Un ado attaque sa mère en justice parce qu’elle lui avait confisqué son smartphone

Un ado attaque sa mère en justice parce qu’elle lui avait confisqué son smartphone

Parfois les adolescents ont des réactions bien surprenantes face à certaines situations. En Espagne, un ado de 15 ans a attaqué sa mère en justice pour lui avoir confisqué son smartphone. Une réaction disproportionnée que le juge n'a pas manqué de souligner. Non seulement le jeune homme a perdu son procès, mais il a en plus eu droit à un joli sermon.

Ah l'adolescence ! Cette période difficile de passage à l'âge adulte laisse place parfois à des réactions bien étonnantes. Néanmoins, certains ados vont tout de même plus loin que d'autres. Et dans le genre relation conflictuelle avec les parents, celui-ci est plutôt bien classée.
En Espagne, à Almeria, **un adolescent de 15 ans a porté plainte contre sa mère** parce que cette dernière lui avait confisqué son smartphone. Oui, c'est assez hallucinant, mais c'est bien vrai. Toute la presse locale en Andalousie en a parlé.

Un ado porte plainte contre sa mère qui l'avait privé de son smartphone

Il s'agit pourtant d'une histoire on ne peut plus banale. L'adolescent à l'origine de la plainte avait des mauvais résultats scolaires depuis quelques temps. Afin de le recadrer, **sa mère lui a confisqué son smartphone.** Une mesure que de nombreux parents peuvent prendre, rien de plus normal.
Mais plutôt que de pester contre sa mère et d'aller bouder à l'arrêt de bus avec ses copains, le jeune garçon de 15 ans a décidé d'aller porte plainte contre sa mère. Face à une demande si surprenante, les policiers ont tenté de raisonner le jeune homme, mais ce dernier a bien validé la plainte pour mauvais traitements.

Le juge félicite la mère

La plainte validée, la mère et l'adolescent sont passés devant le juge Luis Columna. L'histoire ne nous dit pas s'ils y sont partis ensemble en voiture. Toujours est-il qu'après avoir écouté les deux partis, **le juge a non seulement donné raison à la mère, mais il l'a en plus félicitée…**[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

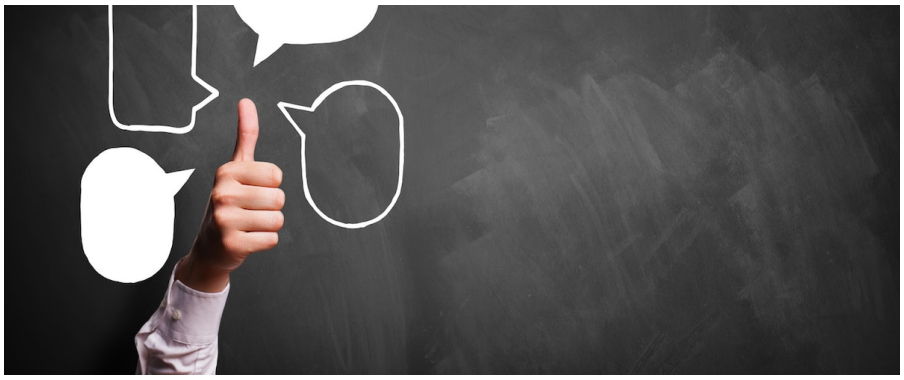
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Insolite : un ado attaque sa mère en justice parce qu'elle lui avait confisqué son smartphone*

Comment bien nettoyer sa réputation sur Internet ?



Comment bien nettoyer sa réputation sur Internet ?

Quand on se lance dans une recherche d'emploi, on regrette parfois des écrits maladroits ou des photos peu flatteuses du passé. Voici comment nettoyer sa réputation sur Internet.
[Lire la suite]

Notre métier : Vous aider à retirer de l'information sur Internet. Que ça soit à l'amiable ou dans le cadre d'une action judiciaire, nous pouvons vous accompagner pour retirer ou rendre moins visibles des informations sur Internet.
contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Nettoyer sa réputation sur Internet, c'est possible ? | JDM*

Tim Cook, patron d’Apple inquiet par l’effet « Fausses news »

Tim Cook, patron d’Apple inquiet par l’effet « Fausses news »

Les fausses news, hoax et articles tendancieux ont une influence néfaste sur l'esprit des internautes, assure Tim Cook, CEO d'Apple. Les grands noms du web doivent réagir.

Les fausses news et rumeurs en tout genre continuent de faire des vagues sur la Toile. Nous trouvons d'un côté des sociétés qui profitent de la manne de clics apportée par de tels messages, forts générateurs de buzz. Et de l'autre les soucis que cela pose en termes de **capacité d'analyse des internautes**, où la croyance béante tend à remplacer de plus en plus souvent l'esprit critique.

Dans une interview accordée au *Daily Telegraph*, **Tim Cook**, patron d'Apple, s'inquiète de ce phénomène, qui gangrène selon lui l'esprit des internautes. *« Nous traversons une période où, malheureusement, certains de ceux qui gagnent sont les acteurs qui passent leur temps à essayer d'obtenir le plus de clics, en diffusant des fausses vérités,* analyse le patron d'Apple. *D'une certaine manière, **cela tue l'esprit des gens**. »*

Une timide réponse au problème

« Nous avons besoin de créer des outils qui aident à diminuer le volume de fausses actualités », propose Tim Cook.
Suite aux dérives sur les réseaux sociaux constatées lors des **élections américaines** de 2017, certains acteurs ont enfin décidé de réagir. C'est une première étape, mais qui reste encore timide. Pas question en effet de supprimer les fausses news, ces dernières étant juste écartées des moteurs de recherche des sites concernés.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).
Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

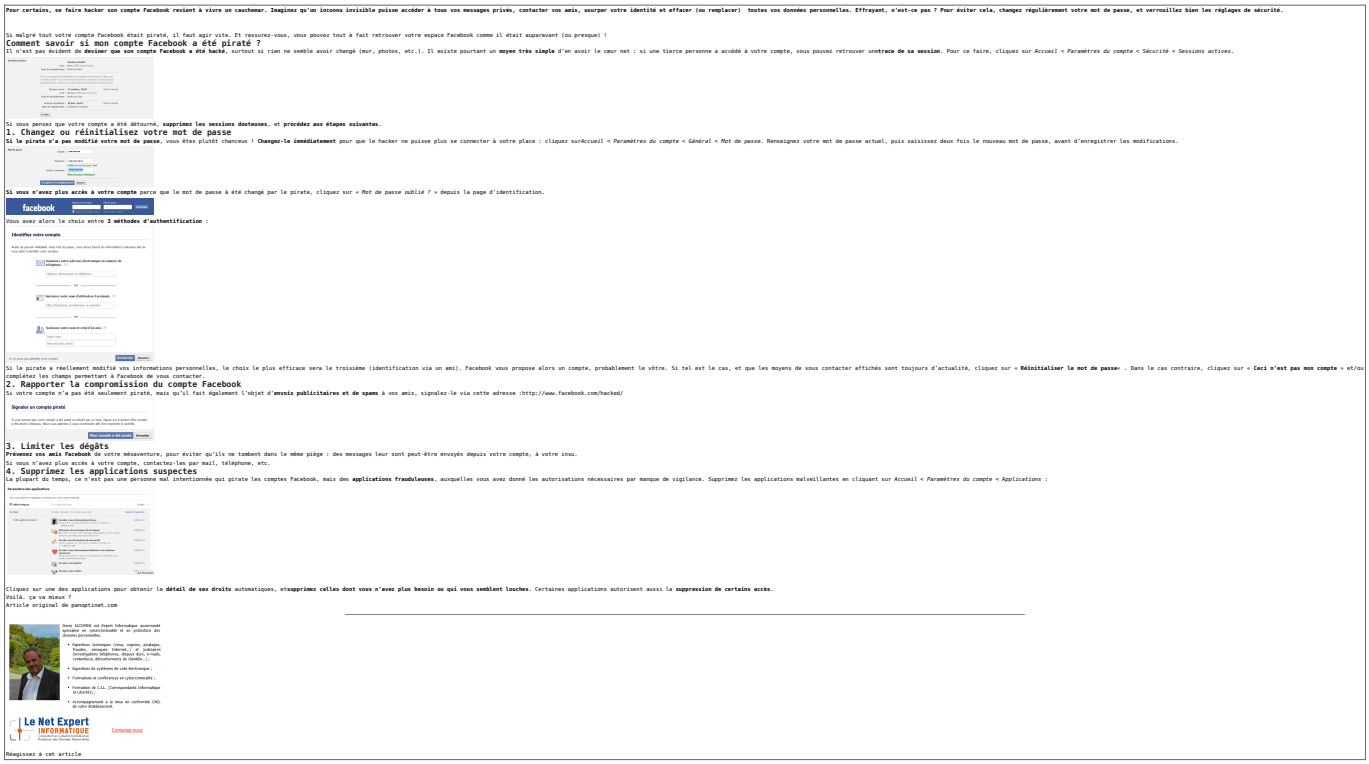
Réagissez à cet article

Original de l’article mis en page : Les fausses news inquiètent le patron d’Apple Tim Cook

---

Que faire quand son compte Facebook est piraté ?

	**Que faire quand son compte Facebook est piraté ?**



Pour certains, se faire hacker son compte Facebook revient à vivre un cauchemar. Imaginez qu'un inconnu invisible puisse accéder à tous vos messages privés, contacter vos amis, usurper votre identité et effacer (ou remplacer) toutes vos données personnelles. Effrayant, n'est-ce pas ? Pour éviter cela, changez régulièrement votre mot de passe, et verrouillez bien les réglages de sécurité.

Si malgré tout votre compte Facebook était piraté, il faut agir vite. Et rassurez-vous, vous pouvez tout à fait retrouver votre espace Facebook comme il était auparavant (ou presque) !

Comment savoir si mon compte Facebook a été piraté ?

Il n'est pas évident de **deviner que son compte Facebook a été hacké**, surtout si rien ne semble avoir changé (mur, photos, etc.). Il existe pourtant un **moyen très simple** d'en avoir le cœur net : si une tierce personne a accédé à votre compte, vous pouvez retrouver une**trace de sa session**. Pour ce faire, cliquez sur *Accueil < Paramètres du compte < Sécurité < Sessions actives*.

Si vous pensez que votre compte a été détourné, **supprimez les sessions douteuses**, et **procédez aux étapes suivantes**.

1. Changez ou réinitialisez votre mot de passe

Si le pirate n'a pas modifié votre mot de passe, vous êtes plutôt chanceux ! **Changez-le immédiatement** pour que le hacker ne puisse plus se connecter à votre place : cliquez sur*Accueil < Paramètres du compte < Général < Mot de passe*. Renseignez votre mot de passe actuel, puis saisissez deux fois le nouveau mot de passe, avant d'enregistrer les modifications.

Si vous n'avez plus accès à votre compte parce que le mot de passe à été changé par le pirate, cliquez sur *< Mot de passe oublié ? >* depuis la page d'identification.

Vous avez alors le choix entre **3 méthodes d'authentification** :

Si le pirate a réellement modifié vos informations personnelles, le choix le plus efficace sera le troisième (identification via un ami). Facebook vous propose alors un compte, probablement le vôtre. Si tel est le cas, et que les moyens de vous contacter affichés sont toujours d'actualité, cliquez sur « **Réinitialiser le mot de passe**» . Dans le cas contraire, cliquez sur « **Ceci n'est pas mon compte** » et/ou compléter les champs permettant à Facebook de vous contacter.

2. Rapporter la compromission du compte Facebook

Si votre compte n'a pas été seulement piraté, mais qu'il fait également l'objet d'**envois publicitaires et de spams** à vos amis, signalez-le via cette adresse :http://www.facebook.com/hacked/

3. Limiter les dégâts

Prévenez vos amis Facebook de votre mésaventure, pour éviter qu'ils ne tombent dans le même piège : des messages leur sont peut-être envoyés depuis votre compte, à votre insu.

Si vous n'avez plus accès à votre compte, contactez-les par mail, téléphone, etc.

4. Supprimez les applications suspectes

La plupart du temps, ce n'est pas une personne mal intentionnée qui pirate les comptes Facebook, mais des **applications frauduleuses**, auxquelles vous avez donné les autorisations nécessaires par manque de vigilance. Supprimez les applications malveillantes en cliquant sur *Accueil < Paramètres du compte < Applications* :

Cliquez sur une des applications pour obtenir le **détail de ses droits** automatiques, et**supprimez celles dont vous n'avez plus besoin ou qui vous semblent louches**. Certaines applications autorisent aussi la **suppression de certains accès**.

Voilà, ça va mieux ?

Article original de panoptinet.com

Réagissez à cet article

Original de l'article mis en page : Que faire quand son compte Facebook est piraté ? | Panoptinet

---

Conséquences innatendues des cyberattaques

Conséquences innatendues des cyberattaques

Les dégâts informatiques de premier jour ne constituent pas la seule conséquence d'une cyberattaque pour une entreprise. Il y a aussi la réduction en nombre des clients, déçus notamment du vol ou de la perte de leurs données. Certains peuvent même penser à poursuivre l'entreprise en justice. L'après est ainsi encore plus dure à gérer pour les dirigeants et les responsables informatiques.

Impact sur la confiance des consommateurs

La préparation d'une cyberattaque peut prendre plusieurs semaines, voire des mois. Par conséquent, leurs effets vont bien au-delà des « simples » dégâts informatiques. Une étude internationale réalisée par VansonBourne et publiée le 12 mai dernier le confirme, en insistant sur des atteintes sur la performance commerciale de la société victime. Elle révèle en effet que la confiance des consommateurs vis-à-vis de cette dernière s'amenuise après les attaques. Logique quand on sait que bon nombre de clients de TV5 Monde et Orange ont encore du mal à oublier les attaques respectives d'avril 2015 et de 2014 ayant entraîné une fuite de données. Cette étude avance même que 34% des Français voient leur loyauté envers une marque ayant laissé fuiter leurs données, diminuée. Les efforts de cybersécurité devront ainsi se trouver dans le plan de toute entreprise qui se veut être compétitive.
Les consommateurs sont également nombreux à perdre le désir d'acheter auprès d'une entreprise victime d'une attaque informatique. Plus de trois sur quatre ont même affirmé qu'ils iraient jusqu'à arrêter l'achat de produits ou services chez cette dernière, notamment si la vulnérabilité exploitée provient de l'erreur de l'équipe dirigeante. Pour une erreur humaine d'un subordonné, les clients sont plus compréhensifs. La publication de cette étude confirme par ailleurs que la sécurité des données figure depuis quelques années parmi les critères les plus considérés par les Français avant une décision d'acheter. Ce paramètre a été pris en compte par 61% des Français en 2015, contre 53% en 2014.

Risques de poursuite en justice

La perte de chiffre d'affaires est donc quasiment incontournable pour toute entreprise qui vient de faire l'objet d'une attaque informatique d'ampleur. Elle est toutefois moins grave par rapport à un autre risque, celui de la poursuite en justice. Cette étude a en effet permis de connaître que 50% des Français sont prêts à poursuivre en justice les entreprises attaquées pour négligence ou inattention apportée à la protection de leurs données personnelles. Target et Sony Picture en ont déjà payé le prix, trouvant même, parmi les auteurs de ces poursuites, leurs propres salariés. Face à ce risque, certaines entreprises envisagent de garder secrètes toutes les attaques atteignant leur système d'information. Serait-ce une bonne initiative de leur part ? La réponse est non. A l'heure d'Internet, la moindre information peut se trouver à la portée de tout le monde. Une éventuelle fuite pourrait ainsi écorner définitivement l'image d'une société choisissant une telle démarche. Au contraire, cette société devrait plutôt informer le plus rapidement ses clients, pour faire preuve de transparence. Cette démarche sera par ailleurs rendue obligatoire par le règlement européen sur la protection des données, un texte dont la mise en vigueur est prévue en mai 2018.

Article original de sekurigi.com complété par Denis JACOPINI

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les traces laissées par les cyberattaques – @Sekurigi

Les données de 112 000 policiers français exposées sur Internet

Les données de 112 000 policiers français exposées sur Internet

Par vengeance vis-à-vis de sa direction, un salarié de la mutuelle de la Police place le fichier des adhérents sur le Cloud de Google. Mettant en péril les données personnelles de 112 000 policiers.

Deux semaines après le meurtre de deux policiers à Magnanville, l'affaire fait évidemment désordre : selon RTL, les données personnelles de 112 000 policiers, ainsi que celles de leurs proches, se sont retrouvées exposées sur le Net. Nos confrères expliquent que la fuite émane d'un salarié de la Mutuelle Générale de la Police qui, par vengeance, aurait copié le fichier des adhérents pour le verser sur le Cloud de Google, où il n'était protégé que par un simple mot de passe. RTL explique qu'une plainte a été déposé la semaine dernière et qu'une enquête a été ouverte à Toulouse sur ces faits.

Un piratage découvert 3 semaines après

Le piratage du fichier des adhérents, qui renferme les adresses et numéros de téléphone des policiers actifs ou retraités, aurait été perpétré par un responsable d'agence de la mutuelle, installé à Limoges, le 2 juin dernier. Mais n'a été découvert par la direction de la mutuelle que 3 semaines plus tard, ce qui soulève quelques questions sur la politique de sécurité de la mutuelle quant aux accès à ce fichier central. Le directeur d'agence suspecté a été mis à pied. Pour expliquer cette indélicatesse, nos confrères parlent d'un conflit opposant le salarié à sa direction concernant des primes.
Google France a été averti de ce détournement du fichier des adhérents de la Mutuelle Générale de la Police et serait en train de nettoyer ses serveurs.
Article original de Reynald Fléchaux

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les données de 112 000 policiers français exposées sur Internet

---

Cybercriminalité : « Il faut qu'on voie que la Côte d'Ivoire réagit » | CIO MAG

Cybercriminalité : « Il faut qu'on voie que la Côte d'Ivoire réagit »

« L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici », assure Denis Jacopini, expert informatique assermenté spécialiste en cybercriminalité et protection des données personnelles. Membre de la Compagnie nationale française des experts de Justice en Informatique et techniques associées (CNEJITA), il a participé du 7 au 8 juin 2016 à Abidjan, à la 8ème édition de l'IT Forum Côte d'Ivoire sur la « Transformation numérique face à la protection des utilisateurs ». Loin des clichés et des idées reçues, le professionnel du crime en ligne a confié à CIO Mag l'image que la Côte d'Ivoire donne de l'extérieur et fait des propositions allant dans le sens de l'amélioration de la lutte contre la cybercriminalité. Sensibilisation des décideurs, opérations coup de poing, médiatisation des arrestations… la Côte d'Ivoire est, selon lui, en bonne voie pour renforcer la confiance dans son environnement numérique.

7 juin 2016. Denis Jacopini à la 8ème édition de l'IT Forum Côte d'Ivoire qui s'est déroulée du 7 au 8 juin dernier à la Maison de l'Entreprise, à Abidjan, sur le thème : « Transformation numérique face à la protection des utilisateurs ».

CIO Mag : Quelle image la Côte d'Ivoire donne-t-elle de l'extérieur dans le domaine de la cybercriminalité ?
Denis Jacopini : Depuis quelques années, la Côte d'Ivoire est connue en Europe comme le pays d'Afrique où se passent la très grande majorité des arnaques sur internet, à un point où lorsque quelqu'un reçoit un email qui vient de Côte d'Ivoire, il pense automatiquement à une arnaque, au mieux se méfie, au pire supprime le message sans même lui accorder la moindre attention. Ainsi, associer la Côte d'Ivoire à des arnaqueurs, n'est pas bon pour l'image du pays. Ceci dit, ma présence ici m'a réconforté.
En lisant la presse spécialisée, dont CIO Mag, je savais déjà que la Côte d'Ivoire réagissait face à ce phénomène, qu'elle mettait en place des méthodes et qu'elle engageait des actions pour permettre à la fois aux directeurs de systèmes d'information – DSI – et aux utilisateurs d'augmenter en compétence et de se soucier de ce problème de sécurité. Et, en venant ici, ça m'a réconforté. Je m'en suis surtout rendu compte au travers du discours du ministre de l'Economie numérique et de la Poste (à l'ouverture de la 8ème édition de l'IT Forum Côte d'Ivoire, NDLR). Il a fait une présentation de la manière dont il voit l'évolution de la Côte d'Ivoire dans le domaine du numérique. Son discours a été rassurant en indiquant que le pays avait à la fois une démarche active dans la cybersécurité et accordait une attention particulière aux moyens permettant d'associer confiance et développement numérique.
On a facilement pu remarquer que le ministre maîtrise le sujet et qu'il sait de quoi il parle. Il est prêt à emmener avec lui le pays dans cette transformation numérique. Quasiment toutes les entreprises vont devoir assurer cette métamorphose. Le pays doit pouvoir les accompagner dans cette transformation numérique. L'enjeu qu'a la Côte d'Ivoire aujourd'hui, c'est justement de dire de manière internationale tout ce qu'elle est en train de mettre en œuvre ici.

C.M : Selon vous quels sont les actions sur lesquelles la Côte d'Ivoire doit miser pour véritablement restaurer son image et créer un environnement numérique de confiance ?
D.J : A mon avis, ça devrait passer par une médiatisation des arrestations. Il y a des milliers de délinquants ayant organisé et mené des arnaques en tous genres à partir de cybercafés. On apprend de temps en temps sur la presse francophone spécialisée que se sont produites des arrestations mais ça reste sur les journaux peux lus. Il faut vraiment s'intéresser à la Côte d'Ivoire et consulter la presse locale pour le savoir. A mon avis, les actions qui sont faites dans le pays mais aussi tous les accords et toutes les coopérations qui sont établis avec les autres pays doivent internationalement être connues et notamment par le grand public qui a besoin d'être rassuré car régulièrement victime d'actes originaires d'ici.
Lorsqu'il y a une coopération qui est mise en place avec l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information, NDLR) en France, avec l'OCLCTIC, l'Office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication, en termes de formation et de sensibilisation en Côte d'Ivoire, il faut que cela se sache. Il faut qu'on voie que la Côte d'Ivoire réagit que les autorités se forment, sont en train de monter en compétence. Maintenant, ce qui manque, ce sont les preuves. Mais les preuves, ce sont effectivement les statistiques pouvant faire mention de l'évolution du nombre d'arrestations que j'espère suivies d'une chute considérable des arnaques qui pourraient venir rassurer les pays victimes. Il y aura toujours des arnaques, mais celles venant de Côte d'Ivoire doivent être combattues sans cesse pour finir par les rendre anecdotiques.

C.M : Hormis les arrestations, une forte sensibilisation de la jeunesse ivoirienne ne peut-elle pas également contribuer à réduire le nombre d'arnaques venant de la Côte d'Ivoire ?
D.J : D'après ce que j'ai compris, les adolescents ou les jeunes qui sont concernés sont des personnes qui, dans la société, sont déjà en marge des règles. Ils essaient de se débrouiller par leurs propres moyens sans passer par la case Travail, la case Honnêteté. C'est tout aussi grave que de se rapprocher de la drogue. Que fait le pays contre la drogue ? Ce qu'elle fait contre ce fléau, elle doit aussi le faire pour combattre la cybercriminalité. Comme dans d'autres régions du monde, s'attaquer à ce phénomène doit se faire en s'appuyant sur des entraides internationales.
« CE QUI MANQUE MAINTENANT CE SONT LES MOYENS POUR LES POUVOIRS PUBLICS DE MENER DES OPÉRATIONS COUP DE POING. GRÂCE À CELA, IL EST PROBABLE QUE LES JEUNES POUVANT ENCORE CHANGER DE VOIE, LE FERONT PAR PEUR.»
L'analyse des flux financiers au travers de réseaux et des trains de vie incohérents avec les revenus connus sont de bonnes pistes à suivre pour comprendre le phénomène de la cybercriminalité. Ce qui manque maintenant ce sont les moyens pour les pouvoirs publics de mener des opérations coup de poing. Grâce à cela, il est probable que les jeunes pouvant encore changer de voie, le feront par peur. Ensuite, pour ceux qui, influencés, n'auront pas envie de rentrer dans le droit chemin, je pense en effet qu'une une forte sensibilisation pourra évidemment contribuer à réduire le nombre d'arnaques venant de Côte d'Ivoire.

C.M : Parlant de moyens, n'est-il pas opportun de renforcer la coopération avec la France et des pays comme le Canada pour muscler les opérations terrain, ce d'autant plus que les populations de ces pays sont bien souvent ciblées par les arnaques venant de Côte d'Ivoire ?
D.J : Jusqu'à maintenant, la coopération n'y était pas. Elle était surtout en Europe. En dehors de l'Europe, c'était très difficile d'établir une coopération. Moi, il y a une question que je me pose : pourquoi d'ici ils vont essayer d'arnaquer la France ou le Canada ? Déjà parce qu'il n'y a pas de barrière au niveau de la langue. Puis, ce sont des pays qui ont des moyens. Qui sont prêts à payer pour rencontrer l'amour. On ne va pas essayer d'arnaquer un pays pauvre. Donc, on s'oriente vers ces pays-là.
Depuis maintenant quelques années, au-delà de l'évolution de la législation, la coopération internationale entre pays intérieurs et extérieurs de l'Europe s'est accentuée. Sans que ces pays n'aient forcément ratifié la Convention de Budapest, seul contrat officiel existant et contenant des protocoles d'entraides entre les autorités compétentes des différents pays impliqués, une entraide entre les organes judiciaires s'est naturellement créée. Aujourd'hui, l'entraide internationale est légion. C'est une forme de coopération qui n'a pas besoin de convention et qui, avec certains pays fonctionne très bien. En partie grâce à cela, la Côte d'Ivoire a commencé ces dernières années à s'attaquer au délinquants du numérique, réaliser des arrestations et amplifier ses actions…

C.M : Vous avez participé à l'IT Forum Côte d'Ivoire 2016 sur la sécurité des utilisateurs des services numériques. Partant de tout ce qui a été dit, comment entrevoyez-vous l'avenir de la Côte d'Ivoire dans 5 à 10 ans ?
D.J : La Côte d'Ivoire est en bonne voie pour sortir la tête de la cybercriminalité. Elle est en bonne voie parce que le combat commence obligatoirement par la sensibilisation des décideurs. Et ce forum a réuni des DSI, des directeurs de la sécurité numérique, des chefs d'entreprises, des officiels, donc des personnes qui décident de l'économie du pays. Si, nous formateurs, consultants, professionnels de la cybersécurité, on a bien fait notre travail pendant ces deux jours, il est clair que les visiteurs sont repartis d'ici avec de nouvelles armes. Maintenant, ceux qui auront été convaincus aujourd'hui ne seront pas forcément ceux qui seront les cibles de demain, des prochaines failles ou des prochaines attaques. Les prochaines victimes continueront à être les utilisateurs imprudents, ignorants et des proies potentielles qui n'ont pas pu être présentes à l'IT Forum. À force de sensibiliser les chefs d'entreprises, les DSI, et de faire en sorte que la sensibilisation à la cybersécurité et aux comportements prudents commence dès l'école, nous auront bientôt une nouvelle génération d'utilisateurs mieux formés et mieux armés.
Un autre phénomène qui tend à être inversé est celui de la faible importance accordée à la sécurité informatique. Quel que soit l'endroit dans le monde, la cybercriminalité est quelque chose d'inévitable et la sécurité informatique, en raison d'une course effrénée à la commercialisation à outrance, a trop longtemps été négligée par les constructeurs et les éditeurs de logiciels. Ils devront sans doute se conformer au concept « Security by design ».
Avant de miser sur sa R&D (Recherche et Développement) pour créer ou répondre à des besoins et commercialiser à tout prix pour rapidement la rentabiliser et ne chercher que les profits financiers, il deviendra bientôt obligatoire de penser sécurité avant de penser rentabilité. Avec l'évolution incoercible du numérique dans notre quotidien (objets connecté, santé connectée, vie connectée), il est indispensable que la sécurité des utilisateurs soit aussi le problème des inventeurs de nos vies numériques et pas seulement de ceux dont le métier est de réparer les bêtises des autres. La Côte d'Ivoire fait désormais partie des pays impliqués par ce combat et je n'ai aucun doute, ce pays se dirige droit vers une explosion de l'usage du numérique et une amélioration de sa lutte contre la cybercriminalité.

C.M : Au niveau international, quelle est la nouvelle tendance en matière de cybercriminalité?
D.J : Au Forum international de la cybercriminalité (FIC 2016), j'ai assisté à une présentation faite par un chercher en cybersécurité autour de l'étude de l'évolution d'un RAT (Remote Access Tool). Des virus utilisant des failles existent déjà mais la présentation portait sur une nouvelle forme de logiciel malveillant encore plus perfectionné en matière d'impacts et de conséquences sur les postes informatiques des victimes. On connaissait des failles en Flash, en Visual Basic et dans d'autres types de langages mais la faille en Java est une faille qui aujourd'hui peut toucher tous les ordinateurs puisqu'énormément de systèmes et de web services sont conçus autour du langage Java.
J'ai trouvé la présentation très intéressante et j'ai trouvé l'effet dévastateur pour tous ceux qui attraperont ce « Méchangiciel ». A la fin de la présentation, j'ai approché l'intervenant et lui ai demandé quel était le moyen de propagation utilisé par ce virus ingénieux du futur ? Il m'a répondu qu'il se propage tout simplement par pièce jointe dans un e-mail. Ça reste aujourd'hui le principal vecteur de propagation de systèmes malveillants. Surtout, si c'est bien monté avec ce qu'on appelle des techniques d'ingénierie sociale, c'est-à-dire des actes qui permettent de manipuler la personne destinataire du piège, par exemple un CV piégé transmis à une agence d'emploi, rien de plus normal, même s'il est piégé ! C'est pourquoi l'autre vecteur sur lequel j'insiste, c'est le vecteur humain, la sensibilisation des utilisateurs afin d'augmenter le taux de prudence qu'ils doivent avoir lorsqu'ils reçoivent un email. Un email piégé a des caractéristiques que l'on peut assez facilement identifier et qui permettent de dire qu'il y a un risque, et mettre une procédure en cas de doute. Pour moi, même s'il existe des lunettes 3D, des hologrammes, des choses complétement folles au niveau technologique, j'ai l'impression que la propagation de la cybercriminalité va pouvoir se faire encore pendant pas mal de temps dans de vulgaires pièces jointes, et probablement encore dans les arnaques et le phishing.
Une fois que le pirate aura obtenu les clefs il pourra mener son attaque par « Menace Persistante Avancée (Advanced Persistent Threat) », autre grande tendance déjà depuis quelques années et encore pour longtemps !
Article original et propos recueillis par Anselme AKEKO

Réagissez à cet article

Original de l’article mis en page : Cybercriminalité : « Il faut qu’on voie que la Côte d’Ivoire réagit » | CIO MAG

Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook

Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook

---

Atlantico : Poster une photo de son enfant sur Facebook peut-il lui porter préjudice ? Si oui, quand ? Et pourquoi ?

Publier une photo de ses enfants sur Facebook – qui est de loin le leader des réseaux sociaux dans le monde – est un acte compréhensible mais qui fait surtout plaisir sur le moment aux parents. Les parents façonnent l'identité numérique de leurs enfants à l'insu de leur plein gré alors même que le droit à l'oubli n'existe pas sur Internet. Plus tard, certaines traces numériques (photos ou vidéos postées avec les commentaires et tags associés) peuvent être utilisées contre eux surtout si les paramétrages de confidentialités sont mal utilisés.

Et même en postant une photo accessible aux seuls amis, celle-ci peut ensuite être partagée plus largement. En outre les personnes qui vont réagir à la photo permettent de révéler l'écosystème relationnel de la personne. Il est facile d'établir des corrélations entre les personnes. Et en fonction du profil des personnes réagissant de déterminer quel est le profil potentiel de l'enfant sur la photo. Pour les préjudices, on pense avant tout à l'attitude d'un recruteur mais ce peut être aussi des amis potentiels de l'enfant qui le jugeront avec un autre regard. Déjà on google une personne avant de la rencontrer ce qui induit un prisme dans la première rencontre. Le préjudice peut intervenir à des périodes charnières de la vie : adolescence où l'individu se construit et est sensible au regard des autres, entrée dans la vie active, rencontre amoureuse, etc.

Comment fonctionne le système de tag ? Quelle est sa fonction ? Pourquoi l'utilise-t-on ?

Il s'agit d'un système mis en place par Facebook qui permet à un utilisateur de Facebook d'indiquer qu'une personne figure sur une photo. En quelque sorte, un traitement manuel du facebooknaute lui-même vient en complément de l'algorithme mis en place par Facebook pour collecter des données personnelles (en l'occurrence les photos des visages des personnes) de nature à faire grandir la base d'information relative à une personne. Facebook peut avec l'expérience lui-même déterminer les personnes reconnues sur les photos, ce qui est parfois bluffant. Facebook peut ensuite, en fonction des références à d'autres posts, déterminer le cercle probable de personnes autour de celle qui a été taguée. Ceci lui permet de faire des suggestions (par exemple amis que l'on pourrait connaître, voire produits ou services que l'on est susceptible d'aimer car les goûts de ses amis sont souvent plus proches des siens que ceux d'inconnus) avec des taux de retour plus pertinents.

L'objectif de Facebook est d'exploiter le *big data* constitué par les photos et leurs tags pour sans cesse améliorer les résultats pour les marques partenaires et qui paient ses services. Par ailleurs, les algorithmes qui permettent de reconnaître les visages et les techniques de bio-identification ne sont qu'à leur début. Demain, à partir d'une simple photo, il sera, avec des outils idoines, possible de dresser le portrait robot d'une personne en allant fouiller sur l'ensemble de la webosphère (pas seulement sur Facebook mais sur l'ensemble des réseaux sociaux et des sites) pour collecter les numéros de téléphone, les adresses mails et d'autres détails personnels associés. Ceci peut présenter des opportunités réelles pour mieux connaître rapidement une personne, mais présente des risques. Des garde-fous et une éthique sont à construire pour éviter que le numérique ne soit un facteur d'exclusion ou un moyen d'ostraciser les internautes. Alors que les États-Unis sont dans le mécanisme d'*opt-out* (utilisation *a priori* des données personnelles sans autorisation préalable), l'Europe préfère l'*opt-in* qui constitue un principe de précaution quant à l'exploitation des données personnelles. Mais force est de constater que les outils majoritairement utilisés en Europe sont Américains et que nous sommes GAFA-dépendant *(Ndlr : GAFA = Google, Apple, Facebook, Amazon)* et qu'en contrepartie de la gratuité d'utilisation d'un service, nous fournissons et souvent avec beaucoup de zèle des données personnelles que ces outils utilisent à la fois avec un traitement automatique et un traitement humain qui le perfectionne comme celui des tags.

Article original de David Fayon Lire la suite…

Réagissez à cet article

Original de l’article mis en page : Pourquoi vous ne devriez jamais publier de photos de vos jeunes enfants sur Facebook | Atlantico.fr

---

Les géants du web s’accordent pour bloquer les contenus illégaux

Les géants du web ensemble pour bloquer les contenus illégaux

---

Alors que les propos haineux sont malheureusement légion sur les réseaux sociaux, plusieurs géants du web ont trouvé un accord avec la Commission Européenne pour respecter un code de conduite. Toutefois, cette solution ne semble pas à ce jour convenir à plusieurs associations de défense des droits.

Les contenus illégaux bientôt bannis d'Internet ?

Depuis de longs mois maintenant, la Commission Européenne s'était fixée comme objectif d'éradiquer une majorité des propos haineux circulant sur la Toile.

Dans ce cadre, elle est parvenue à un accord avec YouTube, Microsoft, Twitter et Facebook pour l'établissement et le respect d'un code de conduite. Ainsi, les différents acteurs se sont engagés à bloquer les contenus gênants dans les 24 heures suivant leur signalement officiel.

En acceptant ce code de conduite pour bloquer les contenus illégaux, les acteurs du web montrent qu'ils ont bien conscience que leurs outils sont utilisés pour diffuser la violence et la haine mais aussi pour recruter des individus susceptibles de rejoindre leurs groupes.

Point positif, ce code de conduite ne vient pas entraver la liberté d'expression sur la Toile, celle-ci étant très importante en particulier pour les géants du web qui l'ont toujours prônée.

Un code de conduite pas suffisant selon les associations de défense des droits

Si la Commission Européenne s'est d'ores et déjà réjouie de l'accord trouvé avec les grandes entreprises du web, celui-ci ne fait assurément pas que des heureux.

En effet, Access Now et European Digital Rights (EDRi), deux associations de défense des droits, ont vivement critiqué cet accord estimant qu'il se contente de rappeler des règles déjà existantes à savoir celles qui consistent à supprimer des contenus illégaux.

Selon ces associations, il aurait donc fallu que le texte aille beaucoup plus loin et qu'il prévoit des poursuites contre ceux qui profèrent des propos haineux sur la Toile. En effet, Joe McNamee, Directeur Exécutif de l'EDRi, juge qu'« il est ironique que la Commission menace les Etats membres de les traduire en justice pour ne pas respecter les lois contre le racisme et la xénophobie alors qu'ils persuadent des entreprises comme Google et Facebook de glisser les infractions sous le tapis ».

Tout est dit…

Article original

Réagissez à cet article

Original de l'article mis en page : Les géants du web ensemble

pour bloquer les contenus illégaux

Vers une nouvelle plainte européenne contre Google

	Vers une nouvelle plainte européenne contre Google

---

Google n'en a pas encore fini avec sa série de déboires judiciaires. Alors que le géant américain fait l'objet d'investigations à propos de son moteur de recherche et de sa plate-forme Androïd pour abus de position dominante, on apprend que le groupe américain pourrait être visé par une nouvelle enquête toujours de la part de la Commission européenne. Cette fois, cela concerne le cœur de l'entreprise, à savoir les services publicitaires.

Le site generation-nt.com qui reprend Bloomberg indique que la nouvelle procédure serait indépendante de deux précédentes et suivre son propre cours. Elle découle d'une procédure lancée depuis 2010 et qui concernerait des contrats avec des clients de Google dont le but était d'écarter l'utilisation de services concurrents.

Seulement, l'action annoncée pourrait être très coûteuse pour le géant américain parce qu'elle touche un domaine qui représente la majeure partie des solides revenus de Google, soit plus de soixante-quatorze milliards de dollars, seulement pour l'année 2015. Une perspective à laquelle il serait très difficile d'échapper puisque generation-nt.com nous apprend que Google a déjà épuisé ses possibilités de négociations avec la Commission européenne…. [Lire la suite]

Réagissez à cet article

Source : *Vers une nouvelle plainte européenne contre Google | CIO-MAG*