

Vous avez besoin de contacter INTERPOL ? Réponse de Denis JACOPINI Expert en Cybercriminalité et Protection des Données

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>.fr</i></p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>LE NET EXPERT SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
 <p>Denis JACOPINI vous informe ICI</p>		<p>Vous avez besoin de contacter INTERPOL ? Réponse de Denis JACOPINI Expert en Cybercriminalité et Protection des Données</p>			

De très nombreux internautes nous contactent pour nous demander soit comment contacter Interpol, soit pour savoir si la personne d'Interpol avec laquelle ils sont en contact existe bien. Réponses de Denis JACOPINI, Expert en Cybercriminalité et Protection des Données.

Interpol esrt une organisation internationale de police criminelle. Elle ne peut pas directement être contactée ou saisie par les victimes. De plus, sauf cas particuliers, Interpol ne rentre jamais en contact avec les victimes.

D'ailleurs, vous pouvez lire sur leur site Internet sur leur site Internet à l'adresse suivante : <https://www.interpol.int/fr/Contacts/Contacter-INTERPOL>

« Les activités criminelles doivent être signalées à votre police locale ou nationale. INTERPOL ne réalise aucune enquête ni arrestation, cela relève de la responsabilité de la police nationale. »

Ainsi, pour que leurs services soient saisis, **VOUS DEVEZ OBLIGATOIREMENT DÉPOSER UNE PLAINTÉ** auprès de votre Police locale ou Gendarmerie selon les pays. En fonction des éléments constituant votre dossier, les services d'Interpol pourront peut-être se charger de traiter des éléments de votre dossier.

ATTENTION :

De nombreux escrocs se font passer pour Interpol en vous promettant de récupérer votre argent ou pire, pour des victimes ayant récupéré leur argent grâce à une personne d'Interpol. CECI EST AUSSI UNE ARNAQUE

INTERPOL NE CONTACTE JAMAIS LES VICTIMES

C'est juste un moyen horrible d'escroquer encore plus une personne s'étant déjà faite escroquer.

Pour info, CYBERARNAQUES le livre !

<https://livre.fnac.com/a11267131/Denis-Jacopini-Cyberarniques>

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?

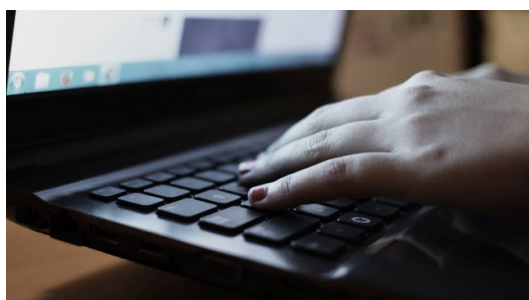
Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Contacter INTERPOL*

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 Linoges a ainsi été contacté sur Internet.

Le 24 février dernier, un garçon de 13 ans qui habite en Haute-Vienne près de Linoges 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 reçois 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 CDP malienne venue

s'inspirer de l'expérience sénégalaise | Le Net Expert Informatique



La CDP malienne venue
s'inspirer de
l'expérience sénégalaise

La Commission de Protection des Données Personnelles du Sénégal (CDP) a reçu 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 composée 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 traitements 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