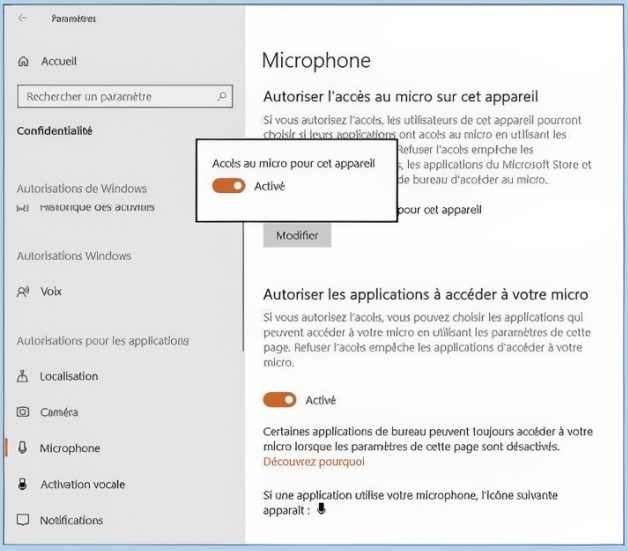
Comment créer un icone sur le bureau qui vous fera gagner du temps à chaque fois que vous quittez l'écran ? Le plus simple est d'utiliser le raccourci clavier **Windows + L**. Mais vous pouvez aussi créer un icone sur votre bureau pour avoir plus de choix. Faites un clic droit sur un espace vide de votre bureau puis choisissez **Nouveau > Raccourci**. Dans le champ qui s'affiche, renseignez **Rundll32.exe user32.dll,LockWorkStation** puis cliquez sur **Suivant**. Donnez un nom à l'icone qui s'affichera sur votre bureau puis sur **Terminer**. Un double clic suffira à verrouiller le PC.





Désactivez l'accès au microphone
> AVEC WINDOWS

Bloquez l'accès au microphone de votre ordi via les **Paramètres** de Windows. Allez dans **Confidentialité > Microphone** et en dessous de **Autoriser l'accès au micro sur cet appareil**, cliquez sur **Modifier**. Passez au mode **Désactivé**. Votre micro sera ainsi désactivé complètement. Si vous passez par **Autoriser les applications à accéder à votre microphone**, attention, vous ne désactivez l'accès que pour les applis sélectionnées et toutes celles du bureau restent autorisées par défaut ! Pour retrouver un microphone opérationnel par défaut et pour tous vos usages, il suffit bien sûr de repasser en mode **Activé** via **Modifier**.



Nettoyer et customiser Facebook
> AVEC FB PURITY

Si vous utilisez Facebook, c'est essentiellement pour suivre les activités de vos amis, voire de certains groupes ou marques. Pas pour voir des publicités, des vidéos commerciales qui démarrent toutes seules, ni même des messages déjà likés qui remontent parce que d'autres personnes les ont commentés. FB Purity veut alléger votre fil d'actualité en vous débarrassant de tout ce qui vous encombre. Il vous aide même à le garder dans son ordre chronologique (ce qui faisait longtemps, avouez-le). Cette extension vous aide globalement à reprendre le contrôle sur ce qui apparaît sur votre écran et à notre époque, c'est déjà beaucoup.

Chiffrer en fichier en ligne
> AVEC FILE LOCK

Besoin de chiffrer un fichier rapidement ? Ne vous embarrassez pas d'un logiciel complexe et passez par le site File Lock. Importez le fichier, entrez un

mot de passe (attention, il n'existe aucun moyen de le récupérer si vous l'oubliez) et validez. Pour déchiffrer ensuite le fichier, même technique : il faut l'envoyer sur le site et donner le code.

Lien : **www.filelock.org**

Oui,
recycler mes papiers, c'est utile.

Pour l'environnement

Le recyclage des papiers permet **d'économiser les matières premières et l'énergie.**

Le recyclage de papier, c'est :

3 fois moins d'eau*

3 fois moins d'énergie*

* comparé à la fabrication de papier non recyclé

Pour l'emploi

La filière du recyclage des papiers **en France, c'est 90 000 emplois non délocalisables.**

Collecte

Papeterie

Centre de tri

Découvrez le recyclage du papier sur www.consignesdetri.fr

CITEO

Le nouveau nom d'Eco-Emballages et Ecofolio

DÉCRYPTAGE

TOUT SAVOIR SUR LES FORMATS VIDÉO : LESQUELS CHOISIR ?

Le choix du format vidéo dépend de plusieurs critères tels que la qualité souhaitée, la compatibilité avec les appareils de lecture, la taille du fichier, et l'usage prévu (montage, diffusion en ligne, archivage, etc.). Voici un aperçu des formats vidéo les plus courants pour vous aider à choisir.

Un fichier vidéo se compose de deux parties : l'une codant l'audio et la vidéo, et l'autre assurant la lecture fluide de la vidéo sans interruption. Ainsi, plutôt que parler de format, certains préfèrent parler de conteneur pour ceux que nous vous présentons ci-après. Un conteneur de fichier vidéo définit la manière dont les données audio, vidéo, et autres sont stockées ensemble. Sélectionner le format (conteneur !) adapté est donc essentiel pour une diffusion efficace. Un format vidéo judicieux assure un chargement rapide et une qualité d'image impeccable. Parmi les formats les plus courants figurent : MOV, AVI, MP4, FLV, WMV, WebM, MKV ou SVF, identifiables par l'extension du fichier. Chacun a ses spécificités.

MOV

- Développé par :

Apple.

- Compatibilité :

Très bien supporté sur les appareils Apple, mais peut nécessiter des logiciels supplémentaires sur Windows.

- Utilisation :

Montage vidéo de haute qualité, diffusion sur des appareils Apple.

- Avantages :

Supporte une haute qualité d'image et plusieurs codecs ; idéal pour l'édition grâce à sa capacité à contenir plusieurs pistes de données.

- Inconvénients :

Les fichiers peuvent être volumineux ; moins universel hors de l'écosystème Apple.

AVI

- Développé par :

Microsoft.

- Compatibilité :

Bonne sur les appareils Windows, peut être moins supporté sur les appareils non-Windows sans logiciels tiers.

- Utilisation :

Stockage de vidéos de courte durée en qualité standard.

- Avantages :

Compatible avec de nombreux appareils et lecteurs; supporte une qualité vidéo relativement élevée.

- Inconvénients :

Les fichiers peuvent être très volumineux, et il ne supporte pas certains codecs plus modernes aussi efficacement que d'autres formats.

MP4

- Développé par :

Moving Picture Experts Group (MPEG).

- Compatibilité :

Extrêmement élevée sur pratiquement tous les appareils et plateformes.

- Utilisation :

Diffusion en ligne, partage sur les réseaux sociaux, lecture sur une grande variété d'appareils.

- Avantages :

Équilibre entre qualité et taille de fichier; supporte à la fois la vidéo et l'audio; très universel et adapté pour le web. MP4 utilise une compression qui peut réduire la taille du fichier avec une perte de qualité minimale, ce qui est idéal pour le streaming et le téléchargement.

- Inconvénients :

La qualité peut être inférieure à celle des formats spécialisés comme MOV pour l'édition vidéo.

LEXIQUE

Ratio (Aspect Ratio)
Le ratio, ou rapport d'aspect, désigne les proportions entre la largeur et la hauteur d'une image vidéo. Il définit l'orientation et la forme de la vidéo affichée. Les ratios communs incluent 16:9 (standard pour la HD et la plupart des contenus modernes), 4:3 (ancien standard pour la télévision analogique), et 21:9 (ultra large, souvent utilisé pour les films).

Bitrate
Le bitrate (ou débit binaire) mesure la quantité de données vidéo transmises ou stockées par seconde. Il est généralement exprimé en mégabits par seconde (Mbps). Un bitrate plus élevé signifie généralement une meilleure qualité d'image, car plus d'informations sont disponibles pour représenter la vidéo, mais cela augmente aussi la taille du fichier.

Échantillonnage (Sampling)
Dans le contexte de l'audio et de la vidéo, l'échantillonnage fait référence à la fréquence à laquelle les données sont capturées ou échantillonnées. Pour la vidéo, cela peut concerner l'échantillonnage de couleur, qui décrit comment les différentes composantes de couleur (rouge, vert, bleu) sont enregistrées et combien d'informations de couleur sont incluses. Par exemple, un espace de couleur 4:2:2 signifie que la luminance est échantillonnée à chaque pixel, mais que la chrominance est échantillonnée à la moitié de la résolution de la luminance.

Codec
Un codec est un dispositif ou un logiciel capable de coder ou de décoder un flux de données ou un signal. Dans la vidéo, les codecs compressent ou décompressent les fichiers multimédias pour réduire leur taille tout en essayant de préserver la qualité originale. Les codecs peuvent être soit des codecs de compression (comme H.264, H.265) qui réduisent la taille du fichier, soit des codecs sans perte qui préservent la qualité au prix d'une plus grande taille de fichier.

Résolution

La résolution indique le nombre total de pixels dans une image, habituellement exprimé en termes de largeur x hauteur. Par exemple, une résolution de 1920x1080 signifie que l'image contient 1920 pixels horizontalement et 1080 pixels verticalement. La résolution est un facteur clé de la qualité d'image, avec des résolutions plus élevées fournissant une image plus détaillée.

Les résolutions usuelles que vous retrouverez actuellement sont les suivantes :

- SD (Standard Definition) : 480p (640x480 pixels).
- HD (High Definition) : 720p (1280x720 pixels).
- Full HD (FHD) : 1080p (1920x1080 pixels).
- QHD (Quad High Definition) : 1440p (2560x1440 pixels). Aussi appelée Quad HD, elle offre quatre fois la résolution de 720p.
- UHD (Ultra High Definition) : > 4K (3840x2160 pixels). Officiellement appelée UHD-1 ou Ultra HD, elle est communément appelée 4K car elle offre quatre fois la résolution de 1080p. > 8K (7680x4320 pixels). Officiellement appelée UHD-2, elle offre quatre fois la résolution de 4K et seize fois celle de 1080p.

Framerate (Taux de trame)

Le framerate, ou taux de trame, est le nombre d'images par seconde (fps) à laquelle une vidéo est affichée. Des framerates communs incluent 24 fps pour les films, 30 fps pour la télévision standard, et 60 fps pour les vidéos à haute fluidité, comme les jeux vidéo ou les retransmissions sportives.

Profondeur de couleur

La profondeur de couleur décrit le nombre de bits utilisés pour représenter la couleur d'un seul pixel. Plus la profondeur de couleur est élevée, plus la gamme de couleurs et de nuances que l'image peut afficher est large. Par exemple, une profondeur de couleur de 8 bits par canal peut afficher 256 nuances de rouge, vert et bleu, tandis qu'une profondeur de 10 bits peut en afficher 1024.

FLV (Flash Video Format)

- Développé par :

Adobe Systems.

- Compatibilité :

Était très répandu pour le streaming sur Internet grâce à l'intégration avec Adobe Flash Player, mais sa popularité a décliné avec la fin du support de Flash.

- Utilisation :

Principalement pour le streaming vidéo en ligne avant l'avènement de technologies plus récentes.

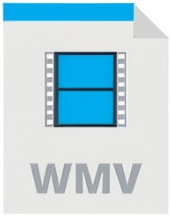
- Avantages :

Bonne compatibilité avec les navigateurs web de l'époque de Flash; conçu pour le streaming efficace sur Internet.

- Inconvénients :

Obsolète, avec une compatibilité et un support en déclin à cause de la disparition d'Adobe Flash.

WMV (Windows Media Video)



- Développé par :

Microsoft.

- Compatibilité :

Bonne sur les systèmes Windows, moins universelle sur les autres plateformes sans logiciels supplémentaires.

- Utilisation :

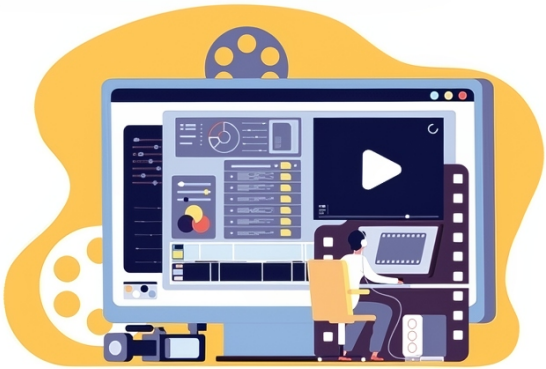
Vidéo en streaming, contenu téléchargeable, et lecture sur les appareils Windows.

- Avantages :

Intégration avec les systèmes Windows et les logiciels Microsoft; supporte la protection des droits numériques (DRM).

- Inconvénients :

Moins compatible avec les appareils non-Windows; qualité parfois inférieure à celle d'autres formats de fichier pour une taille donnée.



WebM

- Développé par :

Projet soutenu par Google.

- Compatibilité :

Très bonne sur les navigateurs web modernes et les plateformes supportant le HTML5.

- Utilisation :

Vidéo en ligne, notamment pour les contenus HTML5 et les sites de streaming comme YouTube.

- Avantages :

Format libre et ouvert; optimisé pour le web avec une bonne qualité et une taille de fichier réduite; supporte la vidéo 4K et la haute dynamique (HDR).

- Inconvénients :

Peut ne pas être le meilleur choix pour tous les scénarios d'édition ou d'archivage vidéo en raison de sa focalisation sur le web.

MKV (Matroska Video)

- Développé par :

La fondation Matroska.

- Compatibilité :

Bonne avec de nombreux lecteurs multimédia, mais peut nécessiter des codecs supplémentaires ou des logiciels spécifiques.

- Utilisation :

Stockage de films ou de séries télé, avec la capacité de contenir plusieurs pistes audio et sous-titres dans un seul fichier.

- Avantages :

Format conteneur flexible pouvant inclure une haute qualité vidéo, plusieurs pistes audio, sous-titres, et métadonnées; supporte presque tous les codecs vidéo et audio.

- Inconvénients :

Sa grande flexibilité peut entraîner des problèmes de compatibilité avec certains appareils moins avancés.

Espace colorimétrique (Color Space)

Un espace colorimétrique est un modèle mathématique spécifique décrivant la manière de représenter les couleurs. Les exemples incluent sRGB pour l'Internet, Rec. 709 pour la HD vidéo, et Rec. 2020 pour l'UHD et le HDR. Choisir le bon espace colorimétrique est crucial pour assurer que les couleurs sont affichées correctement sur différents appareils.

HDR (High Dynamic Range)

Le HDR améliore le contraste et augmente la gamme de couleurs d'une vidéo par rapport au standard dynamic range (SDR), offrant des blancs plus brillants, des noirs plus profonds, et une gamme de couleurs plus large. Cela permet d'obtenir une image plus réaliste et plus détaillée.

Compression

La compression réduit la taille du fichier vidéo en éliminant les informations redondantes ou moins importantes. C'est là que les codecs (lire ci-contre) prennent toute leur importance ! Il existe deux types principaux de compression : la compression avec perte (lossy), qui réduit la taille du fichier en supprimant définitivement certaines données; et la compression sans perte (lossless), qui réduit la taille du fichier sans supprimer d'informations, permettant la restauration exacte de l'original.

ALORS, LEQUEL CHOISIR ?

En résumé, si vous cherchez une compatibilité universelle et une bonne balance entre qualité et taille de fichier, MP4 est souvent le meilleur choix. Pour des projets d'édition vidéo plus professionnels ou si vous utilisez principalement des appareils Apple, MOV peut être préférable. AVI est moins utilisé de nos jours, mais peut toujours être utile pour des applications spécifiques nécessitant sa compatibilité avec des systèmes plus anciens. Pour le stockage sur PC, les formats MP4, AVI, ou WMV sont recommandés pour Windows, tandis que MOV ou MP4 sont préférables pour Mac. Le MKV est un excellent conteneur souvent utilisé pour des architectures complexes avec menus, plusieurs sous-titres ou canaux audio (par exemple pour reproduire une structure DVD ou Blu-ray). Pour la visualisation sur appareils mobiles ou la diffusion sur votre site web, le MP4 est encore le meilleur choix.

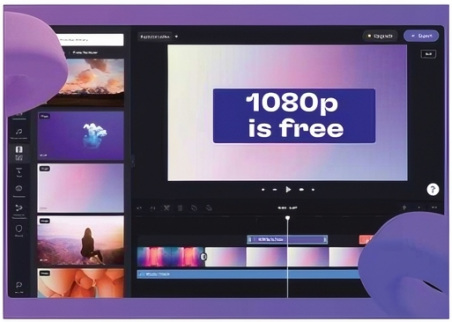
6 OUTILS GRATUITS POUR CONVERTIR ET COMPRESSER VOS VIDÉOS

Il n'y a pas que le montage et l'édition vidéo qui compte, vous l'aurez compris. Nous vous présentons ici six logiciels et services dont la mission principale sera de triturer les formats et codecs de vos vidéos pour une diffusion optimale et sans compromis !

CLIPCHAMP :

Pour débutants connectés

Acquis par Microsoft, ce site propose une interface conviviale, oriente ses utilisateurs en fonction de leurs besoins (web, mobiles, réseaux sociaux). La version gratuite permet la compression en qualité HD (1080p) sans filigrane et offre des éléments de personnalisation gratuits. Vous pouvez lancer la compression de plusieurs vidéos en même temps, un plus indéniable. Vous pourrez enfin publier directement vos fichiers compressés sur



YouTube, Vimeo ou Facebook, là encore c'est bien pensé. Le système de compression est efficace. Tous les formats sont pris en charge et la perte de qualité est quasi imperceptible. Clipchamp offre enfin de nombreux outils de personnalisation pour que vous puissiez tout faire sans quitter le site (ajouts de musiques, images ou vidéos libres de droits par exemple).

Lien : clipchamp.com

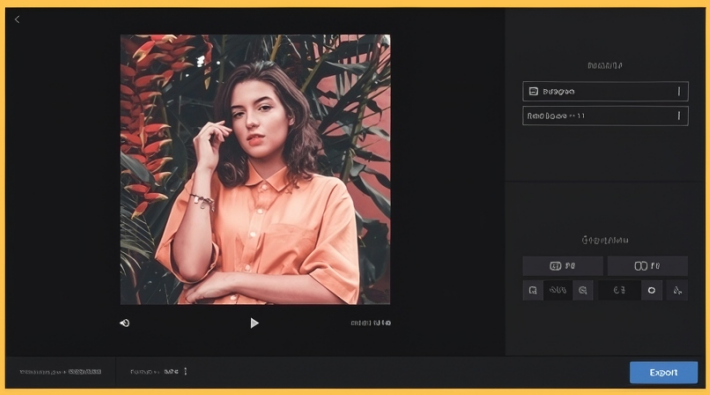
YOUCOMPRESS :

La simplicité sans limite

Cet outil se concentre exclusivement sur la compression de vidéos, images et fichiers audio, sans permettre de réglage manuel du niveau de compression ou du format de sortie. Il est simple d'utilisation : vous sélectionnez le fichier à compresser (ou vous réalisez un glisser-déposer), vous cliquez sur le bouton "Envoyer fichier et compresser" et c'est parti. C'est donc simplissime... mais il le fait bien. Sans filigrane apposé sur votre vidéo et sans limite en termes de nombre de vidéos ou de documents !

Lien : www.youcompress.com

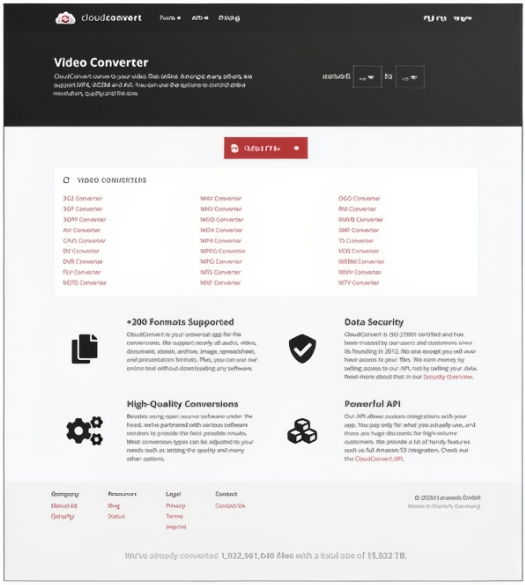
CLIDEO : Trousse à outils en ligne



Disponible en français, Clideo est une suite d'outils en ligne et offre un site esthétiquement plaisant malgré quelques traductions maladroites. Il propose neuf fonctions de base dans sa version gratuite, limitée par l'espace de stockage et l'apposition de filigranes. Vous pouvez donc fusionner, compresser, découper, incruster des sous-titres... Il est capable de compresser MP4, WMV, MOV, VOB, AVI, mais aussi des formats plus rares de fichiers vidéo. Vous pourrez même prévisualiser le résultat avant de le charger, ce qui peut s'avérer assez pratique (notamment si la qualité n'est pas à la hauteur de vos espérances). La version payante, sans engagement, se décline en deux formules à 9 euros par mois ou 72 euros à l'année, offrant un service de compression sans limitation.

Lien : clideo.com

CLOUDCONVERT : En ligne avec limite de 1 Go

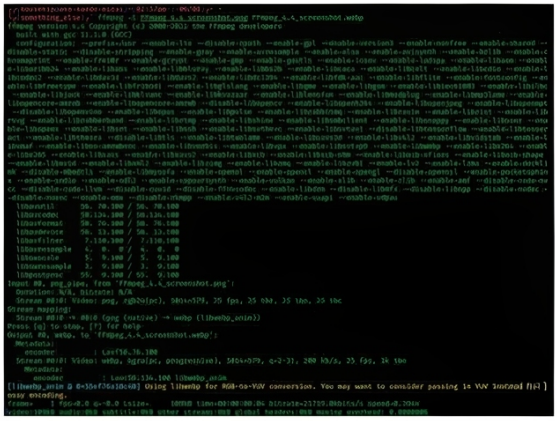


Fondé il ya plus de dix ans, ce service reste plébiscité avec ces quelques 200 formats de fichiers différents, couvrant non seulement la vidéo, mais aussi l'audio, les images, les documents, et même les eBooks. Les utilisateurs peuvent ajuster de nombreux paramètres de conversion pour répondre à leurs besoins spécifiques, y compris la résolution, le débit binaire, et d'autres options avancées. CloudConvert assure la sécurité et la confidentialité des fichiers téléchargés, en les supprimant de ses serveurs après la conversion. Il offre la possibilité d'importer et d'exporter des fichiers directement depuis et vers vos comptes Dropbox et Google Drive, facilitant ainsi la gestion des fichiers dans le cloud.

CloudConvert propose également une API robuste, permettant aux développeurs d'intégrer ses fonctionnalités de conversion dans leurs propres applications. Dans sa version gratuite, il autorise 25 conversions par mois, avec des fichiers d'origine limités à 1 Go.

Lien : cloudconvert.com

FFMPEG : Pour les pros



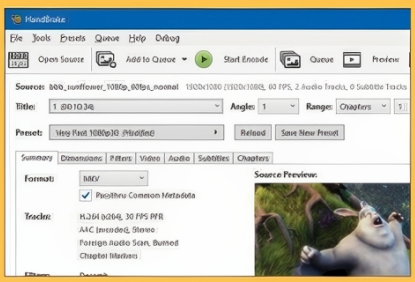
FFmpeg est un outil extrêmement puissant et polyvalent pour l'enregistrement, la conversion et le streaming de vidéo et d'audio, disponible sous licence libre. Il fournit une suite logicielle complète comprenant des bibliothèques et des programmes pour gérer les données multimédias les plus diverses. Au-delà de la conversion et de la compression, il offre des fonctionnalités avancées telles que le découpage, le jointage, le filtre, la rotation, et l'ajustement des taux de bits, permettant une personnalisation profonde des fichiers de sortie. FFmpeg facilite aussi le streaming en direct, capable de diffuser des flux vidéo en temps réel sur le web. Il peut aussi être utilisé pour capturer des sessions vidéo en direct de l'écran d'un ordinateur, idéal pour les tutoriels ou les présentations.

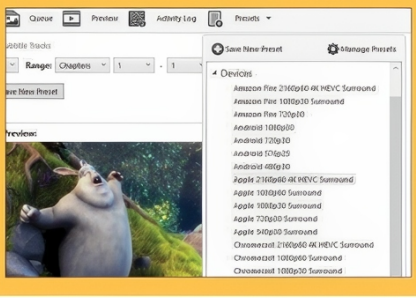
Grâce à sa ligne de commande, FFmpeg offre un contrôle presque illimité sur les options de traitement des médias, rendant possible presque toute opération de traitement vidéo ou audio imaginée. Les nouveaux utilisateurs peuvent justement trouver cette ligne de commande intimidante, et maîtriser FFmpeg peut nécessiter un certain temps d'apprentissage.

Lien : ffmpeg.org

HANDBRAKE : Le meilleur accessible à tous

HandBrake est un logiciel open-source réputé pour sa flexibilité et sa puissance. Disponible pour Windows, macOS et Linux, il peut traiter la plupart des formats vidéo courants et offre un large éventail de codecs vidéo et audio pour la compression, y compris H.264 (x264), H.265 (x265) pour la vidéo, et AAC, MP3, Flac, AC3, ou Vorbis pour l'audio. Il propose des réglages prédéfinis pour optimiser vos vidéos pour différents dispositifs et plateformes, comme les iPhones, iPads, Android, Roku, etc., facilitant la sélection des paramètres de sortie sans nécessiter une expertise technique approfondie. Le logiciel permet également de modifier les vidéos de plusieurs manières, comme



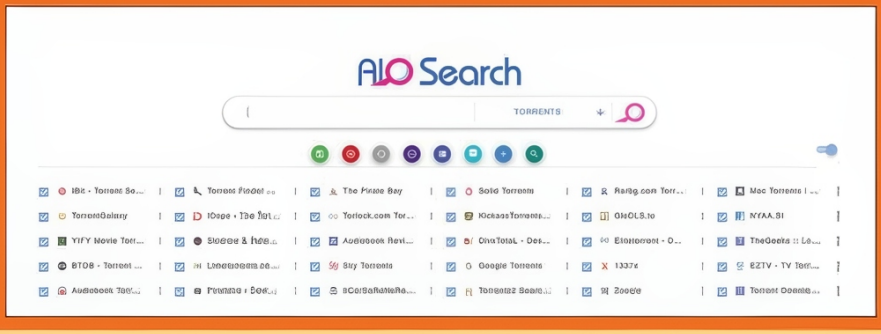


l'ajustement de la résolution, le recadrage, le filtrage (désentrelacement, débruitage, etc.), l'ajout de sous-titres. Étant open-source, HandBrake est entièrement gratuit. Sa communauté active contribue à des mises à jour régulières, améliorant constamment le logiciel. Pour les utilisateurs expérimentés, HandBrake offre des options de personnalisation avancée pour contrôler précisément la qualité et la taille des fichiers de sortie. Bien que les réglages prédéfinis facilitent son utilisation par les novices, la pléthore d'options et de paramètres peut être intimidante pour les utilisateurs moins expérimentés.

Lien : handbrake.fr

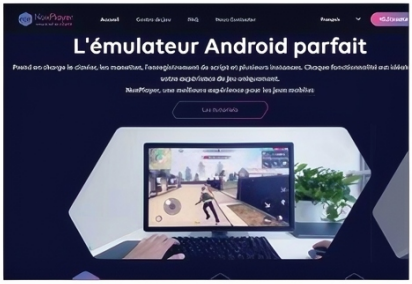
Trouver des torrents > Avec AIO Search

Ce métamoteur (moteur de recherche qui collecte les résultats de plusieurs autres moteurs de recherche) propose d'effectuer des requêtes pour dénicher des fichiers partout sur le Web auprès des plateformes de streaming et de partage de fichiers. Néanmoins, sa grande spécialité repose sur les fichiers Torrents. Il combine ainsi les résultats provenant de pas moins de 30 moteurs de recherche de liens torrents. Si avec ça vous ne trouvez pas ce que vous cherchez, c'est que ça n'existe pas. Son interface se montre plutôt sobre et agréable. On peut éliminer certaines plateformes des résultats et même ajouter d'autres moteurs de recherche. Il permet de trouver à peu près tout y compris les fichiers de sous-titres et même de simples images.



Retrouver vos jeux Android sur PC
> Avec Noxplayer

Retrouvez votre environnement Android sur votre PC. Un accès direct au Playstore vous permet de télécharger et d'ouvrir directement vos jeux. Pour une expérience optimale, configurez manettes, claviers,

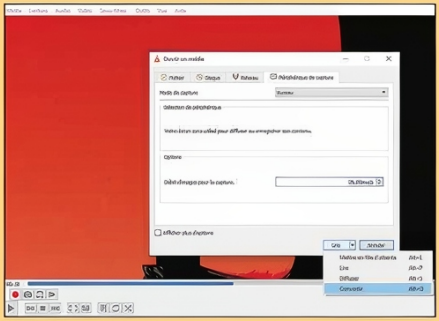


souris, raccourcis, etc. Vous pouvez enfin opter pour un affichage horizontal ou vertical selon le jeu lancé. Un must qui concurrence déjà BlueStacks et qui le devance sur de nombreux points !

Lien : www.bignox.com

Enregistrer votre écran d'ordinateur > Avec VLC

Pour offrir une formation en ligne (ou pour montrer à une autre personne quels gestes accomplir sur un ordinateur), le plus simple est encore d'enregistrer directement votre écran. Et : oui, VLC vous permet cela aussi. Assez dans le menu **Média**, puis sur **Ouvrir un périphérique de capture**. Dans Mode de capture, sélectionner **Bureau.** Soyez attentif aux options : un débit d'image de **25 ima/s** sera privilégié pour obtenir un résultat suffisamment fluide. Cliquez ensuite sur la flèche à droite du bouton Lire pour choisir **Convertir** dans le menu déroulant. Sélectionnez ensuite votre profil d'enregistrement (avec ou sans le son), et cliquez sur **Démarrer** pour lancer l'enregistrement.



BACKBONE : NOUVELLES MANETTES DE JEU MOBILE

Backbone vient de commercialiser sa deuxième génération de manettes de jeu mobile, compatibles iPhone et Android. N'importe quel smartphone peut ainsi se transformer en console portative tout en bénéficiant d'un gameplay traditionnel et d'une très faible latence.
La version blanche de la Backbone One (2e gen) est, elle, dédiée à l'univers Playstation tandis que la noire dispose de boutons classiques. Les versions blanches et noires possèdent au choix une prise Lightning (iPhone 14 et inférieurs) ou USB-C (Android et iPhone 15). Une prise casque 3,5 mm est également située au niveau de la poignée gauche de la manette. Pas de batterie intégrée : les besoins en énergie des Backbones sont directement fournis par le smartphones connecté.

Prix : 119,99 €
Backbone One Standard (2e génération)
Backbone One – PlayStation (2e génération)
Où les trouver ? playbackbone.com

> Des manettes futées et polyvalentes mais à un prix dissuasif (119,99 €) pour beaucoup.

QUOI DE NEUF ?

Pas de grands changements évidents au premier coup d'œil pour les deux nouvelles manettes en comparaison des anciennes, mais des améliorations à souligner cependant : de nouveaux adaptateurs magnétiques interchangeables permettent de s'adapter à la plupart des coques de smartphones tout en conservant une bonne stabilité de l'ensemble. Grâce aux dernières mises à jour du matériel et des performances, les joueurs Backbone peuvent désormais s'adonner à des licences exigeantes comme Call of Duty: Warzone Mobile. Les manettes et le compte Backbone associé sont compatibles avec Apple Arcade, Xbox Game Pass Ultimate, Steam Link pour PC. L'application Backbone organise quant à elle votre bibliothèque de contenus et vos services de streaming.

RADXA ROCK 5C ET ROCK 5C LITE : ALTERNATIVES CRÉDIBLES AU RASPBERRY PI 5 ?

LES RADXA ROCK 5C ET ROCK 5C LITE OFFRENT UN LARGE ÉVENTAIL DE FONCTIONNALITÉS ET DES CONFIGURATIONS DE MÉMOIRE FLEXIBLES À DES PRIX COMPÉTITIFS PAR RAPPORT AU RASPBERRY.

Le paysage des ordinateurs monocartes (SBC) s'enrichit avec l'arrivée de deux nouvelles cartes du fabricant Radxa : la Rock 5C et la Rock 5C Lite. Ces deux modèles sont lancés pour concurrencer directement le Raspberry Pi 5, avec des offres tarifaires attractives démarrant à moins de 30 euros pour la Rock 5C Lite et moins de 50 euros pour la Rock 5C. La première peut proposer jusqu'à 16 Go de RAM LPDDR4x et jusqu'à 32 Go pour la Rock 5C.

ROCK 5C EN DÉTAILS

La Rock 5C, qui ressemble beaucoup visuellement au Pi 5, se distingue par son SoC Rockchip RK3588S2, une puissante configuration octa-core composée de quatre cœurs ARM Cortex-A76 et quatre Cortex-A55, appuyée par un GPU Mali-G610 MP4. Ce dernier offre la capacité d'encoder et de décoder des vidéos jusqu'à 8K, avec une limite à 60 FPS pour le décodage et 30 FPS pour l'encodage à cette résolution. Le chipset intègre également un NPU (unité de traitement neuronal) promettant jusqu'à 6 TOPS de performances théoriques pour des applications d'intelligence artificielle. Outre ses capacités de traitement, la Rock 5C brille par sa connectivité étendue, incluant un port Ethernet Gigabit avec PoE, une sortie HDMI 2.1, des ports USB diversifiés (2x USB 2.0 et 1x USB C), un jack audio combo 3.5 mm ainsi qu'un support pour le Wi-Fi 6 et Bluetooth 5.4.

ROCK 5C LITE : LA PETITE SŒUR

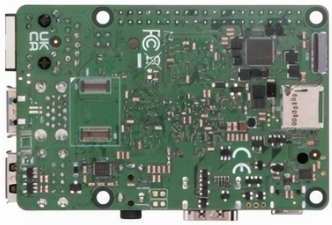
D'autre part, la Rock 5C Lite opte pour un chipset moins puissant, le Rockchip RK3582, réduisant son nombre de cœurs CPU à deux Cortex-A76 et quatre Cortex-A55, sans circuit graphique intégré, et limite son NPU à 5 TOPS. Cette variante peut accueillir de 1 à 16 Go de mémoire vive LPDDR4x et ne supporte pas Android, contrairement à la Rock 5C. Les deux cartes sont, par contre, compatibles avec Radxa OS et Ubuntu.

Prix :

- ROCK 5C Lite	- ROCK 5C
1 GO – 28,95 €	2 GO – 47,95 €
2 GO – 32,95 €	4 GO – 56,95 €
4 GO – 42,95 €	8 GO – 75,95 €
8 GO – 61,95 €	16 GB – 112,95 €
16 GB – 98,95 €	32 GB – 188,95 €

Où le trouver ? **arace.tech**

LA ROCK 5C A DE NOMBREUX POINTS COMMUNS AVEC LE RASPBERRY PI 5, SA CONFIGURATION MATÉRIELLE CONFIRME CETTE PREMIÈRE IMPRESSION.



Les deux modèles proposent diverses options de stockage, incluant un lecteur de cartes, un connecteur eMMC, et un port PCIe 2.1 permettant l'ajout d'extensions NVMe ou SATA. Avec des dimensions compactes proches de celles d'une carte de crédit (85 x 56 mm pour la Rock 5C et légèrement moins pour la Rock 5C Lite), ces cartes sont conçues pour une variété d'applications, allant du développement à l'intelligence artificielle, en passant par des usages multimédias avancés.

SÉLECTION

TOP 15 Logiciels & services GRATUITS

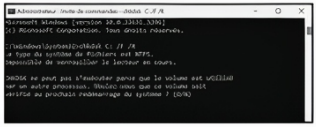
TOP5 PRENDRE SOIN DE VOS DISQUES DURS

CRYSTALDISKINFO : Disque dur et SSD en temps réel

Il surveille et rapporte l'état de santé et les performances de vos disques en temps réel. Utilisant les données SMART (Self-Monitoring, Analysis, and Reporting Technology), il alerte l'utilisateur des potentiels dysfonctionnements avant qu'ils ne deviennent critiques. Facile d'usage et léger, ce logiciel est un must-have.

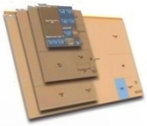
Lien : crystalmark.info

CHKDSK : Intégré à Windows



Chkdsk est un outil Windows dédié à l'inspection et à la réparation des disques. Il s'attaque aux erreurs de système de fichiers, aux secteurs défectueux, et aux problèmes qui peuvent entraîner des pertes de données. Son intégration permet de lancer des vérifications et des réparations directement depuis le menu contextuel, via l'invite de commande.

SPACESNIFFER : Nettoyage



Son interface graphique sous forme de treemap détaille comment l'espace est réparti entre fichiers et dossiers. Outre son approche visuelle unique, SpaceSniffer filtre les résultats par taille, nom ou date, facilitant la chasse aux fichiers inutiles ou oubliés. Un allié précieux pour optimiser l'espace disque et maintenir l'ordre sur son PC.

Lien : www.uderzo.it

CRYSTALDISKMARK : Tester son disque dur

Ce logiciel gratuit réalise des tests de lecture et d'écriture séquentiels et aléatoires pour mesurer la vitesse de votre disque. Simple d'utilisation, il présente les résultats dans une interface claire, permettant aux utilisateurs de comparer les performances avant et après des modifications ou des mises à jour matérielles.

Lien : crystalmark.info

S.M.A.R.T. MONITORING TOOLS : Trousse à outils

Il s'agit d'un ensemble de logiciels conçus pour analyser, surveiller et rapporter l'état de santé des disques durs et des SSD, utilisant lui aussi la technologie d'autosurveillance, d'analyse et de rapport S.M.A.R.T. Ces outils permettent de prévenir les défaillances en alertant sur les anomalies détectées et sont accessibles à tous.

Lien : sourceforge.net/projects/smartmontools/

TOP5 POUR VOS SOUS-TITRES !

OPEN SUBTITLES : La star

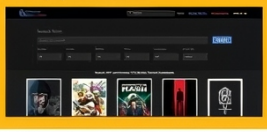
Il s'agit du plus grand site de téléchargement de sous-titres, offrant une vaste collection dans plusieurs langues pour films et séries télévisées XviD. L'interface est conviviale, rendant la recherche et le téléchargement des sous-titres assez aisés.

Lien : www.opensubtitles.org/fr

YIFY SUBTITLES : Premier sur les nouveautés

Connue pour son vaste catalogue de sous-titres de films récents, YIFY Subtitles est une destination privilégiée pour ceux qui cherchent les derniers sous-titres. Le site est bien entretenu avec des mises à jour fréquentes, et les sous-titres sont disponibles en diverses langues.

Lien : yifysubtitles.live



SUBTITLE EDIT : Pro et gratuit

Ce logiciel open source permet de créer, éditer et ajuster des sous-titres avec une précision chirurgicale. Synchronisation, OCR pour convertir les sous-titres incrustés, reconnaissance vocale, etc. : les nombreuses fonctions le destinent aux créateurs ayant déjà une bonne maîtrise de l'édition vidéo.

Lien : www.nikse.dk/subtitleedit

TOP5 PRISE DE CONTRÔLE À DISTANCE

CHROME REMOTE DESKTOP

> Google force

Chrome Remote est l'idéal pour les utilisateurs débutants, ou pour ceux qui recherchent avant tout la simplicité. L'extension se télécharge dans Chrome, et il suffit d'entrer le code généré sur l'ordinateur distant pour que les deux machines soient connectées. Petit bonus : Chrome Remote est également disponible sur les appareils Android ou iOS, ce qui permet de dépanner quelqu'un ou d'accéder à votre PC du bureau même en déplacement !

Lien : **https://remotedesktop.google.com/**

NO MACHINE

> Multi-plateforme

Pas vraiment connu, NoMachine est pourtant une excellente solution de contrôle à distance. Gratuit et multi-plateforme, il permet de se connecter grâce à un identifiant, et de gérer plusieurs ordinateurs. Le top ? La fluidité garantie par le protocole NX, et la sécurité assurée grâce au SSH. L'utilisateur est guidé étape par étape, et peut configurer NoMachine en finesse. Un logiciel à découvrir !

Lien : **http://kelt.co/p/recall**

TEAMVIEWER

> L'incontournable

Logiciel le plus connu en ce qui concerne le partage d'écran ou la prise de contrôle à distance, TeamViewer n'a plus besoin de faire ses preuves. À l'inverse d'Ammyy Admin, l'installation de TeamViewer est nécessaire sur tous les appareils que vous souhaitez utiliser. Vous pouvez également profiter des applis mobiles (sur Android et iOS) pour contrôler votre ordinateur à partir de votre smartphone.

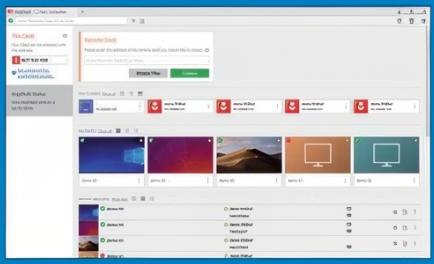
Lien : **https://www.teamviewer.com/fr/**

ANYDESK

> Portable et réactif

C'est grâce à un identifiant que vous pourrez lier les deux ordinateurs. La prise en main est simple et rapide, et AnyDesk présente l'avantage d'être un outil portable : vous pouvez l'utiliser à partir d'une clé USB, et ainsi l'avoir toujours avec vous prêt à fonctionner. Il propose également des fonctionnalités intéressantes, comme l'ajustement automatique de la résolution d'écran.

Lien : **https://anydesk.com/fr r**



ULTRAVNC

> Le petit frenchie

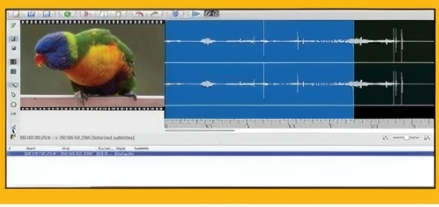
UltraVNC propose un module particulièrement intéressant si vous cherchez une solution ponctuelle : le Simple Clic. Il suffit de télécharger UltraVNC SC, et d'autoriser le contrôle à distance. Dès que la connexion est rompue, UltraVNC SC se désinstalle lui-même. Pas de traces, pas de risques d'une prise de contrôle non souhaitée : c'est une utilisation simple et propre d'un logiciel qui mériterait d'être plus connu.

Lien : **http://www.ultravnc.fr**

JUBLER : Il va à l'essentiel

Plus léger et accessible, il permet de créer et de synchroniser des sous-titres à partir de zéro, en s'appuyant sur MPlayer pour la prévisualisation. Les fonctions clés comprennent la correction de texte, le contrôle de la durée d'affichage, et une intégration facile avec des outils de traduction automatique.

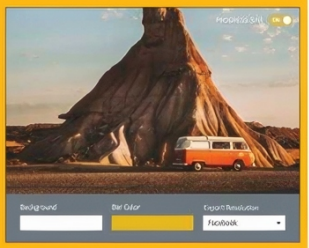
Lien : **www.jubler.org**



SUBTITLEBEE : Transcription audio

Cet outil est conçu spécialement pour les vidéos destinées aux réseaux sociaux et peut transcrire directement l'audio en sous-titres grâce à son IA. La version d'essai est performante, mais se limite à des vidéos de 10 min et 1 Go maximum.

Lien : subtitlebee.com



Casser les codes et décrypter l'info

JE M'ABONNE à PIRATE INFORMATIQUE

LIVRAISON SOUS PLI DISCRET

OFFRE ABONNEMENT

1 AN POUR 17 € (au lieu de ~~19,60 €~~)

2 ANS POUR 29,40 € (au lieu de ~~39,20 €~~)

- LIVRÉ CHEZ VOUS !
- PRATIQUE & ÉCONOMIQUE !

LES GUIDES du HACKER et du PIRATE

> Logiciels et applications exclusifs
> Tutoriels et astuces clairs
> Dossiers pratiques complets pour débutants et experts
> Sélection et test de matériels
> L'actu et les nouveautés !

À DÉCOUPER (OU À PHOTOCOPIER), À COMPLÉTER ET À RENVOYER SOUS ENVELOPPE AFFRANCHIE À :
BII - SERVICE ABONNEMENT - 15, RUE DE MERY - 60420 MÉNÉVILLERS

☐ **Abonnement à Pirate Informatique pour 4 numéros, je joins mon règlement de 17,00 €**
☐ **Abonnement à Pirate Informatique pour 8 numéros, je joins mon règlement de 29,40 €**

☐ OUI, JE M'ABONNE :

Nom _____
Prénom _____
Adresse _____
_____
Code Postal _____
Ville _____
E-Mail _____

☐ Je joins mon règlement par chèque à l'ordre de ID PRESSE (France uniquement)

Offre valable en France métropolitaine uniquement.

POUR NOUS CONTACTER :
abonnement@idpresse.com

Signature obligatoire :

Offre valable jusqu'au 31 décembre 2024. Les délais d'acheminement de La Poste varient selon les régions et pays. Conformément à la loi Informatique et Libertés du 6/1/1978, vous disposez d'un droit d'accès et de rectification quant aux informations vous concernant, que vous pouvez exercer librement auprès de ID PRESSE - IMPASSE DE L'ESPÉRON - VILLA MIRAMAR - 13740 SAUSSET LES PINS

RÉDUCTION DE -25%

LES AVANTAGES :

> **Jusqu'à -25 % sur le prix en kiosques**
> **Ne manquez aucun numéro**
> **Ne soyez plus une victime**
> **Vos magazines livrés chez vous gratuitement**

LES DOSSIERS DU

Pirate

DES DOSSIERS THÉMATIQUES COMPLETS

À DÉCOUVRIR EN KIOSQUES

- PETIT FORMAT
- MINI PRIX
- CONCENTRÉ D'ASTUCES

100% Windows

Actuellement #Guide pratique

LA BIBLE DU HACKER

VIDÉOS

ANONYMAT

CONTRÔLE À DISTANCE

VPN

CONFIDENTIELS

PROTECTION

SURVEILLANCE

MOTS DE PASSE

SPOOFING

PIRATE

INFORMATIQUE

IDPRESSE

L 12730 - 60 - F: 4,90 € - RD

BEL/LUX : 6 € - DOM : 6,10 € - CH : 8,50 CHF - PORT.CONT. : 6 € - CAN : 7,99 $ cad – POL/S : 750 CFP – NCAL/S : 950 CFP - MAR : 50 mad - TUN : 9,8 tnd