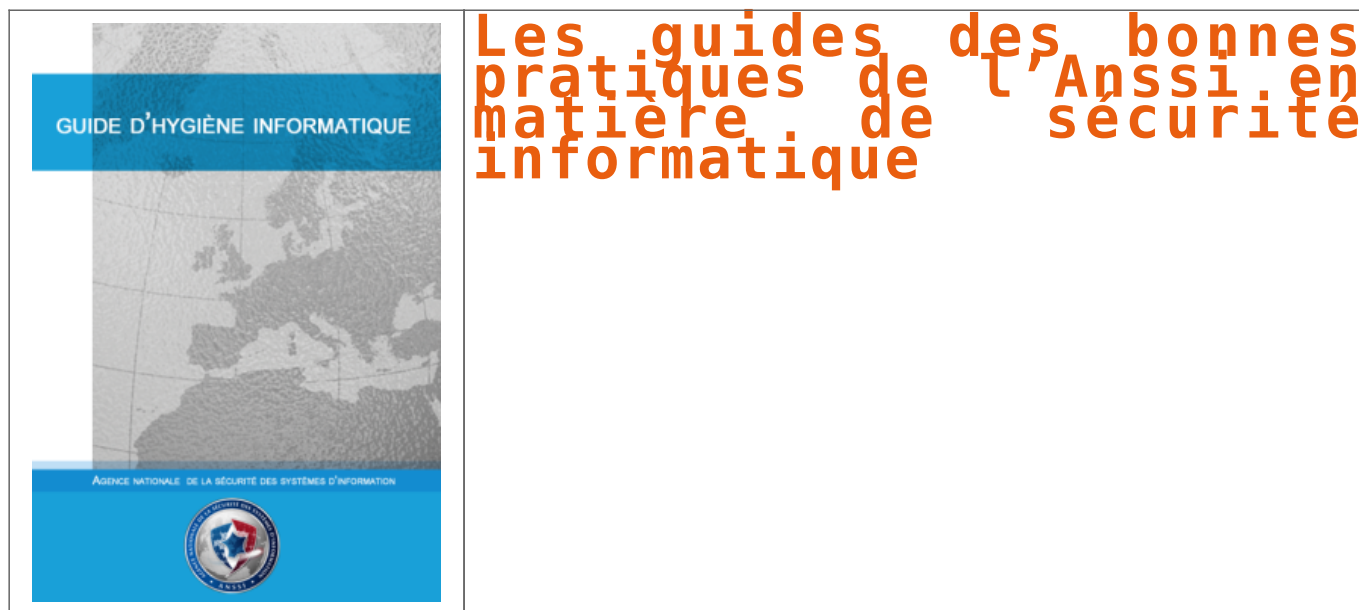


# Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



**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

 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p><b>LE NET EXPERT</b> EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>fr</i></p>	 <p><b>LE NET EXPERT</b> MISES EN CONFORMITE</p>	 <p><b>SPY DETECTION</b> Services de détection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
 <p><b>Denis JACOPINI</b> vous informe</p>	<p><b>Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL</b></p>				

**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.

[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 : *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

---



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					
 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p><b>LE NET EXPERT</b> EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p><b>LE NET EXPERT</b> MISES EN CONFORMITE</p>	 <p><b>SPY DETECTION</b> Services de détection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
		<p>Comment naviguer incognito sur Facebook avec les règles de confidentialité actuelles</p>			

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



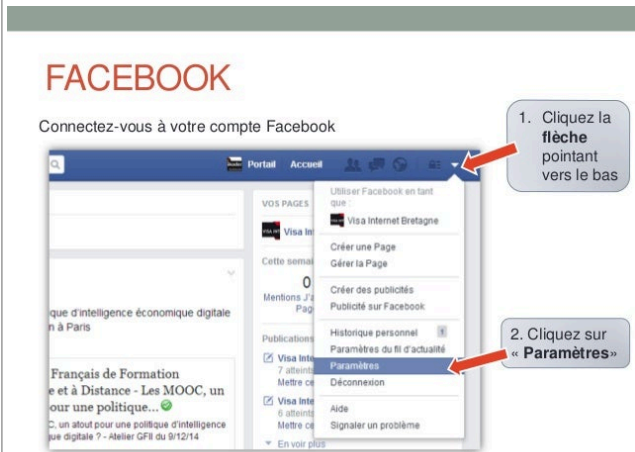
Facebook offre un outil de diagnostic pour se protéger des piratages de comptes

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>

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

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

 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p><b>LE NET EXPERT</b> EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p><b>LE NET EXPERT</b> RGPD CYBER MISES EN CONFORMITE</p>	 <p><b>LE NET EXPERT</b> SPY DETECTION Services de detection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
---	---	--	---	--	--



**Denis JACOPINI**  
vous informe

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

Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.

Les 3 axes vers lesquels votre structure devra progresser seront :

- Technique, par une amélioration des mesures de sécurité en place ;
- Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;
- Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

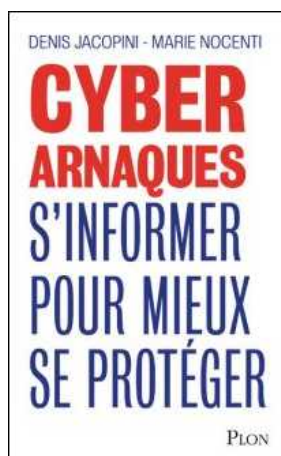
Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

[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](http://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 Millions de victimes de la Cybercriminalité 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](http://Fnac.fr)

---

[https://youtu.be/usg12zkRD9I?list=UUoHqj\\_HKcbzRuvIPdu3FktA](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](http://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](https://www.fnac.fr)

---

**Attention ! Voici ce que les  
cyberdélinquants vous**

# réservent... | Denis JACOPINI

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

 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p>EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <b>LE NET EXPERT</b> fr</p>	 <p><b>RGPD CYBER</b> <b>LE NET EXPERT</b> MISES EN CONFORMITE</p>	 <p><b>SPY DETECTION</b> Services de détection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
<input type="checkbox"/> <b>Attention ! Voici ce que les cyberdélinquants vous réservent</b>					

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

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

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

#### **CHANTAGE A LA VIDEO**

Cette escroquerie consiste pour le cybercriminel à :

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

#### **ARNAQUE AUX FAUX SENTIMENTS**

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

#### **ACHAT /VENTE :**

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

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

#### **SPOILIATION DE COMPTE MAIL OU DE RESEAUX SOCIAUX :**

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

#### **USURPATION D'IDENTITE :**

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

#### **DETOURNEMENT DE TRANSFERT :**

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

#### **FRAUDE SUR SIMBOX :**

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

#### **FRAUDE SUR COMPTE / BANCAIRE :**

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

#### **FRAUDE INFORMATIQUE :**

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

[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 ?

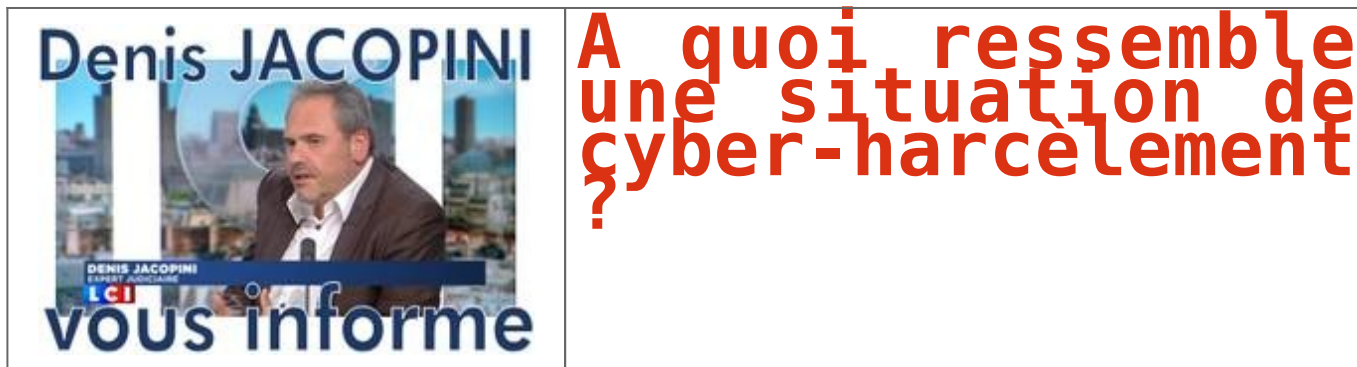
[block id="24760" title="Pied de page BAS"]

Source

<http://cybercrime.interieur.gouv.ci/?q=article/cybercriminalit%C3%A9-attention-voici-ce-que-les-cyber%C3%A9linquants-vous-r%C3%A9servent%E2%80%A6>

# 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]

[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 : 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					
 <b>LE NET EXPERT</b> AUDITS & EXPERTISES	 <b>LE NET EXPERT</b> EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES	 <b>LE NET EXPERT</b> MISES EN CONFORMITE	 <b>SPY DETECTION</b> Services de détection de logiciels espions	 <b>LE NET EXPERT</b> FORMATIONS	 <b>LE NET EXPERT</b> ARNAQUES & PIRATAGES
 <b>Denis JACOPINI</b> vous informe	<b>Harcèlement en ligne : Qui sont les cyber-harceleurs ?</b>				

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]



[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 : 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					
 <p><b>LE NET EXPERT</b> AUDITS &amp; EXPERTISES</p>	 <p><b>LE NET EXPERT</b> EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p><b>LE NET EXPERT</b> RGPD CYBER MISES EN CONFORMITE</p>	 <p><b>LE NET EXPERT</b> SPY DETECTION Services de detection de logiciels espions</p>	 <p><b>LE NET EXPERT</b> FORMATIONS</p>	 <p><b>LE NET EXPERT</b> ARNAQUES &amp; PIRATAGES</p>
 <p><b>Denis JACOPINI</b> vous informe</p>	<p>Et si Google, Facebook ou Amazon payaient les internautes pour utiliser leurs données personnelles ?</p>				

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 ?

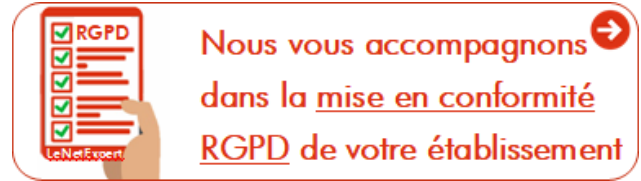
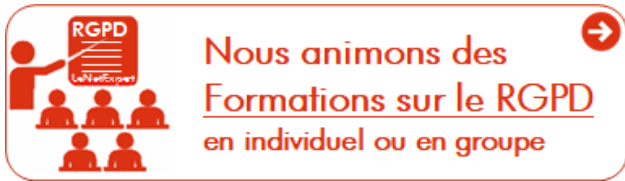
Contactez-nous

---

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 \(Délégués à la Protection des Données\)](#)

---

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

---

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