Fausses applications Pokémon GO. Comment se protéger ? | Denis JACOPINI



Fausses applications Pokémon GO. Comment se protéger ? Les chercheurs ESET découvrent des fausses applications sur Google Play qui cible les utilisateurs de Pokémon GO. L'une d'entre elles utilise pour la première fois une application qui verrouille l'écran (Lockscreen) sur Google Play. Les deux autres applications utilisent la fonctionnalité scareware qui oblige l'utilisateur à payer pour des services inutiles.

Toutes les fausses applications découvertes par ESET et détectées grâce à ESET Mobile Security (application lockscreen nommée « Pokémon GO Ultimate » et les applications scareware

« Guide & Cheats for Pokémon GO » et « Install Pokemongo ») ne sont plus disponibles sur Google Play. Elles ont été retirées de l'app Store suite à l'alerte donnée par ESET. Même si ces fausses applications ne sont pas restées longtemps sur le Google Play, elles ont généré quelques milliers de téléchargements. L'application « Pokémon GO Ultimate », a piégé entre 500 et 1.000 victimes, « The Guide & Cheats for Pokémon GO » en a atteint entre 100 et 50.000 téléchargements.

« Pokémon GO Ultimate » cultive son extrême ressemblance avec la version officielle du célèbre jeu mais ses fonctionnalités sont très différentes : elle verrouille l'écran automatiquement après le démarrage de l'application. Dans de nombreux cas, réinitialiser le téléphone ne fonctionne pas parce que l'application se superpose à toutes les autres, ainsi qu'aux fenêtres du système. Les utilisateurs doivent redémarrer leurs appareils en retirant la batterie ou en utilisant Android Device Manager. Après la réinitialisation, l'application malveillante fonctionne en arrière-plan, à l'insu de sa victime, en cliquant silencieusement sur des annonces à caractère pornographique. Pour se débarrasser de l'application, l'utilisateur doit aller dans Réglages -> Gestion des Applications -> PI Réseau et la désinstaller manuellement.

« Pokémon GO Ultimate » est la première fausse application sur Google Play qui utilise avec succès une fonction de verrouillage d'écran. Comme la fonctionnalité principale de cette application est le clic sur des annonces pornographiques, il n'y a pas de réels dommages. Mais il suffit de peu pour que la fonction de verrouillage d'écran évolue et ajoute un message de rançon, pour créer le premier ransomware par lockscreen sur Google Play.», explique Lukáš Štefanko, Malware Researcher chez ESET.

Alors que l'application « Pokémon GO Ultimate » porte les signes d'un screenlocker et d'un pornclicker, les chercheurs ESET ont également trouvé un autre malware sur Pokémon GO dans Google Play. Les fausses applications nommées « Guide & Cheats for Pokemon GO » et « Install Pokemongo » sur Google Play, appartiennent à la famille des Scarewares. Ils escroquent leurs victimes en leur faisant payer des services inutiles. En leur promettant de leur générer des Pokecoins, Pokeballs ou des uns cufic plusqu'à 999.999 chaque jour — ils trompent les victimes en leur faisant souscrire à de faux services onéreux. (Cette fonctionnalité a récemment été décrite dans un article publié sur WeliveSecurity).

« Pokémon GO est un jeu si attrayant que malgré les mises en garde des experts en sécurité, les utilisateurs ont tendance à accepter les risques et à télécharger toutes applications qui leur permettraient de capturer encore plus de Pokémons. Ceux qui ne peuvent pas résister à la tentation devraient au moins suivre des règles de sécurité élémentaires. » recommande Lukáš Štefanko.

Conseils des experts en sécurité ESET pour les afficionados de Pokémon GO :

- téléchargez uniquement ce qui vient d'une source connue
- lisez les avis en prêtant attention aux commentaires négatifs (gardez en tête que les commentaires positifs ont pu être créés par le développeur)
- lisez les termes et conditions de l'application, concentrez-vous sur la partie qui concerne les permissions requises
- utilisez une solution de sécurité mobile de qualité pour vérifier toutes vos applications

Conseils de Denis JACOPINI

Pour anticiper et vous protéger pour moins de 10€ (10€ est prix de la licence initiale. Une forte réduction sera appliquée au moment du renouvellement au bout d'un an)



Article original de ESET



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des

- Expertises techniques (virus, espions, piratages fraudes, arnaques Internet...) et judiciaire (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 Libertée):
- Accompagnement à la mise en conformité CNI de votre établissement.



Contactez-ne

Suppression d'un contenu web : comment procéder ? | Denis JACOPINI



Suppression d'un contenu web : comment procéder



The Angelet (Mark) (Mark) and the properties of the Control of th
Lance Control of the
See the second s
A DEAD OF MANY CONTROL AND A STATE OF MANY AND
to these to regard upon an open an orderinan a suppress on suppress and super purchased parties in the contract of the contrac
THE ADMINISTRATION OF THE PROPERTY OF THE PROP
Table 1 American Part Part Delical Research and principal and part of the part
That is all an all and a local variables at a local variables at a local variables at a local variable at
Note assess at solvery as you applied to a solvery ?
AND
Extra distribution of the control of
WANTERS TO JUSTICE AND A CONTROL TO JUSTICE AN
Non-million and Market and American Ame
THE RESIDENCE OF THE PROPERTY
A REA or I was the desirate a regime or an entire and a set on the following to the published to be a published to the set of the se
- Middle (Middle) , midd
Language Control Contr
A STATE OF THE PROPERTY OF T
Constant Cons
To an CORRECT OR TO A CORRECT
The Address of Angeles
Service Servic
A STATE OF THE PROPERTY OF THE
** Children's Congress of Cong
THE, I AND THE PART THAN IN THE PART THA
Makes A manufacture and the state of the sta
In this is the activate as an internal an
The Mark I
T-SEAL
The state of the s
A Land Control of the
Seption to the control of the contro
Pennis pe i su sente
to district and control of the contr
and the state of t
200 200 200 100 100 100 100 100 100 100
and an address of the state of
- Apparel To Parametriano
The state of the s
La Bit Expert

LIENS SOURCES

Utilisation des moteurs de recherche en France

http://www.journaldunet.com/ebusiness/le-net/1087481-parts-de-marche-des-moteurs-de-recherche-en-france/

Taux de clic en fonction de la position dans les résultats http://www.mathiasp.fr/blog/seo/quel-est-le-taux-de-clic-en-fo nction-des-positions-dans-google/544

Comment savoir si je suis fiché au FNAEG (Fichier national des empreintes génétiques) ? | Denis JACOPINI



Comment savoir si je suis fiché au #FNAEG (#Fichier national des empreintes génétiques) ?

Pour avoir ces informations, vous devez écrire (en joignant une copie d'une pièce d'identité) à l'adresse suivante :

Pour avoir ces informations, vous devez et Directeur central de la police judiciaire Ministère de l'Intérieur 11 Rue des Saussaies 75800 Paris Cedex 08

Si vous n'avez pas de réponse dans un délai de 2 mois ou si votre demande est refusée, vous pouvez adresser une plainte à la CNIL ou porter plainte auprès des services de police, de gendarmerie ou du procureur de la République.

L'effacement de votre inscription est possible dans certains cas, en vous adressant au procureur de la République du Tribunal de grande instance compétent.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous Denis JACOPINI

Tel : 06 19 71 79 12 formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL. Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant Lager informatique assemiente et formateur specialise en securité informatique, en **Cybert imministre** et en **declaracions à la Chil.** Denis Jacobrat et le met Lagert sont en messine de prendre en character qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et au protection juridique du chef d'entreprise.

Contactez-nous

Cet article vous plait ? Partagez ! Un avis ? Laissez-nous un commentaire !

http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=65372FC5C6502D0A6ED2239F1706AE63?name=FNAEG+(Fichier+national+des+empreintes+g%C3%A9n%C3%A9tiques)+%3A+comment+savoir+si+je+suis+fich%C3%A9+%3F6id=256

Windows 10 : Identifier les applications malveillantes partir des services défaut | Denis JACOPINI

Windows 10 : Identifier applications malveillantes à pa des services par défaut



[block id="24761" title="Pied de page HAUT"]

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

: https://www.winhelponline.com/blog/windows-10-default-servic
es-configuration

Demande de Devis pour un audit RGPD



Special Conference on the Conf				
The state of the s				
Section 1.				
	Eus von gerantinous une confidentialité entrême sur les information, communiquées, les personnes habilitées à consulter ses inf	restions and assetses as secret professional.		
	Printed part that collection for the At-Marin position, and the printed an assessment out offsite.			
1				
	Mile allegade and a second and			
	to have a hispan on one or or of his to describe			
	NOT A STATE OF THE PARTY OF THE		1	
	Milled of our will be delicated in a second of the second	******		
The Continue of the Continue o				
	b. It made impossible describerage part describerage part describerage de la propertie y largered de completation par france la regil la malignatura de la propertie de describera de describera de la propertie describerages part descripadar de des describera de des properties. Basis de la describeration de la properties de la			
	And could be distinct that is first 1. Set (v) Set (market) in First (v) different and 1.	*.*.*		
Manufacture and a state of the				
	Ballot de altra fondam de la fo	#		
	Transfer and the first facilities of	#19090 mm.m		
	Material State of State (State of the State of S			
	The Financial and problems is a problem on a financial and the second of			
	THE STATE OF THE S			
	To be, and setting to the strong of			
	Visited, and selected paint? The contract property of the contract paint of the contrac	*****		
	Visign as continue as horizontale as because due unto two physicians as to those professional and as the desire as	•		
	The procedure country of the control of the country			
	Fig. 10 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1			
-				
* - Mark B - Contract				

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



DÉSIGNATION N° DPO-15945





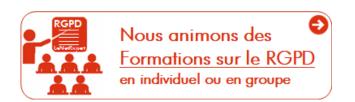
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

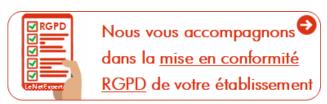
Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une expérience d'une dizaine d'années dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de mise en conformité avec le RGPD.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source : Denis JACOPINI

Bonnes pratiques face à une

tentative de cyber-extorsion | Denis JACOPINI



Bonnes pratiques face à une tentative de cyber-extorsion

Bonnes pratiques face à une tentative de cyber-extorsion

1. Typologie des différents cas de cyber-extorsion

Le type le plus répandu de cyber-extorsion est l'attaque par crypto-ransomware. Ce dernier est une forme de malware qui chiffre les fichiers présents sur la machine infectée. Une rançon est par la suite demandée afin d'obtenir la clef qui permet de déchiffrer les données compromises. Ces attaques touchent autant les particuliers que les acteurs du monde professionnel. Il existe cependant deux autres types de cyber-extorsion auxquels doivent faire face les sociétés.

Le premier cas est celui du chantage faisant suite à un vol de données internes. L'exemple le plus marquant de ces derniers mois est celui du groupe Rex Mundi : ce dernier dérobe des informations sensibles/confidentielles — comme une base clientèle — puis demande une rançon à sa victime sous peine de divulguer son butin et par conséquent de rendre public l'acte de piratage; ce qui peut être fortement compromettant pour la société ciblée comme pour sa clientèle. De nombreuses entreprises comme Dexia, Xperthis, Voo ou encore Labio ont été victimes des chantages du groupe Rex Mundi.

La deuxième pratique est celle du DDoS contre rançon, spécialité des pirates d'Armada Collective. Le modus operandi est simple et efficace : la cible reçoit un email l'invitant à payer une rançon en Bitcoin afin de ne pas se voir infliger une puissante attaque DDoS qui rendrait son site web indisponible à ses utilisateurs. La plupart des victimes sont des sociétés de taille intermédiaire dont le modèle économique est basé sur le principe de la vente en ligne — produits ou services — comme le fournisseur suisse de services de messagerie ProtonMail en novembre 2015.

2. Bonnes pratiques à mettre en place

En amont de la tentative de cyber-extorsion

Un ensemble de bonnes pratiques permet d'éviter qu'une attaque par ransomware se finalise par une demande de rançon.

Il convient de mettre en place une stratégie de sauvegarde — et de restauration — régulière des données. Ces back-ups doivent être séparés du réseau traditionnel des utilisateurs afin d'éviter d'être chiffrés en cas de déploiement d'un crypto-ransomware. Dans ce cas de figure, le système pourra être restauré sans avoir besoin de payer la rançon exigée.

La propagation d'un malware peut également être évitée par l'installation d'outils/solutions de cybersécurité notamment au niveau du client, du webmail et du système d'exploitation (antivirus). Ceci doit obligatoirement être couplé à une mise à jour régulière du système d'exploitation et de l'ensemble des logiciels installés sur le parc informatique.

L'être humain étant toujours le principal maillon faible de la chaîne, il est primordial de sensibiliser les collaborateurs afin qu'ils adoptent des comportements non-risqués. Par exemple : ne pas cliquer sur les liens et ne pas ouvrir les pièces-jointes provenant d'expéditeurs inconnus, ne jamais renseigner ses coordonnées personnelles ou bancaires à des opérateurs d'apparence légitimes (banques, fournisseurs d'accès Internet, services des impôts, etc.).

Ces bonnes pratiques s'appliquent également dans le cas d'un chantage faisant suite à un vol de données internes. Ces dernières sont en général dérobées via l'envoi dans un premier temps d'un spam contenant une pièce jointe malicieuse ou une URL redirigeant vers un site web compromis. Une fois le système d'information compromis, un malware est déployé afin de voler les informations ciblées.

La menace provient également de l'intérieur : un employé mal intentionné peut aussi mettre en place une tentative de cyber-extorsion en menaçant de divulguer des informations sensibles/confidentielles. Ainsi, il est important de gérer les accès par une hiérarchisation des droits et un cloisonnement.

Pendant la tentative de cyber-extorsion

Lors d'un chantage faisant suite à un vol de données internes, il est important de se renseigner sur la véracité des informations qui ont été dérobées. Certains groupes de pirates se spécialisent dans des tentatives de cyber-extorsion basées sur de fausses informations et abusent de la crédulité de leurs victimes. Il en va de même concernant l'origine du corbeau : de nombreux usurpateurs imitent le style du groupe Armada Collective et envoient massivement des emails de chantage à des TPE/PME. Ces dernières cèdent fréquemment à ces attaques qui ne sont pourtant que des canulars.

Il est vivement recommandé de ne jamais payer une rançon car le paiement ne constitue pas une garantie. De nombreuses victimes sont amenées à payer une somme bien plus conséquente que la rançon initialement demandée. Il n'est pas rare de constater que les échanges débutent de manière très cordiale afin de mettre la cible en confiance. Si cette dernière cède au premier chantage, l'attaquant n'hésite pas à profiter de sa faiblesse afin de lui soutirer le plus d'argent possible. Il abuse de techniques basées sur l'ingénierie sociale afin d'augmenter ses profits. Ainsi, l'escroc gentil n'existe pas et le paiement de la rançon ne fait que l'encourager dans sa démarche frauduleuse.

De nombreuses victimes refusent de porter plainte et cela pour plusieurs raisons. Elles estiment à tort que c'est une perte de temps et refusent également de communiquer sur les résultats et conséquences d'une attaque qui ne feraient que nuire à leur image auprès des clients, fournisseurs ou partenaires. Pourtant cette mauvaise stratégie ne fait que renforcer le sentiment d'impunité des attaquants, les confortent dans le choix de leurs modes opératoires et leur permet de continuer leurs actions malveillantes. Il est ainsi vital de porter plainte lors de chaque tentative de cyber-extorsion. L'aide de personnes qualifiées permet de faciliter ce genre de démarches.

En cas d'attaque avérée, il est essentiel pour la victime de s'appuyer sur un panel de professionnels habitués à gérer ce type de situation. La mise en place d'une politique de sauvegarde ou bien la restauration d'un parc informatique n'est pas à la portée de toutes les TPE/PME. Il est nécessaire de faire appel à des prestataires spécialisés dans la réalisation de ces opérations complexes.

Par ailleurs, en cas de publication de la part de l'attaquant de données sensibles/confidentielles, il convient de mettre en place un plan de gestion de crise. La communication est un élément central dans ce cas de figure et nécessite l'aide de spécialistes.

Article original de Adrien Petit



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-nou

Réagissez à cet article

Original de l'article mis en page : Bonnes pratiques face à une tentative de cyber-extorsion [Par Adrien Petit, CEIS] | Observatoire FIC

Spécial Phishing 1/3 : Quelle est la technique des pirates informatiques ?





On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.

1. Vous recevez un courriel piégé

Le courriel suspect vous invite à :

- cliquer sur une pièce-jointe ou un lien piégés
- communiquer des informations personnelles
- 2. L'attaquant se fait passer pour une personne ou un tiers de confiance

L'attaquant est alors en mesure de :

- prendre le contrôle de votre système
- faire usage de vos informations
- Impact de l'attaque
- Intégrité
- Authenticité
- Disponibilité
- Confidentialité

Motivations principales

- Atteinte à l'image
- Appât du gain
- Nuisance
- Revendication
- Espionnage
- Sabotage

[block id="24761" title="Pied de page HAUT"]

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre) Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances

similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître ! Commandez sur Fnac.fr https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source : ANSSI — On vous incite à communiquer des informations importantes ? Ne tombez pas dans le piège.

Comment naviguer incognito

sur Facebook avec les règles de confidentialité actuelles | Denis JACOPINI



Fin novembre, le réseau social Facebook a annoncé son intention de changer ses conditions d'utilisations, principalement pour permettre un meilleur ciblage publicitaires. Et comme vous ne pourrez pas les refuser -considérant que ceux qui continuent à l'utiliser acceptent de fait la mise à jour- mieux vaut connaître les règles à appliquer pour maîtriser au mieux les nombreuses informations de votre profil.

Atlantico : Le réseau social Facebook a mis à jour ses règles de confidentialité au cours du mois de novembre. En quoi celles-ci sont-elles différentes ?

Emilie Ogez : En effet, courant novembre, Facebook a de nouveau modifié sa politique de confidentialité (pour le meilleur et pour le pire), qu'on peut aborder en trois points.

1. La mise en place de l'espace pédagogique « Privacy Basics » : Facebook a souhaité rassurer les utilisateurs en mettant en place une sorte de tutoriel qui les guide pas à pas sur la modification des paramètres. Ces derniers sont divisés en 3 catégories :

- ce qu'on montre aux autres.
- · comment les autres interagissent avec nous
- et ce que nous voyons.
- C'est une bonne chose et ce sont de nouveaux efforts consentis par Facebook pour simplifier les paramètres de confidentialité.
- 2. La mise à jour des conditions d'utilisation, qui seront mises en application le ler janvier 2015 : les conditions d'utilisation de Facebook ont été clarifiées et certains passages reformulés. La politique d'utilisation des données a particulièrement été revue. Et Facebook a décidé d'exploiter de nouvelles données personnelles ; en l'occurrence les localisations de ses utilisateurs. Ainsi, si vous décidez de partager votre position, vous pourrez voir les menus des restaurants à proximité ou le statut de vos amis aux alentours. Les informations relatives aux paiements sont également exploitées par le réseau social.
- 3. Le ciblage publicitaire plus fin : les annonceurs pourront désormais afficher des publicités adaptées aux habitudes des internautes à l'intérieur de Facebook mais aussi en dehors (sites web et des applications de tiers qui ont recours aux services Facebook). Prenons un exemple pour bien comprendre ce changement : « Imaginez que vous envisagez d'acheter un téléviseur et que vous commencez à faire des recherches sur le Web et dans des applications mobiles. Facebook pourrait alors vous montrer des publicités pour obtenir le meilleur prix ou vous faire connaître d'autres marques à considérer ». C'est une importante évolution mais Facebook reste prudent. Le site propose ainsi à l'utilisateur de savoir pourquoi il reçoit telle ou telle publicité mais aussi de les refuser.

Quelle est la marche à suivre pour assurer la maîtrise de ses données personnelles ?

- 1. Un bon début est de commencer par cliquer sur « Aperçu du profil en tant que » sous la photo de couverture de votre profil afin de voir comment certains de vos amis ou le « Public (ceux qui ne sont pas amis avec vous) vous voient.
- 2. Ensuite, passez à la phase « paramétrage » en suivant ces quelques conseils et selon vos souhaits (visibilité importante, limitée, etc.).

Les Photos

Lorsque vous publiez une photo sur Facebook, vous pouvez choisir à qui elle est accessible. Elle est peut être « publique » (et donc visible de tous, sur Facebook et en dehors de Facebook, dans les moteurs de recherche), accessible seulement aux « amis », à vous uniquement (« moi uniquement »), à certains amis (« personnalisé ») ou encore à une liste d'amis que vous aurez créée avant publication. Prenez le temps d'y réfléchir avant de poster ! Si toutefois, vous vous êtes trompés, rassurez-vous, il est encore possible de changer la visibilité la photo (ainsi que celle des plus anciennes).

En cas d'identification sur une photo, vous avez deux possibilités : retirer la mention (ouvrez la photo, cliquez sur « Options » puis sur « Supprimer l'identification ») ou faire en sorte que la photo n'apparaisse pas dans le journal (en la masquant). Mais vous pouvez aussi décider d'examiner toutes les identifications avant qu'elles n'apparaissent sur Facebook

Comme pour les photos, il est possible de choisir à qui chacun de vos statuts est accessible. Certains contenus sont plus privés/intimes que d'autres. Mais c'est à chacun de définir ses propres « limites ». Sachez par ailleurs qu'il est possible de limiter l'accès à vos anciens statuts Facebook. Cliquez sur « Paramètres », puis « Confidentialité ». Vous trouverez alors une option « Limiter la visibilité des anciennes publications sur votre journal ». Lisez les instructions attentivement avant de vous lancer. En ce qui concerne les identifications, la démarche est la même que pour les photos.

Infos personnelles

Il est possible de paramétrer très finement la visibilité de toutes les informations contenues dans son profil (famille et relations, lieux où on a habité, etc.). Par exemple, dans « Emploi et scolarité », pour chaque emploi occupé, vous pouvez très facilement choisir qui peut le voir (cliquez sur « Options » à côté du poste, puis sur « Modifier »).
Facebook propose aussi à ses utilisateurs qu'on ne puisse pas les retrouver au moyen d'un numéro de téléphone, d'une adresse e-mail ou encore via les moteurs de recherche (lien vers le

profil). Pour activer ces options, allez dans les paramètres de confidentialité puis « Qui peut me trouver avec une recherche ? ».

Attention à ce que vous postez sur les Pages et dans les groupes de discussion. Les paramètres de confidentialité que nous avons évogués ne concernent que votre profil. Les messages Dostés sur ces espaces Facebook peuvent être référencés par les moteurs de recherche.

Lorsque vous aimez une Page, elle apparaît sur votre profil. Mais si vous souhaitez que cela ne soit pas le cas, c'est possible. Rendez-vous sur votre profil personnel. Sous votre photo

de couverture à droite, cliquez sur « Plus » puis sur « Mentions J'aime ». Une page regroupant tous vos favoris s'ouvre alors. En cliquant sur le crayon puis sur « Modifier la confidentialité », vous pourrez choisir qui voit vos mentions J'aime.

Pour les groupes, il est possible de les masquer.

Vous pouvez aussi souhaiter que cette section « Mentions J'aime » ne soit tout simplement pas visible du tout. Dans ce cas, sélectionner « Gérer les sections » dans le menu sous « Plus » et désélectionnez « Mentions J'aime ». Même chose pour les groupes.

près cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : http://www.atlantico.fr/decryptage/comment-naviguer-incognito-facebook-avec-regles-confidentialite-actuelles-1927087.html

Que faire si on vous refuse l'accès à votre dossier médical ? | **Denis JACOPINI**

























Nous attirons votre attention sur le fait que cette information est modifiée par la mise en place du RGPD (Règlement Général sur la Protection des données). Plus d'informations ici

https://www.lenetexpert.fr/comment-se-mettre-en-conformite-ave c-le-rgpd Nous l'avons toutefois laissée accessible non pas par nostalgie mais à titre d'information.



Vous avez demandé à avoir accès à votre dossier médical et vous n'avez pas eu de réponse ou une réponse négative ? Si votre dossier est détenu par un hôpital public ou une clinique participant au service public hospitalier, adressez un courrier à la Commission d'accès aux documents administratifs :

CADA

35, rue Saint Dominique

75700 Paris 07 SP

Si votre dossier est détenu par un établissement privé (clinique) ou un médecin libéral (généraliste ou spécialiste), vous pouvez adresser une plainte à la CNIL.

Adresser une plainte à la CNIL

Vous pouvez également porter plainte auprès du procureur de la République du Tribunal de grande instance dont vous dépendez.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



DÉSIGNATION N° DPO-15945





Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

[block id="24761" title="Pied de page HAUT"]

Source :

http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=9 DCFCE66E3DC38F485EA18F87E1E023F?name=Dossier+m%C3%A9dical+%3A+ que+faire+si+on+me+refuse+l%27acc%C3%A8s+%3F&id=265

Elections par Internet et Votes électroniques



Les décrets d'application de la Loi Travail continuent d'arriver en ce dernier mois de l'année 2016. L'ultime en date concerne le vote électronique (1). En tant que représentants du personnel, que vous soyez délégué du personnel ou membre du comité d'entreprise, vous vous demandez quelles sont les conditions à réunir pour recourir à ce type de dispositif. Vous souhaitez savoir quels sont les apports de la Loi Travail sur le vote électronique : quel accord mettre en place et quelles garanties pour le système adopté Voici les 3 points essentiels à connaître à propos du vote électronique !

Avant la loi Travail, le vote électronique n'était possible que sous réserve d'avoir été prévu par un accord collectif. Mais est-ce toujours le cas ? Pour quelles élections peut-on recourir au vote étectronique ? Quelles sont les garanties de régularité de ce vote ? Les élections concernées par le vote électronique

est possible de recourir au vote électronique pour deux élections visées dans le décret du 5 décembre 2016 :

• les **délégués du personnel** ;

· les représentants du personnel au comité d'entreprise.

Sachez qu'il est d'ailleurs possible de combiner vote électronique et vote sous enveloppe, à condition que l'acte qui autorise le recours au vote électronique n'exclue pas cette possibilité

Les modalités du vote électronique
La mise en place du vote électronique est soumise à quelques formalités préalables. Ce recours doit être prévu dans un accord de groupe ou un accord d'entreprise (2).
Désormais, à défaut d'accord collectif, l'employeur peut décider unilatéralement de recourir au vote électronique (2). C'est la nouveauté inscrite dans ce décret d'application de la loi

Sachez aussi que le protocole d'accord préélectoral, qui doit être négocié entre l'employeur et les organisations syndicales représentatives, doit mentionner l'accord collectif ou la

Quel est le contenu du protocole d'accord préélectoral ?

décision de l'employeur de recourir au vote électronique

Lors de la négociation de ce protocole, il faudra tenir compte des contraintes techniques posées par ce vote particulier. En effet, comme tout dispositif électronique, des garanties doivent être prises pour assurer la **régularité du vote** et sa **confidentialité**.

A ce titre, le code du travail établit un cahier des charges à respecter

• des fichiers distincts dans l'urne : il doit y avoir deux fichiers qui doivent être bien séparés. Le premier « Fichier des électeurs » doit permettre l'authentification des électeurs. Le second fichier nommé « Contenu de l'urne électronique » détaillera lui les clés de chiffrement et de déchiffrement, ainsi que le contenu de l'urne. Ce fichier n'est consultable que par les personnes en charge de la gestion et de la maintenance du système de vote (3).

le système de vote doit pouvoir être **scellé** pendant toute la durée du scrutin (4)

· une **expertise indépendante** doit être réalisée **avant le scrutin**(5) par un **expert indépendant** mandaté par l'employeur.

• une assistance technique doit être mise en place par l'employeur pour veiller au bon fonctionnement du système et intervenir en cas de besoin (6). Des tests doivent être effectués sur le matériel avant le déroulement du vote.

Les garanties prévues pour la régularité du vote Le vote électronique doit présenter certaines garanties indispensables à sa régulari • le respect du cahier des charges prévu par la loi.

Il est mentionné dans l'accord collectif ou la décision unilatérale de l'employeur de recourir au vote électronique

Par ailleurs, chaque salarié doit avoir accès à ce cahier des charges selon le décret du 5 décembre 2016 (2). Il peut être mis à leur disposition via l'intranet de l'entreprise ou consultable dans les locaux de l'entreprise.

L'expertise préalable par un expert indépendant.

Tout le système et le matériel de vote doit avoir été examiné par un expert rémunéré par l'employeur.

s'assure de l'existence de la décision unilatérale de l'employeur ou de l'accord collectif autorisant le recours au vote électronique.

Il doit s'assurer également des modalités garantissant la confidentialité et la sécurité du dispositif : l'existence des deux fichiers séparés concernant les électeurs et le contenu de l'urne, l'exclusivité de l'accès aux données électroniques par les gestionnaires du système, le caractère hermétique et scellé du matériel. Il rédigera un rapport sur ces points. Ce dernier doit être tenu à la disposition de la CNIL (7).

La déclaration à la CNIL.

Comme tout dispositif électronique et de stockage informatique de données, le vote électronique doit faire l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés (8).

A ce titre, la CNIL a fait une recommandation relative à la sécurité des systèmes de vote électronique.

Lire la recommandation de la CNIL

Les organisations syndicales représentatives de salariés doivent être informées de l'accomplissement de cette formalité déclarative auprès de la CNIL.

Les résultats du vote.

Si l'acte qui autorise le recours au vote électronique n'a pas exclu le vote sous enveloppe à bulletin secret, sachez qu'il ne sera pas possible d'obtenir des premiers résultats pendant le scrutin. En effet, le récent décret précise bien qu'aucun résultat partiel n'est accessible pendant le déroulement du vote. L'ouverture des enveloppes ne pourra être faite qu'après la clôture du vote électronique (9).

Pour aller plus loin dans vos démarches



e me présente : Denis JACOPINI. Je suis Expert en Informatique indépendant et assermenté spécialisé en Cybercriminalité et en Protection des Données à Caractère Personnel répondant à l'ensemble des critères relatifs aux Experts recommandés par la CNIL en mesure de vous accompagner pour vos élections par voie électronique pendant toutes les phases suivantes :

AVANT ET HORS EXPERTISE (FACULTATIF)

- Analyse technique des réponses des éditeurs à la suite de votre appel d'offres ou consultation ;
- Présentation des résultats de l'analyse technique des réponses des éditeurs au bureau de vote
- Accompagnement pendant toute la phase de rencontre avec l'éditeur jusqu'à la recette du logiciel de vote électronique ;

- Expertise préalable aux élections conforme à la délibération n° 2010-371 du 21 octobre 2010 de la CNIL portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique avec la possibilité d'ajouter dans notre expertise technique des contrôles relatifs à d'autres obligations, normes ou référentiels propres à votre activité professionnelle réglementée (Droit, Santé, Fiscal, Social…) ;

Avis technique préalable à l'ouverture des scrutins ;
Participation à la cérémonie de scellement des urnes (sur place en fonction de nos disponibilités sinon disponibilité à distance et possibilité de présence d'un tiers de confiance) ;

Suivi de vos élections à distance de manière aléatoire

- Participation au dépouillement des urnes (sur place en fonction de nos disponibilités sinon disponibilité à distance et possibilité de présence d'un tiers de confiance) ;

Avis technique à la suite de la clôture des scrutins ;

Vérification de la suppression des données à caractère personnel au terme des délais de recours.

Afin de répondre au mieux à vos besoins et vous établir une proposition chiffrée.

vous pouvez me communiquer le protocole électoral par e-mail à vote-electronique [ar-obas-e]lenetexpert.fr ou à défaut, me communiquer quelques informations relatives à vos élections en remplissant un formulaire d'information accessible à partir du lien suivant :

https://www.lenetexpert.fr/questions-avant-expertise-solution-de-vote-par-voie-electronique

(1) Décret n°2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise

(2) Articles R2314-8 et R2324-4 du Code du travail (3) Article R2324-6 du Code du travail

(4) Article R2324-7 du Code du travail

(5) Article R2324-8 du Code du travail

(6) Article R2324-9 du Code du travail

(7) Articles R2314-12 et R2324-8 du Code du travail

(8) Articles R2314-14 et R2324-10 du Code du travail

(9) Articles R2314-19 et R2324-15 du Code du travail

A Lire aussi :

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

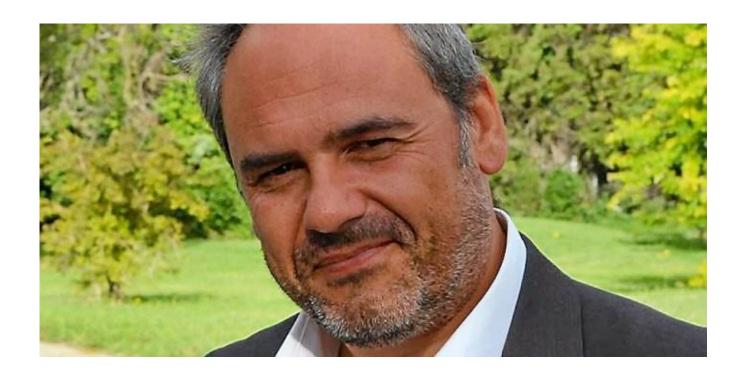
3 points à retenir pour vos élections par Vote électronique Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

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 solution 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

Article original de Juritravail : Vote électronique : les 3 points à retenir !