Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Arnaques et usurpation de vos données personnelles sur internet au Burkina Faso

Face à la multiplication des plaintes pour piratage de comptes mails, usurpation d'identités sur les réseaux sociaux, Facebook notamment, suivi d'arnaques ou de chantage, enregistrées par la Commission de l'Informatique et des Libertés (CIL), il me plaît de rappeler quelques bonnes pratiques à adopter pour éviter de tomber dans le piège des cyberdélinquants.

Ainsi, il convient de prendre les précautions suivantes :

• Ne pas répondre à un courrier électronique (mail) ou à un message dans lequel votre mot de passe, votre adresse mail, votre numéro de compte bancaire, etc. sont demandés pour quelque raison que ce soit ;

• Eviter de saisir ou communiquer ses informations personnelles confidentielles (mot de passe, coordonnées financières…) sur un ordinateur dont on n'a pas l'assurance qu'il est sécurisé ;

• Eviter d'accepter les invitations d'inconnus sur les réseaux sociaux, Facebook notamment ;

• Eviter d'échanger des contenus inappropriés (photos, vidéos intimes) sur les réseaux sociaux en général et sur Facebook en particulier ;

• Eviter de se connecter aux réseaux internet public (wifi ouvert, des aéroports, des salles de conférences…) ;

• Utiliser un logiciel anti-virus, activer le pare-feu pour un minimum de protection de vos ordinateurs personnels, veiller à leurs mises à jour.

La protection de vos données personnelles, notre préoccupation.
LA PRESIDENTE

Réagissez à cet article

Source : *Arnaques et usurpation de vos données personnelles sur internet : conseils (…) – leFaso.net, l'actualité au Burkina Faso*

CyberDélinquence ou CyberCriminalité ? Le terreau de l’argent facile et des créatures de rêve

	CyberDélinquence ou CyberCriminalité ? Le terreau de l’argent facile et des créatures de rêve

La cybercriminalité ou la Cyberdélinquence est devenue un fléau des temps modernes. Mais facile à comprendre. Cependant, qui s'y frotte s'y pique. Tous ceux qui aiment l'argent facile, les belles filles, les sensations fortes, les Bon chics bon genre sont les principales victimes.

Internet est devenu incontournable avec certes des avantages et des inconvénients. Mais en face, il y a des hommes et des femmes prêts à tout, pour détourner les objectifs.

Phénomène de ces dernières années, la cybercriminalité est devenue un fléau.

Les réseaux sociaux attirent toutes ces personnes, souvent aveugles. Au bout du compte, on perd toutes ses plumes, ses économies, son prestige. Les forces de police, de gendarmerie comptent ainsi jouer un grand rôle pour mettre fin à cela. Mais comme l'a dit le Président Macky Sall, il faut mutualiser et partager les informations. Les gouvernements, les forces de sécurité essaient tant bien que mal, à mettre fin à cette forme de délinquance. Un phénomène de société.

Dans une société en mal de repères, on veut tout et tout de suite.

De l'argent, de belles filles, des Don Juan qui vous couvrent de millions, des voyages, mais en … rêve. Tout est fiction dans ce phénomène. En effet, les internautes ou les victimes mordent souvent trop vite à l'hameçon. Qui dans ce Sénégal n'aimerait pas recevoir des millions sans bouger ? Si cela existait, cela ne sortirait pas du cercle d'amis. Une utopie.

Aujourd'hui, nombre de compatriotes sont étranglés par les banques et les problèmes familiaux. Rien que pour l'obtention d'un crédit bancaire, l'on vous demande des « tonnes de paperasse », authentifiés. Ce sont donc des heures et des heures de connexion jamais gratuites. On surfe à longueur de journée. Et à tous les niveaux de notre haute administration. On se connecte pour des banalités, des futilités. Des conversations à vous donner des insomnies, des dettes.

Ils sont hommes d'affaires, étudiants, chômeurs, commerçants, dans toutes les catégories sociales. On « tchatte » et on oublie tout. On est en retard sur tout. Parce que la tête dans les nuages. Vous voyez souvent des personnes, rire, sourire pour un rien, c'est toujours la bonne humeur sur les visages. Jusqu'à ce que tout vous tombe sur la tête. On vous déplume en un temps record, comme devant ces faiseurs de miracles multiplicateurs de billets.

En effet, c'est la nouvelle version. Tout simplement. Comment se fait-il donc, que dans la clandestinité et dans l'illégalité, un inconnu vous détourne du système normal, sur un simple clic. Les victimes sont prises au piège après avoir été identifié. Sur le net, beaucoup de photos sont truquées. Des hommes se font passer pour des femmes, des femmes pour des hommes. Vous tombez toujours sur des personnages de rêve. Et dans votre subconscient, vous êtes prêts ou prêtes à tout. Pour oublier vos dettes, épouser cette perle rare, vous envoler sur une petite île, sans bruits ni tambours.

Loin de votre entourage, l'on vous propose toutes sortes de services jamais gratuits. Dès que l'argent commence à montrer son bout de nez, vous êtes pris comme une souris au piège. C'est d'abord les crédits téléphoniques, les virements, etc. Ce sont souvent des étrangers qui sont rois dans le phénomène. Mais de plus en plus, des Sénégalais y font légion.

Gagner de l'argent, épouser une belle fille, voyager, des dons… Ce qui est surprenant, c'est que beaucoup de victimes regrettent après avoir été dépouillé. Lors des mercredis de la police organisés cet été, le sujet sur la cybercriminalité avait été évoqué.

Devant les cadres, les hautes autorités de la police, la presse, entre autres, des panélistes avaient sonné l'alarme. Face à ce danger, des débats intéressants ont été organisé. Au Sénégal, il existe une entité qui s'occupe des données personnelles à « protéger » ? Et où il existe toujours selon les panélistes « un flou ». Dans un pays où il n'y a pas de textes juridiques spécifiques sur la cybercriminalité.

L'un des panélistes a évoqué un cas qui mérite attention. Celui d'une personne qui est tombée, par hasard sur un faux médecin. Ce dernier voulait à travers l'ordinateur, lui faire un check up. Imaginez un peu la suite. En lieu et place d'un toubib, ce fut un étranger qui après l'avoir photographié et non passé un « scanner », passe à l'acte deux. Le chantage. Mais la victime ne voulait pas que l'affaire s'ébruite. Déduire les frais et renvoyer la somme restante, une astuce payante

Autres faits importants.

Comment se fait-il que pour un « héritage », à recevoir, jamais dans un acte notarié, ou un « don » d'une personne anonyme, l'on puisse procéder à des virements d'argent… sans traces ? Les sociologues commencent à s'intéresser à l'affaire. Et souvent, leurs théories semblent incomprises de ces amateurs de sensations et de divertissements chèrement payés. Et le phénomène commence à devenir difficile à gérer. L'État du Sénégal a mis en place la brigade de lutte contre la cybercriminalité. Récemment, les gendarmeries africaines se sont rencontrées pour l'analyser. Surtout avec ces jeunes de plus en plus exposés. C'est pourquoi, le Président Macky Sall a demandé à toutes ces forces de défense : police, gendarmerie de mettre en place « des plateformes de partage ». Comme il l'a souligné lors cette rencontre, « les criminels ne connaissent pas les zones ». Souvent entre la gendarmerie et la police on parle « d'écoles ou de couleurs de tenue ».

Pour lui, ce qui importe « c'est le résultat ». Sinon, c'est « un éternel rattrapage ». En donnant comme exemple le ministère de l'Intérieur avec « Interpol ». Un phénomène selon lequel, il faut « une sensibilisation en direction de tous les citoyens.

Et pour ceux qui ont la responsabilité de gérer les systèmes informatiques ». Et le renforcement de la coopération internationale. La cybercriminalité n'a pas de frontières. Ou bien tout simplement être comme ce futé. Lorsqu'on lui a demandé une contrepartie, il a tout simplement demandé à son généreux donateur de lui envoyer l'argent, tout en y déduisant les soi-disant frais bancaires. Ce que le généreux « donateur » n'a pas voulu entendre.

Réagissez à cet article

Source : http://www.rewmi.com/cyberdelinquence-ou-cybercriminalite-le-terreau-de-largent-facile-et-de-creatures-de-reve.html

La CDP malienne venue s’inspirer de l’expérience sénégalaise | Le Net Expert Informatique

	La CDP malienne venue s’inspi08rer de l’expérience sénégalaise

La Commission de Protection des Données Personnelles du Sénégal (CDP) a reçue la visite du 02 au 04 Novembre 2015 de son homologue malien, l'Autorité de Protection des Données à caractère Personnel (APDP), venu s'inspirer de son expérience et de sa pratique. Cette visite s'inscrit en effet dans le cadre du renforcement de la coopération et des échanges d'expériences entre les deux institutions qui ont en charge la protection des données à caractère personnel.

La délégation de l'Autorité malienne, avec à sa tête son Président, M. Oumarou A.G Mouhamed Ibrahim AIDARA, était composé de cinq personnes. Cette visite s'explique selon le Président de l'autorité malienne par la volonté de s'imprégner de l'expérience enregistrée par le Sénégal depuis quelques années en matière de protection des données personnelles. Elle se justifie également par les ressemblances constatées dans les deux pays.

M. Oumarou A.G Mouhamed Ibrahim AIDARA a remercié les autorités sénégalaises de leur accueil chaleureux et précisé qu'ils étaient venus pour apprendre du Sénégal.

De son côté, le Président de la CDP, le Dr Mouhamadou LO, a magnifié le début d'une fructueuse collaboration entre les deux institutions, tout en invitant ses responsables à œuvrer pour que le respect de la vie privée des personnes entre dans les habitudes quotidiennes des Maliens. Les deux autorités de protection ont émis le souhait de nouer une collaboration étroite et un appui mutuel dans le cadre de la lutte contre la violation de la vie privée au sein des deux pays.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Source : http://www.dakaractu.com/Protection-des-Donnees-Personnelles-La-CDP-malienne-venue-s-inspirer-de-l-experience-senegalaise_a100379.html

---

Cybercriminalité : Les

gendarmes en pleine enquête | Le Net Expert Informatique

 Le capitaine Abdoulaye Mbodj Ndiaye et ses hommes mènent de nombreuses enquêtes concernant des arnaques par Internet.	**Cybercriminalité : Les gendarmes en pleine enquête**

La Section de recherches de Dakar nous a ouvert ses portes. Coup de chance, elle investiguait justement sur une arnaque par Internet. La victime, une religieuse, y a laissé un joli montant.

«Pour être plus efficaces, il nous manque encore du matériel»

«Ici, c'est le laboratoire des N-Tech», explique Sekou Diatta en nous faisant entrer dans la pièce. Les fameux «N-Tech», ce sont les enquêteurs en cybercriminalité de la gendarmerie sénégalaise.

Le long du mur, une immense étagère remplie de matériel pour perquisitions et scènes de crime. Comme dans les films: sachets plastiques, rubans de signalisation et gants en latex. Mais les enquêtes menées par Sekou Diatta et ses cinq collègues sont plutôt numériques.

«Nous sommes chargés de récolter toutes les informations relatives au délit. Par exemple sur des disques durs ou des clés USB», détaille le spécialiste. Et il espère que son équipe s'agrandira rapidement. «A six, cela fait un peu juste pour couvrir tout le territoire», reconnaît-il.

Ce qui n'empêche pas les enquêteurs de traiter déjà les nombreux cas de cybercriminalité qui touchent le Sénégal actuellement, selon lui. «Mais c'est vrai que pour être plus efficaces, il nous manque encore du matériel.»

Le capitaine Abdoulaye Mbodj Ndiaye est un homme pressé. C'est dans sa voiture de service, en route pour la caserne de gendarmerie, que le numéro 2 de la Section de recherches nous accorde quelques minutes. «Il y a de plus en plus de plaintes liées à des escroqueries sur Internet. Ce sont des affaires très courantes ces derniers temps au Sénégal», explique-t-il tout en conduisant. L'après-midi est déjà bien avancée et il lui reste encore beaucoup de travail. Le matin même, ses hommes sont intervenus dans un bureau de transfert d'argent pour arrêter un arnaqueur.

Mais pas le temps de se féliciter, l'affaire qui le préoccupe actuellement est une fraude à plus de 260 millions de francs CFA (environ 400 000 francs suisses). Sur ce dossier, Abdoulaye Mbodj Ndiaye n'en dira pas plus. En revanche, il accepte de nous laisser assister à l'enquête sur l'escroquerie par Internet dont une religieuse sénégalaise a été victime.

Marie* vient justement de déposer une plainte. «En juillet, j'ai reçu un courriel d'une Canadienne qui voulait correspondre avec quelqu'un au bout du monde», raconte-t-elle. Une proposition que la religieuse accepte avec plaisir. La dénommée Cassandra lui envoie alors plusieurs photos et lui donne de nombreux détails sur sa famille. Quelques échanges de courriels plus tard, la fausse Canadienne fait une proposition étonnante à Marie. «Elle m'a dit qu'elle avait envoyé un colis avec des ordinateurs et des appareils photo à sa sœur au Bénin.» Sauf que celle-ci a dû rentrer au pays en urgence. Cassandra demande donc à la religieuse si elle peut récupérer les paquets à sa place.

Marie a des doutes, mais la Canadienne sait comment la convaincre. «Elle m'a pris par les sentiments en me disant qu'il y avait aussi un album de photos de famille. Cela m'a émue», précise la sœur. Elle entame donc les démarches pour récupérer le colis et apprend qu'elle doit payer des taxes. «Tout a été très vite, j'ai versé la somme demandée pour rendre service», explique-t-elle.

Le colis n'arrivera bien sûr jamais. Intriguée, la religieuse se renseigne sur Internet et découvre qu'elle a été victime d'une arnaque. «Ils m'ont encore appelée pour me réclamer plus d'argent, donc je me suis décidée à porter plainte», précise-t-elle.

Marie souhaite surtout que son escroc soit mis hors d'état de nuire. «Cela m'a choquée, ils prennent vraiment l'argent de n'importe qui. Que tu sois pauvre ou riche», regrette-t-elle.

Investigations numériques

De son côté, le capitaine Abdoulaye Mbodj Ndiaye et ses hommes ont déjà commencé leur enquête. Ils inspectent l'ordinateur portable que la victime a amené avec elle. «Cela nous permet de recueillir un maximum d'éléments numériques pour mener nos investigations», explique-t-il. Ils commencent par analyser le contenu des échanges, en l'occurrence des e-mails Yahoo. «Là, par exemple, on a un numéro du Bénin alors que l'escroc prétend être au Canada», explique un spécialiste en plein travail. Les gendarmes vont ensuite s'attaquer à l'enquête numérique à proprement parler. Cela va notamment leur permettre de récupérer l'adresse IP du suspect. Quelques secondes plus tard, ils la géolocalisent dans un quartier de Cotonou, la capitale du Bénin.

Le capitaine doit donc procéder à une réquisition de coopération internationale pour obtenir plus d'informations sur ce dossier. Ce qui peut parfois prendre du temps. Mais il assure qu'il ne donne pas la priorité à certains dossiers en fonction de l'origine des victimes ou des suspects. «Ce qui compte pour nous, c'est la gravité des cas. Notamment la valeur du délit et le risque d'atteintes physiques», précise-t-il.

Il reconnaît toutefois que devant le nombre croissant d'affaires d'escroquerie, la cinquantaine de gendarmes qu'il dirige est parfois obligée de déléguer à d'autres unités. «Mais nous ne jetons jamais un cas aux oubliettes, nous faisons toujours de notre mieux.» Surtout que la cybercriminalité n'est pas leur seule préoccupation. «C'est pour cela que l'unité spécialisée qui sera créée en novembre prochain est très importante», conclut-il.

Source : http://www.lematin.ch/monde/gendarmes-pleine-enquete/story/22226136
Par Fabien Feissli (textes) et Maxime Schmid (photo)

Le Cameroun se couvre contre la cybercriminalité | Le Net Expert Informatique

	Le Cameroun se couvre contre la cybercriminalité

Un atelier initié par l'Ecole nationale supérieure polytechnique et financé par le Fonds spécial des activités de sécurité du ministère des Postes et télécommunications, veut mettre fin à la vulnérabilité des systèmes d'information des administrations publiques.

La rencontre de Yaoundé intervient en réponse aux intrusions malveillantes, dans le réseau d'interconnexion électronique, des systèmes d'information de l'administration mis en place par le ministère des Postes et télécommunications (Minpostel). Ce phénomène, explique le patron dudit département, Jean Pierre Biyiti bi Essam, cause de nombreuses pertes à l'Etat.

Les chiffres donnent en effet des sueurs froides, interpellant les pouvoirs publics pour une mise sur pied immédiate de nouvelles mesures de lutte contre un fléau planétaire. En 2014, les administrations camerounaises ont accusé plus de 14 milliards de FCfa de manque à gagner du fait de la cybercriminalité. En 2012, la compagnie aérienne nationale Camair-Co a perdu 2 millions FCfa en vente de billets ; Ecobank s'est fait hacker 43 comptes en 24 heures avec 3 milliards de FCfa, l'opérateur Mobile Telecommunications Networks (Mtn) a perdu un 1,8 milliard d'envoi de crédits. Plusieurs personnalités et représentations diplomatiques n'ont pas échappé aux attaques en ligne.

Le phénomène de la cybercriminalité a pris une envergure mondiale et sa propension, au Cameroun, a contraint le Jean Pierre Biyiti bi Essam à se rendre au front le 8 septembre à Yaoundé, pour le lancement d'un atelier de formation des personnels des administrations publiques. Il est question de sensibiliser les personnes en charge desdits systèmes sur les risques qui planent sur les réseaux des administrations, d'améliorer le niveau de sécurité des outils utilisés.

Un premier forum sous-régional sur la cybersécurité et la cybercriminalité s'était tenu du 24 au 27 février 2015 au Palais des congrès de Yaoundé. Organisée en partenariat avec l'Union internationale des télécommunications et le Commonwealth Telecommunication Office (CTO) en collaboration avec Interpol, la Communauté économique et monétaire des Etats de l'Afrique centrale (Cemac) et la Communauté économique des États de l'Afrique centrale (Ceeac), cette rencontre avait permis de mener des réflexions en vue de l'harmonisation des stratégies de lutte contre le phénomène, des régulations et réglementations en matière de cybersécurité et cybercriminalité, des moyens et outils de lutte, l'adoption de bonnes pratiques visant à créer une culture de cybersécurité en Afrique centrale, le renforcement des capacités et le partage des connaissances ainsi que la protection de l'enfant en ligne.

TIC

Les technologies de l'information et de la communication (TIC) se développent de manière exponentielle et irréversible, induisant une nouvelle civilisation ayant pour socle l'économie dite numérique. Force est cependant de souligner que les TIC s'accompagnent d'une poussée vertigineuse d'infractions et crimes de toute nature. Les atteintes aux biens renvoient à la fraude des cartes bancaires, à la vente, par petites annonces ou aux enchères, d'objets volés ou contrefaits, à l'encaissement d'un paiement sans livraison de la marchandise et autres arnaques de la même veine, au piratage d'ordinateurs, à la gravure pour soi ou pour autrui de musiques, films ou logiciels, etc. Les atteintes aux personnes se réfèrent quant à elles à la propagation d'images pédophiles, à la diffusion, auprès des enfants, de photographies à caractère pornographique ou violentes, de méthodes de suicide, de recettes d'explosifs ou d'injures à caractère racial, d'atteinte à la vie privée, etc.

Selon un rapport publié en 2011, McAfee, une société de sécurité informatique basée aux Etats-Unis, indique le «.cm» du Cameroun fait partie des cinq noms de domaine les plus risqués de la planète (.cm, .com, .cn, .ws, .info), avec un taux de risque de 36,7% sur environ 27 millions de noms de domaines analysés. Ce fléau a connu une flambée sans précédent entre juin 2009 et juin 2010. Les cybercriminels sont allés jusqu'à pirater le site officiel des services du Premier ministre en créant un site web frauduleux («http://www.govcamonline.com/») dont la page d'accueil portait les mêmes informations, jusqu'aux appels d'offres lancés sur le vrai site.

C'est ainsi que de nombreuses personnes, tant du Cameroun qu'ailleurs, se sont vues extorquer d'importantes ressources. Bien d'autres sites web camerounais ont également fait l'objet de cyberattaques à l'instar la douane, en 2008, du ministère des Domaines et des Affaires foncières au cours de la même année, de l'université de Yaoundé I en 2009, des quotidiens La Nouvelle Expression et Cameroon Tribune en 2011, etc.

Mesures de sécurité à parfaire

Le Cameroun a développé un certain nombre d'applications visant à automatiser les procédures, dans le cadre de la politique de mise en place de la gouvernance électronique. Il s'agit notamment de Sigipes, Sydonia, Depmi, e-Guce, etc. De même, les activités de transfert électronique d'argent, de consultation des comptes bancaires en ligne et bien d'autres services encore, se développent de manière étonnante. Le monde étant devenu un village planétaire, ces applications n'échappent pas aux menaces cybernétiques. D'où l'implémentation de systèmes visant à lutter contre les cyberattaques.

Une loi (n°2010/012) relative à la cybersécurité et à la cybercriminalité a été promulguée en fin 2010. Elle vise à instaurer la confiance dans l'utilisation des réseaux de communications électroniques et des systèmes d'information, à fixer le régime juridique de la preuve numérique. Elle protège également les droits fondamentaux des personnes physiques, notamment le droit à la dignité humaine, à l'honneur et au respect de la vie privée, entre autres.

Au plan institutionnel, trois structures sont en charge de la gestion de la question de cybersécurité et de la cybercriminalité au Cameroun. D'une part, le Minpostel est chargé de l'élaboration et de la mise en œuvre de la politique de sécurité des communications électroniques et des systèmes d'information, en fonction de l'évolution technologique et des priorités du gouvernement dans le domaine. L'Agence nationale des technologies de l'information et de la communication (Antic), en collaboration avec l'Agence de régulation des télécommunications (ART), assure, pour le compte de l'Etat, la régulation, le contrôle et le suivi des activités liées à la sécurité des systèmes d'information et des réseaux de communications électroniques ainsi que la certification électronique.

Le Cameroun a également entrepris, depuis 2009, de mettre en place, avec le concours de la République de Corée, une plateforme de sécurité appelée PKI (Public Key Infrastructure, ou infrastructure à clé publique), en vue de sécuriser les transactions gouvernementales en ligne. Ce dispositif donne les moyens suffisants au pays d'ouvrir le marché de la certification, dans lequel l'Antic représente à la fois les autorités de certification racine et de certification gouvernementale. Cette architecture s'inscrit dans le cadre des mesures techniques à prendre en vue de garantir la sécurité des transactions gouvernementales dans le cyberespace national. La plateforme de sécurité permet aussi, grâce aux services d'authentification, de non répudiation, d'intégrité et de confidentialité, de prémunir les données et les échanges électroniques gouvernementales d'attaques provenant de cybercriminels.

La Police se dote d’un laboratoire cybercriminalistique informatique | Le Net Expert Informatique

La Police se dote d’un laboratoire cybercriminalistique informatique

La Police nationale s’est dotée d’un laboratoire cybercriminalistique informatique qui est un dispositif qui consiste à mettre des méthodes et protocoles d’investigation permettant de récolter une preuve numérique en vue de mieux lutter contre la cybercriminalité et la cybersécurité, selon Papa Gueye, élève-commissaire à l’Ecole nationale de police.

’’Il s’agit d’un laboratoire cybercriminalistique informatique logé au sein de la Division des investigations criminelles (DIC). Il est équipé avec des matériels de dernière génération et sert à analyser les données et supports informatiques’’, a expliqué M. Gueye.

Il intervenait à une table ronde à l’initiative de la Direction générale de la police nationale sur le thème : ’’La cybercriminalité et la cybersécurité : enjeux et défis pour les forces de sécurité’’.
Cette rencontre qui entre dans le cadre des cycles de conférences intitulées ’’Les mercredi de la police’’, a réuni des experts informatiques, des juristes, des spécialistes en cybercriminalité, plusieurs policiers entre autres participants.

’’De plus en plus les forces de la police sont appelées à faire face à des crimes nouveaux avec une cybercriminalité pointue et trés bien structurée, d’où la nécessité de se doter de ce genre de laboratoire’’, a poursuivi Papa Gueye qui a introduit un exposé intitulé ’’Cybercriminalité au Sénégal : manifestations et réponses des forces de sécurité’’.

Dans sa communication, M. Gueye, ancien officier à la Police, est revenu sur les différents types de cybercriminalité au Sénégal, les réponses apportées par les forces de la police et les obstacles liés à la répression du phénomène. Pour lui, il est ’’obligatoire pour les forces de défense de s’adapter face à des infractions de type nouveau’’.

Il a invité les populations à se rendre auprès de la DIC qui héberge ce laboratoire pour exposer leurs mésaventures si elles sont victimes d’infractions liées à la cybercriminalité. Papa Gueye a aussi insisté sur la nécessité de capaciter les acteurs de la police et de sensibiliser les populations sur ces ’’crimes nouveaux’’.

Source :
http://www.aps.sn/actualites/societe/article/la-police-se-dote-d-un-laboratoire-cybercriminalistique-informatique-commissaire

Le Mali prépare la riposte face à la montée de la cybercriminalité | Le Net Expert Informatique

	Le Mali prépare la riposte face à la montée de la cybercriminalité

Qu'il s'agisse de groupes étatiques ou non-étatiques, l'Internet représente aujourd'hui beaucoup plus de menaces sur la sécurité comme en témoignent les faux mails, les vols de numéros de cartes bancaires, la pédopornographie, le blanchiment d'argent, le trafic de stupéfiants, voire, les activités à des fins criminelles et terroristes. Les cyberattaques se jouent des frontières et des distances, sont anonymes, et il est très difficile d'identifier formellement le véritable attaquant.

Ces attaques peuvent être réalisées facilement, à bas coût et à très faible risque pour l'attaquant. Elles visent à mettre en péril le bon fonctionnement des systèmes d'information et de communication utilisés par les citoyens, les entreprises et les administrations, voire l'intégrité physique d'infrastructures essentielles à la sécurité nationale. D'où la nécessité d'une stratégie concertée de lutte contre le phénomène.
Avec l'organisation de ce colloque dont le maitre d'œuvre est l''Autorité Malienne de Régulation des Télécommunications/TIC et des Postes (AMRTP) accompagnée par l'Agetic, la Sotelma et Africa ITCs consulting, les autorités entendent apporter une réponse et une approche globale de lutte contre le phénomène. L'objectif du colloque est d'une part, d'informer et de sensibiliser les décideurs politiques et administratifs, les acteurs de télécommunication et des TIC, la société civile ainsi les médias sur l'impérieuse nécessité de la mise en place des dispositifs en matière de cyber sécurité et des mesures de lutte contre la cybercriminalité et d'autre part, d'apporter des réponses adéquates aux menaces.
A l'ouverture des travaux, le ministre Choguel Maïga a noté que les actions à mener pour enrayer les cybers menaces sont particulièrement difficiles, dans la mesure où l'on se trouve dans le domaine de l'immatériel, avec des techniques en constante et rapide évolution et que les sites Internet et les données auxquelles l'on accède proviennent souvent de serveurs hébergés dans d'autres pays. « Toutefois, malgré ces difficultés, une impérieuse nécessité d'agir nous incombe et notre action au Mali repose sur une conviction très forte : la liberté a, comme fondement, la sécurité. Cela suppose que, face à la cybercriminalité, nous ne pourrons pas garantir le plein exercice de la liberté des usagers et des citoyens qu'en nous en donnant les moyens adaptés », a indiqué le ministre qui a formulé le vœu que, lors du colloque, les décideurs politiques et administratifs, les acteurs des secteurs de télécommunications et des TIC, les acteurs de la société civile et les médias saisissent l'occasion pour se familiariser davantage avec le concept de cyber-menace et développer à travers des plans d'activités, une stratégie de cyber-sécurité.
Durant deux jours, les acteurs échangeront, avec les experts sur plusieurs thématiques comme le cyber crime de masse, le cyber crime ciblé, le terrorisme internet. Aussi, les participants vont passer au peigne le rôle du citoyen, des institutions et de l'Etat dans la lutte contre la cybercriminalité, l'état des lieux de la cybercriminalité au Mali ainsi le cadre réglementaire et opérationnel.
Rappelons que la cyber sécurité recouvre l'ensemble des mesures de sécurité susceptibles d'être prises pour se défendre contre les attaques. L'augmentation spectaculaire du niveau de sophistication et d'intensité des cyberattaques a conduit ces dernières années la plupart des pays développés à renforcer leur résilience et à adopter des stratégies nationales de cyber sécurité. Dans plusieurs pays, la prévention et la réaction aux cyberattaques ont été identifiées comme une priorité majeure dans l'organisation de la sécurité nationale.

Source : http://maliactu.net/mali-face-a-la-montee-de-la-cybercriminalite-le-mali-prepare-la-riposte-a-la-taille-des-enjeux/
Par Daniel KOURIBA

Le Maroc abritera l'Africa

Security Forum 2015 | Le Net Expert Informatique

Le Maroc abritera l’Africa Security Forum 2015

Le Maroc accueillera les 12 et 13 octobre 2015, l'Africa Security Forum (Forum africain de sécurité). Il verra la participation de nombreux experts, de chercheurs, de spécialistes de la Défense et de la Sécurité africains, ainsi que leurs pairs, notamment européens et américains.

Organisée par le Think Tank Atlantis, en partenariat avec le Forum international des technologies de sécurité (FITS), basé à Paris, la rencontre, qui se tiendra à Casablanca, sera l'occasion pour les experts, de se pencher sur des problématiques liées à la sécurité, et ceci autour d'une plateforme de débats et d'échanges.
L'objectif d'Africa Security Forum est de mettre en présence les grands opérateurs publics et privés de 16 pays africains, les entreprises les plus innovantes et les experts des secteurs concernés par les thématiques génériques retenues pour cette édition 2015.
Le forum, offrira un cadre idéal pour discuter des questions relatives à la sûreté-sécurité, avec de larges champs d'expertise comme ceux de la défense, de la cyber-défense, de l'intelligence stratégique et de la sécurité industrielle. Selon le président d'Atlantis, Driss Benomar, le développement affiché par nombre de pays dans le monde est immanquablement confronté à des problèmes de terrorisme. Ce qui justifie l'urgence de renforcer la sécurité au niveau des frontières et de durcir les contrôles des flux commerciaux et des transports. « Nous sommes dans une conjoncture très importante et nous pensons que ce forum est une initiative nouvelle pour pouvoir échanger les expériences réussies des uns et des autres pour être efficaces à l'avenir », a-t-il estimé lors d'une conférence de presse, tenue ce vendredi 11 septembre à Casablanca et destinée à la présentation du programme d'Africa Security Forum.

Source :
http://www.financialafrik.com/2015/09/14/le-maroc-abritera-lafrica-security-forum-2015/

L’Afrique prend la mesure du danger de la Cybercriminalité | Le Net Expert Informatique

	L’Afrique prend la mesure du danger de la Cybercriminalité

La cybercriminalité est un phénomène qui prend de l'ampleur sur le continent. Et de plus en plus d'États africains prennent des mesures répressives pour décourager ceux qui veulent se lancer dans cette nouvelle forme de délinquance.

C'est dans ce sens que la Tanzanie vient de rejoindre le cercle des pays africains, comme la Zambie, le Nigeria, l'Afrique du Sud, la Mauritanie et le Kenya, qui ont pris le problème de la cybercriminalité à bras-le-corps. En effet, la Tanzanie va introduire une loi prévoyant jusqu'à 10 ans de prison pour les cyberdélinquants.
En mai dernier, une nouvelle loi sur la cybercriminalité était devenue opérationnelle au Nigéria. Qui devenait ainsi le premier pays, en Afrique de l'Ouest, à introduire des règles visant à réglementer le cyberespace selon Pcworld.
La Mauritanie avait, aussi, voté un projet de loi contre la cybercriminalité en août dernier. Ce projet de loi intervenait pour combler un vide juridique, avait expliqué le ministre mauritanien des TIC.
Face à la montée des inquiétudes, plusieurs pays comme la Côte d'Ivoire et le Rwanda jouent la carte de la sensibilisation contre ce fléau.
Alors que la Tanzanie a l'un des taux de cybercriminalité, sur les médias sociaux, les plus élevés en Afrique, le président tanzanien, Jakaya Kikwete, a déjà approuvé la loi sur la cybercriminalité de 2015, qui deviendra opérationnelle cette semaine.
Avec un nombre de plus en plus important d'Africains qui utilisent Internet – en plus des efforts fournis par les États en vue de réduire la fracture numérique -, il devient primordial de lutter, sur le continent, contre la cybercriminalité. Ce sera à coup sûr l'un des défis majeurs à relever dans le domaine du numérique.

Source : http://www.afriq
ueitnews.com/2015/09/09/cybercriminalite
-lafrique-prend-mesure-danger/

L’état des lieux de la protection des données personnelles en Tunisie | Le Net Expert Informatique

L’état des lieux de la protection des données personnelles en Tunisie

Chawki Gaddes, président de l'INPDP explique les missions et ambitions de cette instance chargée de la protection des données personnelles.

Fruit d'un travail juridique entamé en 2002, l'Instance nationale de la protection des données personnelles (INPDP), régie par la loi organique no 2004-63 du 27 juillet 2004, n'a pu être mise en route qu'au début 2009. Et c'est avec la nomination de son 3e président, en la personne du juriste Chawki Gaddes, qui a succédé, le 5 mai 20015, au magistrat Mokhtar Yahiaoui (les présidents et les membres de l'instance sont désignés par décret pour 3 ans), que le travail effectif a réellement démarré.

«Il faut commencer par sensibiliser, vulgariser et expliquer aux Tunisiens ces notions de données personnelles et leur importance aux échelles individuelle et collective dans tout le pays», insiste Chawki Gaddes.

Les données sensibles

Le président de l'INPDP précise, dans ce contexte, que la donnée personnelle est toute information qui permet d'identifier ou de rendre identifiable une personne (articles 4 et 5 de la loi de 2004). En d'autres termes, toute information qui permet à remonter à la personne concernée : nom et prénom, date de naissance, adresse aussi bien physique qu'électronique, numéro de téléphone, plaque minéralogique de la voiture, numéro d'identification, empreintes digitale ou rétinienne, photo, code génétique, état de santé, opérations bancaires, traces informatiques… «Et la liste n'est pas close, car la science et les techniques évoluent et élargissent davantage le champ de définition de cette notion», ajoute M. Gaddes.

Il y a, en effet, aussi, des données que l'on a pris l'habitude de qualifier de «sensibles»: origine raciale ou génétique, convictions religieuses, opinions politiques, antécédents judiciaires… «Ces données sont, par principe, interdites de traitement», souligne le président de l'INPDP. Et on entend par traitement toutes les opérations réalisées de manière automatique ou manuelle sur les données personnelles. Elles touchent à tout le cycle de la vie d'une information, de sa naissance jusqu'à sa mort : la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation l'expédition…

Des règles à respecter

Toutes ces opérations doivent respecter les règles définies par la loi qui stipule dans son article premier que toute action sur les données personnelles doit se faire «dans le cadre de la transparence, la loyauté et le respect de la dignité humaine».

L'opération de traitement doit être connue de la personne concernée et de l'instance de contrôle. Aucun fichier n'est créé ni géré dans le secret, et l'INPDP mettra en ligne sur son site la base de données relatives à tout traitement sur le territoire national. Cela permet au citoyen (et à tout résident) de savoir où les données sont collectées et auprès de qui il peut y accéder et éventuellement s'y opposer. Il s'agit d'éthique, de confiance et d'honnêteté de sorte que la finalité du traitement soit définie à l'avance sans être détournée vers d'autres buts

En définitive, traiter les données personnelles c'est se mettre à l'esprit que l'on gère des êtres humains et non des choses. Il y va donc de la dignité humaine. Le citoyen, de par l'article 24 de la Constitution, a le droit à la préservation de sa vie privée contre toute intrusion qui, de nos jours, est mise à rude épreuve eu égard au recours intensif aux technologies de l'information et de la communication.

La Convention 108

Dans un monde sans frontières, la question n'a pas été laissée au hasard. En effet, les premiers pas dans le domaine de la protection des données personnelles remontent à 1974, en France, avec l'institution d'un identifiant unique, un projet en cours de réalisation en Tunisie.

L'idée a, depuis, fait beaucoup de chemin, malgré l'opposition d'une commission parlementaire française qui considère qu'il s'agit, bel et bien, d'une atteinte aux libertés des individus. C'est ainsi que la loi «Informatique et Liberté» a vu le jour en 1978 pour instituer les règles essentielles en la matière qui ont servi de support à la Convention 108 du Conseil de l'Europe.

La Tunisie, soucieuse de se conformer aux pratiques internationalement reconnues en matière de respect des droits humains, a demandé, en juillet dernier, à adhérer à cette convention en vue d'instaurer un climat de confiance aussi bien vis-à-vis de ses citoyens que des intervenants étrangers. Elle sera le 5e Etat non-européen à adhérer à cette convention, après l'Uruguay, l'Ile Maurice, le Maroc et le Sénégal.

La Tunisie sera, ainsi, labellisée «espace de confiance» dans le monde et pourra faire partie des marchés de traitement des données personnelles (ou offshoring) «qui contribuera à la création de 50.000 postes d'emploi et à une rentrée de devises de pas moins de 2000 millions de dinars. Encore faut-il qu'elle réussisse sa bataille contre la violation des données personnelles», tient à affirmer le président de l'INPDP

L'Europe a fortement besoin d'externaliser le traitement des données personnelles, compte tenu des coûts assez élevés de cette opération dans l'espace européen, et la Tunisie est appelée à saisir cette opportunité, à l'instar de l'Inde ou de la Roumanie, qui profitent déjà de ce filon.

Les abus et des sanctions

La loi qui garantit tous les droits en matière d'usage des données personnelles a prévu aussi des sanctions qui vont de l'amende, légère ou lourde (pouvant atteindre 50.000 dinars), jusqu'à la peine de 2 à 5 ans de prison lorsqu'il s'agit de communication ou de transfert de données vers l'étranger

Pour se rendre compte de l'acuité de cette problématique et de ses retombées sur la vie de tous les jours, il faut parcourir la liste des infractions possibles et qui pourraient passer inaperçues, telle l'installation des vidéo-surveillance dans les lieux autres que ceux ouverts au public, ainsi que la liste des peines et des pénalités encourues.

Bref, c'est tout un chantier qui est ouvert devant l'INPDP, qui se donne pour mission d'inculquer et divulguer la culture de la préservation des données personnelles et sensibiliser le citoyen sur ses droits dans ce domaine.

Quand on sait que jusqu'au mois de mai 2015, aucun dossier se rapportant à un abus commis dans ce domaine n'a encore été traité et qu'aucun rapport d'activité n'a été ni élaboré ni présenté, on mesure le chemin qui reste à faire dans ce domaine. «Nous comptons sur la société civile et sur les médias pour nous aider dans cet effort de communication en faveur de la préservation des données personnelles», conclue Chawki Gaddes.

Source : http://kapitalis.com/tunisie/2015/09/06/chawki-gaddes-letat-des-lieux-de-la-protection-des-donnees-personnelles-en-tunisie/
Propos recueillis par Wajdi Msaed