7 conseils pour se protéger les enfants des cyber pédophiles

	7 conseils pour se protéger les enfants des cyber pédophiles

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]

Réagissez à cet article

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

Vidéos résumant bien l'état des lieux de la cybercriminalité à travers le monde

	Vidéos résumant bien l'état des lieux de la cybercriminalité à travers le monde

---

Chaque jour, 1,5 million de personnes dans le monde sont victimes de la cybercriminalité. C’est une activité si lucrative qu’elle rapporte beaucoup plus que le trafic de drogue.
AFP

https://www.youtube.com/embed/cnzRPvuHFvI

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

Un piratage sur Tor par le FBI prive les victimes d’une justice

Un piratage sur Tor par le FBI prive les victimes d'une justice

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.
C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.
Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.
Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux.
Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?
Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.
Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI
L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.
C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA… [Lire la suite]

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

Quelles sont les modalités de blocage des sites Internet ?

Quelles sont les modalités de #blocage des sites Internet ?

M. Lionel Tardy interroge M. le ministre de l'intérieur sur le décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographiques.
Ce décret précise les modalités d'applications de l'article 6-1 de la loi pour la confiance dans l'économie numérique (LCEN). En complément, il souhaite savoir si, une fois la procédure appliquée, l'OCLCTIC sera également destinataire de données statistiques relatives aux tentatives de connexions aux sites bloqués, et le cas échéant, les modalités de ce recueil.

Texte de la réponse
La loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a doté la France de nouveaux moyens face à la menace constante et croissante à laquelle elle est confrontée. Elle permet, notamment, de mieux combattre la propagande terroriste sur internet. Ses textes réglementaires d'application ont été rapidement publiés et toutes ses dispositions sont donc aujourd'hui applicables. Il en est ainsi des dispositions visant, suivant un dispositif gradué et équilibré garantissant le respect des libertés publiques, à renforcer les capacités de blocage des sites internet faisant l'apologie du terrorisme ou y provoquant. Le décret d'application a été publié dès le 5 février 2015 (décret no 2015-125 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique). S'agissant du nombre de connexions à un site dont l'accès est bloqué, il fait l'objet d'une comptabilisation assurée par la sous-direction de lutte contre la cybercriminalité de la direction centrale de la police judiciaire. Cette comptabilisation s'inscrit dans une démarche d'évaluation du dispositif mais vise aussi à mieux appréhender l'évolution du comportement des internautes. Lorsqu'un internaute tente de se connecter à un site dont l'accès est bloqué, il est immédiatement renvoyé sur une page d'information du ministère de l'intérieur, lui expliquant la nature du blocage et l'informant sur les voies de recours. L'adresse IP est enregistrée. Les adresses IP ainsi collectées ne sont pas exploitées mais permettent une comptabilisation précise du nombre de connexions à chacune des pages bloquées. Les premiers chiffres enregistrés depuis la mise en place du dispositif font apparaître plus de 30 000 connexions par semaine concernant les sites de pédo-pornographie, et 250 connexions en moyenne par semaine concernant les sites à caractère terroriste. Différents éléments peuvent expliquer cet écart. Dans la liste des sites dont l'accès est bloqué, ceux concernant la pédo-pornographie sont plus nombreux que ceux provoquant à des actes terroristes ou en faisant l'apologie (rapport de 3 pour 1). Par ailleurs, les connexions aux sites pédo-pornographiques ne sont pas toujours volontaires (liens publicitaires sur sites pornographiques légaux, « pourriels », etc.). Au-delà de ces dispositions nationales, le ministère de l'intérieur a engagé plusieurs actions à l'échelle européenne et internationale. En témoignent, notamment, les récentes rencontres du ministre de l'intérieur avec les grands acteurs américains de l'internet pour les amener à davantage participer à la régulation des contenus appelant à la commission d'actes terroristes ou en faisant l'apologie. Ces travaux ont notamment permis de décider la création d'une plate-forme de bonnes pratiques dans la lutte contre la propagande terroriste sur internet.

Réagissez à cet article

Source : *Question n°74166 – Assemblée nationale*

Surveillance des salariés et logiciel de détection d'infractions pédopornographique | Le Net Expert Informatique

Surveillance des salariés et logiciel de détection d'infractions pédopornographique

Dans un arrêt du 11 mai 2015, le Conseil d'État confirme une délibération de la Cnil refusant à une entreprise la mise en place sur les postes informatiques d'un logiciel de recherche des infractions à caractère pédopornographique.

Si l'employeur peut exercer une surveillance sur les connexions internet des salariés sur leur poste de travail, de là à pouvoir mettre en œuvre un logiciel ayant pour objet de collecter des données relatives à la consultation par les salariés de sites à caractère pédopornographique, il y a un pas que n'a pas franchi la Cnil ni le Conseil d'État.
En effet, le Conseil d'État a été saisi par une entreprise d'une demande d'annulation de la décision de la Cnil lui refusant l'autorisation de mettre en place un tel logiciel.
La Haut juridiction n'a pas annulé la décision de la Cnil en considérant que la loi informatique et libertés ne permet à une entreprise privée de mettre en œuvre un traitement de données personnelles visant des infractions pénales ou qui peuvent en établir l'existence.

CE 11 mai 2015, n° 375669
Lire la suite….

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/126327/Surveillance-des-salaries-et-logiciel-de-detection-dinfractions-pedopornographique.aspx
Par Dominique Jullien

Google espionne et dénonce

des pédophiles aux Etats Unis. Qu’en est t-il en France ?

Google espionne et dénonce des pédophiles aux Etats Unis. Qu’en est t-il en France ?
Google a fait arrêter un Américain qui échangeait des photos pédopornographiques. Une pratique dont la légalité reste à prouver.

Il a alerté les autorités après avoir découvert des photos pédopornographiques dans les e-mails d’un habitant de Houston (Texas, Etats-Unis), rapporte la chaîne locale KHOU. Ce Texan, déjà coupable d’agression sexuelle sur un garçon de 8 ans en 1994, a été inculpé pour possession de pornographie infantile et promotion de pédopornographie.