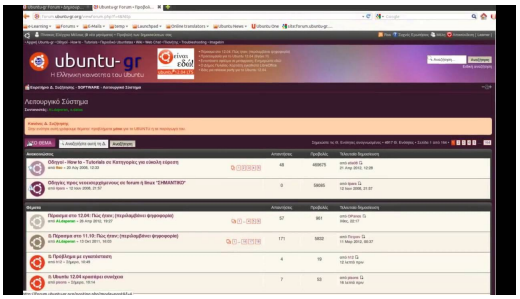
Deux millions de données d’utilisateurs Ubuntu dérobées



Deux millions de données d’utilisateurs Ubuntu dérobées

Le forum de la distribution Ubuntu a été victime d'une grave attaque informatique. Deux millions d'utilisateurs se sont fait voler leurs données.

Le butin du pirate est plus qu'impressionnant. Noms, mots de passe, adresse mails et IP, les données de deux millions d'utilisateurs du forum d'Ubuntu se sont envolées. La nouvelle a été annoncée jeudi dans un communiqué par Canonical l'éditeur d'Ubuntu. *« A 20h33 UTC le 14 Juillet 2016, Canonical et l'équipe ont été informés par un membre du Conseil Ubuntu que quelqu'un prétendait avoir une copie de la base de données des forums. Après enquête initiale, nous avons été en mesure de confirmer qu'il y avait bien eu une exposition des données et nous avons fermé les forums par mesure de précaution. »*

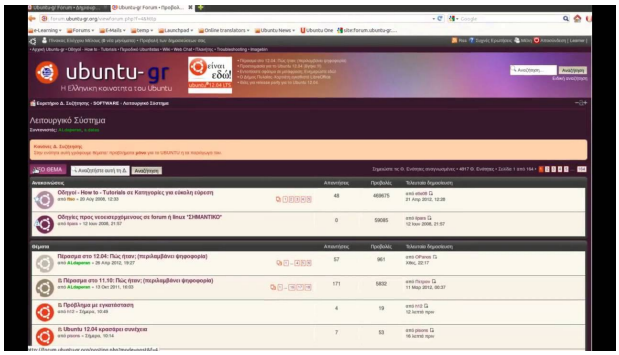
Une attaque par injection SQL

Une enquête plus poussée a révélé que la méthode employée est une injection SQL. Le pirate a pu injecter des requêtes SQL formatées dans la base de données des forums pour ensuite télécharger les datas.

Cependant, le communiqué précise que le hacker n'a pas pu accéder aux mots de passe utilisateur valides ni au référentiel de code Ubuntu ou au mécanisme de mise à jour. Moins certain, le rapport précise que normalement les services Canonical ou Ubuntu en sortent indemnes, comme certains forums.

Tout est plus ou moins rentré dans l'ordre

Des mesures correctives ont été prises et les forums restaurés. Les mots de passe du système et de la base de données ont été réinitialisés et ModSecurity, une Web Application Firewall vient renforcer le dispositif de sécurité. Selon Canonical, ça va mieux, même si après ce genre de vol il est légitime de penser que le mal est fait.



Article original de Victor Miget

Réagissez à cet article

Original de l'article mis en page : Ubuntu : les données de

deux millions d’utilisateurs dérobées

Sanction de la CNIL pour BrandAlley.fr

	Sanction de la CNIL pour BrandAlley.fr

---

La CNIL vient d'infliger une sanction administrative de 30 000 euros à l'encontre de BrandAlley.fr. La société éponyme, derrière ce site de ventes en ligne, est épinglée pour plusieurs indélicatesses à l'égard de la loi de 1978.

Le 13 janvier 2015, une délégation de la CNIL effectuait un premier contrôle sur place pour relever déjà différents manquements de cette société française. Cela aurait pu en rester là si tout avait été rectifié à temps, mais en mars de la même année, une cliente a saisi la CNIL pour se plaindre de difficultés dans l'exercice de son droit d'accès aux données personnelles. Cette internaute adressait d'ailleurs au site de e-commerce une nouvelle lettre en mai 2015, sans plus d'effet.
Le 3 juillet 2015, BrandAlley était du coup mise en demeure par la CNIL de corriger plusieurs points de son système dans les trois mois. Bon prince, la Commission lui accordait un peu plus tard une rallonge de trois nouveaux mois. Les points litigieux visent à :
• Encadrer le traitement relatif à la prévention des fraudes,
• Mettre en place d'une durée de conservation des données clients,
• Recueillir le consentement préalable des clients pour la conservation des données bancaires,
• Prendre en compte de la demande de la plaignante,
• Obtenir l'accord des internautes s'agissant des cookies,
• Cesser de transmettre les données à caractère personnel vers des pays hors UE qui n'assurent pas un niveau suffisant de protection de la vie privée et des libertés et droits fondamentaux.

Dans un courrier de janvier 2016, BrandAllay affirmait à la CNIL qu'elle s'était désormais mise en conformité. Peu satisfaite des réponses « lacunaires », la Commission organisait un nouveau contrôle sur place en février 2016. Contrôle qui a montré la persistance de plusieurs problèmes déjà relevés. En outre, un mois plus tard, elle a effectué un contrôle à distance du site Internet, une possibilité accordée par la loi sur la consommation.
La procédure gagnait alors un tour de vis supplémentaire. La CNIL a désigné un rapporteur, en l'occurrence François Pellegrini, une étape préalable à toute sanction où la société peut encore donner ses explications. Dans ce document désormais public , le rapporteur a constaté plusieurs défauts.

Des réactions trop tardives

Premièrement, BrandAllay.fr n'avait pas déposé dans le délai imparti, de demande d'autorisation pour la mise en œuvre d'un traitement antifraude. Selon les éléments du dossier, c'est « la réception du rapport de sanction qui a conduit la société à effectuer une demande d'autorisation ». Mais beaucoup trop tardivement pour ne pas abuser de la patience de l'autorité administrative…
S'agissant de la durée de conservation des données personnelles, on se retrouve un peu dans même situation. À l'échéance du délai imparti, la société avait indiqué s'être conformé à la norme simplifie 48, celle relative à la gestion de clients et de prospects. Dans le même temps, elle ajoutait que les données clients seraient conservées 5 années durant, à compter de la fin de la relation commerciale. Or ce délai non prévu par la norme en question. Pire, lors du deuxième contrôle sur place, la CNIL a constaté qu' « aucune purge des données n'avait été réalisée ». Les explications fournies par le site de e-commerce – liées à la complexité de mise en œuvre – n'ont pas eu de poids, même si elle a depuis corrigé le tir pour revenir à un délai de conservation de 3 ans.

Cookies, chiffrement, Maroc et Tunisie

S'agissant des cookies, la société mise en demeure avait informé l'autorité de la mise en place un bandeau afin de recueillir le consentement des internautes, avant dépôt de cookies. Le contrôle en ligne effectué en mars 2016 a révélé la solidité de cette affirmation. D'un, le fameux bandeau « était rédigé de telle sorte qu'il n'informait pas les utilisateurs de leur possibilité de paramétrer le dépôt de cookies ». Soit un joli manquement à l'article 32-II de la loi de 1978.
De deux, des cookies à finalités publicitaires étaient déposés dès l'arrivée sur le site, sans l'ombre d'un consentement préalable. Pour ce dernier point, la CNIL n'a finalement pas retenu de grief, s'estimant « insuffisamment éclairée (…) sur la répartition exacte des responsabilités entre l'éditeur du site, les annonceurs et les régies publicitaires concernés ». Par constat d'huissier, BrandAlley a par ailleurs démontré s'être mise depuis d'aplomb.
Ce n'est pas tout. La CNIL a pareillement dénoncé l'absence de chiffrement du canal de communication et d'authentification lors de l'accès à BrandAlley.fr (usage du HTTP, plutôt que HTTPS). Le 29 mars 2016, la société a produit un nouveau constat d'huissier pour montrer à la CNIL que ce défaut se conjuguait désormais au passé. Un peu tard là encore pour la Commission qui a relevé un nouveau manquement.
Enfin, la société transférait vers le Maroc et la Tunisie les données personnelles de ses clients, via l'un de ses sous-traitants. Malgré des affirmations en sens contraire en janvier 2016, la CNIL a relevé en février la persistance de ces transferts. Or, en principe, de telles opérations ne sont possibles que si le pays de destination offre un niveau de protection comparable à celui en vigueur en Europe, ce qui n'était pas le cas ici (pas plus qu'aux Etats-Unis depuis l'invalidation du Safe Harbor par la justice européenne).
Après délibération, la CNIL a décidé de sanctionner la société de 30 000 euros d'amende, outre de rendre public la délibération. Une sanction loin d'être négligeable, le critère de la confiance sur Internet étant cruciale pour un site de e-commerce. La société peut maintenant attaquer, si elle le souhaite, la décision devant le Conseil d'État.

Article original de Marc Rees

Réagissez à cet article

Original de l’article mis en page : Données personnelles : BrandAlley.fr sanctionné par la CNIL

Discorde entre l’Union européenne et les Etats-Unis sur la protection des données personnelles

Discorde entre l’Union européenne et les Etats-Unis sur la protection des données personnelles

En cette période de pause estivale propice aux voyages, nombreux sont ceux qui ont réservé une chambre d'hôtel sur un site internet ou s'apprêtent à poster sur Facebook leurs photos souvenirs. Parmi ces personnes, combien s'interrogeront sur l'utilisation qui peut être faite des données quils auront ainsi (bien involontairement) transmises?

Cette question est au cœur de la problématique de la protection des données personnelles, qui intéresse l'Union européenne, notamment lorsque le transfert se fait d'un pays européen vers un pays tiers. Le principe veut que ce type de transfert de données à caractère personnel vers un pays tiers soit interdit, sauf si le pays en question assure un niveau de protection suffisant pour ces informations.

En juin 2013, les révélations d'Edward Snowden sur la récupération par l'agence de renseignements américaine, la NSA (National Security Agency), des données personnelles des citoyens européens, et donc leur surveillance par les autorités américaines, ont conduit l'UE à revoir les accords existants sur le sujet.

Alors que les négociations étaient en cours, une décision de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2015, a précipité le processus. La Cour avait à se prononcer sur une question posée par la Haute Cour de justice irlandaise relative à la validité des principes dits Safe Harbor (sphère de sécurité). Ceux-ci étaient énoncés dans la décision de la Commission européenne du 26 juillet 2000 dans laquelle elle considérait que les Etats-Unis assuraient un niveau suffisant de protection des données personnelles pour permettre le transfert des données.

Mais la Cour de justice de l'Union européenne a invalidé cette décision. Marquée par les révélations de l'affaire Snowden, elle a constaté que le régime américain de protection des données personnelles « rend possible des ingérences (…) dans les droits fondamentaux des personnes » par les autorités publiques américaines.

La négociation d'un nouvel accord devenait urgente pour les quelques 4.000 entreprises soumises au Safe Harbor devenu caduc et laissant donc place à un vide juridique. Or, le sujet de l'utilisation des données personnelles est particulièrement brûlant quand on connait la valeur de celles-ci pour les entreprises: l'exploitation des données personnelles de ses utilisateurs aurait rapporté 12 milliards de dollars à Facebook en 2014, selon Les Echos.

Le nouveau dispositif, baptisé Privacy Shield (bouclier de protection de la vie privée), a été négocié entre la Commission européenne et les Etats-Unis, qui sont parvenus à un accord le 2 février 2016. Le 13 avril, les autorités européennes de protection des données (la CNIL pour la France) ont émis un avis sur cet accord, où elles expriment de sérieuses préoccupations. Puis le Parlement européen a fait de même dans une résolution votée le 26 mai: les députés européens réclamait de rouvrir les négociations pour apporter plus de garanties. Le 8 juillet, les Etats membres, réunis au sein d'un groupe de travail, ont quant à eux validé le texte, malgré l'abstention de quatre pays, l'Autriche, la Hongrie, la Slovénie et la Bulgarie.

Finalement, le 12 juillet 2016, la Commission européenne adopte sa décision relative au bouclier de protection des données UE-Etats-Unis. La commissaire européenne chargée de la Justice, des Consommateurs et de l'Egalité des genres, Věra Jourová, a déclaré que le Privacy Shield est « un nouveau système solide destiné à protéger les données à caractère personnel des Européens et à procurer une sécurité juridique aux entreprises. Il prévoit des normes renforcées en matière de protection des données, assorties de contrôles plus rigoureux visant à en assurer le respect, ainsi que des garanties en ce qui concerne l'accès des pouvoirs publics aux données et des possibilités simplifiées de recours pour les particuliers en cas de plainte. Le nouveau cadre rétablira la confiance des consommateurs dans le contexte du transfert transatlantique de données les concernant ».

Ainsi, le nouveau système se veut plus protecteur que la précédente « sphère de sécurité »: la collecte des données par les sociétés américaines ne peut notamment pas être utilisée pour des usages non prévus initialement. Egalement, un médiateur aux Etats-Unis sera chargé de recevoir les plaintes des Européens. Tous les ans, la Commission examinera le respect du dispositif par les Etats-Unis.

Toutefois, le bouclier peine à convaincre. Les services de renseignements américains peuvent continuer à intercepter les données personnelles des Européens. Les associations fustigent un accord jugé largement insuffisant, qualifié de bouclier troué par la Quadrature du net. Du côté des députés européens, si la droite (les groupes PPE et CRE) est satisfaite, ce n'est pas le cas des Socialistes, des Verts et des Libéraux. Eux estiment que le nouveau système ne respecte pas les exigences posées par la CJUE: « la CJUE a dit que le problème, c'était les lois américaines. Or rien, dans les textes américains, n'a changé », pointe Jan Philipp Albrecht (Verts).

Le nouvel accord est par conséquent susceptible d'être à nouveau invalidé par les juges européens. Pour finir, il a été élaboré dans le cadre de la directive européenne de 1995 sur la protection des données. Or, cette directive va être remplacée en mai 2018 par un règlement adopté en 2015. L'insécurité juridique, ennemi des entreprises, plane donc toujours. Quant aux citoyens, ils ne peuvent que déplorer que la protection de leur vie personnelle soit mise en balance avec des enjeux économiques et de sécurité.

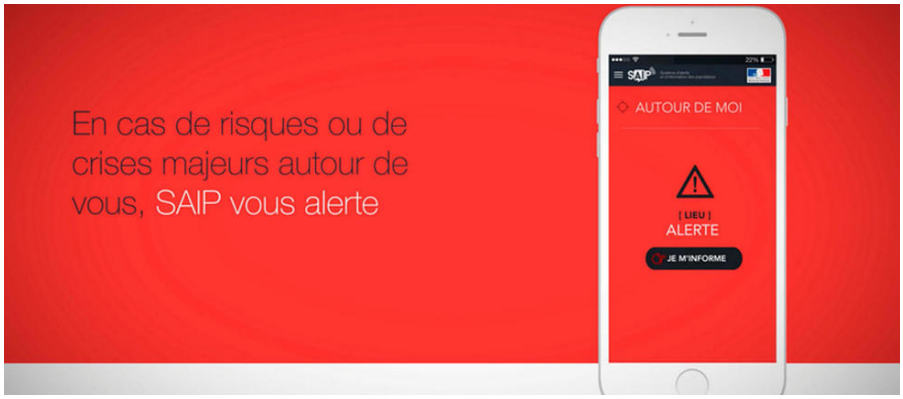
Avec la contribution de la Maison de l'Europe de Paris

Réagissez à cet article

Original de l’article mis en page : Protection des données personnelles: lautre pomme de discorde entre lUnion européenne et les Etats-Unis | www.francesoir.fr

---

Attentat à Nice : l’application « alerte attentat » sur la sellette



Attentat à Nice : l’application « alerte attentat » sur la sellette

---

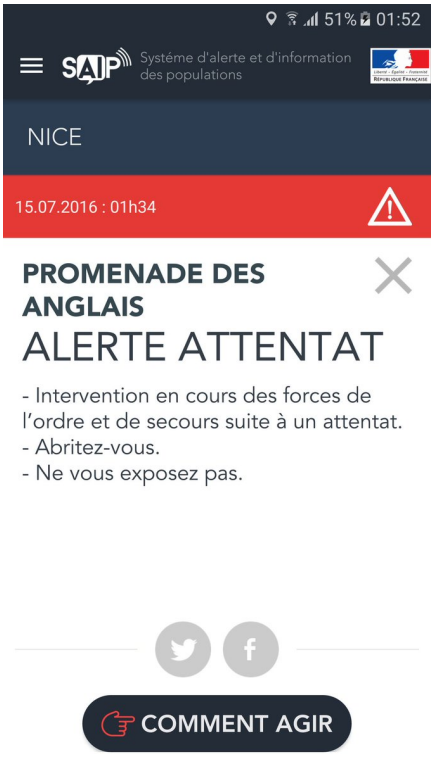
Le dispositif mis en œuvre par le ministre de l'Intérieur, censé prévenir les populations locales d'un attentat en cours, a failli. Les critiques pleuvent.

Chou blanc. L'application SAIP (Système d'alerte et d'information aux populations) « alerte attentat » avait été lancée par le ministre de l'Intérieur, Bernard Cazeneuve, avant l'Euro 2016 de football afin d'informer en temps réel les populations concernées de l'imminence d'une attaque. Hier, elle a tardé à fonctionner à Nice, au moment où le camion meurtrier faisait un carnage sur la promenade des Anglais. Ce dispositif aurait dû s'activer dans les quinze minutes qui ont suivi cet attentat, mais il n'en a rien été.

Les tweetos fustigent cet échec

Sur le réseau social Twitter, les internautes ont épinglé l'inefficacité et l'inutilité de ce système. Selon certains, l'alerte attentat, supposée prodiguer des conseils de survie en cas d'attaque, se serait déclenchée deux heures après le massacre de Nice, soit à un moment où la France entière était déjà informée du drame qu'elle venait de connaître.

Voir l'image sur Twitter



Suivre

Olivier Jaillet @OJaillet

Alerte #attentat sur #SAIP qui se déclenche 2 heures après le drame… Quel est l'utilité de l'application ?? #Nice

02:07 – 15 Juil 2016

•

•

1515 Retweets

•

22 j'aime

Voir l'image sur Twitter

Suivre

Jonathan Quique @jonathanquique

Première notification à 1h34, l'app #SAIP n'était pas prête …

07:16 – 15 Juil 2016

•

•

1 Retweet

•

11 j'aime

Il appartiendrait en fait au préfet du département concerné par un attentat de choisir de déclencher ou non l'alerte sur les smartphones des personnes ayant téléchargé l'application SAIP. On ignore encore si c'est le préfet des Alpes-Maritimes qui a décidé de ne pas faire fonctionner l'alerte, ou s'il s'agit d'un dysfonctionnement.

Article original de Emmanuel Ammar

Réagissez à cet article

Original de l’article mis en page : Attentat à Nice : l’application « alerte attentat » sur la sellette – Le Point

L’Arménie à son agence de protection des données à caractère personnel

L’Arménie à son agence de protection des données à caractère personnel

L’agence de protection des données à caractère personnel a fourni des conseils à plus de 300 organisations en 3 mois

L’Agence de protection des données personnelles, une structure affiliée au Ministère arménien de la justice a fourni des conseils à plus de 300 organismes au cours des trois derniers mois selon sa responsable Suse Doydoyan.
Elle a dit que 98% de ces organisations était des structures privées, “mais nous avons fourni des conseils également aux organisations du secteur public.“
Selon elle, l’agence a aussi fait beaucoup de travail au cours des 100 derniers jours pour étudier l’expérience internationale et a travaillé sur un certain nombre de concepts relatifs. Elle a souligné que l’agence n’est pas un organe répressif, bien que possédant des « leviers d’influence importants, y compris le pouvoir d’engager des procédures administratives.
“Nous pensons que notre fonction est préventive. Nous n’attendons pas que des violations se produisent afin d’infliger des amendes subséquentes, essayant d’abord d’empêcher ces violations“ a-t-elle dit.
L’Agence de protection des données personnelles agit au nom de la République d’Arménie.

Article original de Stéphane

Réagissez à cet article

Original de l’article mis en page : Nouvelles dArménie en Ligne

---

De nouvelles investigations sur l’IP Tracking en préparation

De nouvelles investigations sur l’IP Tracking en préparation

Les cybermarchands sont prévenus : la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) va mener « dans les prochains mois » de nouvelles investigations relatives à l'IP Tracking, cette technique de pistage dont aucun cas avéré n'avait été détecté lors d'une précédente enquête, remontant à 2013.

Certains sites de e-commerce modulent-ils leurs tarifs en fonction du nombre de visites de leurs utilisateurs ? C'est en tout cas ce que soutiennent de nombreuses personnes, au motif que le prix de certains articles augmenterait artificiellement en cas de consultations à répétition d'un même article. Le but : faire croire au consommateur que les biens restants (des billets d'avion ou des chambres d'hôtel par exemple) diminuent et qu'il faut donc passer commande sans tarder… Cette technique est généralement appelée « IP Tracking », dans la mesure où elle repose sur la reconnaissance de l'adresse IP de la connexion utilisée.

La pratique reste toutefois « *difficile à qualifier juridiquement et difficile également à démontrer* » selon Martine Pinville, la secrétaire d'État au Commerce. Interpellée par un sénateur qui lui avait transmis une question écrite en juillet 2015, l'intéressée rappelle que l'enquête menée à ce sujet en 2013 par la CNIL et la DGCCRF était ainsi arrivée à la conclusion qu' « *aucune des techniques observées ne prenait en compte l'adresse IP des internautes comme élément déterminant ou ne visait à moduler le prix des produits ou services proposés aux consommateurs* ».

Aucune plainte de consommateurs enregistrée par la DGCCRF

Pour l'heure, poursuit Martine Pinville, « *la DGCCRF n'a pas été saisie de plaintes de consommateurs concernant des pratiques « d'IP tracking »* ». Bercy n'aurait pas non plus « *eu connaissance de signalements de cette nature* » au sein du réseau de coopération administrative du « G29 » des CNIL européennes.

La secrétaire d'État cherche néanmoins à rassurer : elle annonce que « *le sujet de « l'IP tracking » fera l'objet dans les prochains mois de nouvelles investigations* » de la part de la DGCCRF. Si de telles pratiques venaient à être débusquées, les cybermarchands concernés pourraient être poursuivis pour pratiques commerciales déloyales ou trompeuses, explique Martine Pinville, car « *susceptible[s] d'altérer le comportement économique du consommateur* ». Les contrevenants s'exposeraient alors à des peines pouvant aller jusqu'à deux ans de prison et 300 000 euros d'amende.

Un front pourrait également s'ouvrir en matière de protection des données personnelles. « *L'adresse IP étant une donnée personnelle, il faudrait avant toute exploitation, demander l'accord et le consentement du consommateur ainsi que la déclaration de ces données à la CNIL, en respectant la procédure requise : durée de conservation des données, finalité, etc.* »

Article original de Xavier Berne

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

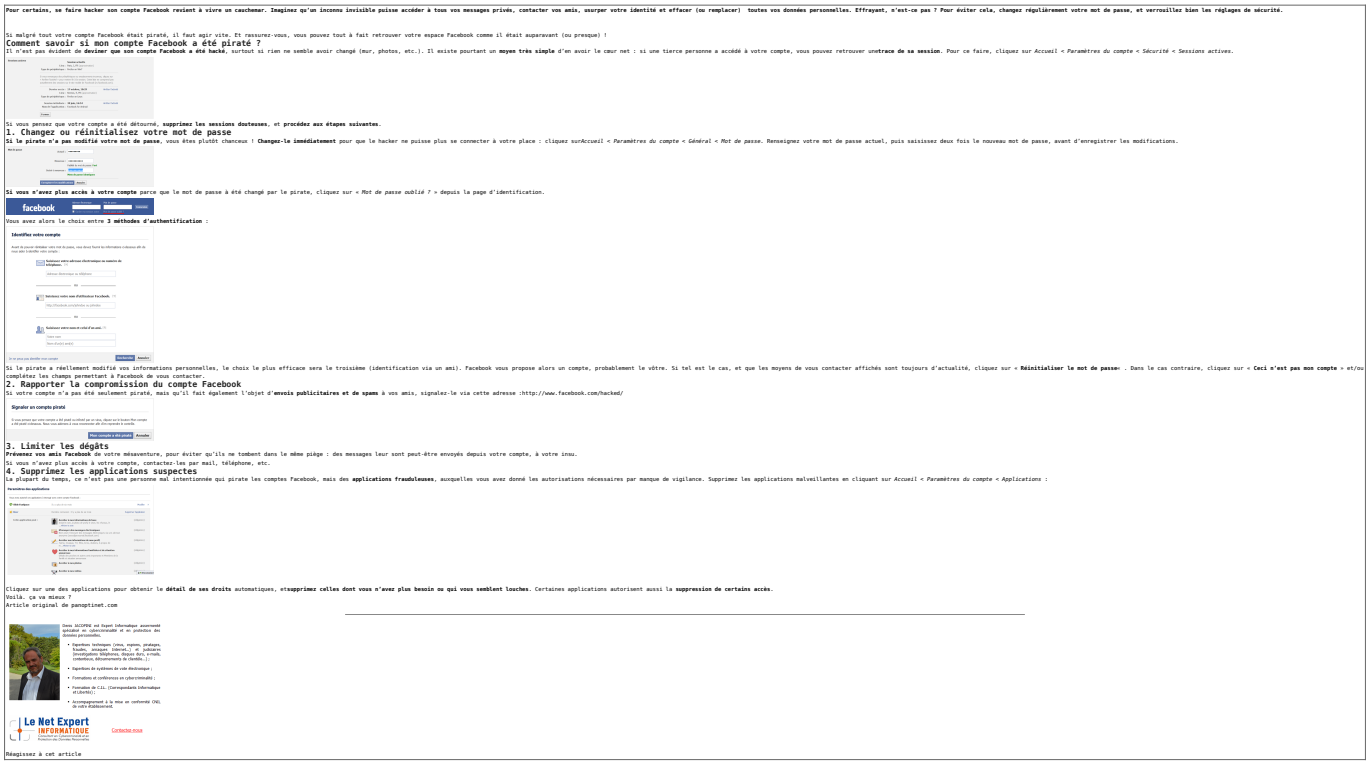
Réagissez à cet article

Original de l'article mis en page : IP Tracking : de nouvelles investigations de la répression des fraudes

---

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

---

Les mots de passe disparaîtront progressivement d'ici 2025

Les mots de passe disparaîtront progressivement d'ici 2025

La technologie de biométrie comportementale et d'authentification à deux facteurs sont à la hausse comme des alternatives plus sûres, selon une étude.

Une étude de 600 professionnels en sécurité de l'opérateur de téléphonie mobile ID TeleSign a révélé que la protection du compte client est un souci majeur pour les entreprises, avec 72 % des personnes interrogées disant que les mots de passe seront éliminés progressivement d'ici à 2025. De plus en plus d'entreprises, selon le rapport, remplacent les mots de passe avec la biométrie comportementale et l'authentification à deux facteurs (2FA) avec 92 % des experts en sécurité affirmant que cela va améliorer la sécurité des comptes considérablement.

« La grande majorité des professionnels en sécurité ne font plus confiance aux mots de passe pour travailler », a déclaré Ryan Disraeli de TeleSign parce que 69 % des répondants ont dit qu'ils ne pensent pas que les noms d'utilisateur et mots de passe fournissent assez de sécurité. Les prises de contrôle de compte (ATO) étaient une préoccupation majeure pour 79 %, alors que 86 % sont préoccupés par l'authentification ID d'identité des utilisateurs du web et des applications mobiles avec 90 % étant touchées par des fraudes en ligne l'an dernier.

Plus de la moitié (54 %) des organisations disent qu'ils passeront à la biométrie comportementale en 2016 ou plus tard tandis que 85 % ont dit qu'ils mettraient en œuvre le 2FA dans les 12 prochains mois. Huit des 10 répondants croient que la biométrie comportementale ne dégradera pas l'expérience utilisateur.

Lire l'étude complète ici

https://iatranshumanisme.files.wordpress.com/2016/07/telesign-report-beyond-the-password-june-2016-1.pdf

Article original de Jaesa

Réagissez à cet article

Original de l'article mis en page : Les mots de passe disparaîtront progressivement d'ici 2025 | Intelligence Artificielle et Transhumanisme

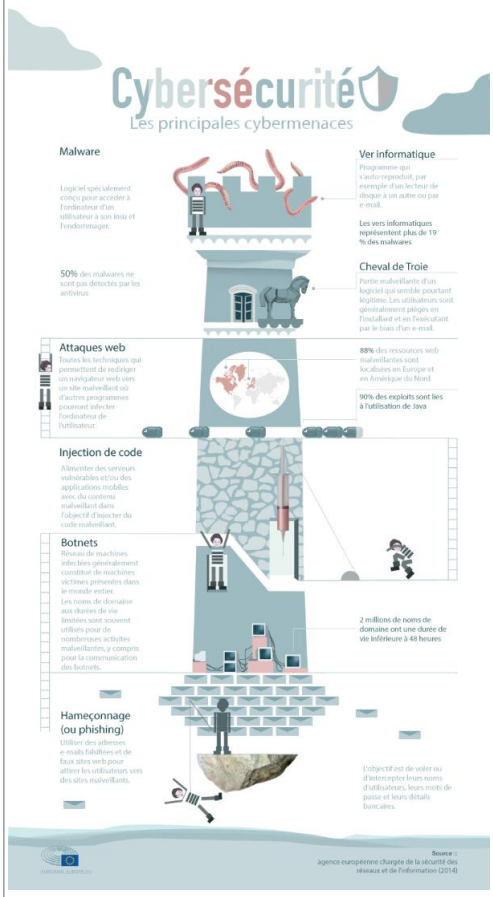
---

Directive sur la sécurité des

réseaux et des systèmes d’information

Directive sur la sécurité des réseaux et des systèmes d’information

Nos sociétés digitalisées reposent de plus en plus sur des réseaux électroniques qui peuvent faire l'objet de cyberattaques aux conséquences importantes. Afin de mieux faire face à ce type de menaces en ligne, le Parlement et le Conseil ont conclu en décembre dernier un accord sur les premières règles européennes en matière de cybersécurité. Celles-ci ont été soutenues par l'ensemble du Parlement réuni en session plénière ce mercredi 6 juillet.



Vols d'identité, faux sites web de banques, espionnage industriel ou inondation de données qui rendent un serveur incapable de répondre : les menaces en ligne sont nombreuses et visent tant les particuliers que les entreprises et les autorités publiques.
Les incidents et les attaques des systèmes d'information des entreprises et des citoyens pourraient représenter un coût de 260 à 340 milliards d'euros par an, selon les estimations de l'Agence européenne chargée de la sécurité des réseaux et de l'information.
Les cyberattaques menées contre certaines infrastructures clés de nos sociétés, comme les services bancaires, les réseaux d'électricité ou le secteur du contrôle aérien, peuvent avoir des conséquences particulièrement importantes sur notre quotidien.
Dans le cadre d'un Eurobaromètre publié en février 2015, les citoyens européens ont exprimé de fortes inquiétudes à propos de la cybersécurité : 89 % des internautes évitent de diffuser des informations personnelles en ligne. Selon 85 % des sondés, le risque d'être victime de cybercriminalité est de plus en plus important.

Vote en plénière
Les députés ont approuvé la directive sur la sécurité des réseaux et de l'information dans l'Union, qui définit une approche commune autour de la question de la cybersécurité.
Le texte prévoit une liste de secteurs dans lesquels les entreprises qui fournissent des services essentiels, liés par exemple à l'énergie, aux transports ou au secteur de la banque, devront être en mesure de résister aux cyberattaques.
La directive les oblige notamment à signaler les incidents de sécurité graves aux autorités nationales. Les fournisseurs de services numériques tels qu'Amazon ou Google devront également notifier les attaques majeures aux autorités nationales.
Ces nouvelles règles sur la cybersécurité visent également à renforcer la coopération entre États membres en cas d'incidents.

Téléchargez la directive sur la sécurité des réseaux et des systèmes d'information – texte approuvé par le Parlement et le Conseil :
http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/fr/pdf
Article original du Parlement Européen

Réagissez à cet article

Original de l’article mis en page : Cybersécurité : mieux faire face aux attaques en ligne

---

Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest

Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest

Au Bénin, les cybercriminels sont habituellement connus sous le nom de « Gaymans. » Les premières méthodes d'escroquerie concernaient les réseaux de jeunes se faisant passer pour des homosexuels, pour appâter des personnes de la même orientation sexuelle dans les pays occidentaux, d'où le nom de « Gayman » donné à la plupart des cybercriminels opérant à partir du Bénin.

Le phénomène fait son apparition dans les années 2000 et se caractérise essentiellement par des arnaques en ligne par des individus sans connaissance particulière en informatique, mais avec de solides atouts en psychologie.

Pour Nicaise Dangnibo, le directeur de l''Office central de répression de la cybercriminalité (OCRC), une unité spéciale de la police béninoise, « le phénomène a pris ses racines à partir du Nigeria, l'un des tout premiers pays d'Afrique de l'Ouest confrontés au phénomène de la cybercriminalité. »

Avec les premières mesures de rétorsion mises en place par les autorités nigérianes, les cybercriminels se sont massivement délocalisés au Bénin et en Côte d'Ivoire.

Ces derniers copiaient sur Internet des photos de jeunes hommes « beaux et musclés » à la recherche de l'âme soeur.

Les méthodes d'escroquerie se sont ensuite diversifiées, pour s'étendre au love chat, au porno-chantage, puis à des montages complexes de fausses affaires.

"Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net."

Pierre Dovonou Lokossou

Gestionnaire de projets technologiques

Selon Pierre Dovonou Lokossou, gestionnaire de projets technologiques, « la première arnaque via l'Internet au Bénin a eu lieu deux ans après l'arrivée du web dans le pays. Il s'agissait d'un Nigérian se prénommant Christopher qui avait escroqué un pasteur américain (Jim), en se faisant livrer 40 ordinateurs, 10 imprimantes et un millier de bibles, en échange d'un chèque délivré par une banque fictive ».

Pierre Dovonou Lokossou raconte qu'à cette époque, « la plupart des mails indésirables (spams) provenant du Bénin étaient en anglais. La répression des actes de cybercriminalité au Nigéria avait vite fait de déverser au Bénin et dans la sous-région de jeunes Nigérians qui pouvaient désormais poursuivre en toute impunité leurs sales besognes… »

« Par la suite, ajoute-t-il, de l'anglais, les spams ont commencé à être rédigés dans un français approximatif, signe qu'avec le séjour de ces cybercriminels anglophones au Bénin, l'apprentissage de la langue française a été mis à contribution. »

Mais actuellement, à en croire le gestionnaire de projets, « le phénomène a pris de l'ampleur dans toute la sous-région ouest-africaine ». « Aussi bien des Béninois que des Togolais et des Burkinabè, des Nigériens et des Ivoiriens s'adonnent à cœur joie à ce cyber-banditisme », précise-t-il.

Offres de vente

Il s'agit le plus souvent de propositions de prêts, voire de dons ou d'offres de vente assez diversifiées diffusées sur des sites internet, ou parfois envoyées sous forme de spams aux internautes.

Les offres de vente vont des appareils électroménagers aux métaux précieux en passant par les téléphones portables, les ordinateurs, les véhicules, voire les animaux ou les domaines fonciers.

Une étudiante en Relations internationales, Adidjath Kitoyi, raconte avoir été contactée en 2012 sur le réseau social Facebook par « une Suissesse âgée de 83 ans atteinte d'un cancer au stade très avancé » qui souhaitait lui céder « une fortune héritée de ses parents et qui se trouve dans les coffres d'une banque à Genève ».

Appâtée, Adidjath s'était empressée d'envoyer à une adresse indiquée (qui se révèlera inexistante) tous les documents administratifs réclamés par son interlocuteur avant d'effectuer à l'attention d'un « intermédiaire » basé en Côte d'Ivoire un transfert de 150 000 FCFA représentant « les frais de dossiers ».

Par la suite, il ne lui était plus possible de communiquer avec la Suissesse donatrice, ni avec l'intermédiaire en Côte d'Ivoire.

La mésaventure d'Adidjath Kitoyi n'est qu'un cas parmi des centaines, voire des milliers d'autres victimes des cybercriminels.

Pierre Dovonou Lokossou distingue trois catégories de cybercriminels.

« La première est celle de ces jeunes qui n'ont pas un emploi légal connu et qui ne fréquentent que les cybercentres ou qui sont toujours avec leur ordinateur portatif et qui ont un train de vie largement au-dessus de la moyenne. Ils changent souvent de motos ou de voitures. Ils peuvent disparaître du quartier pendant des mois et réapparaître pour faire croire aux gens qu'ils étaient en France ou à Abidjan, alors qu'ils étaient en prison ou en cavale; la deuxième catégorie est celle des jeunes qui vont, soit au collège, soit à l'université, ou qui ont un emploi, mais s'adonnent à la cybercriminalité et à divers autres actes d'escroquerie; la troisième catégorie comporte les jeunes qui sont embauchés souvent par les cyber-bandits de la première ou deuxième catégorie et qui jouent le rôle d'assistants. Ce sont eux qui vont récupérer l'argent à la banque, qui jouent le rôle de secrétaire, d'avocat, de notaire pour confirmer au téléphone que le patron ou "son client" est quelqu'un de "bonne foi"…

Dispositif législatif

De 1997 à ce jour, ce qui n'était alors qu'un cas isolé à l'époque s'est mué en un cas d'école. De 2005 à 2010 notamment, le nombre de jeunes quittant les bancs au profit des cybercafés a considérablement augmenté.

Aujourd'hui encore, le phénomène est palpable et les nombreuses descentes de la police ne découragent pas les malfaiteurs.

A la sous-direction des crimes économiques et financiers de la police béninoise (ex-Brigade économique et financière-BEF), la cellule de lutte contre la cybercriminalité a déjà eu à effectuer plusieurs arrestations.

De source proche de ce service de police, quelques-uns des auteurs de ces forfaits via le web croupissent en prison.

La loi portant lutte contre la corruption, adoptée en 2011, qui y consacre tout son chapitre XV (« Des infractions cybernétiques, informatiques et de leur répression »), condamne fermement la cybercriminalité.

L'article 124 dispose notamment : « Quiconque a procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, est puni d'un emprisonnement d'un an à cinq ans et d'une amende de deux millions de francs CFA à vingt millions. »

Mais du dispositif législatif à la réalité sur le terrain, semble exister un grand fossé.

La note d'alerte de l'ambassade de France au Bénin citée plus haut est sans ambages :

Toutefois, des réflexions existent sur le plan local en faveur de la lutte contre la cybercriminalité.

En 2010, le professeur agrégé de droit, Joseph Djogbénou, concluait ainsi une étude intitulée « la cybercriminalité : enjeux et défis pour le Bénin » :

« Le cybermonde appelle la cybercriminalité. A la lumière de l'ensemble de ces considérations, la réponse nationale devra répondre à une double exigence de cohérence. En premier lieu, elle doit, et il ne saurait en être autrement, tenir compte de la convention de Budapest avec laquelle elle doit nécessairement être compatible. En second lieu, elle doit forcément s'inscrire dans un environnement régional propice. La situation est donc mûre (à notre sens) pour un instrument régional en la matière. Toutefois, il faut sur ce sujet un changement d'approche. En effet, l'examen des travaux réalisés jusqu'ici montre que la cybercriminalité n'est pas traitée de façon spécifique, mais comme un aspect particulier de la criminalité organisée. Ici encore c'est aux experts béninois et africains de mettre en exergue la nécessité et l'exigence d'une approche spécifique de la question. C'est à ce prix que l'Afrique parviendra à s'arrimer à la révolution post-industrielle en cours. »

Pour sa part, le gestionnaire de projets technologiques, Pierre Dovonou Lokossou appelle à éviter le piège de la résignation : « Internet a certes révolutionné le monde au point qu'il serait difficile d'imaginer un autre monde sans internet ; mais, autant les coupeurs de routes existent et pourtant nous circulons sur nos routes, autant les flibustiers existent et pourtant nous naviguons sur les eaux ; autant les cybercriminels existeront toujours et nous allons toujours surfer sur le net. »

Le plus urgent, selon lui, « c'est que nos autorités prennent le taureau par les cornes pour freiner de façon drastique ce fléau qui n'honore pas le Bénin et la sous-région ouest-africaine. »

Article original de Virgile Ahissou

Réagissez à cet article

Original de l’article mis en page : Le Bénin, capitale de la cyber-arnaque en Afrique de l’Ouest – SciDev.Net Afrique Sub-Saharienne