Quelques préconisations sur la géolocalisation des personnes vulnérables | Denis JACOPINI

Quelques préconisations sur la géolocalisation des personnes vulnérables

Les particuliers, les établissements hospitaliers ou médico-sociaux peuvent aujourd'hui utiliser des appareils de suivi électroniques (bracelets, boîtiers, etc.) pour assurer la sécurité de personnes âgées, malades, ou de jeunes enfants.

Afin de respecter les droits de ces personnes, la CNIL a fait les recommandations suivantes :
• Recueillir si possible l'accord de la personne concernée ou celui de ses représentants légaux ou de ses proches. La personne doit au minimum être informée ;
• Les appareils doivent pouvoir être désactivés et réactivés par les personnes concernées, lorsque celles-ci sont en possession de leurs moyens ;
• La procédure de gestion des alertes doit être précisée dans un protocole ;
• Privilégier les systèmes qui laissent à la personne concernée l'initiative de la demande d'assistance, plutôt qu'une surveillance permanente ;
• S'appuyer sur une évaluation personnalisée des risques et non sur une logique de prévention collective. La géolocalisation ne doit pas être utilisée systématiquement pour toutes les personnes âgées ou tous les enfants accueillis dans un établissement.

Avant de faire le choix d'utiliser ce type d'appareil, une évaluation collégiale et pluridisciplinaire doit donc être menée par l'équipe qui prend en charge la personne vulnérable.

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

S o u r c e :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=9DCFCE66E3DC38F485EA18F87E1E023F?name=G%C3%A9olocalisation+des+personnes+vuln%C3%A9rables+%3A+les+pr%C3%A9conisations+de+la+CNIL&id=299

Usurpation d’identité, propos diffamatoires, concurrence déloyale, atteintes à votre E-réputation – Nous pouvons vous aider | Denis JACOPINI

Usurpation d’identité, propos diffamatoires, #concurrence déloyale, atteintes à votre E-réputation – Nous pouvons vous aider

Victime de la cybercriminalité : Quelqu'un vous #insulte sur Internet (propos diffamatoires), se fait passer pour vous (usurpation d'identité sur Facebook, Twitter, viadeo, linkedin, instagram, par e-mail), ou diffuse certaines de vos informations confidentielles, vous pouvez rapidement devenir victime d'une atteinte à votre e-réputation.
Pour initier une action vers la personne malveillante en direction soit d'une arrangement à l'amiable ou d'une action judiciaire, vous devez constituer un dossier avec un maximum d'éléments prouvant la légitimité de votre action.
Denis JACOPINI, Expert Informatique assermenté et spécialisé en protection des données personnelles et en cybercriminalité a rassemblé dans ce document quelques actions qui devront être menées et est en mesure de vous conseiller et de vous accompagner dans vos démarches.

Nous pouvons classer les atteintes à la e-réputation en 3 grandes catégories :

a) Atteintes à la vie privée (par exemple en diffusant ou divulguant des informations personnelles ou confidentielles)
b) Dénigrements, injures, propos diffamatoires, citations hors contextes et médisances
c) Usurpation d'identité
Lors qu'un expert est contacté pour une mission sur un de ces sujets, un constat d'huissier peut éventuellement avoir été demandé, notamment pour constater les faits reprochés. Sans constat, l'expert devra se baser soit sur les informations ou documents que lui communiquera la victime (avec pour issue une vérification de l'exactitude ou de l'intégrité des informations) ou bien procédera à un constat des faits lors de sa mission.

Plusieurs types d'informations peuvent être soumises à l'expert :

Expertiser un e-mail, un post sur un forum, un réseau social ou bien des informations apparaissant sur des supports tels qu'un moteur de recherche, annuaire Internet ou bien un site Internet se fait d'abord en analysant le contexte, puis en réalisant quelques étapes au moyen d'outils spécifiques :

Expertise d'E-mails

En l'absence de procédés de signature électronique garantissant l'intégrité absolue d'un e-mail et de procédé de traçabilité pouvant garantir l'envoi et la distribution dans la boite destinataire d'un e-mail, et, étant quasiment systématiquement dans l'impossibilité de pouvoir expertiser le système informatique à la fois de l'expéditeur et du destinataire, l'expert est souvent bien démuni pour prouver l'absence de fraude dans un « change électronique.
Les premières informations à relever sont bien évidemment la « date de l'e-mail », « l'identité du ou des correspondants » mais aussi une information qui apporte une véracité supplémentaire au mail incriminé : « la continuité des échanges ». (**CAPTURES D'ECRAN DATEE, IMPRESSION DU MAIL**)
La deuxième information très importante est pour les connaisseurs, « l'entête de l'e-mail ». Les informations contenues dans la zone cachée de l'e-mails peuvent certes venir confirmer les informations précédemment relevées, mais également avoir des informations sur les serveurs source, destination et intermédiaires impliqués dans l'échange électronique. (**LA FONCTION D'AFFICHAGE DE L'ENTÊTE D'UN EMAIL FAIT PARTIE DE LA PLUPART DES LOGICIELS DE MESSAGERIE**)
La dernière information pouvant être fort utile consiste à rechercher des informations sur le propriétaire du nom de domaine du serveur à l'origine du message (voir procédure dans la rubrique relative aux expertises de sites internet).
Avec les éléments recueillis, l'expert pourra apporter des éléments permettant à l'avocat d'engager auprès de la personne à qui l'atteinte à la e-réputation est reprochée une demande de réparation à l'amiable ou par voie judiciaire.
Les éléments recueillis permettront, par voie judiciaire, de présenter une requête à un juge, laquelle permettra à l'expert d'obtenir d'autres éléments techniques relatives à l'échange.
Lire notre dossier au sujet des signatures électroniques
http://www.lenetexpert.fr/dossier-du-mois-juin-2014-lutilisation-juridique-documents-numeriques-lere-dematerialisation-outrance/

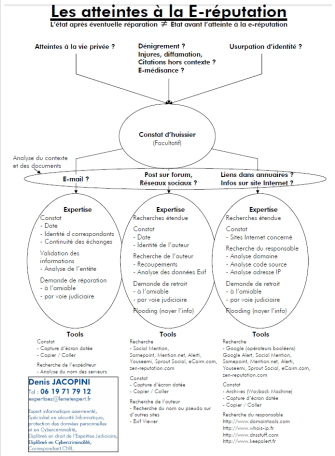
Expertise de post sur forum ou sur les réseaux sociaux ?

Les forums ou les réseaux sociaux peuvent être aussi les dépositaires malgré eux d'échanges ayant pour conséquence l'atteinte à la réputation d'une victime.
Les premières informations à relever sont bien évidemment la « date du message » et « l'identité de l'auteur ». (**CAPTURES D'ECRAN DATEE, CODE SOURCE, ECHANGES AVEC LE FOURNISSEUR DU SERVICE**)
D'autres éléments peuvent nous aider à identifier l'auteur physique d'un message par recoupement d'informations recueillies sur Internet ou dans d'autres sites d'échanges tels que des indices dans les propos ou des informations dans les images utilisées (**recherche sur Google, Social Mention, Samepoint, Mention.net, Alerti, Youseemi, Sprout Social, eCairn.com, zen-reputation.com…**).
Tout comme avec les éléments permettant d'identifier l'expéditeur d'un e-mail, l'expert pourra apporter des éléments permettant d'identifier l'auteur des faits permettant ainsi d'engager seul ou au travers d'un l'avocat, auprès de la personne à qui l'atteinte à la e-réputation est reprochée une demande de réparation à l'amiable ou par voie judiciaire.
Les éléments recueillis permettront, par voie judiciaire, de présenter une requête à un juge, laquelle permettra à l'expert d'obtenir d'autres éléments techniques relatives à l'échange.
Remarque :
En cas de difficulté de faire retirer l'information à l'origine de l'atteinte à la E-réputation, la technique du Flooding peut être utilisée. Elle consiste à noyer l'information par une profusion d'information au contenu cette fois maîtrisé et intelligemment choisi.

Expertise d'informations sur des annuaires ou de sites Internet

Lorsque des contenus portant atteinte à l'E-réputation se trouvent sur des sites Internet, la procédure consiste à identifier le responsable du contenu portant atteinte à la réputation de la victime. Le point d'entrée pour avoir des informations relatives au nom de domaine est principalement le bureau d'enregistrement pouvant nous renseigner sur les coordonnées des différents contacts.
Nous pouvons facilement nous trouver confrontés à plusieurs contacts :
• le contact qui a déposé le nom de domaine
• celui qui a réglé le nom de domaine
• celui qui a ouvert l'hébergement
• celui qui a réglé l'hébergement
• celui ou ceux qui ont mis en ligne le site internet
• celui qui a mis en ligne l'information incriminée
• et enfin l'auteur, et donc responsable, de l'information concernée
Ceci peut représenter autant de contacts pouvant être impliqués ou non dans notre expertise.
Le point d'entrée pour avoir des informations sur ces contacts est principalement le bureau d'enregistrement (Un bureau d'enregistrement (registrar en anglais) est une société ou une association gérant la réservation de noms de domaine Internet).
Nous pouvons avoir plus d'information sur les différents contacts relatifs à un nom de domaine (propriétaire, contact administratif, contact technique) en utilisant la fonction « whois » proposé par les bureaux d'enregistrement ou sur https://www.whois.net.
Voici quelques exemples de registres avec les domaines de premier niveau qu'ils maintiennent :
• VeriSign, Inc. : .com ; .net ; .name
• Public Interest Registry et Afilias : .org ;
• Afilias : .info ;
• CIRA : .ca ;
• DENIC : .de ;
• Neulevel : .biz ;
• AFNIC : .fr ;
• EURid : .eu ;
• Nominet : .uk
Pour pouvez facilement trouver les informations publiques relatives aux noms de domaines grâce aux sites Internet suivants :
• http://www.domaintools.com
• http://www.whois-ip.fr
• http://www.dnsstuff.com
• http://www.keepalert.fr
• http://whois.domaintools.com
Pour information
L'afnic met à notre disposition un formulaire nous permettant de lui demander de procéder à la levée d'anonymat d'un particulier (personne physique), titulaire d'un nom de domaine enregistré sous diffusion restreinte (le nom et les coordonnées du titulaire sont masqués et n'apparaissent pas dans l'annuaire Whois) et sous les extensions opérées par l'AFNIC.
https://www.afnic.fr/medias/documents/RESOUDRE_UN_LITIGE/afnic-formulaire-divulgation-donnees-perso-06-14.pdf
Il est clair que si un prestataire a mis en ligne à la demande de son client les propos concernés par la mission, il devra produire la preuve qu'il a agit à la demande d'un tiers et son identification.
Le code source peut également nous fournir des indications sur le type de logiciel utilisé pour développer le site Internet et le niveau technique du créateur du site Internet.

Enfin, il peut être parfois utile de retrouver le contenu d'un site internet à une date antérieure.
Pour cela, il existe un outil représentant les archives d'Internet : **Internet Archive.**
L'Internet Archive, ou IA est un organisme à but non lucratif consacré à l'archivage du Web et situé dans le Presidio de San Francisco, en Californie. Le projet sert aussi de bibliothèque numérique. Ces archives électroniques sont constituées de clichés instantanés (copie de pages prises à différents moments) d'Internet, de logiciels, de films, de livres et d'enregistrements audio.
Site Internet de Internet Archive : https://archive.org
Accès direct au **WayBackMachine** : http://archive.org/web



Autres délits pour lesquels les Experts Informatiques peuvent être contactés :

Le Cybersquatting
Le Cybersquatting, aussi appelé cybersquattage, est une pratique consistant à enregistrer un nom de domaine correspondant à une marque, avec l'intention de le revendre ensuite à l'ayant droit, d'altérer sa visibilité ou de profiter de sa notoriété.
Parmi les buts recherchés par les cybersquatteurs nous avons :
• Spéculation au nom de domaine
Le cybersquatteur achète un nom de domaine très percutant ou gênant en vue de faire du chantage auprès de l'ayant-droit, pour que celui-ci achète le nom de domaine au cybersquatteur à un tarif élevé.
• Page parking
Le nom de domaine contient des liens sponsorisés qui rapportent des revenus au cybersquatteur. Idéalement, les liens sponsorisés sont en rapport avec le thème de la marque parasitée.
• Boutique d'e-commerce
Le nom de domaine pointe vers une boutique vendant généralement des produits similaires au commerçant dont la marque est cybersquattée. Il s'agit souvent de produits de contrefaçon, le cybersquatteur reprenant les repères visuels de la boutique officielle.
Cette pratique s'apparente au phishing car il s'agit de piéger le consommateur en usurpant l'identité d'un tiers.
• Nuisance à la marque
Le site fait passer un message péjoratif ou dénigrant à l'égard de la marque.
Les actions possibles contre le cybersquattage :
En France, le cybersquattage n'est pas passible de sanctions pénales, seules des actions civiles sont envisageables.
Les actions les plus courantes concernent en atteinte à une marque (propriété intellectuelle) ou encore parasitisme. Des actions peuvent respectivement être portées devant le tribunal de grande instance (TGI) ou le tribunal de commerce dans le cas de conflit entre commerçants.
Procédure extrajudiciaire :
Les organismes qui gèrent les noms de domaines (registres) et les parties prenantes (titulaire du nom de domaine et ayant-droit sur la marque) étant souvent de nationalités multiples d'une part, et les procédures judiciaires étant longues et couteuses d'autre part, l'ICANN a mis au point une procédure extrajudiciaire permettant au plaignant de recourir devant le registre pour récupérer un nom de domaine : la procédure UDRP.
Cette procédure est payante et la décision est à la discrétion du registre. Une décision judiciaire ultérieure prévaudra cependant sur la décision UDRP.

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 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 améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.metronews.fr/info/paris-on-refuse-de-lui-louer-un-appartement-a-cause-de-son-profil-internet/modC!uUpMqgL3WsBnc/

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 500, et la plus dangereuse d'entre elles, « Install Pokemongo » a atteint entre 10.000 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 œufs chanceux – jusqu'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 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.

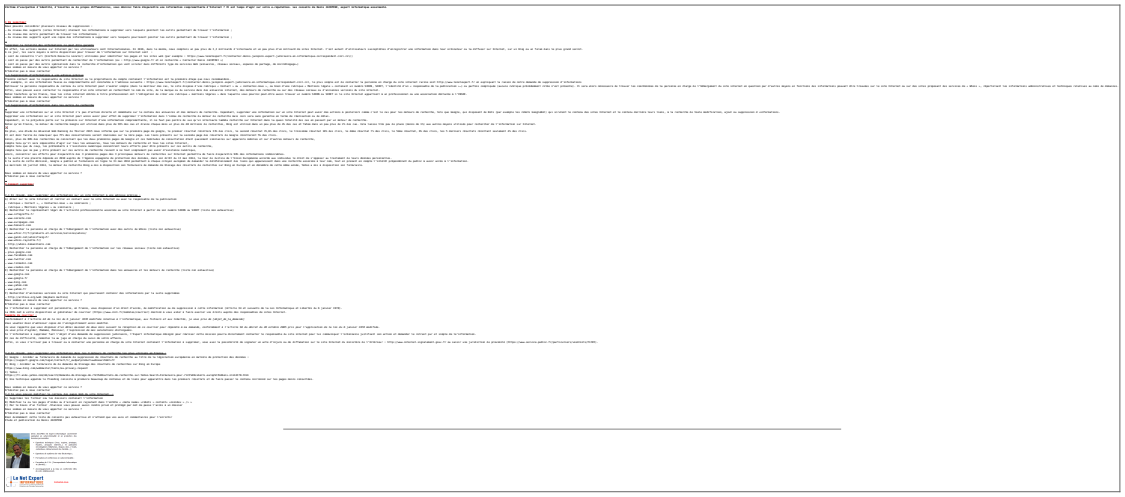
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

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

Suppression d'un contenu web : comment procéder ?



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-fonction-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 :
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

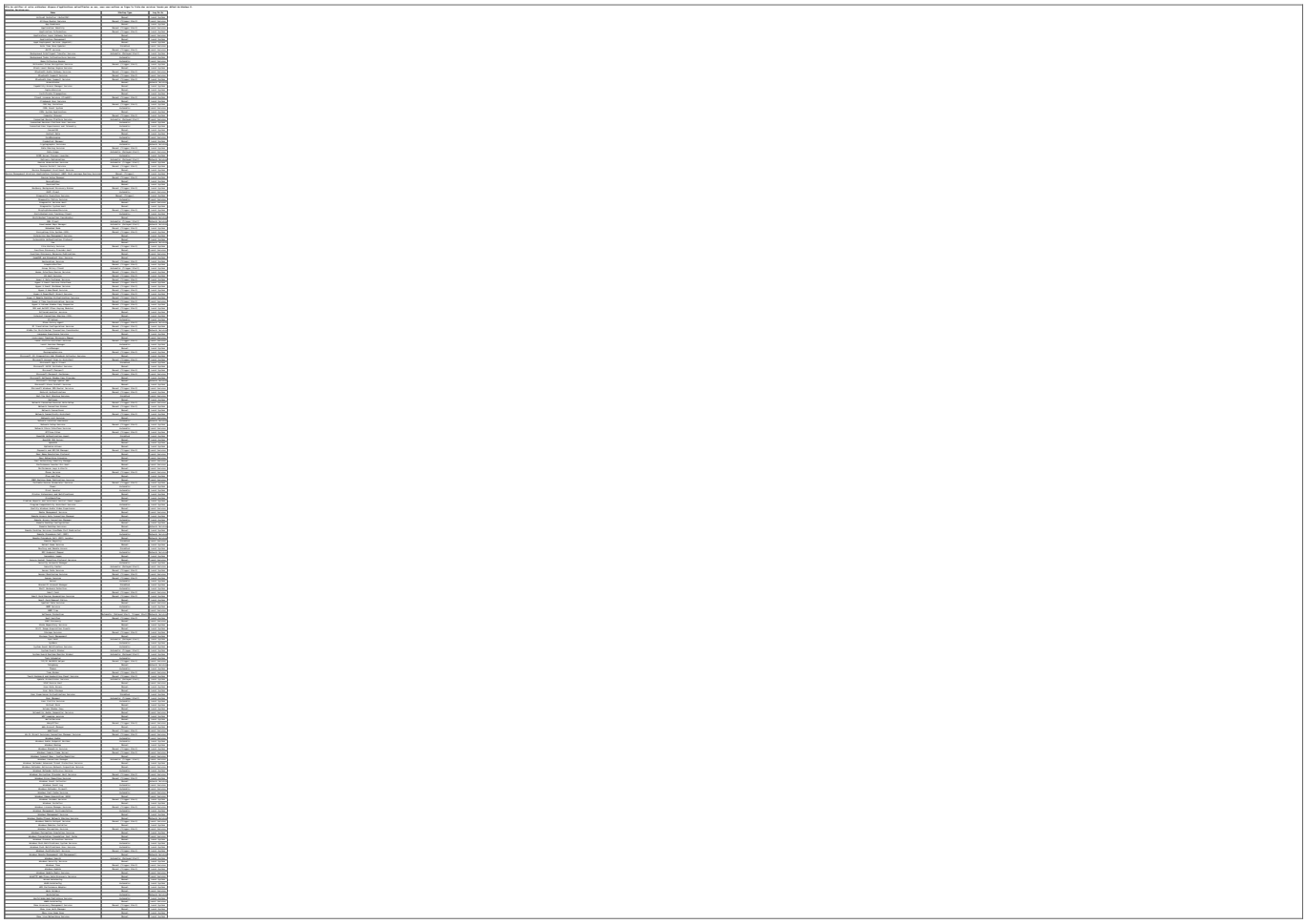
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source :
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+%3F&id=256

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

Windows 10 : Identifier les applications malveillantes à partir 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 ?

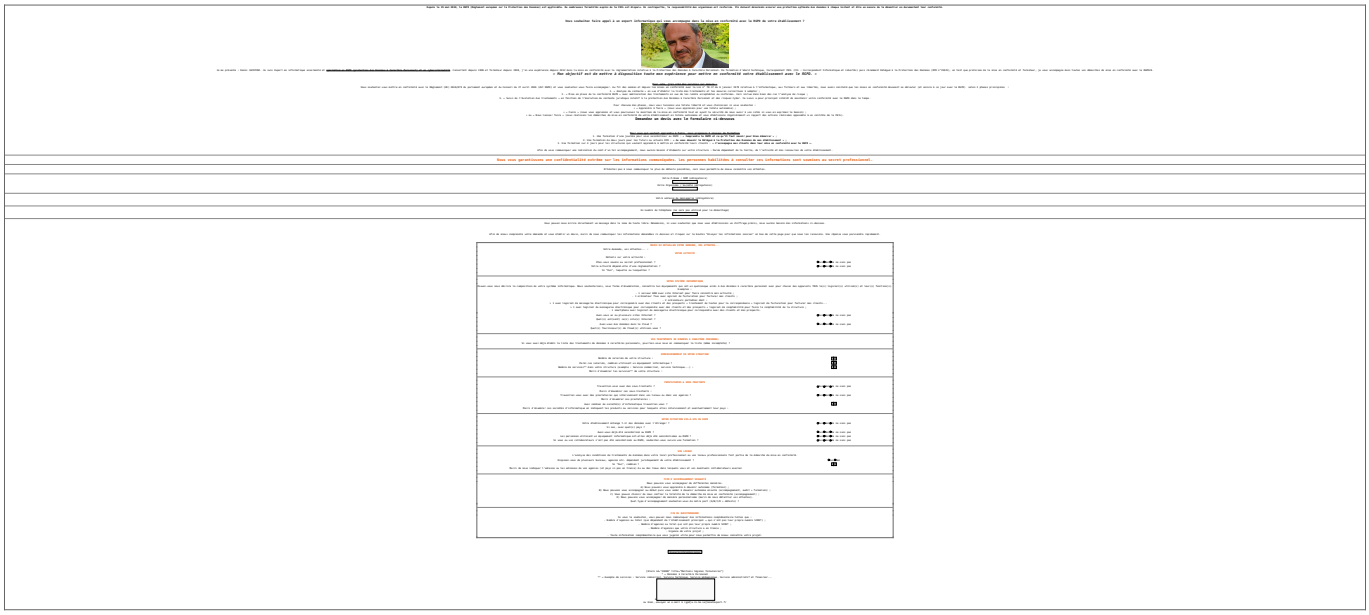
Attaques informatiques : comment les repérer ?

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

Source : https://www.winhelponline.com/blog/windows-10-default-services-configuration

Demande de Devis pour un audit RGPD

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



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

Numéro de formateur
93 84 03041 84
Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Datadock
Organisme validé
et référencé

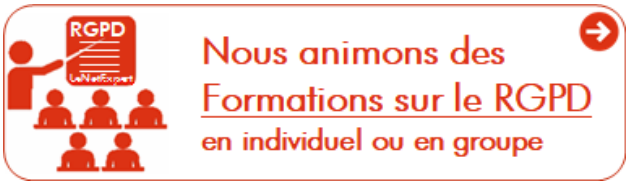
Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

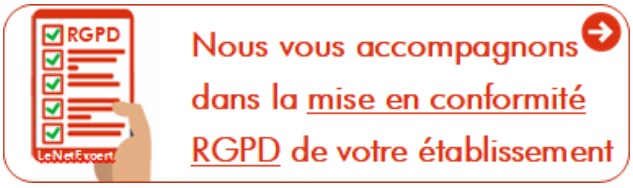
Contactez-nous

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

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

3. Impact de l’attaque

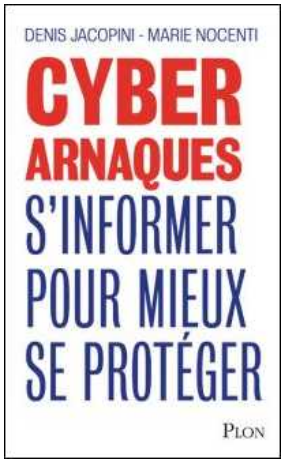
• Intégrité
• Authenticité
• Disponibilité
• Confidentialité

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 2010 (Symantec) 13,8 Milions de victimes de la 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

Comment naviguer incognito sur Facebook avec les règles de confidentialité actuelles

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 1er 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 de 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.

Statuts
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 ? ».

Groupes / fan pages
Attention à ce que vous postez sur les Pages et dans les groupes de discussion. Les paramètres de confidentialité que nous avons évoqués ne concernent que votre profil. Les messages postés 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.

Après 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