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*

Comment maîtriser sa réputation sur Internet ?

Comment maîtriser sa réputation sur Internet ?

La montée des outils en ligne et leur utilisation massive fait évoluer notre visibilité : nous jouissons tous d'une e-réputation ou image en ligne qu'il s'agit de piloter, suivre, voire rectifier. Il est nécessaire de définir les messages que nous souhaitons véhiculer et surveiller les éléments négatifs qui peuvent apparaître.

Tout ce que nous communiquons volontairement ainsi que l'ensemble des données issues d'autres interlocuteurs constituent une masse d'informations visibles et disponibles qui forgent une image de soi sur le net et construisent la perception des internautes sur notre identité.

Pourquoi l'utiliser ?

Gérer sa e-réputation est désormais devenu incontournable : il s'agit de réfléchir à l'image que l'on souhaite développer, aux messages que nous délivrons, aux modes de communication adéquats pour notre objectif. Faire de la veille sur sa e-réputation nécessite également une analyse claire et étayée de ce que disent et pensent les internautes de nous.

Il n'y a pas de moment précis pour développer sa e-réputation : c'est un travail de tous les jours et de longue haleine. Néanmoins, certains contextes ou périodes stratégiques (par exemple des entretiens avec des chasseurs de tête ou des directeurs de ressources humaines) sont des moments clé pour se googliser !

Comment l'utiliser ?

7 étapes pour maîtriser son identité en ligne :

• Définir sa stratégie de communication personnelle : votre Personal Branding, vos messages phares, les personnes ou organismes à atteindre et les meilleurs canaux de communication à utiliser.

• Élaborer sa net strategy : sur quels outils web voulez-vous apparaître ? Faut-il créer de nouveaux supports ? Par exemple, vous pouvez être présents sur les réseaux sociaux professionnels existants tels que Viadeo LinkedIn mais également créer vote blog personnel pour mettre en avant votre expertise.

• Se construire un » personnage » : choisissez les mots-clés et les images qui vous représentent.

• Faire vivre son identité numérique et sa » marque » par une présence régulière et un mode de communication identifiable.

• Décider d'être présent (ou pas) sur les différents réseaux sociaux personnels et professionnels et personnaliser les préférences et paramètres de sécurité ou confidentialité : maîtrisez au mieux votre image et la visibilité de vos informations.

• Ne pas hésiter à supprimer ou bannir des utilisateurs si nécessaire.

• Faire de la veille et regarder régulièrement comment on apparaît dans les moteurs de recherche. Analysez les commentaires que les autres font de vous et réagissez !

Gérer sa e-réputation est un exercice d'analyse et de diagnostic des résultats positifs, neutres ou négatifs qui apparaissent quand on recherche son nom sur les principaux moteurs de recherche. Avoir du contenu positif qui apparaît sur la première page d'un moteur de recherche comme Google contribue à asseoir votre image et à véhiculer des éléments positifs potentiellement contributeurs du succès ou de nouveaux business. Si un bad buzz vous concernant apparaît, le détecter rapidement grâce à la veille permet de réagir et de répondre à vos détracteurs en mettant en oeuvre les actions correctrices utiles…. [Lire la suite]

Réagissez à cet article

Source : *La e-réputation : maîtriser son identité en ligne – Paperblog*

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*

Comment analyser votre e-réputation sur Internet en un instant ?

	Comment analyser votre e-réputation sur Internet en un instant ?

Nothing to Hide devrait intéresser certains d'entre vous et c'est tout à fait normal car ce service va vous permettre d'analyser votre e-réputation en quelques secondes. Grâce à lui, vous saurez donc si tous les contenus partagés sur vos profils sociaux pourront un jour se retourner contre vous. Plutôt pratique, non ?
Les internautes sont de plus en plus actifs sur les réseaux sociaux et certains d'entre eux n'hésitent pas à partager toute leur vie sur Twitter, Facebook ou même Instagram.

Le moment est peut-être venu de commencer à soigner votre e-réputation.
Le problème, c'est que la plupart de ces données sont rendues publiques. Il suffit donc d'une requête bien sentie sur un de ces services pour trouver les photos et les publications de n'importe quel utilisateur.

Avez-vous confiance en votre e-réputation ?
La question qui se pose, c'est évidemment de savoir si votre futur patron appréciera de vous voir poser à poil devant l'objectif avec votre cousin Bébert sur les plages nudistes de la Baule, ou s'il appréciera le petit coup de gueule que vous aviez poussé en novembre 2013 contre « ces salauds de patrons qui vous sucent jusqu'à la moelle ».
Dans ce contexte, il est tout à fait primordial de soigner son e-réputation et Nothing to Hide va justement vous permettre de prendre un peu de recul sur tout ce que vous publiez à longueur de temps sur vos profils sociaux.
Le service va ainsi commencer par vous demander de vous connecter à vos comptes Twitter, Facebook, LinkedIn et Instagram.
Lorsque ce sera fait, il vous posera une vingtaine de questions personnalisées en fonction des contenus publiées sur cette plateforme et il vous demandera notamment si vous assumez telle ou telle photo ou si vous être toujours d'accord avec cette vieille publication que vous aviez (forcément) oubliée.

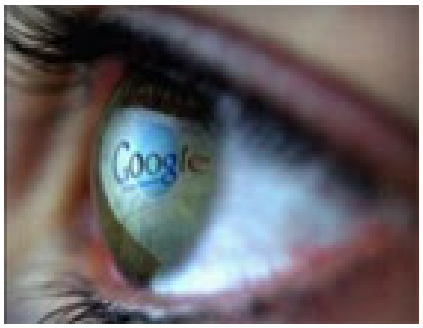
La procédure dure quelques minutes à peine
La procédure dure quelques minutes. Ensuite, le service vous affichera un score variant en fonction de vos données et de vos réponses.
Il vous permettra de savoir si vous assumez réellement vos publications et si votre réputation numérique se porte bien.
Mieux, Nothing to Hide va aussi vous attribuer un grade et il affichera en plus quelques alertes dans la foulée. Elles ne sont pas toutes très pertinentes en revanche. Tenez, par exemple, le service me reproche de ne pas connaître tous mes followers sur Instagram par exemple.
Ceci étant, il devrait tout de même être utile à certains d'entre vous, et surtout à ceux qui sont en recherche d'emploi.
Oui, car les recruteurs trainent aussi beaucoup sur les réseaux sociaux…

… [Lire la suite]

Réagissez à cet article

Source : *Avec Nothing to Hide, vous allez pouvoir analyser votre e-réputation en un instant*

Un casque de réalité virtuelle totalement autonome signé Google



Un casque de réalité virtuelle totalement autonome signé Google

---

Alors que la rumeur initiale prêtait à Google l'intention de développer un casque de réalité virtuelle fonctionnant avec un smartphone, le Wall Street Journal affirme qu'il s'agirait en fait d'un appareil totalement autonome.

Google travaillerait sur un casque de réalité virtuelle tout en un, capable de fonctionner sans être connecté à un smartphone, un ordinateur ou une console de jeu. C'est ce qu'affirme le Wall Street Journal qui ajoute que la firme de Mountain View compte sortir cette année une évolution de son Carboard, le casque en carton qui s'adapte sur des smartphones.

Il s'agirait cette fois d'une version en plastique qui intégrerait des capteurs et un processeur. En début de semaine, le Financial Times avait fait allusion à ce second modèle, mais n'avait pas évoqué de casque tout en en un.

Selon les informations du Wall Street Journal, le modèle autonome sur lequel planche Google serait équipé d'un processeur haute performance développé par Movidius, l'entreprise qui lui fournit déjà les puces pour ses terminaux du Projet Tango. Il incorporerait aussi des caméras frontales pour suivre les mouvements de tête de l'utilisateur. La date de lancement de ce casque ne serait pas encore très claire. En revanche, le modèle en plastique pourrait être dévoilé … [Lire la suite]

Réagissez à cet article

Source : *Google développerait un casque de réalité virtuelle totalement autonome*

La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données

La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données

---

La Commission Nationale de l'Informatique et des Libertés a publiquement mis en demeure Facebook de ne plus placer de cookies indésirables sur les postes des utilisateurs et d'arrêter le transfert des données personnelles de ses membres vers les Etats-Unis.

Le géant des réseaux sociaux a 3 mois pour se conformer à cette décision sous peine de sanction. La Commission Nationale de l'Informatique et des Libertés (CNIL) a ordonné à Facebook de stopper le transfert de certaines données personnelles de ses utilisateurs vers les Etats-Unis et de changer la façon dont elle récolte leurs données lorsqu'ils visitent son site web.
Dans sa mise en demeure, rendue publique lundi en fin de journée, la CNIL reproche ainsi à Facebook de transférer les données de ses membres aux Etats-Unis sur la base du Safe Harbor « ce qui n'est plus possible depuis la décision de la Cour de Justice de l'Union Européenne du 6 octobre 2015 », rappelle la commission.
La liste des griefs ne s'arrête pas là : « Le site dépose sur l'ordinateur des internautes des cookies à finalité publicitaire, sans les en avoir au préalable correctement informés ni avoir recueilli leur consentement », indique la CNIL.
Autre constat et non des moindres : « La CNIL a constaté que le site Facebook est en mesure de suivre la navigation des internautes, à leur insu, sur des sites tiers alors même qu'ils ne disposent pas de compte Facebook. En effet, le site dépose un cookie sur le terminal de chaque internaute qui visite une page Facebook publique, sans l'en informer. »… [Lire la suite]

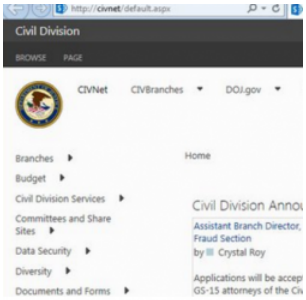
Réagissez à cet article

Source : *La CNIL lance un ultimatum à Facebook au sujet des*

cookies et des transferts de données – Le Monde Informatique

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*

Toutes les versions de Windows touchées par une faille critique

Toutes les versions de Windows touchées par une faille critique

---

Toutes les versions de Windows, dont Windows 10, sont affectées par une faille critique pour laquelle un correctif est disponible. La vulnérabilité permet d'exécuter arbitrairement du code.

Le dernier Patch Tuesday de Microsoft est léger en correctifs critiques, mais une faille majeure cependant affecte l'ensemble des versions supportées de Windows.

Dans son bulletin de sécurité mensuel, Microsoft informe les utilisateurs de la nécessité de patcher immédiatement une vulnérabilité sérieuse au niveau de la façon dont le système d'exploitation gère certains fichiers. Toutes les versions de Windows sous support sont concernées, de Windows Vista à Windows 10.

La faille (MS16-013) pourrait permettre à un attaquant d'exécuter arbitrairement du code comme l'utilisateur authentifié sur la session Windows. Les risques sont donc accrus pour les utilisateurs avec un compte doté des droits administrateur.

Autres vulnérabilités dans Office, IE et Edge

Pour réaliser l'attaque, le pirate doit amener l'utilisateur à ouvrir un fichier Journal spécialement forgé. Il pourra ainsi exécuter des programmes, supprimer des données et même créer de nouveaux comptes avec tous les droits sur le poste Windows.

Windows Server 2016 Tech Preview 4 est également affecté par la vulnérabilité et le correctif doit donc aussi être déployé sur ces configurations. Microsoft précise toutefois n'avoir à ce jour détecté aucune exploitation de cette faille Windows.

A noter que l'éditeur a publié trois autres correctifs pour des vulnérabilités critiques de Windows et Office.

MS16-012 corrige une faille permettant à un attaquant d'exécuter du code en exploitant un fichier PDF compromis. Les utilisateurs de Windows 8.1 et Windows 10 sont principalement touchés. Le problème de sécurité a été signalé à l'éditeur par un tiers et ne ferait pas l'objet d'attaques.

MS16-015 remédie à plusieurs failles de corruption mémoire dans Microsoft Office. Elles autorisent des attaques par le biais de fichiers Office malveillants. Leur exploitation permet d'obtenir des droits équivalents à ceux de l'utilisateur de la session ouverte.

MS16-022 corrige enfin de nombreuses vulnérabilités d'Adobe Flash Player dans Windows 8.1 et versions suivantes de l'OS Microsoft.

L'éditeur diffuse par ailleurs un patch cumulatif pour Internet Explorer (MS16-009) et le nouveau navigateur de Windows 10, Microsoft Edge (MS16-011). Les différentes failles ne feraient l'objet d'aucune exploitation avant la diffusion des correctifs, toujours selon la firme de Redmond… [Lire la suite]

Réagissez à cet article

Source : *Toutes les versions de Windows touchées par une faille critique*

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

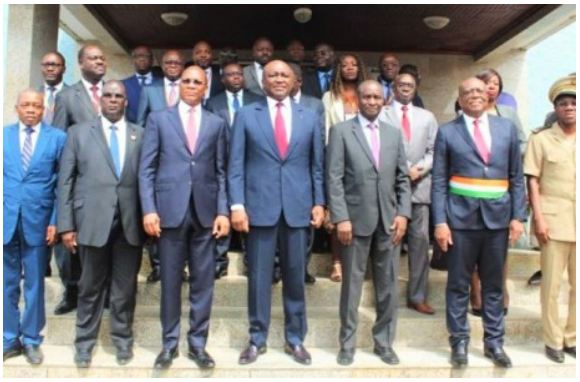
11h20-12h00 Plénière 3
CAS 3 – FICHIER D'ETAT CIVIL
Modernisation du Fichier d'état civil, quel enjeu pour la gouvernance locale ?
Modérateur: André GRISSONNANCHE, PDG Exense
– M. Frédéric Massé, VP SAP,
– Mme Emilie Scalier, GDexpert
– M. Mouhamed Tidiane Seck, Directeur Associé Performances Management 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*