

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

<input type="checkbox"/>	Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques
--------------------------	---

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

1. CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE

Entrer un mot de passe permettant de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable est un geste quotidien de sécurité.

Choisir un mot de passe difficile à décoder par une tierce personne ou par du piratage informatique est ainsi un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

Comment bien choisir son mot de passe ?

Définissez des mots de passe composés d'au moins 12 caractères

- mélangeant majuscules, minuscules, chiffres et caractères spéciaux
- n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance
- ne formant pas de mots figurant dans le dictionnaire

Comment faire en pratique ?

Pour cela 2 méthodes simples :

- la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CDn€7am
- la méthode des premières lettres : « Un tiens vaut mieux que deux tu l'auras » : ltvnQ2tl'A

Quelques recommandations supplémentaires

- n'utilisez pas le même mot de passe pour tout, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle
- méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe

2. ENTRETIENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES

En mettant à jour régulièrement les logiciels de vos appareils numériques

Dans chaque système d'exploitation (Android, MacOS, Linux, Windows,...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité.

Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations longtemps encore après leur découverte ou même leur correction. Il donc **nécessaire de procéder aux mises à jour régulières des logiciels.**

Comment faire ?

- configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible
- ou téléchargez les correctifs de sécurité disponibles en utilisant pour cela exclusivement les sites Internet officiels des éditeurs
- en effectuant couramment des sauvegardes

3. Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur

Comment faire ?

- utilisez des supports externes tels qu'un disque dur externe, un CD ou un DVD enregistrable pour enregistrer et sauvegarder vos données.

4. PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité et de conduire des activités d'espionnage industriel.

Une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet.

Voici quelques recommandations générales :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données, par exemple avec des partenaires commerciaux
- ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux
- utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle...) et une adresse destinée aux autres services en ligne (forums, jeux concours...)

5. PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

L'emploi d'ordinateurs portables, d'ordiphones (*smartphones*) ou de tablettes facilite le quotidien lors des déplacements professionnels. Pourtant, voyager avec ces appareils nomades peut mettre en péril des informations sensibles sur l'entreprise ou vous travaillez.

Précautions à prendre avant de partir en mission

- utilisez le matériel dédié à la mission prêté par votre entreprise (ordinateur, clefs USB, téléphone)
- sauvegardez aussi vos données sur un support amovible pour les retrouver en cas de perte
- si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur
- apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport

Pendant la mission

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel)
- si vous êtes contraint de vous séparer de votre téléphone, retirez la carte SIM et la batterie
- en cas d'inspection ou de saisie de votre matériel par des autorités étrangères, informez votre organisation
- n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation

6. SÉCURISEZ VOTRE WI-FI

Si l'utilisation du Wi-Fi est une pratique attractive, elle permet, lorsque le point d'accès n'est pas sécurisé, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes.

C'est pour cette raison que l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise.

Le Wi-Fi, solution pratique et peu coûteuse, peut cependant être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre box. Pour ce faire, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès.

Quelques recommandations générales :

- modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet
- vérifiez que votre box dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes)
- modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents (cf. Choisissez des mots de passe robustes)
- ne divulguez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement
- activez et configurez les fonctions pare-feu / routeur.
- désactivez le Wi-Fi de votre borne d'accès lorsqu'il n'est pas utilisé

7. SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

Monsieur Paul, directeur commercial, rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Monsieur Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone,...) personnels et professionnels.

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
- ne stockez pas de données professionnelles sur vos équipements communicants personnels

En savoir plus sur le AVEC ou BYOD :

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle est cependant très problématique pour la sécurité des données personnelles et professionnelles (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur). De la même façon, il faut éviter de connecter des supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

8. SOYEZ AUSSI PRUDENT AVEC VOTRE ORDIPHONE (SMARTPHONE) OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR

Alexandre possède un ordiphone. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, les éditeurs peuvent accéder à tous les SMS présents sur son téléphone.

Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires d'hygiène informatique :

- n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer
- en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement
- effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre ordinateur ou ordiphone

9. SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES

Suite à la réception d'un courriel semblant provenir d'un de ses amis, Madame Michel a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Madame Michel le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,...).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoyez habituellement vos contacts
- si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
- n'ouvrez pas et ne retapez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

10. SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

Lorsque vous réalisez des achats en ligne, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur.

Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs)
- assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple

Si possible, lors d'un achat en ligne, privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.

De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire.

11. TÉLÉCHARGEZ LES PROGRAMMES, LOGICIELS SUR LES SITES OFFICIELS DES ÉDITEURS

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

- C'est la raison pour laquelle il est vivement recommandé de télécharger vos programmes sur les sites officiels des éditeurs
- Enfin, désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir, afin de vérifier qu'ils ne sont pas infectés par un quelconque virus ou spyware.



Réagissez à cet article

Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage

✕	Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage
---	---

Vous êtes victime d'une arnaque ou d'un piratage sur Internet ? Votre témoignage nous permettra peut-être de vous aider.

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice.

Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes) ;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante : ...)
- Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).

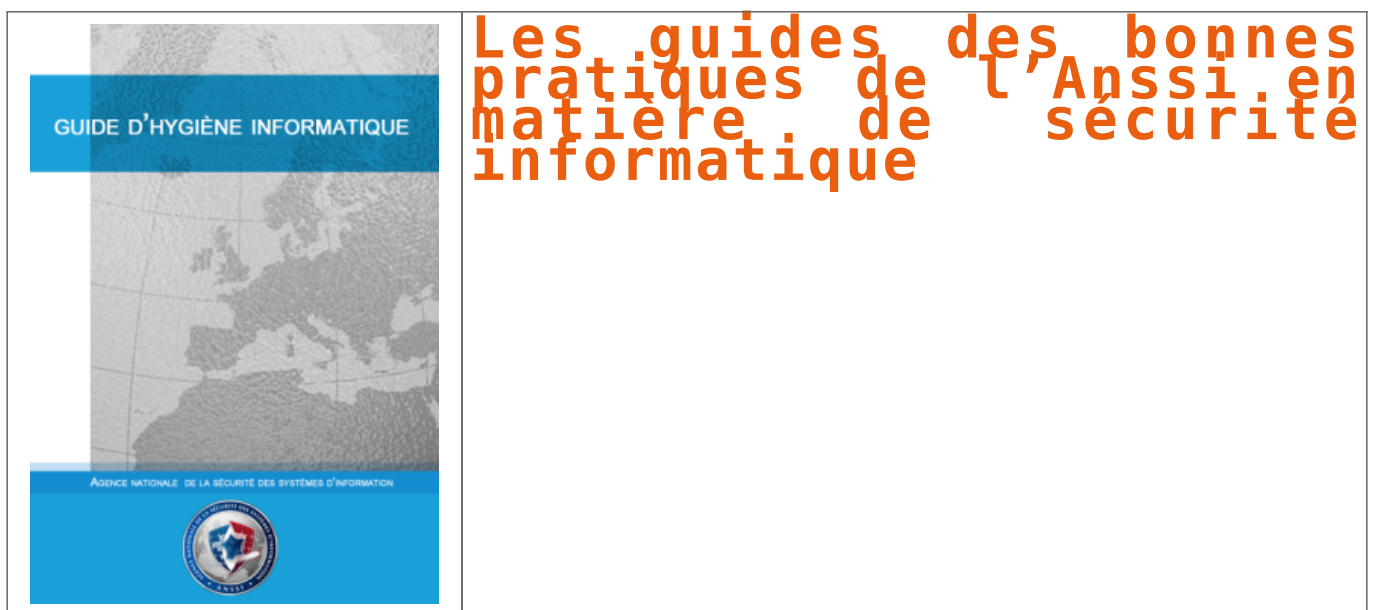
Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



Réagissez à cet article

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

Expert Informatique 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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

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



Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Sur une publication, vous pouvez être identifié :

- **directement** (exemple : nom, prénom, etc.)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :

- **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.

En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

1. Signaler la publication à effacer

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.

Twitter : Signaler la divulgation d'informations privées

Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram

Facebook : Utiliser le lien » Signaler «

situé à côté de la publication, de la photo ou du commentaire

Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image

LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité

Youtube : Réclamer une atteinte à la vie privée

Dailymotion : Sous chaque vidéo figure un bouton » Signaler cette vidéo «

en cliquant dessus, vous aurez à remplir un formulaire.

2. Si le réseau social ne fait pas partie de cette liste

- Rendez-vous vous en bas de la page d'accueil du réseau social ;
- Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
- Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
- Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

Quelle réponse attendre du réseau social ?

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.

En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.

En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

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 : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*

5 règles d'or pour les utilisateurs des réseaux sociaux | Denis JACOPINI

 5 règles d'or pour les utilisateurs des réseaux sociaux

Le nombre total d'individus dans le monde est de 7,4 milliards. Fin 2015, Facebook a atteint les 1,59 millions d'utilisateurs. Avec une augmentation annuelle de 17%, le géant des réseaux sociaux est tout simplement trop important pour être ignoré. Ceci étant dit, c'est aussi vrai pour beaucoup d'autres réseaux sociaux.

Les 310 millions d'utilisateurs actifs par mois sur Twitter postent 347 222 fois en moyenne. Plusieurs d'entre eux tweetent plus d'une centaine de fois par jour, et nombreux sont ceux à tweeter une fois par jour. Plus de 40 millions de photos ont été partagées sur Instagram depuis son lancement, et plus de 80 millions de photos y sont publiées chaque jour.

Ceci représente une énorme quantité de données : certaines importantes, d'autres intéressantes ou encore inutiles. Les réseaux sociaux, avec leurs propres tendances et leurs propres lois, fonctionnent comme une extension du monde réel, qui a un énorme impact sur nos vies hors-ligne. Dans cet article, nous vous dévoilons quelques règles simples que chaque utilisateur de réseaux sociaux devrait garder en tête.

1. N'alimentez pas les trolls

Les trolls sur Internet sont des provocateurs qui se joignent à des conversations dans le but d'agacer les autres utilisateurs pour le « fun ». On peut trouver des trolls n'importe où : sur les forums, les chats, et autres plateformes de communication en ligne. Les forums des nouveaux médias sont connus pour la participation élevée de trolls. D'ailleurs, il y en a plein sur les réseaux sociaux.

Comment devez-vous parler aux trolls ? D'aucune façon ! Ignorez-les. Plusieurs personnes se font prendre au piège et engagent alors des débats houleux en essayant d'expliquer leur point de vue et passent une grande partie de leur temps et de leur énergie en vain. Quelqu'un a toujours tort sur Internet. Ne perdez pas votre temps et votre énergie pour des trolls.

[View image on Twitter](#)

Si vous n'avez pas de chance, vous pourriez tomber sur un troll en quête de revanche, en spammant votre e-mail, ou même en essayant de ruiner votre vie. Par exemple, un couple américain a perdu du temps, de l'argent, leur travail et même détruit leur mariage en étant les victimes de cyberintimidation, se traduisant par des canulars téléphoniques (swatting) et autres formes d'harcèlement hors-ligne.

2. Ne postez pas ou ne partagez pas de contenu illégal

Les Emirats Arabes Unis et la Nouvelle Zélande disposent de lois qui punissent sévèrement les trolls et la cyberintimidation avec des sanctions allant de 35 000\$ à la prison.

Toutefois, vous pouvez écoper d'une amende ou même être confronté à des conséquences bien plus graves pour avoir posté, partagé du contenu ou toutes autres actions relatives dans bon nombre de pays. Par exemple, deux hommes ont été condamnés à quatre ans de prison après avoir créé une page Facebook qui encourageait une révolte. Un homme au Bangladesh a été envoyé en prison pour avoir plaisanté sur son souhait de voir le premier ministre mort. Par conséquent, mieux vaut être au courant des lois de chaque pays et de s'en souvenir au moment de publier ou partager sur Facebook ou Twitter.

3. Ne partagez pas des arnaques

Les fraudeurs piègent souvent les victimes avec des histoires choquantes telles que des bébés mourants, des chiots qui se noient, ou d'anciens combattants. De tels articles font le tour des réseaux sociaux en criant à l'aide. En réalité, ils sont déployés dans le but de voler de l'argent, de diffuser des malwares et des méthodes d'hameçonnage.

[View image on Twitter](#)



Follow

[CityNews Toronto](#)

[@CityNews](#)

Consumers warned about online scam involving free puppies <http://ow.ly/YAgcm>

3:14 AM – 22 Feb 2016

*

*

2020 Retweets

*

99 likes

De tels articles génèrent beaucoup de partages, mais la majorité d'entre eux sont des arnaques. De vrais appels au secours proviennent en général de votre famille, amis, et amis de vos amis. Ayez toujours en tête que ce sont les pages officielles des entreprises qui mettent en place ce type d'aide et non pas des individus inconnus.

C'est la raison pour laquelle il vaut mieux rester vigilant et vérifier chaque article avant de cliquer sur « aimer » ou « partager ». Pas envie de tous les contrôler un par un ? Ne prenez donc pas de risques pour vous et vos amis.

4. Pensez aux réactions des lecteurs

Vous avez probablement des collègues, des supérieurs et des clients parmi vos connections Facebook ou Instagram. Lorsque vous postulez pour un emploi, il est très probable par exemple que les ressources humaines jettent un coup d'œil à votre profil sur les réseaux sociaux. Prenez en compte ce que vous voulez leur montrer, et plus important encore, ce que vous ne voulez pas.

Vous devez aussi réfléchir prudemment à ce que vous publiez sur les pages d'autres utilisateurs et sur des comptes publics tels que des entreprises ou des universités. Par exemple, en 2013, un homme originaire de Pennsylvanie a été renvoyé pour avoir « complimenté » une étudiante en ligne. Son commentaire n'avait rien de sexuel ou d'inapproprié, mais de toute évidence la mère de la jeune fille n'avait pas apprécié. Un an auparavant, une professeure de Moses Lake, Washington, avait été virée parce qu'une femme qu'elle n'avait jamais rencontrée s'était plainte d'un de ces articles. Il s'agit de quelques exemples parmi tant d'autres qui prouvent qu'il vaut mieux garder ses photos personnelles et ses articles pour des amis sûrs.

Si vous avez besoin d'aide pour dissimuler vos articles privés des regards indiscrets, vous pouvez retrouver nos articles sur les paramètres de confidentialité de Facebook, Twitter, Instagram, LinkedIn, et Tumblr.

[View image on Twitter](#)

Follow

[Kaspersky Lab](#)

[@kaspersky](#)

Check your Facebook privacy settings NOW <https://kas.pr/3Wpw>

8:13 PM – 26 Oct 2015

*

*

2525 Retweets

*

1313 likes

5. Ne dévoilez pas vos données publiques

De nombreux réseaux sociaux proposent d'« enregistrer » la géolocalisation lorsque vous prenez une photo, postez du contenu ou montrez les lieux que vous avez visités. Si vous êtes intéressé par un événement, le réseau social peut en informer vos amis au cas où ils voudraient vous accompagner.

Par défaut, tout le monde peut accéder à vos données, et les cybercriminels ont mille et une méthodes de s'en servir, ça peut aller de s'introduire dans votre maison jusqu'à voler votre identité numérique. C'est la raison pour laquelle nous vous recommandons vivement de dissimuler ce type des données à des personnes inconnues, à l'aide des paramètres de confidentialité de Facebook.

C'est aussi une bonne occasion pour que vous n'ajoutiez pas n'importe qui aveuglément : les gens envoient des demandes d'amis qui peuvent s'avérer être des bots, des trolls ou même des hackers. Même si Facebook vous informe que vous avez des dizaines d'amis en commun, n'acceptez pas de demandes si vous n'êtes pas certain que ce soit des connaissances sûres.

Article original de John Snow

Reagissez à cet article

[Reagissez à cet article](#)

Original de l'article mis en page : 5 règles d'or pour les utilisateurs des réseaux sociaux | Nous utilisons les mots pour sauver le monde | Le blog officiel de Kaspersky Lab en français.

Comment naviguer incognito sur Facebook avec les règles de confidentialité actuelles | Denis JACOPINI

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



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 vous
- 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>

Facebook offre un outil de diagnostic pour se protéger des piratages de comptes |

Denis JACOPINI



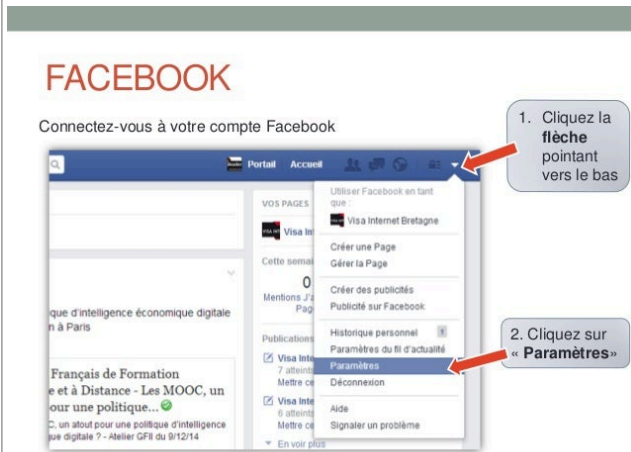
Facebook offre un outil de diagnostic pour se protéger des piratages de comptes

Les membres de F18facebook peuvent désormais contrôler la sécurité de leur compte. Voici l'outil proposé par le réseau social pour prévenir le piratage des données personnelles.

Facebook n'est pas réputé pour la transparence de ses paramètres de confidentialité et de protection des données personnelles. A tel point qu'à de nombreuses reprises, les membres du réseau social se sont retrouvés perdus dans les options de partage leurs informations personnelles, mettant en danger la sécurité de leur compte Facebook. L'outil que vient de dévoiler Facebook va aider les utilisateurs à s'y retrouver. De manière simple et centralisée, Facebook permet à chacun de visualiser les réglages actifs sur son compte : niveau de confidentialité des informations partagées, applications connectées au compte, partage de localisation géographique, secret des messages échangés etc...

Le diagnostic de la sécurité des comptes se poursuit ensuite par le passage en revue des paramètres de protection : certaines applications inutilisées sont-elles encore actives, les alertes de connexion au compte sont-elles signalées par email, et l'utilisation du mot de passe du compte est-elle conforme aux usages? Avec cet outil, Facebook montre qu'il prend très au sérieux les menaces de piratage de compte de plus en plus pressantes, et invite ses membres à procéder à la vérification de leur compte Facebook dans les meilleurs délais.

A ce jour, le réglage des paramètres de sécurité dans Facebook se fait dans le menu suivant :



Vous arriverez ensuite sur une liste de paramètres à modifier. Il faudra cliquer sur « Sécurité »



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.commentcamarche.net/news/5866867-piratage-de-compte-facebook-offre-un-outil-de-diagnostic>

A quoi ressemble une situation de cyber-harcèlement ?

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



A quoi ressemble une situation de cyber-harcèlement ?

Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

A quoi ressemble une situation de cyber-harcèlement ?

- Happy slapping : lynchage en groupe puis publication de la vidéo sur un site
- Propagation de rumeurs par téléphone, sur internet.
- Création d'un groupe, d'une page ou d'un faux profil à l'encontre de la personne.
- Publication de photographies sexuellement explicites ou humiliante
- Messages menaçants, insulte via messagerie privée
- Commande de biens/services pour la victime en utilisant ses données personnelles

[lire la suite]

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 : Réagir en cas de harcèlement en ligne | CNIL

Harcèlement en ligne : Qui sont les cyber-harceleurs ?

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



Harcèlement en ligne : Qui sont les cyber-harceleurs ?

Selon un rapport européen, près de 10 % de la population européenne a subi ou subira un harcèlement*. Voici quelques conseils si vous êtes victime de ces violences sur internet et les médias sociaux.

Qui sont les cyber-harceleurs ?

Un internaute peut être harcelé pour son appartenance à une religion, sa couleur de peau, ses opinions politiques, son comportement, ses choix de vie ... Le harceleur peut revêtir l'aspect d'un « troll » (inconnu, anonyme) mais également faire partie de l'entourage de la victime (simple connaissance, ex-conjoint, camarade de classe, collègue, voisin, famille ...)...[lire la suite]



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 : Réagir en cas de harcèlement en ligne | CNIL

Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ?

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



Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ?

Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ? L'idée n'est pas nouvelle, mais elle a officiellement été reprise par Gavin Newsom, le nouveau gouverneur de la Californie. « Les consommateurs devraient avoir le droit de partager la richesse créée à partir de leurs données », a fait valoir l' élu démocrate, mardi 12 février, lors d'un discours devant les parlementaires locaux.

M. Newsom propose de créer un « *dividende sur les données* ». Les contours de la future loi restent à définir, tout comme son calendrier. Mais le gouverneur promet « *quelque chose d'audacieux* ». Son projet pourrait se heurter à l'opposition des grands groupes Internet, qui disposent toujours d'importants appuis politiques à Sacramento, la capitale de la Californie. Le puissant lobby Internet Association se dit d'ailleurs déjà sur ses gardes...[lire la suite]

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.



**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)

Réagissez à cet article

Source : *Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ?*