

PIRATE

INFORMATIQUE

TEST VPN

WINSCRIBE :

**SA VERSION
GRATUITE
REMPORTE TOUS
LES SUFFRAGES**

LE GUIDE

HACKING de A à Z

ÉMULATEUR

**JOUEZ AUX
JEUX VIDÉO
DE VOTRE JEUNESSE
AVEC DOSBOX**



F-DROID

**TROUVEZ DES
APPLIS
TERDITES
LIBÉRÉES
DE GOOGLE**

E-MAIL CRYPTÉ

**CÉDEZ À LA
NOUVELLE VERSION
DE TUTANOTA**

BLACK DOSSIER

MOTS DE PASSE

» COMMENT TOUT TROUVER & TOUT PROTÉGER



- ☒ DOCUMENTS
- ☒ MESSAGERIES
- ☒ WINDOWS
- ☒ SERVICES, ETC.



SOMMAIRE

BLACK DOSSIER

12-19



**MOTS
DE PASSE :**
TOUT **TROUVER**,
TOUT **PROTÉGER...**

HACKING

20-26

KALI LINUX en vadrouille
avec **PI-TOP CEED** !



27-29

AIRMORE, votre smartphone
tout entier dans votre ordi !



30-31

MICROFICHES

ANONYMAT

32-35

CLOUD : un cloud **CHIFFRÉ**
pour les **PROS** !



36-39

TUTANOTA :
la **NOUVELLE**
VERSION qui
révolutionne l'e-mail !



SOUTENEZ-NOUS !

Vous découvrez ce magazine en l'avant 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 10 ans, sans publicité et sans hausse de prix depuis 7 ans.

40-42

Gratuit ou payant

WINDSCRIBE :

un des **MEILLEURS VPN...**

44-47

F-DROID : un magasin
d'**APPLIS LIBRES !**

49-51

MICROFICHES



PROTECTION

52-54

AVIRA PASSWORD MANAGER : la
garantie de **MOTS DE PASSE SÛRS**

55

MICROFICHES



MULTIMÉDIA

56-62

DOSBOX & D-FEND :
tout pour profiter de vos
VIEUX JEUX !



64-65 >
**NOTRE SÉLECTION
DE MATÉRIELS**



PIRATE
N°41 INFORMATIQUE

Mai / Juin. 2019

Une publication du groupe ID Presse.

Impasse de l'Espéron - Villa Miramar

13960 Sausset Les Pins

E-mail : redaction@idpresse.com

Directeur de la publication :

David Côme

Donald : Benoît Bailleul

Riri, Fifi & Loulou :

Kevin Poireault, Kevin Dachez & Baptiste G.

Tic&Tac : Sergueï Afanasiuk

& Stéphanie Compain

Correctrice : Marie-Line Bailleul

Imprimé en France par

/ Printed in France by :

Léonce Deprez

ZI Le Moulin 62620 Ruitz

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.

ÉDITO

BONJOUR AUX HABITUÉS COMME AUX NOUVEAUX VENUS !

La nouvelle formule de Pirate Informatique vous a séduits et nous sommes ravis d'avoir reçu autant d'encouragements. Le pari était risqué, comme à chaque fois que l'on change une équipe qui gagne. Dans ce numéro nous vous avons écoutés (comme depuis 10 ans) en vous proposant des sujets que vous aviez envie de nous voir aborder. C'est ainsi que nous avons préparé des sujets sur un VPN gratuit (mais sérieux), les moyens de transférer simplement des fichiers entre votre smartphone et votre ordinateur, un coffre-fort de mots de passe, de l'e-mail chiffré et du Kali Linux ! Enfin, pour la récréation,

nous vous avons préparé un sujet sur le retrogaming. Une cure de jouvence pour nous autres gamers de plus de 40 ans, mais aussi un moyen pour les plus jeunes de découvrir des classiques de cet art si sous-estimé. Outre les rubriques habituelles, vous trouverez chaque mois un grand dossier de plusieurs pages sur un sujet particulier alors n'hésitez pas à nous faire part de vos commentaires et de vos souhaits pour les prochaines éditions sur benbailleul@idpresse.com

Bonne lecture et merci pour ces dix dernières années... Vous avez fait de *Pirate Informatique* le seul magazine du genre dans le monde francophone.

Benoît BAILLEUL



La parole est aux PIRATES !

À moins de vivre dans un tonneau, vous n'avez pas pu passer à côté : les 25 et 26 mai prochain, ce sont les élections européennes dans les 27 États membres de l'Union. La France devra élire 74 députés (et peut-être 5 de plus si d'ici là les Britanniques se décident à partir) sur les 705 que compte le parlement européen. Alors pourquoi parler uniquement du Parti Pirate ? Déjà parce qu'on fait ce qu'on veut, ensuite parce que dans Parti Pirate, il y a «pirate», mais aussi parce que c'est le seul parti véritablement européen...



<https://europeennes.partipirate.org>

Depuis quelques numéros nous parlons souvent du Parti Pirate (PP), car nous sommes particulièrement séduits par son mode de fonctionnement et ses idées novatrices. Né en Suède en 2006, le Parti Pirate s'est internationalisé et un parti européen organisé voit le jour en 2014. Après 2 députés en 2009, mais un seul en 2014, le parti, même s'il est un petit Poucet de la politique, est aussi le seul parti vraiment européen avec des sections dans presque tous les pays de l'union et une poussée très forte en République tchèque par exemple.

IPAS UN PARTI D'ANARCHISTES

Dans le dernier numéro, nous avons abordé le principe de démocratie liquide (ou délégative), chère au Parti Pirate, qui allie représentativité, démocratie directe et qui permet de déléguer un vote à une personne de confiance. Vous êtes mécanicien et on vous demande votre avis sur la santé ? Donnez votre voix à un ami médecin ! Vous êtes médecin, mais vous n'y connaissez

rien en macro-économie ? Donnez votre voix à votre pote mécanicien qui lit tout plein de livres à ce sujet ! C'est simple et cela évite de donner son avis sur des sujets que vous ne maîtrisez pas totalement. Outre ce concept novateur, le PP propose un programme très complet. On est très loin de l'idée que certains ont d'un parti d'anarchistes qui veut légaliser le téléchargement. On y parle d'agriculture durable, d'environnement (climat, énergies renouvelables), des transports, d'accès égal aux soins, de lutte contre l'évasion fiscale, de réglementation des brevets (pour éviter les abus notamment de l'industrie pharmaceutique) et même d'un programme spatial. Plus fort, alors que les citoyens sont parfois fâchés avec une Europe qui leur semble lointaine, peu démocratique et toute puissante, le PP souhaite une « assemblée de citoyens, élue au suffrage direct, chargée de rédiger un nouveau traité européen afin de clarifier et de remplacer les traités actuels et de répondre au besoin de réforme démocratique au sein de l'Union, à condition qu'elle soit acceptée par les citoyens de l'Union par référendum. »

Notre Programme Européen



Pour une agriculture durable



Pour une Europe démocratique



Pour partager des connaissances



Pour faire le lien



Pour mieux gérer les déchets



Financement



Pour une sécurité internationale



Pour un accès égal aux soins



Pour réduire l'inertie



Pour un transport de qualité



Pour les données personnelles



Le programme du Parti Pirate est complet et découpé en 11 points principaux : nous vous invitons à les découvrir en suivant ce lien : <https://europeennes.partipirate.org>

POUR LE PARTAGE DES CONNAISSANCES

Chez Pirate Informatique, d'autres bonnes idées ont retenu notre attention comme le droit à sa vie privée («L'anonymat ne dispense aucune personne d'assumer la responsabilité de leurs actes»), le partage des connaissances, la promotion de la culture libre, mais aussi et surtout une réforme du droit d'auteur : «La copie, le stockage, l'utilisation et l'accès à des œuvres littéraires et artistiques à des fins non commerciales doivent non seulement être légalisés, mais protégés par la loi et activement promus». Exit les DRM et bonjour à un Internet sans frontières avec une libre circulation des connaissances...

Interview de Florie Marie, porte-parole et tête de liste du Parti Pirate en France

Florie Marie a 31 ans et après avoir travaillé à Europe Écologie Les Verts, elle a adhéré au Parti Pirate en 2017. Attirée par ce parti non traditionnel, elle a été successivement militante puis coordinatrice pour la région Île-de-France, elle a participé à écrire les nouveaux statuts du parti et depuis juin 2018 elle fait partie du trio de porte-parole. Pour ces élections, elle est tête de liste pour le Parti Pirate français.

EN VISITANT LE SITE OFFICIEL DU PP POUR CES ÉLECTIONS, NOUS AVONS ÉTÉ SURPRIS DE VOIR QU'IL VOUS MANQUAIT DE L'ARGENT, Y COMPRIS POUR IMPRIMER LES BULLETINS...

Effectivement, il nous faudrait 270 000 € pour cela et encore plus pour les imprimer en double pour les mettre dans les enveloppes envoyées aux électeurs. Pour une campagne traditionnelle avec des affiches, il nous faudrait 400 000 €. Nous en sommes pour l'instant très loin, mais la campagne n'a pas encore commencé [l'interview a eu lieu le 5 avril 2019, NDLR]

C'EST TRÈS SURPRENANT ! NOUS PENSIONS QU'IL ÉTAIT OBLIGATOIRE DE METTRE À DISPOSITION UN BULLETIN PAR ÉLECTEUR... MAIS COMMENT FONT LES GENS ALORS ? ILS DOIVENT IMPRIMER LEUR BULLETIN ?

C'est ça. Lorsque la liste sera prête [le 3 mai 2019, NDLR], nous mettrons le bulletin à télécharger sur le site de la campagne. Les militants et électeurs ont l'habitude de ce système. Il y en a même qui s'inquiètent déjà de ne pas voir le bulletin...

Mais c'est injuste, on ne peut pas prétendre être une démocratie et imposer que les candidats soient riches pour participer à une élection. Nous ne sommes pas dans une démocratie dans ces conditions, nous sommes dans une ploutocratie.



"Rendre le pouvoir à chaque citoyen, et réapprendre la démocratie"



VOUS ÊTES PARTISANS DU BULLETIN UNIQUE [UN BULLETIN OÙ TOUTES LES LISTES SÉRAIENT PRÉSENTES ET OÙ L'ÉLECTEUR N'AURAIT QU'À COCHER LA CASE QU'IL DÉSIRE, NDLR]. C'EST DE NOTRE POINT DE VUE INCOMPRÉHENSIBLE DE NE PAS OPTER POUR CETTE SOLUTION. VOUS PENSEZ QUE C'EST POUR DÉCOURAGER LES PETITS PARTIS ?

Je ne le pense pas, j'en suis sûr. Car en plus de coûter cher pour les petits partis, c'est une aberration écologique en ce qui concerne l'impression, mais aussi le transport de ces bulletins. On voit ici que le système électoral français est verrouillé. Tout est conçu pour décourager les petits partis à se présenter. Non seulement le code électoral est très codifié, mais les partis en place n'ont aucun intérêt à ce que cela change puisque les remboursements des campagnes sont dépendants des résultats. Les petits partis ne peuvent pas y avoir droit : c'est un cercle vicieux qui permet aux gros d'écraser les autres, mais ce n'est pas le seul système permettant d'asseoir la domination des gros : en procédant à un redécoupage de la carte électorale dans certaines circonscriptions, parfois à la rue près, on peut manipuler le système. On pourrait aussi parler des dons privés limités à 7500€/personne, mais qui sont détournés par de grosses compagnies. Imaginons une société qui donne 7500 € à 15 ou 20 salariés pour qu'ils en fassent don à un parti. Cela permet à ce parti d'encaisser l'argent sans problème et au salarié de déduire une grosse somme sur ses impôts, car les dons sont déductibles.



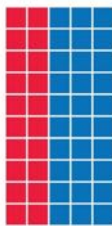
COMMENT SE PASSE UNE CAMPAGNE AU PP ?

Il n'y a aucun professionnel au Parti Pirate, nous sommes tous bénévoles et avec notre manque de moyens financiers, nous privilégions Internet comme porte-voix. Nous avons prévu une campagne courte mais intense, on ne peut pas demander à tout le monde de prendre des congés pour faire campagne, mais certains d'entre nous pourront le faire donc on capitalisera sur ceux là pour assurer une bonne visibilité à nos idées. Et puis on compte un peu sur la conscience professionnelle des journalistes pour bénéficier d'une équité du temps de parole... Sinon concrètement, nous sommes pour la plupart ultra connectés ce qui nous permet d'être réactifs et créatifs, de travailler en équipe et ce malgré la distance ou les disponibilités des uns et des autres. Je vis à Strasbourg, Cédric (deuxième de liste), vit dans le sud-ouest de la France, mais on se parle tous les jours, et je ne vois pas comment on pourrait se passer de nos outils numériques qui sont chaque jour un peu plus performants grâce au travail monstrueux de nos adhérents et de nos soutiens.

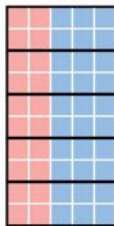
VOILÀ UN EXEMPLE TRÈS CARICATURAL MAIS QUI MONTRE SIMPLEMENT COMMENT IL EST POSSIBLE DE FAUSSER LES RÉSULTATS D'UNE ÉLECTION...



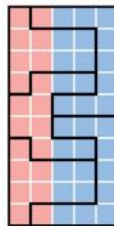
COMMENT VOLER UNE ÉLECTION ?



Sur 50 quartiers, 60 % des gens votent pour les bleus et 40 % des gens votent pour les rouges.



En découplant en 5 circonscriptions égales et linéaires, les bleus gagnent logiquement.



Et en découplant en 5 circonscriptions alambiquées (et bien sûr, calculées à l'avance), les rouges gagnent par 3 contre 2 alors qu'ils ont moins de votants.



QUEL EST L'OBJECTIF DU PP POUR CES ÉLECTIONS ?

Notre objectif c'est de porter nos idées dans le débat politique même si nous sommes trop peu écoutés par la presse (on attend toujours nos invitations aux débats organisés par les chaînes de télévision...). Nous souhaitons être présents, faire parler de nous et nous faire connaître, mais une campagne électorale c'est aussi et surtout le meilleur moyen pour nos membres d'apprendre à comprendre les institutions et ainsi renforcer leurs arguments sur les grands changements que nous voulons mettre en oeuvre. Nous souhaitons aussi faire connaître notre mode de fonctionnement horizontal. Lorsqu'on entre au PP, on n'est pas un simple adhérent qui paye sa cotisation, on participe vraiment à la vie du parti, on fait immédiatement partie de l'Assemblée Permanente avec un vrai droit de parole et de prise de décisions. C'est très différent de ce qu'on a l'habitude de voir dans d'autres organisations avec un pouvoir central et une représentativité (les citoyens ou militants qui votent pour un député ou un chef qui s'exprime en leurs noms, NDLR). Et c'est cette représentativité qui pose problème à notre sens, et qu'on n'a de cesse de remettre en question dans notre engagement militant. Il n'y a qu'à voir les prises de position de certains députés pour se demander ce qu'ils font là...

LE PARTI PIRATE A BESOIN DE VOUS !

Fondé en 2006, Le Parti pirate est un parti politique créé sur le modèle de son homologue suédois. Sa devise est «liberté, démocratie, partage». Son programme se développe sur la base de la protection des droits et libertés fondamentales, aussi bien dans le domaine numérique qu'en dehors : légalisation du partage hors marché, lutte contre le fichage abusif, indépendance de la justice, transparence de la vie politique et ouverture des données publiques.

Si vous voulez adhérer : <https://adhesion.partipirate.org> ; Si vous souhaitez faire un don : <https://don.partipirate.org>



LES DOSSIERS DU **Pirate**

DES DOSSIERS
THÉMATIQUES
COMPLETS

À DÉCOUVRIR
EN KIOSQUES

PETIT FORMAT

MINI PRIX

CONCENTRÉ
D'ASTUCES



LE GUIDE
2019
ANTI-PLANTAGE



TOP 10



SITES DE TÉLÉCHARGEMENT ILLÉGAUX

Tous les premiers vendredis du mois, le site NextWareZ présente son classement des sites de téléchargement et de streaming les plus visités par les Français... Peu de changement depuis la dernière fois mais toujours quelques bonnes adresses à glaner.

1.	Annuaire-Téléchargement	Site de DDL généraliste francophone	=
2.	YggTorrent	Tracker torrent francophone généraliste	=
3.	Torrent9	Tracker torrent francophone généraliste	=
4.	Extreme-Down	Site de DDL généraliste francophone	=
5.	LibertyVF	Site de streaming & DDL francophone	=
6.	VoirFilms	Site de streaming généraliste francophone	=
7.	SerieStreaming	Site de streaming généraliste francophone	RE
8.	Streamiz	Site de streaming généraliste francophone	+1
9.	VoirSeries	Site de streaming généraliste francophone	E
10.	StreamComplet	Site de streaming généraliste francophone	-2

Sources : NetxWareZ.com

DOWN

Vous les connaissez, vous les avez vues dans James Bond ou Harry Potter. Les célèbres cabines téléphoniques rouges britanniques ont fait leur temps. Pour les remplacer, l'opérateur BT, anciennement British Telecom, a fait appel à sa

filiale InLinkUK. Cette entreprise est spécialisée dans la création de bornes téléphoniques nouvelle génération révolutionnaires : WiFi public ultra-rapide, chargeur pour smartphone intégré, appels gratuits et une tablette pour accéder à différentes fonctionnalités, comme des cartes ou les sites des services publics. Une belle innovation détournée très rapidement par certains criminels.

Vous vous en doutez, avec de telles possibilités (appels gratuits et anonymes, WiFi haut-débit), des dealers se sont très vite rendu compte du potentiel « commercial » de ces bornes high-tech. Elles sont un excellent moyen de communiquer efficacement et discrètement avec leurs clients. Prise de rendez-vous ou de commande, quantité, type de drogue, tout se faisait dans la rue, aux yeux de tous. Le quartier de Tower Hamlets a été sévèrement touché. La police locale affirme que les 5 bornes installées dans ce secteur de Londres ont grandement facilité plus de 20 000 transactions illégales, en seulement 15 semaines. À WhiteChapel, tout près de la City londonienne (l'équivalent du quartier de la Défense à Paris), un autre rapport des forces de l'ordre prouve qu'une de ces cabines aurait rapporté à elle seule plus de 1,5 millions d'euros (1,28 millions de livres) à un gang. Pour mettre fin à ces détournements gênants et coûteux, BT et InLinkUK ont développé un algorithme miracle : il leur permet de traquer, bloquer, désactiver les appels dits « anti-sociaux », comprenez ceux qui ne ressemblent pas à une conversation lambda. Comment fonctionne cet algorithme ? Il analyse les fréquences des appels, la durée, la localisation des émetteurs et destinataires. Il compare ensuite ces informations avec les données de la police, et identifie les communications suspectes. Ceci fait, les numéros concernés sont immédiatement bannis du système, et ne peuvent plus utiliser les bornes.



En Bref...

LE CHIFFREMENT LUMINEUX CHEZ CLOUDFLARE

La société Cloudflare qui gère entre 5 et 10% du trafic Internet mondial dispose d'un moyen rigolo pour chiffrer les données qui transitent par leur service : ils filment un mur de 100 lampes à lave. Comme les mouvements de ces respacées des années 70 sont imprévisibles, ils génèrent des clés de chiffrement 100 % aléatoires alors qu'il est très difficile d'obtenir un résultat similaire avec un ordinateur.

UNE FAILLE TRÈS CRITIQUÉE...

Certains smartphones Xiaomi disposent d'une application anti-malware préinstallée, appelée Sécurité (Guard Provider dans la liste des processus). Or, elle a dernièrement été pointée du doigt par Check Point, un spécialiste mondial de la sécurité. Xiaomi s'est donc excusé, a corrigé la faille, mais c'est maintenant au tour d'Avast de répliquer. En effet, la société tchèque est à l'origine de cette fameuse appli, et pour eux le risque d'attaque était très réduit voire même expérimentale. Il faut savoir que Check Point et Avast sont concurrents à la base : ceci expliquant cela...

DES MOUCHARDS DANS LES STATIONS DE MÉTRO ET LES GARES

Ils sont partout ! Les panneaux lumineux diffusant des spots publicitaires seraient des outils pour tracer les possesseurs de smartphone passant à proximité des fameux écrans. Cela défraye la chronique depuis quelques jours, certains écrans publicitaires que l'on trouve dans les stations de métro et gares françaises seraient équipés d'une carte WiFi permettant d'identifier l'adresse MAC d'un smartphone, dont la connectivité WiFi est activée, se trouvant à moins de 10 mètres de l'écran. À première vue rien d'illégal là-dedans, les données collectées sont uniquement utilisées afin de mesurer l'audience. La Commission nationale informatique et liberté (Cnil) a audité et validé le principe en 2017. « Le procédé (...) garantit une anonymisation totale des informations de flux de trafic, comptage et parcours. Les adresses récoltées sont supprimées dans un délai de quelques minutes » assure Isabelle Bordry, fondatrice de Retency. Dans les faits il s'agit de mesurer le nombre de personnes ayant eu accès au panneau, soit le taux d'exposition et d'évaluer l'impact de cette exposition publicitaire sur leur comportement soit le taux de conversion. Ces valeurs permettent à Métrobus, qui vend ces panneaux, de proposer des tarifs adaptés à la « rentabilité » de cet espace publicitaire. En résumé plus les taux d'exposition et conversion sont élevés plus la place sera chère ! Si vous ne souhaitez pas faire partie de cette étude de marché vous pouvez vous rendre sur le site de Retency pour vous opposer à la collecte et l'exploitation de vos données. Autre option, désactivez la connectivité WiFi générale de votre appareil en allant dans les paramètres de votre téléphone. Dernier recours, ce programme créé par des activistes anti-pub, proposé en open-source sur la plate-forme Framagit, qui serait capable d'interférer avec le comptage de Retency en envoyant des adresses MAC aléatoires. Selon Thomas Bourgenot, militant de l'association « Résistance à l'agression publicitaire », ce programme de résistance aux publicitaires serait une première d'un point de vue numérique.





TOP 15 SÉLECTION DE LOGICIELS



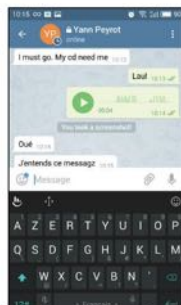
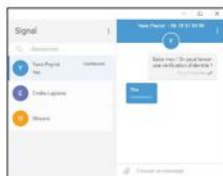
Vous vous demandez quel logiciel choisir pour tel ou tel usage ? En cherchant sur le Net, vous vous retrouvez avec des produits incomplets ou payants ? Dans chaque numéro, retrouvez ici notre Top 5 dans 3 catégories. La crème de la crème !

TOP5 MESSAGERIE CHIFFRÉE

SIGNAL

C'est la messagerie préférée d'Edward Snowden ! Disponible sur Windows, Mac, Linux et mobiles (iOS & Android), Signal vous permet de converser avec des messages chiffrés de bout en bout, de téléphoner de manière sécurisée avec un correspondant lui aussi possesseur de l'appi et de s'envoyer des pièces jointes.

Lien : <https://signal.org/fr/>



TELEGRAM

Pointée du doigt pour avoir le malheur d'être utilisée par des djihadistes, Telegram est une application de tchat pour mobile et ordinateur. Telegram ne propose pas de conversation téléphonique, mais comme son concurrent, il intègre un chiffrement de bout en bout. Le problème, que relèveront les anti-Telegram, est que cette fonctionnalité n'est pas activée par défaut. Il faut en effet aller dans le menu, puis faire **New Secret Chat** pour initier une conversation privée.

Lien : <https://telegram.org>

WICKR

Wickr est un logiciel multisupport (Windows, Linux, iOS, Android, Mac) permettant de chiffrer vos messages, des photos ou autres fichiers. Vous choisissez qui peut lire ce que vous envoyez et le déchiffrement se fait localement par l'intermédiaire des serveurs de Wickr. Une fois la transmission terminée, tout est effacé.

Lien : <https://wickr.com>



SECUSHARE

Secushare n'est pas une messagerie, mais ce service en ligne permet de chiffrer un fichier local en AES-128 pour ensuite l'uploader sur un espace de stockage à usage unique. Dès que votre destinataire aura récupéré le document, il sera effacé des serveurs. Le site vous donnera le mot de passe aléatoire choisi pour vous ainsi que deux URL. La première permet d'avoir accès au fichier sans avoir besoin de mot de passe et la deuxième vous donne accès au fichier sans la clé. Bien sûr cette solution est à privilégier si vous pouvez envoyer la clé par un autre moyen sécurisé.

Lien : <https://securesha.re>

JITSI

Jitsi est un logiciel de VoIP qui fonctionne comme Skype. Il est par contre ouvert et compatible avec deux protocoles, XMPP et SIP. De logiciel à logiciel, les conversations sont chiffrées avec le protocole ZRTP qui garantit la confidentialité. Côté Tchat, les conversations sont aussi chiffrées.

Lien : <https://jitsi.org>

TOP5 CHIFFREMENT

TRUPAX

Un logiciel basé sur TrueCrypt qui permet de chiffrer des fichiers et des dossiers sans avoir à créer un volume auparavant. Ces éléments seront considérés comme des conteneurs à part entière. Plus besoin de créer des volumes chiffrés trop grands de peur de manquer de place un jour. Pour plus de sécurité, les fichiers originaux pourront être supprimés (en plusieurs passes) une fois la copie bien à l'abri dans son conteneur chiffré.

Lien : www.codeon.com



AXCRYPT

Un clone très puissant de TrueCrypt qui permet de chiffrer un seul fichier sans avoir à créer de volumes spéciaux. Alors que certains

logiciels proposent tout un arsenal pour chiffrer vos données sensibles (création de conteneurs cachés, sauvegarde incrémentielle compactée, etc.), AxCrypt va au plus simple. Le logiciel ne comporte même pas d'interface graphique, toutes les fonctionnalités sont accessibles via le menu contextuel du clic droit.

Lien : <https://www.axcrypt.net/fr/>

AESCRYPT

Depuis que le projet TrueCrypt n'est plus considéré comme « sûr », les utilisateurs peuvent se tourner vers des logiciels alternatifs comme AESCrypt. Ce dernier est multi-plate-forme. Ce n'est pas celui que nous conseillerons pour débuter, mais il est très bon dans son domaine.

Lien : www.aescrypt.com



TOP5 PROTECTION WIFI

WIFI GUARD

Wifi Guard est un logiciel très simple. Il scanne à intervalle régulier votre réseau pour voir quels sont les périphériques ou ordinateurs qui s'y connectent. Une fois que vous avez dressé la liste des appareils autorisés, il vous prévient dès qu'un nouveau venu se fera connaître. Attention c'est une version d'essai !

Lien : <https://wifi-guard.fr/uptodown.com/windows>

WIFI PASSWORD DECRYPTOR



WiFi Password Decryptor permet de retrouver le mot de passe égaré ou oublié de votre connexion Internet Wi-Fi. Il suffit de le lancer sur un PC pour retrouver la clé avec le SSID correspondant ! Le logiciel déchiffre le mot de passe en scannant le module Windows Wireless Configuration Manager.

Lien : https://wifi_password_decryptor.fr/downloadastro.com

WIFITE

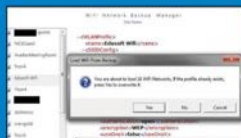
Wifite automatise les tests de pénétration. Sous réserve d'avoir une carte Wi-Fi compatible avec l'injection de paquet, Wifite va tester les réseaux des environs et tenter de s'y introduire, qu'ils soient protégés en WEP ou WPA. Plus fort, il va même essayer de forcer l'entrée des box ou routeurs protégés par WPS. Attention, ce logiciel ne fonctionne que sous Linux.

Lien : <https://github.com/derv82/wifite2>

WIFI NETWORK BACKUP MANAGER UTILITY

Wifi Network Backup Manager Utility vous permettra de sauvegarder, de restaurer et d'installer vos configurations WiFi en quelques clics sous Windows. Vous pourrez ainsi récupérer l'ensemble de vos identifiants et mots de passe WiFi sur votre ordinateur puis les retrouver au besoin instantanément sur une machine neuve, un système réinstallé de zéro, un ordinateur de travail ou encore les transférer rapidement à vos amis.

Lien : <https://frama.link/E3MnBcdP>



KICKTHEMOUT

Rappelons que cet outil sous Linux vous permet simplement de déconnecter des périphériques de votre réseau et de profiter de toute la bande passante. Sélectionnez des périphériques spécifiques ou tous les périphériques avant de lancer une attaque ARP spoofing sur votre réseau local pour mettre à la porte les squatters. Vous êtes en collocation, à la bibliothèque ou dans n'importe quel endroit avec une connexion Wi-Fi que vous partagez ? Grâce à KickThemOut, vous pouvez faire en sorte de bannir les autres utilisateurs pour garder toute la bande passante !

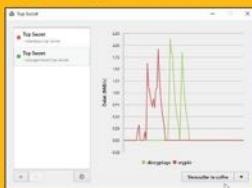
Lien : <https://github.com/k4m4/kickthemout>



CRYPTOMATOR

Cryptomator crée un coffre-fort virtuel qui se comportera comme un volume virtuel monté sur votre ordinateur. Vous devrez l'ouvrir via votre mot de passe pour accéder à vos fichiers en clair et en ajouter ou supprimer de nouveaux. Une fois le coffre-fort verrouillé, le lecteur virtuel est démonté et personne ne pourra y accéder sans mot de passe. Même vous si vous avez oublié ce précieux sésame.

Lien : <https://cryptomator.org>



VERACRYPT

VeraCrypt est né suite à une étude sur TrueCrypt demandée par un client de IDRIX en 2012. Cette étude n'a pas trouvé de problème de sécurité majeur (une faiblesse connue concernant la dérivation de clé de chiffrement). C'est ce dernier point qui a poussé Mounir Idradi à concevoir VeraCrypt comme un « fork » de TrueCrypt. Le but était de remédier à ce défaut en augmentant le niveau de sécurité face aux attaques par force brute qui sont devenues très performantes.

Lien : www.veracrypt.fr



MOTS DE PASSE :



TOUT TROUVER,
TOUT PROTÉGER...



Le problème avec les mots de passe c'est quand les choisissant trop bien, on les oublie et s'ils sont trop faciles à deviner, votre sécurité est en danger. Et ces sésames sont partout : document, e-mail, Windows, sites, services, WiFi, etc. Voyons comment protéger ceux que vous avez et retrouver ceux que vous avez perdus...

» RÉCUPÉRATION AUTOMATIQUE

RECALL RÉCUPÈRE VOS MOTS DE PASSE EN LOCAL

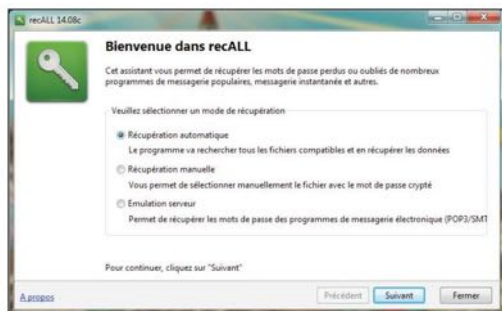
Voici un petit logiciel à la fois très pratique et diabolique. recALL permet de récupérer toute sorte de mots de passe stockés dans les méandres de votre disque dur. Même s'il s'agit bien sûr d'une solution pour retrouver ses sésames avant un formatage ou en cas de changement de PC, on peut bien sûr imaginer d'autres utilisations...

Difficile de faire plus simple que recALL. Après l'avoir installé, il suffit de laisser faire le logiciel pour vous. Il ira chercher des mots de passe, des codes d'accès ou des numéros de licence dans des endroits de votre Windows dont vous ne soupçonneriez même pas l'existence (dossier d'installation, base de registre, etc.). Ces emplacements sont préenregistrés et toutes sortes de logiciels sont passés au crible : Windows, Office, antivirus, client mail, tous les mots de passe mémorisés par une vingtaine de navigateurs, client FTP, messagerie instantanée, logiciels commerciaux, jeux vidéo, etc. Avec presque 3 000 références, ce serait bien le diable si recALL ne trouvait pas ce que vous cherchez.

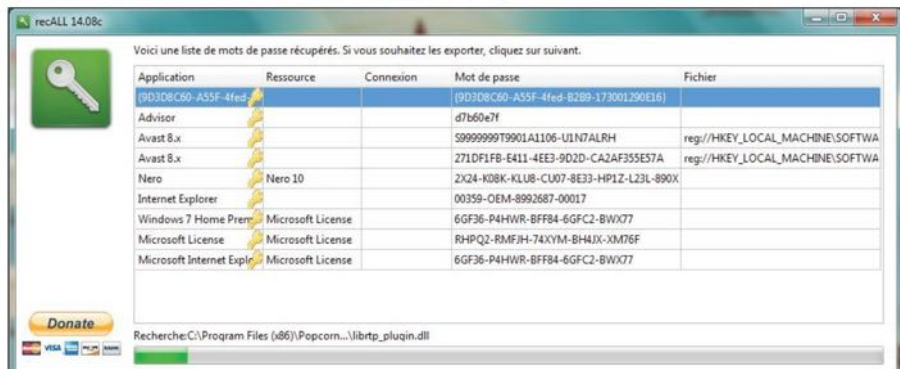
3 000 LOGICIELS DANS LA BASE DE DONNÉES !

Bien sûr, les codes d'accès Wi-Fi sont compris dans le lot. Il est possible de rechercher dans un secteur du disque ou de récupérer tout ce qui se présentera à vous. Les données seront alors enregistrées dans un fichier CSV ou un autre format de votre choix. Encore plus fort, recALL peut émuler un serveur FTP, POP et SMTP pour récupérer le mot de passe d'une application qui ne serait pas supportée. Inutile de vous préciser que votre antivirus va grincer des dents lors de l'installation. En effet, on imagine aisément ce que quelqu'un de malintentionné pourrait faire sur le PC d'une victime...

Lien : <http://kelt.co/p/recall>



Attention, recALL
peut être utilisé
par des brigands
qui en voudraient
à vos sésames...



» CRACK DEPUIS UN HASH

CRACK DE MOTS DE PASSE AVEC JOHNNY

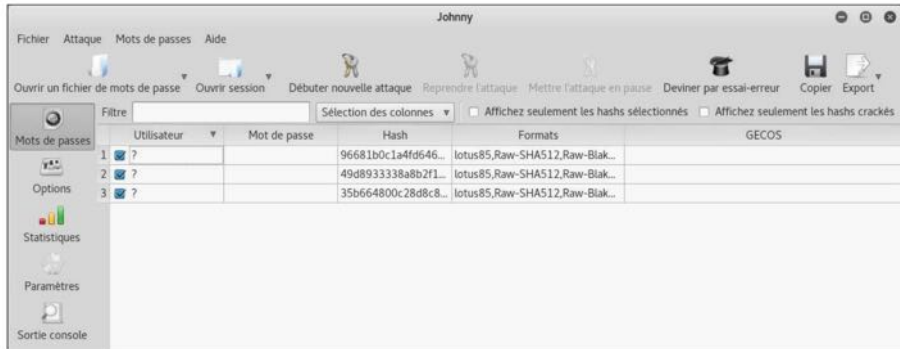
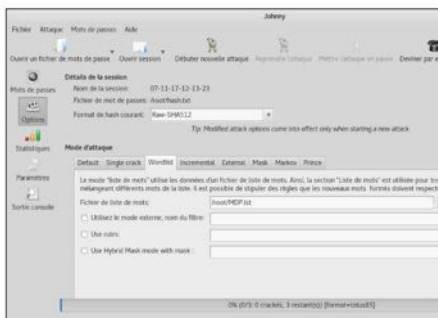
Nous vous avions déjà parlé de John The Ripper, mais jamais du petit frère : Johnny. Celui-ci est en fait une interface graphique de son illustre ancêtre. Disponible sous Linux et Windows, ce logiciel va vous permettre de crackier du mot de passe sans taper une ligne de code...

Disponible dans la version complète de Kali Linux, mais aussi sous Windows, Johnny n'est qu'une interface graphique. Il va chercher l'emplacement de John The Ripper et va interpréter les manipulations que vous faites en ligne de commande. Avant de voir des méthodes complexes dans un prochain article, nous allons nous concentrer sur l'attaque par dictionnaire sur des hash. En effet, la plupart des utilisateurs d'ordinateurs sont peu rigoureux lors du choix de leurs mots de passe. Ils optent parfois pour des mots qui veulent dire quelque chose (Jésus ou cocorico), mais aussi des sésames trop faciles à deviner (psg78, azertyuiop, SuperGégé, etc.) Car les bons «dicos» que l'on trouve sur le Net prennent en compte les tendances et les hackers ajoutent aussi régulièrement les mots de passe crackés ou volés à tel ou tel site piraté. Si vous croyez être original avec MasterKebab123, vous avez tout faux...

UN COUP DE DICTIONNAIRE DANS LES DENTS !

Une attaque par dictionnaire va donc essayer tous les mots contenus dans sa base de données un à un. Cependant, il faudra garder en tête que tous les utilisateurs ne sont pas français et qu'il faudra avoir sous le coude plusieurs dicos dans plusieurs langues pour arriver à ses fins. La bonne chose de cette méthode, c'est que lorsque le logiciel a épuisé vos dictionnaires, vous êtes sûr que le mot de passe ne s'y trouve pas tel quel. Il faudra alors passer à une autre méthode ou ajouter des éléments à vos mots de passe potentiels (préfixe, suffixe, chiffre, majuscule, etc.)

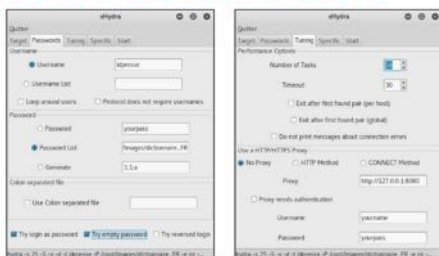
Lien : <http://openwall.info/wiki/john/johnny>



» CRACK DE MOTS DE PASSE EN LIGNE

KALI LINUX : HAIL HYDRA !

Hydra c'est bien sûr une organisation ennemie jurée de Captain America, mais c'est aussi un redoutable logiciel qui peut cracker du mot de passe en ligne sur une cinquantaine de protocoles ou bases de données : Telnet, FTP, HTTP, HTTPS, IRC, VNC, SSH, SMTP, MySQL, XMPP, IMAP, etc. Pour cela, il nous faudra compter sur un dictionnaire de mots de passe et d'un peu de chance...



Nous vous mettons souvent en garde sur l'importance du choix de vos mots de passe et ce n'est pas pour rien ! Avec très peu de connaissances en informatique, un pirate à la petite semaine pourrait faire de votre vie un enfer (usurpation d'identité, défaçage de votre site, vol de données, etc.) Car on utilise des mots de passe tellement souvent sur Internet que certains utilisateurs font l'erreur de choisir le même partout. C'est bien sûr une chose à éviter, car il suffit qu'un seul de vos comptes se fasse pirater pour que les autres ne tombent comme des dominos. De même, n'utilisez pas de mots de passe permettant de deviner les autres (kiki75, kikiPaname, TheKiKidu75, etc.) ou faciles à deviner.

NE VOUS CROYEZ PAS À L'ABRI !

Hydra fonctionne en ligne. Alors que nous devions auparavant avoir un hash en main pour tenter de cracker le mot de passe correspondant, ce n'est pas le cas ici. Hydra va directement envoyer des requêtes vers un serveur cible. Nous vous déconseillons bien sûr de l'utiliser sur une machine qui ne serait pas la vôtre. Si vous n'avez pas envie d'installer ou d'utiliser Kali Linux, il existe aussi une version Windows appelée THC-Hydra que vous trouverez ici : www.thc.org/thc-hydra. Attention, votre navigateur et votre antivirus ne vont pas aimer...

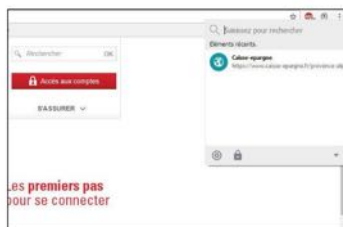
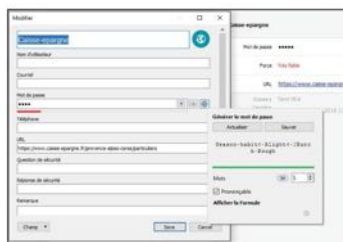
Lien : <https://tools.kali.org/password-attacks/hydra>

» COFFRE-FORT À MOTS DE PASSE

SÉCURISEZ VOS MOTS DE PASSE AVEC ENPASS

Keepass, Password Safe, Xecrets, Dashlane, LastPass... les solutions pour mettre de côté et protéger vos sésames ne manquent pas. Enpass a l'avantage de ne demander aucune inscription et de stocker localement vos données tout en les chiffrant.

Enpass, tout comme Keepass, propose un niveau de sécurité optimal. Toutes les infos contenues dans le logiciel sont chiffrées à l'aide d'une clef AES 256 bits. Pour y accéder, une seule solution. Renseigner le mot de passe maître que vous êtes le seul à connaître. Le choix de ce dernier est important. Enpass entrepose vos documents importants. L'accès à ces derniers est protégé par votre mot de passe maître. Vous enregistrez également les informations de vos cartes bleues pour éviter d'avoir à retaper ces dernières lorsque vous effectuez un achat en ligne. Une entrée adresse est là pour ne pas avoir à renseigner cette dernière à chaque fois que vous remplissez un formulaire. Toutes ces fonctions de remplissage automatique présupposent l'installation d'une extension de navigation



UN SERVICE MULTIPLATEFORME

À la différence d'un service comme LastPass, Enpass ne vous expose pas à un piratage de vos données personnelles à distance. Les clefs de chiffrement sont en effet stockées localement et non pas sur un serveur distant. Notez qu'Enpass se synchronise entre plusieurs appareils. Pour ce faire, les clefs de chiffrement doivent être rattachées à l'un de vos comptes de Cloud (Dropbox, Google Drive...). Dans la langue de Molière et facilement configurable, Enpass est gratuit...

Lien : www.enpass.io

➤ RÉCUPÉRATION EN LOCAL

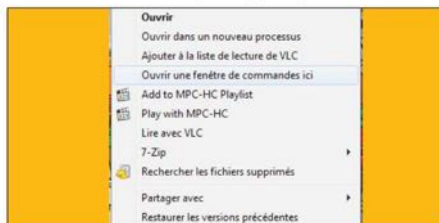
RÉCUPÉRATION DE MOTS DE PASSE AVEC LAZAGNE

Si vous avez physiquement accès à un ordinateur, LaZagne va analyser le contenu de la base de registre et des dossiers pour afficher tous les mots de passe qui traînent en clair : navigateurs, logiciels, bases de données, réseaux WiFi, etc.

Lien : <https://github.com/AlessandroZ/LaZagne>

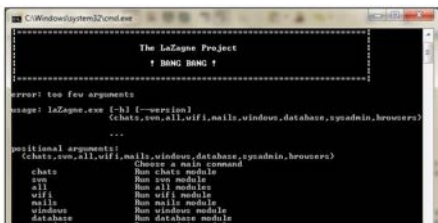
01) EN LIGNE DE COMMANDE

Décompactez le fichier ZIP et placez le contenu où vous le souhaitez. Rendez-vous dans le dossier **LaZagne-master\Windows**. Maintenez la touche **Maj** du clavier, faites un clic droit dans **Standalone** puis cliquez sur **Ouvrir une fenêtre de commande ici**. Pour connaître la liste des commandes, faites **lazagne.exe** puis tapez sur **Entrée**.



02) À L'ACTION !

Vous pouvez constater qu'il suffit de taper **lazagne.exe** **browsers** pour récupérer les mots de passe contenus dans les navigateurs ou **lazagne.exe mails** pour les clients POP/IMAP/SMTP. Pour obtenir absolument tous les mots de passe contenus dans le PC, il suffit de taper **lazagne.exe all**. Magique !



➤ RÉCUPÉRATION DES N° DE LICENCE ET E-MAILS

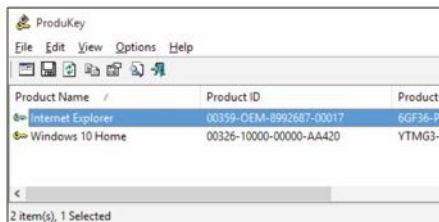
LES LOGICIELS «NIRSOFT»

NirSoft est un site, certes austère, où vous trouverez plus de 180 logiciels gratuits pour vous faciliter l'informatique. Parmi ces derniers, on trouve aussi des programmes pour récupérer des mots de passe de comptes e-mail ou des clés de licence.

Lien : www.nirsoft.net

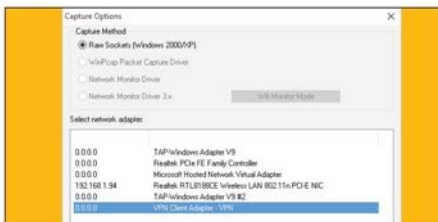
01) PRODUKEY

ProduKey permet de facilement récupérer le numéro de licence de votre Windows, de votre pack Office ou d'autres produits Microsoft. Vous pourrez ainsi réinstaller vos produits sur un autre PC si vous en changez.



02) SNIFFPASS

Ce logiciel va «sniffer» votre réseau à la recherche de mots de passe POP3, IMAP4, SMTP, FTP et HTTP. Si vous avez une connexion, mais que vous avez perdu le mot de passe, lancez le logiciel et SniffPass le retrouvera pour vous.



» RÉCUPÉRATION DU MOT DE PASSE WINDOWS

INVITEZ-VOUS DANS WINDOWS !

Dans d'anciens numéros, nous avons vu comment utiliser Offline NT Password & Registry Editor pour réinitialiser un mot de passe de session Windows. Le problème, c'est que ce logiciel ne fonctionne pas avec les dernières versions de Windows et qu'il n'est pas « discret ». Kon-Boot permet quant à lui de s'inviter sur une session sans que le propriétaire ne soit au courant...

Si vous avez perdu votre mot de passe Windows ou que vous devez accéder au contenu du PC d'un de vos amis (avec son consentement bien sûr), Kon-Boot est la solution idéale. Non seulement vous pourrez accéder aux données, mais vous le ferez en toute discrétion puisqu'une fois que Kon-Boot sera désactivé rien ne laissera présager que vous êtes passé par là...

COMMENT SE PROTÉGER DE KON-BOOT ?

Bien sûr, Kon-Boot est destiné aux bidouilleurs, aux réparateurs ou aux experts en sécurité, mais sa seule existence montre que n'importe qui peut avoir accès à vos données sans que vous soyez au courant (puisque le mot de passe reste le même). La seule faiblesse de Kon-Boot réside dans son incapacité à accéder à une partition chiffrée. Nous vous conseillons donc VeraCrypt pour ce faire. Sans aller aussi loin, vous pouvez aussi installer WinLogonView de NirSoft qui va surveiller incognito votre ordinateur et dresser une liste de données concernant les accès (heure de connexion, heure de déconnexion, durée, logiciels utilisés, etc.). Enfin, vous pouvez mettre en place un mot de passe de BIOS. Même si ce dernier n'est pas infailible, il ajoutera une sécurité supplémentaire et fera perdre du temps au pirate qui tentera de s'inviter sur votre session.

Lien : <http://goo.gl/KMaGQ9>

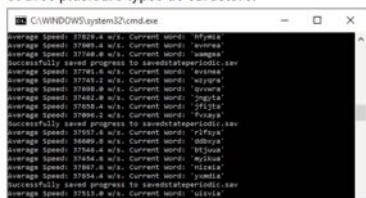


» DÉBLOQUEZ N'IMPORTE QUEL PDF

PDFCRACK : LA DERNIÈRE CHANCE

Par le passé, nous avons vu les différentes protections d'un fichier PDF : mot de passe d'autorisation et mot de passe d'ouverture. Le premier pose rarement problème alors que le second est beaucoup plus difficile à crackner. Nous avons néanmoins quelques solutions...

Le mot de passe d'ouverture (user password) d'un fichier PDF va, comme son nom l'indique, interdire l'ouverture d'un document, mais l'opération va en plus chiffrer le fichier avec l'algorithme RC4 128 bits. Pas de contournement possible ici, il faudra traiter ce mot de passe avec un des deux techniques que nous avons abordé dans nos articles sur John The Ripper : l'attaque par dictionnaire. Il s'agit en fait d'essayer le plus de mots possible afin de trouver le bon. Pour cela il faut un logiciel et une liste de mots dans lequel il ira piocher. Il est possible de trouver ce type de liste sur Internet dans plusieurs langues et avec plusieurs types de caractère.



ATTAQUE PAR DICTIONNAIRE

PDFCrack est un logiciel destiné à fonctionner sur système Linux, mais il existe une version pour Windows. Il permet de tirer profit des processeurs multicœurs et de la puissance de plusieurs ordinateurs (cluster). La progression est automatiquement sauvegardée pour reprendre un projet en cours. Sur notre PC de test, PDFCrack a été capable de passer en revue 37 500 mots de passe à la seconde. Pour tester la liste complète de notre dictionnaire de 10 millions de sésames, il ne lui faudrait que 5 minutes.

Lien : <http://andi.flowrider.ch/research/pdfcrack.html>

» DÉBLOQUEZ N'IMPORTE QUEL ZIP

LES ZIP : COMMENT LES VERROUILLER ET...LES DÉVEROUILLER

Après notre série sur les moyens de cracker un mot de passe d'ouverture de fichier PDF, nous attaquons un nouveau chapitre avec les archives. Qui n'a pas déjà fait son malin en protégeant un fichier ZIP ou RAR avec un mot de passe pour se rendre compte deux ans plus tard qu'il a oublié le sésame ?

Le problème avec les logiciels qui offrent de cracker les archives ZIP, RAR ou autres, c'est qu'ils proposent monts et merveilles sans pour autant donner satisfaction : souvent lents, parfois obsolètes, certains fonctionnent, mais vous demanderont de passer à la caisse au moment de vous révéler le mot de passe. Pour commencer cette série d'articles, nous allons voir comment compresser une archive en spécifiant un mot de passe d'ouverture (pour ceux qui ne savent pas comment faire) puis nous concentrer sur le format ZIP avec le logiciel **frackzip** sous Windows. Ce dernier, en plus d'être gratuit et open source, a l'avantage de proposer l'attaque par dictionnaire en plus du brute force. Il n'est malheureusement pas compatible avec d'autres types d'archives comme le RAR ou le 7Z.

NOS ZIP DE TEST...

Dans les prochains numéros, nous verrons des solutions plus complètes sous Linux et plus puissantes avec notamment la possibilité d'utiliser le GPU de votre carte graphique. Mais revenons à **frackzip**... Pour nos démonstrations, nous avons créé des fichiers compressés que nous allons tenter de cracker. Test1, 2, 3 et 4 sont des ZIP avec pour mot de passe **toto, Jesus, delopa** et **H4j!p*U%J4s**. Notons que la méthode AES parfois utilisée par certains logiciels pour interdire l'accès au contenu du ZIP n'est pas prise en charge par **frackzip**. Ne vous inquiétez pas, car la vieille méthode **ZipCrypto** est toujours la plus utilisée.

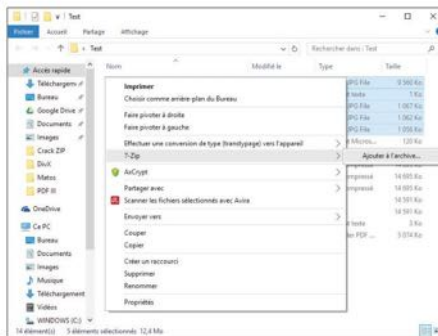
Lien : www.7-zip.org

Lien : <http://goo.gl/y8Lbsx>

PROTÉGEZ UNE ARCHIVE PAR MOT DE PASSE

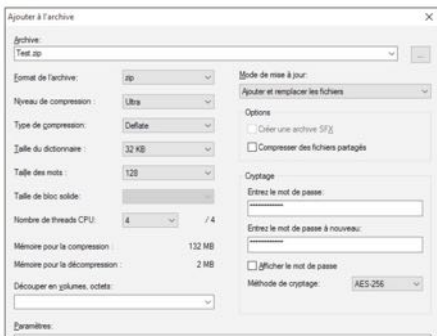
01 > NOTRE LOGICIEL

Pour interdire l'ouverture d'une archive, nous allons utiliser le logiciel gratuit **7-Zip**. Il permet de créer des fichiers ZIP, TAR, WIM, etc. Il dispose en plus de son propre format très performant, le 7Z. Téléchargez ce logiciel en fonction de votre système d'exploitation (32 ou 64 bits). Si vous ne le savez pas, faites un clic droit dans **Ordinateur** ou **Ce PC** (menu démarrer) et cliquez sur **Propriétés**. Après avoir choisi un dossier, un fichier ou un groupe de fichiers, faites un clic droit puis dans le menu contextuel, sélectionnez **7-Zip > Ajouter à l'archive...**



02 > LE CHIFFREMENT

Vous pourrez ici choisir le format, le niveau de compression et d'autres données techniques qu'il vaut mieux laisser par défaut. Dans la partie **Cryptage**, entrez votre mot de passe (sans caractères accentués). Notez que selon le format d'archives choisi vous pouvez changer la méthode. Restez sur l'**AES-256** plus sûr, mais attention, la version Windows de **frackzip** ne peut que retrouver des mots de passe chiffrés en **ZipCrypto**. Mieux vaut utiliser cette méthode très répandue si vous voulez vous amuser...

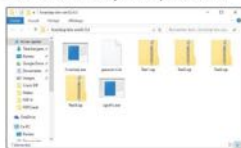


DÉVERROUILLEZ UNE ARCHIVE...

01 LA MISE EN PLACE DES ÉLÉMENTS

Commençons par dézipper le contenu du logiciel dans un dossier appelé **crackzip** que nous placerons dans C:\ pour plus de commodité. Comme nous allons essayer en premier la méthode par dictionnaire, il va nous falloir une liste de mot de passe.

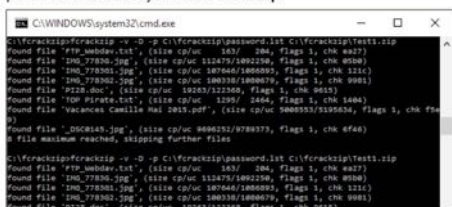
Vous en trouverez ici www.openwall.com/passwords/wordlists en version gratuite. Pour des dictionnaires en français vous pouvez aussi aller ici : <http://goo.gl/gEbEss>. Mettez votre dico au format LST (**password.lst**) dans le même dossier que le programme et que vos fichiers de test. Attention dans votre fichier, les entrées devront être organisées : un mot de passe par ligne !



02 ATTAQUE PAR DICTIONNAIRE

Maintenez la pression sur la touche **Maj** du clavier, faites un clic droit dans le dossier contenant vos fichiers de test, votre dico et **crackzip** puis sélectionnez **Ouvrir une fenêtre de commandes ici**. Pour commencer l'attaque par dictionnaire, tapez **crackzip -v -D -p C:\crackzip\password.lst C:\crackzip\Test1.zip**.

Le switch **-v** permet d'avoir plus d'explications pendant le processus, **-D** spécifie l'attaque par dictionnaire et **-p** montre le chemin du fichier contenant les mots de passe potentiels. Pour notre **Test1.zip**, rien ne se passe ! En effet, **toto** ne fait pas partie du dico... Essayons avec **Test2.zip**.

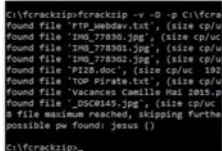


03 SECONDE TENTATIVE

Tapez **crackzip -v -D -p C:\crackzip\password.lst C:\crackzip\Test2.zip** et validez.

Le logiciel trouvera **jesus** en quelques microsecondes ! Pour **delopa**, une attaque par dictionnaire ne donnera rien. Il faut donc utiliser la méthode brute force. Comme nous ne sommes pas censés savoir le mot de passe, il convient de commencer par le plus simple.

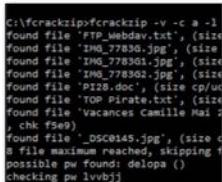
Nous allons donc essayer toutes les suites de caractères minuscules. Nous pouvons aussi tenter de définir une longueur minimale et maximale. La plupart des mots de passe choisis « à la va-vite » font entre 4 et 8 caractères. Nous allons donc taper **crackzip -v -c a-l-4-8 C:\crackzip\Test3.zip**



04 LA MÉTHODE BRUTE FORCE

Ici, le switch **-c** suivi de **a** montre que nous ne recherchons que des caractères minuscules. Il faudrait mettre **-c aa11** pour chercher en plus les majuscules, les chiffres et les caractères spéciaux. Enfin, **-l** (un L minuscule) permet de spécifier la longueur. Au bout de 12 secondes, **delopa** est découvert ! **crackzip** continuera la recherche à cause d'une marge d'erreur de 0,4% causée par la structure de certains fichiers ZIP.

Bien sûr, si nous avions demandé à **crackzip** de chercher aussi les majuscules et les chiffres, le temps de réaction aurait été bien plus long. Lorsque vous cherchez un mot de passe, il faut commencer par le plus simple pour tendre vers le plus compliqué... Inutile de faire l'essai avec **Test4.zip**, car, vous l'aurez compris, le temps de calcul serait trop long. Il faudrait un super ordinateur ou des centaines de machines reliées en cluster pour y parvenir.



POURQUOI TOTO, JESUS, DELOPA ET H4J^P^U^J4S ?

Comme pour nos articles sur les PDF, nous avons choisi ces mots de passe, car ils sont très représentatifs des sésames que l'on peut généralement trouver.

***toto** est très faible et peut très bien se retrouver par dictionnaire ou par brute force.

***jesus** est très simple à trouver par attaque dictionnaire. Et comme les caractères accentués sont interdits dans la constitution du mot de passe, un francophone écrira **jesus** et non **jesús**, plus difficile à trouver.

***delopa** est plus complexe, car il ne veut rien dire et une attaque par dictionnaire serait peu efficace. Par contre, comme il ne comprend que des minuscules et qu'il fait seulement 6 caractères de longs, une brute force est très accessible.

***H4J^P^U^J4S** est notre mot de passe le plus solide. Évidemment absent des dictionnaires, c'est aussi un cauchemar à crackner en brute force. À moins d'avoir 4000 ans devant soi ou d'avoir de gros indices sur sa construction (nombres de caractères, etc.)



POUR QUI ?

Pour les curieux qui veulent expérimenter Kali Linux sans monopoliser leur PC

POUR QUOI FAIRE ?

Pour disposer d'une solution de pentesting transportable

KALI LINUX EN VADROUILLE AVEC PI-TOP CEED !

LEXIQUE

*RASPBERRY PI :

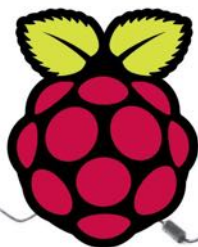
Le Raspberry Pi est un nano-ordinateur à base de processeur ARM qui permet de faire tout un tas de projets pour une somme dérisoire (35 €) : PC de bureau, robotique, domotique, media center, etc.

*KALI LINUX :

Kali Linux, anciennement BackTrack, est une distribution spécialisée dans le hacking : pentesting, crack de mots de passe, mappage de réseau, etc. Même si cette version dispose de moins de logiciels et de moins de «force de frappe» qu'un PC «normal», c'est un véritable tour de force de l'avoir sur la Framboise. Bien sûr, vous pouvez utiliser Kali comme système «généraliste» même si vous allez devoir installer certains logiciels à la main (LibreOffice, multimédia, retouche photo, etc.)

*PENTESTING :

Mot valise réunissant «penetration» et «testing». Il s'agit de tester les forces et les faiblesses d'un ordinateur, d'un réseau, d'un site ou d'une base de données avec des logiciels spécialisés. Bien sûr, ces derniers peuvent être utilisés à des fins moins nobles.



Le Pi-top CEED est un écran inclinable avec une partie creuse permettant de recevoir un Raspberry Pi. Avec ce micro-ordinateur très bon marché, on peut très bien se constituer un PC d'appoint facilement transportable grâce au CEED. Mais ce qui va nous intéresser ici c'est la capacité de la «Framboise» à accueillir Kali Linux...

Vous avez sans doute déjà vu le Pi-top, cet ordinateur portable qui accueille un Raspberry Pi. La même société a créé le Pi-top CEED, une version moins onéreuse qui ne comprend pas de clavier ni de trackpad. Livrée avec son OS «maison», cette coque «deluxe» est un outil d'apprentissage destiné aux enfants et aux enseignants, mais nous allons en faire tout autre chose !

PI-TOP CEED + RASPBERRY PI

Ne coûtant que 150 €, l'appareil dispose d'un bel écran non tactile de 14 pouces qui peut s'incliner à loisir. Une trappe amovible permet d'y placer un Raspberry Pi qui se branche sur un circuit qui s'occupe de l'alimentation et de l'affichage. Sur ses rails en métal, on peut aussi ajouter une carte de prototypage, de plus on pourra y loger une souris ou une antenne WiFi supportant le mode «Monitor» pour faire de l'analyse de paquets. Le CEED n'a pas de haut-parleur. On peut en ajouter un, mais quel intérêt pour nous ? Les finitions sont très soignées, le montage est très accessible et l'appareil est facilement transportable (moins de 1 kg). Dans la boîte on trouve :

- Le Pi-top
- Une alimentation
- Une carte micro-SD 16 Go avec Pi-topOS
- 4 supports magnétiques pour fixer le Raspberry 2B ou 3B

KALI LINUX SUR PROCESSEUR ARM

Depuis que le Raspberry 3 est sorti, les développeurs peuvent se permettre de réaliser des OS plus gourmands ou proposant des logiciels demandant plus de ressources. C'est le cas de Kali Linux. En effet, pour cracker un mot de passe en brute force, il faut un processeur qui envoie la sauce. Bien sûr un ARMv8 se montrera beaucoup moins puissant qu'un processeur de PC mais il faut voir cette solution RaspberryPi+Kali comme une solution «portable». Il est tout de même possible de faire d'autres choses que du crack de mots de passe avec Kali : audit réseau, injection SQL, analyse de hash, sniffing, spoofing, etc. Pour tout cela, pas besoin d'un Core i7. Voyons comment installer ce système sur le Raspberry Pi et l'utiliser à travers le Pi-top CEED...



PI-TOP : UN OS AUSSI !



Pi-Top OS est le système d'exploitation officiel de l'appareil. Dérivé de Linux Debian, il dispose de 2 bureaux distincts : un environnement classique avec une barre de menu et une corbeille très semblables à Rapsbian tandis que l'autre est dédié au contenu d'apprentissage. On y trouve des logiciels de programmation : Scratch, Python, Node-RED, etc. Le logiciel musical SonicPi est aussi de la partie, tout comme Chromium et Minecraft. On trouve aussi 3D Slash qui permet de créer des objets en 3D et CEED Universe, un jeu d'aventures où les enfants peuvent apprendre la programmation Python où chaque quête correspond à une leçon. C'est gratuit alors profitez-en si vous le désirez...






KALI LINUX S'INVITE SUR RASPBERRY PI !

PRATIQUE



01 > TÉLÉCHARGEMENT DE L'IMAGE «CUSTOM»

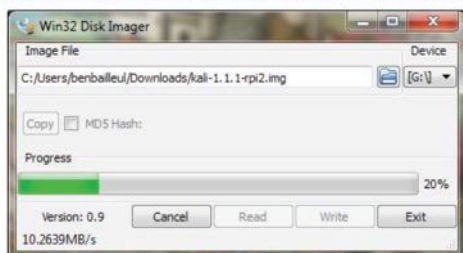
Commençons par placer l'image de Kali spécialement conçue pour les appareils à base de processeur ARM. Suivez notre lien et allez dans la section **Raspberry Pi Foundation**. Vous trouverez ici l'image pour le Raspberry Pi 3 64 bits. Une fois décompactée, vous devriez avoir au final un fichier **kali-linux-2019.1-rpi3-nexmon-64.img**. Pour mettre le contenu de ce dernier dans la carte, il faudra utiliser les logiciels Win32 Disk Imager ou Etcher.



Name	Torrent	Size	Version	SHA256Sum
Kali Linux RPI	Torrent	824M	2019.1	a4a95b5c044638c062f83bd580abe880da5a3d8da1f1833c0ec1870408024
Kali Linux RPi0w Nexmon	Torrent	636M	2019.1	98449eb2b980be875ae2e804425a33297643e8a4f4964ee83f22a49f3f57d1
Kali Linux RaspberryPi 3 64 bit	Torrent	805M	2019.1	e5484de542469f04cdabf4b0ccea976bf4c48c19685771c613ebddc04c0b02

02 > INSTALLATION DES FICHIERS

Téléchargez le logiciel et munissez-vous d'une carte SD d'au moins 16 Go. Lancez Win32 Disk Imager, sélectionnez **kali-linux-2019.1-rpi3-nexmon-64.img** avec l'icône en forme de dossier puis spécifiez l'emplacement de la carte SD dans la colonne **Device**. Ne vous trompez pas sous peine d'effacer le contenu d'un de vos disques durs ! Faites **Write** et attendez la fin du processus. Notez que pour revenir en arrière et récupérer une carte en FAT32, il faudra passer par le logiciel gratuit MiniTool Partition Wizard.



UNE FOIS INSTALLÉ EN VERSION COMPLÈTE, KALI LINUX PROPOSE DES LOGICIELS TRÈS AXÉS SUR LE HACKING. ATTENTION, CE N'EST PAS UN OS POUR LES HORS-LA-LOI, MAIS PLUTÔT POUR LES CURIEUX OU POUR CEUX QUI VEULENT SÉCURISER AU MIEUX LEUR PETIT MONDE INFORMATIQUE...



LES RAILS MÉTALLIQUES DERRIÈRE LA TRAPPE AMOVIBLE PERMETTENT DE PLACER D'AUTRES MODULES, MAIS SURTOUT LE RASPBERRY PI. LES AIMANTS SONT TRÈS PUISSANTS ET L'OUVERTURE SUR LE CÔTÉ PERMET D'AVOIR ACCÈS AUX PORTS USB ET RJ45. L'UNIQUE ALIMENTATION (POUR L'ÉCRAN ET LE RASPBERRY) N'EST PAS MICRO-USB, MAIS AU FORMAT JACK 5 MM. LE BOUTON DE MISE EN MARCHÉ EST UN PEU RAIDE PAR CONTRE LA TIGE EN MÉTAL AU DOS PERMET D'INCLINER LE PI-TOP CEED SUR 65°.





03 > BRANCHEMENT ET LANCEMENT

Il est temps de brancher le Raspberry Pi et de démarrer le système. Le login est **root** et le mot de passe est **toor**. Normalement la carte SD sera redimensionnée pour profiter de tout l'espace de stockage. Faites en sorte de mettre le clavier en Français (**Settings>Keyboard**). Attention, l'interface et les menus resteront en anglais. Ouvrez un terminal et faites **apt-get update** puis **apt-get install kali-linux-full** pour télécharger le build complet de Kali Linux (utilisez la même commande avec **--fix-missing** si vous avez des erreurs). Devrait ensuite s'ensuivre une longue session de téléchargement et d'installation (plus de 5Go). À la fin, vous retrouverez WireShark, John The Ripper, nmap, Hydra, Aircrack, SQLMap et tous les autres logiciels de cette distribution !

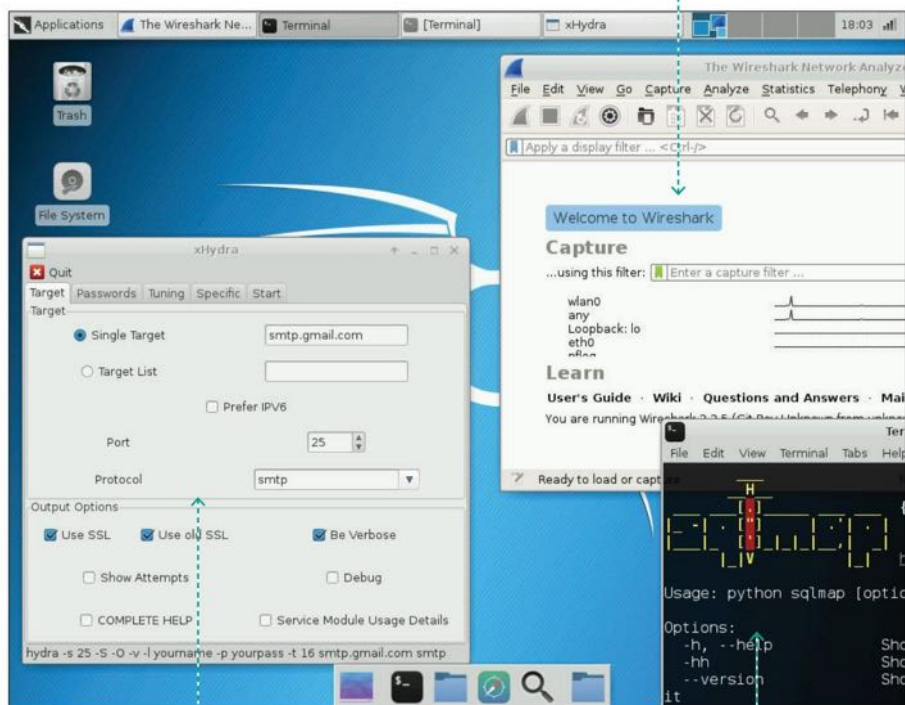


LE CEED EST PLUS FACILE À
MONTER QUE SON GRAND FRÈRE
LE PI-TOP. IL EST DISPONIBLE EN
VERT OU GRIS ANTHRACITE.



04 > KALI EN VERSION COMPLÈTE

Wireshark est un logiciel d'audit réseau. Il est capable d'analyser tous les paquets qui transitent sur votre réseau domestique ou pro. En utilisant ce logiciel vous pourrez intercepter diverses informations. Il s'agit bien sûr de voir si votre réseau est perméable ou pas...



Hydra (ici son interface graphique hydra-gtk) permet de cracker des mots de passe en utilisant la technique brute force ou un dictionnaire de sésames. Un outil très puissant pour vérifier votre propre sécurité bien sûr... Si cela vous intéresse, nous venons de faire un article de présentation de ce logiciel dans ce magazine.



SQLMap est un logiciel d'automatisation d'injection SQL. Il s'agit d'une attaque permettant d'envoyer du code dans un formulaire qui pourra être interprété comme un sésame valide.

BEST-OF APPLIS 2019

MINI PRIX 3,90 €

LE GUIDE DES APPLIS INDISPENSABLES... ET GRATUITES! 

Android

Mobiles & Tablettes

MT

AVRIL - JUIN 2019

+ 30 ASTUCES & TUTOS INCLUS

BEST-OF 2019

480 APPLIS GRATUITES!

☒ TESTÉES ☒ APPROUVÉES!

+ 68 JEUX ADDICTIFS

31 TRAVAIL & BUREAUTIQUE **36 SÉCURITÉ & VIE PRIVÉE** **36 SPORTS & SANTÉ** **28 FUN & INSOLITE** **51 VIDÉOS & MUSIQUE** 



**CHEZ VOTRE MARCHAND
DE JOURNAUX**



AIRMORE, VOTRE SMARTPHONE TOUT ENTIER DANS VOTRE ORDI !

POUR QUI ?

Pour tout le monde !

POUR QUOI FAIRE ?

Accéder à tous les fichiers de votre smartphone depuis votre ordinateur et les gérer gratuitement, sans fil et sans rien télécharger. Et bien plus encore...

Transférer ses fichiers entre son smartphone et son ordinateur n'a jamais été aussi simple.

Marre de la nouvelle version trop complexe de WeTransfer ? Pas satisfait des autres services de transfert de fichiers ? Avec une simple connexion WiFi (ou même sans, si vous avez un smartphone Android), AirMore va vous faciliter la vie. Gratuit, multi-plate-forme (PC, Mac, Linux, Android & iOS), sans aucune installation ni inscription, En plus d'être un bon gestionnaire de fichiers mobile, AirMore vous permet de voir, organiser, modifier, supprimer tous les contenus de votre smartphone depuis un navigateur Web.

DES PETITS PLUS INGÉNIEUX

Avec une ergonomie irréprochable, ce service de l'entreprise hong-kongaise Apowersoft est un véritable couteau suisse de la gestion de fichiers. Et si vous lui demandez gentiment, il peut même émuler votre smartphone sur le web, synchroniser vos notes entre tous vos appareils et vous permettre de stocker des fichiers dans le cloud. Et il fonctionne aussi entre plusieurs smartphones. Que demander de plus ?

**LEXIQUE*****HOTSPOT : :**

Il s'agit d'un point d'accès sans fil pour se connecter à internet.



EN REVANCHE, POUR OBTENIR PLUS D'ESPACE DE STOCKAGE, IL VA falloir se mettre AU CHINOIS...



GÉRER TOUS LES FICHIERS DE VOTRE SMARTPHONE DANS VOTRE NAVIGATEUR

PRATIQUE


01 > SE CONNECTER À SON SMARTPHONE VIA SON NAVIGATEUR

Installez l'appli AirMore sur votre smartphone et rendez-vous sur web.airmore.com sur le navigateur de votre ordinateur. Scannez le QR code avec votre smartphone. Pas de wifi ? Connectez votre ordinateur au réseau hotspot fourni par l'application, puis entrez l'adresse indiquée dans votre navigateur (Android seulement). Si vous avez des problèmes (et un smartphone Android 1.2.0 ou plus), cliquez sur les trois points en haut à droite de l'application sur votre smartphone, puis recopiez l'adresse IP indiquée



dans votre navigateur. Vous n'y arrivez toujours pas ? Là, on ne peut plus rien pour vous...

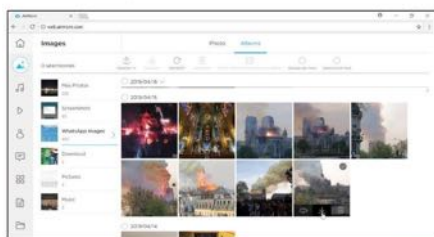
02 > GÉRER TOUS LES FICHIERS DE SON SMARTPHONE SUR SON ORDINATEUR

En quelques secondes, vous pouvez voir vos **contacts**, vos **fichiers multimédias**, vos **messages**, vos **applis** et toute l'arborescence de votre mémoire interne ou carte SD. Profitez aussi d'un compte rendu de l'état de votre smartphone : version d'Android, état de la batterie, appareil noté ou non, numéro de série, etc.



03 > PROFITER DES CONTENUS DE SON SMARTPHONE SUR SON ORDINATEUR

Vous avez pris 3 000 photos en Italie avec votre smartphone et vous voulez les montrer à votre meilleure amie au plus vite ? AirMore vous permet de visionner tous vos contenus multimédias sans avoir à les télécharger, directement depuis web.airmore.com. Vous pouvez aussi télécharger, organiser ou supprimer tous vos fichiers ou dossiers, et même en importer depuis votre ordinateur vers votre smartphone.



LA SUITE APOWERSOFT



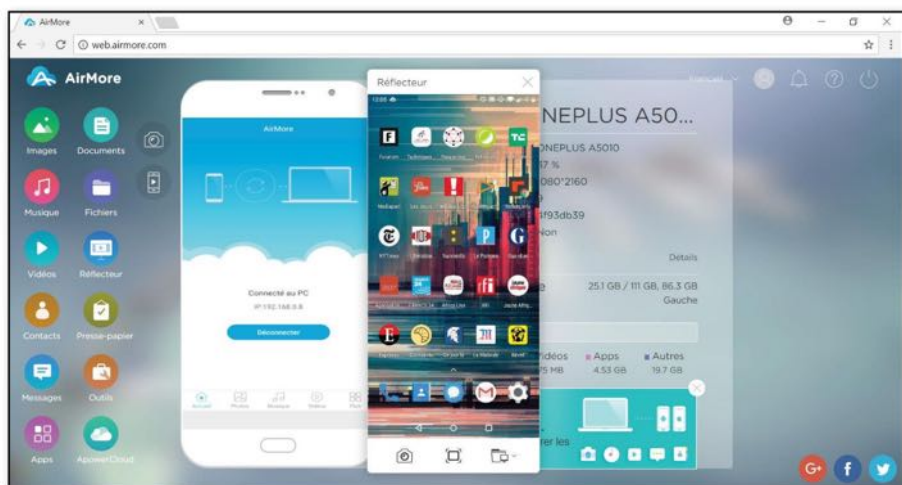
Si toutes les autres fonctions ne nécessitent que l'appli mobile AirMore, d'autres encore sont disponibles sous la marque Apowersoft, mais elles demandent un peu plus d'engagement de la part de l'utilisateur. ApowerCloud, la plus intéressante, propose de stocker jusqu'à 1 Go de données sur le cloud mais requiert une inscription. D'autres outils, comme ApowerManager, un logiciel de gestion des données mobile, sont téléchargeables

Lien : www.apowersoft.fr/gestionnaire-smartphone



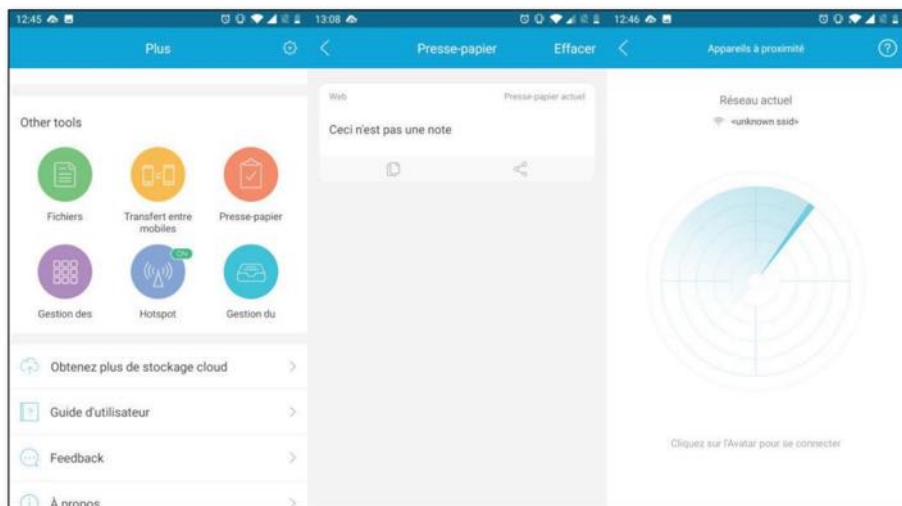
04 > UN ÉMULATEUR DE VOTRE SMARTPHONE EN PLUS !

AirMore propose aussi un mode miroir grâce auquel vous pouvez recevoir, en temps réel, l'image du bureau de votre téléphone sur votre ordinateur, et faire des captures d'écran. Si jamais vous faites un exposé sur les applis de rencontre...



05 > ET ENCORE D'AUTRE OUTILS...

Ajoutez des notes dans votre **presse-papier** sur web.airmore.com, elles s'enregistreront directement sur votre téléphone. Transférez des fichiers entre plusieurs téléphones grâce au réseau hotspot en vous connectant sur l'appareil qui apparaît sur le radar. Pour encore plus de possibilités, voir l'encadré (mais là, il faudra s'inscrire, ou télécharger des applications tierces).





Contourner la vérification de licence > AVEC LUCKY PATCHER

Lucky Patcher va simplement contourner la vérification des licences sur votre machine Android pour lancer les applis que vous avez déjà achetées (ou que vous ne voulez pas payer tout de suite). Téléchargez et installez Lucky Patcher sur votre appareil rooté (avec la BusyBox d'installée). Installez l'APK de l'application que vous convoitez, mais surtout ne la démarrez pas. Utilisez le mode **Auto** et attendez que Lucky Patcher aille chercher le patch adéquat. Selon l'appli, il vous sera peut-être demandé de copier à la main les dossiers d'une licence dans `/sdcard/Android/Obb`. Lucky

Patcher ne fonctionne pas avec votre fichier APK ? Pas de panique, les développeurs ajoutent des patches tous les jours !

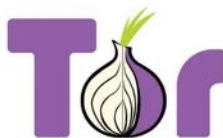
Lien : <http://lucky-patcher.netbiew.com>



Tor dans une clé USB > AVEC THE PORTABLE FREWARE

Si vous voulez faire découvrir Tor à un ami ou si vous ne pouvez pas installer de logiciels sur l'ordinateur que vous voulez utiliser (cybercafé, travail, impossibilité, etc.), la solution passe par la version de Tor Browser compilée par The Portable Freeware, un site regroupant plein de logiciels conçus pour fonctionner sans installation depuis une clé USB. Téléchargez l'EXE et placez-le sur une clé USB. Attention, n'ajoutez pas d'extension supplémentaire sous peine de mettre en péril votre anonymat.

Lien : <https://goo.gl/36kyXH>



Détecter une partition chiffrée

> AVEC ENCRYPTED DISK DETECTOR

Le logiciel Encrypted Disk Detector permet de rechercher les partitions chiffrées qui seraient éventuellement contenues dans un disque dur, une clé USB ou une carte mémoire. Il va analyser la zone d'amorçage du périphérique pour déterminer une probabilité qu'une partition soit chiffrée avec TrueCrypt, PGP, Safeboot ou BitLocker. Attention, il ne détecte pas les conteneurs, mais uniquement les partitions (y compris cachées). Elles seront affichées en jaunes. Et pour ceux qui souhaitent chercher aussi les conteneurs chiffrés (mais uniquement issus de TrueCrypt), vous pouvez aussi utiliser TCHunt : <http://goo.gl/kUWMS0>

Lien : www.magnetforensics.com



Plusieurs OS sur une clé USB > AVEC MULTIBOOTUSB

Si vous êtes un petit curieux et que aimez jongler entre différentes distributions Linux (LiveCD/USB ou pas), vous connaissez sans doute déjà Rufus, Yumi ou XBoot, mais peut-être pas MultiBootUSB. Ce logiciel sous Windows et Linux permet de placer des ISO sur une clé USB en vue de charger différents systèmes : d'autres distrib' Linux, mais aussi des DVD de réparation ou de diagnostic (Hiren's Boot CD, AVG Rescue CD, Ultimate Boot CD, etc.). Les utilisateurs de Windows qui veulent aussi jongler avec les versions de l'OS de Microsoft peuvent faire la même chose avec WinToFlash.

Lien : <http://multibootusb.org>



Un appareil Androids sous contrôle total > AVEC KERNEL MANAGER

Vous êtes l'heureux possesseur d'un mobile rooté et vous cherchez une boîte à outils pour exploiter tout le potentiel de votre appareil ? L'application Kernel Manager est la réponse à votre problème. Le



nombre d'options de paramétrage est ahurissant : changer la fréquence du CPU, mettre l'appareil en sous-tension ou en surtension, modifier l'intensité du vibreur, gérer le niveau sonore du casque et du haut-parleur du téléphone, etc.

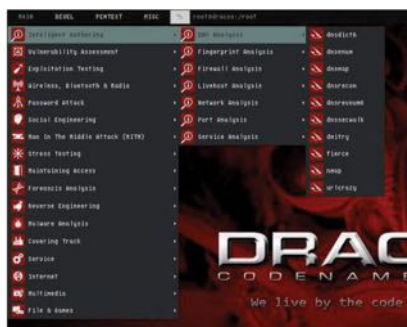
Fonction intéressante, la possibilité de créer des profils d'utilisateurs, pour adapter tous ses paramètres selon l'usage (quotidien, économie d'énergie, performance, etc.). Une appli très complète, qui demande néanmoins des connaissances techniques sur Android.

Lien : <https://goo.gl/1roKBE>

Pentesting en ligne de commande > AVEC DRACOS

Si Kali Linux est devenu trop «casu» pour vous depuis qu'on peut l'installer sans avoir BAC +23, Dracos est fait pour vous ! C'est une distribution Linux qui, comme Kali, se concentre sur le côté pentesting et sécurité sauf que cette dernière ne s'utilise qu'en ligne de commande. A voir absolument si vous êtes un vrai barbu !

Lien : <https://dracos-linux.org>



Formater en FAT32 un disque dur de plus de 32 Go > AVEC FAT32FORMATTER

Le problème avec les disques durs de plus de 32 Go, c'est que vous ne pouvez pas les formater en FAT32 sous Windows. Pourtant, le format NTFS n'est pas compatible avec tous les systèmes. Imaginez que vous vouliez utiliser votre disque dur sur un Mac ou un Media Center... Pour résoudre ce problème, il suffit de télécharger le logiciel Fat32Formatter, de décompresser l'archive puis de le lancer. Sélectionnez ensuite votre disque dans la liste, cochez la case **Quick Format** puis cliquez sur **Start**. Plus de problème !

Lien : <http://project-rainbowcrack.com>





POUR QUI ?

Pour les pros qui
veulent un cloud
abordable

POUR QUOI
FAIRE ?

Pour stocker vos
fichiers sensibles
dans un espace
sécurisé

CLOUD : UN CLOUD CHIFFRÉ POUR LES PROS !

Il y a peu de solutions qui permettent aux professionnels de stocker de manière chiffrée leurs documents. Les services gratuits sont rarement adaptés aux besoins des entreprises tandis que les solutions pros sont parfois trop complexes à appréhender. Il est de surcroît dangereux de compter uniquement sur une solution en local à cause des ransomwares et autres saletés. Pour ces TPE/PME, Cloud propose un solution sur-mesure à un prix abordable.

LEXIQUE

*RSA 2048
BITS :

Le chiffrement RSA (nommé d'après le nom de ses inventeurs : Rivest, Shamir et Adleman) est un algorithme de cryptographie asymétrique utilisant les nombres premiers pour la création des clés. Pour casser cet algorithme, il faudrait réussir à factoriser un nombre de 617 chiffres. Une récompense de 200 000 \$ est offerte à celui qui réussira...



Les infections et les ransomwares sont devenus la bête noire des entreprises. En faisant confiance à une sauvegarde en local sur un petit serveur ou sur un simple disque dur, les TPE/PME se mettent en danger, car le chiffrement ne met pas à l'abri d'un chiffrement malicieux supplémentaire. Et c'est sans compter les vols de matériel ou les erreurs de manipulation. Rien ne vous empêche d'utiliser une solution locale, mais le cloud a plusieurs avantages. Le seul hic c'est que le chiffrement est souvent absent et qu'on ne sait jamais vraiment où sont les données...

POURQUOI CELUI-LÀ ET PAS UN AUTRE ?

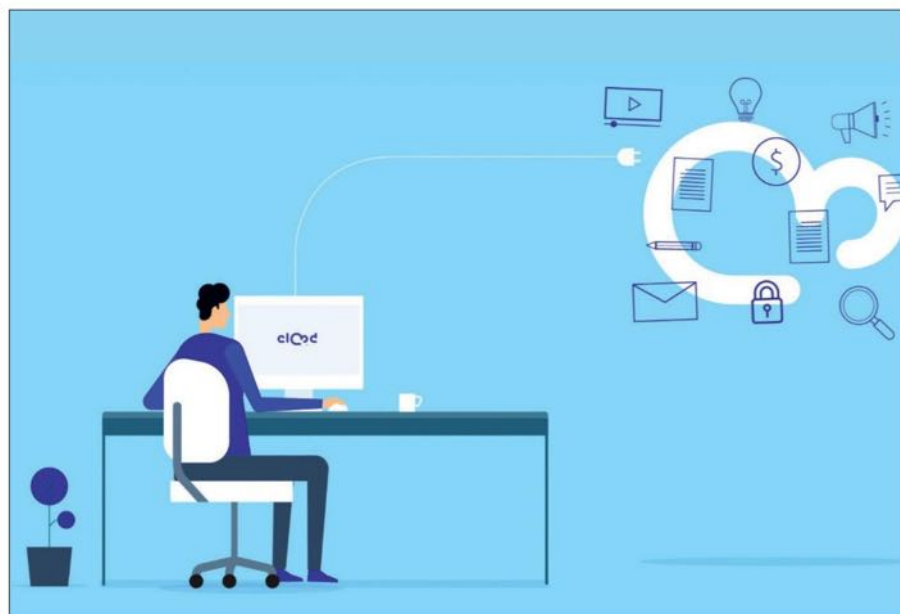
Clood est un service pensé pour les petites et moyennes entreprises et les micro-entrepreneurs pour stocker des documents importants : fiches de paye, comptabilité, feuille de présence, contrats, etc. Clood est aussi localisé en France et géorépliqué dans notre beau pays : cela veut dire que vos données sont stockées dans plusieurs endroits à la fois, mais toujours sur le territoire national. Cela garantit l'intégrité de vos données même en cas d'attaque de sauterelles, d'épidémie de gale afghane, de tremblement de terre ou de panne d'un des serveurs. Vos données sont aussi à l'abri de nos belles lois européennes comme la GPRD. Un ransomware a sévi dans les ordinateurs de votre entreprise ? Pas de problème puisque Clood est loin (genre en Auvergne ou à Vesoul) et même en cas de «boulette», il gère très bien le «versioning» (gestion de versions). Une attaque des «Chinois du FBI» ? Avec du RSA 2048 bits, le club des ninjas du 13^{ème} arrondissement pourra s'amuser quelques siècles sur votre clé solide comme un pilier All Blacks sous MDMA.

MAIS COMBIEN ÇA COÛTE ?

Clood propose 2 formules : une à 24€ HT/mois pour 100 Go et une autre à 99€ HT/mois pour 500 Go. Il est aussi possible de demander une offre sur-mesure et d'accéder à un compte de démo pour tester le service, mais il faut demander gentiment !



**CLOUD STOCKE ET CHIFFRE
VOS DOCUMENTS DANS PLUSIEURS
SERVEURS EN FRANCE...**





CLOUD : UNE INTERFACE CLAIRE...

PRATIQUE


01 > L'INSCRIPTION

Pour utiliser Clood, il suffit de s'inscrire comme avec n'importe quel service en ligne. Vous pouvez aussi demander un essai si vous venez de notre part...



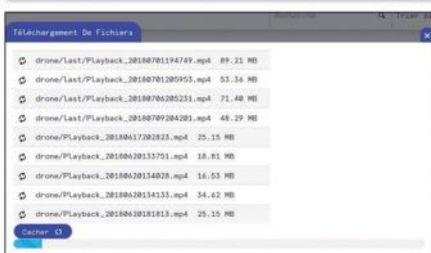
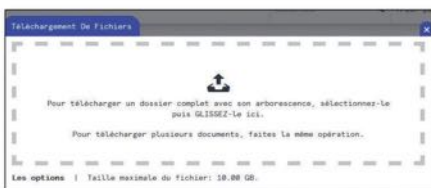
02 > L'INTERFACE

Le tableau de bord est très simple : combien il vous reste d'espace, liste de vos fichiers, etc. Invitez vos collaborateurs à travailler sur vos fichiers... Le chiffrement est géré par le site : vous n'avez rien à faire.



03 > L'UPLOAD

Pour uploader il suffit de glisser-déposer vos fichiers. Avec notre connexion pourrie, nous avons mis 380 Mo à l'abri en une demi-heure. Attention, les fichiers ne peuvent pas dépasser 10 Go, mais vous pouvez faire des dossiers pour regrouper des fichiers.



Interview de Esteban Mauvais, CTO et co-fondateur de Clood



Esteban Mauvais, qui écrit parfois des articles dans nos pages quand il ne fait pas de jardinage avec son Raspberry Pi ou qu'il ne trolle pas son monde sur LinkedIn, est le CTO et co-fondateur de Clood. Il répond à nos questions...



COMBIEN DE PERSONNES TRAVAILLENT CHEZ CLOUD ET COMMENT EST PARTIE CETTE AVENTURE ?

Actuellement nous sommes 5 personnes à travailler chez Cloud. Christophe (CEO et cofondateur) s'occupe de la stratégie et du business development. Kevin s'occupe de faire coller la stratégie de développement aux ressources disponibles. Florian et moi-même sommes en charge de l'ensemble des développements produit. Notre objectif est de le faire évoluer au fil du temps pour coller à 100% avec nos valeurs : transparence, sécurité, assistance ! Nous travaillons avec une agence de communication pour le marketing, mais nous attendons une sixième personne qui viendra prendre le relais sur ces sujets.

Il y a 1 an, nous lançons Monkey Co avec Florian et étions à la recherche de projets innovants, et à forte capacité de croissance. Notre objectif était de devenir CTO externalisé afin de voir évoluer un projet dans le temps. Nous avons reçu plusieurs centaines de propositions en quelques jours ! Parmi les propositions, celle de Christophe et Kevin avec l'ambition de développer un cloud français, simple et intuitif, avec une nouvelle technologie de chiffrement et de stockage de données qui permettait d'assurer un niveau de protection inédit des documents des entreprises. Le projet nous a de suite plu, car il venait répondre à une véritable problématique actuelle, et le sérieux de l'équipe nous a convaincus. Après quelques réunions téléphoniques et un après-midi de brainstorming dans un bar, la collaboration commençait !



À QUI EST DESTINÉ CLOUD ?

Il faut savoir déjà que Cloud émerge d'un constat : la sécurisation de la donnée dans les TPE/PME est très souvent reléguée au second plan. Pourquoi ? Parce que la digitalisation des données s'est faite brutalement. Avec Cloud nous avons souhaité offrir une solution à la portée de tous, initiés ou pas. Nous mettons à disposition de nos utilisateurs un moyen sécurisé de stocker leurs documents professionnels. Le tout sur une interface épurée et intuitive. Nous avons vu beaucoup trop d'usines à gaz lors de notre étude de l'offre existante.

En bref, notre promesse est simple : Tu es une startup, un indépendant, une TPE, une PME ? Tu n'as pas envie que tes données finissent n'importe où ? Tu as envie d'avoir de la visibilité sur ce que deviennent tes données une fois dématérialisées ? Viens chez Cloud ! On te promet de la transparence (tout est stocké sur des serveurs dans nos belles campagnes françaises), de la réactivité (t'as un problème ? Tape notre 05 et une personne de notre équipe te répond directement), et de la sécurité (nous sommes certains de la fiabilité de notre produit, vous pouvez y aller !). Cloud est en plus spécialement conçu pour le partage et la collaboration. Un onboarding en 4 clics et une gestion des partages hyper intuitive.



ON ENTEND PARLER DE CLOUD DEPUIS DES ANNÉES, POURTANT LES PETITES ENTREPRISES ONT DU MAL À S'Y METTRE, COMMENT VOUS EXPLIQUEZ CELA ?

Je pense qu'il y a plusieurs raisons à cela. D'abord cela est probablement dû à la mauvaise réputation

des clouds existants en matière de sécurité de la donnée et de leurs politiques de confidentialité. Qui n'a pas entendu parler du « Patriot Act » qui permet au gouvernement US de lire tous les documents des entreprises ? Quand on sait que la plupart des acteurs du cloud sont américains, on comprend que les entreprises n'aient pas vraiment envie de leur confier leurs documents... C'est pour ça que Cloud est français, c'est pour ça que Cloud stocke les documents des entreprises sur des serveurs français, et c'est pour ça que Cloud respecte les lois françaises, dont le fameux RGPD. Les clouds sont aussi trop techniques. Les chefs d'entreprise dont ce n'est pas le métier et n'ayant pas de spécialiste informatique au sein de leurs équipes ne s'intéresseront pas d'eux-mêmes au cloud. C'est pour ça que Cloud est là !



SI LE CLIENT DISPARAIT DANS LA NATURE, VOUS LUI DONNEZ COMBIEN DE TEMPS AVANT DE SUPPRIMER LES DONNÉES ?

Les tarifs de Cloud sont mensuels, sans engagement, sans limites d'utilisateurs. Les clients peuvent stopper à tout moment sans justificatif. Tant que le règlement est effectué, nous conservons les données. Dans le cas contraire, en cas de cessation de paiement, nous prévenons par mail et téléphone l'entreprise afin de leur permettre d'extraire leurs données. Dans notre politique d'utilisation, il est stipulé que les données sont conservées 6 mois après cessation de paiement. Au-delà de ce délai, nous nous donnons le droit de les supprimer.



COMMENT FONCTIONNE LE CHIFFREMENT ET POURQUOI NE PAS AVOIR OPTÉ POUR UN CHIFFREMENT DE BOUT EN BOUT ?

Nous avons choisi de lancer Cloud avec les fondamentaux d'un cloud : stockage et partage collaboratif, pour une question de temps. Le chiffrement de bout en bout n'est pas encore présent pour des raisons techniques comme la prévisualisation des documents, le partage du cloud et surtout pour ne pas perdre les données en cas de perte de mot de passe. Une alternative arrive avec un chiffrement de bout en bout sur des clés dossiers.



L'APPLI MOBILE, C'EST PRÉVU ?

Très clairement oui, cependant une application bureau (Windows, Mac et Linux) sera présentée en priorité.



C'EST QUOI LA PROCHAINE ÉTAPE CHEZ CLOUD ?

La prochaine étape, ou plutôt les prochaines étapes, car chez Cloud on a plein d'idées ! D'un point de vue technique : développer la sauvegarde par version, le chiffrement de bout en bout, la synchronisation et un gestionnaire de mots de passe... D'un point de vue stratégique : consolider notre présence sur le marché français en faisant grandir le nombre d'entreprises clientes de Cloud. Nous avons pour ambition de devenir le partenaire privilégié des TPE/PME françaises !

**POUR QUI ?**

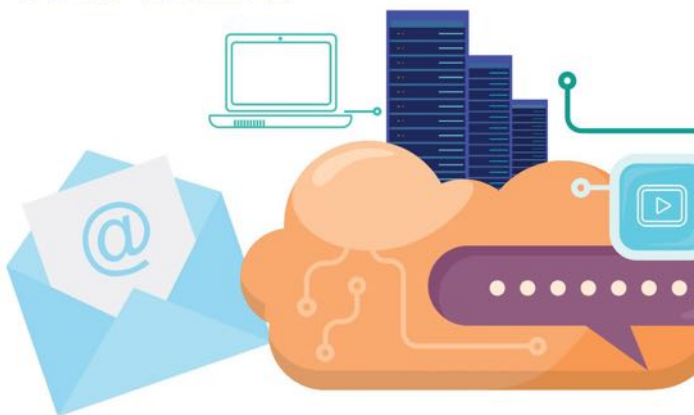
Pour les utilisateurs qui veulent un e-mail chiffré sans avoir fait BAC+12

POUR QUOI FAIRE ?

Profiter d'un e-mail sécurisé sans avoir à forcément payer...

TUTANOTA : LA NOUVELLE VERSION QUI RÉVOLUTIONNE L'E-MAIL !

Tutanota est un webmail qui propose un chiffrement de bout en bout avec la possibilité d'inviter une personne sans que celle-ci n'ait de compte. C'est ingénieux, mais Tutanota vient de signer une nouvelle version avec des fonctionnalités encore plus intéressantes sur ordinateur et sur mobile...

**LEXIQUE*****CHIFFREMENT DE BOUT EN BOUT :**

Ou «end-to-end» dans la langue de Kim Kardashian (l'anglais pas le hobbist, suivez un peu !). Il s'agit d'un système de communication où seules les personnes impliquées peuvent lire les messages échangés. Il évite le problème d'écoute électronique, car les clés ne sont pas échangées sur le réseau.

Tutanota est un service de Webmail situé en Allemagne et qui propose un chiffrement de bout en bout en local. Cela veut dire que tout le processus de chiffrement se fait depuis chez vous, sur votre navigateur. Impossible pour les personnes de Tutanota de savoir de quoi vous parlez ou pour un pirate de glaner des informations vous concernant : vos données vous appartiennent qu'il s'agisse de vos écrits ou de votre carnet d'adresses.

LA RECHERCHE DANS LES E-MAILS CHIFFRÉS : IMPOSSIBLE ? PAS AVEC TUTANOTA

Tutanota permet de communiquer de manière chiffrée avec un correspondant qui n'est pas inscrit au service (voir notre n°35). Mais depuis peu, le client Tutanota a fait peau neuve. Non seulement le design est plus joli, mais l'architecture a été changée pour rendre l'interface plus rapide. Plus joli, plus rapide, c'est bien. Mais il y a une chose qui est très rare chez les services de ce type, c'est la recherche dans les e-mails. À cause du chiffrement, cette fonctionnalité est très difficile à mettre en œuvre. Pourtant cette nouvelle version de Tutanota s'acquitte très bien de cette tâche. Il faudra juste laisser



le temps à l'appli de prémâcher le processus. Plus vous avez d'e-mails et plus la recherche sera longue, mais cela reste tout de même très pratique.

SUR MOBILE ET DESKTOP

Et comme on aime bien la nouveauté chez Tutanota, non seulement le service offre la même chose sur mobile (Android et iOS), mais les développeurs proposent maintenant un client desktop (Windows, Mac, Linux) pour ceux qui sont allergiques aux interfaces Web. Et bien sûr vous pouvez toujours communiquer chiffré avec des correspondants qui ne disposent pas de Tutanota grâce à un astucieux système de mot de passe...





LE CLIENT DESKTOP DE TUTANOTA

PRATIQUE

01 > L'INSTALLATION

Disponible pour les PC sous Windows, Linux, mais aussi sous MacOS, le client est disponible en utilisant notre lien. Si vous avez un compte, vous n'avez qu'à entrer vos identifiants, mais si ce n'est pas le cas vous pouvez vous inscrire depuis le logiciel. Après avoir rentré votre code de vérification, votre navigateur va alors générer votre couple de clés. Tapez une nouvelle fois votre mot de passe pour être dirigé vers l'interface principale.

02 > LES PARAMÈTRES

Comme sur le webmail classique, vous aurez une boîte de réception, d'envoi, un filtre à spam, une liste de contacts et la possibilité d'attacher une pièce jointe. Il est aussi possible depuis Paramètres (dans le menu aux trois barres horizontales en haut à droite) de changer de mot de passe, vérifier les heures des précédentes connexions et les tentatives ratées d'accéder à votre boîte (pratique pour savoir si un tiers a tenté de vous pirater), comprises dans l'offre payante) et le nombre de Go qu'il vous reste.

Client	Dernier accès	Adresse IP
Firefox Browser	18 04	
<Ce client>	18 04	
Firefox Desktop	ven. 22 jan 201...	77.151.95.33
Firefox Desktop	ven. 22 sept 20...	77.151.95.33

Le client et l'adresse IP ne sont stockés que chiffrés.

Sessions fermées

Celui-ci seront supprimés 2 semaines après fermeture.
Le client et l'adresse IP ne sont stockés que chiffrés.

MOBILE ANDROID : SUR LE PLAY STORE OU SUR F-DROID...



Fidèle à son idéal de discrétion et de respect de la vie privée, l'appli Tutanota pour Android est maintenant disponible sur le store alternatif F-Droid pour éviter de passer par la case «Google» (voir notre article page XX). Le service est bien sûr gratuit, mais en optant pour une version payante, vous pourrez avoir un domaine perso, entre 5 ou 20 alias, un support personnalisé, un formulaire de contact chiffré à implémenter sur votre site et jusqu'à 10 Go d'espace de stockage. Il faudra cependant déboursier entre 1,20 € et 6 € par mois (avec 2 mois offerts si vous payez à l'année). Tentez la version gratuite, cela n'engage à rien ! Lien : <https://f-droid.org/fr/>



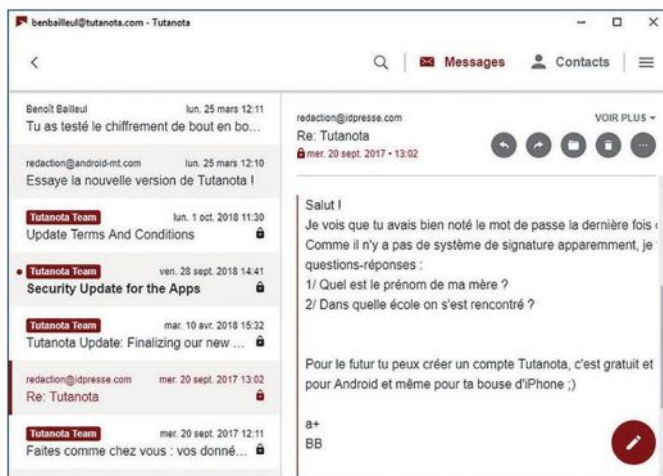
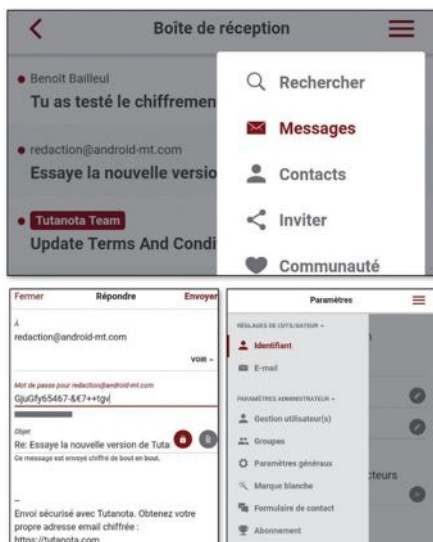
03 > VOTRE E-MAIL : CHIFFRÉ OU PAS !

En bas à droite, cliquez sur le stylo puis écrivez votre message. De base, il sera chiffré pour les utilisateurs de Tutanota, mais si le service détecte que votre correspondant n'utilise pas Tutanota, il vous demandera alors un mot de passe pour que votre ami puisse lire votre message. Votre correspondant recevra un e-mail avec un lien. Il faudra qu'il clique dessus puis qu'il rentre le mot de passe que vous lui aurez communiqué. Il peut mettre en mémoire ce dernier s'il se connecte d'un ordinateur privé. Il pourra même vous répondre depuis son navigateur. Le même mot de passe sera utilisé pour ce correspondant donc pas besoin d'échanger 50 sésames différents. Mais si vous désirez envoyer un message «normal» c'est aussi possible : il suffit de cliquer sur le cadenas pour supprimer le chiffrement. Notez que les pièces jointes sont aussi chiffrées.



04 > SUR MOBILE AUSSI !

Et sur mobile Android ou iOS ? C'est pareil ! Si vous avez beaucoup d'e-mails, la recherche à l'intérieur des messages chiffrés peut prendre un peu plus de temps, mais toutes les fonctionnalités sont là !



TUTANOTA SE PRÉSENTE COMME UN CLIENT MAIL NORMAL. L'INTERFACE EST EN FRANÇAIS ET TOUTES LES FONCTIONNALITÉS SONT EXPLIQUÉES TRÈS SIMPLEMENT. LA RECHERCHE DANS LES E-MAILS EST UNE EXCLUSIVITÉ DE TUTANOTA !



POUR QUI ?

Pour les curieux
qui veulent
essayer un VPN de
qualité sans payer
immédiatement

POUR QUOI FAIRE ?

Reste anonyme
sur Internet, se
protéger des
malwares lors
d'une connexion
sauvage et
changer d'IP

GRATUIT OU PAYANT WINDSCRIBE : UN DES MEILLEURS VPN...

De nos jours, les VPN sont de plus en plus populaires. Windscribe se démarque des autres par de nombreuses fonctionnalités fort sympathiques, une offre gratuite confortable ainsi qu'un accent sur le respect de votre vie privée. L'utilisant depuis maintenant 6 mois, j'ai décidé de vous faire partager mon expérience d'utilisation et mon avis sur ce service...

Merci à Baptiste G. pour cet article - <https://blog.baptiste0928.net/>

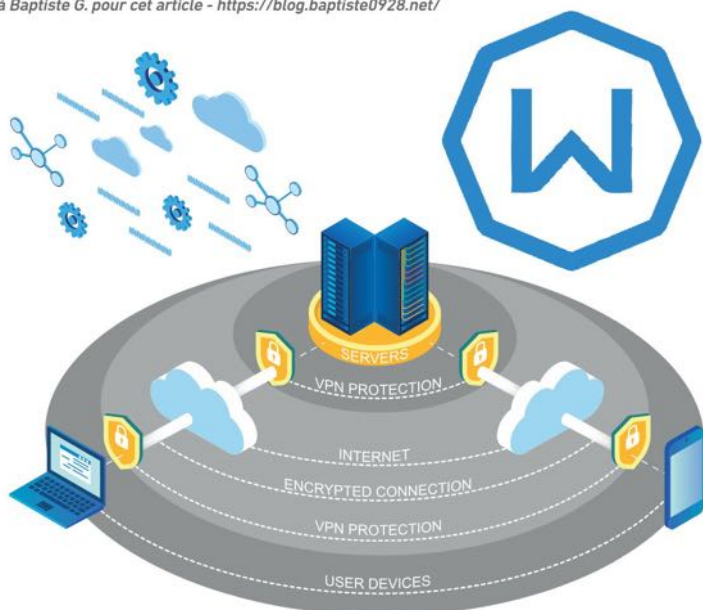
LEXIQUE

*VPN :

Un Virtual Private Network est un service qui va chiffrer les données qui circulent entre vous et Internet. Cela permet d'éviter l'espionnage, de protéger son emplacement, de se connecter depuis des points d'accès inconnus, de rester anonyme sur Internet et de contourner les bridages et la géolocalisation de certains sites (Netflix, Hulu, Play Store, etc.)

*FIVE EYES :

Ce terme désigne un accord entre les services secrets de 5 pays : Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis.



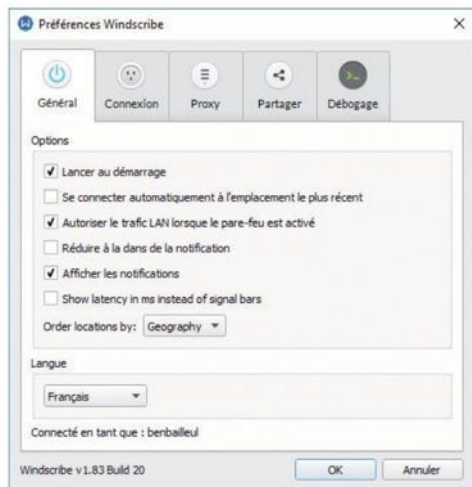
PWindscribe est un VPN basé au Canada (oui ce pays fait partie des Five Eyes, mais puisqu'un VPN ne peut être considéré comme un FAI et qu'il ne garde aucune donnée, il peut difficilement collaborer avec les services secrets). Le service propose également une extension de navigateur, proposant de nombreuses fonctionnalités pour protéger votre vie privée. Il existe une offre gratuite ainsi qu'une version Pro, facturée 49\$ par an (43,50 € ou 3,55 €/mois). Comme une liste est beaucoup plus claire qu'un long texte, voici les principales fonctionnalités de Windscribe :

- 60 pays disponibles (10 gratuitement), pour un total de plus de 120 villes.
- Données illimitées (10 Go/mois dans l'offre gratuite)
- Aucun log pouvant vous identifier, chiffrement solide (AES-256 + authentification SHA512 + clé RSA 4096 bit)
- R.O.B.E.R.T. : Filtrage des IP pour bloquer les malwares, les publicités et bien plus
- Générateur de configurations pour l'utiliser sur tous vos appareils (uniquement en Pro)
- IP statiques à partir de 2\$/mois
- Redirection de port

L'application de bureau ajoute un pare-feu pour bloquer les fuites de données hors du VPN, la possibilité d'utiliser un point d'accès WiFi passant par le VPN et un proxy local pour vos autres appareils. L'extension de navigateur propose une double connexion avec l'application bureau, le blocage des publicités et des trackers, la modification du fuseau horaire par celui du pays où vous êtes connecté, la suppression des cookies à la fermeture des onglets, un raccourcisseur d'URL et un agent utilisateur aléatoire pour brouiller les pistes. Ce dernier point est très intéressant, car il permet de ne pas laisser d'empreinte unique de votre activité. Car même derrière un VPN, on peut savoir quel navigateur, quel type de clavier ou OS vous utilisez et ces informations peuvent être utilisées contre vous.

UN VPN À PART...

À première vue, il se démarque peu de ses concurrents, mais à y regarder de plus près, on y trouve de véritables avantages. Le premier est certainement R.O.B.E.R.T. Il permet de bloquer les publicités directement à leur racine, et donc il est efficace partout dès que le VPN est connecté. Il est donc possible



LE VPN PROPOSE PAS MAL DE RÉGLAGES, MAIS VOUS POUVEZ LES IGNORER COMPLÈTEMENT : WINDSCRIBE EST DESTINÉ AUX DÉBUTANTS MÊME SI LES FONCTIONNALITÉS SONT NOMBREUSES.

de bloquer les publicités sur la plupart des applications mobiles ou PC. La version 2.0 de cette fonctionnalité a ajouté la possibilité de personnaliser fortement cet outil. Il est possible de choisir une liste de blocages, et de définir des règles personnalisées pour les domaines souhaités. Malheureusement, R.O.B.E.R.T. ne bloque que les malwares en version gratuite et n'est pas personnalisable. Les fonctionnalités de l'extension de navigateur sont également fortement appréciables. Celle-ci, entièrement gratuite, remplace d'autres extensions du même type. Les IP statiques et la redirection de port sont deux fonctionnalités utiles dans certains cas, mais elles sont en supplément et nécessitent un abonnement Pro. La redirection de port, quant à elle, nécessite une IP statique, même s'il est possible d'en configurer une temporairement sur une IP publique. Concernant la vie privée, Windscribe assure ne conserver aucune donnée personnelle, ce qui est confirmé par leur politique de confidentialité.

Windscribe est probablement l'un des meilleurs VPN actuels. Il propose, pour un prix dans la moyenne, de nombreuses fonctionnalités inédites. L'offre gratuite est également très satisfaisante même si avec 10 Go/mois, il faudra surtout l'utiliser lorsque vous n'êtes pas sur votre réseau local ou lorsque vous en avez vraiment besoin. Concernant les points négatifs, certains se plaignent d'une lenteur de connexion, mais cela ne se ressent pas sur les serveurs Pro.



WINSCRIBE : COMMENT SE LANCER ?

PRATIQUE

01 > LE CLIENT WINDOWS

Sur le site, cliquez sur **Get Started** puis **Windows** pour installer le client. Commencez l'installation et lorsque votre pare-feu se réveillera, autorisez l'accès de l'application. Dites que vous n'avez pas de compte et créez-en un. Même si c'est facultatif, entrez votre adresse e-mail pour avoir 10 Go de trafic gratuit au lieu de 2 Go. Notez que vous pourrez avoir 5 Go supplémentaires en faisant la promo du service sur Twitter...



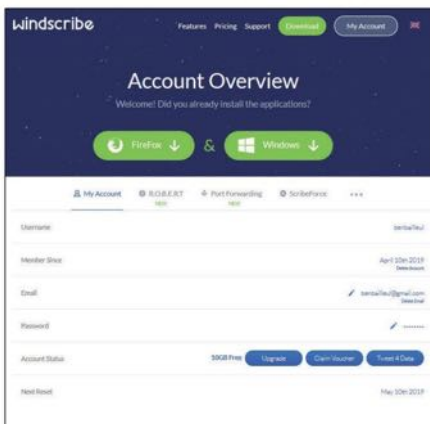
02 > VOTRE PAVILLON DE COMPLAISANCE...

Une fois installé, le programme va se lancer tout seul : mettez-le sur **ON** pour faire passer votre trafic via le VPN. Sur cette petite fenêtre, vous verrez votre nouvelle IP (vous pouvez choisir d'autres destinations même si la plupart sont comprises dans l'offre payante) et le nombre de Go qu'il vous reste.



03 > LE MENU

En cliquant dans le menu avec les trois barres horizontales, vous aurez accès aux Préférences avec les réglages de proxy, de DNS, le mode de connexion, etc. Normalement, vous n'aurez à toucher à rien ici. Dans Mon compte, vous aurez un récapitulatif de votre profil.



04 > VOTRE NOUVELLE IP...

En utilisant des services comme <https://mon-ip.io>, vous verrez que votre lieu de connexion est bien celui indiqué. Notez qu'en optant pour la version payante, le trafic est illimité et vous aurez accès à 100% des fonctionnalités. En payant par mois, vous devrez débours 8€ alors qu'en payant annuellement, l'addition descend à 3,55 €/mois...

Quelle est mon adresse IP ?

185.20.99.216



NOS GUIDES WINDOWS 100% PRATIQUES

POUR UN PC

- + Puissant
- + Beau
- + Pratique
- + Sûr



Chez votre marchand
de journaux

**POUR QUI ?**

Pour ceux qui ne veulent rien avoir affaire avec Google

POUR QUOI FAIRE ?

Éviter le Play Store et profiter d'applis ne nécessitant pas (ou peu) d'autorisations...

F-DROID : UN MAGASIN D'APPLIS LIBRES !



Vous avez un smartphone ou une tablette sous Android, mais vous aimeriez bien vous passer de Google, de son Store, de ses applis et de son tracking permanent. Impossible ? Pas du tout puisque vous pouvez très bien passer par un magasin d'applis respectueux de la vie de chacun et complètement légal...

À la rédaction, nous préférons les mobiles sous système Android aux iPhone. Question d'idéologie : pourquoi choisir un système fermé où vous avez la désagréable impression de ne pas réellement posséder votre appareil ? Mais le problème avec Android c'est Google ! Car même si l'OS cousin de Linux est open source, la tentaculaire compagnie américaine y met son grain de sel. Impossible par exemple d'installer des applications depuis le Google Play Store si vous n'avez pas de compte Google/Gmail : impensable pour les défenseurs de la vie privée. Plutôt que de



risquer la contamination par un malware en téléchargeant les fichiers APK nécessaires à l'installation d'une nouvelle application, nous vous conseillons d'utiliser F-Droid.

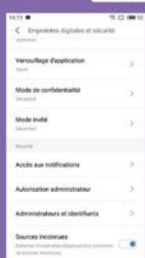
F-DROID : POURQUOI ET POUR QUI ?

Promu par la Free Software Foundation, F-Droid propose des applications qui peuvent être installées à la manière du Play Store, mais vous pouvez aussi les télécharger depuis le site au format APK. Ce magasin est utilisé par diverses variantes d'Android comme Replicant, LineageOS et OmniROM. Le fabricant de smartphones écoresponsables et anti obsolescence programmée Fairphone recommande F-Droid à leurs clients. Pour utiliser ce magasin, il suffit d'aller sur le site officiel et de scanner le QR Code pour télécharger l'appli qui vous donnera accès à toutes les autres. Mais que trouve-t-on sur F-Droid et est-ce adapté à tout le monde ?

ATTENTION AUX APK !

Utiliser un fichier APK (l'équivalent des fichiers EXE sous Windows) est très facile, mais attention, car en téléchargeant n'importe quoi, on peut se retrouver avec un virus. Sur Android ces malwares prennent la forme de dialers (des applis qui appellent automatiquement des numéros

surtaxés) ou d'adwares qui affichent de la publicité (cela vide votre forfait data et vos batteries). N'ayez crainte, car sur F-Droid, les applis sont vérifiées, bien plus que sur le Play Store où Google a bien du mal à décortiquer la quantité de nouvelles applis qui débarquent tous les jours. Si vous avez une version d'Android antérieure à la version 8 «Oreo», il faudra aller dans **Paramètres > Sécurité** puis cocher **Sources inconnues** pour lever l'interdiction des APK étrangers. Pour les versions 8 et 9 d'Android, il suffira d'accepter l'installation quand vous verrez le message d'avertissement.



FAIRPHONE 2 : UN SMARTPHONE RESPECTUEUX DE VOTRE VIE PRIVÉE



Le Fairphone 2 est un modèle de smartphone modulaire misant sur des matériaux responsables et sur le refus de l'obsolescence programmée. Il est tout à fait possible d'acheter des pièces détachées ou d'améliorer les composants sans racheter tout un téléphone. À l'heure où nous écrivons ces lignes, le Fairphone 2 tourne sous Android 7 «Nougat» avec les correctifs de sécurité de septembre 2018. La version d'Android n'est pas dérangeante, par contre au niveau sécurité, il vaut mieux passer par des OS alternatifs. Fairphone vous encourage à changer de crémerie et la communauté est prête à vous aider. Actuellement, outre l'Android «classique», vous trouverez OpenOS (un Android sans Google), LineageOS, SailfishOS, UbuntuTouch, etc. Au niveau des caractéristiques techniques, il ne s'agit



pas d'un modèle qui vous permettra de jouer aux derniers jeux 3D, mais c'est un smartphone complet avec un SoC Snapdragon 801, 2 Go de RAM, 32 Go de stockage extensible, dual SIM avec des appareils photo devant et derrière et une batterie de 2420 mAh. On le trouve chez Orange et Sosh avec un abonnement, mais le prix seul refroidi un peu : plus de 450 €, c'est un peu beaucoup pour un smartphone de 2015...

Lien : www.fairphone.com/fr

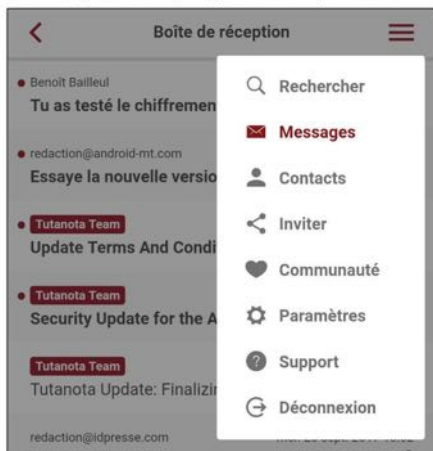


LES ALTERNATIVES CRÉDIBLES AUX APPLIS DU PLAY STORE...

PRATIQUE


01 > MESSAGERIE

Côté client e-mail, il y a de quoi faire sur F-Droid. K-9 Mail supporte les protocoles POP3, IMPAP et Push IMAP et permet d'utiliser une couche de chiffrement avec OpenPGP. Mais vous pouvez aussi opter pour Tutanota qui est un très



bon service avec la possibilité d'envoyer un e-mail chiffré à un correspondant qui ne dispose pas de l'appli... La version gratuite ne souffre d'aucune limitation gênante.

02 > NAVIGATION INTERNET

Pour la navigation sur Internet, vous trouverez deux très bonnes applis : Firefox Lite est une version légère de Firefox qui provient directement de la fondation Mozilla tandis que Fennec est un fork basé sur le moteur Gecko qui a pour but d'éliminer les parties «propriétaires» dans le code de Firefox.



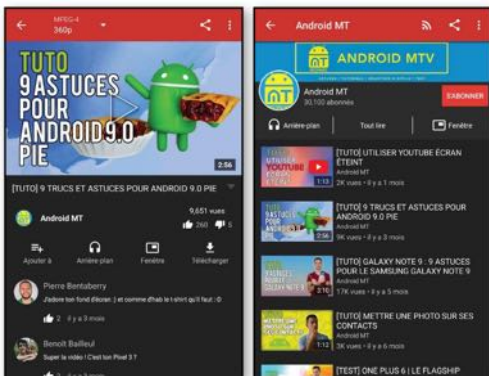
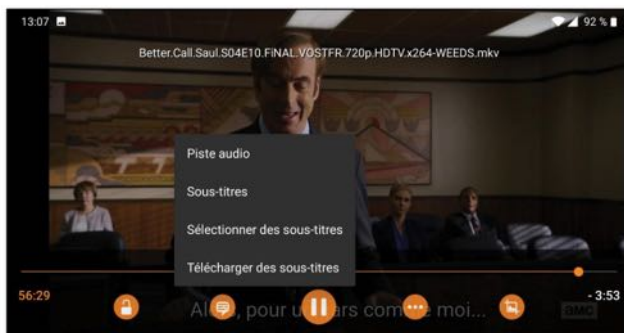
03 > GPS

OSMAnd~ remplacera habilement votre appli GPS ou Google Maps. Elle est libre, utilise les fonds de cartes libres via l'utilisation d'OpenStreetMap et permet un chargement des cartes en local sur le smartphone et donc utilisables hors zone de couverture 4G ou à l'étranger, là où les frais de roaming peuvent être importants.



04 > PLAYER MULTIMÉDIA

Inutile de présenter la meilleure appli dans ce domaine. VLC Media Player gère vos vidéos, vos MP3 et vos flux réseau avec une aisance déconcertante. Contrôle des sous-titres et des pistes audio, égaliseur, pas besoin de codecs additionnels, gestion des tags : il ne manque rien...

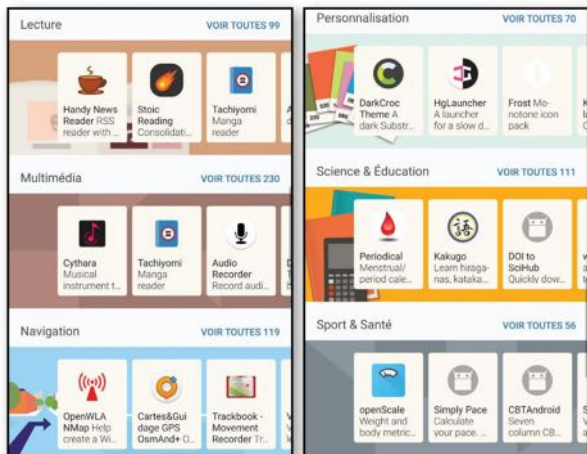


05 > VIDÉO EN LIGNE

Si vous aimez YouTube, F-Droid propose des alternatives. Il ne s'agit pas de nouvelles plates-formes, mais d'applis qui récupèrent les vidéos pour les proposer sur une interface différente. NewPipe n'utilise aucune librairie de Google ni l'API YouTube : vous n'avez donc pas besoin d'un compte Google pour y aller ! WebTube propose à peu près la même chose...

06 > AUTRES

Impossible de faire une liste exhaustive des applis qui valent le détour. Vous trouverez notamment Wikipedia, twitlatte (client Twitter et Mastodon), OpenCamera pour la photo, Faceslim pour Facebook, DNS66 pour changer vos DNS, NextCloud, Minetest, Oversec (chiffrement, voir Pirate Informatique n°32), MuPDF, AdAway, Yalp Store (pour récupérer une appli du Play Store au format APK sans compte Google) et toutes les applis de Guardian Project comme Haven (voir notre n°36) ou Orbot (n°30).



N°7
en kiosques
NOUVEAU!

Le **GUIDE** non officiel de l'utilisateur **WINDOWS 10**



PC & Tablettes



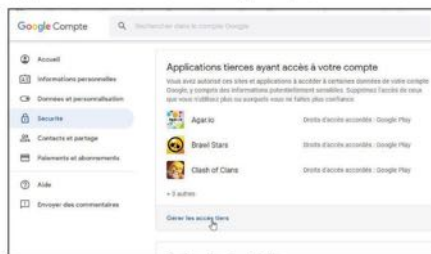
RÉVOQUER DES AUTORISATIONS

PRATIQUE

Quelles applications ont accès à votre compte Google ? Un point à vérifier, et à corriger le cas échéant.

01 > VÉRIFIER LES APPLICATIONS

Rendez-vous à l'adresse indiquée ci-dessus, et connectez-vous à votre compte Google si ce n'est déjà fait. Puis allez à la rubrique **Sécurité**, à gauche, et descendez à la section **Applications tierces...** (si elle n'apparaît pas, tout va bien).



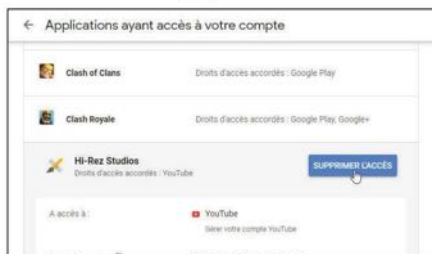
INFOS [**Compte Google**]

Où le trouver ? [myaccount.google.com]

Difficulté :

02 > SUPPRIMER DES AUTORISATIONS

Cliquez sur **Gérer les accès tiers**. Si apparaît ici une application que vous n'utilisez pas (ou plus), cliquez dessus puis faites **Supprimer l'accès**. Vérifiez également la section **Se connecter à l'aide de Google**, juste en-dessous.



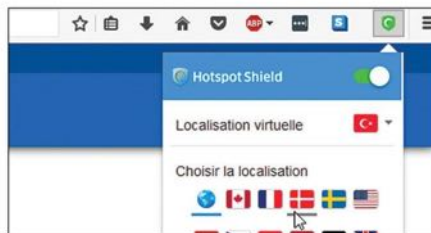
MASQUER SON ADRESSE IP

PRATIQUE

L'adresse IP identifie votre ordinateur sur Internet. Avec l'extension **Hotspot Shield**, vous pouvez utiliser une IP d'emprunt.

01 > CHANGER D'IP

Une fois l'extension installée, il suffit de cliquer sur son icône (un genre de bouclier) et d'activer le service. Cliquez ensuite sur un drapeau pour utiliser une IP en provenance du pays choisi. N'hésitez pas à en essayer plusieurs si la connexion ralentit trop.



INFOS [**Hotspot Shield**]

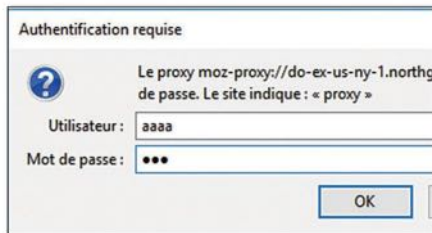
Où le trouver ? [<https://goo.gl/o8LqMY> (Firefox)]

<https://goo.gl/7vAYAY> (Chrome)]

Difficulté :

02 > PASSER EN NAVIGATION PRIVÉE

Si vous utilisez la navigation privée, il se peut que vous voyiez une fenêtre demandant un mot de passe quand vous essayez de vous connecter à un site normalement inaccessible. Entrez n'importe quoi dans les deux champs (une lettre suffit) et validez pour basculer sur le site.



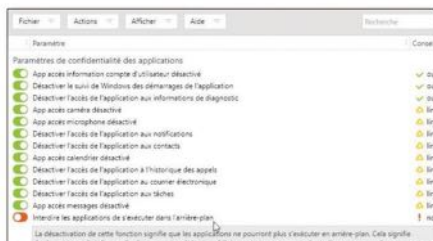


DÉSACTIVER LES ESPIONS DE WINDOWS 10

Certaines fonctions indiscrettes ne figurent pas dans les paramètres de confidentialité de Windows 10. Pour les désactiver, utilisez O&O ShutUp10.

01> EXAMINEZ LES OPTIONS

Téléchargez et lancez le logiciel. Pour chaque option proposée, vous pouvez obtenir des explications en cliquant sur la ligne. Certaines sont recommandées (**oui**), d'autres plutôt recommandées mais pouvant entraîner quelques limitations (**limité**), d'autres déconseillées (**non**).



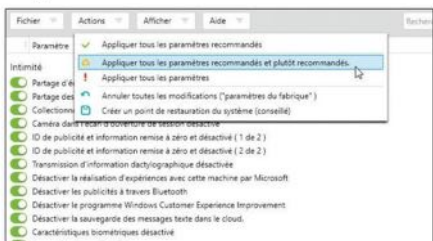
INFOS [O&O ShutUp10]

Où le trouver ? [<https://www.oo-software.com/fr/shutup10>]

Difficulté :  

02> FAITES VOS CHOIX

Cliquez sur l'interrupteur, en début de ligne, pour modifier une option. Par sécurité, le logiciel vous propose de créer un point de restauration système : acceptez. Vous pouvez aussi appliquer en bloc certaines catégories de paramètres, via le menu **Actions**. Vos choix faits, refermez le logiciel.



VÉRIFIER UNE URL RACCOURCIE

Très pratiques pour abréger une adresse Internet, les URL raccourcies (type goo.gl, [tinyurl](https://tinyurl.com), bit.ly) sont parfois utilisées pour nuire. En cas de doute, utilisez Unshorten.me pour découvrir ce qui se cache derrière.

01> TAPER L'URL

Tapez ou copiez l'adresse raccourci dans le champ prévu à cet effet, sur la page d'accueil d'unshorten.me (une copie est préférable, elle évite les erreurs ou les confusions). Puis cliquez sur le bouton **Un-Shorten**.



INFOS [Unshorten.me]

Où le trouver ? [<https://unshorten.me>]

Difficulté :  

02> VÉRIFIER LE LIEN

Le site déchiffre l'URL et affiche une miniature de la page correspondante. Vous pouvez vous rendre directement dessus (bouton **Visit Website**), ou consulter d'abord son score de fiabilité (**Internet Safety User Score**) s'il ne vous inspire pas confiance.



Vérifier son VPN > AVEC DNS LEAK

Les fuites de DNS, c'est-à-dire l'envoi accidentel de paquets d'informations utilisant le DNS de votre fournisseur d'accès Internet au lieu de celui utilisé par votre VPN, posent un réel problème d'anonymat. Lancez un test sur DNS Leak. Si les serveurs affichés ne sont pas ceux de votre VPN, c'est que vous êtes potentiellement vulnérable.

Lien : www.dnsleaktest.com

Test complete

Query round Progress... Servers found

1 3

Sponsored by



Ultimate IP leak Protection

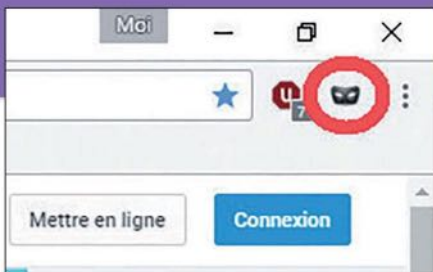
IP	Hostname	ISP	Country
109.0.64.15	resolver28.dns.sfr.net	SFR	France 
109.0.65.15	resolver27.dns.sfr.net	SFR	France 

Basculer Chrome en navigation privée

> AVEC GO INCOGNITO

Disponible sur Chrome, l'extension Go Incognito est parfaite pour faire passer un onglet en navigation privée, même si vous l'avez ouvert en mode normal. Appuyez simplement sur l'icône de l'extension, à droite de la barre d'adresse. Cela ferme l'onglet initial, l'efface de l'historique, et le rouvre dans une fenêtre de navigation privée. Simple et efficace.

Lien : <https://goo.gl/eSAEvc>



Empêcher la localisation > AVEC LOCATION GUARD

Même si vous n'utilisez pas de VPN ou de solution d'anonymat, vous n'avez pas forcément envie que les sites sur lesquels vous vous connectez sachent où vous vous trouvez. L'extension Location Guard évite d'avoir à refuser manuellement le partage de sa localisation. Vous pouvez paramétrer pour chaque site un refus permanent, l'envoi d'une localisation aléatoire, voire fantaisiste.

Lien : <https://goo.gl/PHSVLf>
(Firefox)

Lien : <https://goo.gl/TvGwdU>
(Chrome)

Location Guard		Low
Options	⚙️	Protection: m <input type="checkbox"/>
Privacy Levels	🔗	Cache location for: <input type="checkbox"/>
Fixed Location	📍	<input type="checkbox"/>
FAQ	❗	
Demo	👉	

**POUR QUI ?**

Pour les internautes qui ont le même mot de passe partout... et qui veulent changer ça !

POUR QUOI FAIRE ?

Pour stocker tous ses mots de passe de manière sécurisée, les retrouver facilement sur tous ses appareils sans avoir à les retenir.

AVIRA PASSWORD MANAGER : LA GARANTIE DE MOTS DE PASSE SÛRS

Plus connue pour son antivirus, la société de sécurité numérique Avira propose aussi un gestionnaire de mots de passe. Facile d'accès et disponible sur toutes les plates-formes principales (navigateurs, ordinateurs et smartphones), le vrai plus d'Avira réside néanmoins dans sa version pro, qui donne accès à une véritable vigie sur vos mots de passe.

**LEXIQUE*****MOT DE PASSE MAÎTRE :**

Il s'agit du seul mot de passe que vous devrez absolument retenir pour accéder à tous les autres. Il doit être unique et suffisamment long. Vous pouvez choisir une phrase de passe plutôt qu'un mot de passe, par exemple.

***CLOUD :**

Un service cloud propose de stocker des données "en nuage", c'est-à-dire sur des serveurs distants, accessibles de n'importe où sur internet.

« 81 % des vols de données sont causés par des mots de passe faibles ou dérobés. » S'appuyant sur une étude du site web allemand Security Insider, Avira affiche ce constat alarmant en page d'accueil de son service de gestionnaire de mots de passe. Avec son extension pour navigateurs, Avira Password Manager est assez

complet, même en version gratuite : il permet d'importer ses mots de passe, les stocker et d'en générer de nouveaux pour les modifier. Avec une mention particulière à la fonction remplissage des champs de connexion (identifiant et mot de passe), qui reconnaît le compte automatiquement, là où d'autres services nécessitent un ou deux clics en plus.

DES ALERTES SÉCURITÉS BIEN PRATIQUES, MAIS PAYANTES

Disponible sur Chrome, Firefox, Windows, Mac, Android et iOS, Avira Password Manager est tout terrain, bien qu'un peu envahissant car souvent installé avec d'autres produits Avira. En plus des mots de passe, Avira Password Manager propose de conserver des notes sécurisées, un service devenu assez commun pour les gestionnaires de mots de passe dans le cloud. Mais son véritable atout est sa version Pro, qui permet de surveiller ses mots de passe, détecter de potentielles failles de sécurité de ses services et aide à les résoudre (voir encadré).

La protection des mots de passe est une notion à ne pas prendre à la légère...

VERSION PRO POUR PLUS DE SÉCURITÉ



En souscrivant à la version Pro d'Avira Password Manager, à 24,95€/an, vous êtes informé du niveau de sécurité de tous vos mots de passe, visible dans l'onglet **État de Sécurité**. Ce service payant permet aussi de détecter les failles de sécurité potentielles de tous vos comptes, grâce au site [havebeenpwned.com](https://shop.avira.com/30/surl-WMSXztetLc), et vous indique la marche à suivre pour les résoudre.

État de Sécurité

Votre état de sécurité : **Moyen**

50%

2/3 Comptes à améliorer

1/1 Comptes piratés

0/1 Sites Internet non sécurisés

1/1 Complexité du mot de passe

1/1 Mots de passe réutilisés

Activer les contrôles de violation de la sécurité : une fois ces contrôles activés, vos identifiants et mots de passe seront contrôlés afin de détecter de possibles infractions avec le service havebeenpwned.com

QUE FAIRE ?

Connectez-vous à votre compte yahoo.com et modifiez votre mot de passe.

Voici comment procéder :

1. Connectez-vous à votre compte yahoo.com
2. Accédez à l'emplacement du site yahoo.com permettant de modifier le mot de passe de votre compte, généralement au niveau de la gestion du compte, du profil utilisateur ou des paramètres de sécurité.
3. Gérez un mot de passe complexe avec Avira Password Manager. Faites cela facilement à partir de la fenêtre contextuelle intégrée.
4. Modifiez le mot de passe pour yahoo.com avec le mot de passe généré.
5. Confirmez l'enregistrement du mot de passe généré dans la fenêtre contextuelle Avira Password Manager.

Modifier le mot de passe

État de Sécurité

Votre état de sécurité : **Critique**

33%

3/3 Comptes à améliorer

2/2 Comptes piratés

0/2 Sites Internet non sécurisés

2/2 Complexité du mot de passe

2/2 Mots de passe réutilisés

Activer les contrôles de violation de la sécurité : une fois ces contrôles activés, vos identifiants et mots de passe seront contrôlés afin de détecter de possibles infractions avec le service havebeenpwned.com

l'analyse de tous vos comptes en vue de détecter les violations de données, les vulnérabilités de sites Internet et les mots de passe insuffisamment sécurisés.

Si nous détectons une menace pour votre compte, nous vous recommanderons des mesures à prendre pour renforcer la sécurité de votre compte.

Activer



LE LOGICIEL PASSE EN REVUE VOS IDENTIFIANTS ET VOUS CONSEILLE EN CAS DE FAIBLESSES...



PROTECTION



INFOS [Avira Password Manager]

Où le trouver ? [<https://www.avira.com/fr/avira-password-manager>]

Difficulté :

GÉRER SES MOTS DE PASSE AVEC AVIRA PASSWORD MANAGER

PRATIQUE



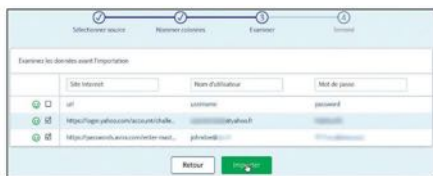
01 > INSTALLER L'APPLICATION ET L'EXTENSION

Après vous être inscrit avec un **mot de passe maître**, cliquez sur **Verify account** dans l'e-mail qui vous a été envoyé. Cliquez ensuite sur **Download now**, puis installez l'application et activez l'extension **Avira Password Manager** (et **Protection Web Avira** si vous le souhaitez).



02 > IMPORTER LES MOTS DE PASSE DE VOTRE NAVIGATEUR

Si vous avez enregistré vos mots de passe dans votre navigateur, cliquez sur **Importer maintenant** dans le troisième champ d'astuces au centre de l'écran. Cliquez ensuite sur **Import** depuis **navigateur > Autoriser > Importer > Terminé**.



03 > AJOUTER UN MOT DE PASSE MANUELLEMENT



Connectez-vous au service de votre choix (Gmail, par exemple). Une fenêtre apparaît et vous propose d'enregistrer vos identifiants et mot de passe dans Avira Password Manager. Cliquez sur **Enregistrer**. Il est aussi possible d'ajouter ses identifiants et mots de passe en cliquant sur le **bouton +** dans l'interface d'Avira Password Manager.

04 > SE RECONNECTER AUTOMATIQUEMENT À UN SERVICE



Vous souhaitez vous reconnecter à un service sans avoir à taper vos identifiants et mot de passe ? Avira Password Manager les remplit pour vous. Sur Gmail, par exemple, vous n'avez qu'à cliquer 2 fois sur **Suivant**.

05 > MODIFIER UN MOT DE PASSE



Connectez-vous au service de votre choix (continuous sur Gmail) et rendez-vous sur la page de modification de votre mot de passe. Dans le champ du nouveau mot de passe, cliquez sur l'**icône du Générateur de mot de passe Avira**. Cliquez ensuite sur **Utiliser mot de passe**. Validez la modification (en cliquant sur **Modifier** le mot de passe dans le cas de Gmail). Une fenêtre s'affiche en haut à droite de l'écran. Cliquez sur **Mettre à jour**.

06 > LES AUTRES SERVICES AVIRA [BONUS]

Cliquez sur l'**icône Avira** dans la barre des tâches en bas de votre écran. Avira vous propose une dizaine d'autres services, comme un antivirus, un VPN ou encore un gestionnaire de mises-à-jour.

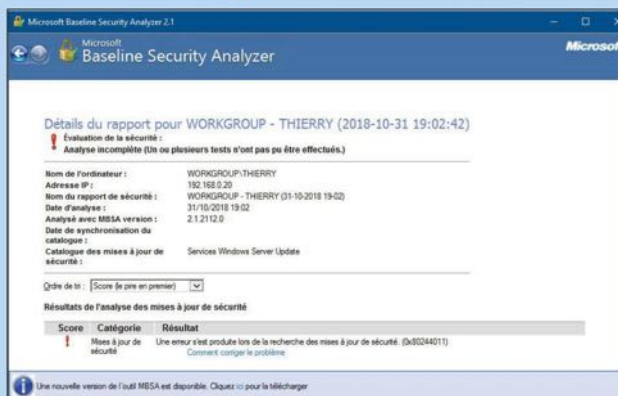


Repérer les vulnérabilités

> AVEC MICROSOFT BASELINE SECURITY ANALYSER

Microsoft Baseline Security Analyzer (MBSA) récupère depuis les serveurs Microsoft les dernières informations publiées sur les failles et patches de sécurité. Il teste tous les points du système susceptibles de présenter une faille de sécurité (comptes actifs, solidité des mots de passe, présence des patches, logiciels récemment installés, configuration du pare-feu, etc.). Pour chaque point contrôlé, si la sécurité semble insuffisante, voire défaillante, le logiciel explique comment mettre en œuvre la parade adéquate.

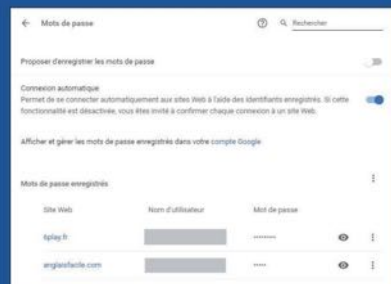
Lien : <http://goo.gl/UBHss>



Désactiver l'enregistrement des mots de passe

> AVEC CHROME

Pratique l'enregistrement des adresses ou des mots de passe dans Chrome, pour éviter de retaper ces informations. Mais pas forcément très sûr, surtout si d'autres personnes ont accès à votre ordinateur.

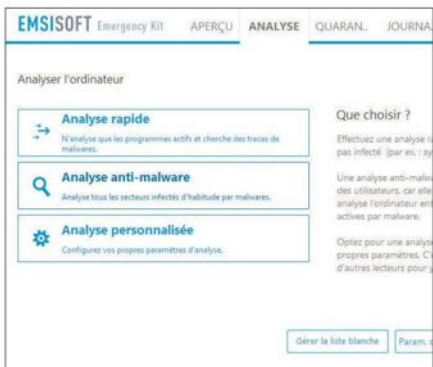


Pour contrôler tout cela, affichez les **Paramètres** de Chrome. À la rubrique **Personnes**, inspectez les sections **Mots de passe**, **Modes de paiement** et **Adresses et autres**. Vous pouvez désactiver l'enregistrement, et effacer des informations.

Emporter un antivirus

> AVEC EMSISOFT EMERGENCY KIT

Un antivirus sur une clé USB, c'est bien pratique pour analyser une machine dépourvue de protection et sans connexion Internet. Emsisoft Emergency Kit est un antivirus portable. Après avoir téléchargé le programme,



il suffit de décompresser l'archive sur une clé USB et le tour est joué. 512 Mo suffisent, parfait pour recycler une vieille clé !

Lien : www.emsisoft.com/fr/software/eeek

**POUR QUI ?**

Pour les nostalgiques qui ont connu les jeux sur disquettes

POUR QUOI FAIRE ?

Pour émuler les jeux PC sous DOS qui ne fonctionnent plus sur les machines actuelles

DOSBOX & D-FEND : TOUT POUR PROFITER DE VOS VIEUX JEUX !



Vous souhaitez ressortir vos vieux jeux PC des années 80/90 ? Le problème c'est que la plupart ne tourneront pas avec un PC récent. En effet, ils étaient faits pour fonctionner sous DOS, un système d'exploitation qui n'est même plus présent dans les Windows de nos jours. Alors, comment faire pour retrouver la magie de votre enfance ? Avec le logiciel DOSBox qui permet d'émuler le DOS de nos vieux coucous d'antan. C'est la seule solution sous Linux, mais les possesseurs de PC sous Windows disposent de D-Fend, une interface graphique pour DOSBox plus conviviale...

Vous avez fait du rangement dans le garage et vous avez retrouvé un trésor que vous pensiez perdu : *Doom*, *Speedball 2*, *Discworld*, *Command&Conquer*, *Civilization*, *Alone in the Dark*, *Sim City 2000* et *Wing Commander*. Autant de magnifiques jeux vous ayant procuré des heures de bonheur sur votre PC de l'époque. Bien sûr, vous vous empressiez de mettre le CD de votre jeu préféré dans votre lecteur, mais rien ne fonctionnait comme en 1994... En effet, les ordinateurs ont bien changé depuis qu'Ayrton Senna a fait son dernier tour de piste et que la Corée du Nord est devenue une dictature dynastique stalinienne : les jeux refusent de démarrer dans votre PC à base d'Intel Core i7. Il vous manque le système sur lequel tournaient ces chefs-d'œuvre : le MS-DOS.

PLUS DE DOS AVEC WINDOWS DEPUIS 18 ANS

Ce système d'exploitation était en fait accolé aux premières versions de Windows, mais a disparu avec Windows XP (il est en fait présent, mais le noyau NT de XP n'utilise plus MS-DOS comme système de base). Le système de rétrocompatibilité fonctionnant très mal, il faudra donc émuler le vieux système DOS avec un logiciel spécial : DOSBox. Ce dernier va recréer un environnement DOS en émulant des composants supportés par ce dernier, comme une carte graphique ou carte son ancienne génération, bref de quoi faire tourner des jeux allergiques à nos nouvelles machines. Comme ce logiciel est assez âpre à prendre en main et que les lignes de commande DOS sont assez pénibles, une équipe de passionnés a créé D-Fend Reloaded (qui est en fait un «fork» du vieillissant D-Fend). Ce logiciel a la particularité d'intégrer DOSBox et de proposer une interface de type Windows.

LEXIQUE

*ABANDONWARE :

Il s'agit d'un jeu trop vieux pour faire entrer de l'argent dans les caisses des ayants droit (éditeur, développeurs, etc.). Le jeu est dit abandonné, car il n'est plus exploité par personne. Parfois, les sociétés qui l'ont développé ont même disparu. Le fait de le partager librement sur Internet est toléré et même parfois volontaire de la part des éditeurs. Attention, des jeux considérés comme abandonware ne le sont plus dès qu'un éditeur les ressort dans le commerce.

*MS-DOS :

Pour «Microsoft Disk Operating System». Il s'agit d'un système d'exploitation antérieur à Windows, mais qui est resté accolé à ce dernier dans les versions 3.11, 95, 98 et Me. XP marque le début des problèmes pour les vieux jeux avec la migration vers le noyau NT.

Attention, les vieux jeux ne sont pas forcément gratuits : ne tombez pas dans l'illégalité...

LTF ABANDONWARE FRANCE

Si vous n'avez pas la chance d'avoir retrouvé vos vieux jeux ou que vous les avez vendus pour mettre de l'essence dans votre 103 Peugeot (avec pot Polini !), pas besoin de faire les vide-greniers ou d'acheter des oldies à prix d'or sur eBay. Il existe des sites spécialisés dans la paléontologie vidéoludique comme LTF Abandonware France qui recense et met à disposition des jeux au format disquette et CD. On y trouve aussi les visuels, les musiques, les jaquettes, les manuels (nécessaire pour certaines mesures anti-piratage d'époque) et même des publicités d'époque. Ne prenez que les jeux au format DOS : DOSBox n'émule pas Windows !

Lien : www.abandonware-france.org





Liste de compatibilité

Pour être sûr que vos jeux soient pris en charge par DOSBox, il existe un site qui dresse une liste mise à jour. Vous pouvez chercher par ordre alphabétique, ou par mot clé. Pour chaque jeu, vous trouverez son degré de compatibilité : runnable, playable ou supported. Sachez, cependant, qu'il y a plus de 3800 jeux au compteur... Les plus connus sont bien sûr ceux qui fonctionnent le mieux. Sur cette page, vous trouverez aussi une notice et des tutos en anglais.

Lien :

<http://goo.gl/gfdBT7>



DOSBox
CROSS Platform
"Way more FPS than Counterstrike!"

News Crew Information Status Downloads Compatibility Forum Links Login Latest version: **0.74-2**

First char: Latest added: Game search:

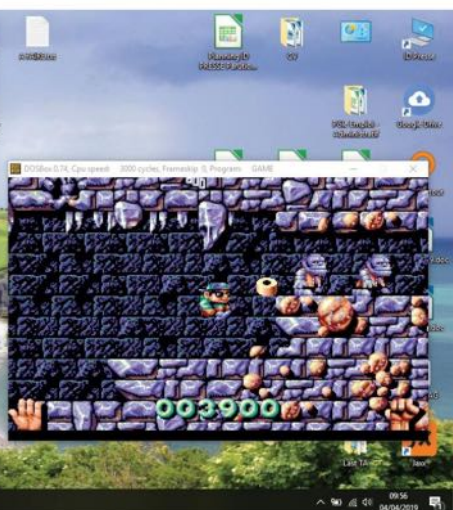
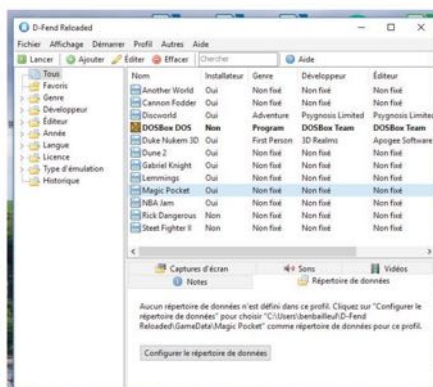
DOSBox does NOT host these games. This list is a compatibility list. If you are looking for games, you can visit www.classicdosgames.com or ictp.com.

Game directory (browsing from A)

Game:	Year:	Version:	Status:
A (230)	1988	0.74-2	runnable - playable - supported
A Dudley Dilemma	1992	0.72	supported
A Line in the Sand	1986	0.72	supported
A Mind Forever Voyaging	1989	0.72	supported
A Nightmare on Elm Street	1989	0.70	supported
A-10 Tank Killer	1991	0.72	supported
A-10 Tank Killer 1.5	1989	0.74-2	supported
A-Maze	1991	0.73	supported
A-Train (Take the A-Train 3)	1991	0.74-2	supported
A.G.E.	1991	0.73	supported
A320 Airbus	1991	0.73	supported
A4 Networks	1995	0.73	supported
Azard	1988	0.70	supported
Abadon del Crimen, La	1992	0.73	supported
Abandoned Places 1	1992	0.74-2	supported
ABC Monday Night Football	1989	0.72	supported
Abenteuer Europa	1994	0.74-2	supported
Abms The Lion	1996	0.74-2	supported
Abrams Battle Tank	1988	0.72	supported

DOSBox Tutorial
DOSBox Manual
Looking for classic PC games?
Get them at GOG.COM
Cheap and DRM-free!

DE BASE, DOSBOX ET D-FEND LANCENT LES JEUX DANS UNE FENÊTRE, MAIS IL EST POSSIBLE DE BASCULER EN MODE PLEIN ÉCRAN (ALT+ENTRÉE). LA RÉOLUTION DE CERTAINS JEUX EMPÊCHERA CEPENDANT DE FAIRE DES MIRACLES ET SI VOUS N'AVEZ PAS JOUÉ À CERTAINS TITRES DEPUIS 25 ANS, VOUS RISQUEZ DE VOUS PRENDRE UNE CLAQUE : LES GRAPHISMES SONT TOUJOURS PLUS BEAUX DANS NOS SOUVENIRS...



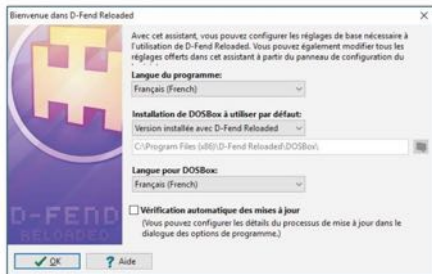


D-FEND RELOADED SOUS WINDOWS

PRATIQUE

01 > LANCEMENT

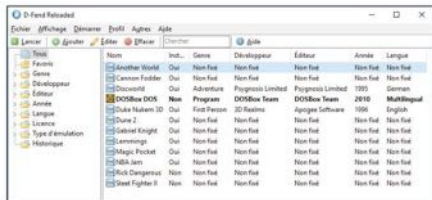
La version 1.4.4 de D-Fend Reloaded comprend à l'intérieur DOSBox (v0.74). Vous n'aurez donc pas à installer ce dernier pour pouvoir jouer. Si vous êtes déjà utilisateur de DOSBox, il suffira de spécifier le chemin de votre dossier d'installation juste après la première mise en route de D-Fend Reloaded. Depuis cet **Assistant de 1er lancement**, vous



pourrez aussi choisir la langue du programme, la langue de DOSBox et la recherche automatique de mise à jour.

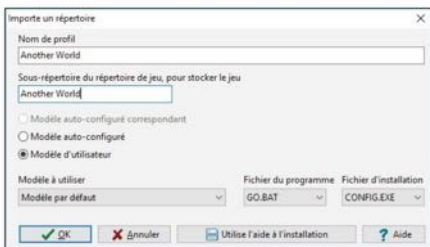
02 > LES JEUX

Après avoir validé, vous allez vous retrouver sur la fenêtre principale de D-Fend Reloaded. Imaginons que vous n'avez plus les jeux en votre possession. Nous vous invitons à les télécharger sur www.abandonware-france.org au format archive. Notez que pour le RAR et le ZIP, il n'y aura pas de problème tandis que le 7Z, non supporté par D-Fend, demandera une étape de plus.



03 > LE CHOIX DU MODÈLE

Pour commencer le paramétrage, faites juste glisser votre archive dans la fenêtre principale. Une nouvelle fenêtre va alors apparaître. Ici, vous devrez mettre le nom du jeu (dans notre exemple *Another World*) puis le nom du dossier sous lequel seront stockés les fichiers. À vous ensuite de choisir entre trois options : **Modèle auto-configuré correspondant** si le jeu est enregistré dans la base de données de D-Fend (si cette dernière n'est pas grisée, choisissez-la), **Modèle auto-configuré** permettant de sélectionner un jeu présentant les mêmes caractéristiques et **Modèle utilisateur** vous donnant le droit de paramétrer vos préférences à la main.



LES TYPES DE MODÈLES

Les « modèles » sont des configurations virtuelles de vieux PC : **Normal DOS Game**, **Complexe DOS Game with 3D graphics**, etc. À vous de choisir celui qui convient le mieux pour chaque jeu si jamais **Modèle auto-configuré correspondant** apparaît en grisé (voir étape 3). Heureusement, les jeux les plus connus sont déjà paramétrés à la base dans D-Fend Reloaded, mais si vous êtes perdu, dans **Ajouter > Ajouter à partir d'un modèle**, vous retrouverez des indications à côté de chaque modèle pour cerner au mieux vos besoins.

ET AVEC UN VRAI CD OU UN ISO ?

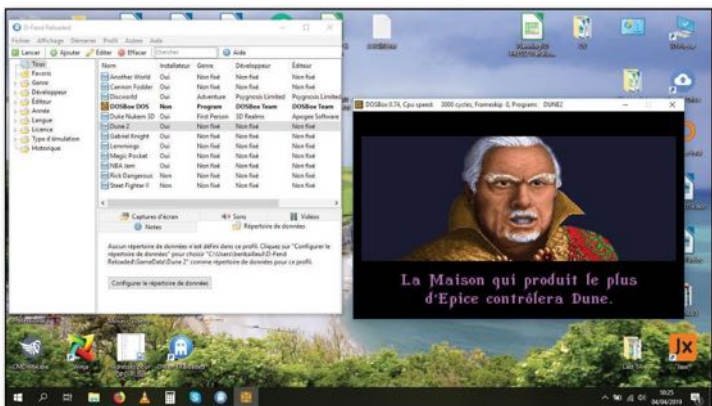
Si vous avez en votre possession les jeux de votre jeunesse, il faudra agir légèrement différemment. Ajoutez votre lecteur optique à D-Fend en faisant **Ajouter > Installer à partir d'un média source** puis **Installer à partir d'un vrai lecteur CD** dans le cas d'un jeu CD, **Installer à partir d'une image de CD** (pour un ISO ou un couple CUE/BIN) ou **Installer à partir d'une image de disquette**. Suivez les instructions qui peuvent varier d'un jeu à l'autre...





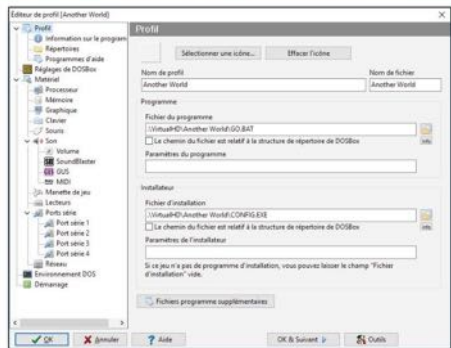
04 > JOUEZ !

Après avoir trouvé le bon modèle, puis sélectionné le fichier programme (en EXE) et le fichier d'installation (généralement Setup), vous pouvez valider. Le jeu se retrouvera dans la fenêtre principale. Double-cliquez dessus. Le jeu se lance en plein écran. Vous pouvez revenir à un mode fenêtré avec **Alt+Entrée**. Notez qu'il faudra parfois lancer un fichier Setup pour que les manettes ou le son soient pris en compte dans les réglages de D-Fend...



05 > CAS PARTICULIERS ET PROFIL

Si vous disposez d'un jeu qui est dans une archive du genre .7z, il faudra décompresser le jeu dans le dossier de votre choix puis faire **Ajouter>Ajouter à partir d'un modèle**. Choisissez le type du modèle (voir encadré) et remplissez les champs à la main (Nom, fichier programme et fichier d'installation). Si vous êtes perdu, vous pouvez aussi décompresser le 7Z pour remettre le contenu dans un ZIP et revenir à l'étape 3)... Validez pour retrouver votre jeu dans l'interface principale. Notez que vous pouvez éditer les paramètres de votre jeu en faisant un clic droit sur son profil. À partir de cette fenêtre, vous pourrez modifier le nom de profil, le fichier programme, le fichier d'installation, etc. Sur la gauche, vous pourrez changer la partie «hardware» : carte son, carte graphique, clavier, manette, etc.



RETROGAMING AVEC UNE FRAMBOISE ?



Mais pourquoi utiliser votre PC à 500 € (surtout si vous devez faire découvrir Lemmings à vos enfants) alors que le Raspberry Pi est en mesure de faire tourner DOSBox pour 35 € ? Il faut dire que notre Framboise a bien plus de «pêche» qu'un vieux i486 DX et même si l'architecture ARM n'a rien à voir avec celle des x86, cela tourne très bien. Sous Windows, il existe des interfaces graphiques (comme D-Fend Reloaded), mais sur la Framboise, il faudra taper des lignes de commande...DOS. Rien d'insurmontable pour les barbus que vous êtes ! Notez enfin que Recalbox intègre DOSBox donc pas besoin de jongler avec les cartes SD si vous avez déjà cette distribution.





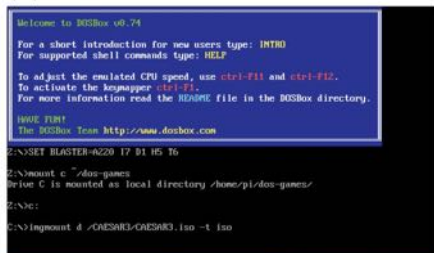
il faudra lancer **install.exe** (ou **setup.exe**) puis lancer le jeu (ne changez pas le chemin d'origine). Pour les images de CD c'est un peu différent...

05 > ET AVEC L'IMAGE D'UN CD ?

Pour les images de CD (format .img ou .iso par exemple), il faudra monter le fichier dans le lecteur D:\> avec :

```
c:\> imgmount d jeu/jeu.img -t iso
c:\> d:
```

Lorsque vous verrez le prompt, il faudra taper la commande permettant de lancer le jeu. Pour être sûr de votre coup, regardez à l'intérieur de l'image pour trouver le fichier EXE qui permettra de lancer l'installation.



06 > LES SAUVEGARDES

Attention, lorsque votre jeu va fonctionner vous serez tellement content de retrouver votre jeunesse que vous allez y jouer comme si vous aviez 14, 18 ou 22 ans.



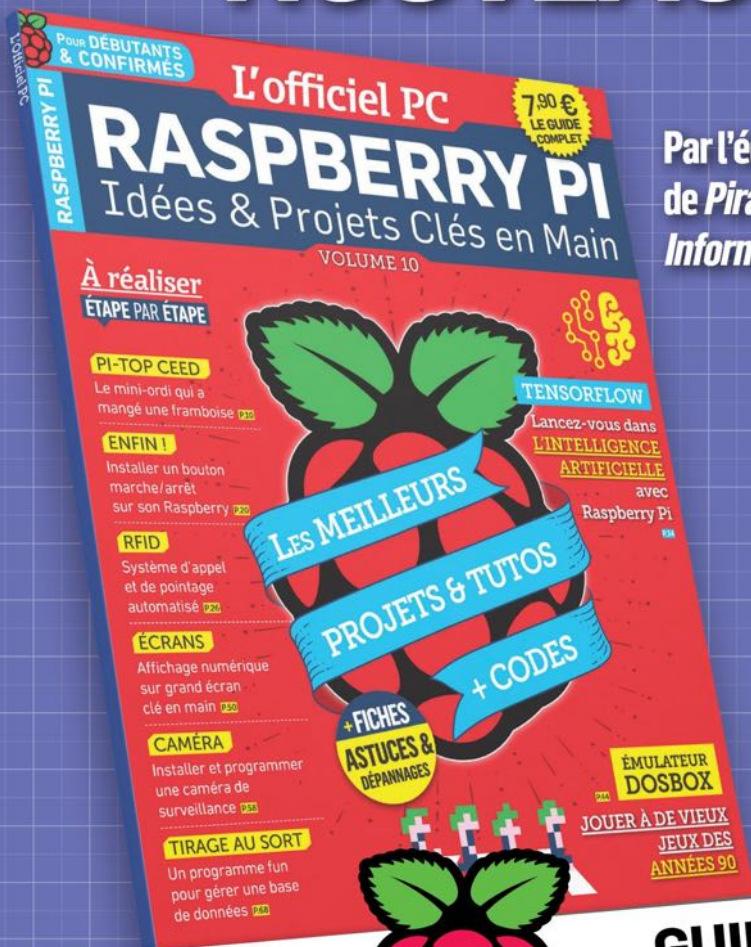
Nous vous conseillons néanmoins de faire quelques essais au niveau des sauvegardes pour être bien sûr que votre progression soit bien prise en compte. Nous vous conseillons de faire une courte partie puis de relancer le jeu et de tenter de charger la sauvegarde avant de vous lancer dans 5 heures d'Ultima. Si vous avez un problème avec tel ou tel jeu, il faudra malheureusement chercher au cas par cas...

07 > QUELQUES RACCOURCIS

- Alt+Entrée** Passer en mode plein écran
- Alt+Pause** Marque une pause
- Ctrl+F1** Montre le mappage du clavier
- Ctrl+F5** Prend une capture d'écran (à récupérer dans le dossier Capture)
- Ctrl+F6** Commencer et arrêter l'enregistrement d'un fichier sonore .wav
- Ctrl+F7** Baisse le frameskip (pour ralentir les animations trop rapides)
- Ctrl+F8** Augmenter le frameskip (pour accélérer les animations trop lentes)
- Ctrl+F9** Fermer DOSBox
- Ctrl+F10** Permet de «sortir» la souris de la fenêtre d'émulation au cas où vous devriez utiliser un autre logiciel.
- Ctrl+F11** Baisse le nombre de cycles de DOSBox pour ralentir l'émulation
- Ctrl+F12** Augmente le nombre de cycles de DOSBox pour accélérer l'émulation
- Alt+F12** Configure tous les paramètres pour une rapidité maximum (bouton «turbo»)



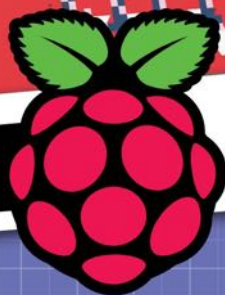
NOUVEAU !



Par l'équipe
de *Pirate*
Informatique !

L'officiel PC
RASPBERRY PI
Idées & Projets Clés en Main

**GUIDE
COMPLET**



CHEZ VOTRE MARCHAND DE JOURNAUX



» MINI PC ACUTE ANGLE AA-B4 : COMPLET ET BON MARCHÉ...

Ce mini PC au design très sympa dispose d'un processeur Quad Core Intel Apollo Lake (max 2,2 GHz) épaulé par 8 Go de RAM et d'un circuit graphique Intel HD Graphics 500. Un peu juste pour jouer aux derniers titres, il s'agit d'un ordinateur complet et plutôt véloce pour le prix. Il vous offre un fonctionnement fluide et une expérience multitâche stable. Grâce au processeur graphique Intel HD Graphics 500, vous bénéficiez d'une suite complète pour la domination du jeu et d'une expérience de visionnage vraiment transparente. Pour le stockage on peut compter sur une mémoire EMMC de 64 Go pour le système d'exploitation Windows 10 et d'un disque dur SSD de 128 Go pour vos fichiers. Côté connectique, on trouve une prise HDMI, un port RJ45 10/100/1000, le WiFi ac et 2 ports USB 3.0. L'appareil dispose même d'une batterie en cas de coupure de courant permettant de sauvegarder votre travail et de quitter Windows proprement...

Prix : 179 €

Lien : <https://frama.link/JMXQRXmU>



» LAN TURTLE, ATTAQUES «MAN-IN-THE-MIDDLE»

LAN Turtle est un dongle USB proposant une sortie Ethernet permettant de réaliser des attaques «Man-in-the-Middle». Même verrouillé, un PC ou un Mac permettra à un périphérique USB de se connecter et

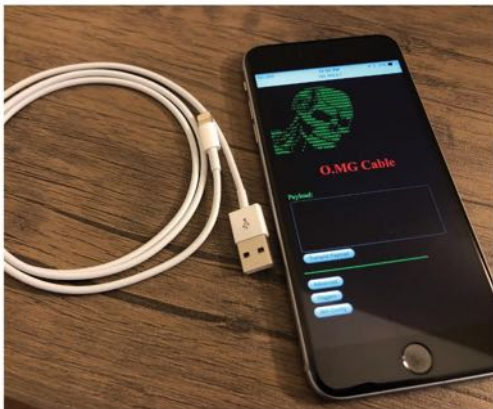


comme LAN Turtle sera aussi reconnu comme un adaptateur Ethernet, cette connexion sera préférée au WiFi. C'est là que l'attaquant pourra intercepter le trafic, poser une backdoor, etc. Les possibilités sont même plus vastes qu'avec le PoisonTap (Pirate Informatique n°32). Depuis peu, on trouve aussi une version 3G à 125 €...

Prix : 53 € Lien : <https://lantturtle.com>

» OMG CABLE, ENCORE À L'ESSAI

Mike Govern est un chercheur en sécurité informatique qui a créé le OMG Cable (pour «Offensive Mike Govern Cable», mais OMG signifie aussi «Oh My God !») Ce dernier contient une puce WiFi. Lorsque ce câble un peu fourbe est connecté à un PC, la puce



utilise le courant du port USB et l'appareil peut ensuite exécuter des commandes sur la machine de la victime pour y extraire des données. Le pirate récupérant les informations depuis une interface Web sur une machine connectée au même réseau WiFi. Le but pour le chercheur n'est pas de vendre sa trouvaille, mais de sensibiliser les utilisateurs : on ne peut même plus faire confiance à un simple câble !

Prix : N.C Lien : <https://frama.link/0dKHA6yU>

» POWERBANK MANA DE GLOBAL CHARGER : GARANTI ET ÉCHANGEABLE À VIE !

Les batteries de secours ou «powerbank» sont très pratiques, mais il se pose souvent le problème de l'obsolescence : les charges et décharges successives rendent ces appareils assez fragiles et il arrive qu'elles ne remplissent plus leur fonction au bout de 1 ou 2 ans. La société française Global Charger a trouvé la solution avec sa gamme de batteries «Mana»... Ces batteries de 4000 ou 10000 mAh (2 ou 5 cellules) sont équipées d'un cordon micro USB, mais aussi de 2 adaptateurs (USB-C ou iPhone) permettant de recharger n'importe quel smartphone récent sans disposer de câble. Un câble supplémentaire est d'ailleurs fourni (USB type A vers micro USB) pour recharger 2 appareils en même temps. La norme 5V/1A figure dans les standards de l'industrie : aucun risque pour votre appareil. La batterie est rechargeable de 0 à 100 % en 4 heures (4 LEDs permettent de contrôler l'état de la charge) et il faut environ 2 heures pour recharger un appareil même si cela dépend un peu de votre modèle. Nous sommes par exemple passés de 60 % à 100 % en 1h10.



«La batterie c'est la vie !»

Mais ce qui est intéressant avec la gamme Mana de Global Charger c'est qu'elles sont échangeables à vie !

Si la votre marque des signes de fatigue, vous pouvez aller l'échanger contre une autre dans les lieux agréés et plus de 40 festivals en France. Pour en savoir plus concernant les lieux où vous pouvez procéder à l'échange : www.globalcharger.fr/service-mana. La société s'occupe du SAV, s'engage contre l'obsolescence programmée et permet grâce à ce système d'échange de limiter l'impact sur l'environnement. Pierre Cattani nous explique : «Nos batteries sont recyclées pour la plupart par le biais d'une association spécialisée. Nous tentons aussi de mettre en place une réparation que nous faisons nous-même en ouvrant la batterie pour changer le câble intégré et en remplaçant la batterie lithium dans une nouvelle coque quand c'est possible». Les batteries sont aussi personnalisables. Il suffit d'envoyer le visuel ou le logo que vous voulez voir imprimer sur la coque en l'envoyant directement ou en utilisant le template mis à disposition sur le site.

Prix : De 25 à 40 € Lien : <https://frama.link/vaz8J0Bf>

» USB RUBBER DUCKY DELUXE, ATTAQUES VIA LE CLAVIER



Vous ne le savez peut-être pas, mais Windows et les antivirus font une confiance aveugle aux claviers. En effet, lorsque vous branchez un clavier, aucun logiciel ne va vérifier qu'il s'agit bien d'un



appareil de ce type alors qu'une clé USB étrangère ou un disque dur externe ont toutes les chances d'être un minimum auscultés. Partant de ce constat, des petits malins ont créé l'USB Rubber Ducky, une clé USB qui se comporte comme un clavier sauf que ce dernier a la particularité d'écrire tout seul le code que vous aurez placé dans sa carte SD. On peut imaginer des scripts permettant de récupérer un mot de passe Wi-Fi, un compte Facebook, pirater un FTP, etc. Tant que vous avez accès à la machine et que la session n'est pas verrouillée, vous avez tous les droits... Dans sa version «Deluxe», l'appareil est livré avec une prise USB OTG permettant de «s'amuser» avec des appareils mobiles.

Prix : 35 € Lien : <https://frama.link/shpGtqRY>



CLASSEMENT



WORLD HACK WEB

Lors de nos recherches ou au détour d'une discussion, nous faisons connaissance avec des sites ou des services intéressants. Au lieu de les garder pour nous, nous les partageons dorénavant sur cette page... N'hésitez pas à nous envoyer vos sites de prédilection à cette adresse : benbailleul@idpresse.com



AV-TEST

> RECHERCHE EN MALWARE

AV-Test est l'institut de recherche indépendant allemand pour la sécurité informatique. L'organisme utilise des systèmes d'analyse développés dans ses propres laboratoires, garantissant ainsi des résultats qui ne sont pas influencés par des tiers et qui sont toujours compréhensibles pour tous les systèmes d'exploitation.

Lien : www.av-test.org/fr



PORTABLEAPPS

> VOS PROGRAMMES SUR UNE CLÉ USB

Ce site permet de transformer tous vos programmes préférés en programmes «portables» prêts à être emportés sur une clé USB. Le service propose aussi des packs thématiques préconçus. Il suffit de brancher votre clé USB sur un ordinateur (ou de vous connecter à votre cloud) pour être comme chez vous.

Lien : <http://portableapps.com>



FRAMBOISE314

> RASPBERRY PI

François Mocq est un passionné d'informatique, de programmation et d'électronique.

Il est aussi le créateur de Framboise314, le site numéro un en France au sujet du Raspberry Pi. Vous savez maintenant où vous rendre si vous voulez en savoir plus sur cette bécane...

Lien : www.framboise314.fr



YGGTORRENT

> TRACKER SEMI-PRIVÉ

C'est le successeur du disparu t411. Un très bon tracker à mettre dans vos favoris. Il faudra vous inscrire, respecter la notion de ratio et utiliser un client Torrent pour les téléchargements... Attention, les clones pullulent !

Lien : <https://yggtorrent.gg>

YggTorrent website showing a list of torrents. The table lists various torrents with columns for name, size, seeders, leechers, and status.

NAME	SIZE	SEEDERS	LEECHERS	STATUS
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%
Game of Thrones (2011-2019) [1080p] [x264] [AAC] [5.1] [100MB]	12.1	120	120	100%

DEALABS > DES BONS PLANS EN PAGAILLE !

C'est une trouvaille que le rédacteur en chef a faite sur Twitter. Dealabs vous propose les meilleurs plans hi-tech du Net (mais pas que) : Offres de remboursement, réductions, offres spéciales, déstockages, soldes, etc. Il suffit de cliquer et de profiter des promos...

Lien : www.dealabs.com



LE MAILING-LIST OFFICIELLE de *Pirate Informatique* et des *Dossiers du Pirate*

**INSCRIVEZ-VOUS
GRATUITEMENT !**

De nombreux lecteurs nous demandent chaque jour s'il est possible de s'abonner. La réponse est non et ce n'est malheureusement pas de notre faute. En effet, nos magazines respectent la loi, traitent d'informations liées au monde du hacking au sens premier, celui qui est synonyme d'innovation, de créativité et de liberté. Depuis les débuts de l'ère informatique, les hackers sont en première ligne pour faire avancer notre réflexion, nos standards et nos usages quotidiens.

Mais cela n'a pas empêché notre administration de référence, la «Commission paritaire des publications et agences de presse» (CPPAP) de refuser nos demandes d'inscription sur ses registres. En bref, l'administration considère que ce que nous écrivons n'intéresse personne et ne traite pas de sujets méritant débat et pédagogie auprès du grand public. Entre autres conséquences pour la vie de nos magazines : pas d'abonnements possibles, car nous ne pouvons pas bénéficier des tarifs presse de la Poste. Sans ce tarif spécial, nous serions obligés de faire payer les abonnés plus cher ! Le monde à l'envers...

La seule solution que nous avons trouvée est de proposer à nos lecteurs de s'abonner à une mailing-list pour les prévenir de la sortie de nos publications. Il s'agit juste d'un e-mail envoyé à tous ceux intéressés par nos magazines et qui ne veulent le rater sous aucun prétexte.

Pour en profiter, il suffit de s'abonner directement sur ce site

<http://eepurl.com/FLOOD>

(le L de «FLOOD» est en minuscule)

ou de scanner ce QR Code avec votre smartphone...



NOUVEAU !

La rédaction se dote d'un compte Twitter !
twitter.com/ben_IDPresse



Vous trouverez des news inédites, des liens exclusifs vers des articles au format PDF et nous vous tiendrons aussi au courant de la sortie des publications. Rejoignez-nous !

TROIS BONNES RAISONS DE S'INSCRIRE :

- 1 Soyez averti de la sortie de *Pirate Informatique* et des *Dossiers du Pirate* en kiosques. Ne ratez plus un numéro !
- 2 Vous ne recevrez qu'un seul e-mail par mois pour vous prévenir des dates de parutions et de l'avancement du magazine.
- 3 Votre adresse e-mail reste confidentielle et vous pouvez vous désabonner très facilement. Notre crédibilité est en jeu.

Votre marchand de journaux n'a pas *Pirate Informatique* ou *Les Dossiers du Pirate* ?

Si votre marchand de journaux n'a pas le magazine en kiosque, il suffit de lui demander (gentiment) de vous commander l'exemplaire auprès de son dépositaire. Pour cela, munissez-vous du numéro de codification L12730 pour *Pirate Informatique* ou L14376 pour *Les Dossiers du Pirate*.

Conformément à la loi «informatique et libertés» du 6 janvier 1978 modifiée, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent.



ANONYMAT

LIBERTÉ

SMARTPHONE WHATSAPP

RASPBERRY PI ANTIVIRUS

MOTS DE PASSE

ANTI-SURVEILLANCE

MATÉRIELS ESPIONS

PRISE DE CONTRÔLE

JEUX VIDÉO

CLOUD

CHIFFRAGE CRACK



PIRATE
INFORMATIQUE



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