

25% des collégiens ont déjà été victimes de cyber-violences

<input type="checkbox"/>	25% des collégiens ont déjà été victimes de cyber-violences
--------------------------	--

Selon la Depp, 94 % des collégiens « se sentent bien » dans leur établissement. Mais pour autant, le sentiment d'insécurité demeure, ainsi que les cyberviolences.

Les **cyber-violences** concerne tous les collégiens. Selon les chiffres de la Depp sur les **violences** par **Internet** et par téléphone, 25 % des **collégiens** déclarent avoir connu « au moins une atteinte » via les nouvelles technologies.

En 2017, 11 % des **adolescents** ont déclaré avoir été l'objet d'insultes ou d'humiliations, et 18 % ont été l'objet, sur les **réseaux sociaux** ou via des **smartphones**, de rumeurs colportées, de vidéos humiliantes ou d'usurpations d'identité. Dans le détail, 9 % des **collégiens** ont déjà été l'objet de rumeurs par Internet, 8 % ont reçu des photos ou vidéos humiliantes (10 % de filles contre 8 % de garçons), et 6 % ont vu leur identité numérique usurpée.

Pour 7 % des **collégiens**, le nombre d'atteintes déclaré (au moins trois différentes) « peut s'apparenter à du **cyber-harcèlement** », explique l'étude. Selon la Depp, le cyber-harcèlement est « davantage subi par les filles (8 % contre 6 % pour les garçons) et les élèves de 3e » (8 %, contre 6 % en 6e)...[lire la suite]

Dernière enquête nationale de la Depp (direction de l'évaluation, de la prospective et de la performance)

LE NET EXPERT

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX → MISE EN CONFORMITÉ)**
 - **ANALYSE DE VOTRE ACTIVITÉ**
 - **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
 - **IDENTIFICATION DES RISQUES**
 - **ANALYSE DE RISQUE (PIA / DPIA)**
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
 - **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
 - **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est 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).



Réagissez à cet article

Source : *Climat scolaire : 25% des collégiens ont déjà été victimes de cyber-violences* » VousNousIls

Parents et futurs parents : Anticiper les risques du harcèlement sur Internet

x	Parents et futurs parents : Anticiper les risques du harcèlement sur Internet
---	--

Si le harcèlement est bien connu, le cyberharcèlement l'est beaucoup moins ! Le cyberharcèlement est une forme de cybercriminalité qui se caractérise par l'utilisation de la technologie pour harceler ou menacer en ligne une personne ou une entreprise.

L'assaillant s'infiltré dans les e-mails, la messagerie instantanée, les chats, les comptes de réseaux sociaux et les comptes bancaires en ligne, etc. de ses victimes pour les faire chanter.

En d'autres termes, il s'agit de harcèlement, mais dans le cyberspace.

Attention toutefois à ne pas confondre cyberharcèlement et trolling. Si le trolling désigne la participation d'un groupe ou d'une personne isolée à un acte de harcèlement en ligne, il comporte généralement une note d'humour – alors que le cyberharcèlement affiche des intentions malveillantes.

Les différents types de cyberharcèlement

- Prendre ou publier de vraies ou fausses photos à caractère sexuel de la victime ou de ses proches ;
- Suivre à la trace le moindre mouvement des victimes à l'aide d'un dispositif GPS installé sur leur véhicule ;
 - Menacer la victime ou ses amis et sa famille par e-mail ;
- Mettre en ligne des informations personnelles telles que le nom, l'adresse, les numéros de sécurité sociale et de téléphone de la victime ;
- Pirater et enregistrer des e-mails, des SMS et des billets publiés sur les réseaux sociaux pour les utiliser dans le but de harceler ou de faire chanter la victime ;
- Pirater le compte de la victime sur les réseaux sociaux pour y publier des contenus et commentaires offensants ;
- Dévoiler des informations personnelles erronées dans le but de discréditer la victime sur son lieu de travail ;
- Utiliser le compte de réseau social ou l'e-mail de la victime pour harceler et contacter d'autres personnes ;
- Créer des sites Web malveillants, de faux profils sur les réseaux sociaux et des blogs bidon sur la victime...[lire la suite]

LE NET EXPERT

:

- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - AU RGPD
 - À LA FONCTION DE DPO
 - **MISE EN CONFORMITÉ RGPD / CNIL**
 - **ÉTAT DES LIEUX RGPD** de vos traitements)
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
 - **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
 - **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est 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).

Réagissez à cet article

Source : *Le cyberharcèlement augmente chaque année : comment s'en protéger ? – Global Security Mag Online*

Conseils pour protéger vos enfants du Cyberharcèlement

	Conseils pour protéger vos enfants du Cyberharcèlement
---	---

Le succès des nouvelles technologies auprès des jeunes mineurs implique de nouveaux défis pour les parents. Les protéger du cyberharcèlement en fait partie. Les attaques personnelles à travers les réseaux sociaux ou les applications de messagerie instantanée chez les jeunes se multiplient. Voici neuf conseils pour protéger vos enfants du cyberharcèlement.

Pour éviter que les mineurs ne soient victimes de ce genre d'agressions, il est important que les parents soient au courant des activités de leurs enfants sur internet. Comment ? En les alertant des dangers potentiels auxquels ils s'exposent et en leur montrant les bons usages des nouvelles technologies.

Rester ouverts à la discussion

Le dialogue parents/enfants doit être facilité. Cela passe par l'information, à commencer par leur expliquer les risques auxquels ils s'exposent en utilisant internet et les conséquences de leurs mauvaises actions. Aussi, les enfants ne doivent pas hésiter à partager leurs expériences en ligne avec leurs parents, leurs frères et sœurs ou d'autres adultes de confiance, notamment sur des sujets qu'ils ne maîtrisent pas encore bien, de par leur jeune âge. En tant que parents, n'hésitez pas à leur dire qu'ils peuvent vous parler de tout, surtout s'ils ont des doutes ou des craintes.

Mettre en place des règles

La mise en place de règles d'usage concernant Internet est également un moyen de protéger votre enfant du cyberharcèlement. Refuser des demandes d'amis, des offres ou des conseils envoyés par des inconnus ou provenant d'applications non officielles ou non vérifiées est la première des règles à faire appliquer. Le Centre pour l'éducation aux médias et à l'information (Clemi) a édité un guide pratique (« La Famille Tout-Ecran ») pour accompagner les parents et sensibiliser les enseignants sur les pratiques médiatiques des élèves. Le guide est téléchargeable ici.

Leur montrer comment réagir face au cyberharcèlement

En cas de cyberharcèlement ou d'autres problèmes liés à internet, l'enfant doit savoir que la première chose à faire est d'en parler à un adulte de confiance. Dites-lui aussi que les messages sont des preuves importantes et ne doivent donc pas être effacés si jamais le problème se transforme en délit et fait l'objet d'une plainte. Enfin l'enfant doit être averti qu'il ne doit pas non plus répondre au cyberharcèlement par le cyberharcèlement, dans un désir de vengeance.

Sécuriser leurs appareils

Les experts recommandent aux parents d'installer un système de contrôle parental sur tous les dispositifs électroniques ayant un accès à internet (ordinateurs et tablettes). La plupart des programmes de sécurité, comme les antivirus ou les pare-feux disposent d'une option « Contrôle Parental », un service qui permet aux adultes d'avoir la main sur l'utilisation d'internet par les mineurs et de bloquer certains contenus...[lire la suite]

LE NET EXPERT

:

- FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
 - MISE EN CONFORMITÉ RGPD / CNIL
 - ÉTAT DES LIEUX RGPD de vos traitements
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - RECHERCHE DE PREUVES (outils Gendarmerie/Police)
 - ORDINATEURS (Photos / E-mails / Fichiers)
 - TÉLÉPHONES (récupération de Photos / SMS)
 - SYSTÈMES NUMÉRIQUES
 - EXPERTISES & AUDITS (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - SÉCURITÉ INFORMATIQUE
 - SYSTÈMES DE VOTES ÉLECTRONIQUES

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est 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).

Réagissez à cet article

Source : *Cyberharcèlement – Des conseils pour protéger vos enfants*

Alerte : Hameçonnage (phishing) – Attention aux

courriels frauduleux sur la carte Vitale V3 avec le logo de Service-public.fr

	Alerte : Hameçonnage (phishing) – Attention aux courriels frauduleux sur la carte Vitale V3 avec le logo de Service-public.fr
---	--

Service-public.fr, le site officiel de l'administration française, vous met en garde contre l'envoi de courriels frauduleux se faisant passer pour Service-public.fr.

Le dernier cas signalé concerne un courriel les invitant à télécharger un formulaire pour obtenir, sous 24 heures, la nouvelle carte Vitale V3.

Ces courriels n'émanent pas de Service-public.fr.

Il s'agit vraisemblablement d'une manœuvre frauduleuse pour inciter les internautes à livrer leurs données personnelles.

N'y répondez pas et supprimez-les de votre messagerie électronique.

Si vous avez déjà communiqué vos données bancaires, prévenez votre banque pour faire opposition. Service-public.fr ne demande pas d'argent, n'en rembourse pas et ne cherche jamais à recueillir des coordonnées bancaires.

Illustration 1Crédits : © Dila



Rappel :

- Si vous recevez des messages non sollicités sur votre messagerie électronique, vous pouvez l'indiquer sur signal-spam .
 - Pour signaler des contenus ou des comportements illicites sur internet, connectez-vous au site internet-signalement.gouv.fr .
- ...[lire la suite]

LE NET EXPERT

:

- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
 - **MISE EN CONFORMITÉ RGPD / CNIL**
 - **ÉTAT DES LIEUX RGPD** de vos traitements)
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est 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).

Réagissez à cet article

Source : Hameçonnage (phishing) -Attention aux courriels frauduleux sur la carte Vitale V3 avec le logo de Service-public.fr | service-public.fr

7 conseils pour se protéger les enfants des cyberpédophiles



Les spécialistes de la cybercriminalité de la police judiciaire niçoise tirent la sonnette d'alarme. Trop d'enfants sont laissés seuls avec un ordinateur dans leur chambre, exposés au danger. Voici quelques conseils pour s'en prémunir.

1. Mettez le moins de photos personnelles possibles sur les réseaux sociaux, de vous, de votre famille ;
2. On ne divulgue pas le vrai nom de l'enfant, ou sa photo sur Internet ;
3. Il ne doit pas accepter de nouveaux contacts inconnus: ni par e-mail, ni sur les réseaux et autres applications sociales ;
4. Les parents doivent se tenir informés des risques ;
5. Sensibiliser les enfants lors d'un dialogue familial constructif ;
6. Ne jamais laisser un ordinateur dans une chambre d'enfant, seul, sans surveillance. « *Il doit se trouver dans la pièce principale, sans code d'accès.* » ;
7. Ne pas laisser les enfants opérer des achats seuls sur le Net.

L'Éducation nationale a publié une étude de 2014: 4,5% des collégiens disaient subir un cyber harcèlement, c'est-à-dire une violence verbale, physique ou psychologique répétée. Un élève sur cinq a déjà été victime de cyberviolence...[lire la suite]

LE NET EXPERT :

- **SENSIBILISATION / FORMATIONS :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, suivez nos formations ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

EXPERTISES TECHNIQUES : Dans le but de prouver un dysfonctionnement, de déposer ou vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense

;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

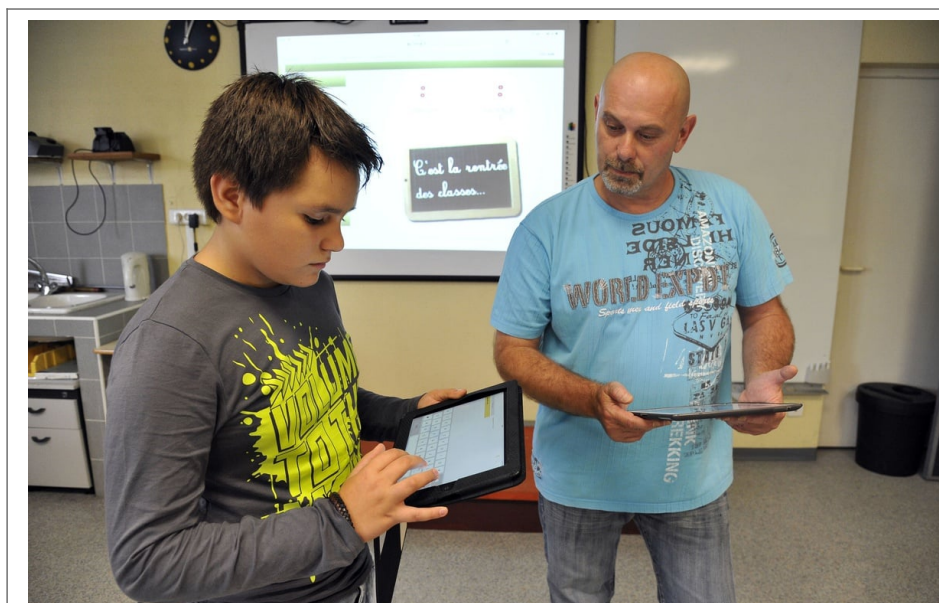
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : 7 conseils pour se protéger des cyber pédophiles –
Nice-Matin

Les données personnelles des écoliers français vont-elles échapper à Google?



Les données
personnelles
des écoliers
français
vont-elles
échapper à
Google?

Une «note interne» diffusée en mai ouvrait la possibilité aux entreprises du numérique de collecter des données scolaires. Les parents d'élèves avaient protesté auprès du ministre de l'Education. Jean-Michel Blanquer compte revoir la politique en la matière.

Pas d'école pour Google, Facebook, et autres géants du numérique, regroupés sous l'appellation Gafa. Jeudi, le porte-parole du gouvernement a indiqué que le ministre de l'Education Jean-Michel Blanquer comptait limiter l'accès de ces entreprises aux données scolaires des élèves.

Le ministre compte « revenir sur une circulaire [en fait, une lettre interne] signée deux semaines avant les présidentielles, qui ouvre très largement, peut-être trop largement l'accès des Gafa dans l'école », a expliqué Christophe Castaner.

Publicités ciblées

Rappel des faits : le 12 mai dernier, Matthieu Jeandron, délégué au numérique éducatif, adresse une lettre aux délégués académiques du numérique. Dans ce courrier, révélé par le Café pédagogique, il explique qu'il n'y a pas « de réserve générale sur l'usage des outils liés aux environnements professionnels chez les grands fournisseurs de service du web ». Un peu plus loin, il indique qu'il ne voit pas de « blocage juridique de principe à la connexion d'un annuaire avec l'un de ses services ».

En clair, cela signifie que Google, Facebook, et autres entreprises du numérique auraient pu collecter des listes d'élèves avec leurs noms, leurs classes, voire même leurs notes dans le cadre de travaux effectués en ligne. Ces données peuvent rapporter de l'argent : par exemple, on peut imaginer que Google, ayant connaissance des difficultés d'un élève, lui « propose » des publicités ciblées sur les cours en lign...[lire la suite]

NOTRE MÉTIER :

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
 - **MISE EN CONFORMITE RGPD / FORMATION DPO**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Les données personnelles des écoliers français vont-elles échapper à Google?*

Piratage massif d'Instagram : comment protéger ses données personnelles ?

✕	Piratage massif d'Instagram : comment protéger ses données personnelles ?
---	--

Le réseau social a reconnu avoir été victime d'un piratage massif qui pourrait avoir touché plusieurs millions d'utilisateurs. Voici des conseils pour éviter d'en faire les frais.

Vous avez peut-être un point commun avec Rihanna, Taylor Swift et Zinedine Zidane. Comme eux, vous faites peut-être partie des six millions de comptes Instagram dont les données personnelles ont récemment été dérobées par des hackers et mises en vente sur le DarkNet. Le pirate revendiquant le braquage a transmis un échantillon de 10.000 données au site spécialisé américain Ars Technica. Il réclame 10 dollars par compte piraté et propose des remises pour les achats de lots sur un site éphémère baptisé Doxagram...[lire la suite]

@LeoDuff0ff

Pourriez-vous expliquer comment activer la double authentification ? C'est pas forcément évident pour le grand-public

En réponse à **@LeoDuff0ff**

Hello, il suffit d'aller dans les paramètres de l'app, dans l'onglet « authentification a deux facteurs » puis d'ajouter un num de téléphone.



NOTRE MÉTIER :

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
 - **MISE EN CONFORMITE RGPD / FORMATION DPO**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Piratage massif d'Instagram : comment protéger ses données personnelles*

Les internautes obligés de révéler leur identité

✖	Les internautes obligés de révéler leur identité
---	---

Dès le 1er octobre, les réseaux sociaux et forums de discussion chinois devront s'assurer de l'identité des internautes pour leur permettre de poster des commentaires en ligne.

Les plateformes internet chinoises devront impérativement vérifier l'identité de leurs usagers avant de les laisser poster des commentaires en ligne, a indiqué Pékin, confirmant le tour de vis de la censure imposée par le régime communiste.

A partir du 1er octobre, tous les opérateurs de réseaux sociaux ou forums de discussion devront «s'assurer de la véritable identité» de leurs utilisateurs avant de leur permettre de poster des contenus et commentaires en ligne, selon un règlement publié vendredi par l'Administration chinoise de l'internet, un organisme gouvernemental...[lire la suite]

NOTRE MÉTIER :

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
 - **MISE EN CONFORMITE RGPD / FORMATION DPO**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *20 minutes – Les internautes obligés de révéler leur identité – Stories*

Découvrez tout ce que Google sait de vous

Découvrez tout ce que Google sait de vous

Le géant de la recherche vient d'inaugurer une nouvelle page, limpide et fonctionnelle, pour vous faciliter la vie.

La page Google Mon activité

La nouvelle page *Google Mon activité* est désormais le point de rendez-vous par excellence à l'heure de décortiquer tout ce que Google archive à votre sujet.

+ Cliquer ici pour accéder à la page Google Mon activité

Les yeux ébahis, vous découvrez minute par minute, heure par heure, jour par jour, **l'enregistrement détaillé de vos activités** au cœur des services Google.

Sont encodées vos activités et vos recherches sur: Android, Chrome, Google Maps, Recherche, Recherche d'images, Recherche de vidéos, Trajets Google Maps, YouTube.



Le 5 juillet, Google à l'affût a gardé la trace tangible de 358 activités sur notre compte Google, via le navigateur Chrome, la recherche, YouTube...PHOTO: CAPTURE D'ÉCRAN

Consulter l'historique de vos trajets

En marge de cet archivage obsessionnel, Google se fait fort d'**enregistrer vos déplacements** via la puce GPS de votre smartphone et/ou de votre tablette.

«Redécouvrez les lieux que vous avez visités et les itinéraires que vous avez empruntés dans l'historique de vos trajets», positive le moteur de recherche.

+ Cliquer ici pour consulter l'historique de vos trajets associé à votre compte Google



Les points rouges sur la carte montrent tous les endroits où Google vous a identifié grâce à la puce GPS de votre appareil mobile.PHOTO: CAPTURE D'ÉCRAN

La plate-forme pousse le vice jusqu'à présenter le classement des «lieux que vous fréquentez le plus souvent».

Effacer des données archivées

Vous souhaitez éclaircir, voire supprimer, cet archivage effréné de vos données personnelles?

Soulagement, la page *Google Mon activité* vous en laisse la possibilité, sans vous mettre des bâtons dans les roues.

À partir de la page *Google Mon activité*, cliquez sur *Supprimer des activités par*



La section Supprimer des activités par vous permettra d'effacer partiellement ou totalement les données personnelles archivées par Google.PHOTO: CAPTURE D'ÉCRAN

Limiter la collecte des données

Une fois le nettoyage de printemps bouclé, libre à vous de **limiter partiellement ou autant que possible la collecte des données personnelles**.

Prenez à nouveau la direction de la page *Google Mon activité*.

Cliquez sur *Commandes relatives à l'activité*



Via la section *Commandes relatives à l'activité*, vous pourrez brider l'espionnage de Google.PHOTO: CAPTURE D'ÉCRAN

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Voici comment consulter tout ce que Google sait de vous – Lavenir Mobile*

Une agence de voyages victime d'une incroyable attaque informatique dans le Gard

x	Une agence de voyages victime d'une incroyable attaque informatique dans le Gard
---	--

L'agence JCS, basée à Poulx (Gard), est spécialisée dans les séjours autour du thème de la taumachie. Entre le 15 et le 20 juin derniers, elle a subi un véritable déferlement de messages d'insultes et de menaces, via les réseaux sociaux, sur sa page Facebook et sur son site internet.

Par Hervé Sallafranque, France Bleu Gard Lozère



La capture d'écran du lancement de l'attaque informatique sur Facebook, réalisée par le responsable de l'agence – xxx

L'attaque des **anticorrida**, partie de France, s'est ensuite répandue à une très grande vitesse et l'agence a reçu des **messages venus du monde entier**. Son responsable a réussi à identifier la personne à l'origine de l'attaque : une dame basée dans les Alpes-Maritimes. Il a décidé de déposer plainte à la gendarmerie de Marguerittes ce samedi.

Des messages d'insultes venus des États-Unis, d'Australie, de Russie et du Brésil

« Le phénomène a été d'une ampleur énorme », explique le responsable de l'agence, Jean-Charles Roux. Parfois jusqu'à **1.200 messages d'insultes par jour** au plus fort de l'attaque, le week-end des 17 et 18 juin.

L'agence JCS est la seule en France à proposer ce genre de séjours. C'est sans doute pour cela qu'elle a été la cible des anticorrida, même si Jean-Charles Roux a du mal à comprendre un tel **déchaînement de haine**...[lire la suite]

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

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

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



Réagissez à cet article

Source : *Une agence de voyages victime d'une incroyable attaque informatique dans le Gard*