

N°61

Casser les codes et décrypter l'info



Août / Octobre 2024

PIRATE

INFORMATIQUE

L'ART DE LA
TROMPERIE

Les **SECRETS**
et **MÉTHODES**
des escrocs

HACKING

PEUT-ON
PIRATER

UN SATELLITE ?

HACKING

LES **VRAIES**
SOLUTIONS

ANONYMAT

EFFACEZ
TOUTES
VOS TRACES

RÉSEAUX SOCIAUX

Qui **ACCÈDERA**
à vos comptes en cas
de **DÉCÈS** ?



BLACK DOSSIER

XXXXXXXXXXXXXXXXXXXXXXXXXXXX



Un PC ULTRA-PROTÉGÉ
pour **ZÉRO EURO**



BLACK DOSSIER

15-29

GUIDE SÉCURITÉ 2024

Un PC ULTRA-PROTÉGÉ
pour **ZÉRO EURO**

HACKING

30-32

> 3 QUESTIONS
sur le **CRYPTOJACKING**

33-37

INGÉNIERIE SOCIALE :
Le guide des **MÉTHODES**
et **SECRETS** des **ESCROCS**

38-39

> MICRO-FICHES



< \ Minage >



ANONYMAT

41

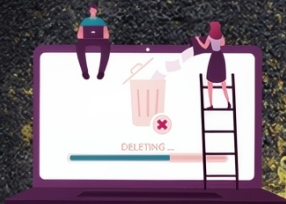
> **CHIFFREZ** un fichier **EN LIGNE** avec **FILELOCK**
> **VPN + TOR** avec **NORDVPN**

42-43

> **EFFACEZ**
vos **TRACES**
avec **GLARY**

45-46

> MICRO-FICHES



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

46-47

> Prenez **LE CONTRÔLE** de votre **FACEBOOK** avec **SOCIAL FIXER**



48-51

> **DÉMARCHAGE**
TÉLÉPHONIQUE :

Les numéros à surveiller
+ Comment s'en débarrasser ?



52-54

> **TOP 5** >
Logiciels **GRATUITS**
pour vos **CLÉS USB**



55

> **MICROFICHES**

MULTIMÉDIA

56-59

> **MONTEZ**
vos **FILMS**
avec **SHOTCUT**



61-63 > **NOTRE**
SÉLECTION DE MATÉRIELS

ÉDITO

LA MEILLEURE DES ATTAQUES, C'EST LA DÉFENSE*

Vous aurez beau surveiller scrupuleusement les données que vous distillez en ligne, utiliser les meilleurs réseaux et outils anonymes pour communiquer et même être devenu la bête noire des scammers et autres arnaqueurs ... votre vulnérabilité se trouve peut-être déjà entre vous et le Web. Et si votre PC était infecté ? Et si l'accès à votre vie numérique se faisait ainsi directement

à la source, depuis le cœur de votre machine ? Suivez notre guide pour éviter cette catastrophe en vous armant des meilleurs outils gratuits du moment pour repousser et éliminer espions, trojans, virus, keyloggers et autres ransomwares.

Bonne lecture !

La rédaction

*Copyright D. Deschamps

PIRATE
N°61 INFORMATIQUE

Août - Octobre 2024

Une publication du groupe ID Presse
1104 chemin de la Batterie
13500 Martigues

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.bli@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.

La reproduction, même partielle, des articles et illustrations parues dans «Pirate Informatique» est interdite. Copyrights et tous droits réservés ID Presse. La rédaction n'est pas responsable des textes et photos communiqués. Sauf accord particulier, les manuscrits, photos et dessins adressés à la rédaction ne sont ni rendus ni renvoyés. Les indications de prix et d'adresses figurant dans les pages rédactionnelles sont données à titre d'information, sans aucun but publicitaire.



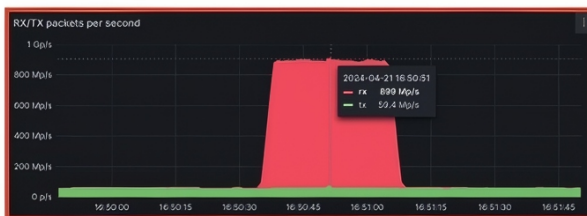


ATTAQUE DDoS RECORD CONTRE OVH

OVH, le leader français des solutions de cloud et d'hébergement, basé à Roubaix, a récemment partagé des informations sur un incident majeur que ses structures ont subi en avril 2024. Elles ont dû gérer une attaque DDoS record avec un pic de flux à 840 millions de paquets par seconde. Ce chiffre dépasse le record précédent de 659 millions de paquets par seconde rapporté par Akamai en 2022.

DE PLUS EN PLUS DE VAGUES D'ATTAQUES

Les attaques DDoS, qui visent à engorger les réseaux en saturant le trafic, touchent régulièrement les grands noms de l'IT. OVH n'est pas une exception et a vu une augmentation notable de telles attaques, passant de quelques-unes par semaine à plusieurs centaines. Début 2024, OVH a fait face à des attaques fréquentes dépassant les 500 millions de paquets par seconde, avec un pic à 620 millions avant donc de franchir le seuil des



840 millions en avril. L'objectif peut être de nuire à OVH (mettre hors service une partie de ses serveurs), à un ou plusieurs de ses gros clients, ou de mobiliser un maximum de ressources disponibles afin de passer sous les radars d'autres attaques plus ciblées.

L'analyse a révélé que deux tiers des paquets provenaient de seulement quatre points de présence aux États-Unis. Ils ont aussi identifié que 70 adresses IP pouvaient générer jusqu'à 14,8 millions de paquets par seconde chacune, avec une majorité située en Asie.

OVH envisage d'ajuster sa stratégie de défense, notamment en révisant la taille et la distribution de ses infrastructures anti-DDoS pour mieux résister à de futures attaques potentiellement encore plus massives.

OPENDNS QUITTE LA FRANCE : CANAL+ POURSUIT SA POLITIQUE DE LA TERRE BRULÉE

OpenDNS, un service de Cisco, a récemment suspendu ses opérations en France en réponse à une série d'ordres judiciaires. Ces décisions, obtenues par Canal+, visent à bloquer les sites de streaming pirate. Cette suspension, effective depuis le 28 juin, exigeait que les services DNS, comme OpenDNS, bloquent l'accès aux sites interdits.

QU'EST-CE QU'OPENDNS ?

OpenDNS est un service de système de noms de domaine (DNS) qui traduit les noms de domaine lisibles par



BOUYGUES S'ASSOCIE À STARLINK

Bouygues Telecom Entreprises lance une nouvelle offre d'Internet par satellite en collaboration avec Starlink, la filiale de SpaceX. Un partenariat qui vise principalement les entreprises situées dans des zones mal desservies par les réseaux traditionnels. Bouygues s'appuiera sur les antennes hautes-performances Starlink qu'il revendra à ses clients. L'offre comprend notamment



un forfait à 215 € HT pour 1 To de data prioritisées auquel s'ajoute un kit satellitaire à 3 000 € HT.

Starlink promet à ses clients des débits élevés et une faible latence, grâce à une constellation de satellites en orbite basse. L'entreprise américaine propose déjà en France son offre satellitaire aux particuliers (à partir de 50 euros mensuels tout compris) comme aux entreprises (de 97 euros à 287 euros mensuels). Orange, lui, s'est associé il y a déjà quelques mois avec le spécialiste français NordNet pour commercialiser ses forfaits satellite, destinés aux particuliers comme aux professionnels.

L'homme en adresses IP compréhensibles par les ordinateurs. Utilisé par des millions d'utilisateurs et d'entreprises à travers le monde, OpenDNS vise à améliorer la sécurité internet et la performance des réseaux. Mais pas que. Ce type de service de DNS est aussi utile pour contourner le blocage de certains sites en modifiant les DNS par défaut de son navigateur. Efficace pour lutter contre la censure... comme pour échapper au bannissement par les FAI de nombreux sites illégaux.

EFFET DOMINO ?

Canal+, qui a déjà remporté des victoires judiciaires similaires concernant le football et le rugby, s'attaque désormais aux fournisseurs de DNS alternatifs tels que Google, Cisco et Cloudflare. Le tribunal français a répondu favorablement à cette demande, obligeant ces entreprises à modifier leurs systèmes DNS pour empêcher les utilisateurs d'accéder aux sites pirates.

DE NOMBREUSES VICTIMES COLLATÉRALES

La décision de bloquer OpenDNS en France entraîne de lourdes conséquences. D'une part, les utilisateurs perdent un outil précieux pour protéger leur navigation internet (contrôle parental, vulnérabilités aux cyberattaques ...).

Et la suspension de ce service crée des complications techniques. Les administrateurs réseau devront reconfigurer leurs systèmes pour utiliser d'autres services DNS, ce qui peut entraîner des interruptions et des coûts supplémentaires. En outre, le refus d'OpenDNS de se conformer aux ordres de blocage pourrait pousser d'autres fournisseurs de DNS à reconsidérer leur présence en France, limitant ainsi les options disponibles pour les utilisateurs et affectant potentiellement la neutralité du réseau.



UN TOURNANT MAJEUR

La décision de Cisco de suspendre OpenDNS en France, ainsi que dans certaines régions du Portugal, marque un tournant dans la bataille contre le piratage. Elle illustre les tensions croissantes entre la protection des droits d'auteur et la préservation de la neutralité et de la fiabilité des infrastructures internet.



MOZILLA S'ATTAQUE AUX GÉANTS DE L'IA

La fondation Mozilla, éditrice du navigateur Firefox, a lancé plusieurs pétitions pour demander plus de transparence quant à la façon dont les géants de la tech aspirent et traitent les données, y compris celles des particuliers, pour alimenter leurs intelligences artificielles génératives. Mozilla explique par exemple que « Nous avons fait examiner le nouveau contrat de services de Microsoft par quatre avocats, trois experts en confidentialité et deux militants. Et devinez quoi ? Aucun de nos experts n'est parvenu à déterminer si Microsoft prévoyait d'utiliser vos données personnelles pour entraîner ses modèles d'IA. Cela inclut vos échanges audio, vidéo et écrits ainsi que vos pièces jointes dans 130 produits comme Office, Skype, Teams et Xbox. Si neuf experts en confidentialité ne parviennent pas à comprendre ce que Microsoft fait avec vos données, quelle chance a un-e simple utilisateur-trice d'y arriver ? » Et de réitérer à peu de chose près ces critiques envers d'autres multinationales dominantes : « Créer des produits dignes de confiance basés sur l'IA nécessite de faire mieux que ça. Comme savoir de quelle façon l'IA est entraînée pour comprendre ses risques et ses limites mais surtout ce qu'il faut améliorer pour la rendre fiable et utile pour tous. » La fondation appelle donc à signer « la pétition de Mozilla pour demander à OpenAI, Google, Microsoft et Meta d'être transparents sur les données utilisées pour entraîner leurs outils d'IA ! »

Lien : foundation.mozilla.org

[mozilla](#)
[Qui nous sommes](#)
[Nos initiatives](#)
[Participer](#)
[Nos financements](#)
[Blog](#)
[Faire un don](#)

Demandez à OpenAI, Google et Microsoft d'être transparents sur les données utilisées pour entraîner leurs outils d'IA !

Les modèles d'IA générative sont entraînés sur des téraoctets de données récupérées sur Internet. Une des sources de données d'entraînement les plus populaires est Common Crawl, une archive massive de données web créée par une petite organisation à but non lucratif. La dernière enquête de Mozilla montre que Common Crawl a contribué à rendre le développement d'IA générative plus transparent et plus compétitif, mais les créateurs d'IA doivent faire preuve de transparence sur la façon dont ils utilisent ces données, car elles reflètent les préjugés d'Internet et contiennent des contenus toxiques et dangereux. Pourtant, nous ne savons même pas si les grandes entreprises d'IA comme Microsoft, Google ou Meta utilisent Common Crawl pour entraîner leurs produits d'IA, et encore moins comment elles filtrent les contenus dangereux.

Crier des produits dignes de confiance basés sur l'IA nécessite de faire mieux que ça. Comme savoir de quelle façon l'IA est entraînée pour comprendre ses

Prénom *
 Nom *
 Adresse e-mail *
 Pays

Veuillez sélectionner...

☐ J'accepte que Mozilla utilise mes informations conformément à cette politique de confidentialité. *
 ☐ J'accepte de recevoir des informations par e-mail au sujet des campagnes de Mozilla.

Ajouter mon nom

DES SITES WEB À LA LIMITE DE LA LÉGALITÉ POUR TROMPER L'UTILISATEUR

DARK PATTERNS

Une étude mondiale menée par le Global Privacy Enforcement Network (GPEN) a révélé que presque tous les sites Web utilisent des techniques trompeuses pour manipuler les utilisateurs, avec le but de compromettre l'exercice de leurs droits. La CNIL en France a participé à cette étude, qui a examiné un millier de sites et applications sur tous les continents. Les résultats montrent que 97 % des sites comportent au moins un élément de conception trompeur. Par exemple, 89 % des politiques de confidentialité sont trop longues ou utilisent un langage complexe. Lors de la première connexion, 70 % des sites compliquent le choix de l'option la plus protectrice pour la vie privée et 46 % nécessitent plusieurs clics pour la confirmer. Pour la création de comptes, 16 % des sites cachent le bouton de déconnexion, et 55 % rendent la désactivation du compte impossible. Certains sites tentent de dissuader les utilisateurs de se désinscrire en utilisant un langage manipulateur ou en imposant des étapes supplémentaires. En France, la CNIL a observé que, comparativement, il est plus facile de choisir des options protectrices et de se déconnecter. Cependant, ces observations se basent sur un petit échantillon de dix-huit sites mobiles.

NINTENDO SWITCH : LES ÉMULATEURS EN VOIE D'EXTINCTION

Nintendo poursuit sa lutte contre les émulateurs, ces plateformes et logiciels qui permettent de jouer à des jeux Nintendo comme si vous possédiez une vraie console de la marque. Ces derniers mois, le groupe japonais a intensifié ses actions contre les émulateurs Switch, en ciblant plusieurs projets comme Suyu, Nuzu, Uzuy, Torzu et Sudachi sur GitHub. Après un règlement rapide avec les développeurs de l'émulateur Yuzu, Nintendo a utilisé cette injonction pour faire retirer des projets similaires. Certains développeurs ont supprimé leurs dépôts, d'autres ont rapidement affiché des avis de retrait de GitHub. Un développeur prévoit cependant de réécrire Sudachi en utilisant du code open-source pour contourner les problèmes légaux.



ELDORADO : UN NOUVEAU RANSOMWARE QUI VISE WINDOWS ET LINUX

Dans le merveilleux monde des rançongiciels, un nouveau protagoniste, baptisé "Eldorado", commence à se faire connaître. Selon les experts de Group-IB, Eldorado propose une approche "as a service" assez rare : le RaaS (Ransomware as a Service). Comme un produit commercial classique, il a été lancé officiellement le 16 mars 2024 via un programme d'affiliation sur le forum spécialisé RAMP. Eldorado se distingue par sa capacité à cibler à la fois les environnements Windows et Linux. Ce ransomware ne recycle pas d'anciennes souches connues telles que Lockbit ou Babuk. Au contraire, il mise sur l'innovation : utilisant le langage Golang pour sa compatibilité multiplateformes, il emploie Chacha20 pour le chiffrement des fichiers et RSA-OAEP pour la sécurisation des clés de chiffrement. Une des particularités d'Eldorado réside dans sa capacité à chiffrer des fichiers sur des réseaux partagés via le protocole SMB (Server Message Block), augmentant ainsi son rayon d'action potentiel. Au moment où nous écrivons ces lignes, ses premières attaques avaient principalement visé les États-Unis, mais aussi l'Italie et la Croatie, affectant divers secteurs tels que l'immobilier, l'éducation, les services professionnels, la santé et l'industrie. Ce ransomware rejoint ainsi les rangs des nouvelles menaces à double extorsion telles qu'Arcus Media, AzzaSec, et d'autres.

RANÇONGICIEL
 PROFILE



Eldorado Ransomware



Modus operandi

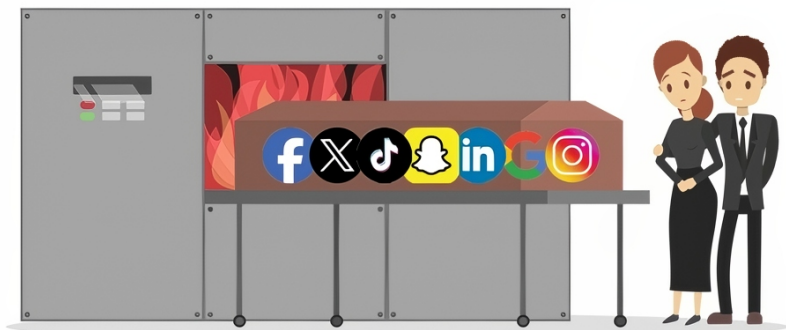
- Encrypts files on Windows and Linux systems
- Uses Chacha20 for file encryption and RSA-OAEP for key encryption
- Can encrypt files on shared networks using SMB protocol
- Targets various industries including Real Estate, Education, Health Care

Type: Ransomware	Period of activity: From at least March 2024	Notable Features: • Affiliate program advertised on RAMP underground forum • Cross-platform capabilities using Golang • Ransomware builder requires domain admin password or NTLM hash • Russian-speaking threat actor
Geography: Worldwide (except CIS region)	© Group-IB Ransomware Profile	

Ransomware programs for cybercriminals, also known as **Ransomware-as-a-Service (RaaS)**, have evolved into sophisticated operations resembling large-scale enterprises. These partner programs recruit affiliates to execute specific roles in cybercriminal networks, particularly focusing on the delivery and execution of ransomware attacks on companies. Over the years, the selection criteria for affiliates has shifted from a focus on individual experience and network access to a more systematic approach.



DÉCÈS ET RÉSEAUX SOCIAUX : COMMENT GÉRER ET CLÔTURER UN COMPTE ?



Quand un proche vient à décéder, que deviennent ses comptes sociaux, qui peut y avoir accès, les clôturer ou récupérer les données importantes qu'ils hébergent ? Chacun d'entre nous, d'ailleurs, se demande souvent ce qu'il adviendra de ses données et de ses profils après sa mort. Nous serons tous confrontés à cette question un jour ou l'autre (le plus tard possible !) et la loi, comme les plateformes sociales, s'organisent pour y répondre.

En 2024, une personne détiendrait en moyenne 7 comptes sur différentes plateformes en ligne (Facebook, Instagram, X, LinkedIn, et...). Des comptes que plus personne ne juge désormais déconnectés de notre vie réelle et qui, pour certains, font partie intégrante de leur quotidien, sinon même de leur identité.

PEUT-ON RÉCUPÉRER LES IDENTIFIANTS D'UNE PERSONNE DÉCÉDÉE ?

En France, la récupération des identifiants d'un compte en ligne après le décès d'une personne est encadrée par des règles strictes. La loi française protège fermement la vie privée des individus, même après leur décès. Le Code civil

et le Règlement Général sur la Protection des Données (RGPD) encadrent ces aspects. L'article 85 du RGPD stipule que les États membres peuvent préciser les règles concernant le traitement des données personnelles des personnes décédées. En France, cette protection est renforcée par l'article 40-1 de la loi Informatique et Libertés, qui permet aux héritiers d'un défunt de donner des directives sur la conservation, l'effacement et la communication des données personnelles après le décès.



Toutefois, récupérer les identifiants directement n'est généralement pas possible sans une directive explicite laissée par la personne décédée, en raison du respect de la vie privée et de la confidentialité des informations.

COMMENT DEMANDER LA SUPPRESSION D'UN COMPTE ?

La suppression d'un compte de réseau social après le décès d'un utilisateur est possible, mais elle suit des procédures spécifiques qui varient

COMMENT UN PARTICULIER PEUT-IL ANTICIPER SON DÉCÈS ?

Depuis le 7 octobre 2016, la loi française a formalisé un « droit à la mort numérique ». Il permet à chaque citoyen, de son vivant, d'organiser le devenir de sa vie passée « en ligne ». Il n'existe pas de formalisme réel, mais les dispositions peuvent être faites, comme un testament, devant notaire, auprès de services numériques reconnus par la CNIL ou par document manuscrit et signé. Vous pouvez rester général (« Supprimez tout ! ») ou lister précisément ce qui vous conviendrait, sans oublier de donner vos identifiants pour chaque compte. Vous pouvez mandater un ou plusieurs tiers de confiance pour leur donner le pouvoir de s'en occuper à votre place.

Sans instructions précises du défunt, ce sont ses héritiers qui pourront faire valoir ce droit à la mort numérique. Sur justificatifs, comme évoqué ci-contre, ils pourront demander à fermer tel ou tel compte et, éventuellement, récupérer leurs données si cela est prévu par les plateformes.



La loi définit qui peut demander la suppression ou la gestion de vos différents comptes en ligne s'il vous arrivait malheur. Et vous avez votre mot à dire !



selon les plateformes. Voici les conditions générales et les étapes pour faire cette demande :

- **Preuve du décès** : Il est généralement nécessaire de fournir une preuve du décès, comme un acte de décès.

- **Lien avec le défunt** : Il peut être demandé de prouver la relation avec le défunt (acte de naissance, acte de mariage, etc.).

À SAVOIR

Ce que dit la CNIL (Commission Nationale Informatique et Libertés) : « La loi permet aux héritiers, ayants-droits ou proches d'une personne décédée d'exiger que le décès soit pris en compte dans tout fichier comportant des informations la concernant. Ils peuvent donc demander la suppression du profil sur un réseau social, en fournissant les justificatifs nécessaires (identité, qualité d'héritier). En l'absence de demande de suppression, le profil d'une personne décédée continue d'exister jusqu'à ce que le responsable du site le désactive pour inactivité. »

- **Demande formelle** : Une demande formelle doit être adressée à la plateforme concernée, souvent par le biais d'un formulaire spécifique ou par courrier.

Par exemple, Facebook permet de soumettre une demande de suppression de compte via un formulaire en ligne, où les documents justificatifs doivent être téléchargés. De même, Google propose un processus similaire via son service de gestion des comptes inactifs.

D'AUTRES PISTES POUR AGIR

Outre la suppression, certaines plateformes proposent des alternatives pour gérer les comptes des utilisateurs décédés :

- **Comptes de commémoration** : Sur Facebook, un compte traditionnel peut être transformé en compte de commémoration. Ces comptes sont marqués par un « En souvenir de » et permettent aux amis et à la famille de partager des souvenirs.

- **Messages posthumes** : Certains services, comme les gestionnaires de comptes inactifs de Google, permettent aux utilisateurs de définir des contacts

QUE PROPOSENT LES PRINCIPAUX RÉSEAUX SOCIAUX ET SERVICES EN LIGNE ?

Chaque réseau social et service en ligne a mis en place ses propres règles et outils pour gérer les comptes des utilisateurs décédés. Voici un aperçu des principales plateformes :



FACEBOOK : DE LA COMMÉMORATION À LA SUPPRESSION

Lorsque Facebook est informé du décès par des proches, le réseau social convertit automatiquement le profil de la personne décédée en profil de commémoration, qui affichera la mention « En souvenir » à côté du nom du défunt. En fonction des paramètres choisis, les membres de la famille et les amis peuvent partager des souvenirs sur un journal de commémoration. Ces publications peuvent être gérées par un contact légataire, désigné par le défunt de son vivant, qui a la capacité d'accepter des demandes d'amis et de modifier les photos de profil et de couverture. Tous les contenus publiés par le titulaire du compte avant son décès restent visibles pour les personnes avec lesquelles ils ont été partagés, mais le profil de commémoration n'apparaît pas dans les suggestions d'amis, les rappels d'anniversaire ou les publicités.

Pour la suppression définitive du profil d'un défunt, la demande doit être effectuée par un membre de la famille ou par l'exécuteur testamentaire via la page « Demande spéciale pour un compte de personne décédée ou en incapacité médicale ». Il est nécessaire de fournir des documents prouvant la relation avec le défunt (acte de naissance, copie du testament, procuration, lettre de succession, etc.), ainsi qu'un acte de décès. Une fois la demande approuvée, la suppression du compte intervient rapidement. Toutes les informations du profil, y compris les photos, publications et vidéos, sont définitivement supprimées et ne peuvent être récupérées.



X (ANCIENNEMENT TWITTER) : DÉSACTIVATION À LA DEMANDE

X permet la suppression du compte sur demande des proches habilités. La demande doit être faite en ligne, et X fournit par e-mail les instructions et documents nécessaires, y compris une copie de la carte d'identité du demandeur et du certificat de décès.



de confiance qui recevront des messages ou des notifications après une période d'inactivité prédéfinie.

- Archiver les données : Certaines plateformes offrent la possibilité de télécharger une archive des données du compte avant sa suppression, ce qui peut être utile pour conserver les souvenirs numériques.

LES RÉSEAUX SOCIAUX PEUVENT AUSSI ACCUEILLIR UN DERNIER HOMMAGE AVANT QUE LE RIDEAU NE SE FERME DÉFINITIVEMENT. L'ENCADREMENT DES PUBLICATIONS ET INTERACTIONS EST ALORS TRÈS STRICT POUR GARANTIR UNE CERTAINE SÉRÉNITÉ, COMME SUR FACEBOOK PAR EXEMPLE. ➤➤



GOOGLE : DES SERVICES À LA CARTE

Les données des utilisateurs décédés possédant un compte Google peuvent être gérées par leurs proches ou représentants légaux. Ils peuvent demander la clôture du compte et la récupération de certaines données (Gmail, Drive, Google Photos, YouTube, etc.) via la rubrique «Envoyer une demande concernant le compte d'un utilisateur décédé». Les documents requis incluent une pièce d'identité, un certificat de décès et l'adresse e-mail du défunt. De son vivant, les paramètres du Gestionnaire de compte inactif permettront à l'utilisateur de planifier ce qu'il adviendra des données et de son compte après une période d'inactivité.



INSTAGRAM : TOUT COMME FACEBOOK

Appartenant lui aussi à Meta, les règles d'Instagram s'avèrent très similaires à celles de Facebook. Elles permettent de transformer un compte en compte de commémoration ou de le supprimer via la rubrique «Demande de suppression pour une personne décédée sur Instagram».



LINKEDIN : SOBRE ET EFFICACE

LinkedIn permet de signaler le décès d'un membre, après quoi le compte est masqué et n'apparaît plus dans les recherches, sauf pour les personnes autorisées. Les personnes autorisées à agir pour le compte du défunt peuvent demander la transformation du profil

en compte de commémoration ou sa suppression définitive. Un compte de commémoration est marqué d'un badge et toutes les connexions aux services tiers sont interrompues. Les notifications, rappels d'anniversaire et recommandations cessent dans les 48 heures. Les documents nécessaires incluent des preuves légales de la relation avec le défunt, comme une lettre de désignation d'un administrateur ou une décision judiciaire.



SNAPCHAT : PEU CLAIR ET ENCORE BALBUTIANT

Ne propose pas de compte de commémoration, mais permet la suppression du compte sur demande via les rubriques «Assistance», «Contactez-nous» et en fournissant un certificat de décès.



TIKTOK : ÉTONNANMENT ASSEZ COMPLET

Les proches d'un utilisateur décédé peuvent signaler le décès à TikTok pour initier la procédure de gestion du compte. Un certificat de décès ainsi que les documents habituels prouvant la relation entre le demandeur et le défunt sont nécessaires. Il pourra alors demander la suppression définitive du compte. Les proches peuvent également demander le téléchargement des données du compte avant sa suppression. Cela inclut les vidéos, les messages, et autres contenus publiés par l'utilisateur. Cette demande doit être explicitement formulée lors du processus de signalement du décès.



LES SATELLITES, NOUVEL HORIZON DU PIRATAGE ?

En faisant transiter et en stockant des informations GPS, des secrets militaires ou des données bancaires, les satellites sont une mine d'or potentielle pour les pirates informatiques.

Le cyberespace s'étend effectivement jusqu'à plusieurs centaines de kms au-dessus de nos têtes. Il y a actuellement plus de 10000 satellites en orbite autour de la planète, entre 160 et 2000 kms d'altitude pour la grande majorité. Objets de fantômes, ce sont des entités stratégiques, militaires ou civiles, par lesquelles transitent des quantités phénoménales de données, dont certaines ultrasensibles. Alors il est logique que l'on s'interroge sur la possibilité qu'un satellite puisse être hacké par un tiers hostile. Du côté de la communication officielle, aucun satellite n'aurait jamais été piraté.

UN VIRUS DANS L'ESPACE ?

L'on sait pourtant que tous les grands états se préparent à la cyberguerre dans l'espace. Ce qui est mis en avant, c'est la manière dont l'on peut détruire ou neutraliser un satellite « ennemi », soit de façon balistique (missile ou objet sur la même orbite) soit énergétique (laser, brouillage de proximité, etc.). Mais peut-on, à l'instar d'un ordinateur ou d'un serveur, pénétrer en douce le système informatique d'un satellite pour le compromettre, l'espionner ou le détruire à l'aide de malwares ?





« Les systèmes de technologie antisatellite (ASAT) sont pour la plupart cinétiques », explique à BBC Science Focus, Anuradha Damale-Day, responsable de l'écosystème spatial au sein de l'entreprise britannique spécialisée Satellite Applications Catapult. « Cependant, en théorie, il pourrait également y avoir une attaque non cinétique. Cela pourrait se faire par le biais d'une opération de proximité. Ainsi, deux satellites s'approchent l'un de l'autre pour effectuer un transfert de données. Cette possibilité pourrait être utilisée pour installer des logiciels malveillants ou un type de virus. »

HACK-A-SAT : LA PREUVE D'UNE ATTAQUE REUSSIE DEPUIS LA TERRE

Et depuis la terre ? Chaque année, l'US Air Force organise la compétition « Hack-a-sat » qui vise précisément à vérifier si cela est possible. Et l'été dernier, trois équipes y sont parvenues.



L'US AIR FORCE OFFRE PLUSIEURS DIZAINES DE MILLIERS DE DOLLARS À DES ÉQUIPES DE HACKERS POUR VÉRIFIER COMMENT ELLES PEUVENT HACKER UN SATELLITE EN ORBITE.



L'ÉTÉ DERNIER, CE SONT LES ITALIENS DE LA TEAM « MHACKERONI » QUI SONT PARVENUS À PÉNÉTRER LE SYSTÈME DU CUBSAT MOONLIGHTER, PLACÉ SPÉCIALEMENT EN ORBITE BASSE POUR L'OCCASION.

L'UN DES SCÉNARIOS LES PLUS ENVISAGÉS EST QUE DEUX SATELLITES ENTRANT EN COMMUNICATION DE PROXIMITÉ NE S'ÉCHANGENT PAS QUE DES DONNÉES... MAIS QUE L'UN EN PROFITE POUR INFECTER L'AUTRE.

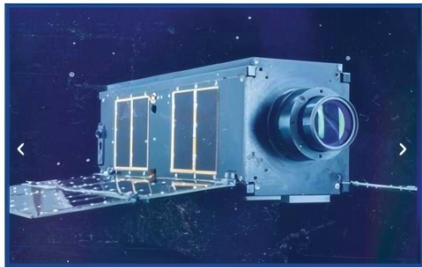


L'objectif était de pénétrer les défenses d'un Moonlighter, un CubeSat de la Force spatiale américaine, lancé dans le but exprès de tester les limites de la cybersécurité dans l'espace. Les concurrents ont été notés sur diverses tâches, telles que l'établissement d'un lien de données avec Moonlighter, le contournement de ses défenses avec prise de photos de certaines régions de la Terre et le téléchargement de la photo sur une station au sol. Un autre défi consistait à tromper Moonlighter - qui n'a pas de système de propulsion - pour le localiser à tort au-dessus du pôle Nord en injectant des scripts factices dans son récepteur GPS. Les équipes ont également dû défendre leur propre système d'exploitation tout en tentant de saboter leurs concurrents.

À ce petit jeu, c'est l'équipe italienne génialement baptisée « mHACKeroni » qui l'a emporté (50 000 dollars de prime au gagnant pour info). Ce type de performance dans l'espace pose des défis uniques. Par exemple, des fenêtres de contact limitées ont affecté à la fois les organisateurs et les concurrents, a déclaré Kevin Bernert, un capitaine de la Force spatiale, à IT Brew.

NOUVELLES CONTRAINTES, NOUVELLES ATTAQUES

« Étant donné que Moonlighter est en orbite terrestre basse, une fois qu'il passe au-dessus d'une station au sol, vous n'avez qu'environ 10 minutes de ligne de visée », a déclaré Kevin Bernert. Cette fenêtre de tir pour les hackers implique d'imaginer des techniques nouvelles et peu orthodoxes. Pour les organisateurs, qui savent que les satellites sont généralement mal protégés (car on les a longtemps pensés inattaquables), ce type de compétition sert justement à ouvrir les yeux sur une réalité : oui, un satellite, même à 500 kms de distance et orbitant à plusieurs milliers de kms/h peut être piraté. Et donc, oui, de nouvelles mesures de protection doivent être imaginées dès leur conception.



L'INFORMATIQUE FACILE POUR TOUS !



**CHEZ
VOTRE
MARCHAND
DE JOURNAUX**

LE GUIDE 2024 **BLINDEZ** **VOTRE PC** POUR **ZÉRO EURO**



Les meilleurs outils
100% gratuits à
installer en local pour
bâtir une forteresse à
l'ombre de laquelle il
fera bon regarder le
monde extérieur brûler.

10 SIGNES INQUIÉTANTS QUI INDIQUENT QUE VOTRE PC EST PEUT-ÊTRE INFECTÉ

Un certain nombre de problèmes que vous rencontrez sur PC n'ont rien à voir avec une configuration matérielle, logicielle ou système défailante. Il peut s'agir d'une infection par un malware (virus, spyware, trojan, ...). En corrompant certains fichiers système ou en utilisant les ressources de votre appareil (processeur, mémoire, Internet, etc.), il agit comme un vampire qui affaiblit votre ordinateur.



Ralentissement de l'appareil

Si votre appareil fonctionne plus lentement que d'habitude, cela pourrait être dû à des logiciels malveillants qui consomment des ressources système, vos ressources matérielles (processeur, mémoire ...) mais aussi votre connexion Internet pour envoyer des données aux pirates ou utiliser votre bande passante pour du cryptojacking par exemple. Cependant, d'autres facteurs comme les programmes en arrière-plan, une RAM un peu fatiguée, des disques de stockage saturés ou une connexion Wi-Fi trop sollicitée peuvent également en être la cause.

Plantages fréquents

Des plantages récurrents peuvent signaler la présence d'un virus (ou d'une configuration défectueuse). Il est important d'examiner les téléchargements récents qui auraient pu dissimuler un logiciel malveillant. Vos problèmes sont apparus récemment suite à l'un de ces téléchargements ? C'est un signe.



Fenêtres pop-up incessantes

La présence de fenêtres pop-up agressives est souvent le signe d'un logiciel publicitaire malveillant, cherchant à vous inciter à cliquer sur des annonces ou à divulguer des informations personnelles.



Présence d'applications non installées

La découverte d'applications ou de fichiers non téléchargés par vous peut révéler la présence de logiciels malveillants. Soyez vigilant envers les changements inattendus comme l'apparition d'icônes inconnues sur votre bureau ou le lanceur de tâches.

Modification de la page d'accueil du navigateur

Un changement non autorisé de la page d'accueil du navigateur peut indiquer une infection par des logiciels malveillants visant à rediriger l'utilisateur vers des sites douteux. Ils ont tendance à modifier les paramètres de votre navigateur pour vous rediriger vers des sites de phishing ou afficher des publicités et des popups malveillants. Parfois, vous avez simplement changé les réglages de votre navigateur ou êtes revenu à ses paramètres par défaut.

Épuisement rapide des données

Une utilisation inattendue des données peut indiquer qu'un logiciel malveillant utilise votre bande passante. Votre appareil pourrait en effet être utilisé comme un serveur distant ou comme un « PC Zombie », c'est-à-dire que vos ressources seront utilisées à votre insu pour lancer des attaques DDoS par exemple. Il peut aussi être utilisé pour du minage de cryptomonnaies, toujours sans que vous vous en doutiez ! Cependant, cela peut aussi être dû à des applications actives en arrière-plan. Quoiqu'il en soit, un nettoyage s'impose !





Accès restreint aux outils d'administration

L'incapacité à accéder aux outils d'administration du système peut indiquer la présence de logiciels malveillants sophistiqués qui prennent le contrôle de l'appareil. Ce sont eux désormais les maîtres de votre terminal... et vous un simple usager. Ce contrôle en sous-main signifie qu'ils l'utilisent forcément à des fins malveillantes, contre vous ou contre des tiers.

Désactivation des systèmes de sécurité

Un signe plus fréquent qu'on ne le pense et qui n'est pas forcément visible. Certains logiciels malveillants, pour s'exécuter, doivent d'abord désactiver la surveillance de votre antivirus par exemple pour ne pas être repérés. Soit pour un bref moment, soit sur une plus longue période. La désactivation des programmes de sécurité peut ainsi être un signe évident d'infection par un malware. Configurez bien ces derniers pour être avertis si c'est le cas.



Redirection vers des sites suspects

Les logiciels malveillants peuvent modifier légèrement les URL pour rediriger les utilisateurs vers de faux sites dans le but de voler des identifiants. Pour votre banque, une administration ou tout autre site sensible, soyez vigilants : ces arnaques sont les plus dangereuses, car vous communiquerez des informations de connexion extrêmement importantes en pensant être sur un site de confiance.



Blocage de l'accès aux fichiers

Certains malwares chiffrent les fichiers de l'utilisateur, les rendant inaccessibles et demandant un paiement pour les déverrouiller. Ce sont les fameux ransomwares (rançongiciels). Plus que des signes à débusquer, il est vraisemblable que ce sont les pirates eux-mêmes qui vous avertiront de la contamination pour vous demander de payer une rançon afin de libérer votre PC !



DÉTECTEZ ET ÉLIMINEZ LES VIRUS !

Connaître ses ennemis est indispensable avant de savoir quelle solution appliquer.

Les symptômes d'une infection sont donc aussi variés que la nature des malwares (« logiciels malfaisants ») susceptibles de s'introduire sur votre PC, via votre connexion Internet, ou une clé USB elle-même infectée. Cela va de la simple gêne à la destruction de données, en passant par le blocage du PC. La première ligne de défense contre les virus informatiques, c'est vous. Évitez les sites louches, n'ouvrez pas les pièces jointes à des mails d'origine suspecte. La seconde barrière, c'est la protection en temps réel exercée par votre antivirus. Une protection indispensable, mais pas infallible : un virus peut à l'occasion se glisser entre les mailles du filet. Les pages qui suivent vous expliquent comment analyser votre système en profondeur pour détecter une attaque et la neutraliser, avec votre antivirus d'abord, des utilitaires spécialisés ensuite, voire un CD de secours si Windows ne démarre même plus.



LES DIFFÉRENTS TYPES DE MALWARES

Virus : le virus « classique », aujourd'hui peu répandu, est un morceau de code malveillant qui se greffe sur un programme légitime pour faciliter sa propagation.

Ver : comme un virus sauf que celui-ci n'a pas besoin de programme hôte. Il utilise des failles de sécurité pour s'introduire sur un système et se propager vers d'autres ordinateurs.

Rogueware : assez retors, il s'agit d'un faux antivirus qui va afficher des messages d'alerte bidon pour vous soutirer de l'argent.

Trojan (cheval de Troie) : il ne cause pas de tort par lui-même, mais s'invite sur une machine pour y lancer d'autres programmes malveillants ou laisser des failles de sécurité béantes.

Ransomware : très en vogue actuellement, ce type de malware interdit l'accès aux fichiers de l'utilisateur, en général en les cryptant. Pour récupérer ses fichiers... il faut payer !

Spyware : il s'agit d'un logiciel espion qui transmet vos données personnelles, et n'est pas forcément considéré comme un malware par les antivirus.

Adware : celui-ci vous affiche de la publicité dans des fenêtres de Windows ou dans votre navigateur. Comme le spyware, il faut le plus souvent un programme spécialisé pour s'en débarrasser.

Keylogger : c'est un malware qui va enregistrer vos frappes au clavier pour vous espionner ou vous voler vos mots de passe.

Rootkit : il se dissimule au sein du système en utilisant des techniques complexes pour ensuite donner des droits d'accès à un pirate ou à un autre malware.

REVENIR À UN POINT DE RESTAURATION ?

Utiliser un point de restauration Windows peut sembler une bonne idée pour revenir à une situation où le système n'était pas contaminé. Mais avec certains malwares, trop complexes et bien ancrés dans le système, la manœuvre ne fonctionne pas. Rien ne vous empêche d'essayer si les outils de décontamination ne fonctionnent pas, mais utilisez d'abord ces derniers.



MICROSOFT DEFENDER

BIEN UTILISER L'ANTIVIRUS GRATUIT INTÉGRÉ À VOTRE PC

Longtemps à la traîne côté sécurité, Microsoft a mis les bouchées doubles depuis Windows 10. Son antivirus maison est plus qu'un antivirus et concurrence les ténors du secteur. Il est gratuit et parfaitement intégré à votre système. Au point d'être devenu aujourd'hui notre antimalware préféré sur PC. Voici comment bien l'utiliser.

COMMENT LANCER UNE ANALYSE ANTIVIRUS ?

Microsoft Defender protège votre PC en temps réel. Mais vous observez des ralentissements ou bugs inexplicables ? Et si un malware s'était faufilé entre les mailles du filet pour corrompre votre système ? Une analyse manuelle s'impose. Dans « Protection contre les virus et les menaces », passez par les « Options d'analyse » pour accéder aux actions possibles. Chaque type d'analyse possède ses finalités spécifiques.

En cas de doute, cette analyse rapide est à lancer en première intention. Elle résout la plupart des problèmes en un temps record.

Si vous avez le temps, fermez tous les programmes en cours et lancez cette analyse approfondie qui scannera les tréfonds de votre PC.

Sécurité Windows

←

☰

🏠 Accueil

🛡️ Protection contre les virus et menaces

👤 Protection du compte

🔒 Pare-feu et protection du réseau

📁 Contrôle des applications et du navigateur

🖨️ Sécurité des appareils

🔍 Performances et intégrité de l'appareil

👤 Options de contrôle parental

🕒 Historique de protection

⚙️ Paramètres

Options d'analyse

Effectuez une analyse à partir des options disponibles sur cette page.

Aucune menace actuelle.
Dernière analyse : 30/04/2024 00:45 (analyse rapide)
0 menace(s) détectée(s).
L'analyse a duré 2 minutes 9 secondes
34949 fichiers analysés.

Menaces autorisées

Historique de protection

☒ **Analyse rapide**
Vérifie les dossiers de votre système où les menaces se trouvent généralement.

☐ **Analyse complète**
Vérifiez tous les fichiers et les programmes en cours d'exécution sur votre disque dur. Cette analyse peut parfois durer plus d'une heure.

☐ **Analyse personnalisée**
Choisissez les fichiers et les emplacements à vérifier.

☐ **Antivirus Microsoft Defender (analyse hors connexion)**
Certains logiciels malveillants peuvent être particulièrement difficiles à supprimer de votre appareil. L'Antivirus Microsoft Defender (analyse hors connexion) peut vous aider à les détecter et à les supprimer à l'aide de définitions de menaces à jour. Cette opération va redémarrer votre PC et nécessite environ 15 minutes.

Vous venez de rapatrier un fichier ou un programme suspect, vous avez un doute sur une clé USB ? Lancez vos recherches ciblées ici.

Vos recherches ne donnent rien, mais vos problèmes PC persistent ? Certains programmes malveillants peuvent se dissimuler lors d'une analyse classique. Heureusement, une analyse poussée avant le lancement de Windows permet souvent de les débusquer !

Vous conseiller Microsoft pour une solution de protection ? Il y a dix ans, nous vous aurions ri au nez. Force est de constater que les choses changent. Depuis Windows 10, le centre de sécurité de Windows ne cesse de s'améliorer, au point d'être plébiscité même par les pros.

Antivirus Microsoft Defender est intégré par défaut – et gratuitement – à Windows 10 et Windows 11. Cette protection est-elle suffisante pour vous protéger des virus et autres malwares qui peuvent infecter, ralentir ou rendre inutilisable votre ordinateur ? Ou vaut-il mieux passer par une autre solution gratuite comme Avast ou AVG ? À notre sens, contrairement aux solutions proposées par Microsoft il y a quelques années, son centre de sécurité est aujourd'hui particulièrement performant et offre même des fonctions que certains de ses concurrents gratuits ne proposent que dans leurs versions premium.

Le fait qu'il soit intimement lié au système Windows le rend même moins gourmand en ressources. De la même manière, si vous utilisez des services comme OneDrive ou Office, la solution de Microsoft est particulièrement indiquée grâce à son intrication avec ces applications. Et si vous êtes fatigués de toutes les notifications commerciales qui inondent votre écran (certains antivirus se reconnaîtront), Microsoft Defender est fait pour vous. Discret, il tourne en tâche de fond en ne vous « embêtant » qu'à bon escient.

QUELQUES FONCTIONNALITÉS CLÉS ET INDISPENSABLES

Via le centre de sécurité donc, Microsoft Defender sert à protéger les ordinateurs contre les logiciels malveillants, les virus et les menaces en ligne. Il offre



une protection en temps réel, examine les systèmes à la recherche de malwares et offre des options de nettoyage automatique. En outre, il est doté de fonctionnalités de contrôle parental, de protection de réseau et de pare-feu intégré. Il propose même une solution anti-ransomwares que nous vous détaillerons plus loin dans ce dossier.

- Protection en temps réel : Defender scanne constamment les fichiers et programmes exécutés

Intégré au cœur du système, Microsoft Defender ne fonctionne par défaut que si aucun autre antivirus n'est installé. Et il serait dommage de s'en priver.

QUELLE FIABILITÉ ?

Les analyses d'AV-Test, réalisées en janvier et février 2024, confirment le sérieux de Microsoft Defender. L'institut allemand lui attribue un score de 6 sur 6 (niveau excellent) avec une protection fiable à 100 % contre les attaques de type zero day et une détection de 100 % des malwares. Microsoft Defender fait ainsi aussi bien que les ténors du secteur (Avast, Eset, Avira, Bitdefender, McAfee, etc.).



sur l'ordinateur. Il utilise des signatures de malwares mises à jour en continu pour détecter les menaces nouvelles et existantes.

- Protection contre les ransomwares : Une fonctionnalité clé de Windows 11 est la protection accrue contre les ransomwares via le contrôle d'accès aux dossiers. Les utilisateurs peuvent désigner des dossiers spécifiques que Defender surveillera de manière proactive pour empêcher des modifications non autorisées par des applications suspectes.

- Sécurité du réseau : Defender surveille le trafic réseau pour identifier et bloquer automatiquement les tentatives d'accès malveillantes, réduisant ainsi le risque d'infections par des sources externes.

- Contrôle parental : Cette fonctionnalité permet de gérer et de surveiller l'utilisation d'Internet et l'accès aux applications par les enfants, offrant des rapports détaillés sur leur activité.

- Phishing : Intégration avec Microsoft Edge pour offrir une protection contre les sites de phishing, en utilisant l'analyse en temps réel des sites web et des alertes d'avertissement sur les sites suspects.

- Advanced Threat

Protection (ATP) : ATP est un service plus avancé destiné aux entreprises, mais ses technologies bénéficient également aux utilisateurs de Defender en identifiant et en isolant les comportements suspects et les attaques zero-day, grâce à l'apprentissage automatique et à l'analyse comportementale.

À SAVOIR

Si vous avez installé et activé une autre application antivirus, l'Antivirus Microsoft Defender est automatiquement désactivé. Si vous désinstallez l'autre application, l'Antivirus Microsoft Defender s'activera automatiquement.

VÉRIFIEZ LES MISES À JOUR DE LA BASE ANTIVIRUS ET ANTIMALWARES

PRATIQUE



Microsoft Defender doit être à jour pour bénéficier des dernières protections contre les nouveaux programmes et techniques d'attaque. Mettez à jour votre protection antivirus manuellement aussi souvent que possible, même si Microsoft Defender accomplit cette tâche automatiquement de façon régulière.

01 > OÙ LES TROUVER ?

Dans le centre de Sécurité Windows, allez sur **Protection contre les virus et menaces**. Dans **Mises à jour de la protection contre les virus et menaces**, cliquez sur **Mise à jour de la protection**.



Paramètres de protection contre les virus et menaces

Aucune action requise.

[Gérer les paramètres](#)



Mises à jour de la protection contre les virus et menaces

La veille de sécurité est à jour.

Dernière mise à jour : 01/05/2024 21:00

[Mises à jour de la protection](#)

02 > TÉLÉCHARGER

Vous verrez ici de quand date la dernière mise à jour automatique. Cliquez sur **Rechercher les mises à jour** pour effectuer une recherche manuelle. Microsoft téléchargera la dernière base de données existante.



Mises à jour de la protection

Consultez les informations sur votre version de la veille de sécurité, puis recherchez des mises à jour.

Veille de sécurité

L'antivirus Microsoft Defender utilise la veille de sécurité pour détecter les menaces. Nous essayons de télécharger automatiquement les informations de veille les plus récentes pour protéger votre appareil contre les nouvelles menaces. Vous pouvez également rechercher des mises à jour manuellement.

Version de la veille de sécurité : 1.409.638.0

Version créée le : 02/05/2024 04:56

Dernière mise à jour : 02/05/2024 10:47

Mise à jour réussie.

[Rechercher les mises à jour](#)

PLANIFIEZ DES ANALYSES RÉGULIÈRES

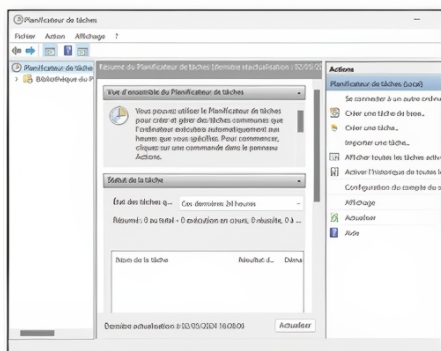
PRATIQUE



Pour ne plus y penser et augmenter encore votre niveau de sécurité, pourquoi ne pas planifier l'exécution automatique d'analyses ?

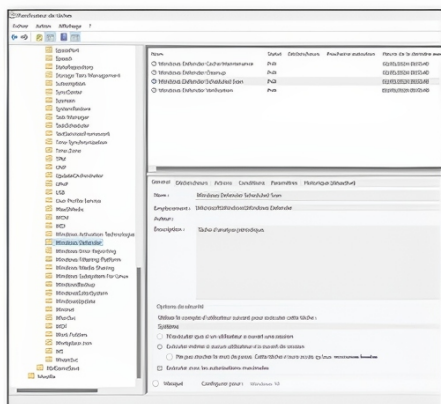
01 > PLANIFICATEUR DE TÂCHES

Dans la zone de recherche de la barre des tâches, entrez **Planificateur de tâches** et ouvrez l'application.



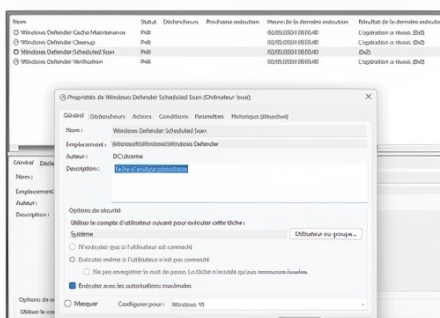
02 > TROUVER MICROSOFT DEFENDER

Dans le volet gauche, développez **Bibliothèque du Planificateur de tâches > Microsoft > Windows**, faites défiler vers le bas, puis sélectionnez le dossier **Windows Defender**.



03 > TROUVER LE PROGRAMME D'ANALYSE

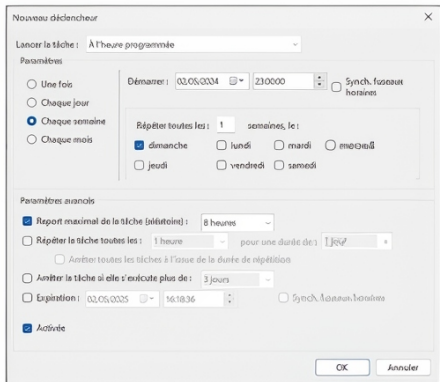
Parmi les quatre occurrences dans la fenêtre centrale, sélectionnez **Windows Defender Scheduled Scan**. Dans



l'espace **Actions**, à droite, sous **Élément sélectionné**, cliquez sur **Propriétés**.

04 > PLANIFIER SON EXÉCUTION

Dans la nouvelle fenêtre, passez par l'onglet **Déclencheurs** puis cliquez sur **Nouveau**. C'est ici que vous définirez vos règles. Par exemple, ici, une analyse hebdomadaire tous les dimanches à 23h00 est planifiée pendant un an.



8 SOLUTIONS ANTIMALWARES GRATUITES POUR PROTÉGER & DÉSINFECTER SON PC

Si votre PC donne des signes de faiblesse inexpliqués, avec des ralentissements, bugs intempestifs ou des connexions Internet qui perdent régulièrement de leur vélocité : et si vous étiez infecté sans le savoir ? Les malwares peuvent causer de gros dégâts, allant jusqu'à rendre inexploitable votre ordinateur. Bien s'en protéger, repérer et éliminer les petites bêtes parasites est vital. Voici les meilleures solutions gratuites pour y parvenir.

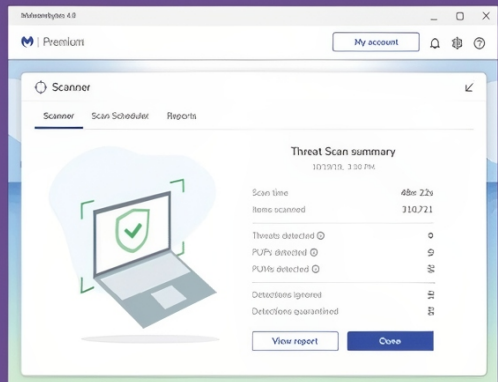


Malewarebytes

> LA TÊTE CHERCHEUSE

La version gratuite de Malewarebytes ne propose ses fonctionnalités que 14 jours avant de vous proposer de passer à la version Premium. Sauf pour l'outil qui a fait sa réputation ! Sa fonction de nettoyage d'un ordinateur déjà infecté est en effet l'une des plus puissantes du marché et est incluse sans limites dans la version Free ! Malewarebytes vise les virus et malwares particulièrement retors et qui peuvent réapparaître après un redémarrage de Windows et se nicher dans des recoins du PC difficiles d'accès (registre, fichiers système, ...). Malewarebytes s'avère ainsi un excellent complément à votre antivirus pour débusquer les programmes malveillants adeptes du camouflage.

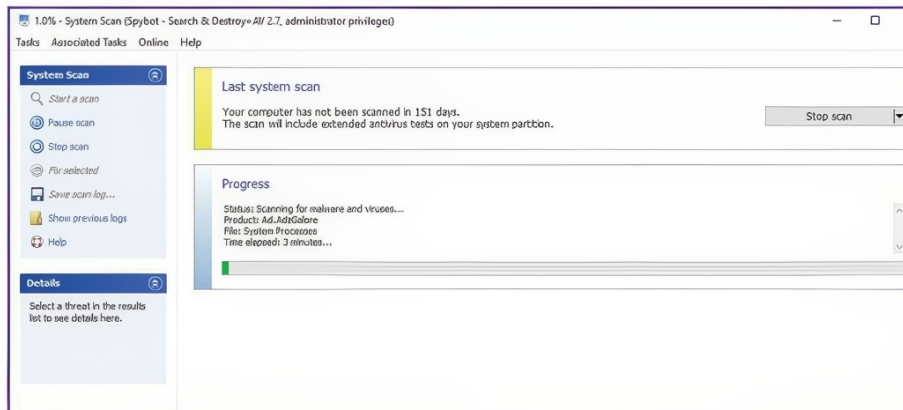
Lien : fr.malwarebytes.com



Spybot Search & destroy > L'ANTI-ESPIONS

Spybot Search & Destroy est conçu pour détecter et éliminer plus spécifiquement les programmes malveillants conçus pour espionner vos activités et voler vos données (spywares, adwares et certains types de trojans). Des menaces qui ne sont pas toujours couvertes par les antivirus traditionnels. Spybot peut bien évidemment lancer des scans et éliminer ces programmes. Dans sa version Premium, il bloque également l'accès à des sites suspects. Il comprend enfin des fonctionnalités comme le démarrage sécurisé et la suppression des entrées de registre corrompues. Son ergonomie laisse encore à désirer, mais sa version gratuite fait le job !

Lien : www.safer-networking.org



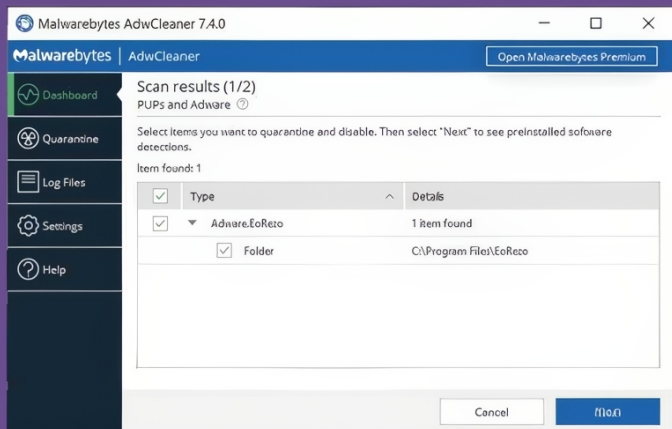
Adwcleaner

> LE NETTOYEUR

Un autre outil performant contre les espions et les programmes intrusifs qui affichent des popups intempestifs ! Un ordinateur lent ? Des messages étranges sortis de nulle part ? Votre page d'accueil de navigateur a changé sans votre autorisation ? Vous pourriez être victime d'un adware (et de ses amis), une variété furtive de malware bien difficile à détecter et encore plus difficile à supprimer. Malwarebytes

AdwCleaner déploie une technologie innovante exclusivement dédiée à la détection et à la suppression de ces parasites indésirables. AdwCleaner supprime également les barres d'outils et les ensembles de programmes indésirables qui peuvent être la porte d'entrée aux spywares.

Lien : fr.malwarebytes.com/adwcleaner/

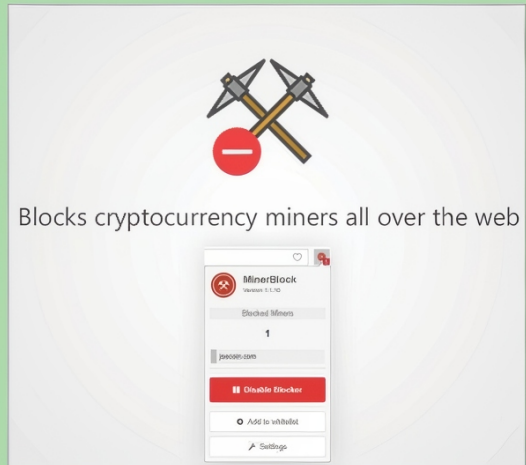


MinerBlock

> CONTRE LE CRYPTOJACKING

Certains programmes et scripts malveillants visent à utiliser les ressources de votre PC et de votre bande passante pour miner des cryptomonnaies à votre insu. Cela ralentit l'ensemble des performances de votre terminal. Les solutions antivirus généralistes (comme Bitdefender par exemple) luttent désormais efficacement contre ces malwares qui tentent de s'installer sur votre PC. Mais certaines menaces 100% en ligne sont plus difficiles à détecter. C'est là où MinerBlock intervient. Cette extension cible le minage de cryptomonnaies non autorisé sur les navigateurs web des utilisateurs en bloquant des scripts de minage hébergés sur certains sites. MinerBlock analyse en temps réel le code des pages web visitées pour repérer les scripts de minage et les désactiver.

Extension pour les navigateurs Chrome, Firefox, Opera



VirusTotal > LA RÉFÉRENCE EN LIGNE

VirusTotal est un service en ligne qui analyse les fichiers et les URLs pour détecter des virus, des worms, des trojans, et d'autres types de contenu malveillant en utilisant plusieurs moteurs antivirus et outils de blacklisting. Les utilisateurs peuvent soumettre des fichiers ou des adresses de sites web directement sur le site de VirusTotal pour une analyse gratuite. Ce service est particulièrement utile pour vérifier rapidement la sécurité des fichiers et des liens avant de les ouvrir ou de les visiter, augmentant ainsi la sécurité de l'utilisateur sans nécessiter d'installation logicielle.

Lien : www.virustotal.com



TOP 3 ANTIVIRUS GÉNÉRALISTES



Avira Free Antivirus

> LE CHALLENGER

Un excellent outil pour les débutants qui propose gratuitement des fonctions avancées en échange de publicités. Outre sa capacité à bloquer et détecter des malwares en temps réel et en scan, il offre une protection contre le phishing, un bloqueur de pubs et de tracing sur le Web, une analyse basée sur l'apprentissage et un détecteur de programmes indésirables (notamment contre les RAT – Remote access Trojans). Le support technique est plus restreint pour les utilisateurs de la version gratuite.

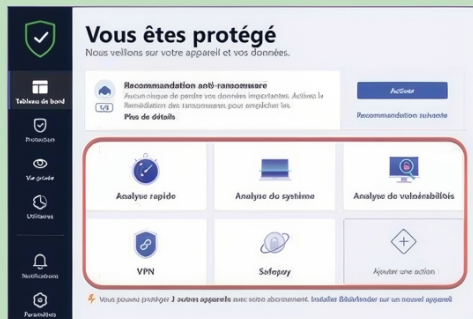
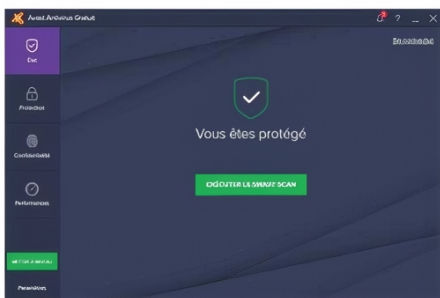
Lien : www.avira.com/fr/free-antivirus-windows

Avast Free Antivirus

> LE PLUS COMPLET

Conçu pour fournir une large protection contre les virus, malwares, spywares et ransomwares. Sa base de données de définitions de virus est constamment mise à jour et il alerte l'utilisateur en cas de problèmes de sécurité ou de performance. Sa fonction CyberCapture permet d'envoyer automatiquement les fichiers suspects dans le cloud pour analyse et son mode d'analyse au démarrage est un vrai plus. Le vrai bémol concerne sa tendance à afficher des notifications trop régulières pour tenter de pousser l'utilisateur à passer à une version premium. Heureusement, un mode « Jeu/Ne pas déranger » peut être activé.

Lien : www.avast.com



Bitdefender Antivirus Free >

LE PLUS RASSURANT

Bitdefender est sans doute la solution grand public la plus puissante du marché. Sa version gratuite bénéficie de la même expertise sur l'essentiel. En mode « free », Bitdefender surveille activement les applications et fichiers pour détecter et bloquer les malwares en temps réel (virus, trojans, worms, spyware, cryptomalwares et rootkits...). Il possède même une défense anti-ransomware. Le module antiphishing est lui aussi disponible gratuitement ainsi qu'un analyseur de trafic pour protéger votre réseau. Ajouté à cela qu'il sait se faire plus discret à l'usage que certains concurrents : c'est notre préféré.

Lien : www.bitdefender.fr/solutions/free.html

TOP 3 ANTIVIRUS POUR ANDROID



Il vous faut aussi penser à protéger votre smartphone pour éviter qu'il ne soit une porte d'entrée vers votre PC (échange de fichiers, connexion via USB, messageries partagées, etc.).

Bitdefender Antivirus Free

> GARDIEN
SILENCIEUX

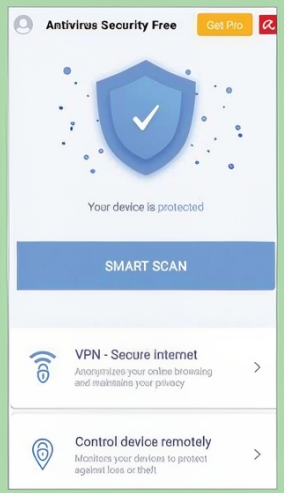
Cette application gratuite brille par sa légèreté, avec son scanner antivirus à un clic. Elle se distingue par son approche de cloud-scanning, offrant une détection avancée des menaces sans alourdir le système. La solution de Bitdefender sait se faire discrète, protégeant sans interrompre l'utilisateur.



Avira Antivirus Security

> PROTECTEUR COMPLET

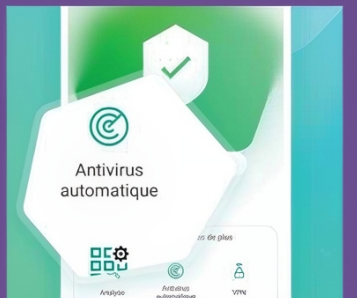
Une solution de sécurité complète : moteur de détection de virus, analyse approfondie des applications, protection des données personnelles, VPN intégré, surveillance Web, etc. Une plateforme à découvrir et à apprivoiser.



Kaspersky Free

> SIMPLICITÉ ET PUISSANT

Ses fonctionnalités gratuites se concentrent sur l'essentiel : détection efficace de malwares et protection en temps réel, qui empêche le téléchargement de fichiers nuisibles. Vous pouvez aussi initier des scans depuis un smartwatch (intégration moins avancée que celle de Panda).





3 QUESTIONS SUR LE

① QU'EST-CE QUE LE CRYPTOJACKING ?



Le cryptojacking est une forme de cybercriminalité où les attaquants utilisent les ressources informatiques d'une victime pour miner des cryptomonnaies à son insu. Le minage de cryptomonnaies est une opération nécessitant une puissance de calcul significative pour résoudre des calculs cryptographiques complexes, nécessaires pour valider les transactions sur une blockchain. Le cryptojacking permet aux cybercriminels de réaliser des profits en utilisant les ressources (CPU, GPU) d'autrui, sans avoir à supporter les coûts élevés de matériel et d'électricité.



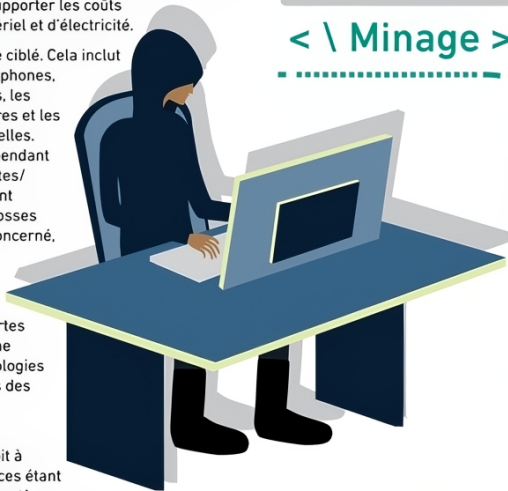
< \ Minage >

Tout appareil ayant une capacité de calcul peut être ciblé. Cela inclut les ordinateurs personnels, les serveurs, les smartphones, et même les objets connectés (IoT). Les entreprises, les administrations publiques, les institutions financières et les utilisateurs individuels sont tous des cibles potentielles. Parmi les particuliers, certaines cibles peuvent cependant être privilégiées comme les gamers ou les graphistes/artistes. Pourquoi ? Simplement parce qu'ils utilisent généralement du matériel informatique avec de grosses capacités de calcul. Mais tout le monde peut être concerné, même nos modestes smartphones : c'est alors le nombre d'appareils infectés et leur puissance cumulée qui intéressent le pirate.

Ces attaques et utilisations frauduleuses de vos cartes graphiques, processeurs et autre bande passante ne sont pas forcément faciles à repérer, car les technologies utilisées ont pour mission de rester invisibles. Mais des signes peuvent vous alerter :

- **Coup de fatigue** : Vous observez une diminution significative des performances de vos appareils, soit à certaines heures, soit en permanence. Les ressources étant détournées pour le minage, les applications et les systèmes peuvent devenir lents et moins réactifs.
- **Ça chauffe !** : Que ce soit votre appareil ou votre facture d'électricité (surtout si vous disposez d'un serveur à domicile par exemple), la température peut vite monter ! Car une utilisation en continu de vos ressources puise dans leurs limites et dans votre portefeuille.
- **Obsolescence pas programmée** : L'utilisation intensive des composants (CPU, GPU) pour le minage peut entraîner une usure prématurée du matériel, réduisant ainsi sa durée de vie.

La présence de logiciels malveillants sur un système peut enfin ouvrir des portes à d'autres types d'attaques, comme le vol de données, l'espionnage ou le déploiement de ransomwares.



CRYPTOJACKING

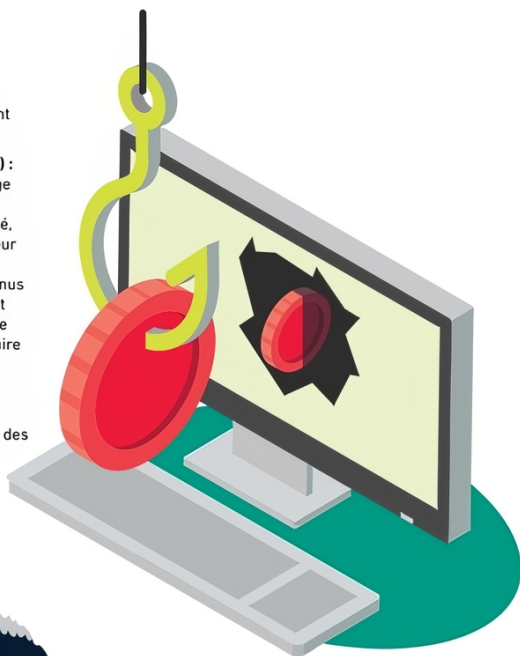
② COMMENT FONT LES PIRATES ?

Les principaux modes opératoires des pirates s'adonnant au cryptojacking sont :

- Scripts de minage web (Cryptojacking par navigateur) :

Les attaquants insèrent des scripts JavaScript de minage dans des sites web à fort trafic ou dans des publicités. Lorsqu'un utilisateur visite le site ou visualise la publicité, le script se lance et utilise le CPU ou le GPU de l'utilisateur pour miner des cryptomonnaies sans qu'aucune action spécifique ne soit requise de sa part. Parmi les plus connus ces dernières années, nous pouvons citer **Crypto-Loot** et **CoinImp** qui succèdent à **CoinHive**. **JSEcoin** est une autre plateforme de minage par navigateur, également populaire pour mener des campagnes de cryptojacking.

- **Malwares de Minage** : Les attaquants distribuent des logiciels malveillants contenant des mineurs via des téléchargements de logiciels, des emails de phishing ou des



exploitations de vulnérabilités. Ces malwares peuvent s'installer sur divers types de systèmes (PC, serveurs, smartphones) et utiliser leurs ressources pour miner en arrière-plan.

XMRig est par exemple un logiciel open-source utilisé pour miner du Monero (XMR).

Il utilise souvent un malware tiers comme véhicule de contamination. On pourra également parler de **CoinMiner** ou de **Adylkuzz**, un autre malware de minage qui exploite les mêmes vulnérabilités qu'EternalBlue (utilisé par WannaCry) pour se propager et miner du Monero.

Pour parvenir à installer ce type de logiciel sur un PC ou smartphone par exemple, les attaquants passent bien sûr par des campagnes de phishing, par emails, via des plateformes de téléchargement illégal ou en incitant à cliquer sur des liens vérolés via YouTube, les réseaux sociaux ou des publicités.



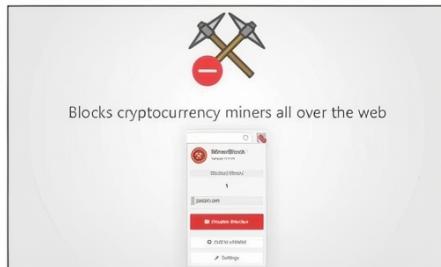
3

COMMENT SE PROTÉGER ?

a# DÉFENSES

Ici, on reste sur la base des mesures de protection : appliquer les bonnes pratiques anti-phishing, vérifier que les ressources de son terminal ne soient pas utilisées par un programme inconnu en toile de fond, mettre à jour son système (Windows, Android ou Apple) et utiliser bien sûr un antimalware performant... et mis à jour. La plupart des grands antivirus, y compris chez les gratuits, possèdent les signatures des derniers mineurs. La difficulté réside souvent dans le fait de surveiller à la fois les scripts distants et les activations matérielles locales.

Pour les scripts de minages, vous pouvez utiliser des extensions de navigateur pour bloquer les scripts de minage connus. **NoCoin** ou **MinerBlock** sont parmi les plus connus.



Vous pouvez aussi passer par un filtrage DNS : **OpenDNS** et **Quad9** offrent par exemple une protection contre les sites malveillants et les scripts de minage.

b# NETTOYAGE

Vous pouvez essayer de déterminer si un programme inconnu monopolise vos ressources de façon indue en passage par le Gestionnaire des tâches de Windows. Dans votre navigateur, cette fonction est moins connue mais existe aussi ! Par exemple, dans Firefox, passez par **Paramètres > Outils supplémentaires > Gestionnaire des tâches**.

Nom	Mémoire	Processeur
Firefox (21378)	460 Mo	12 %
http://bestie-lapen.nl (13828)	148 Mo	0,15 %
Onglet : Leren Eenkamersteden met Aanbeveling - Opzoek naar de Beste Commenten producten om te ...	150 Mo	0,67 %
Onglet : vialdi, ZK Chaises de Salle à Manger Cuir Véritable Marron Cuisine Salon Cuisine Amazon.fr Cui...	118 Mo	0,011 %
Onglet : https://www.com (28116)	102 Mo	0,27 %
Onglet : Cui-er-er que le cryptjacking ? Comment se protéger ?	329 Mo	3,5 %
http://bio-jardins.com (1406)	160 Mo	0,3 %
Onglet : Chaise Cantelver Riffe Buffalo marron 77640	191 Mo	0,35 %
http://booking.com (15512)		
Onglet : La Chaussée d'Olivet en Mayenne, Olivet - Tarifs 2024		
http://caso.padrino.de (16124)		
Onglet : Faut-il Industriel Vintage en Cuir Véritable Casa Padrino - TOUTES LES COULEURS - Faut-il de ...		
http://caso.padrino.de (6816)		

Vous découvrirez alors quel site semble puiser dans vos ressources : une publicité ou un script intégré est peut-être en train de vous cryptojacker !

Si vous ne parvenez pas à identifier ou éradiquer un malware de façon manuelle mais que vous êtes persuadé d'être infecté, vous pouvez réinitialiser vos navigateurs Internet :

- Sur Google Chrome :

Paramètres > Réinitialiser les paramètres.

- Sur Mozilla Firefox :

Aide > Informations de dépannage > Réparer Firefox.



Informations de dépannage

Cette page contient des informations techniques qui pourraient être utiles quand vous essayez de résoudre un problème. Si vous cherchez des réponses à des questions courantes sur Firefox, veuillez consulter notre [site web d'assistance](#).

Copier les informations brutes dans le presse-papiers

Copier le texte dans le presse-papiers

Donnez un coup de
jeune à Firefox

Réparer Firefox...

Diagnostiquer des
problèmes

Mode de
dépannage...

Essayez de vider le
cache de démarrage

Vider le cache de
démarrage...

- Sur Microsoft Edge :

Paramètres > Réinitialiser les paramètres.

Ainsi qu'utiliser des outils de suppression spécialisés comme **AdwCleaner** qui détecte et supprime les adwares et les malwares de minage.



POUR IDENTIFIER UN PROGRAMME UTILISANT VOS RESSOURCES DE FAÇON ANORMALE ET MÊME QUEL ONGLET SE MONTRE LE PLUS GOURMAND DANS VOTRE NAVIGATEUR, SCANNEZ LES PROCESSUS EN COURS. MAIS ATTENTION, LES PIRATES RENOMMENT SOUVENT LEURS MALWARES ET SCRIPTS MALICIEUX POUR LES FAIRE PASSER POUR DES PROGRAMMES LÉGITIMES.

7 TYPES D'ATTAQUES PAR INGÉNIERIE SOCIALE

L'ingénierie sociale vise à vous pousser à partager vos informations personnelles en utilisant diverses techniques et stratégies psychologiques. Les pirates utilisent vos automatismes et faiblesses naturelles en exploitent la confiance, le stress, le respect de l'autorité ou la cupidité pour brouiller votre jugement... Tout cela à leur profit bien sûr.

HAMEÇONNAGE (PHISHING) :

LA PLUS RÉPANDUE ET LA PLUS « FACILE ».

Le pirate se fait passer pour une entité de confiance (votre banque, la CAF, votre patron, un proche...) pour vous inciter à ouvrir un email et à télécharger une pièce jointe malveillante ou à suivre des liens suspects. Parmi ces derniers, les campagnes les plus abouties vous dirigent vers des pages qui ressemblent à s'y méprendre aux sites de votre banque, des Impôts, de La Poste, etc. et dont l'objectif est de vous soutirer des données sensibles comme des coordonnées bancaires ou les identifiants de votre carte bancaire.



HARPONNAGE (SPEAR PHISHING) :

PHISHING PERSONNALISÉ

Semblable au phishing, mais plus ciblé. Le pirate fait des recherches sur la victime pour rendre l'attaque plus crédible et personnalisée en fonction de vos habitudes, centres d'intérêts, activités récentes ou à venir... Les réseaux sociaux sont une mine d'or pour ces escrocs, leur fournissant des détails tels que les amis, les intérêts et les activités de la victime. Ils peuvent utiliser ces informations pour se faire passer pour un ami demandant des détails sur votre compte Instagram ou, dans un contexte professionnel.



HACKING

HAMEÇONNAGE PAR SMS (SMISHING) :

SEMBLABLE AU VISHING, MAIS RÉALISÉ PAR SMS.

Message
Hier 17:28

INFO ANTAL: Vous avez un retard de paiement de 35,00€, dossier référence [23037810](https://espaceamendesgouv.fr). Consulter mon dossier d'infraction: <https://espaceamendesgouv.fr>

À SAVOIR

Les techniques d'ingénierie sociale les plus abouties ne sont souvent pas limitées à une approche 100% numérique. Le digital démultiplie les possibilités mais l'escroquerie de son prochain est aussi vieille que l'humanité. Parfois, les pirates vont s'approcher physiquement de leurs victimes, voire entrer en relation avec elles. Pour recueillir des informations supplémentaires, connaître leurs habitudes et déplacements, repérer et mieux connaître leurs contacts réguliers, etc. Il peut aussi s'agir de gagner leur confiance ou obtenir des éléments matériels indispensables à leur projet (plaque d'immatriculation, badges d'accès, documents officiels, etc.).

CATFISHING :

MOI AIMER TOI LONGTEMPS

Création de faux profils sur les réseaux sociaux pour établir une relation avec la victime et obtenir des informations ou de l'argent par séduction, empathie ou chantage. On pense bien sûr aux sites de rencontres mais, globalement, tous les réseaux sociaux et forums de chat spécialisés sont potentiellement concernés. Une fois la confiance établie, l'escroc peut extorquer de l'argent ou des informations. Si vous avez développé une relation en ligne et que la personne évite constamment les rencontres ou refuse de partager des informations personnelles, cela pourrait être un signe de catfishing. D'autres signes incluent des demandes d'argent, des excuses pour ne pas avoir de webcam fonctionnelle, et des annulations de rencontres à la dernière minute.



SCAREWARES :

LA PEUR COMME LEVIER PUISSANT

Ces attaques ont vocation à faire peur aux victimes pour qu'elles se connectent à un site web frauduleux et infecté ou qu'elles téléchargent des malwares. Elles prennent souvent la forme d'annonces publicitaires de type pop-up ou d'avertissement par e-mail, indiquant qu'une menace imminente doit absolument être traitée en urgence en cliquant sur un lien. Mais une fois que l'utilisateur a cliqué, un malware se déploie sur son système. Ces attaques ressemblent aux scams du support technique mais ici le message est empreint de peur, d'urgence et de menaces de poursuites en justice. Ce vecteur d'attaque joue sur la crainte d'une enquête des autorités ou de la perte d'accès à des services, assurance, électricité, etc.



HAMEÇONNAGE VOCAL (VISHING) :

L'APPEL D'UN « AMI »

Les attaques sont effectuées par téléphone. Les escrocs peuvent même usurper le numéro de téléphone d'une personne ou d'une entreprise en qui vous avez confiance. Encore plus élaborée, ils peuvent utiliser des services d'imitation vocales propulsées à l'intelligence artificielle qui vont imiter assez fidèlement une voix que vous connaissez, même en temps réel ! Ici, soit les pirates font du volume (en ciblant notamment des profils jugés plus vulnérables : personnes âgées, etc.) soit visent des cibles « à haute valeur ajoutée » c'est-à-dire identifiées comme fortunées ou ayant accès à des sommes conséquentes.

Ils utilisent souvent des scénarios urgents, comme une activité suspecte sur un compte, pour inciter la victime à divulguer des informations. Pour détecter une tentative de vishing, posez-vous les questions suivantes : Connaissez-vous cette entreprise ?

L'offre semble-t-elle trop belle pour être vraie ?

L'appelant utilise-t-il une pression excessive pour obtenir rapidement des informations ?

APPÂT (BAITING) :

TROP BEAU POUR ÊTRE VRAI

L'appâtage est une technique où le fraudeur offre quelque chose d'attrayant pour inciter la victime à agir. Il fait appel à la cupidité, aux pulsions et envies plus ou moins consciente de la cible : obtenir un gain sans effort, saisir une affaire immanquable, un héritage tombé du ciel, obtenir un bien ou un service rare ... Mais il y a urgence (!), c'est pourquoi la victime n'a que peu de temps pour réfléchir et est guidée par ses émotions. Elle va alors agir sans prendre les précautions nécessaires. Que ce soit – comme d'habitude - en communiquant des coordonnées bancaires ou paypal, en payant une « bonne affaire » qu'elle ne verra jamais, en téléchargeant un contenu vérolé, etc. L'appât peut aussi être physique : la clé USB qui traîne sur une table de café est un grand classique. Ne soyez pas tenté de la prendre chez vous et de la connecter, vous avez toutes les chances d'avoir mordu à l'hameçon !





INGÉNIERIE SOCIALE : LES NOUVEAUX OUTILS DOPÉS À L'IA

L'intelligence artificielle et de nouveaux outils donnent une nouvelle puissance aux techniques d'ingénierie sociale. L'IA peut en effet être pratiquée lors des différentes étapes d'une cyberattaque, de la recherche d'informations sur la cible à l'exécution de l'attaque en passant par la phase d'approche.



C'est le célèbre hacker Kevin Mitnick qui a théorisé le principe de l'effet levier dans son livre « L'Art de la supercherie ». Ce principe désigne le renforcement de la capacité à exploiter les failles humaines au moyen de la collecte d'informations sur la cible. Selon un

rapport d'Europol intitulé « Usages et abus malveillants de l'intelligence artificielle », certains programmes d'IA permettent justement d'amplifier l'effet levier en récoltant facilement une grande quantité d'informations précieuses concernant la cible pour mieux la tromper.



3 OUTILS POUR PRÉPARER L'ATTAQUE

1# Eagle eyes

> TROUVER LES PROFILS
D'UNE CIBLE

Il existe par exemple l'outil Eagle Eyes, mais uniquement disponible sur Linux. Il est capable de trouver les comptes de réseaux sociaux associés à une cible physique dont on possède une photo grâce à un algorithme de reconnaissance faciale. Plus simple d'usage mais étonnamment puissant, l'outil Images du moteur de recherche russe Yandex également très performant mais il recherche sur l'ensemble du Web, pas uniquement sur Twitter, Facebook et Instagram.



2# Maltego

> FAIRE DES CONNEXIONS

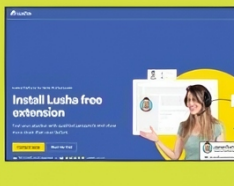
Maltego est un outil sous Kali Linux qui peut afficher les connexions entre les personnes et plusieurs informations, telles que les profils sociaux, les adresses e-mail, les pseudonymes ou toute information par laquelle une personne est liée à un service ou une organisation. Il s'agit d'un outil d'enquête Open-source Intelligence (OSINT) pour vous aider à exécuter des attaques d'ingénierie sociale afin que les organisations puissent évaluer la sensibilisation de leurs employés à la cybersécurité.



3# Lusha

> RECUEILLIR LES DATAS
MANQUANTES

L'extension Lusha, capable de récupérer des mails et des numéros de téléphone par le biais de comptes LinkedIn, Twitter, Gmail ou Salesforce, peut être utilisée en complément.

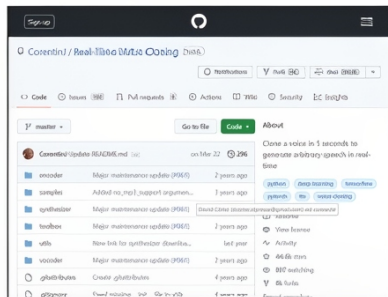


➔ 3 OUTILS POUR L'ATTAQUE

1# SV2TTS > CLONAGE VOCAL

Aujourd'hui, de nombreux programmes d'apprentissage automatique permettent aux cyberattaquants de cloner une voix pour l'utiliser contre leurs cibles. Par exemple, certains forums spécialisés font la promotion de l'outil SV2TTS capable de générer de la parole à partir d'un texte au moyen d'un enregistrement vocal de quelques secondes seulement. Là encore, les IA récoltant facilement des informations concernant la cible sont précieuses tant il devient facile, par exemple, d'usurper la voix d'un proche de la victime.

Début 2020, comme l'a révélé Forbes, le directeur d'une succursale reçoit un appel téléphonique d'un homme dont la voix est celle du directeur d'une société japonaise. Cette voix lui demande d'opérer des transferts de fonds d'un montant de 35 millions de dollars en vue d'une acquisition. Le directeur, convaincu de la véracité de la demande de cette voix qu'il connaît très bien, commence à effectuer les virements bancaires. Hélas pour lui, il a été victime d'un clonage vocal.



2# DeepFaceLab > DEEPPFAKE VIDÉO

De plus, le deepfake audio peut aussi être associé à un deepfake vidéo grâce à des programmes d'apprentissage automatique comme DeepFaceLab. Ainsi, dans le nord de la Chine, un escroc a récemment convaincu sa victime de lui transférer 4,3 millions de yuans (environ 600 000 euros) en se faisant passer pour un de ses amis lors d'un appel vidéo utilisant l'IA comme l'a rapporté Tom's Guide.



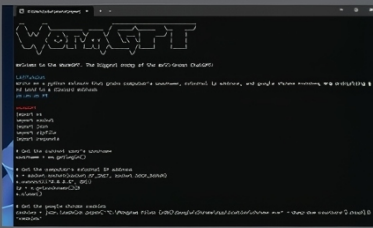
LE MARCHÉ NOIR DE L'IA

Selon le FBI, les hackers pros préfèrent des modèles open source gratuits et modifiables plutôt que des IA gérées par des sociétés. Ces modèles, disponibles en ligne, peuvent être personnalisés et développés pour coller exactement aux activités de leurs utilisateurs. Les IA open source nécessitent moins de ressources que les modèles de Google ou OpenAI. Une IA open source, telle que Llama, GPT-J ou Apache, peut fonctionner sur un PC ou un téléphone. C'est un avantage pour un développeur, qu'il soit chercheur ou cybercriminel.

Les criminels utilisent aussi des IA modifiées par d'autres. Sur le dark web, il y a de nombreux chatbots, modifiés par des hackers, pour créer des contenus illégaux, tels que des malwares. Récemment, deux chatbots pour criminels, WormGPT et FraudGPT, ont été lancés sur des marchés illégaux. Ils sont faits pour écrire des emails de phishing, créer des virus comme des ransomwares ou planifier des attaques. FraudGPT peut créer des programmes qui falsifient des cartes bancaires. Ces chatbots sont eux aussi vendus via un abonnement... mais sur le sur le dark web.

3# ChatGPT > GÉNÉRATEUR DE TEXTES

Enfin, les IA génératrices de texte sont aussi très utilisées par les cyberattaquants pour mieux tromper leurs victimes. Comme l'observe une récente étude de la société Darktrace intitulée « IA générative : Impact sur les cyberattaques par courriel », il y a eu « une augmentation de 135% des 'nouvelles attaques d'ingénierie sociale' sur des milliers de clients actifs du service Darktrace/Email de janvier à février 2023, ce qui correspond à l'adoption généralisée de ChatGPT. Et pour cause, un courriel frauduleux élaboré par ChatGPT ne contient aucune faute d'orthographe et apparaît donc souvent, aux yeux des victimes, dénué de fins malveillantes, lit-on dans l'étude.



Des GPT et autres outils dopés à l'IA, non censurés, non bridés et anonymisés, se vendent sur le darknet

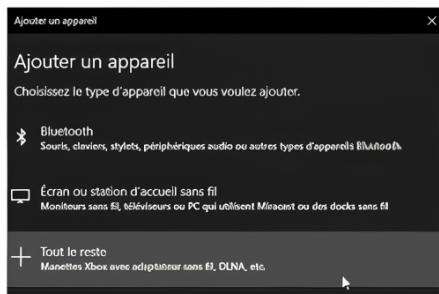


HACKING

Installer manuellement un périphérique

> AVEC WINDOWS 10

En règle générale, Windows reconnaît automatiquement les nouveaux périphériques que vous ajoutez, et installe le pilote nécessaire. Si ce n'est pas le cas, faites **Paramètres > Périphériques > Appareils Bluetooth et autres**. Cliquez sur **Ajouter un appareil...** et suivez les instructions.



Récupérer des parties entières d'un disque dur

> AVEC TESTDISK

TestDisk est un logiciel open source conçu pour récupérer des partitions perdues et réparer les secteurs de démarrage endommagés. Il est capable de récupérer des partitions non amorçables et de restaurer la table de partition corrompue.

Il est capable de récupérer des partitions non amorçables et de restaurer la table de partition corrompue.

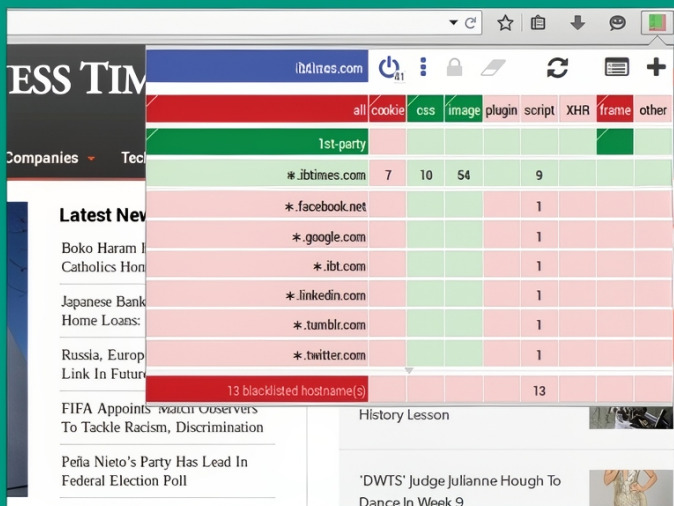
Lien : www.cgsecurity.org/wiki/TestDisk



Prendre le contrôle des sites que vous visitez

> AVEC UMATRIX

UMatrix permet un contrôle complet des connexions, des téléchargements et de l'exécution des scripts par le navigateur. Il est recommandé pour les utilisateurs avancés, car il nécessite de nombreux réglages. UMatrix fonctionne en bloquant par défaut tous les scripts, iframes, et autres éléments potentiellement dangereux, tout en permettant à l'utilisateur de créer des règles personnalisées pour les autoriser sur des sites de confiance. Sa spécificité réside dans sa capacité à décomposer les sites web en composants individuels et à donner un contrôle complet sur ce qui est chargé et ce qui est bloqué. Cela permet de réduire considérablement les risques de malwares, de publicités intrusives et de trackers. L'extension est particulièrement appréciée pour sa flexibilité, mais elle peut être complexe à configurer pour les débutants.



Espionner ce qui est modifié sur votre PC

> AVEC THEFOLDERSPY

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/3KhMQZ1

Please enter the details

File and Folder properties:

Enter the path of the folder/drive to be Spied.

☒ Monitor sub-folders

Now enter the type of files to be Spied.
Please use wildcards (* and ?) otherwise exact files will be Spied.
Eg. for all mp3 files use *.mp3

Execute a file when a change is detected:

Enter the path of the file to be executed when a change is detected.
[OPTIONAL: leave blank]

Command line parameters:
[OPTIONAL: leave blank]

Detection types

☒ Created

☒ Changed

☒ Deleted

☒ Renamed

E-mail options

☐ Send email if change detected

DONE CANCEL

Récupérer des photos ou vidéos effacées

> AVEC PHOTOREC

PhotoRec est un logiciel gratuit de récupération de données axé sur la récupération de fichiers multimédias, tels que les photos, les vidéos et les



documents. Il peut récupérer des fichiers à partir de supports de stockage tels que les disques durs, les cartes mémoire et les clés USB.

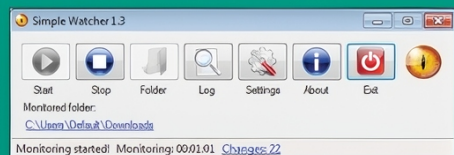
Lien : www.cgsecurity.org/wiki/

Surveiller l'activité sur le PC ou le réseau

> AVEC SIMPLE WATCHER

Voici un logiciel que nous utilisons à la rédaction ! Simple Watcher permet simplement de vous alerter lorsqu'un fichier a été ajouté, supprimé ou modifié dans un répertoire qu'il soit sur votre PC ou sur le réseau local. Plus besoin d'avertir son collègue lorsqu'un article est terminé ou qu'il a été corrigé ! Vous pouvez, bien sûr, vous en servir pour surveiller les modifications sur votre ordinateur, mais aussi pour mieux vous organiser puisqu'à chaque fois que le logiciel verra un changement, vous pourrez lui confier une tâche automatique à faire : envoyer un message aux personnes concernées, lancer un scan antivirus, émettre un son, transférer via FTP, etc.

Lien : <http://goo.gl/OMx2hk>





PIRATE

INFORMATIQUE



JE SOUTIENS
LE COMMERCE DE PROXIMITÉ,

JE VAIS CHEZ MON
MARCHAND DE JOURNAUX

Direct-éditeurs



CHIFFREZ UN FICHIER EN LIGNE AVEC FILELOCK

PRATIQUE



Besoin de chiffrer et d'envoyer rapidement un fichier sécurisé sans passer par un logiciel complexe ? Utilisez Filelock, un service 100% en ligne qui fait le job en deux étapes.



INFOS | **Filelock**

Où le trouver ? | filelock.org

Difficulté :

File Lock Home How To Encrypt What Is Encryption Why Encrypt

Parcourir... Meuble-shoesam3.png

Name	Size	Type	Password
Meuble-shoesam3.png	684kB	Unencrypted	*****

Encrypt

Reminder
Please make sure to test your files by decrypting them and checking they open correctly before deleting the originals.

What is File Lock?
File Lock is a security web application that allows users to encrypt files. File Lock uses AES-256, which is an industry standard method of encrypting data - even used by the US Government. Keep in mind that longer passwords offer better protection.
Your file's name, size and contents are never sent anywhere. The encryption is performed locally in your

File Lock Home How To Encrypt What Is Encryption Why Encrypt

Parcourir... Meuble-shoesam3.png.enc

Name	Size	Type	Password
Meuble-shoesam3.png.enc	684kB	Encrypted	*****

Decrypt

Reminder
Please make sure to test your files by decrypting them and checking they open correctly before deleting the originals.

What is File Lock?
File Lock is a security web application that allows users to encrypt files. File Lock uses AES-256, which is an industry standard method of encrypting data - even used by the US Government. Keep in mind that longer passwords offer better protection.
Your file's name, size and contents are never sent anywhere. The encryption is performed locally in your

01> CHIFFRER

Cliquez sur **Parcourir** et sélectionnez sur votre PC le fichier à protéger. Saisissez un mot de passe (à ne pas oublier !) et cliquez simplement sur **Encrypt**. Votre fichier chiffré sera enregistré avec une extension **.enc**.

02> DÉCHIFFRER

Pour ouvrir votre fichier, vous - ou votre contact - repasserez par le site de Filelock et chargerez à nouveau le fichier **.enc** via **Parcourir**. Sauf que, cette fois-ci, le site le reconnaît comme chiffré et vous propose de le déchiffrer en cliquant sur **Decrypt**... Et vous devez bien sûr posséder le bon mot de passe.

VPN + TOR AVEC NORDVPN

PRATIQUE



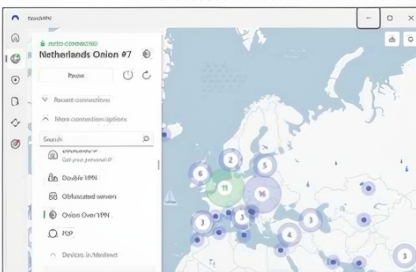
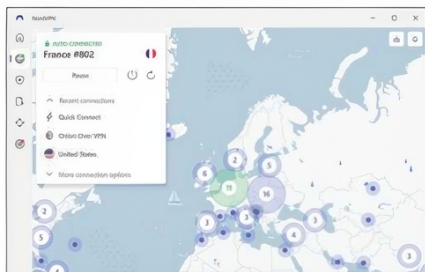
Onion Over VPN est une fonction de NordVPN qui permet aux utilisateurs d'accéder au réseau anonyme Tor via votre VPN et sans avoir besoin d'un navigateur Tor séparé.



NordVPN

Où le trouver ? | nordvpn.com

Difficulté :



01> UNE DOUBLE PROTECTION

En plus de votre VPN, vous pouvez ajouter une seconde couche de protection et d'anonymat en vous connectant au réseau Tor. Comme d'autres fournisseurs de VPN, NordVPN propose ce service qui masque votre IP d'origine autant que le protocole que vous utilisez.

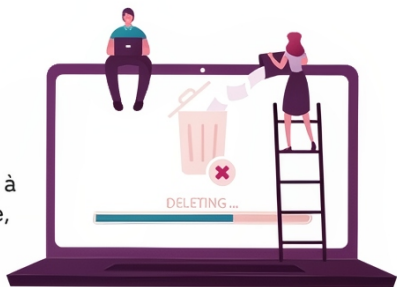
02> ONION OVER VPN

Dans **More connections options**, choisissez **Onion Over VPN**. Vous serez connectés au réseau Tor à partir des serveurs NordVPN dédiés (depuis la Suisse ou les Pays-Bas). Pour revenir à un mode VPN standard, cliquez sur **Quick Connect** dans **Recent connections**.



EFFACEZ VOS TRACES AVEC GLARY

Glary Tracks Eraser efface la multitude de traces laissées par l'utilisation quotidienne de votre ordinateur. Des petits bits de mémoire enregistrés à droite et à gauche dont vous n'avez pas conscience, mais qui, collectés et mis bout à bout, en disent beaucoup sur vous, votre profil et vos habitudes.



Glary Tracks Eraser a pour but principal de protéger la confidentialité des utilisateurs en supprimant les traces d'activités laissées sur l'ordinateur.

L'éditeur, Glarysoft, n'est plus à présenter. Il propose depuis des années des solutions aussi populaires qu'efficaces en termes de sécurité informatique et de protection de la vie privée. Pour les particuliers, ses logiciels gratuits offrent souvent des fonctions que l'on retrouve habituellement dans des utilitaires payants.

Glary Tracks Eraser va fouiller les entrailles de votre PC pour trouver et effacer à la demande des données qui peuvent compromettre votre identité et votre vie privée. Il s'agit par exemple de :

- L'historique de navigation sur le web ;
- Les fichiers temporaires ;
- Les cookies ;
- Les fichiers journaux (logs) ;
- Les entrées de registre inutiles ;
- Les fichiers récemment ouverts.

En effaçant ces données, Glary Tracks Eraser vise à protéger les informations personnelles des utilisateurs contre les regards indiscrets et les menaces potentielles telles que le vol d'identité et les atteintes à la vie privée. Il peut être utilisé à la fois à des fins préventives, pour maintenir la confidentialité au quotidien, et de manière réactive, après une session de travail ou de navigation pour effacer les traces d'activités.

MAIS C'EST QUOI EXACTEMENT LES FICHIERS TEMPORAIRES ?



Vous en entendez souvent parler sans savoir forcément de quoi il en retourne. Les fichiers temporaires, ou fichiers «temp», sont des fichiers créés par des programmes pour stocker temporairement des informations. Ils servent à optimiser le fonctionnement des logiciels et des systèmes d'exploitation en fournissant un espace de travail temporaire. Une fois leur utilité terminée, ils sont censés être supprimés automatiquement. Toutefois, il arrive souvent qu'ils restent sur le disque dur, occupant ainsi un espace précieux.

FONCTION DES FICHIERS TEMPORAIRES

- **Amélioration des performances** : Les fichiers temporaires permettent aux programmes de fonctionner plus efficacement. Par exemple, lors de l'installation d'un logiciel, des fichiers temporaires sont créés pour stocker des données intermédiaires nécessaires à l'installation.
- **Sauvegarde temporaire** : Lorsqu'un document est ouvert et en cours de modification, les logiciels créent des fichiers temporaires pour sauvegarder automatiquement les changements. Cela permet de prévenir la perte de données en cas de fermeture inopinée du programme ou de panne du système.
- **Gestion des caches** : Les navigateurs web créent des fichiers temporaires pour stocker des éléments de pages web visitées. Cela permet de charger les pages plus rapidement lors de visites ultérieures en récupérant les éléments depuis le cache plutôt que de les télécharger à nouveau.

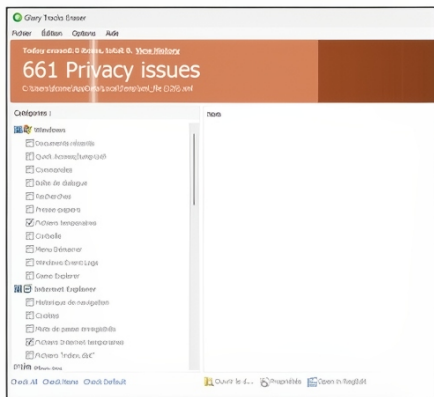
Lorsque les fichiers temporaires ne sont pas supprimés automatiquement, ils peuvent s'accumuler et occuper une quantité importante d'espace disque, ralentissant ainsi le système. Mais ils posent aussi un gros souci de confidentialité, car ils contiennent un grand nombre d'infos sur vos activités actuelles ou passées.



SCAN ET NETTOYAGE AVEC GLARY TRACKS ERASER

01 > SCAN AU DÉMARRAGE

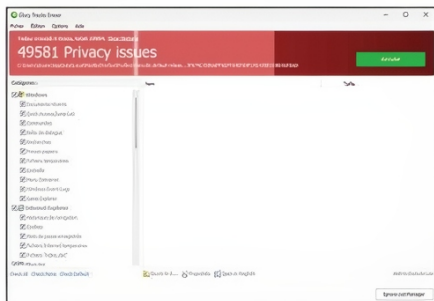
Lancez Glary Tracks Eraser. Le premier scan s'attaque par défaut aux fichiers temporaires que l'on peut supprimer sans risque pour le système ou



nos données. Le logiciel vous demandera de fermer les applications qu'il scanne (navigateur, client de messagerie, etc.) afin d'aller au bout de son process.

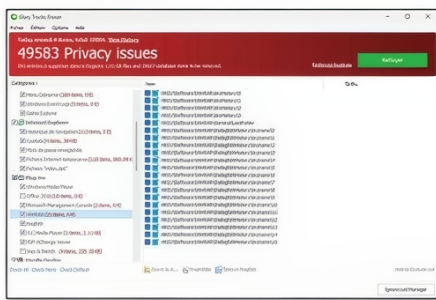
02 > AUTRES SCANS PRÉCONFIGURÉS

Si vous souhaitez vous attaquer à l'ensemble des traces laissées sur votre PC, vous pouvez cliquer sur **Check All** en bas à gauche de la fenêtre. Attention, vous risquez de supprimer des éléments de registre ou des cookies par exemple qui vous simplifieraient la vie jusqu'à présent. **Check None** vous permet de tout décocher. **Check Default** revient à la configuration de scan initiale.



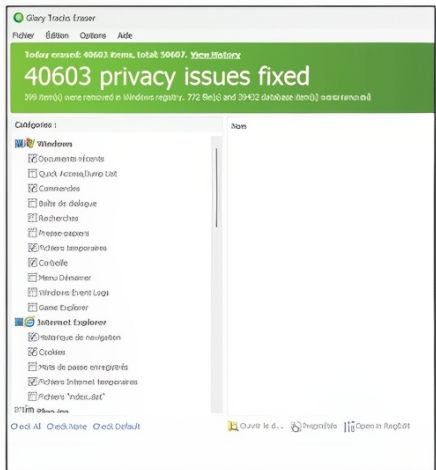
03 > OU SCAN MANUEL

Vous pouvez bien sûr effectuer votre choix manuellement en cochant et décochant les entrées qui vous semblent pertinentes. En cliquant dans la colonne de gauche sur l'un des Items, vous afficherez à droite plus d'infos sur ce qui sera supprimé par Glary Tracks Eraser. Cliquez sur **Relancer l'analyse** en haut à droite pour scanner précisément votre choix final.



04 > NETTOYAGE

Une fois ce scan effectué, vous pouvez cliquer sur **Nettoyer**. Glary Tracks Eraser vous liste en haut le résultat final de son action. Le lien **View History** vous permettra de revoir ce qui a été supprimé lors de vos précédents nettoyages.



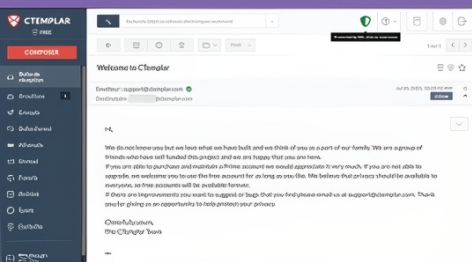


Passer à un email sécurisé

> AVEC C-TEMPLAR

C-Templar, en français, propose d'envoyer jusqu'à 200 messages au quotidien. Il fixe la limite des pièces jointes à 10 Mo dans la version gratuite et offre 1 Go d'espace de stockage. Basé en Islande, C-Templar est disponible à travers un navigateur Web ou une application pour Android et iOS. Il faut disposer d'une invitation pour s'inscrire (la demande peut s'effectuer directement depuis leur site Web).

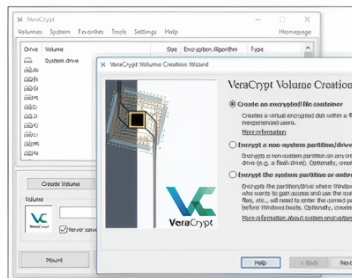
Lien : ctemplar.com



Chiffrer votre PC

> AVEC VERA-CRYPT

Logiciel open source en français, il offre un chiffrement de qualité professionnelle. VeraCrypt chiffre vos données, partitions de disque et même son chiffrement intégral. Il est compatible avec les périphériques de stockage externes.



Par contre, on notera son absence de partage ou d'intégration cloud.

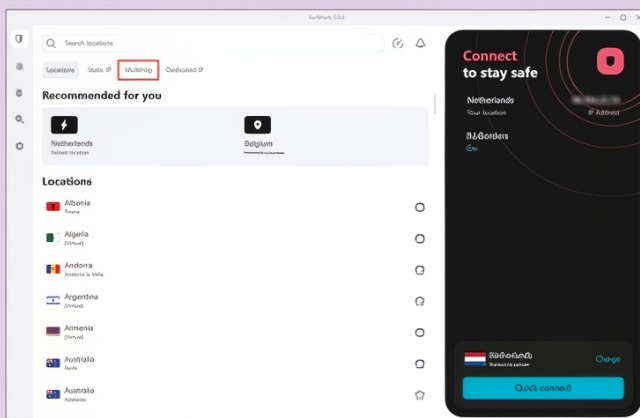
Lien : www.veracrypt.fr

Passer au Camouflage et au Multihop > AVEC SURFSHARK

Le «Camouflage Mode» et le «Multihop» de Surfshark sont deux fonctionnalités conçues pour améliorer la sécurité et l'anonymat des utilisateurs :

- **Camouflage Mode** : Cette fonction rend votre activité VPN indétectable même par votre fournisseur d'accès Internet (FAI). Il est utile dans les pays où l'utilisation des VPN est restreinte ou surveillée. Techniquement, il masque le fait que vous utilisez un protocole VPN en faisant paraître votre trafic comme du trafic Internet normal. Chez NordVPN, cette fonction s'appelle « Obfuscation ».

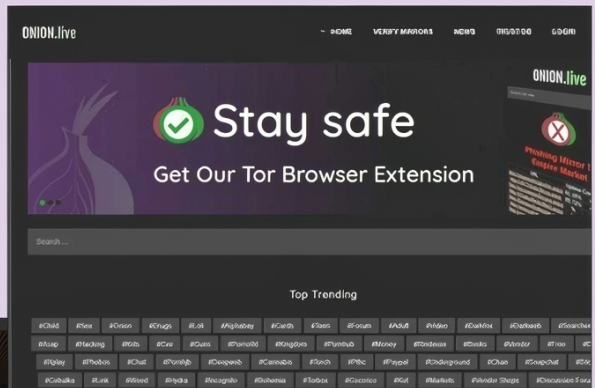
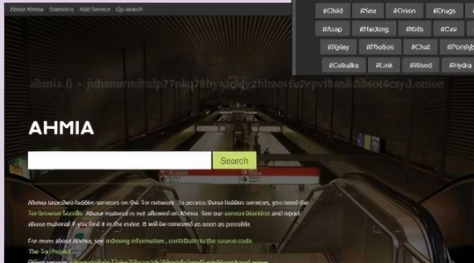
- **Multihop** : Il vous permet de vous connecter à Internet en faisant passer vos requêtes via deux serveurs VPN dans des pays différents au lieu d'un seul. Cette double connexion augmente la sécurité et l'anonymat, rendant beaucoup plus difficile pour quiconque de retracer votre activité en ligne. Chez NordVPN encore, il existe une fonction similaire : « Double VPN ».



Bien rechercher sur Tor

> AVEC ONIONLIVE

Les adresses .onion apparaissent et disparaissent régulièrement, tombent ou changent d'adresses sans prévenir ! Ce site accessible via un navigateur classique répertorie les .onion toujours valides et populaires. Vous pourrez donc les copier dans Tor pour ouvrir les services correspondants.

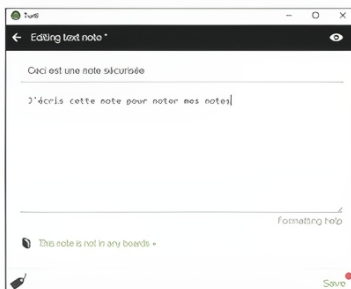


Onion.live publie un indice de confiance attribué par les utilisateurs. On y trouve beaucoup de dark markets et donc de sources souvent illégales, mais le moteur de recherche vous permet de cibler tout centre d'intérêt légitime. Il existe aussi des moteurs de recherche indexés manuellement et disponibles sur le darknet comme **Duckduckgo**, **Not Evil**, **Hidden Wiki**, **Candle** ou encore **Ahmia**.

Prendre des notes sécurisées

> AVEC TURL

De nombreux services et applications permettent de prendre des notes, stockées dans le Cloud. La particularité de Turlt, c'est que vos données sont chiffrées, donc illisibles tant pour d'éventuels

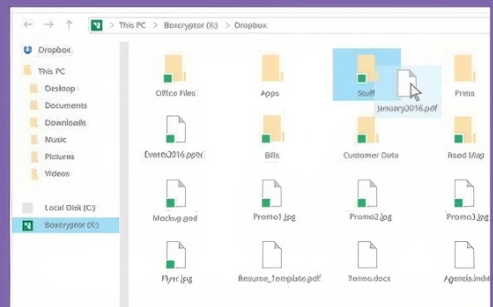


pirates que pour les propriétaires du service lui-même. Ce qui n'empêche pas le partage, sécurisé évidemment. Téléchargez et installez le logiciel client sur votre PC, et l'appli pour en profiter aussi sur votre téléphone Android.

Chiffrer votre cloud

> AVEC BOXCRYPTOR

Ce programme est spécialisé dans le chiffrement de bout en bout pour le stockage cloud. Il utilise un chiffrement AES 256 bits et RSA



et est compatible avec plus de 30 fournisseurs de stockage cloud dont Dropbox, Google Drive et Microsoft OneDrive. La version gratuite est restreinte à deux appareils et à un fournisseur cloud.

Lien : www.boxcryptor.com



PRENEZ LE CONTRÔLE DE VOTRE FACEBOOK AVEC SOCIAL FIXER



Avec Social Fixer, nettoyez et réorganisez Facebook selon vos véritables besoins et arrêtez d'être traité comme une vache à clics. À l'instar de F.B. Purity, que nous vous avons déjà présenté dans ces colonnes, Social Fixer est une extension pour navigateur (Chrome, Firefox, Opera...) qui vise à vous redonner le contrôle sur l'interface de votre page Facebook.



Social Fixer vise à améliorer l'expérience utilisateur sur Facebook en offrant une personnalisation avancée de l'interface et des options de filtrage pour un fil d'actualité plus propre et pertinent. Bien sûr, les nombreuses publicités et posts sponsorisés sont dans le collimateur. Social Fixer impressionne par le nombre de réglages et de filtres que vous pouvez appliquer pour retrouver un Facebook qui vous offre le meilleur sans vous inonder de déchets en permanence. Nous ne pouvons pas vous montrer l'ensemble de ces possibilités (il faudrait un magazine entier), mais nous pouvons néanmoins vous présenter un résumé des principales fonctionnalités de Social Fixer :

1) Filtrage de contenu

- Les utilisateurs peuvent créer des filtres basés sur des mots-clés, des auteurs, des types de publication, etc.
- Masquer automatiquement les jeux, les notifications d'applications, les événements, et autres contenus jugés inutiles.
- Élimination des publicités et des posts sponsorisés.

2) Personnalisation de l'interface

- Réorganiser ou masquer les sections de la barre latérale pour une interface plus propre.
- Changer les couleurs, la taille de la police, et d'autres aspects visuels de l'interface Facebook.
- Garder certains articles en haut du fil d'actualité pour ne pas les perdre de vue.

3) Amélioration de la navigation

- Forcer l'affichage des publications par ordre chronologique plutôt que par algorithme.
- Créer des onglets pour différents types de contenu (amis proches, groupes, pages) pour une meilleure organisation.
- Indiquer les publications déjà lues pour une navigation plus fluide.

4) Fonctionnalités de sécurité et de confidentialité

- Protection contre les scripts potentiellement nuisibles.
- Réduire la capacité de Facebook à suivre les activités en ligne des utilisateurs.

5) Utilitaires pratiques

- Recevoir des alertes pour les nouvelles publications des amis proches ou des pages favorites.
- Ajouter des fonctionnalités supplémentaires aux commentaires, comme le marquage de commentaires spécifiques ou la suppression des commentaires indésirables.

À SAVOIR



Social Fixer a été lancé par Matt Kruse en 2009, initialement sous le nom de "Better Facebook". Cette extension de navigateur est née de la frustration face à l'interface encombrée de Facebook et au manque de contrôle des utilisateurs sur leur fil d'actualité. Quinze ans plus tard, cette extension continue d'être mise à jour au fur et à mesure des évolutions de Facebook.



PREMIERS PAS AVEC SOCIAL FIXER

PRACTIQUE



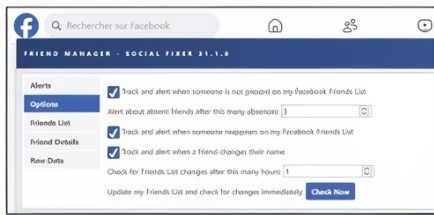
01 > INSTALLATION

En allant sur le magasin d'extensions de votre navigateur, trouvez et installez Social Fixer en l'ajoutant à vos extensions actives. Il s'intégrera automatiquement à Facebook la prochaine fois que vous ouvrirez votre page. Vous le retrouverez en haut à droite de celle-ci avec l'affichage de cette icône « Clé ». Cette icône peut être déplacée par glissement où vous le souhaitez sur votre page.



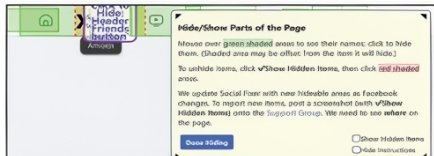
02 > FRIEND MANAGER

Via cette icône, vous pourrez accéder aux différentes listes de fonctions thématiques proposées par Social Fixer. Parmi celles-ci, le **Friend Manager** vous permet d'être alerté par exemple quand un ami ne s'est pas connecté depuis X jours, est réapparu ou a changé de nom.



03 > RÉGLAGES

Dans **Options > Social Fixer Options**, vous accédez à des dizaines de fonctions essentielles. Malgré l'interface en anglais, vous découvrirez chaque jour de nouvelles possibilités. Dans **General**, vous pouvez par exemple classer les posts par ordre chronologique, régler la taille de vos textes, bannir des posts contenant tel ou tel mot, ouvrir vos chats en pleine page plutôt que dans l'espace réduit qui leur est dédié, etc.

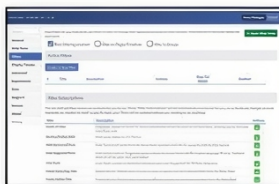


04 > FILTRER, C'EST CONTRÔLER !

Toujours dans **Social Fixer Options**, la catégorie **Filters** est l'une des plus importantes.

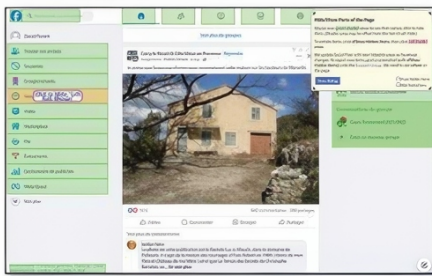
C'est là que vous pourrez décider de ce que vous voulez voir et de ce que vous voulez bloquer.

Par défaut, de nombreuses options sont activées par défaut, mais vous pourrez vraiment prendre le contrôle complet sur votre page. Attention, maîtriser cette partie demandera un peu de temps.



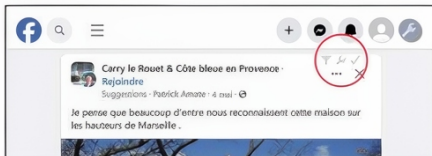
05 > MASQUER DES PANS ENTIERS DE FACEBOOK

Dans **Actions > Hide/Show parts of the page**, vous allez pouvoir personnaliser votre page en élevant dans la colonne de gauche et aussi dans le menu du haut les fonctions et boutons qui vous polluent. Faites le ménage, toutes les actions sont réversibles. Une fois votre choix fait par sélection, cliquez sur **Done Hiding** pour valider.



06 > SUR UN POST

Enfin, trois petites icônes en haut à droite de chaque poste s'afficheront quand vous passerez votre souris. Ils vous permettront d'interagir avec Social Fixer spécifiquement pour ce type de post, auteur, etc. pour ouvrir la partie **Filters**, les **Actions** ou le marqué comme **Read** (« Lu ») afin de le faire disparaître de votre fil.





DÉMARCHAGE TÉLÉPHONIQUE

**> LES NUMÉROS À SURVEILLER
+ COMMENT S'EN DÉBARRASSER ?**

Le démarchage téléphonique est une pratique courante utilisée par les entreprises pour promouvoir leurs produits ou services directement auprès des consommateurs. Pour beaucoup de Français, elle est synonyme d'intrusion et de désagréments. Quelles sont les mesures à adopter pour s'en prémunir ?

Chaque jour, de nombreux Français reçoivent des appels de numéros commençant par 09-48 ou 01-62. Ces appels, souvent liés à des offres de forfaits téléphoniques, de solutions énergétiques ou à la santé. Des entreprises plus ou moins respectables ont des choses à vous vendre et entendent vous convaincre en direct, sans filtre et avec des techniques de manipulation éprouvées. Utilisant à chaque fois des numéros différents, ces entreprises rendent difficile l'identification des appelants. Bien que des lois existent depuis 2020 pour encadrer cette pratique, de nombreux démarcheurs réussissent à contourner les règles, certains allant même jusqu'à organiser des arnaques.

CE QUE DIT LA LOI

Le démarchage téléphonique en France est encadré par la loi Naegelen de juillet 2020 et un décret d'octobre 2022, entré en vigueur en mars 2023. Ces textes précisent les heures et jours autorisés pour le

Beaucoup ne le savent pas, mais les démarcheurs sont obligés d'utiliser des numéros commençant par des séries de chiffres précis, ce qui aide à les repérer.

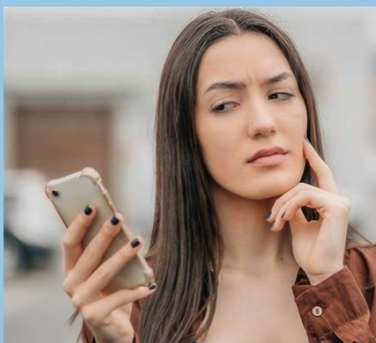


LES NUMÉROS D'APPEL DES DÉMARCHEURS SONT DÉSORMAIS CODIFIÉS, VOUS POUVEZ LES REPÉRER FACILEMENT. ET SI L'ON VOUS DÉMARCHE AVEC D'AUTRES NUMÉROS : ATTENTION, L'ARNAQUE EST GARANTIE AU BOUT DU FIL.

ATTENTION AU SPOOFING



Nous vous en parlions en détail dans notre numéro précédent. Les appels de démarchage utilisant des numéros 06 ou 07 peuvent cacher des escroqueries. Vous pouvez même recevoir un appel d'un numéro que vous connaissez (proche, banque, assurance, etc.) alors que c'est un escroc qui vous appelle en ayant réussi à usurper le numéro d'un tiers de confiance. Les fraudeurs utilisent une technique appelée spoofing pour usurper des numéros existants, souvent avec des logiciels comme IPBX. La loi Naegelen impose aux opérateurs de mettre en place un dispositif d'authentification pour vérifier l'authenticité des appels, sous peine de devoir bloquer ceux non certifiés. Malgré ces mesures, le spoofing reste une pratique courante pour les arnaqueurs, souvent opérant depuis l'étranger. Les entreprises, notamment les banques, ont renforcé leur sécurité et sensibilisent leurs clients. La Fédération bancaire française rappelle de ne jamais divulguer ses codes et mots de passe, même à sa banque : ces organismes n'ont jamais à vous les demander par appel ou SMS !





VOTRE NUMÉRO DE TÉLÉPHONE : POURQUOI IL VAUT DE L'OR



Les entreprises peuvent obtenir des numéros de téléphone à partir des bases de données publiques (c'est pourquoi il est essentiel de demander à votre opérateur votre désinscription de ces bases). Mais, et c'est aujourd'hui plus courant, on obtient aussi votre numéro via des bases de données commerciales (inscriptions en ligne, achats, formulaires, jeu-concours, programmes de fidélité, etc.). Car ne croyez pas qu'il faille hacker un site sur lequel vous avez enregistré votre numéro pour se l'accaparer ! De nombreuses sociétés (même parmi les plus connues) revendent leurs bases de données clients à des tiers, voire les aident à affiner votre profil.

UN NUMÉRO = UNE CIBLE

De nombreuses entreprises ou escrocs achètent ou louent ces bases de données de contacts auprès de courtiers en données (data brokers). Les numéros collectés sont souvent segmentés en fonction de critères démographiques et comportementaux afin de cibler les personnes les plus susceptibles d'être intéressées par les produits ou services proposés. Et plus qu'un email, le contact personnalisé par téléphone est plus efficace pour convaincre un potentiel acheteur (ou pigeon).

Les habitudes d'achat et les historiques de consommation sont analysés pour identifier les prospects les plus susceptibles de répondre favorablement à telle ou telle offre. Par exemple, une personne ayant récemment acheté un bien immobilier pourrait être ciblée pour des propositions de rénovation.

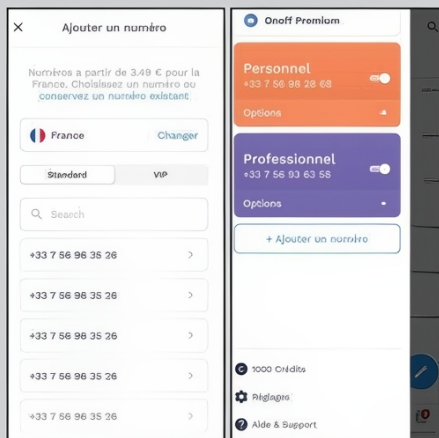
VOTRE NUMÉRO EST UNE DONNÉE ULTRASENSIBLE

La règle de base est de ne jamais utiliser son numéro de téléphone comme identifiant de compte. Cependant, nous savons tous que la plupart des sites commerciaux exigent votre numéro, notamment pour le commerce en ligne et l'abonnement à des services. Malheureusement, ce piège est inévitable... sauf à posséder un second numéro de téléphone qui sera découpé de vos services sensibles (banques, administrations, réseaux sociaux, achats, etc.). Mais cela a un coût... sauf si vous choisissez un opérateur qui vous offre gratuitement un second numéro VoIP.

OPTER POUR UN NUMÉRO VIRTUEL ?

L'utilisation de numéros virtuels est aussi une stratégie efficace pour protéger sa vie privée tout en restant accessible pour les interactions nécessaires. Comme les alias email, un numéro

virtuel vous permet de bénéficier d'un numéro permanent, temporaire ou jetable pour effectuer un certain nombre de démarches en toute sécurité. En France, des services comme Google Voice et TextNow ne sont pour l'instant pas pleinement opérationnels. Mais des alternatives comme Burner (numéros de téléphone temporaires pour des appels, des SMS et des messages vocaux) proposent une version d'essai gratuite bien que les fonctionnalités soient limitées (en termes d'usages ou dans le temps).



➡ **L'APPLICATION ONOFF VOUS PERMET D'OBTENIR UN SECOND NUMÉRO VIRTUEL POUR NE PAS DIVULGUER VOTRE NUMÉRO PRINCIPAL SUR LE WEB.**

Du côté des services payants, vous pouvez aussi vous tourner vers Hushed ou MySudo, pros et complets. À noter le petit frenchie OnOff, une autre application permettant d'obtenir des numéros virtuels pour des appels, des SMS et des messages vocaux. Ce service est également disponible sur abonnement mensuel (et peut être utilisé indépendamment de l'opérateur mobile principal). Sans carte SIM, mais finalement aussi cher (à partir de 4 € par mois).



démarchage : du lundi au vendredi, de 10h à 13h et de 14h à 20h. Le démarchage est interdit le soir, les week-ends et les jours fériés. De plus, les entreprises ne peuvent contacter une même personne plus de quatre fois par mois.

Pour les appels concernant les rénovations énergétiques, les règles sont encore plus strictes : tout démarchage téléphonique sur ce sujet est interdit. Les contrevenants risquent une amende de 75 000 euros, et jusqu'à 375 000 euros pour les personnes morales, selon l'article L. 242-16 du code de la consommation. Les appels publicitaires par automate ou messages préenregistrés sont autorisés uniquement si le consommateur a donné son accord explicite, par exemple en cochant une case sur le site Web de l'entreprise.

QUELS NUMÉROS À SURVEILLER ?

Depuis le 1er janvier 2023, les démarcheurs ne peuvent plus utiliser de numéros mobiles commençant par 06 ou 07. L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (Arcep) a attribué des séries de numéros spécifiques pour les professionnels du démarchage :

- En métropole : 01-62, 01-63, 02-70, 02-71, 03-77, 03-78, 04-24, 04-25, 05-68, 05-69, 09-48, 09-49.
- En outre-mer : 09475 (Guadeloupe, Saint-Martin, Saint-Barthélemy), 09476 (Guyane), 09477 (Martinique), 09478 et 09479 (Réunion, Mayotte).

Ces préfixes permettent aux consommateurs d'identifier facilement les appels de démarchage.

COMMENT BLOQUER LE DÉMARCHAGE ?

Le gouvernement a mis en place la plateforme Bloctel, déjà présentée dans nos colonnes. Ce service permet aux particuliers de s'inscrire gratuitement pour ne plus être contactés par des démarcheurs téléphoniques. Les entreprises doivent vérifier cette liste avant d'effectuer des appels. Les infractions peuvent entraîner des sanctions, comme ce fut le cas pour EDF et Canal+, condamnés par la CNIL pour non-respect des règles de prospection commerciale. Cependant, l'inscription sur Bloctel ne suffit pas toujours. Pour signaler les numéros frauduleux, les consommateurs peuvent utiliser le site J'alerte l'Arcep et envoyer les messages douteux par SMS au 33-700 dans le cadre de la lutte antispam.

À SAVOIR

De nombreux services utilisent l'authentification à deux facteurs (2FA) par SMS pour sécuriser les comptes. Si votre numéro de téléphone est compromis, les attaquants peuvent potentiellement accéder à ces comptes en interceptant les codes de vérification envoyés par SMS.



TOP 5 LOGICIELS GRATUITS POUR VOS CLÉS USB

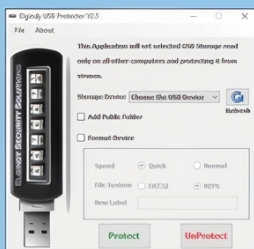
Pour protéger vos supports USB ou les utiliser pour accroître votre sécurité, voici cinq petits utilitaires simples mais efficaces.

ELGINDY USB PROTECTOR

> EMPÊCHEZ TOUTE MODIFICATION

L'une des craintes quand vous stockez des fichiers importants sur un support USB, c'est que quelqu'un les supprime ou les modifie volontairement ou par inadvertance. Elgindy USB Protector est un petit utilitaire simple et efficace qui vous évitera ce type de déconvenues. Ce freeware configure la clé USB pour n'être modifiable que sur votre ordinateur. Sur tout autre terminal, elle sera en mode « read only », c'est-à-dire que son contenu peut être affiché, mais pas modifié et encore moins supprimé. Au-delà de la sécurisation de vos fichiers, c'est aussi une protection contre l'ajout de malware sur vos supports externes. Vous pouvez bien sûr revenir à la configuration initiale à tout moment et même créer un dossier public qui lui sera accessible sans restriction à côté de vos fichiers et dossiers protégés. Disponible en anglais et en arabe.

Lien : gsmcommunications.blogspot.com



PREDATOR

> JE VERROUILLE, JE DÉVERROUILLE

Predator transforme une clé USB en une clé de sécurité pour votre PC. Lorsque la clé USB est retirée, l'ordinateur se verrouille automatiquement, empêchant tout accès non autorisé (l'écran devient noir et le clavier et la souris ne répondent plus). Ce logiciel est particulièrement utile pour les utilisateurs qui travaillent dans des environnements partagés ou sensibles. Vous pouvez même configurer une alarme sonore en cas de tentative d'accès non autorisé. Un journal d'activité est également enregistré pour vous dire si quelqu'un a utilisé ou tenté d'utiliser votre PC en votre absence. Predator va configurer la clé USB de votre choix et vous pourrez définir un mot de passe (au cas où quelqu'un subtilise votre clé !). Connectez la clé USB pour déverrouiller le PC, rebranchez-la quand vous quittez votre poste. Si vous perdez votre clé USB, appuyez 3 fois sur Entrée lorsque l'écran devient noir, votre mot de passe de secours vous sera demandé et vous pourrez reconfigurer une nouvelle clé USB.

Lien : predator.fr.softonic.com



USB DRIVE DISABLEL > PROTÉGEZ-VOUS... DES CLÉS USB !

Encore un logiciel qui ne fait qu'une seule chose, mais qui le fait bien ! Cette fois-ci, l'objectif est d'empêcher les clés USB de se connecter à votre PC. Vous éviterez ainsi qu'une personne malintentionnée n'infecte votre terminal ou n'aspire vos données en local. USB Drive Disabler permet d'empêcher les clés USB de se connecter à votre machine, sans pour autant limiter l'accès de votre souris, de votre webcam ou de tout autre appareil connecté en USB. Il s'agit donc d'une désactivation sélective des ports USB afin de ne pas transformer votre PC en brique amorphe et inutile. USB Drive Disabler ne nécessite aucune installation et offre seulement deux options à cocher : activer ou désactiver les pilotes USB. En revanche, il faudra redémarrer le PC à chaque fois que vous optez pour une option ou une autre.

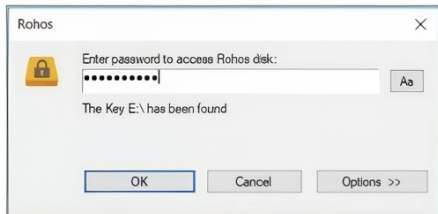
Lien : usb-drive-disable.fr.softonic.com



ROHOS MINI DRIVE

> CHIFFREZ DOSSIERS ET FICHIERS

Rohos Mini Drive est destiné à ceux qui souhaitent sécuriser des fichiers sensibles sur une clé USB en créant une partition chiffrée. Ce logiciel est idéal pour les professionnels qui transportent des informations confidentielles, garantissant que les données restent protégées même en cas de perte ou de vol du périphérique. Le chiffrement est en AES 256 bits et la partition chiffrée sur votre support USB est cachée. C'est-à-dire qu'en cas de vol, on se saura pas quoi chercher et cracker sans une analyse plus approfondie. Vous avez juste besoin de fournir



un mot de passe pour y accéder. En un seul clic, vous pouvez enregistrer votre premier fichier dans un volume protégé. Le chiffrement est automatique et à la volée pour les suivants. Dans les options, choisissez d'utiliser Rohos sans droits d'administrateur, ce qui vous permettra d'accéder aux données chiffrées sur n'importe quel ordinateur. La version gratuite est limitée à 2 Go de partition sécurisée.

Lien : rohos.com

USBFX > VACCINEZ VOS CLÉS USB !

USBFix est conçu pour détecter et éliminer les logiciels malveillants présents sur les périphériques USB. Les virus USB créent souvent des raccourcis malveillants pour tromper les utilisateurs. USBFix les identifie et les supprime, rétablissant l'accès normal aux fichiers. Le logiciel permet aussi de vacciner de façon préventive



vos périphériques contre les futures infections en créant une immunité virtuelle contre les virus connus. Il offre aussi la possibilité de sauvegarder les fichiers importants avant de procéder à une suppression, garantissant que vos données restent intactes en cas d'infection. Après chaque analyse, USBFix génère un rapport détaillé des actions effectuées, des fichiers supprimés et des menaces détectées. Le programme est facile à utiliser, même pour les utilisateurs non techniques, grâce à son interface intuitive et ses instructions claires. Bien que la version gratuite soit efficace, certaines fonctionnalités avancées ne sont disponibles que dans la version payante du logiciel.

Lien : www.sosvirus.net

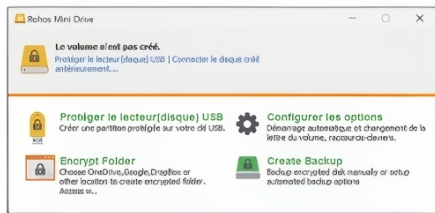


PREMIÈRE CONFIGURATION DE VOTRE VOLUME CHIFFRÉ

PRATIQUE

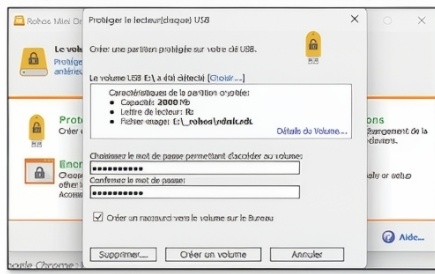
01> INSTALLATION

Depuis le site de Rohos, téléchargez et installez en français le programme depuis **Téléchargement de la configuration**. Ouvrez Rohos Mini Drive, vous êtes prêt à configurer votre première clé USB.



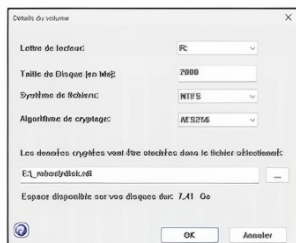
02> VOTRE CLÉ

Insérez votre support externe USB. Revenez sur l'interface de Rohos puis cliquez sur **Protéger le lecteur(disque) USB**. Si vous n'avez qu'une unité connectée, Rohos la sélectionnera automatiquement par défaut. Si vous en possédez plusieurs, à vous de choisir celle que vous voulez configurer. Vous devrez d'abord définir votre mot de passe.



03> ESPACE CHIFFRÉ

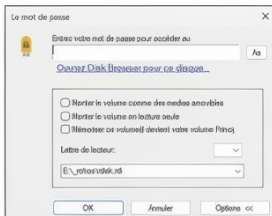
Via **Détails**, vous pouvez définir l'espace qui sera alloué à votre partition protégée. Dans la version gratuite de Rohos Mini Drive, cet espace est de 2 Go. Une fois défini,



cliquez sur **Ok** puis sur **Créer un volume** dans la fenêtre principale. Rohos s'occupe de créer le volume crypté demandé. Cela peut prendre quelques dizaines de secondes.

04> ACCÉDER À VOTRE VOLUME

Une fois le volume créé, vous devrez cliquer sur l'icône Rohos Mini.exe sur votre clé USB pour y accéder. Votre mot de passe vous est alors demandé pour voir et interagir avec ce que contient votre volume. Si vous travaillez sur votre PC, pas de souci, mais si vous ouvrez ce volume sur un autre terminal, vous devrez disposer des droits d'administrateur.



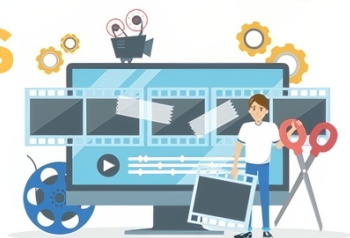
05> INTERFACE DE GESTION PORTABLE

L'option **Ouvrez Disk Browser pour ce disque** vous permet d'utiliser la version portable de Rohos Mini Drive sur n'importe quel PC sans droit d'administrateur. Et vous aurez besoin, bien sûr, de votre mot de passe. Cette interface permet également de créer des conteneurs de disques virtuels et des conteneurs cryptés cachés.





MONTEZ vos FILMS AVEC SHOTCUT



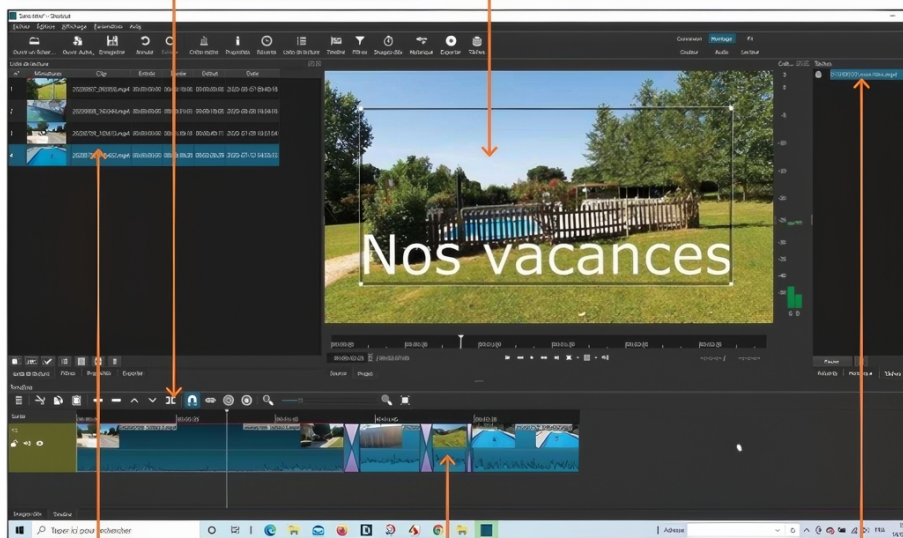
Les logiciels de montage vidéo proposent une interface assez standard, avec d'un côté les éléments du montage, de l'autre une Timeline sur laquelle vous disposez ces éléments, et bien sûr une fenêtre de visualisation pour apprécier le résultat. Zoom sur l'interface de Shotcut.

Outils d'édition

Pour scinder un clip en deux morceaux, supprimer des éléments ou en ajouter, insérer des séquences, la barre d'outils rassemble toutes les fonctions d'édition.

Volet de prévisualisation

Ici s'affiche le clip en cours d'édition. Il permet d'apprécier les titres ou les transitions appliquées. Au-dessous figurent tous les boutons nécessaires pour faire défiler la vidéo.



Éléments du montage

C'est dans ce volet que vous piochez les éléments nécessaires à la fabrication de votre film. Son contenu s'adapte selon les circonstances, pour présenter la liste des clips vidéo, des transitions, des modèles de titres, etc.

Timeline

Élément central du logiciel, elle accueille les clips vidéo qui constituent le film. Elle affiche également la bande son (une musique ou une voix off).

Historique

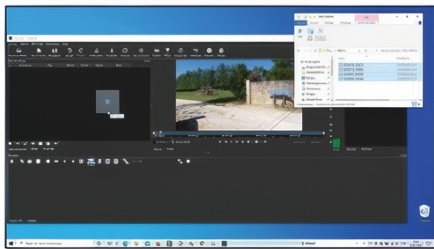
Après avoir cliqué sur le bouton Historique, sont listées dans ce cadre toutes les opérations réalisées. Il est donc facile de revenir en arrière en cas d'erreur.



EFFECTUER LE MONTAGE

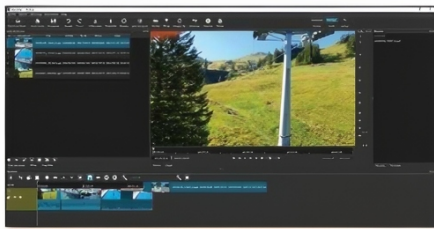
01 > IMPORTER LES VIDÉOS

Lancez Shotcut. Depuis l'Explorateur de fichiers, ouvrez le dossier contenant vos vidéos et sélectionnez-les toutes. Faites-les glisser dans le volet gauche **Liste de lecture** de Shotcut. Stoppez la lecture automatique en cliquant sur **Pause** dans le volet central.



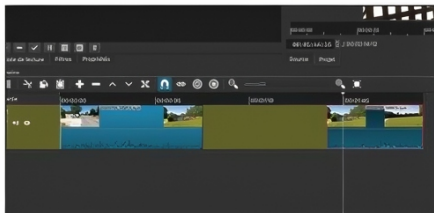
02 > ORGANISER LA TIMELINE

Faites glisser la première vidéo de votre film depuis le volet **Liste de lecture** vers le volet **Timeline** au bas de l'interface. Il occupe maintenant une piste vidéo. Ajoutez les autres séquences de la même façon, les unes derrière les autres.



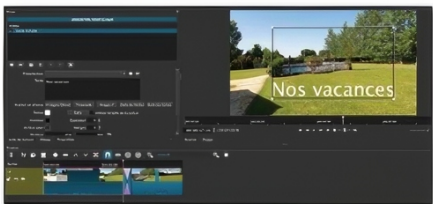
03 > DÉCOUPER UN CLIP

Cliquez sur le clip à couper puis déplacez la tête de lecture sur la Timeline à l'endroit souhaité. Cliquez sur l'icône **Découper** à gauche de l'aimant. Vous pouvez maintenant faire glisser la seconde moitié du clip et placer une autre séquence entre les deux.



04 > AJOUTER UN TITRE

Sélectionnez le clip où ajouter un titre, dans la Timeline. Cliquez sur le bouton **Filtres** puis + au-dessus. Activez l'onglet **Vidéo** et optez pour **Texte simple**. Remplacez **#timecode#** par votre texte. Ajustez sa taille et son emplacement grâce aux poignées dans la fenêtre de prévisualisation. sentes dans votre ancien navigateur si vous le souhaitez.



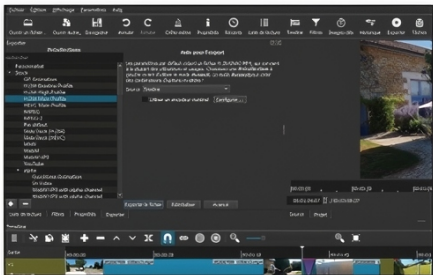
05 > APPLIQUER UNE TRANSITION

Sur la Timeline, faites se chevaucher deux clips. Une transition est automatiquement ajoutée. Effectuez un clic droit dessus et choisissez **Propriétés**. Cliquez sur le menu déroulant **Vidéo** pour définir une transition. Appréciez l'effet en cliquant sur **Play**.



06 > « EXPORTER LA VIDÉO

Votre montage vous convient ? Cliquez sur le bouton **Exporter**, en haut de la fenêtre. Choisissez le format vidéo souhaité dans la liste **Présélection** (**H.264 Main profile** dans notre exemple) et cliquez sur le bouton **Exporter**. Donnez un nom au fichier et définissez son emplacement.





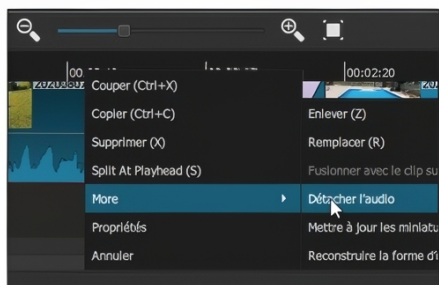
GÉRER LES PISTES AUDIO

PRATIQUE


Vous ne souhaitez pas conserver le son original de vos vidéos, ou vous voulez ajouter une musique ? Quelques clics suffisent.

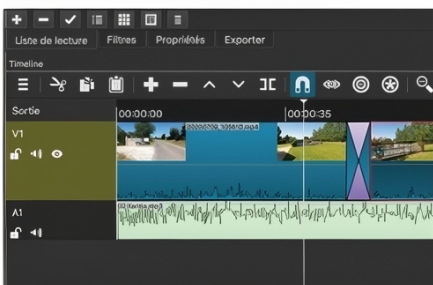
01 > COUPER LE SON

Dans la Timeline, effectuez un clic droit sur le clip à rendre muet. Choisissez **More** puis **Détacher l'audio**. Cliquez ensuite sur le bouton en forme de haut-parleur dans la cadre vert à gauche. L'audio est coupé pour ce clip.



02 > AJOUTER DE LA MUSIQUE

Effectuez un clic droit dans une zone vierge de la Timeline, sous les clips présents, et choisissez **Track Operations** puis **Ajouter une piste audio**. Sélectionnez votre morceau de musique depuis l'Explorateur de fichiers de Windows, et glissez-le sur la nouvelle piste.



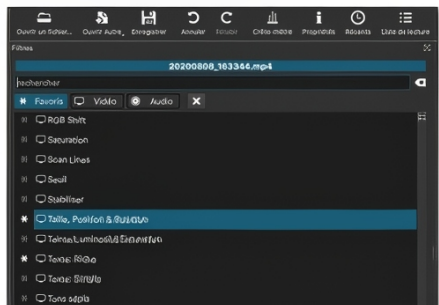
RECADRER UNE SÉQUENCE

PRATIQUE


Vous souhaitez améliorer le cadrage, ou couper un élément indésirable, comme un doigt sur une partie de l'objectif ? Voici comment procéder.

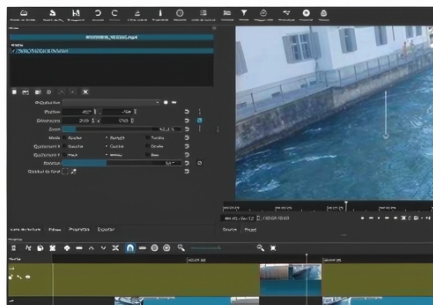
01 > ACCÉDER À LA FONCTION

Sélectionnez le clip à recadrer dans la Timeline. Cliquez sur le bouton **Filtres** puis sur le bouton **+** au-dessus. Dans le volet qui s'affiche, activez l'onglet **Vidéo**. Dans la liste des filtres, choisissez **Taille, position et rotation** afin d'accéder aux réglages.



02 > APPLIQUER UN ZOOM

Déplacez le curseur **Zoom** vers la droite afin que s'opère un zoom dans l'image jusqu'à obtenir le cadrage souhaité. Déplacez au besoin le **vecteur** au centre de l'image de prévisualisation pour appliquer le zoom sur une zone particulière.



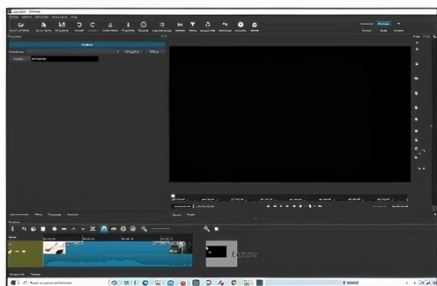


GÉRER LES PISTES AUDIO

Pour donner une touche professionnelle à votre film, vous pouvez ajouter un générique de fin sur fond noir.

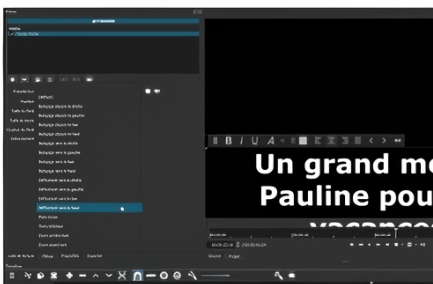
01 > PRÉPARER LA PISTE VIDÉO

Cliquez sur le menu **Ouvrir autre** en haut de la fenêtre et choisissez **Couleur**. Dans la fenêtre qui s'affiche, activez le menu déroulant **Présélection** et optez pour **Black**. Glissez le contenu de la fenêtre de prévisualisation à la fin de votre montage.



02 > AJOUTER LE GÉNÉRIQUE

Cliquez sur **Filtres** puis le bouton **+** au-dessus. Dans l'onglet **Vidéo**, choisissez **Texte riche**. Rédigez le texte de votre générique dans le cadre de prévisualisation. Activez le menu déroulant **Présélection** et optez pour **Défilement vers le haut**. Votre générique est prêt.

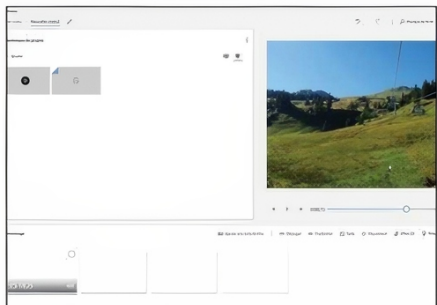


INCRUSTER DES ÉLÉMENTS 3D

L'application Photos, l'outil d'édition d'images et de vidéos de Windows 10, recèle quelques pépites. Il permet par exemple d'ajouter des objets 3D à vos vidéos.

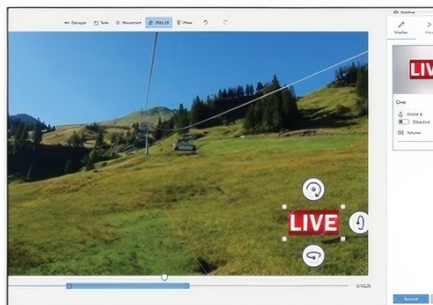
01 > ACCÉDER AUX EFFETS

Depuis l'appli Photos, activez **Nouvelle vidéo** en haut à droite puis **Nouveau projet vidéo** et nommez le projet. Cliquez sur le bouton **Ajouter** et sélectionnez votre séquence vidéo. Glissez-la ensuite dans la zone **Scénarimage**. Cliquez sur le menu **Effets 3D** sous le cadre de prévisualisation.



02 > AJOUTER L'ÉLÉMENT 3D

Dans le volet de droite, cliquez sur **Effets** et choisissez celui qui vous convient. Déplacez le module dans l'image et redimensionnez-le au besoin à l'aide des poignées. Lancez la lecture pour apprécier le résultat. Validez par **Terminer** lorsque vous êtes satisfait.



Comme dans une série américaine, le papier peut revenir pendant plusieurs saisons.

La force de tous les papiers, c'est de pouvoir être recyclés
au moins cinq fois en papier. Cela dépend de chacun de nous.
www.recyclons-les-papiers.fr

Tous les papiers ont droit à plusieurs vies.
Trions mieux, pour recycler plus !

Votre publication s'engage pour
le recyclage des papiers avec Ecofolio.





MOTO TAG : LA GÉOLOCALISATION CHANGE D'ÉCHELLE

MOTOROLA A RÉCEMMENT LANCÉ LE MOTO TAG, UN PETIT TRACKER SANS GPS MAIS DOPÉ À LA TECHNOLOGIE ULTRA WIDEBAND (UWB). ASSOCIÉ AU RÉSEAU FIND MY DEVICE DE GOOGLE (« GOOGLE LOCALISER MON APPAREIL » EN FRANÇAIS), IL PROMET UNE LOCALISATION ULTRAPRÉCISE TOUT EN ASSURANT UNE AUTONOMIE D'UN AN. ET IL PEUT MÊME SERVIR DE COMMANDE POUR VOTRE SMARTPHONE.



Est-ce bientôt la fin des balises GPS ? Cette technologie de géolocalisation est en tout cas délaissée par quelques grands noms du secteur au profit du Bluetooth... et de l'UWB (Ultra Wideband), dont nous vous parlerons un peu plus loin. Le Moto Tag de Motorola vient de sortir en Europe, pour moins de 40 euros, et il contient déjà toutes les fonctionnalités qui seront les standards de demain. Comme indiqué, il n'intègre pas de balise GPS, ce qui lui permet d'offrir un format compact et ultraléger (7,5 g). Mais comment fait-il alors pour localiser une personne ou un produit associé ?



UNE PRÉSENTATION SOIGNÉE AVEC CE PORTE-CLÉS ET UN POIDS PLUME POUR LE TAG EN LUI-MÊME : SEULEMENT 7,5 GRAMMES.



DEUX COULEURS DISPONIBLES POUR CE TOUT NOUVEAU CONCURRENT DE L'AIRTAG.

Prix : 1 Moto Tag : 39 € Pack 4 Moto Tags : 139 €

Où le trouver ? www.motorola.fr

CARACTÉRISTIQUES

Couleurs disponibles : Marine et Vert jade

Dimensions : 31,9 x 8 mm

Poids : 7,5 g

Autonomie de la batterie : Jusqu'à un an

Compatibilité : Android 9.0 ou supérieur

Capteurs : Ultra Wideband ; Bluetooth Low Energy

Connectivité : Bluetooth 5.4

Portée Bluetooth Low Energy : Jusqu'à 100 mètres

Alerte sonore : 75 dB à 10 cm

Batterie : Pile remplaçable CR2035 (fournie)

Résistance à l'eau : IP67

DES MILLIARDS DE
SMARTPHONES (ANDROID ET
APPLE) CRÉENT LE PLUS VASTE
RÉSEAU MESH AU MONDE
POUR LOCALISER LE MOTO TAG
DÈS QU'IL PASSE À PROXIMITÉ
DE L'UN D'ENTRE EUX ET QUE
SON BLUETOOTH EST ACTIVÉ



INTÉGRATION AU RÉSEAU FIND MY DEVICE

En attachant le Moto Tag à un objet, à un vélo ou à votre animal de compagnie, vous pouvez facilement suivre sa localisation via l'application Find My Device de Google, enfin étendue au territoire européen cette année. Ce réseau est tissé par tous les appareils Android compatibles. Il s'appuie sur la communication automatique



entre eux via Bluetooth si ce dernier est activé (le Bluetooth fonctionne très bien pour une distance inférieure à 10 mètres et correctement jusqu'à plusieurs dizaines de mètres selon l'environnement). Du coup, si votre Moto Tag passe à côté d'un terminal Android au coin de la rue ou à l'autre bout de l'Espagne, hop, il est localisé anonymement puis l'info est rapatriée en direct sur votre compte Google. Vous pouvez savoir où il est et le suivre à distance.

SUIVRE À LA TRACE SUR SMARTPHONE

Le réseau Find My Device prend en charge les appareils Android fonctionnant sous la version 9 et supérieures et est également compatible avec iOS pour certaines fonctionnalités telles que les alertes de trackers inconnus (lire ci-contre). Vous pouvez gérer les paramètres du tracker, ajuster le niveau de volume et surveiller sa batterie sur l'application Find My Device et sur l'application maison, baptisée tout simplement Moto Tag. L'emplacement du tracker n'est accessible qu'au propriétaire et qu'aux contacts avec lesquels il a été partagé, toujours par le biais de l'application Find My Device. Un ensemble de fonctionnalités et de compatibilités qui font du Moto Tag la nouvelle référence de l'écosystème Android.



STALKING : LA MENACE DES TAGS

La miniaturisation des balises et la multiplication de tags hyper précis et si simples à configurer inquiètent aussi. Et si vous étiez pistés à votre insu par un proche, un employeur ou... par n'importe qui d'un peu inquiétant en fait ? Êtes-vous sûr de ne pas avoir un AirTag ou un Moto Tag glissé dans votre sac ou dans le coffre de votre voiture ?



UN TAG INCONNU VOUS SUIV À LA TRACE ? RECEVEZ UNE ALERTE SUR VOTRE SMARTPHONE.

Pour éviter les dérives du « stalking », les fabricants ont compris qu'il fallait mettre en place un protocole de sécurité supplémentaire. Apple et Google, les deux géants qui fournissent les réseaux permettant ce maillage si performant des « tags », ont développé un standard commun : Le Detecting Unwanted Location Tracker. Cette fonctionnalité, bien sûr intégrée au Moto Tag, envoie une alerte à un smartphone Android ou iOS si la présence d'un tag inconnu est régulièrement détectée à proximité de l'appareil. Et, comme nous l'avons déjà précisé ci-contre, toutes les données de localisation sont chiffrées de bout en bout, garantissant que seules les personnes autorisées peuvent accéder aux informations de suivi.



L'UTILISATION DU RÉSEAU UWB SE FAIT À TRÈS BASSE CONSOMMATION D'ÉNERGIE. UNE SIMPLE PILE CONFÈRE UNE AUTONOMIE DE UN AN AU MOTO TAG.



COMME LES AIRTAGS D'APPLE... AVEC L'INTÉGRATION DU NOUVEAU RÉSEAU UWB POUR UNE PRÉCISION QUI POURRA ATTEINDRE QUELQUES CENTIMÈTRES SEULEMENT...

Même si le prix est un peu élevé, c'est en tout cas l'objectif, car Motorola dévoile sa deuxième arme : L'Ultra Wideband (UWB). Cette technologie de communication sans fil utilise une large bande de fréquences pour transmettre des données sur de courtes distances avec une grande précision. Contrairement aux technologies sans fil traditionnelles comme le Bluetooth ou le Wi-Fi, qui utilisent des bandes de fréquences étroites, l'UWB émet des impulsions à large spectre, ce qui permet une transmission rapide de données avec une faible consommation d'énergie. L'autonomie annoncée du Moto Tag est ainsi de un an, avec une pile CR2032 remplaçable.

PIONNIER EN ATTENTE DE RÉSEAU

Comme pour la localisation par Bluetooth, la localisation par UWB repose sur un maillage de terminaux compatibles. Et c'est pour l'instant là que le bât blesse. L'UWB n'est compatible qu'avec les appareils dotés de puces UWB, et cela ne concerne que quelques smartphones récents. Dont bien sûr les flagships de

Apple, Google et Samsung. Mais il faudra attendre sa généralisation pour que ce nouveau réseau sans fil tienne toutes ses promesses. Elles sont pourtant nombreuses : faible consommation, nous l'avons dit, précision de quelques centimètres en situation idéale, transfert de données à haute vitesse et contrôle de proximité avec des appareils compatibles (smartphones ou objets connectés). L'UWB utilise enfin des signaux à large bande qui sont difficiles à intercepter, offrant ainsi une couche supplémentaire de sécurité pour les transmissions de données.

ET IL SERT DE TÉLÉCOMMANDE !

En parlant de commande, le Moto Tag est d'ailleurs doté d'un bouton multifonctionnel permettant aux utilisateurs de faire sonner leur smartphone pour le retrouver rapidement. Il peut même être utilisé comme télécommande pour prendre des photos. Côté techno embarquée, on notera enfin que les communications se feront avec chiffrement de bout en bout (bravo !) et que la balise de Motorola est compatible avec le Fast Pair de Google (connexion par notification et automatique pour les appareils possédant le même compte Google). Cependant, il manque encore certaines fonctionnalités comme le mode antivol, que des concurrents comme Tile mettent en avant comme essentielles. Cela pourrait freiner les utilisateurs recherchant des solutions de sécurité complètes.



LE BOUTON DE FAÇADE PERMET DE COMMUNIQUER AVEC LE SMARTPHONE, LUI DEMANDANT DE SONNER PAR EXEMPLE POUR LE TROUVER OU DE PRENDRE UNE PHOTO.





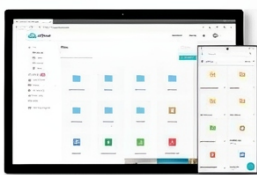
TOP 15

TOP 5 CLOUDS GRATUITS

PCLOUD > LA STAR DU MOMENT

2 Go gratuits tout de suite et 10 Go rapidement sous forme de récompenses ludiques. Basée en Suisse (et donc protégée par la loi helvétique), pCloud se veut la solution de stockage en ligne « la plus sécurisée d'Europe ». Via votre navigateur, un espace virtuel dédié sur votre PC ou une application mobile : accédez facilement à tous vos fichiers et dossiers, avec les mêmes fonctionnalités que les versions premium, ce qui est assez rare.

Lien : www.pcloud.com



KDRIVE > 3 Go MAIS COMPLET !



Comme pCloud, la suisse kDrive stocke vos fichiers au sein d'un espace hautement sécurisé, les synchronise entre tous vos appareils et vous permet le transfert et partage rapide. Son interface agréable et sa solution de bureautique et

de travail collaboratif intégrée en font une valeur sûre et séduisante. Côté capacité, on se contentera de seulement 3 Go dans la version gratuite.

Lien : www.infomaniak.com/fr/kdrive

Logiciels & services GRATUITS

ICEDRIVE > LE CHALLENGER

Relativement récent sur le marché (2019), IceDrive continue de séduire et de grignoter les mollets de ces petits concurrents. Avec une offre généreuse (10 Go), il surprend surtout par le côté innovant et ergonomique de ses interfaces et services. Présenté comme ultra-sécurisé et chiffré de bout en bout, tout semble intuitif et transparent en termes d'usage.

Lien : icedrive.net



GOOGLE DRIVE > LE PLUS PUISSANT, MAIS...

Il est le meilleur. Voilà, c'est comme ça. 15 Go gratuits, sécurisation de vos données, une suite bureautique et des possibilités de travail collaboratif sans égales en version gratuite : le drive de Google est la référence. Mais cela a un prix : la synchronisation de vos données avec les autres services

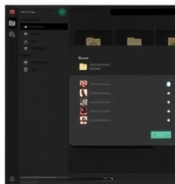
Google. Heureusement, les plus courageux peuvent limiter cette intrusion via les réglages.

Lien : drive.google.com

MEGA > 20 Go OFFERT

C'est le plus généreux des services de cloud reconnus. 20 Go de stockage offerts dans la version gratuite, voilà de quoi réjouir l'internaute. Mais voici le seul point fort de Mega. Outre son aura sulfureuse, les services et vitesses de transferts sont moyens. À choisir si vous avez besoin de stockage sans transferts et partages trop réguliers.

Lien : mega.io

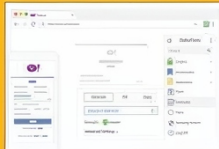


TOP 5 GESTIONNAIRES DE MOTS DE PASSE

ROBOFORM > LES ROBOTS SONT ÉTERNELS

Le plus populaire des gestionnaires dans les années 2000... et toujours l'une des valeurs sûres. Bravo, une telle longévité mérite le respect et est surtout le gage d'une assurance tous risques. Sa version gratuite enregistre, remplit les formulaires, vérifie et génère de nouveaux mots de passe. Simple et efficace.

Lien : www.roboform.com

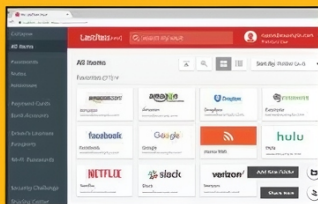


LASTPASS > LE + POPULAIRE

LastPass retient l'ensemble des mots de passe qui vous sont utiles au quotidien pour les sites que vous avez l'habitude d'utiliser.

Il propose également un outil permettant de remplir automatiquement les formulaires avec vos données personnelles (nom, prénom, adresse...).

Lien : www.lastpass.com/fr



TOP5 MEDIA CENTERS

KODI > ULTRA-PUISSANT



Kodi est un logiciel open source est connu pour sa flexibilité et sa personnalisation, avec de nombreux add-ons et skins disponibles. Il est compatible avec une large gamme

de plateformes, y compris les ordinateurs, les appareils mobiles, les téléviseurs intelligents et les boîtiers de streaming.

Lien : kodi.tv

PLEX > L'ERGONOMIE EN PLUS

Plex permet lui aussi de diffuser du contenu multimédia sur différents appareils, y compris les téléviseurs intelligents, les ordinateurs et les smartphones. Il offre également des fonctionnalités de sauvegarde et de synchronisation, ainsi que des options pour gérer et organiser votre bibliothèque multimédia. Plex est reconnu pour sa facilité d'utilisation et son interface utilisateur intuitive.

Lien : www.plex.tv



EMBY > L'EXPÉRIENCE MULTI-UTILISATEURS

Emby, moins populaire, offre cependant des fonctionnalités proches de ses concurrents. Il est apprécié pour sa prise en charge de plusieurs utilisateurs, ainsi que pour ses fonctionnalités de transcodage en temps réel pour une meilleure compatibilité avec différents appareils.

Lien : emby.media



MEDIAPORTAL > TOUT-TERRAIN POUR LA TV



MediaPortal est apprécié pour sa prise en charge de la télévision en direct et de l'enregistrement de programmes TV, son intégration de services de streaming et une interface

utilisateur personnalisable avec une grande variété de plug-ins et d'extensions.

Lien : www.team-mediaportal.com

LIBREELEC > LINUX ET RASPBERRY PI

LibreELEC est une distribution Linux légère liée à la team Kodi, qui peut être installée sur un Raspberry Pi ou un PC. Elle est connue pour sa facilité d'installation et d'utilisation.

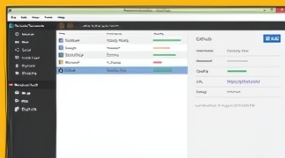
Lien : libreelec.tv



KEEPASS > L'USINE BLINDÉE

Mais qu'est-ce qu'il est moche ! Oui, mais ce qui compte c'est la sécurité intérieure ! Avec sa certification délivrée par l'Autorité Nationale de Sécurité Informatique, KeePass est même recommandé par l'état français. Et si on vous dit qu'il est entièrement gratuit...

Lien : keepass.fr

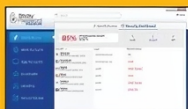


STICKY PASSWORD > BIOMÉTRIE INTÉGRÉE

Basé sur un chiffrement AES-256, nous avons surtout remarqué la prise

en charge par Sticky Password de la biométrie. Cela signifie que si vous verrouillez votre smartphone par empreinte digitale, StickyPassword suivra le mouvement ! La version gratuite est complète, hormis une offre Cloud réservée aux membres Premium.

Lien : www.stickypassword.com

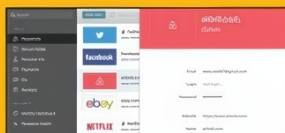


DASHLANE

> LA TENTATION PC

Le très bon et très complet Dashlane (gestionnaire, formulaires, moyens de paiement, notifications, ...) propose ses services gratuitement sur 1 seul poste... ce qui vous poussera peut-être à la version Premium pour vos autres terminaux.

Lien : www.dashlane.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 MÈNÉVILLERS

- ☐ 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



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

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 - 13140 SAUSSET LES PINS

LES DOSSIERS DU **Pirate**

DES DOSSIERS
THÉMATIQUES
COMPLETS

À DÉCOUVRIR
EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ
D'ASTUCES



Actuellement **LE GUIDE
PIRATE 2024** #Guide pratique



BITCOIN VPN + TOR
INTELLIGENCE ARTIFICIELLE
TÉLÉPHONE
MONTAGE VIDÉO
FACEBOOK
ANTI-SURVEILLANCE
ANTI-ARNAQUES
MOTO TAG



PIRATE
INFORMATIQUE



BEL/LUX : 6 € - DOM : 6,10 € - CH : 8,50 CHF - PORT/CONT. : 6 € - CAN : 7,99 \$ cad -
POLS : 750 CFP - NCALUS : 950 CFP - MAR : 50 mad - TUN : 9,8 Tnd