# Un site Internet pour le règlement en ligne des litiges


Un site Internet pour le règlement en ligne des litiges

---

**Si vous avez un problème concernant un achat en ligne, vous pouvez utiliser ce site pour essayer d'obtenir un règlement extrajudiciaire.**
Pour l'utiliser, vous devez vivre dans l'Union Européenne et le professionnel concerné doit y être établi
Les professionnels de certains pays peuvent également utiliser ce site pour déposer plainte contre un consommateur concernant un bien ou service vendu en ligne. … [Lien vers le site https://webgate.ec.europa.eu]

---

Réagissez à cet article

Source : *Accueil – Règlement en ligne des litiges*

---

# Comment un pirate a fait pour pirater Le FBI ?


Comment un pirate a fait pour pirater Le FBI ?

**Il y a quelques jours un pirate a pris contact avec le site Motherboard pour se vanter d'avoir récupéré des données sur un ordinateur du département de la Justice américain. Aujourd'hui un autre site, The Telegraph, indique que, selon un porte-parole du service, les données ne seraient pas à caractère sensible mais que des investigations sont en cours.**
Sur le site qui a dévoilé l'affaire en premier il est intéressant de suivre le récit de l'attaquant qui a réussi à pirater le système.

Tout a commencé lorsqu'il a réussi à avoir accès à un compte email appartenant à sa victime, un employé du département de la justice. Il n'explique pas comment il a pu obtenir cet accès mais a pu utiliser le compte puisqu'il est rentré en contact avec le journaliste par ce biais.

**Le département de la justice a fourni le code**
A partir du compte le hacker a tenté de se connecter, sans succès dans un premier temps, au portail intranet du département de la Justice. Devant cet échec, il a ensuite directement pris contact avec le support du service prétextant être nouveau et n'arrivant pas à accéder au portail. Son correspondant l'a simplement questionné pour savoir s'il était en possession du code de sécurité et, constatant que ce n'était pas le cas, lui en a fourni un sans difficulté.

Une fois connecté au service, le pirate a ensuite pu prendre la main à distance sur l'ordinateur personnel de sa victime. C'est ce qui lui a permis de récupérer les données, dont les noms et informations de contacts de 22000 employés du FBI. Sur 1 To de fichiers, seuls 200 Go seraient passés entre les mains du pirate qui dit détenir des documents incluant des informations de contact de militaires et des numéros de cartes de crédit.
Un compte email est relativement simple à pirater puisqu'il s'agit la plupart du temps de deviner ou dérober le mot de passe grâce à des méthodes d'ingénierie sociale. Des protections supplémentaires existent pourtant, la plupart des services proposent notamment un système de double authentification qui nécessite la saisie d'un code reçu par SMS en plus du mot de passe… [Lire la suite]

---

Réagissez à cet article

Source : *Piratage du FBI : le hacker a simplement demandé le code d'autorisation – CNET France*

# Google déclare la guerre à Daech

| | |
|---|---|
|  | **Google déclare la guerre à Daech** |

**Le moteur de recherche vient d'annoncer la mise en place de nouveaux moyens pour lutter contre la radicalisation en ligne. Facebook et Twitter collaborent.**


Le moteur de recherche Google prend des mesures pour lutter contre la radicalisation sur Internet. Le moteur de recherche Google prend des mesures pour lutter contre la radicalisation sur Internet.

La cyberguerre est déclarée. Engagée après les attentats de Paris par les très mystérieux hackers d'Anonymous, elle est aujourd'hui rejointe par Google. Lors d'une réunion avec le comité des affaires intérieures britanniques, Anthony House, un cadre de l'entreprise de Moutnain View, a exposé les plans mis en place pour lutter contre la propagande djihadiste, rapporte The Telegraph . Le géant du Web prévoit de rediriger les recherches « pro-Daech » vers des sites luttant contre la radicalisation. En effet, parmi les recrues de l'État islamique, nombreuses sont celles qui ont été endoctrinées derrière leur écran.

Mais, si l'offensive semble nouvelle, les géants d'Internet n'en sont pas à leur coup d'essai. En 2014, Google avait déjà fait retirer 14 millions de vidéos, dont certaines pour propagande, de sa plateforme YouTube.

Selon Yahoo News, Facebook a pour sa part développé au moins cinq cellules dédiées à la lutte contre le terrorisme et suit au plus près les profils signalés. Enfin, le réseau social travaille en collaboration étroite avec des imams, pour aider à la déradicalisation.

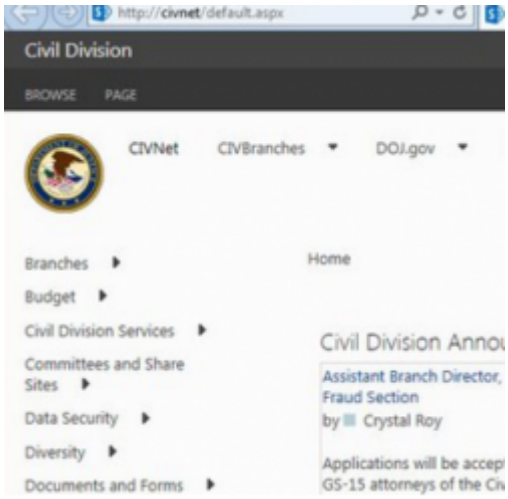
De son côté, Twitter déclare avoir supprimé plus de 10 000 comptes ouvertement djihadistes. Nick Pickles, chargé de la politique publique du site de microblogging en Grande-Bretagne, a annoncé : « Twitter, qui a 320 millions d'utilisateurs, emploie plus de 100 personnes pour s'occuper du contenu inapproprié. » Dans cette cyberbataille, Anonymous vient de trouver des alliés de taille. … [Lire la suite]

---

Réagissez à cet article

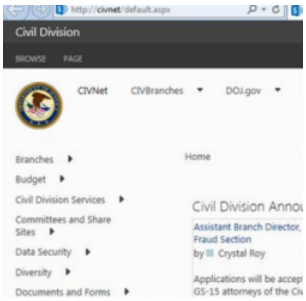
Source : *Google déclare la guerre à Daech*

# Hack au FBI : Les données privées de 22 175 employés du FBI piratées




Hack au FBI : Les données privées de 22 175 employés du FBI piratées

**Un hacker est parvenu à s'introduire sur l'intranet du ministère américain de la Justice et à télécharger 200 Go de fichiers incluant des noms, numéros de téléphones et mails de 22 175 employés du FBI mais également des données personnelles relatives à 9 372 personnes travaillant pour le ministère de la Sûreté Intérieure des Etats-Unis.**




Hack au FBI. Ce n'est malheureusement pas le nom d'une nouvelle série, mais bel et bien d'un second incident de sécurité majeur qui a permis de divulguer plusieurs dizaines de milliers de données personnelles d'employés du FBI mais également du ministère de la Sûreté Intérieure (Departement of Homeland Security). Si dans le précédent épisode du Hack of FBI en novembre dernier 3 000 coordonnées de policiers et de militaires américains s'étaient retrouvés dans la nature, le volume est donc cette fois-ci beaucoup plus important. Ainsi, le hacker, opérant sous le pseudonyme DotGovs sur Twitter, a publié une liste de 22 175 employés travaillant au FBI – parmi lesquels des agents spéciaux, analystes et officiers – incluant leurs noms, prénoms, fonctions mais également numéros de téléphone ainsi que leurs adresses mails. D'après Motherboard, qui s'est entretenu avec le hacker, ce dernier a également en sa possession des données personnelles appartenant à 9 372 employés de la Sûreté Intérieure américaine. Des données qui ont été également mises en ligne en tout début de semaine.

Alors que pour le précédent hack de données personnelles des employés du FBI, le groupe de hackers Crackas With Attitude s'en était pris au compte mail AOL du patron de l'agence, Mark Giuliano, le vol de données opéré par le mystérieux DotGovs a été effectué d'une toute autre manière. Ainsi, ce dernier a réalisé son méfait en piratant un compte mail d'un employé du département américain de la Justice. Le hacker a ensuite contacté le support du ministère en indiquant ne pas pouvoir se connecter au portail web. « Alors je les ai appelés et leur ai dit que j'étais nouveau et leur ai demandé comment accéder au portail », a expliqué le hacker à Motherboard. « Ils m'ont demandé si j'avais un code token, j'ai dit non, ils m'ont dit que ça allait et d'utiliser le leur. » Une fois connecté, le hacker raconte alors avoir cliqué sur un lien l'ayant amené sur une machine virtuelle en ligne et entré les identifiants du compte mail déjà hacké. « J'ai cliqué dessus et ai eu un accès total à l'ordinateur », a expliqué le pirate.

## Un détournement classique

« Ces comptes détournés peuvent uniquement être détectés grâce à la capacité d'observer et de détecter les changements dans le comportement de l'utilisateur, par exemple la connexion de l'utilisateur à son compte à un horaire inhabituel ou d'un endroit inhabituel, la vitesse de frappe sur son clavier ou d'execution des commandes, etc. C'est ce que l'on appelle, l'analyse comportementale des utilisateurs. Cette technologie permet de fournir un profil réel de chaque utilisateur, basé sur des caractéristiques personnelles – en quelque sorte sorte une empreinte digitale – et ainsi de détecter tout comportement anormal du compte utilisateur et d'en référer instantanément à l'équipe de sécurité voire même de bloquer en temps réel l'activité de l'utilisateur jusqu'à nouvel ordre », a par ailleurs précisé dans un communiqué Zoltán Györkő, PDG de l'éditeur en sécurité Balabit.
En tout, ce sont près de 200 Go de données confidentielles qui ont été téléchargées, alors que le hacker indique avoir eu accès à 1 To de données. « J'ai eu accès à ces données mais n'ai pas pu tout prendre », fait savoir DotGovs. Parmi les contenus qui sont passés entre ses mains ou ses yeux, on trouverait aussi des mails de militaires ainsi que des numéros de cartes bancaires. Suite à la parution de ces listes hackées de plus de 30 000 employés, le DHS a réagi par le biais de son porte-parole S.Y. Lee : « Nous recherchons les articles relatant les informations de contacts des employés du département de la sûreté intérieure qui ont été divulgués. Nous prenons très au sérieux ces articles, cependant rien ne permet d'indiquer à ce jour qu'il y ait eu violation d'informations sensibles ou personnelles. » … [Lire la suite]

---

Réagissez à cet article

Source : *Les données privées de 22 175 employés du FBI piratées – Le Monde Informatique*

---

# Programme de la 6eme Edition IT Forum à Dakar au Senegal Replay-


## Programme de la 6eme Edition IT Forum à Dakar au Senegal

---

**Colloque, Rencontre, IT Forum pour les managers IT africains**


**PROGRAMME DU JEUDI 18 FEVRIER 2015**
9h00-9h10 DISCOURS DE BIENVENUE
Par M. Mohamadou DIALLO, Directeur de la publication de Cio Mag
9h10-9h20 ALLOCUTION D'OUVERTURE
Approche nationale et régionale en matière de Cybercriminalité
Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications
9h20-9h30 ALLOCUTION Pays Invité d'honneur
Lutte contre la cybercriminalité, la Côte d'Ivoire renforce son arsenal
Par M. Bruno N. KONE, Ministre de la Postes et des Technologies de la Communication de Côte d'Ivoire, Porte-parole du Gouvernement

9h30-9h50 KEYNOTE SPEAKER
Pas d'Economie Numérique sans cyber-sécurité : Comment faire face aux tendances du numérique tout en maitrisant les défis du Cyberespace ?
Par M. Thierry BRETON, Président Directeur Général d'ATOS
9h50-10h00 KEYNOTE SPEAKER
L'Arrivée des réseaux haut débit, un accélérateur ou un moyen efficace de lutter contre les cyberattaques
Session Introductive
9h50-10h30 2 POINTS DE VUE
– Cybersécurité et protection des données à caractère personnel
Par M. Mouhamadou LO, Président de la Commission de Protection des Données Personnelles (CDP) du Sénégal
– Cybercriminalité : un enjeu international
Par M. Ali Drissa BADIEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest
Questions / Réponses

10h30-11h00 Pause café et visite des stands

11h00-12h00 Plénière 1
Cloud, Mobilité, big data, internet des objets, Byod : Comment intégrer les nouvelles tendances tout en maîtrisant les nouveaux risques inhérents ?
Modérateur: Commandant Guelpechetchin OUATTARA, Directeur de l'informatique et des Traces Technologiques de Côte d'Ivoire
· Représentant opérateur (Orange/Tigo ou Expresso Télécom)
· M. Chris MORET, Responsable de la Global Business Line CyberSecurity d'Atos Big Data & Secrity
· Dr. Alioune DIONE, Directeur des Systèmes d'Information de la Douane
· Colonel Julien DECHANET, Officier Cyber des Eléments français en Afrique de l'Ouest
· M. Jean-Paul PINTE, Expert International en Cybercriminalité,
· Alain DOLIUM, Co-fondateur et CEO EMEA North America de South Mobile Service,
Questions / Réponses

12h00-13h00 Plénière 2
Plan Numérique et Administration électronique : Quelles perspectives ?
Modérateur : M. Alain DUCASS, Expert en Transformation Digitale
· Présentation des grandes lignes du Plan stratégique pour le numérique (Côte d'Ivoire/Sénégal) Par M Euloge Kipeya SORO, Directeur Général de l'Agence Nationale du Service Universel des Télécommunications ( ANSUT)
· M. Malick NDIAYE Directeur de Cabinet du Ministère des Poste et des Télécommunications du Sénégal
· M. Mouhamed Tidiane Seck, Directeur Associé Performances Management Consulting
· M. Cheikh BAKHOUM, Directeur Général de l'Agence de l'Informatique de l'Etat (ADIE)
. M. Brice DEMOGE, Directeur du développement Secteur Public et Afrique – GFI Informatique
Questions / Réponses
13h00-14h00
Pause Déjeuner
14h00-15h00 Plénière 3
Retours d'expériences : solutions
· Plan de Sauvegarde et réplication des donnée après un incidents
· SAP s'engage pour la préservation du Parc Niokolokoba
· Cloud, l'essentiel pour les entreprises
Par Opérateur (Orange/Tigo ou Expresso Télécom)
· Applications métiers en mode Cloud, GFI informatique / Cegid
– Big data et sécurité, M. Alain DOLIUM, CEO South Mobile Services
Questions / Réponses
15h00-16h00 Plénière 4
Quelles solutions face à l'internationalisation de la cybercriminalité ?
· Modérateur : M. Pape Assane TOURE, Magistrat, Secrétaire général adjoint du Gouvernement
· M. Pape GUEYE, Elève Commissaire de Police, Ancien Chef de la Brigade de lutte contre la cybercriminalité
· M. Jean-François BEUZE, Président Directeur Général de Sifaris
· · M. Ali El AZZOUZI, Président Directeur Général Data Protect
· M. Richard NOUNI, Directeur Général de CFAO Technologies
· Retour d'expériences du secteur bancaire
Questions / Réponses

16h00-16h30
Pause café et visite des stands
16h30-17h30 Plénière 5
Point d'Echange Internet et ouverture du marché des FAI : Vers une amélioration de la qualité de l'Internet au Sénégal ?
Modérateur : M. Mohamadou SAIBOU, Directeur de l'ESMT Dakar
· M. Cheikh BAKHOUM, Président de SENIX (Point d'Echange Sénégal)
· M. Tidjane DEME, Google Afrique
· M. Ali Drissa BADIEL, Représentant de l'UIT (Union Internationale des Télécommunications) en Afrique de l'Ouest
· M. Alex CORENTHIN, Président d'ISOC Sénégal
· Représentant de l'ARTP
Questions / Réponses

17h30-17h45
SDE/Sodeci (Société d'électricité et d'eau de Côte d'Ivoire) face aux enjeux de l'électronique
SEM Sylvestre, Directeur Général de GS2E (Groupement d'intérêt économique de CIE et SODECI).
Clôture

17h45-18h00
DISCOURS DE CLOTURE
Perspectives sur les enjeux du haut débit mobile au Sénégal avec l'arrivée de la 4G
Par M. Yaya Abdoul KANE, Ministre de la Poste et des Télécommunications
**PRE-PROGRAMME DU VENDREDI 19 FEVRIER 2015**
Réflexion sur les chantiers de Modernisation de l'administration publique – Trois cas
9h00-9h15 Ouverture
DISCOURS D'OUVERTURE
Par M. Alioune SARR, Ministre du Commerce, du Secteur informel, de la Consommation, de la Promotion des produits locaux et des PME du Sénégal
9h15-10h00 Plénière 1
CAS 1 – SIGIF (Système Intégré de Gestion des Informations financières)
Le SIGIF, un enjeu de modernisation et de transparence dans la gestion des comptes publics
· Gestion intégrée des finances publiques : Retour d'expériences de la Côte d'Ivoire
Par Nongolougo SORO, Directeur Général de la SNDI
· Direction Générale de la comptabilité publique et du Trésor
· M. Ibrahima FAYE, Chef de l'Equipe Projet SIGIF au Ministère de l'Economie des Finances et du Plan
· M. Frédéric MASSE, VP SAP
· M. Jean-Michel HUET, Associé BearingPoint
Questions / Réponses

10h00-11h00 Plénière 2
CAS 2 – GUICHET UNIQUE
Guichet unique et impact sur le Doing business
· Directeur du commerce au Ministère du commerce
· Ibrahima DIAGNE, DG de Gaindé 2000
· Représentant de l'Apix
· Dr. Alioune DIONE, DSI de la Douane Sénégalaise`
Questions / Réponses

11h00-11h20
Pause café et visite des stands

11h20-12h00 Plénière 3
CAS 3 – FICHIER D'ETAT CIVIL
Modernisation du Fichier d'état civil, quel enjeu pour la gouvernance locale ?
Modérateur: André GRISSONNANCHE, PDG Exense
– M. Frédéric Massé, VP SAP,
– Mme Emilie Scalier, GDexpert
– M. Mouhamed Tidiane Seck, Directeur Associé Performances Management Consulting
– Jean-Pierre La Hausse de la Louvière, CEO d'iSTEC
– ADIE
– Ministère de l'Intérieur
– Direction de l'état civil
Clôture

12h00-12h20
DISCOURS DE CLOTURE
Par M. Abdoulaye Diouf SARR, Ministre de la gouvernance locale, du développement et de l'aménagement du territoire du Sénégal
12h20
Cocktail déjeunatoire

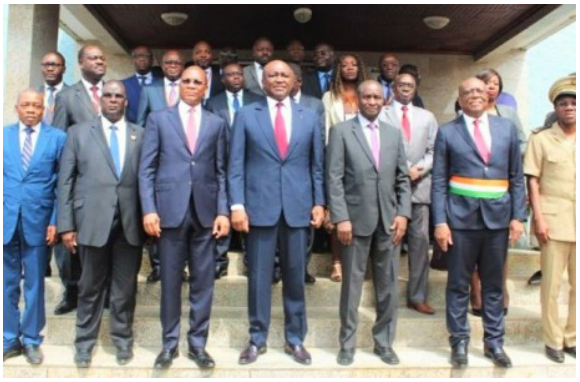
---

Réagissez à cet article

Source : *Programme 6eme Edition IT Forum Senegal – Colloque, Rencontre, IT Forum pour les managers IT africains*

---

# La cybercriminalité obstacle au développement de la Côte d’Ivoire

| | |
|---|---|
|  | La cybercriminalité obstacle au développement de la Côte d’Ivoire |

---

**La cybercriminalité constitue un obstacle au développement économique et social des pays africains, d'autant que cela détériore l'image des Etats et freine l'activité des investisseurs. C'est le constat fait par la centaine d'experts réunis depuis lundi à Grand-Bassam, Côte d'Ivoire, dans le cadre d'une Conférence internationale visant le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone.**

Organisée par l'Autorité de régulation des télécommunications/TIC de Côte d'Ivoire (ARTCI), la cérémonie d'ouverture de cette conférence, en présence du ministre d'Etat, ministre de l'Intérieur et de la Sécurité, Hamed Bakayoko, a permis au ministre de l'Economie numérique et de la Poste Bruno Koné de tirer sur la sonnette d'alarme.

Il a en effet appelé les spécialistes des questions de cybersécurité à rester sur le qui-vive, nonobstant le « solde positif » entre les avantages du numérique et les menaces qui en découlent. Difficile de lui donner tort. Le marché ouest-africain de la cybercriminalité parle de lui-même.
En 2013, la Côte d'Ivoire avait été durement touchée par ce fléau, avec une perte de 26 milliards de FCFA. Au Sénégal, on parle d'une perte de 15 milliards de FCFA due à la fraude sur la toile. Suffisant pour installer un climat de méfiance dans les transactions financières électroniques et un défaut de crédibilité face aux investisseurs.
Autant le dire : un plan d'action sur la cybersécurité et la cyberdéfense dans l'espace francophone s'avère nécessaire. Venus d'une vingtaine de pays, les experts présents à cette conférence internationale ont trois jours, pour proposer une stratégie concrète … [Lire la suite]

---

Réagissez à cet article

Source : *Côte d’Ivoire : plus de 100 experts dénoncent la cybercriminalité comme obstacle au développement | CIO-MAG*

---

# La cybersécurité un problème sous estimée par les chefs d’entreprises

| | |
|---|---|
|  | La cybersécurité un problème sous estimée par les chefs d’entreprises |

---

**Les entreprises se jugent souvent prêtes à résister aux cyber-attaques alors que la réalité est bien souvent moins reluisante.**

Plusieurs études sorties récemment convergent pour montrer un tableau assez catastrophique de la cybersécurité des entreprises alors que la perception affichée par celles-ci est plutôt marquée par l'optimisme. Ou bien faut-il mieux parler d'inconscience ? Ainsi, 62% des entreprises ont déjà subi une tentative de fraude selon une étude de Sage. 12% en ont même subi au moins cinq. La fraude la plus courante reste la fameuse *fraude au président*(usurpation d'identité d'un dirigeant pour obtenir un virement à l'étranger) : 80% des entreprises affectées l'ont rencontrée. 18% ont été victimes d'un *test bancaire* et 14% d'une fraude interne (cas classique : substitution de RIB).

Les trois quarts des DAF craignent avant tout les fraudes d'origines externes. La*fraude au président* et la falsification de RIB sont largement cités avant des cyber-attaques sur des données financières (un quart seulement des répondants). Des processus métier ont été mis en place pour parer ces fraudes non-technologiques comme la séparation créateur/valideur d'un paiement, la double signature… Le respect des procédures et la vigilance interne ont suffi à détecter des fraudes dans de nombreux cas. Mais 30% des entreprises continuent de valider leurs virements par un simple fax ! Suivant les recommandations des organismes professionnels, la bascule vers les traitements informatisés (EBICS TS, via les portails bancaires, etc.) est malgré tout bien engagée.

**Une méconnaissance des bonnes pratiques et des règles**

Mais il n'en demeure pas moins que la méconnaissance des bonnes pratiques pour sécuriser l'information reste importante. Selon une étude Solucom/Conscio, 46% des collaborateurs ne sont pas préparés à réagir à de l'ingénierie sociale dont la *fraude au président* n'est qu'un exemple caricatural. Pourtant, selon les auteurs de l'étude, l'ingénierie sociale est la méthode principale pour s'introduire dans les systèmes d'information des entreprises ou réaliser des fraudes, notamment par usurpation d'identité ou de couple identifiant/mot de passe.

Si 88% des collaborateurs sont sensibilisés aux règles pour gérer les mots de passe, 47% seulement les adoptent. Un mécanisme technique est donc nécessaire pour obliger à respecter les bonnes pratiques. Enfin, la même étude mentionne que la réglementation sur les données personnelles est méconnue par la majorité des collaborateurs, entraînant de ce fait un important risque juridique pour leurs entreprises.

**Bienvenue aux malwares**

L'ingénierie sociale est décidément bien ancrée dans les pratiques des cyber-criminels. Cibler précisément les attaques permet notamment, selon l'étude publiée par Cisco, d'introduire des #ransomware. Ce type d'attaque génèrerait 34 millions de dollars par an et par campagne. Etre victime de tels pratiques est assez gênant, ce qui explique sans doute que seules 21% des entreprises informent leurs partenaires, 18% les autorités et 15% leur compagnie d'assurance.

Bien entendu, les fondamentaux du cybercrime sont toujours d'actualité avec des variantes pour les maintenir au goût du jour. La compromission de serveurs est ainsi un classique pour mener des attaques indirectes, notamment via des CMS mal mis à jour. La compromission de domaines WordPress a ainsi augmenté de 221% entre février et octobre 2015. Parmi les mauvaises pratiques qui se développent, la non-mise à jour des infrastructures est en croissance.

La fuite de données via les navigateurs, souvent négligée, est pourtant en pleine croissance : des extensions malveillantes affecteraient 85% des entreprises. Les attaques à base de DNS sont également en plein boum, d'autant que les experts DNS ne travaillent que rarement avec les experts en sécurité. Malgré tout, il est estimé que la rapidité de détection d'une intrusion a augmenté même si elle reste dans une fourchette de 100 à 200 jours.

La cybersécurité sera le sujet de la Matinée Stratégique de CIO le 16 février 2016 : Cybersécurité : Les nouvelles menaces contre le système d'information. … [Lire la suite]

---

Réagissez à cet article

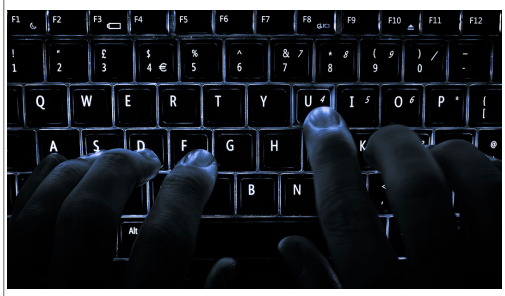
Source : *La cybersécurité reste une problématique sous estimée dans les entreprises – Le Monde Informatique*

# Comment les hackers font-ils pour pirater toutes vos données informatiques ?

| | |
|---|---|
|  | Comment les hackers font-ils pour pirater toutes vos données informatiques ? |

**Aujourd'hui, les informations sont partout avec le développement d'Internet. Il est donc important de savoir se prémunir contre les techniques employées pour nous pirater ou nous nuire. Surtout que les hackers, ces pirates du web, se développent de plus en plus et emploient des techniques toujours plus redoutables. SooCurious vous présente les techniques développées par ces génies malveillants de l'informatique.**

Vous le savez certainement, le monde d'Internet est dangereux et est le terrain de jeu de personnes malveillantes. Ces gens sont appelés des hackers : ce sont des pirates informatiques qui se servent de leur ordinateur pour récupérer des informations privées ou pour infiltrer des serveurs de grosses entreprises. D'où l'importance de bien choisir ses mots de passe. Avant de pirater, le hacker va enquêter sur sa cible. Il va chercher tout ce qu'il peut savoir sur la personne, à savoir l'adresse IP, le type de logiciels installés sur l'ordinateur de la « victime ». Ils trouvent facilement ces informations grâce aux réseaux sociaux, aux forums en ligne. Une fois qu'ils ont récupéré ces données, le travail de piratage peut commencer.



Hacker n'est pas à la portée de tout le monde : il faut une maîtrise totale de l'informatique pour y parvenir. Ces pirates 2.0 ont plusieurs techniques pour parvenir à leurs fins. La première d'entre elles est le clickjacking. L'idée est de pousser l'internaute à fournir des informations confidentielles ou encore de prendre le contrôle de l'ordinateur en poussant l'internaute à cliquer sur des pages. Sous la page web se trouve un cadre invisible, comme un calque, qui pousse la personne à cliquer sur des liens cachés.
Par exemple, il existe des jeux flash où l'internaute doit cliquer sur des boutons pour marquer des points. Certains clics permettent au hacker d'activer la webcam.

**Autre technique, peut-être plus courante, celle du phishing.**
Appelée aussi l'hameçonnage, cette action opérée par le pirate vise à soutirer une information confidentielle comme les codes bancaires, les mots de passe ou des données plus privées. Pour récupérer un mot de passe, un hacker peut aussi lancer ce qu'on appelle « une attaque par force brute ». Il va tester une à une toutes les combinaisons possibles (cf. faire un test avec Fireforce) avec un logiciel de craquage. Si le mot de passe est trop simple, le hacker va rapidement pénétrer votre ordinateur. D'autre part, les hackers cherchent parfois à craquer les clés WEP, afin d'accéder à un réseau wi-fi. Encore une fois, si la clé est trop courte, le craquage est facile. Le hacking se développant, des techniques de plus en plus pointues se développent.

**Vol des données bancaires via Shutterstock**
Il existe maintenant des armées de hackers ou des groupes collaborant dans le but de faire tomber des grosses entreprises ou des banques. Début 2016, la banque internationale HSBC a été piratée. A cause de cela, leur site était totalement inaccessible, ce qui a créé la panique chez les clients de cette banque. Cet épisode n'est pas isolé. Il est même le dernier d'une longue série. Pour parvenir à semer la panique dans de grandes firmes, ils utilisent des techniques plus ou moins similaires à celles présentées ci-dessus, mais de plus grande envergure.

**La technique du social engineering n'est pas une attaque directe.**
C'est plutôt une méthode de persuasion permettant d'obtenir des informations auprès de personnes exerçant des postes clés. Les pirates vont cibler les failles humaines, plutôt que les failles techniques. Un exemple de social engineering serait l'appel fait à un administrateur réseau en se faisant passer pour une entreprise de sécurité afin d'obtenir des informations précieuses.

**Autre méthode, celle du défaçage.**
Cette dernière vise à modifier un site web en insérant du contenu non désiré par le propriétaire. Cette méthode est employée par les hackers militants qui veulent dénoncer les pratiques de certains gouvernements ou entreprises. Pour ce faire, le hacker exploite une faille de sécurité du serveur web hébergeant le site. Ensuite, il suffit de donner un maximum d'audience au détournement pour décrédibiliser la cible. En avril 2015, le site de Marine Le Pen a été victime de défaçage : des militants ont publié une photo de femme voilée avec un message dénonçant la stigmatisation des musulmanes par le FN.

Enfin, les hackers se servent aussi du DDOS (déni de service distribué), qui sature un service pour le rendre inaccessible et du Buffer Overflow, qui provoque une défaillance dans le système pour le rendre vulnérable… [Lire la suite]

---

Réagissez à cet article

Source : *Comment les hackers font-ils pour pirater toutes vos données informatiques ? | SooCurious*

---

# Le site Internet des Pays de la Loire piraté

| | |
|---|---|
|  | **Le #site Internet des Pays de la Loire piraté** |

---

**Après le site web du Parti Socialiste, les Anonymous ont attaqué celui du conseil régional des Pays de la Loire pour protester contre une pétition demandant l'évacuation de la ZAD de Notre-Dame des Landes.**

Le site Internet du Conseil régional des Pays de la Loire a été altéré suite à une attaque dans la nuit de dimanche à lundi revendiquée par les Anonymous selon France Bleu. Le groupe d'activistes entend protester contre le projet d'aéroport à Notre-Dame des Landes et plus précisément contre la pétition en ligne demandant l'évacuation de la ZAD (Zone d'aménagement différée) à l'initiative de Bruno Retailleau, président du conseil régional. Le site est toujours bloqué avec une page indiquant simplement : « Cette page est introuvable. Merci de revenir un peu plus tard. »


Dans un communiqué, le groupuscule indique que « grâce au piratage du site du Conseil régional nous entendons démontrer à tous et toutes comment les citoyens ont été délibérément trompés et manipulés par Bruno Retailleau ». Les activistes, qui assurent avoir récupéré le listing des votants, contestent en effet l'organisation de cette pétition : « Nous avons pu constater que certains mails sont comptabilisés plusieurs dizaines de fois, et les mêmes adresses IP ont pu inscrire des dizaines d'adresses mails à la suite, sans aucune vérification, poursuivent les Anonymous. N'importe quelle adresse mail peut ainsi s'enregistrer sans aucune preuve de son authenticité. Au total, près de 40 % des signatures seraient à décompter. »

## Aucune donnée dérobée

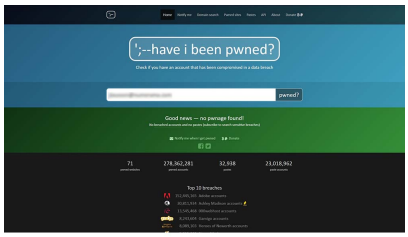
Ce n'est pas la première fois que les Anonymous s'intéressent au projet d'aéroport de Notre-Dame des Landes. Le 26 janvier dernier, ils avaient déjà lancé une attaque de type DDoS contre le site web du Parti Socialiste pour protester pêle-mêle contre l'instauration de l'État d'urgence, les perquisitions et les arrestations non-fondées qui ont notamment touché les opposants à l'aéroport de Notre-Dame des Landes. Le groupe avait précisé qu'il envisageait d'autres actions « si l'état d'urgence n'était pas rectifié ». C'est désormais chose faite avec le blocage du site des Pays de la Loire qui n'est toujours pas revenu à cette. Le Conseil général, qui s'active toujours avec ses prestataires pour remettre sa vitrine, a indiqué … [Lire la suite]

---

Réagissez à cet article

Source : *Les Anonymous piratent le site des Pays de la Loire – Le Monde Informatique*

# Comment vérifier si vos données ont été piratées

| | |
|---|---|
|  | **Comment vérifier si vos données ont été piratées** |

**Un service sur lequel vous êtes inscrit a été piraté et vous craignez pour vos données personnelles ? Un site permet de vérifier si votre e-mail est concerné.**
Il ne se passe pas une semaine sans que l'actualité ne se fasse l'écho d'une attaque informatique ayant visé un site web ou une application, et leurs données personnelles. Et l'histoire est souvent la même d'une affaire à l'autre. Il s'agit en général de pirates qui profitent d'une faille dans la protection du service pour dérober les données personnelles de ceux qui ont ouvert un compte en faisant confiance à la sécurisation des données.


**Gare à votre e-mail !**

Ces informations sont ensuite diffusées sur le net, exploitées pendant des actions de phishing (hameçonnage) destinées à récupérer frauduleusement d'autres éléments ou bien font l'objet d'un commerce.
**Normalement, les sites qui ont fait l'objet d'un piratage alertent leurs membres par mail. En règle générale, celui-ci comporte des indications sur ce qui s'est passé et, surtout, des recommandations à suivre sans tarder : modification du mot de passe et surveillance des comptes en banque, par exemple.**
**Mais il peut arriver que ce courrier ne soit pas vu par le destinataire : parce qu'il est tombé dans les spams, parce qu'il a été supprimé par mégarde ou parce que l'internaute utilise depuis un moment une nouvelle adresse de courrier électronique.**
*EST-CE QUE JE ME SUIS FAIT AVOIR ?*
*D'où l'intérêt d'un site comme « **Have I Been Pwned ?** » (que l'on pourrait traduire par « est-ce que je me suis fait avoir ? »). Le principe est simple : vous entrez votre adresse mail dans le champ prévu à cet effet et le site vous indique si votre mail est concerné par une fuite de données personnelles.*
*Deux cas de figure peuvent se présenter.*


*Pas de problème !*
*Si votre mail n'est pas recensé sur « Have I Been Pwned ? », c'est bon signe. Cela veut dire que sur les services dont le site assure le suivi, votre adresse n'a – a priori – pas fait l'objet d'une fuite. Mais attention, si le site ne trouve rien, cela ne veut pas dire que tout va pour le mieux dans le meilleur des mondes.*
*En effet, vous êtes peut-être présent sur des services dont le piratage n'a pas été relevé par « Have I Been Pwned ? », ou dont les listings de données n'ont pas été diffusés. De plus, il peut être sage de vérifier que tout va bien avec vos autres adresses, si vous en avez. Car peut-être étiez-vous inscrit avec un ancien mail.*


*C'est mauvais signe.*
*Et dans le cas contraire ? Si votre mail figure dans la base de données de « Have I Been Pwned ? », c'est le moment de s'inquiéter. Les sites qui n'ont pas su vous protéger seront visibles dans un encart situé plus bas. Dans notre cas, l'une de nos adresses était utilisée sur deux sites qui ont été piratés en septembre et décembre 2015.*
*Si votre mail figure dans la base, sachez que des éléments complémentaires, comme la date de la fuite et la nature des données compromises (le mot de passe, le nom d'utilisateur ou l'activité sur le site web), sont donnés, lorsqu'ils sont connus.*
***HAVE I BEEN PWNED ?***
*À l'heure actuelle, « Have I Been Pwned ? » prend en compte 71 sites web ou applications et plus de 278 millions de comptes compromis. Parmi les services qui sont pris en compte figurent Adobe, Ashley Madison, Gmail, Snapchat, YouPorn, Battlefield Heroes ou encore Yahoo. Un classement liste également les dix piratages les plus spectaculaires.*
*Reste une question, qui est tout à fait légitime : « Have I Been Pwned ? » n'est-il pas un site de façade qui ne servirait en fait qu'à inciter les internautes à donner leurs adresses web, dans le but de mener ensuite des **campagnes de hameçonnage** pour dérober encore plus de données personnelles ?*
*Dans sa **foire aux questions**, le site assure qu'aucune information de ce type n'est gardée en mémoire. Quant à la personne qui s'occupe de ce service, il s'agit d'un informaticien indépendant a priori digne de confiance, **Troy Hunt**. Celui-ci n'est pas un total inconnu : c'est un expert reconnu dans le milieu de la sécurité informatique et a été distingué par Microsoft.*

---

***Réagissez à cet article***

Source : *Un site pour vérifier si vos données ont été piratées – Tech – Numerama*