

Ce qu'il faut savoir sur les jouets connectés



Ce qu'il
faut savoir
sur les
jouets
connectés

S'ils s'invitent en nombre dans les magasins et sur les listes au Père Noël, les jouets connectés suscitent quelques craintes. Voici un petit guide pour s'y retrouver.

Tablettes, robots, peluches, jeux de société... Difficile de ne pas trouver une catégorie de jouets dont un ou plusieurs modèles n'ont pas une version connectée. De récents scandales montrent que le secteur n'est pas encore tout à fait au point pour que les plus jeunes puissent s'amuser en toute sécurité. En sept questions, Pixels fait le tour de cette tendance et des précautions à prendre pour que Noël ne tourne pas à une mise sur écoute.

[...]

Si l'on considère les jouets connectés au regard de la loi informatique et libertés, plusieurs questions s'avèrent importantes :

- le fabricant informe-t-il de façon claire les utilisateurs (en tout cas les parents) sur le fait que le jouet enregistre des données ? Recueille-t-il clairement leur consentement ? Le jouet ou l'appli invitent-ils bien les parents à réaliser cette étape importante au lieu de laisser l'enfant passer rapidement dessus ?
- est-il pertinent et nécessaire pour le fabricant de récupérer ces données ? Par exemple, est-il utile de demander l'adresse postale ou le nom complet d'un enfant pour faire fonctionner un jouet ? A quoi peuvent servir ces données au fabricant ?
- s'agissant de la sécurité de ces données : un mot de passe fort est-il requis ? Comment les données sont-elles chiffrées, où sont-elles stockées, et pendant combien de temps ? Qui peut y accéder ?

Les fabricants font-ils attention ?

Difficile de répondre puisque les fabricants ne sont mis en défaut que lorsqu'un problème de protection des données ou de vulnérabilité du jouet surgit, souvent bien après la commercialisation du produit.

En ce qui concerne la France, certains fabricants consultent en amont la Commission nationale informatique et libertés (CNIL) pour s'assurer d'être en conformité avec la loi. D'autres sont moins scrupuleux par souci d'économies. Ils utilisent par exemple des composants standards, parfois peu sécurisés, pour que le jouet ne soit pas trop cher.

Il y a aussi une limite technique. Si, après la mise sur le marché, un fabricant souhaite apporter une correction, il peut le faire sur une application ou un logiciel mais pas sur le jouet lui-même. Il faudrait rappeler le produit...[lire la suite]

LE NET EXPERT

:

- MISE EN CONFORMITÉ RGPD / CNIL
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- 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 (réécupération 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).

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 (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, conteneurs, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;



Contactez-nous

Réagissez à cet article

Source : Ce qu'il faut savoir sur les jouets connectés

7 règles simples pour

protéger votre entreprise contre les cyber-attaques



7 règles simples pour protéger votre entreprise contre tes cyber-attaques

Il ne se passe pas un jour sans que l'on entende parler de cyber-attaques, ce qui peut causer la détresse de certaines entreprises. Si de grandes entreprises telles que Merck ou Pizza Hut ne parviennent pas à empêcher des cyber-attaques, comment les autres peuvent-elles faire face ? Il ne se passe pas un jour sans que l'on entende parler de cyber-attaques, ce qui peut causer la détresse de certaines entreprises. Si de grandes entreprises telles que Merck ou Pizza Hut ne parviennent pas à empêcher des cyber-attaques, comment les autres peuvent-elles faire face ? Ceci est bien entendu la mauvaise attitude à adopter. Bien que les grandes entreprises aient plus de ressources à leur disposition, beaucoup de violations de données sont la conséquence de simples failles de cyber-sécurité peu coûteuses à résoudre. Vous trouverez ci-dessous 7 points que les entreprises devraient observer afin de limiter les risques de cyber-attaque.

1. Créez un mot de passe sûr
2. Ne réutilisez pas et ne partagez pas vos mots de passe
3. Sauvegardez vos fichiers importants
4. Méfiez-vous des attaques d'hameçonnage
5. Appliquez des "patches"
6. Protégez vos biens matériels

Organisez des formations de personnel

Les problématiques listées ci-dessus devraient être abordées durant les formations de sensibilisation du personnel mais on ne peut attendre de la part des employés à ce qu'ils s'en souviennent après une seule formation. En effet, les employés devraient être formé au cours de leur intégration mais devraient également bénéficier de rappels annuels ou de formations ponctuelles lors d'incidents de sécurité. Des formations de sensibilisation du personnel régulières permettront aux employés de se souvenir des règles à suivre.

LE NET EXPERT

- FORMATIONS / SENSIBILISATION :
 - CYBERCRIMINALITÉ
- PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
 - AUDIT RGPD ET CARTOGRAPHIE 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 (réécriture 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 assurément 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 DORTEFP (Numéro formateur n°93 84 03041 84).



Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des données à caractère personnel

Contactez-nous

Réagissez à cet article

Source : 7 règles simples pour protéger votre entreprise contre les cyber-attaques – IT Governance Blog FR

Google Detects Android Spyware That Spies On WhatsApp, Skype Calls



Google Detects Android Spyware That Spies On WhatsApp, Skype Calls

In an attempt to protect Android users from malware and shady apps, Google has been continuously working to detect and remove malicious apps from your devices using its newly launched Google Play Protect service.

Google Play Protect—a security feature that uses machine learning and app usage analysis to check devices for potentially harmful apps—recently helped Google researchers to identify a new deceptive family of Android spyware that was stealing a whole lot of information on users.

Discovered on targeted devices in African countries, Tizi is a fully-featured Android backdoor with rooting capabilities that installs spyware apps on victims' devices to steal sensitive data from popular social media apps like Facebook, Twitter, WhatsApp, Viber, Skype, LinkedIn, and Telegram.

« The Google Play Protect security team discovered this family in September 2017 when device scans found an app with rooting capabilities that exploited old vulnerabilities, » Google said in a [blog post](#). « The team used this app to find more applications in the Tizi family, the oldest of which is from October 2015. »

Most Tizi-infected apps are being advertised on social media websites and 3rd-party app stores, tricking users into installing them...[[lire la suite](#)]

LE NET EXPERT

• MISE EN CONFORMITÉ RGPD / CNIL

- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- 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 (réécriture 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).

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 ;

Source : Google Detects Android Spyware That Spies On WhatsApp, Skype Calls

70 % des attaques informatiques partent d'un problème humain. Il est urgent de sensibiliser votre personnel.

 <p>Denis JACOPINI VOUS INFORME LCI</p>	<p>70 % des attaques informatiques partent d'un problème humain. Il est urgent de sensibiliser votre personnel.</p>
--	--

En matière de cybersécurité, l'Europe a décidé de légiférer mais des disparités existent.

Explications avec Julie Gommes, experte en cybersécurité lors de la SME Assembly 2017 (Assemblée annuelle des PME organisée par la Commission européenne) à Tallinn (Estonie). Pour elle, la première faille de sécurité est entre la chaise et l'ordinateur.

[Article source]

LE NET EXPERT

- 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
 - 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 (réécriture 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).

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 ;

Uber : ces inquiétants témoignages de Français qui rapportent des piratages



Uber : ces
inquiétants
témoignages
de Français
qui
rapportent
des
piratages

La révélation fin novembre 2017 du hacking géant de Uber, qui s'est fait voler les données de 57 millions d'utilisateurs à travers le monde, a de quoi inquiéter les habitués de l'appli. Si l'entreprise assure que leurs coordonnées bancaires sont à l'abri, des Français témoignent avoir vu leur compte piraté pour des sommes parfois très conséquentes. Un séisme dans le joyeux monde des applis. La direction d'Uber a admis cette semaine que les données de 57 millions de ses utilisateurs avaient été piratées en octobre 2016. Après avoir donc dissimulé ce hacking d'ampleur pendant un an, l'entreprise s'est empressée d'assurer ce mardi 21 novembre que les coordonnées bancaires des usagers concernés n'avaient pas été dérobées. « Cela me paraît très bizarre qu'Uber ne stocke qu'une partie des données dans son Cloud Amazon, celui qui a été hacké par les pirates, sans les numéros de cartes bancaires », relève pour Marianne Julie Gommès, experte en cyber-sécurité. « Que les données bancaires ne soient pas du tout concernées me semble peu probable », abonde Claire Juiff, experte conseil en gestion de crise et formée au cyber-risque...[lire la suite]

LE NET EXPERT

- MISE EN CONFORMITÉ RGPD / CNIL
- AUDIT RGPD ET CARTOGRAPHIE de vos traitements
- 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 (réécupération 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).

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](#)

Réagissez à cet article

Source : *Uber : ces inquiétants témoignages de Français qui rapportent des piratages*

Une faille permet d'écouter 77 % des smartphones Android



Android
NOUGAT

Une faille
permet
d'écouter
77% des
smartphones
Android

Voilà qui risque d'augmenter la paranoïa de celles et ceux qui pensent qu'ils sont écoutés, via leur smartphone, à tout moment de la journée : les chercheurs de MWR Labs ont découvert une nouvelle faille majeure qui toucherait plus des trois quarts des smartphones Android en circulation. Une faille que Google a comblée, mais seulement dans Android 8.0 Oreo.

Le problème de cette nouvelle faille, c'est qu'elle est très facilement exploitable par un développeur mal intentionné : il ne s'agit pas d'une attaque à proprement parler mais d'un souci dans les autorisations données aux applications.

Le service Android MediaProjection au centre de cette nouvelle faille

Les chercheurs de MWR Labs ont découvert que Google, qui développe Android, a réalisé un changement majeur dans les autorisations d'un des services les plus anciens d'Android : MediaProjection. Ce service est en mesure d'enregistrer l'audio ainsi que l'écran du smartphone et est utilisé par certaines applications...[lire la suite]

LE NET EXPERT

:

- **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
- **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).

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** ;

Source : *Une faille permet d'écouter 77 % des smartphones Android*

Uber : Les données de 57 millions d'utilisateurs ont été piratées



Uber : Les données de 57 millions d'utilisateurs ont été piratées

Les noms ainsi que les adresses électroniques et numéros de téléphone ont été subtilisés, mais les données bancaires auraient été épargnées.

Le PDG d'Uber a révélé mardi que les données de 57 millions d'utilisateurs à travers le monde ont été piratées à la fin 2016. Parmi les 57 millions d'utilisateurs figurent 600 000 chauffeurs dont les noms et numéros de permis de conduire ont été récupérés. Les noms des utilisateurs ainsi que leurs adresses électroniques et numéros de téléphone mobile ont été subtilisés, a indiqué Dara Khosrowshahi, dans un communiqué.

Sur la base d'expertises externes, le patron affirme que l'historique des trajets, les numéros de cartes et de comptes bancaires, les numéros de Sécurité sociale et les dates de naissance des utilisateurs n'auraient en revanche pas été piratés.

M. Khosrowshahi, qui a été nommé à la tête d'Uber fin août, souligne qu'il a été informé « récemment » de cet incident. Il précise que deux personnes ne faisant pas partie de l'entreprise seraient responsables de ce piratage. « *L'incident n'a pas atteint les systèmes de l'entreprise ni son infrastructure* », ajoute-t-il par ailleurs.

Selon Bloomberg, Uber aurait payé 100 000 dollars les hackers afin qu'ils ne divulguent pas cet incident, une information qui n'a pas été confirmée par Uber...[lire la suite]

LE NET EXPERT

- 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
 - 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 (réécupération 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).

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** ;



Source : *Uber révèle que les données de 57 millions d'utilisateurs ont été piratées*

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



**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'infiltre 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 (réécriture 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).

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

Alerte : Une faille de sécurité sur des jouets connectés expose les enfants



Alerte :
Une
faille de
sécurité
sur des
jouets
connectés
expose
les
enfants

Une association de consommateurs britannique alerte sur une faille de sécurité liée à la connexion Bluetooth de certains jouets connectés et appelle à ce que ces derniers soient retirés de la vente.

Alors que certains ont déjà effectué les premiers achats de Noël, l'association britannique de consommateurs Why ? alerte les consommateurs sur le risque présenté par plusieurs jouets connectés : la peluche Furby Connect, le robot i-Que, le petit chien Toy-Fi Teddy et les animaux CloudPets. En cause : **une faille de sécurité** qui permet à toute personne ayant une connexion Bluetooth et ayant téléchargé l'application de ces jouets de se connecter à ces derniers, sans mot de passe ou étape de sécurité.

Une situation rendue possible par la **non-sécurisation de la connexion Bluetooth** de ces jouets, selon les tests réalisés par Why ? avec l'aide de Stiftung Warentest, l'équivalent allemand de l'UFC Que choisir...[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).

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** ;

Source : VIDÉO – Une faille de sécurité sur des jouets connectés expose les enfants

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 (réécupération 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