Grand-Quevilly : Le cyber-harcèlement fait une nouvelle victime

	Grand-Quevilly : Le cyber-harcèlement fait une nouvelle victime

Qu'est-ce qui a poussé Orlane, 13 ans, à se jeter de la fenêtre du 7 è étage de son immeuble du Grand-Quevilly?La collégienne, qui s'est suicidée le 10 mars dernier, a t-elle été harcelée par l'une de ses camarades? L'enquête se poursuit.

L'une des camarades d'Orlane a été placée en garde à vue mardi. La jeune fille est soupçonnée d'avoir volé les codes internet d'Orlane et de s'être emparée de photos de sa camarade seins nus. Aucune charge n'a été retenue contre elle à ce stade de l'enquête. Elle a été laissée libre à l'issue de son audition.
Cette affaire est une illustration du cyber-harcèlement. Le harcèlement a toujours existé mais le développement des réseaux sociaux amplifie considérablement les dégâts…[la vidéo]

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

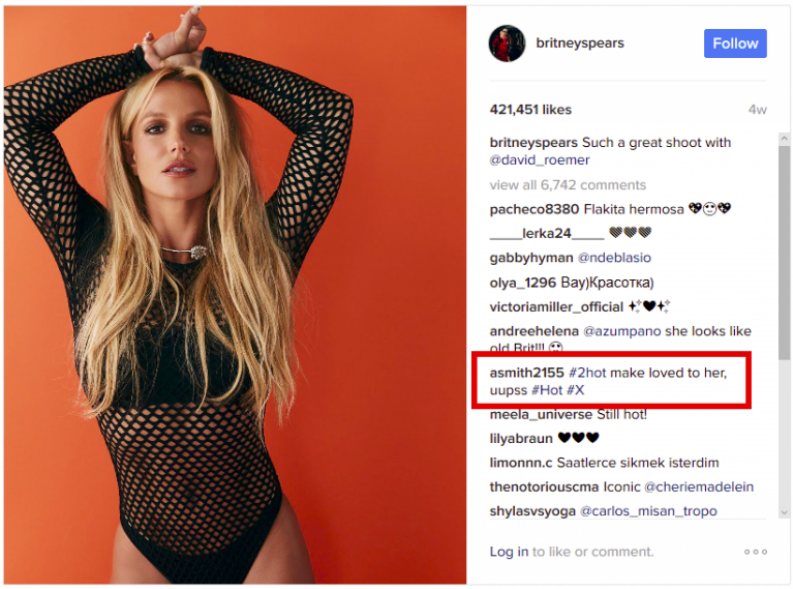
Source : *Suicide d'une collégienne au Grand-Quevilly : le cyber-harcèlement en cause – France 3 Normandie*

L'Instagram de Britney Spears, une planque pour les hackers russes

L'Instagram de Britney Spears utilisé par des hackers russes pour planquer l'adresse de leur serveur c&c

---

Un groupe de pirates russes a utilisé le compte officiel de Britney Spears sur Instagram pour cacher la direction de leurs serveurs de commandes et contrôle.



Vivons heureux, vivons cachés ! Cet adage s'applique parfaitement aux cybercriminels. Encore faut-il trouver la bonne planque ! Des chercheurs d'Eset, éditeur de sécurité, viennent de détecter une des cachettes d'un groupe de pirates russes, Turla. Ce dernier œuvre depuis 2007 et est à l'origine dun rootkit sophistiqué Uburos, créé en 2014. Spécialisé dans le cyberespionnage, Turla est soupçonné d'être d'origine russe ou pour le moins russophone. Ses techniques de piratage sont très élaborées, mais la découverte d'Eset est particulièrement originale.
Les chercheurs ont en effet déniché une backdoor dans les commentaires publiés sur le compte officiel de Britney Spears sur Instagram. Ce trojan donne des informations de localisation des serveurs de commandes et contrôle du groupe Turla.
…[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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle... ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *L'Instagram de Britney Spears, une planque pour les hackers russes*

La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

	La Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation

---

Face à la vague d'attentats qui frappe l'Europe, la Commission européenne discute actuellement de quelques changements dans les réglementations afin de permettre aux forces de Police d'accéder aux données des utilisateurs des services de Google et Facebook, sans autorisation préalable d'un Juge.

Les vagues d'attentat et la peur ambiante sont bien souvent l'occasion pour les gouvernements de voter des lois liberticides, et ce pourrait à nouveau être le cas dans toute l'Europe. La Commission européenne réfléchit actuellement à changer les réglementations afin de permettre aux forces de police d'aller piocher des informations dans les comptes des réseaux sociaux des utilisateurs, sans accord préalable de qui que ce soit.

Concrètement, le projet évoque même la possibilité pour les policiers d'origine étrangère de consulter les données privées des profils de ces réseaux sociaux, afin notamment d'enquêter sur un touriste ou une personne d'un autre pays de l'Union européenne. Exemple : vous partez en Italie pour quelques jours et vous faites arrêter par la police locale, ces derniers pourraient alors éplucher vos profils sociaux pour tenter d'obtenir plus d'informations sur vous, et ce, sans rien demander à la France.

Actuellement, trois projets de ce type ont été proposés et soumis à étude, l'un d'entre eux pouvant être adopté d'ici la fin de l'année 2018. Une des propositions évoque la possibilité de copier les données directement depuis le Cloud de la plateforme sociale afin d'en faire une sauvegarde et éviter la disparition des données en cas d'enquête…[lire la suite]

Commentaire de Denis JACOPINI

Entre Facebook qui analyse et espionne ses membres et les OPJ (Officiers de Police Judiciaire) qui peuvent consulter les données collectées par Facebook, il n'y a qu'un pas pour que ce même type de démarche soit aussi engagée auprès de Google pour qu'on nous mette des radars automatiques sur Internet qui nous flashent dès que quelqu'un en train picoler publie une photo.

Sans plaisanter, ces projets de loi consistent à permettre à des OPJ d'accéder aux zones privées de Facebook, car vous savez que lorsque vous publiez quelque chose sur Facebook, cet ajout peut être public (tout le monde peut le consulter et le voir) ou privé et il n'y a qu'un juge qui peut forcer Facebook à communiquer le contenu privé d'un compte. Ce projet ne changera rien pour ceux qui n'ont rien à se reprocher, et pas grand chose pour ceux qui ont quelques chose à se reprocher. Les OPJ pourrons disposer plus rapidement des contenus privés pour alimenter leurs enquêtes.

Il est fort probable à l'avenir qu'un autre réseau social soit utilisé par les malfrats l'histoire de faire courrier le chat…

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en RGPD (Protection des Données à Caractère Personnel).

- Audits RGPD
- Accompagnement à la mise en conformité RGPD
- Formation de Délégués à la Protection des Données
- Analyse de risques (ISO 27005)
- Expertises techniques et judiciaires ;
- Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle… ;
- Expertises de systèmes de vote électronique ;

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

Contactez-nous

ou suivez nous sur

Réagissez à cet article

Source : *Europe : la Police pourrait prochainement consulter vos données personnelles sur Facebook sans autorisation*

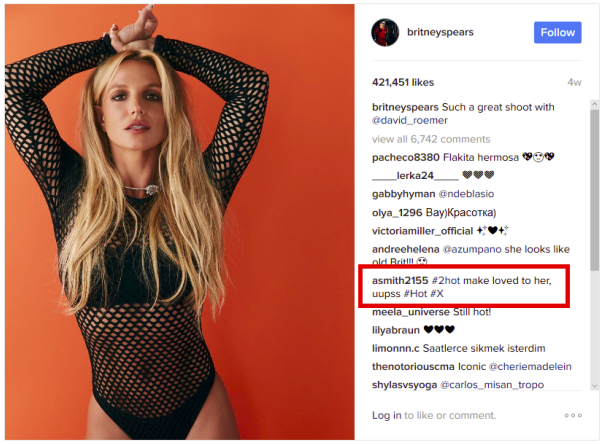
Instagram détourné pour espionner des membres de gouvernements

Instagram détourné pour espionner des membres de gouvernements

---

Turla, le groupe de cyberespionnage qui cible des représentants de gouvernements et des diplomates, lance une nouvelle attaque en se servant d'Instagram®. En février 2017, Forcepoint® a publié une liste de sites Internet récemment compromis.

Les cybercriminels utilisent **la technique d'attaque de trou d'eau**, qui vise à rediriger les victimes ayant cliqué sur un site compromis vers leurs serveurs C&C. Les chercheurs ESET® ont repéré **une extension de Firefox® qui utilise une URL bit.ly pour renvoyer vers les serveurs C&C. Le chemin de l'URL est diffusé via des commentaires d'une publication Instagram.** Dans l'échantillon analysé par ESET, l'un des commentaires s'affiche sur une photo du compte officiel de Britney Spears.



© https://www.instagram.com/p/BO8gU41A45g/

Pour obtenir l'URL bit.ly, l'extension scrute les commentaires de chaque photo et pour chaque commentaire en calcule un hash. Si la valeur de hash correspond à un code de déclenchement, l'extension exécute une opération pour convertir le commentaire en URL.

« L'utilisation par Turla des réseaux sociaux pour récupérer les adresses C&C ne facilite pas la tâche aux chercheurs en cybersécurité. Il est difficile de distinguer le trafic malveillant du trafic légitime sur les réseaux sociaux, » explique Jean-Ian Boutin, Senior Malware Researcher chez ESET. Par ailleurs, c**ette technique offre plus de souplesse aux pirates :** « comme l'information nécessaire pour obtenir l'URL du serveur C&C n'est autre qu'un commentaire sur les réseaux sociaux, **le cybercriminel a la possibilité de le modifier ou de l'effacer** à tout moment, » poursuit Jean-Ian Boutin.

Pour éviter d'être infecté par une attaque de trou d'eau de ce type, les chercheurs ESET recommandent de :

- mettre à jour les navigateurs et les plugins des navigateurs
- éviter de télécharger ou d'installer des extensions venant de sources non vérifiées
- utiliser une solution de sécurité (à jour) capable de détecter les sites Internet compromis

Seuls 17 clics ont été enregistrés sur ce lien en février lorsque le commentaire a été posté. Le nombre étant relativement faible, ESET suppose qu'il s'agit d'un test pour une attaque de plus grande envergure.

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)

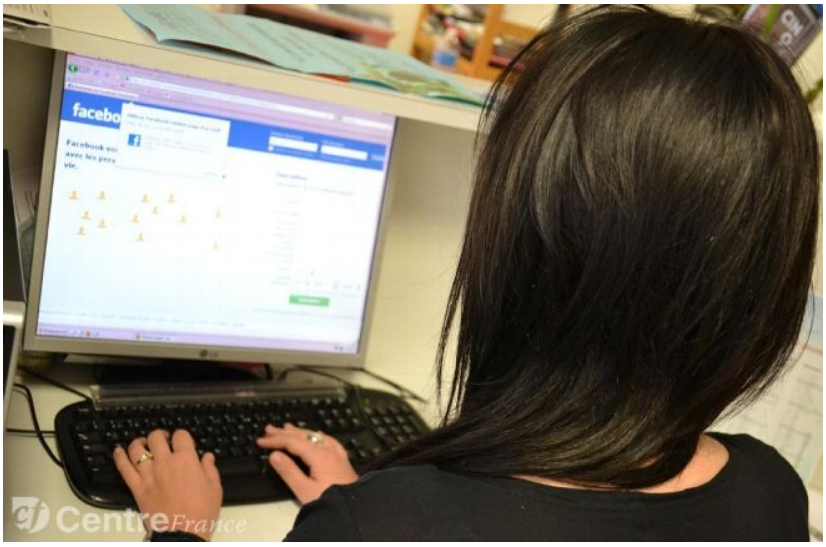
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *ESET*

Conférence-débat sur la cybercriminalité. Quels dangers, quelle prévention ? Entrée gratuite.



Conférence-débat sur la cybercriminalité. Quels dangers, quelle prévention ? Entrée gratuite.

La médiathèque de Roanne propose, le samedi 13 mai prochain, une conférence-débat sur le thème « Cybercriminalité : déjouer les pièges ». Ce sera une immersion en 1 h 30 dans les méandres de la toile.

Comme chaque trimestre, la médiathèque de Roanne organise une conférence-débat pour aborder des thématiques liées au multimédia et à internet, le samedi 13 mai, de 15 heures à 16 h 30, avec pour sujet « Cybercriminalité : déjouer les pièges » ou « Comment profiter d'internet en toute sécurité ».

Autour d'une présentation très interactive, cette conférence-débat permettra de répondre aux nombreuses questions que peuvent se poser les utilisateurs du web.

Escroqueries, dérives et esquives

Sécurité et risques sur le net, messagerie, mobilité, arnaques en tous genres, prévention, vocabulaire et procédures, pratiques des jeunes, légalité ou pas dans le streaming, virus, mots de passe sécurisés… seront les notions abordées au fil de cet atelier ouvert à tous.

« C'est une formule qui est assez bien reçue et qui plait au public. La conférence-débat se veut très interactive et ouverte », annonce Franck Guigue, responsable des espaces des pratiques numériques à la mairie de Roanne, qui sera l'animateur de cette rencontre. Elle sera aussi l'occasion pour les internautes de faire le point sur les escroqueries les plus fréquemment rencontrées et donner les clés aux utilisateurs du web pour esquiver les nombreux attrape-nigauds.

Pratique. Samedi 13 mai, de 15 heures à 16 h 30, à la médiathèque de Roanne, avenue de Paris. Conférence ouverte à tout public. Entrée libre. Renseignements sur le site internet : www.bm-roanne.fr

---

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

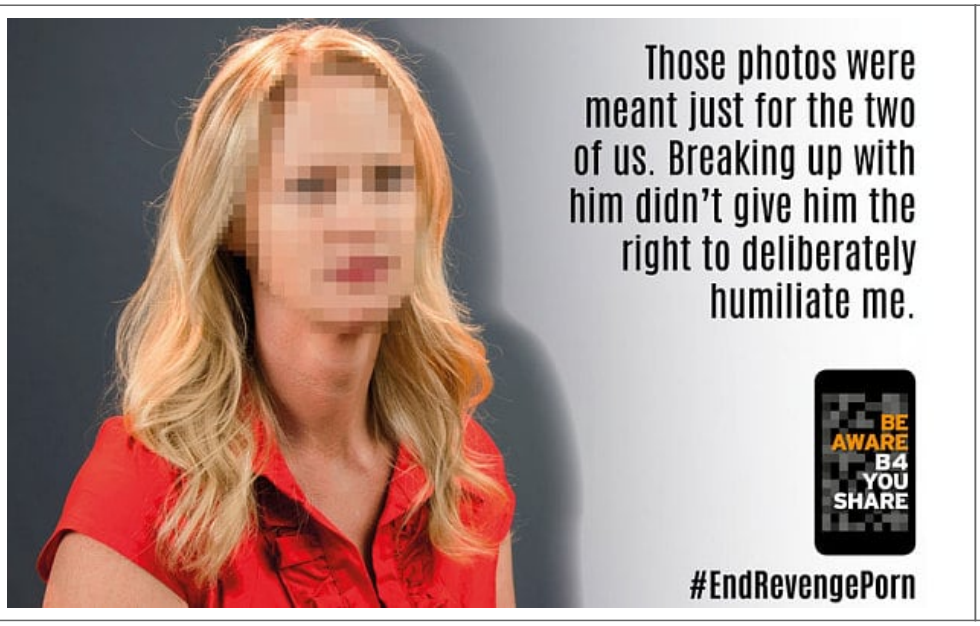
Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *La cybercriminalité : quels dangers, quelle prévention ? – Roanne (42300) – Le Pays*

Le « revenge porn » dans la loi pour une République numérique



Le « revenge porn » dans la loi pour une République numérique

Nous nous penchons ici sur une des nouvelles conquêtes de la loi du 7 octobre 2016 pour une République numérique.Nous avons déjà examiné certaines facettes de cette loi sur les questions d'e-réputation, notamment celle du droit à l'effacement pour les mineurs (notre actualité du 26 janvier 2017) et celle de la mort numérique (celle du 3 février). Voici à présent la prévention pénale du revenge porn, qui du reste vient de connaître une illustration judiciaire intéressante.

Par Didier FROCHOTN

Notion de *revenge porn*

On nomme sous cette élégante expression franglaise l'action qui consiste à se venger d'une personne en rendant publique des contenus pornographiques, réalisés avec ou sans accord de l'intéressé(e) mais qui n'a jamais donné son accord pour leur publication, dans le but évident de l'humilier. Il s'agit fréquemment de « retombées collatérales » d'une séparation de couple qui se passe mal. Il n'est pas nécessaire d'être footballeur professionnel pour se trouver au cœur d'une tourmente médiatique très traumatisante pour la victime, comme en témoigne certain(e)s de nos client(e)s qui en 'ont vécu une.

Le *revenge porn* face au droit

La Cour de cassation s'était déjà prononcée sur cette question le 16 mars 2016 (actualité du 18 mars) dans une affaire où elle avait alors écarté le délit pénal de publication d'image. Dans ce cas précis, la personne avait été consentante à la réalisation d'une vidéo d'ébats sexuels avec son conjoint, mais pas de sa mise en ligne après séparation.

Nous nous sommes montré quelque peu critique sur cette décision qui certes se bornait à appliquer l'interprétation stricte de la loi pénale. Nous montrions alors quelles autres voies la Cour aurait pu suivre. Et nous avions annoncé le futur renforcement de l'arsenal pénal en cas de vengeance par publication de contenus à caractère sexuel par la loi pour une République numérique alors en gestation.

Un renforcement de l'arsenal juridique pénal

L'article 67 de la loi du 7 mars 2016 est donc venu renforcer le code pénal en créant, sous les articles 226-1 et 226-2 (délit d'atteinte volontaire à l'intimité de la vie privée par transmission de propos tenus en privé ou par captation et diffusion d'image, puni d'un an de prison et de 45 000 € d'amende), un nouvel article 226-2-1 qui renforce les sanctions pénales dans les cas spécifiques de contenus à caractère sexuel…[lire la suite]

Réagissez à cet article

Source : *Le « revenge porn » dans la loi pour une République*

numérique

« 13 Reasons Why », Selena Gomez se penche sur le problème du cyber-harcèlement – Grazia.fr

	« 13 Reasons Why », Selena Gomez se penche sur le problème du cyber-harcèlement

---

L'actrice et chanteuse revient avec la série « 13 Reasons Why » sur Netflix. Une série racontant le suicide d'une adolescent

La vie de Selena Gomez est loin d'être un long fleuve tranquille. Enfant-star, adolescente adulée et épiée aux quatre coins du monde grâce (ou à cause) de la série *Les Sorciers de Waverly Place*, la jeune femme avoue avoir eu du mal à gérer sa célébrité et le flot de critiques qui va avec. C'est ce qu'elle admet dans une interview accordée à *The New York Times*. Selena Gomez y a été interrogé au sujet de la nouvelle série qu'elle produit : « 13 Reasons Why », une adaptation d'un roman de Jay Asher qui raconte l'histoire d'une adolescente qui se suicide à cause du cyber-harcèlement qu'elle subit au lycée. Achetée par Netflix, la série sera disponible dès le 31 mars.

Selena voit une « *histoire miroir* » par rapport à la sienne. Elle s'explique : « *J'ai l'impression que cette série reflète ce qui s'est passé dans ma vie*« . L'interprète de « Same Old Love » ajoute : « *Je pense que Jay Asher a compris que je savais ce que signifiait être victime de harcèlement. Je sais très bien ce que c'est d'être harcelée. J'étais scolarisée dans la plus grande école du monde qui n'est autre que Disney Channel*« .

Supprimer Instagram

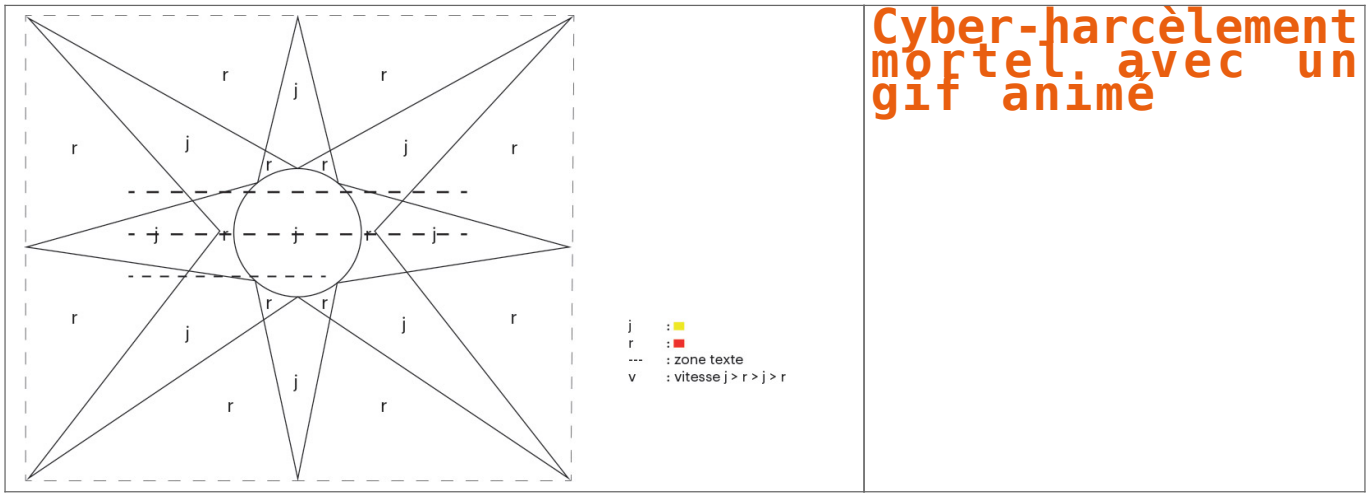
Un harcèlement qui ne s'est pas arrêté à la fin de sa scolarité, mais qui se poursuit encore aujourd'hui. La jeune femme est suivie par plus de 46 millions d'abonnés. Et parmi ceux-là, il y en a qui déversent chaque jour des centaines de messages haineux. « *Parfois, on ne peut pas les éviter… Tu es concentré sur les négatifs. Ce n'est pas juste 'tu es moche'. C'est comme s'ils voulaient vous couper de votre âme. Imaginez comment vous vous sentez déjà vis-à-vis de vous-même et vous avez quelqu'un qui écrit tout un paragraphe pointant chaque petite chose de vous, même si c'est juste physique*« . Pour s'épargner les commentaires de haine, Selena Gomez a pris ses distances avec la plateforme de partage de photos et vidéo. Sa solution ? « *Je supprime l'application au moins une fois par semaine*« .

Par Sabine Bouchoul

Réagissez à cet article

Source : *« 13 Reasons Why », Selena Gomez se penche sur le problème du cyber-harcèlement – Grazia.fr*

Cyber-harcèlement mortel avec un gif animé



Un journaliste américain a été victime d'une très violente crise d'épilepsie en regardant une image animée envoyée, à dessein, par un troll. Le responsable, arrêté, risque dix ans de prison.

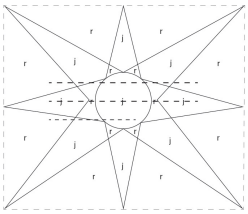
On connaissait le gif comme objet de plaisanterie web, il pourra désormais être aussi considéré comme une arme pouvant tuer. Le tribunal de Dallas s'apprête à juger John Rayne Rivello, utilisateur de Twitter et harceleur présumé du journaliste Kurt Eichenwald. L'arme du – presque – crime : une image animée envoyée à l'attention du reporter, provoquant une crise d'épilepsie qui aurait pu être mortelle.
Comme l'explique le blog Big Browser du *Monde*, le journaliste, collaborateur de *Newsweek* ou *Vanity Fair*, était connu pour ses positions anti-Donald Trump, qu'il relayait également sur Twitter. Il ne cachait pas non plus sa condition épileptique.
Mi-décembre, à la suite d'une discussion animée sur Fox News, où il était interviewé par l'éditorialiste (très) conservateur Tucker Carlson, Eichenwald subit les assauts de plusieurs soutiens à Trump sur son compte Twitter. Une journée malheureusement normale sur les réseaux sociaux, mais qui s'est très mal terminée. L'un des trolls, répondant au nom clairement antisémite de @jew_goldstein, lui envoie un gif stroboscopique, agrémenté du message : *« Tu mérites une crise pour ton message. »*
La femme d'Eichenwald trouvera peu après son mari sur le sol de bureau, le message Twitter clignotant sur son écran, comme le rapporte son avocat au *New York Times*. Après avoir appelé les secours, elle a répondu à l'envoyeur : *« C'est sa femme qui parle. Vous avez causé une attaque. J'ai récupéré vos informations. J'ai appelé la police et leur ai fait part de votre agression. »*
Suivre


Kurt Eichenwald
✔@kurteichenwald
@jew_goldstein This is his wife, you caused a seizure. I have your information and have called the police to report the assault.
05:31 – 16 Dec 2016
•
•
2 6942 694 Retweets
•
4 0594 059 j'aime

La réaction épileptique de Kurt Eichenwald, qui a duré huit minutes selon le *Dallas News*, a été particulièrement violente : incapacité de travailler durant plusieurs jours, perte de la sensation de la main gauche et trouble de l'élocution durant plusieurs semaines. De quoi pousser la police de Dallas et le FBI à mener une enquête sérieuse.

Un iPhone, son Cloud et des preuves

Un mandat de recherche a été émis à l'encontre de @jew_goldstein et a permis de remonter la piste de plusieurs messages privés envoyés par le compte anonyme au sujet de Kurt Eichenwald. Dans ses échanges, l'utilisateur parlait de la condition médicale du journaliste et espérait *« qu'il fasse une crise »* voire *« qu'il meure »*. La police a été capable de relier le compte Twitter à un numéro de téléphone, puis à un modèle de smartphone – un iPhone 6 – qui les a ensuite menés, après avoir cité Apple à comparaître, au Cloud appartenant à un certain John Rayne Rivello.
Dans ses données, les enquêteurs ont trouvé une liste de preuves accablantes : l'image animée qui a provoqué la crise, une capture d'écran du tweet en question et de la réponse de la femme du journaliste, une capture d'écran de la page Wikipédia de Kurt Eichenwald, modifiée avec une fausse date de décès (le jour de l'envoi du tweet), une autre capture d'une liste d'éléments pouvant déclencher une crise d'épilepsie ou encore l'adresse du domicile du journaliste.
Pour l'avocat de Kurt Eichenwald, interrogé par *Newsweek*, l'action de Rivello sur Twitter *« n'est pas différente de celle de quelqu'un qui envoie par courrier une bombe ou des enveloppes remplies d'anthrax »*.
John Rayne Rivello s'apprête à passer devant le tribunal de Dallas avec une accusation tout à fait inédite. Le troll de 29 ans est accusé de cyber-harcèlement avec *« utilisation d'une arme mortelle »*, en l'occurrence l'image animée. Rivello encourt jusqu'à dix ans de prison. Ou quand le gif ne fait plus rire du tout.



Source : *Cyber-harcèlement : quand le gif animé devient une arme mortelle – L'actu Médias / Net – Télérama.fr*

Alerte : Comptes Twitter piratés. Comment les pirates ont fait et comment vous en

protéger ?

	**Alerte : Comptes Twitter piratés. Comment les pirates ont fait et comment vous en protéger ?**

De nombreux comptes, dont celui du ministère français de l'Economie, ont été piratés, mercredi matin, par un message évoquant le référendum constitutionnel du 16 avril en Turquie.

« #Allemagne nazie #Pays-Bas nazis. Voici une petite claque ottomane pour vous. » Mercredi 15 mars au matin, de nombreux comptes Twitter de personnalités et d'institutions ont publié un message, débutant par une croix nazie, évoquant le référendum constitutionnel du 16 avril en Turquie.

Parmi les victimes de ce piratage massif et hautement politique se trouvent :
• Le Ministère français de l'Economie,
• Le journal économique Forbes,
• Le Monde,
• Le site d'Alain Juppé,,
• le magazine « Envoyé spécial »,
• L'Académie de Rennes,
• Reuters au Japon,,
• le compte de l'émission « Envoyé Spécial »,,
• Nike en Espagne,,
• Unicef USA,,
• la Philharmonie de Berlin,
• Comptes d'université américaine…

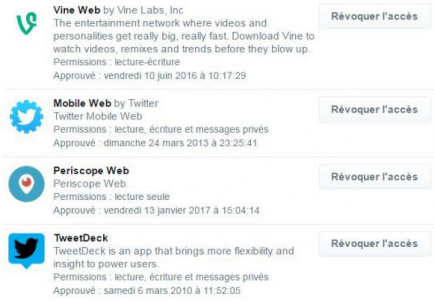
Le compte Twitter officiel de Bercy a été piraté mercredi 15 mars. (CAPTURE D'ÉCRAN)

Comment les pirates ont procédé

Pour réussir cette opération, le ou les pirates n'ont, a priori, pas eu recours à un système de détournement de mots de passe des comptes Twitter concernés. La faille provient, en fait, d'une « application tierce » : Twitter Counter, un outil payant et indépendant du réseau social. En échange d'une autorisation d'accès au compte, cette application propose aux entreprises et institutions des statistiques avancées, comme un suivi détaillé du nombre d'abonnés.
L'application Twitter Counter a confirmé, mercredi matin, le piratage de son service, et a annoncé le lancement d'une enquête interne. Dans un message posté sur le réseau social, l'entreprise rappelle qu'elle ne conserve pas les mots de passe de ses clients et assure qu'elle a désormais bloqué l'option qui lui permettait de poster des messages sur le compte de ses clients.
Cette méthode de piratage ne concerne malheureusement pas seulement les comptes Twitter d'importance. Si vous êtes un adepte du réseau social, vous avez sans doute déjà été tenté d'installer une application tierce vous permettant, par exemple, d'identifier les utilisateurs qui ont cessé de suivre votre compte. Celles-ci, comme Twitter Counter, ont de grandes chances de pouvoir publier des tweets en votre nom.

Comment savoir si votre compte est vulnérable

Pour vérifier l'identité des programmes tiers ayant accès à votre compte, rendez-vous dans la catégorie « Applications » des paramètres de Twitter. Vous trouverez une liste de tous les programmes tiers que vous avez installés, ainsi que les différents niveaux d'autorisations d'accès de ces applications à votre compte.
Si vous voyez l'application « Twitter Counter » dans cette liste, cliquez sur le bouton « Révoquer l'accès » en face d'elle.
Si certaines vous semblent farfelues ou peu sûres, vous pouvez également les signaler auprès de Twitter en cliquant sur « Signaler l'application » après avoir révoqué leur accès à votre compte.
Dans l'exemple ci-dessous, l'application Periscope est ainsi autorisée à lire uniquement des tweets, Vine à lire et à publier, et Tweetdeck à lire, publier, et accéder aux messages privés.



Notre avis

Je pense qu'il est anormal qu'une application tierce à Twitter comme « Twitter Counter » ait des droit d'écriture directement sur les comptes Twitter de ses abonnés ?
Pour ceux qui ne le savent pas, Twitter Counter permet d'analyser l'évolution de votre compte Twitter en « nombre de tweets, d'abonnés, de retweets et de mentions ».
Pourquoi une telle application à imposé à ses utilisateurs de pouvoir écrire sur leur compte ? Un simple droit en lecture est suffisant pour connaître le nombre d'abonnés, de tweets, retweets…
Partez à la chasse aux applications intrusives en vous rendant dans :
Twitter > Paramètres et fonctionnalités > Applications
et n'hésitez pas à « **Révoquer l'accès** » pour chacune des applications suspectes.

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Twitter : comment Bercy et d'autres comptes officiels ont été piratés (et comment vous en protéger)*

Les messages de WhatsApp peuvent être facilement lus par la CIA

Les messages de WhatsApp peuvent être facilement lus par la CIA

L'organisation WikiLeaks a reçu une importante base de données révélant les techniques de cyber-surveillance et de piratage de la CIA. Selon ces informations l'agence de renseignement américaine peut facilement accéder aux messageries, y compris WhatsApp et Telegram.

La Central Intelligence Agency (agence centrale de renseignement, CIA) est capable de contourner le cryptage de certaines applications populaires de messagerie, y compris WhatsApp et Telegram, selon les documents publiés par WikiLeaks aujourd'hui.
« Ces techniques permettent à la CIA de contourner le cryptage de WhatsApp, de Signal, de Telegram, de Wiebo, de Confide et de Cloackman en piratant les téléphones « intelligents » sur lesquels ces applications sont installées et de collecter les enregistrements audio et les messages avant que le cryptage ne soit activé », informe le document publié par WikiLeaks.

© FLICKR/ VIN CROSBIE
Espionnage en plein ciel: Air France dans le viseur des services secrets US et UK

Cette fuite a semé le trouble parmi les utilisateurs de WhatsApp, dont beaucoup ont réagi avec virulence aux nouvelles selon lesquelles l'application aurait commencé à partager des données avec Facebook l'année dernière.
La révélation de WikiLeaks suggère que les espions du gouvernement américain ont eu accès aux messages des utilisateurs malgré la mise en place d'un cryptage de bout en bout, qui est pourtant conçu pour protéger la confidentialité des utilisateurs.
Cependant, il se pourrait que la CIA n'ait pas piraté les applications elles-mêmes, mais craqué les outils de cryptage en attaquant les smartphones des utilisateurs.

© AFP 2017 SAUL LOEB
WikiLeaks publie plus de 8.700 documents concernant les capacités de cyber-espionnage de la CIA

Le site de Julian Assange, WikiLeaks, a annoncé le 7 mars la publication d'une nouvelle série de fuites sur la CIA sous le code « Vault 7 » qui sera, d'après le communiqué de l'organisation, la plus importante publication de documents confidentiels sur l'agence.
La première partie des fuites, intitulée « Year Zero », comprend 8 761 documents et fichiers qui ont été collectés sur un réseau isolé de haute sécurité du Centre Cyber Intelligence (département de la CIA) à Langley, dans l'État de Virginie.
Les fuites de « Year Zero » révèlent les capacités de piratage de la CIA contre un large éventail de produits américains et européens, notamment Windows, iPhone, Android et même les téléviseurs Samsung, qui ont été transformés en microphones cachés par le programme Weeping Angel…[lire la suite]

Réagissez à cet article

Source : *Les messages de WhatsApp peuvent être facilement lus par la CIA*