

Denis JACOPINI était présent aux cotés de grands experts en cybersécurité à Abidjan pour le 8ème IT Forum 2016



Denis JACOPIN était présent à l'IT Forum 2016 les 7 et 8 juin derniers. Invité aux cotés des plus grands Experts en Cybersécurité, la 8ème édition de ce Forum a eu pour thème Protection des Données, Gestion de l'identité numérique, Protection des transactions à l'ère du numérique : Risques, Enjeux et Stratégies de mise en oeuvre. Voici ses impressions.

Je tiens enfin à remercier tous les partenaires et sponsors sans qui ce Forum n'aurait pas été possible, et enfin, je tiens à remercier chaleureusement le public présent et attentif jusqu'aux ultimes minutes des dernières interventions des panélistes dont j'ai eu l'honneur et le privilège de faire partie.

Durant ces deux jours j'ai à la fois côtoyé des professionnels d'excellente facture et de réputation internationale proposant des produits relatifs à la cybersécurité et d'aide à la transformation numérique., et je me suis retrouvé face à un public d'une attention universitaire, des chefs de grandes entreprises et de grands DSI (Directeurs des Systèmes d'Information) venu écouter les avis et les conseils d'experts et surtout réfléchir avec nous aux moyens à mettre en œuvre pour aider la Côte d'Ivoire à négocier le virage vers un numérique plus sécurisé pour les entreprises et plus rassurant pour les utilisateurs.

Dès l'ouverture de l'IT Forum, nous avons été réconfortés par le discours de Monsieur Bruno Nabagné Koné, Ministre de l'Economie numérique et de la Poste, Côte d'Ivoire rassurant l'assemblée de sa volonté de permettre à son pays une évolution vers un numérique de confiance en ces mots: « Pas de développement économique sans cyber sécurité »



Quelques mots échangés avec Monsieur Bruno Nabagné Koné, Ministre de l'Economie numérique et de la Poste m'ont rassuré. Il compte bien tout mettre en œuvre pour respecter ces propos : « Pour que nos pays puissent continuer à tirer le meilleur profit de ces technologies, il faut un environnement où les utilisateurs sont en confiance. ».

Ce n'est plus seulement au plus haut niveau de l'état, ni au niveau des autorités du pays que cette révolution à lieu. J'ai pu assister à une des étapes essentielles vers une transformation des mentalités numériques et reste persuadé que désormais la Côte d'Ivoire pourra aussi compter sur ses DSI pour mettre en application sans relâche les règles de base d'un vrai hygiène informatique.

De part notre expérience et notre expertise, nous accompagnerons la Côte d'Ivoire dans sa démarche de sensibilisation, de qualification et surtout nous l'aiderons à redorer son blason terni par l'image d'un pays ayant sur son sol brouteurs et autres arnaqueurs.

Ce forum a aussi été l'occasion à l'assemblée d'avoir enfin, après un déballage de solutions de sécurité protégeant d'un nombre très restreint de problèmes, une liste d'un grand nombre d'attaques que la Côte d'Ivoire a à craindre et va devoir combattre sans relâche ces prochaines années.

Au cours de nos interventions, nous avons apporté la preuve à l'auditoire que la solution pour lutter contre la cybercriminalité ne peut pas être techniques. En effet, sur un ensemble de 11 techniques d'attaques courantes, Denis JACOPINI a démontré que seulement 3 pouvaient être maîtrisées par la mise en place de solutions techniques parfois coûteuses.

La prochaine étape, indispensable à mon sens, sera la lourde tâche consistant à faire évoluer les mentalités et les comportements des utilisateurs, dernier maillon de la chaîne sur lequel aucun garde fou technique n'est en mesure de totalement compenser son manque de connaissance des bonnes pratiques. Il restera donc une faille essentielle à combler, celle de l'humain qu'il sera nécessaire d'accompagner avec tact et pédagogie.

Photo : Mathieu Photo & Camera



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.

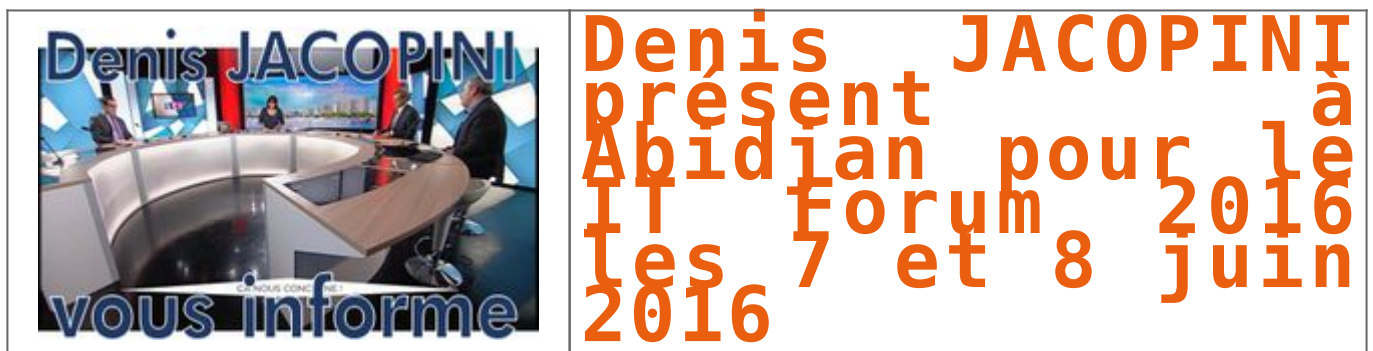


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Le Net Expert Informatique – Expert cybercriminalité, Expert déclarations CNIL, Expert sécurité Informatique, Expert Judiciaire en Informatique, formateur cybercriminalité, formateur CNIL, consultant cybercriminalité, Avignon Vaucluse Aix en Provence Montpellier Marseille Limoges Paris – Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016

Denis JACOPINI présent à Abidjan pour le IT Forum 2016 les 7 et 8 juin 2016



Cybersécurité en Afrique : état des lieux et perspectives



Avec 20% de sa population connectée à Internet, l'Afrique est un continent en voie de connexion au cyberspace. Une partie des pays du continent profite des retombées économiques du numérique mais ceux-ci doivent aussi faire face aux cybermenaces qui mettent en péril leur développement dans le cyberspace. Dès lors, comment se construit la cybersécurité en Afrique?

L'ENJEU DE LA CONNECTIVITÉ AVANT CELUI DE LA CYBERSÉCURITÉ

Avant d'évoquer pleinement la question de la cybersécurité en Afrique, il convient au préalable de poser une série de constats sur le niveau de connectivité du continent africain... [Lire la suite]



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.



[Contactez-nous](#)

Article original : *Cybersécurité en Afrique : état des lieux et perspectives* – SOLUCOMINSIGHT

Auteur : JULIEN DOUILLARD Consultant

Réagissez à cet article

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016



La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM

8^{ème} EDITION

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.

Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.

De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.

En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.

Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes... mais qui montrent aussi rapidement leurs limites !

Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.

En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),

Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des

rencontres les plus importantes.

QUAND

Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier

LIEU

Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –

PROGRAMME

<http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire>



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.



[Contactez-nous](#)

Réagissez à cet article

Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

<http://it-forum.ci>

<https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911>

Les ‘ ‘dix commandements’ ’ de base pour ne pas être une victime d'arnaque

Denis JACOPINI  vous informe	Les ‘ ‘dix commandements’ ’ de base pour ne pas être une victime d'arnaque
---	---

Les cybercriminels continuent de faire de nombreuses victimes à travers le monde. Si des moyens de répression de cette activité criminelle sont entrepris dans nos différents pays, l'un des moyens les plus efficaces de l'éradiquer reste la prévention.



Dans cet article, la Plateforme de lutte contre la cybercriminalité (PLCC) fait un rappel en 10 points des mesures à prendre pour naviguer sur la toile en toute sécurité.

- 1- Changer régulièrement vos mots de passe. (Un site = Un mot de passe unique)
- 2- Aucune autorité judiciaire, de police ne possède d'adresse mail gratuite de type Hotmail, Yahoo, Gmail...
- 3- Ne divulguez pas d'informations personnelles sur Internet. Prenez le temps de sécuriser vos comptes ainsi que ceux de vos enfants. Ne rendez pas visibles vos contacts sur Facebook ou autre réseau sociale.
- 4- Allez toujours sur une adresse commençant par <https://>, officielle et habituelle pour vous connecter à votre compte bancaire, à votre messagerie ou autres réseaux sociaux.
- 5- Evitez d'envoyer des photos ou vidéos, de vous, à caractère sexuelle ou tout autre position indélicate.
- 6- Ne versez jamais d'argent par Mandat Cash ou Western Union à une personne que vous ne connaissez pas, que vous n'avez jamais rencontrée physiquement.
- 7- Méfiez-vous des trop bonnes affaires. Ne cédez jamais à la précipitation. Les bases d'une transaction sont les mêmes dans la réalité et sur Internet. Une annonce trop alléchante cache souvent une arnaque. Renseignez-vous, comparez les prix et les produits avant d'acheter.
- 8- Cessez tout contact si votre interlocuteur (que vous ne connaissez pas) vous demande de l'argent sous prétexte de frais, de maladie, de transport...
- 9- Remettez vous souvent en question. Il n'y a pas de profil type de victime, personne n'est à l'abri sur Internet. Les cyberdélinquants jouent parfois sur notre confiance excessive en nos capacités.
- 10- Ayez un anti-virus efficace et à jour sur votre ordinateur.

Une fois de plus, la PLCC vous exhorte à la prudence !... [Lire la suite]



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.



[Contactez-nous](#)

Réagissez à cet article

Source : *Lutte contre la cybercriminalité: Voici les ‘‘dix commandements’’ de base pour ne pas être une victime d’arnaque*

La Lutte Contre la Cybercriminalité en Côte d’Ivoire. Plus qu’un enjeu économique, une réputation à la clé

	La Lutte Contre la Cybercriminalité, en Côte d’Ivoire. Plus qu’un enjeu économique, une réputation à la clé
---	---

La Côte d'Ivoire a très longtemps souffert d'une image que l'on associait régulièrement aux diverses arnaques sur Internet. Le pays doit avant tout rassurer.

Il suffit d'analyser les principales arnaques sévissant sur les réseaux sociaux, sites de loisirs ou petites annonces en France pour qu'on constate que l'interlocuteur à l'identité fausse mais attrayante soit accessible à partir d'un numéro +225, l'indicatif de la cote d'ivoire.

Certes, Maliens et Nigériens font aussi partie de la fête, mais que ça soit Monsieur Loulou ROBERT, Monsieur Jean OVIDIE, Monsieur Alain BRULIN, se faisant passer tout à tour pour une personne intéressée par un véhicule, une poupée barbie ayant reçu un coup de foudre, votre meilleur ami à qui on a volé son téléphone et ses papiers ou bien une riche personne désirant partager son héritage, ces brouteurs sont Ivoiriens.

Devant l'ampleur du phénomène et l'enjeu majeur que représente la sécurité des systèmes d'information à l'échelle de la Côte d'Ivoire, de l'Afrique et du monde entier, les autorités et les acteurs économiques du pays ont commencé il y a quelques années à réagir en multipliant des actions de formations, de sensibilisation et de perfectionnements technologiques.

Cependant, dans le but de faciliter le développement économique en Côte d'Ivoire et en Afrique des principales entreprises en les rassurant, créer et organiser des forums en 2016 (Conférence internationale sur le renforcement de la cybersécurité et de la cyberdéfense dans l'espace francophone à Grand-Bassam en février dernier et le 8ème édition de l'IT Forum à Abidjan en juin prochain) est un bon début mais ne suffit pas.

En effet, enfin d'enrayer le phénomène de la cybercriminalité, il est important, essentiel et urgent que la Côte d'Ivoire et ses voisins de l'Afrique de l'ouest s'engage à adhérer pour une coopération internationale comme a commencé à le faire à ce jour (15/04/2016), un seul pays d'Afrique, l'Afrique du Sud, en signant la Convention de Budapest.

Source : Denis JACOPINI

Illustration : <http://abidjantv.net>

Etat des signatures et ratifications de la Convention de Budapest

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité »
« Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).



- Mises en conformité RGPD ;
- Accompagnement à la mise en place de DPO ;
- Formations (et sensibilisations) à la cybercriminalité (Autorisation n°93 84 03041 84) ;
- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



[Contactez-nous](#)

Réagissez à cet article

La Côte d'Ivoire va exiger des passeports biométriques aux frontières



La Côte d'Ivoire va exiger des passeports biométriques aux frontières

Bientôt, la Côte d'Ivoire va exiger des passeports biométriques et des cartes d'identités sécurisées à ses frontières. « Sans ces documents, on ne pourra plus entrer en Côte d'Ivoire », a prévenu le ministre d'Etat, ministre de l'Intérieur et de la Sécurité, Hamed Bakayoko.

C'était au cours de la conférence de presse qu'il a co-animée mardi après-midi avec le Procureur général Adou Kouamé Richard, sur l'attentat terroriste de Grand-Bassam, survenu le dimanche 13 mars dernier.

Des propos du Procureur général Adou Kouamé Richard, il ressort que « *l'exploitation efficiente des documents électroniques* » trouvés sur la plage de Grand-Bassam a permis de remonter jusqu'au nommé Kounta Dallah. Cet individu, dont on ignore pour l'instant l'identité et la nationalité, a été présenté par les conférenciers comme le cerveau des attentats qui ont fait 19 victimes et 33 blessés.

A en croire le ministre d'Etat, Hamed Bakayoko, l'enquête se poursuit pour identifier certains individus. Déjà, il faut noter que les preuves numériques ont permis d'interpeller 15 personnes, qui sont à ce stade de l'enquête considérées comme des prévenus. Dans cette affaire, la Côte d'Ivoire bénéficie du soutien du Bureau régional du FBI basé au Sénégal, d'Interpol, de la France, du Mali et du Maroc... [Lire la suite]



Réagissez à cet article

Source : *Attentat de Grand-Bassam : la Côte d'Ivoire va exiger des passeports biométriques aux frontières* | CIO-MAG

Accord de coopération entre le Sénégal et la France pour faire face à la cybercriminalité



Accord de coopération entre le Sénégal et la France pour faire face à la cybercriminalité

La lutte contre la cybercriminalité préoccupe les autorités de la sous région et principalement sénégalaises. l'Agence de l'Informatique de l'Etat (ADIE) Sénégalaise et la ANSS française (Agence Nationale de la Sécurité des Systèmes d'Informatique) ont procédé ce mardi à la signature d'un accord de coopération. Cet accord vise essentiellement à lutter contre la cybercriminalité dans toute sa globalité. Cheikh Bakhom, Directeur Général de l'ADIE a rappelé que le phénomène de la cybercriminalité est un frein à la croissance tout en précisant qu'il est équivalent au volume du trafic de drogue dans le monde.

« C'est un accord de coopération entre le Sénégal et la France dans le cadre de faire face à la cybercriminalité au Sénégal et la France, car c'est un secteur où il faut mutualiser les efforts » selon Cheikh Bakhom.

Il estime d'ailleurs que les préjudices liés à la cybercriminalité sont énormes. « C'est un frein à la croissance et tous les pays du monde y pâtissent. C'est des chiffres alarmes et astronomique qui envoisinent ceux liés au trafic de drogue ».

Pour le Directeur Général Adjoint de l'ANSS, Amiral Dominique RIBAN, « les Etats Unis d'Amérique estiment à 500 milliards de dollars l'économie parallèle à la cybercriminalité. Ainsi cet accord de partenariat entre la France et le Sénégal vient renforcer les liens internationaux entre nos deux pays pour faire face aux attaques cybercriminelles et d'espionnage».

« Nous allons essayer d'apporter la connaissance (réflexions, idées...) du cyberspace et échanger des informations opérationnelle en procédant par la formation, la sensibilisation et la protection des citoyens face à la cybercriminalité. Nous signons cet accord pour améliorer la sécurité globale du cyberspace» renchérit Amiral Dominique RIBAN

Pour Phillippe Kouamé représentant la Cote d'Ivoire, l'identification des Cybers cafés est aussi un facteur essentiel pour une lutte effective contre le fléau.

Abordant les événements douloureux du dimanche dernier dans son pays, Philippe Kouamé estime que ce séminaire qui a conduit à un accord entre ADIE et ANSS est important car « quand on parle de terrorisme, il y'a toujours des Technologies de l'Information et de la Communication (TIC) qui sont utilisées par les terroristes pour planifier ces attaques ».

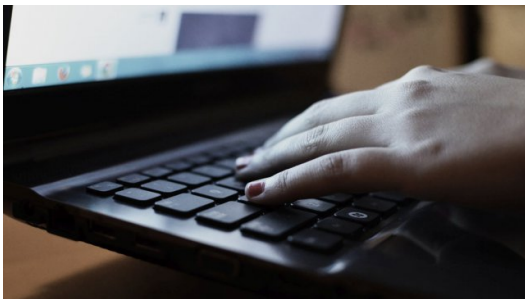
Cet accord donne les prémices de la mise en place de stratégies nationales de cybersécurité au Sénégal... [Lire la suite]



Réagissez à cet article

Source : *Le Sénégal renforce ses liens avec la France pour faire face à la cybercriminalité | SeneNews.com – Actualité au Sénégal, toute actualité du jour*

Arnaque à la SexTape – Ne vous découvrez pas d'un clic



Arnaque à la
SexTape – Ne
vous découvrez
pas d'un clic

Mélange de Sexe et d'Extorsion, la Sextorsion, autrement dit l'utilisation du sexe pour faire chanter des internautes, est un phénomène qui prend de l'ampleur sur internet. Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Limoges a ainsi été contacté sur Internet.

Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Limoges a ainsi été contacté sur Internet. Une « prétendue » jeune fille l'a abordé sur les réseaux sociaux et l'a encouragé à se déshabiller devant sa webcam puis lui a demandé 150 € en mandat-cash sous peine de diffuser la vidéo. Une grosse frayeur pour l'adolescent qui a eu le bon réflexe de prévenir ses parents.

D'abord abordé puis dragué, le mode opératoire est bien rodé pour ces cyberdélinquants et peut toucher la plupart d'entre vous.



Adultes ou adolescents, ils sont de plus en plus nombreux à tomber dans le piège

LA TECHNIQUE

1- Repérage

La technique consiste à repérer ses victimes sur des sites renfermant des nids de cibles faciles. Les forums, les réseaux, sociaux, les sites de rencontre, les sites de loisirs et de manière générale tous les sites internet favorisant le dialogue, les rencontres amicales et surtout amoureuses sont les plus couramment utilisés.

Ce ne fait pas pour au prédateur d'aborder dans la même journée plusieurs dizaines de cibles. L'essentiel est d'avoir un minimum quotidien de victimes pour s'assurer un revenu minimum et régulier.

Trouver des victimes sur Internet pourrait bien finir un jour, comme les envois en masse de mailings ou des opérations en masse de phishing, par avoir ses propres statistiques de retour (Un pourcentage assuré de victimes par rapport au nombre de cibles).

2- Le contact

Une fois la cible repérée, il faut la verrouiller.

Si la cible est un homme, l'usurpateur prendra la peau (les photos et les vidéos) d'un modèle de beauté féminin; et si la cible est une femme, c'est à un bel étalon ou quelqu'un excessivement attentionné que le pirate ressemblera. Il n'y a que l'embarras du choix sur Internet. Un simple clic droit sur une photo permet de l'enregistrer sur son ordinateur et ensuite de l'utiliser impunément.

Le dialogue est alors très dirigé, cherchant à faire parler la victime d'elle, la complimentant, lui trouvant un nombre important de points communs (ça fait partie des techniques de manipulation comportementale que ces voyous savent très bien utiliser) cherchant à instaurer un climat de confiance, développer de la complicité et surtout faire naître, **DES SENTIMENTS** !

Ne vous en faites pas pour le malfrat, quoi qu'il vous dise, il n'a de son côté aucun sentiment, il attend juste que des sentiments commencent à naître chez sa proie et on peut alors considérer qu'elle est malheureusement verrouillée.

3- Le piège

Il existe une technique similaire consistant à vous dérober de l'argent et parfois même, des montants faramineux. Mais c'est la tournure d'une arnaque à la Sextape que prendra la relation à distance si vous avez une Webcam.

Rapidement, au bout de quelques heures ou quelques jours, une fois les sentiments vous faisant quitter le monde rationnel mais plutôt voyager dans le monde des émotions, votre interlocuteur, le plus beau ou la plus belle du monde vous invite à vous dévoiler physiquement pour son plus grand bonheur. Une démarche plus ou moins naturelle vous ne direz, dans le cadre d'une relation amoureuse qui commence à s'installer...

Cependant, à l'autre bout de la souris, l'interlocuteur malintentionné est prêt à appuyer sur sa gachette pour ... vous enregistrer en train de vous dénuder, en train de jouer.

Une fois cette étape franchie, le piège s'est refermé et votre interlocuteur ou votre fausse interlocutrice détient précieusement des images compromettantes.

4- Le chantage

Une fois le piège refermé sur vous, et cette étape franchie, le cybercriminel s'empresse de mettre fin au jeu sexuel pour le remplacer par un jeu de force, consistant à vous menacer de dévoiler sur Internet d'envoyer à votre famille, à votre employeur ou à d'autres de vos contacts la vidéo ou les photos compromettantes capturées si vous ne payez pas une somme d'argent. C'est du chantage (action d'extorquer de l'argent ou tout autre avantage par la menace, notamment de révélations compromettantes ou diffamatoires).

Les pirates vous demanderont à tous les coups, pour conserver l'anonymat grâce à des complices, de régler par mandat cash, western union ou par monnaie électronique, naturellement anonyme.

5- Que faire pour s'en protéger ?

L'action la plus citoyenne que vous pourriez faire consisterait à nous aider à faire de la prévention en partageant cet article, en parlant à votre entourage ou à vos proches de l'existence de ce fléau pour éviter qu'ils se fassent attraper, car une fois le piège refermé sur vous, vu que les communicatins peuvent être surveillées, enregistrées, sauvegardées et partagées dans le cloud, il est souvent trop tard pour supprimer toutes traces de photos ou vidéos compromettantes et ceci, même si vous payez la rançon.

Quelques conseils

- Sois méfiant à l'égard de ceux qui veulent en savoir trop.
- Ne donne aucune information sur toi ou sur ta famille (comme ton nom, ton numéro de téléphone, ton adresse ou celle de ton école...) sans en parler avec tes parents.
- Si tu repis ou si tu vois quelque chose qui te met mal à l'aise, ne cherche pas à en savoir plus par toi-même, déconnecte toi et parles-en à tes parents.
- Si tu envisages de rencontrer quelqu'un que tu as connu en ligne n'y va jamais sans en parler à tes parents.
- Supprime, sans les ouvrir, les mails que tu n'as pas demandés ou qui te sont envoyés par des personnes en qui tu n'as pas confiance.
- N'achète jamais rien sur Internet, sauf si tes parents sont avec toi pour te conseiller.
- Ne donne jamais un mot de passe.

6- Et si c'est trop tard

Si c'est malheureusement trop tard pour vous et que vous êtes bel et bien victime d'arnaque à la Sex Tape, il faut surmonter sa honte et en parler à des amis ou des confidents. Si vous êtes mineur, parlez-en immédiatement à vos parents. Il faut relativiser, se dire que ce n'est pas catastrophique. Vous êtes juste victime d'une escroquerie.

Ensuite, il est important que pouvoir récolter le maximum d'éléments techniques qui permettront de remonter jusqu'à l'auteur de cette machinerie. Pseudos, courriers électroniques avec leurs entêtes, récupérer les adresses IP, garder les SMS, etc., sont un point de départ solide pour une enquête.

Il est également important de porter plainte.

Si vous n'avez pas encore payé, malgré les menaces ou la diffusion de vidéos, ne le faites surtout pas. Payer n'engagera pas la personne à supprimer les informations compromettantes.

Si vous pensez avoir été victime d'une escroquerie sur Internet, mais n'êtes pas sûr, si vous voulez des conseils suite à une tentative d'escroquerie dont vous auriez été victime, vous pouvez contacter la plateforme téléphonique Info Escroqueries, où des policiers et des gendarmes vous répondent au 0811 02 02 17 (coût d'un appel local) », porter plainte en brigade de Gendarmerie ou au Commissariat de Police ou bien signaler l'acte malveillant dont vous êtes victime sur la plateforme PHAROS (Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements) sur www.internet-signalement.gouv.fr.

Ces escroqueries sentimentales sont souvent organisées, par des réseaux structurés, depuis des pays d'Afrique, où la justice peine à se faire entendre même si le cyber harcèlement est puni en France par l'article 222-33-2-2 du code pénal (2014) de 2 ans à 3 d'emprisonnement et de 30 000 à 45 000 € d'amende.

 Réagissez à cet article

Auteur : Denis JACOPINI

Sources :

<http://lci.tf1.fr/france/faits-divers/escroquerie-a-la-sextape-sur-le-net-comment-reagir-6280167.html>

<http://france3-regions.francetvinfo.fr/limousin/haute-vienne/cybercriminalite-un-jeune-limousin-victime-de-sextorsion-937350.html>

<https://www.internet-signalement.gouv.fr>

La cybercriminalité obstacle

au développement de la Côte d'Ivoire



La
cybercriminalité
obstacle au
développement de
la Côte d'Ivoire

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

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

Il a en effet appelé les spécialistes des questions de cybersécurité à rester sur le qui-vive, nonobstant le « solde positif » entre les avantages du numérique et les menaces qui en découlent. Difficile de lui donner tort. Le marché ouest-africain de la cybercriminalité parle de lui-même.

En 2013, la Côte d'Ivoire avait été durement touchée par ce fléau, avec une perte de 26 milliards de FCFA. Au Sénégal, on parle d'une perte de 15 milliards de FCFA due à la fraude sur la toile. Suffisant pour installer un climat de méfiance dans les transactions financières électroniques et un défaut de crédibilité face aux investisseurs.

Autant le dire : un plan d'action sur la cybersécurité et la cyberdéfense dans l'espace francophone s'avère nécessaire. Venus d'une vingtaine de pays, les experts présents à cette conférence internationale ont trois jours, pour proposer une stratégie concrète ... [Lire la suite]



Réagissez à cet article

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