

Victime d'une arnaque vous demandant de régler par coupons recharges PCS ? Pas de panique !

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Victime d'une arnaque vous demandant de régler par coupons recharges PCS ? Pas de panique !

Les escroqueries à la Carte prépayée et aux coupons recharges PCS Mastercard (ou Transcash ou Tonéo) se développent de plus en plus et ont tendance à remplacer certaines arnaques plus anciennes, mais désormais mieux détectées par les internautes

Par mail ou via Facebook, ils envoient tout d'abord soit un appel au secours venant d'une personne proche ou toute autre raison aboutissant à un chantage.

Ils demandent ensuite de recharger leur carte de crédit par ce nouveau moyen très moderne qu'est la carte prépayée PCS Mastercard. Souvent les personnes ne connaissent même pas le principe de rechargement de carte de crédit mais lorsque l'interlocuteur nous explique qu'il suffit simplement de descendre au bureau de tabac en bas de chez nous, d'acheter 1, 2, 3 ou 4 tickets de rechargement (coupons recharges), puis de lui envoyer les codes pour répondre à sa demande, beaucoup commencent à flairer le piège.

Ce moyen de paiement vient en remplacement des mandats cash ou des versement par Western Union qui ont aujourd'hui une telle mauvaise réputation que leur nom seul éveille des soupçons pour la plupart d'entre nous.. Il permet de rendre impossible de remonter jusqu'au destinataire par la voie judiciaire habituelle.

Ainsi, que ça soit quelqu'un qui se fait passer pour un ami qui vous signale avoir perdu ses papiers ou son téléphone en vous suppliant de l'aide par ce moyen de paiement ou une personne qui exerce sur vous un chantage :

- N'hésitez pas à porter plainte en commissariat de Police ou en Brigade de Gendarmerie (en fonction de votre résidence) ;
- Vous pouvez utiliser un site internet de pré-plainte sur Internet (<https://www.pre-plainte-en-ligne.gouv.fr>)
- Ne répondez plus à ses messages ;
- Signalez ses agissements sur www.internet-signalement.gouv.fr ;

Si vous avez du temps à perdre, vous pouvez aussi vous amuser à les mener en bateau, **les capacités de nuisance de ces arnaqueurs du dimanche étant très limitées** à seulement pouvoir vous envoyer des e-mails ou vous téléphoner si vous avez commis l'imprudence de leur communiquer votre numéro. Vous pouvez rétorquer en leur faisant croire que vous allez les payer ou que vous avez aussi besoin d'un coupon de recharge PCS pour vous déplacer pour aller en acheter un !

Attention :

Si vous êtes en contact avec une personne se présentant comme victime s'étant faite arnaquer par un escroc et que cette dernière vous communique ensuite les coordonnées d'un contact chez Interpol présenté comme son sauveur, fuyez ! Il s'agit aussi d'une arnaque.

Interpol ne rentre jamais en contact directement avec les victimes !

Ceux qui vous soutiennent le contraire ou qui vous contactent directement en se faisant passer pour Interpol ont malheureusement aussi pour objectif de vous soutirer de l'argent.

Plus d'infos sur : <https://www.lenetexpert.fr/contacter-interpol-en-cas-darnaque-est-une-arnaque/>

Remarque :

Il est possible qu'au moment où vous êtes sur le point de déposer plainte, la personne en face de vous cherche à vous dissuader. C'est normal, face aux faibles chances de retrouver l'auteur de l'acte délictueux, ils considèrent comme une perte de temps le fait de devoir traiter votre demande sous forme de plainte et vous inviteront à déposer une main courante.

Insistez pour déposer plainte car sans cette acte citoyen qu'on ne peut vous refuser (en faisant bien attention de le faire en mentionnant la bonne qualification juridique), vous ne laisserez pas passer la moindre chance (même si elle est minime) de faire arrêter l'escroc.

Pour information

- Les délits d'usurpation d'identité, pouvant être associé au phishing selon l'article 226-4-1 du code pénal sont punis d'un an d'emprisonnement et de 15 000 € d'amende.
- Selon l'article Article 312-1 du code pénal, le délit d'extorsion ou de tentative d'extorsion (demande d'argent en échange de ne pas supprimer des données ou de ne pas divulguer des secrets volés) est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.
- Les délits d'escroquerie ou tentative d'escroquerie, selon les articles 313-1, 313-2 et 313-3 du code pénal, sont punis de cinq ans d'emprisonnement et de 375 000 euros d'amende.

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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](#)



Source : *Comment fonctionne une escroquerie à la Carte prépayée et aux coupons recharges PCS Mastercard, Transcash ou Tonéo? | Ms2i On Air*

Attention ! Voici ce que les cyberdélinquants vous réservent... | Denis JACOPINI

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x

x

x

x

x

x

x

Attention ! Voici ce que les cyberdélinquants vous réservent

Ingénieux, fourbes, malicieux... Des qualificatifs qui désignent bien les cyberdélinquants qui parasitent la toile, nos réseaux sociaux. Pourtant s'ils rivalisent d'astuces en tout genre, un mode opératoire se dessine sous nos yeux. A nous de savoir les identifier et de préserver l'intégrité de nos informations personnelles, et de notre portefeuille.

Dans le souci de vous faire de vous-même votre première protection contre ces cyberdélinquants, la Plateforme de lutte contre la cybercriminalité de Côte d'Ivoire (PLCC-CI) vous donne quelques types d'arnaque que ces derniers utilisent pour nous spolier.

Voici dans les grandes lignes, quelques-unes des arnaques auxquelles la PLCC fait face et que vous devez apprendre à identifier.

CHANTAGE A LA VIDEO

Cette escroquerie consiste pour le cybercriminel à :

- Faire connaissance avec sa victime sur les réseaux sociaux, site de rencontre, forum, etc.
- Établir une relation de confiance au fil des discussions
- Proposer à la victime de passer sur un service permettant la visiophonie par webcam
- Favoriser une conversation vidéo plus intime puis profiter pour capturer le flux vidéo des images susceptibles de porter atteinte à la vie privée de la victime
- Demander de fortes sommes d'argent à la victime en menaçant de diffuser ces vidéos sur internet

ARNAQUE AUX FAUX SENTIMENTS

Une arnaque classique. Elle consiste pour le cyber délinquant d'établir une relation de confiance avec sa proie pour mieux l'attendrir puis l'arnaquer ensuite.

ACHAT /VENTE :

En réponse à une offre de vente en ligne sur internet, un prétendu acheteur résidant ou en déplacement en Côte d'Ivoire demande les coordonnées bancaires ou autres du vendeur pour un virement ou l'expédition dudit marchandise avec fausse promesse de règlement des réceptions.

L'escroc passe des commandes de matériels à des exportateurs ou des entreprises en France au nom d'entreprises fictives et propose de payer soit par des cartes de crédit, soit par virement.

SPOLIATION DE COMPTE MAIL OU DE RESEAUX SOCIAUX :

Cette pratique consiste pour le cyber délinquant de prendre possession de votre compte mail ou autre dans le but de perpétrer une usurpation d'identité en envoyant des emails à vos correspondants, en leurs apprenant que soit vous a eu un accident soit vous êtes fait agressé et que vous avez besoin d'argent.

USURPATION D'IDENTITE :

Elle consiste pour le cyber délinquant de se faire passer pour vous. En pratique, c'est le fait pour l'usurpateur d'utiliser soit votre photo, votre carte d'identité ou toute autre chose vous appartenant et qui vous représente.

DETOURNEMENT DE TRANSFERT :

La pratique consiste pour l'escroc de faire le retrait de l'argent qui vous était destiné à votre insu. Pour ce faire, il collecte des informations sur les codes de transfert et aidé par d'autres personnes, il fait le retrait avec de fausse pièce.

FRAUDE SUR SIMBOX :

C'est une technique frauduleuse qui consiste à transiter les appels internationaux en appel et ce au préjudice de l'opérateur de téléphonie et du gouvernement.

FRAUDE SUR COMPTE / BANCAIRE :

C'est l'utilisation frauduleuse de numéro de carte ou compte pour réaliser des paiements sur internet.

FRAUDE INFORMATIQUE :

C'est le fait d'accéder ou de se maintenir frauduleusement dans un système dans tout ou partie d'un système de traitement pour l'entraver, soit pour le supprimer ou, modifier ou le copier.

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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](#)



Source

<http://cybercrime.interieur.gouv.ci/?q=article/cybercriminalit%C3%A9-attention-voici-ce-que-les-cyberd%C3%A9linquants-vous->

Info pratique : Attitude à adopter en cas de réception d'un e-mail étrange voire douteux | Denis JACOPINI

Info pratique : Attitude à adopter en cas de réception d'un e-mail étrange voire douteux

Vous recevez un e-mail étrange voire douteux, vous craignez être victime d'une arnaque ? Apprenez à les identifier et adoptez une attitude visant à contribuer à la destruction de ces réseaux.

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

x	x	x	x	x	x
x	<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-Cyberarnaques>

Réagissez à cet article

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 ?

Quel est notre métier ?

Former et accompagner les organismes à **se mettre en conformité avec la réglementation numérique (dont le RGPD)** et à **se protéger des pirates informatiques.**

Quel sont nos principales activités ?

▪ **RGPD**

- FORMATION AU RGPD
- FORMATION DE DPO
- AUDITS RGPD
- MISE EN CONFORMITÉ RGPD
- ANALYSES DE RISQUES (PIA / DPIA)

▪ **CYBERCRIMINALITÉ**

- FORMATIONS / SENSIBILISATION D'UTILISATEURS

- RECHERCHE DE PREUVES

- **EXPERTISES**

- EXPERTISES PRIVÉES
- EXPERTISES DE VOTES ÉLECTRONIQUES
- EXPERTISES JUDICIAIRES
- RECHERCHE DE PREUVES
- RÉCUPÉRATION DE DONNÉES PERDUES (SMS, Photos, Contacts...)



Notre Expert, Denis JACOPINI, est Expert en Informatique assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

« Mon métier consiste à mettre à votre disposition l'expérience que j'ai acquise pendant des dizaines d'années et

les connaissances que je maintiens continuellement à jour par des formations, certification et diplômes permanentes car le savoir c'est comme une mise en conformité, c'est une démarche quotidienne qui permet une amélioration sur le long terme.

Denis JACOPINI »

Besoin d'un Expert ? contactez-nous

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](#)



Source : *Contacter INTERPOL*

La carte d'identité biométrique ne protège pas les données personnelles

✖	La carte d'identité biométrique ne protège pas les données personnelles
---	--

Invité sur les ondes de l'émission matinale Expresso ce mardi 13 juin 2017, Chawki Gaddes, président de l'instance nationale de la protection des données personnelles Tunisienne souligne que le projet de loi relatif à la carte d'identité biométrique présente certains risques sur la vie privée et la protection des données des citoyens. Ceci est valable au niveau des contenus comme à celui des mécanismes de leur création, utilisation et gestion, particulièrement avec les nouvelles technologies d'information et de communication.

Il a aussi attiré l'attention sur le fait que la reconnaissance automatique des personnes constitue une source d'inquiétude en l'absence du cadre légal judiciaire pour la protection des libertés et des droits des personnes. A ce stade il ajoute qu'il est nécessaire de prévoir la mise en place du cadre légal pour les utilisations possibles et autorisées de la carte d'identité biométrique.

Quant à l'adresse de la personne sur sa carte d'identité, Chawki Gaddes considère ceci absurde et inacceptable, vu que l'adresse n'est pas un constituant d'identité et que ça pourrait changer.

Sur la même question d'absence de cadre légal, le président de l'instance nationale de la protection des données personnelles a appelé à la nécessité de mettre en place une loi spéciale relative au système des renseignements. Ce dernier est très important, tout Etat dans le monde entier dispose d'un système de renseignement et procède aux opérations d'écoutes téléphoniques, c'est pour cela qu'il faut prévoir une loi convenable, qui permet à l'Etat de protéger la sécurité et la défense nationale...[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Chawki Gaddes : La carte d'identité biométrique ne protège pas les données personnelles*

3 auteurs d'arnaques aux faux sentiments arrêtés : 235 ans de prison pour les trois prévenus



3, auteurs
d'arnaques
aux faux
sentiments
arrêtés :
235 ans de
prison
pour les
trois
prévenus

Trois individus de nationalité nigériane ont été condamnés aux États-Unis à une peine totale de 235 ans de prison. Des adeptes de l'arnaque sentimentale.

Âgés de 30 à 45 ans, trois ressortissants nigériens ont été condamnés la semaine dernière aux États-Unis à des peines de 25 ans, 95 ans et 115 ans de prison. Membres d'un groupe de cybercriminels d'une vingtaine de personnes actif depuis au moins 2001, ils avaient été extradés depuis l'Afrique du Sud en 2015.



Ce groupe était basé au Nigeria et aux États-Unis. Les individus sont accusés d'avoir mené et participé à diverses escroqueries en ligne ayant causé des pertes de plusieurs dizaines de millions de dollars. Parmi celles-ci, l'arnaque sentimentale.

En l'occurrence, un arnaqueur utilisait par exemple une fausse identité sur un site de rencontres afin d'établir une relation amoureuse avec une victime. Une fois la confiance de la victime gagnée, elle était incitée à envoyer de l'argent.

Les arnaqueurs pouvaient aussi faire effectuer des transferts d'argent. Du blanchiment d'argent via Western Union et MoneyGram qui sont des noms régulièrement évoqués par des adeptes de l'arnaque sentimentale.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : Arnaque à la nigériane : 235 ans de prison pour trois prévenus

Le CMRPI lance une campagne de sensibilisation à la Cybercriminalité



Le Maroc lance une campagne de sensibilisation à la lutte contre la cybercriminalité.

Quels défis que le Maroc doit-il relever pour lutter contre la cybercriminalité ?

Quelles sont les réalisations déjà accomplies ?

Réponses avec Youssef BENTALEB (Président du CMRPI : Centre Marocain de Recherche Polytechnique et d'Innovation).

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Le Sénat nigérian approuve le

vote électronique pour les élections de 2019

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x

x

x

x

x

x

x

Le Sénat nigérian, approuve le vote électronique pour les élections de 2019

La chambre supérieure du Nigéria, le Sénat a approuvé le vote électronique lors des futures élections organisées par la Commission électorale nationale indépendante (CENI), notamment les élections générales de 2019.

Le Sénat, qui a examiné le rapport de son comité sur la Commission électorale nationale indépendante (CENI) portant sur un projet de loi pour la modification de la Loi électorale no 6, 2010 et pour d'autres questions connexes, qui a été adopté lors de la plénière de jeudi, a également légalisé l'utilisation du lecteur de carte à puce électronique pour les prochaines élections.

La carte à puce électronique a été introduite lors des élections de 2015.

Selon le Sénat, la Commission a adopté le vote électronique à toutes les élections ou toute autre méthode de vote qui peut être déterminée par la Commission.

Le Sénat a ajouté que l'amendement exige le vote électronique sans ambiguïté, mais donne également au Conseil le pouvoir discrétionnaire d'utiliser d'autres méthodes s'il est impossible d'utiliser le vote électronique lors des élections.

[Réagissez à cet article](#)

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

[Notre sélection d'articles sur le vote électronique](#)

[Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise](#)



Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solutions de vote électronique ;

• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

[Contactez-nous](#)

Source : *Le Sénat nigérian approuve le vote électronique pour les élections de 2019 – Apanews.net*

**100 000 emplois en Tunisie
grâce aux smart-cities et
objets connectés**

✕	100 000 emplois en Tunisie grâce aux smart-cities et objets connectés
---	--

La Tunisie se met au numérique pour son développement économique. Avec la régression de l'une des principales sources de revenu qu'est le tourisme, la Tunisie ambitionne d'optimiser son économie avec le projet « Tunisie Numérique 2020 ».

Le numérique, dans l'économie de la Tunisie, représente déjà 11% de taux de croissance annuelle et 7% du PIB, devant le secteur du tourisme. Avec les initiatives privées, le gouvernement travail à faire progresser ce chiffre.

« C'est la première fois que le secteur public se dit : « Je ne vais pas tout faire tout seul et il y a des secteurs que je connais mal », « De notre côté, nous sommes conscients qu'après la révolution, le rôle de la société civile devient plus important et c'est pourquoi nous mettons notre savoir-faire au service de la Tunisie », a expliqué l'entrepreneur, éditeur du logiciel Badredine Ouali, qui préside également le partenariat public-privé Smile Tunisia.

D'ici 2020, le gouvernement tunisien vise créer 100 000 emplois en misant sur les smart-cities ou les objets connectés.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Tunisie: 100 000 emplois grâce aux smart-cities et objets connectés | Africa Top Success

Forum sur les données personnelles au Sénégal



Forum sur les données personnelles au Sénégal

La Commission de protection des données personnelles, en partenariat avec le cabinet Futurs choisis a organisé, jeudi, un forum de sensibilisation à l'intention de certains corps de métier. La rencontre a permis d'échanger et de communiquer en langue nationale sur l'intérêt de protéger ses informations personnelles face aux risques multiples : évolution des technologies, atteintes à la vie privé sur les réseaux sociaux et installation tous azimuts de vidéos surveillances.

Fort de sa mission de communication et sensibilisation, la Commission des données personnelles (Cdp) a pris l'initiative de rencontrer, jeudi, certains corps de métier évoluant surtout dans le secteur informel, notamment les commerçants, pour échanger avec eux, en langue wolof, sur la loi sur les protections de données personnelles, des missions de la Cdp, l'importance de la protection des données personnelles, etc.

Le séminaire a été également une occasion pour la présidente de la Cdp, Awa Ndiaye, de revenir sur les multiples atteintes à la vie privée enregistrées par la commission et relatives aux réseaux sociaux et à l'installation de caméras de surveillance dans certaines entreprises privées.

L'équipe du cabinet Futurs choisis a présenté, en langue wolof, à l'assistance, les missions et le rôle de la Commission de protection des données personnelles non sans préciser l'intérêt de protéger ses données personnelles que Pr Abdoullah Cissé a même qualifié de « sutura » en wolof. Pour lui, en un moment de l'histoire, on pouvait se fier à quelqu'un tout en ayant la certitude que le secret pouvait être gardé. Mais, avec la floraison des nouvelles technologies de l'information et de la communication, cette ère est révolue. D'où l'intérêt, pour lui, de protéger ses données personnelles pour ne pas être victime de diffamation, d'escroquerie, comme il est constaté de plus en plus sur les réseaux sociaux.

Atteintes à la vie privée

La présidente de la Cdp s'est aussi exprimée sur l'installation tous azimuts de caméras et vidéosurveillances. Selon elle, de plus en plus de commerçants installent dans les marchés des caméras de surveillance sans compter les domiciles et entreprises privés qui s'y mettent aussi. Pour Mme Ndiaye, cette installation n'est pas interdite parce que chacun a le droit de se préoccuper de sa sécurité. Toutefois, la présidente demande à ce que les détenteurs de ces caméras de surveillance se mettent en règle par rapport à la loi pour la protection des données à caractère personnel qui régule toute la vidéosurveillance.

« Les détenteurs de caméras de surveillance doivent se mettre en règle avec la loi en déclarant ces vidéosurveillances auprès de la Cdp avant de les installer car ils ne doivent pas être installées n'importe où, surtout dans le cadre du travail, dans les entreprises privées », indique-t-elle. A l'en croire, ils ont eu des cas d'ouvriers qui se sont indignés d'être sous caméras vidéosurveillance 24 h/24h alors que la loi l'interdit et prévoit même des sanctions d'ordre administratives voire pénales.

Les atteintes à la vie privée sur les réseaux sociaux ont été également abordées lors de ce séminaire. En ce sens, renseigne la présidente de la Cdp, au total, ils ont reçu 200 plaintes depuis que la Commission existe, et ce nombre ne cesse d'augmenter non pas à cause de l'installation de vidéosurveillances, mais par rapport aux réseaux sociaux.

« De plus en plus de personnes se voient menacées dans leur intégrité et leur vie privée. Ces derniers n'hésitent pas à se rapprocher de la Cdp pour faire effacer certaines de leurs données qui ont été diffusées de façon illicite », informe-t-elle.

Par Maguette Guèye DIEDHIOU

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Le Soleil – Forum sur les données personnelles : La Cdp sensibilise le grand public en wolof