

Les bons réflexes contre les attaques informatiques |

Denis JACOPINI

 **Les bons réflexes contre les attaques informatiques**

350 milliards d'euros par an : selon le McAfee Report on the Global Cost of Cybercrime publié en 2014, tel est le coût estimé des attaques informatiques à l'échelle mondiale. Depuis le début de l'année, les attaques se sont multipliées, notamment suite aux attentats de Charlie Hebdo, mettant plus que jamais en péril la sécurité des données des entreprises et des institutions. Un rapport publié le 16 février dernier par Kaspersky Lab a quant à lui révélé l'attaque d'une centaine de banques depuis 2013 par un gang organisé.

Afin d'appréhender au mieux ces offensives, il est important d'en comprendre les tenants et les aboutissants et d'avoir à l'esprit les réflexes qui permettent de s'en prémunir.

Des attaques aux motivations multiples

De plus en plus de sites internet sont victimes d'attaques dites de « défiguration » perpétrées par des hacktivistes revendiquant des convictions religieuses, politiques ou encore contestataires. On trouve également certains attaquants qui agissent uniquement pour l'amusement, mais ces scénarios se font de plus en plus rares. En général, seule la page d'accueil du site est modifiée pour signifier leur passage et évouer leurs revendications. On trouve également d'autres attaques qui, elles, sont plus furtives (ou en tout cas tentent de l'être) et consistent à voler des informations à des fins de rançonrage par exemple. Les vols de données bancaires (carte de crédit, numéros de comptes) permettent quasiment à eux du détournement d'argent, l'achat de services ou encore de matériels en ligne. Ces criminels, bien organisés, offrent des services de tout type à d'autres criminels : du kit d'infection, à l'envoi de spam massif, en passant par des serveurs de contrôle (c2c) pilotant des milliers de machines « zombies » permettant des attaques DDoS (Déni de service distribué). Tous n'ont pas le même niveau technique, certains ne sont d'ailleurs que des « presse-bouton », alors que d'autres ont la capacité de créer des virus, ou des programmes exploitant des failles de sécurité.

Mais comment s'y prennent-ils ? Ces malveillants utilisent une faille de sécurité dans un programme qui peut provenir d'une erreur de conception (un protocole mal sécurisé par exemple), de programmation ou d'implémentation (failles connues comme shellshock, heartbleed ou ghost), de configuration (oubli du mot de passe par défaut après une installation) ou encore d'une erreur d'utilisation par une personne utilisant un mot de passe trop faible par exemple. L'humain est donc au centre de cette problématique.

Le plus souvent ces attaques débouchent sur du détournement d'argent ou la diffusion de données sur internet. Les conséquences financières pour les entreprises peuvent être considérables, sans compter l'impact que cela peut avoir sur l'image de l'entreprise victime d'un piratage. Dès lors, quels réflexes adopter face à ces diverses attaques et failles ?

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

Contactez-nous

Adopter les bonnes pratiques pour limiter les risques

Les attaques ne cessent de croître dans la mesure où l'enjeu financier pour les criminels est très important. Lorsque l'on sait que l'attaque par déni de service est accessible pour seulement 30 à 70 dollars la journée et qu'un spam ne revient qu'à 10 dollars par tranche d'1 million d'e-mails*, ce type de pratique n'est pas prêt de cesser. A ce premier enjeu s'ajoute le manque de vigilance dont font preuve les internautes. Le risque de s'infecter est en effet omniprésent : il suffit de cliquer sur un lien drainant un logiciel malveillant ou encore de partager un contenu infecté.

Quand bien même le risque zéro n'existe pas, la grande majorité de ces attaques pourrait être bloquée, dès lors que l'on adopte les bonnes pratiques pour se protéger et protéger autrui. Le maître mot est l'anticipation et la capacité à réagir rapidement en cas d'intrusion, la mise en œuvre d'un pare-feu ou d'un anti-virus pour se protéger n'étant pas suffisante. Le processus organisationnel de sécurisation est en effet plus important que les outils de protection eux-mêmes (on a en général un rapport de 80-20).

Pour ce faire, l'un des points majeurs est la gestion des mises à jour. Lorsqu'une faille tombe, celle-ci peut-être déjà exploitée plus ou moins massivement. S'en suit la douloureuse phase consistant à tester si le programme régresse ou non dans son fonctionnement avant une mise en production. Durant toute cette période, le programme est encore exposé à une potentielle exploitation de la faille. Cela sous-entend qu'il faut d'une part valider aussi vite que possible, et d'autre part essayer de se protéger temporairement avec des outils de type Firewall ou IPS. Il est aussi bon de rappeler que ces outils de protection sont aussi faillibles que les autres et qu'ils peuvent être contournés.

Dans le cas où l'attaque a déjà eu lieu, sur un site web par exemple, la première chose à faire est de bloquer le site. Cette phase est primordiale dans la mesure où un site piraté peut renvoyer des logiciels malveillants aux internautes le consultant. La deuxième étape est de sauvegarder tous les journaux, les données et programmes du site ainsi que la base de données, avant de procéder à une analyse du système pour connaître l'origine de l'attaque. Cette analyse est primordiale pour une remise en production du site. Elle permet de connaître par quel moyen les attaquants sont entrés dans le système et ce qu'il faut mettre à jour. Le mieux est de revenir sur une version de sauvegarde dont on est sûr qu'elle n'a pas été affectée par la compromission et de la mettre à jour. Parallèlement, il est également vivement conseillé de porter plainte afin que ces attaques soient référencées par les autorités et que des mesures soient prises.

S'il est crucial de prendre en compte la problématique de sécurité lors de la création d'un projet informatique, il est tout aussi indispensable d'en assurer la maintenance afin d'anticiper les attaques et de pouvoir les gérer efficacement, et ainsi minimiser leur impact sur l'activité de l'entreprise.

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

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire.

Source : <http://www.journaldunet.com/solutions/expert/60082/attaques-informatiques-decryptage-du-phenomene-et-reflexes-a-adopter.shtml>

Par Sébastien Delcroix - NFrance

Cybercriminalité – Retour sur les principales attaques informatiques en France et dans le monde | Denis JACOPINI



Cybercriminalité – Retour sur les attaques informatiques en France et dans le monde qui ont fait la une

Selon la commission européenne, la cybercriminalité englobe 3 catégories d'activité criminelles :

- 1) Les atteintes directes à des systèmes informatiques** (ou Système de traitement automatisé de données, ou encore S.T.A.D.) en perturbant leur fonctionnement, tels que les attaques par déni de services (appelé aussi denial of service attack ou aussi DOS) destinées à faire tomber un serveur (comprenez rendre inaccessible ou mettre en panne un serveur) à distance.
- 2) Réaliser des actes illicites en utilisant les outils numériques** (escroqueries, vols de données bancaires ou personnelles, espionnage industriel, atteinte à la propriété intellectuelle, sabotage, accès frauduleux, fraudes, usurpation d'identité, phishing, création de PC zombies, contamination d'autres postes informatiques ou d'autres serveurs...)
- 3) Modifier le contenu d'un espace numérique pour y déposer ou diffuser des contenus illicites** (pédopornographie, racisme, xénophobie).

Les cyberdélinquants n'ont d'autre objectif que de gagner beaucoup d'argent. Virus, spams, et autres botnets drainent plusieurs centaines de millions de dollars chaque année à travers le monde.

Sans nous étaler sur les 144 milliards de courriers électroniques qui transitent dans le monde chaque jour dont 70% ne sont que du spam, les 10 millions de français victimes d'actes cybercriminels et 75% de ces actes de cybercriminalité qui sont de grande envergure (Norton 2013) qui concernent les 3,2 milliards d'internautes dans le monde en 2014 (dont la moitié pour l'Asie), vous trouverez ci-dessous, par

ordre anté-chronologique, quelques principaux actes cybercriminels recensés par notre Expert, Denis JACOPINI.

Vous pouvez directement contacter Denis JACOPINI ici

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](#)

30/09/2015 : Les sites Web du gouvernement thaïlandais attaqués

[Consulter](#)

12/09/2015 : Cyberattaque contre le site officiel de la Commission électorale centrale (CEC) de Russie

[Consulter](#)

05/08/2015 : La SNCB victime d'un piratage

[Consulter](#)

25/07/2015 : Le Pentagone visé par une cyber-attaque russe
[Consulter](#)

28/07/2015 : Les e-mails de hauts gradés de l'armée américaine piratés
[Consulter](#)

18/07/2015 : Piratage du site de rencontres adultères Ashley Madison
[Consulter](#)

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** ;



06/07/2015 : Hacking Team, société d'espionnage informatique hacké
[Consulter](#)

19/05/2015 : Un hacker a modifié en vol la puissance d'un réacteur
[Consulter](#)

14/05/2015 : Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag
[Consulter](#)

14/05/2015 : Des hôtels suisses victimes d'un piratage informatique
[Consulter](#)

12/05/2015 : Kaspersky annonce être victime d'une Cyberattaque
[Consulter](#)

05/05/2015 : Arnaque aux faux virements : Vol de 15 millions d'euros à Intermarché
[Consulter](#)

29/04/2015 : Des pirates informatiques volent 5 millions de dollars à Ryanair
[Consulter](#)

10/04/2015 : Lufthansa victime d'une cyberattaque
[Consulter](#)

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



[Consulter](#)

02/01/2015 : Les données de deux millions d'abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.

[Consulter](#)

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** ;



**Le Net Expert
INFORMATIQUE**

Consultant en Cybercriminalité et en
Protection des Données Personnelles

[Contactez-nous](#)

26/12/2014 : PlayStation et Xbox victimes d'une panne après une cyber-attaque. Les joueurs de Xbox (ci-dessus) et de Playstation ne peuvent actuellement plus connecter leur console aux services en ligne en raison d'un piratage.

[Consulter](#)

21/12/2014 : Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30

ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.

[Consulter](#)

19/12/2014 : Le régulateur mondial d'internet, l'Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

[Consulter](#)

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](#)

18/12/2014 : Une usine métallurgique allemande a subi une cyberattaque qui a provoqué des dégâts matériels conséquents, a révélé jeudi la publication d'un rapport gouvernemental allemand, cité par le site ITworld.

[Consulter](#)

18/12/2014 : L'ICANN (Le régulateur mondial d'Internet)

victime d'un piratage informatique

[Consulter](#)

21/10/2014 : Staples a annoncé mener une enquête concernant un possible piratage de cartes de paiement, le numéro deux mondial des articles de bureau allongeant ainsi potentiellement la liste des entreprises américaines visées par une cyber-attaque.

[Consulter](#)

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** ;



**Le Net Expert
INFORMATIQUE**

Consultant en Cybercriminalité et en
Protection des Données Personnelles

[Contactez-nous](#)

14/10/2014 : Le service de stockage de documents a pris les devants et réinitialisé les comptes utilisant les informations volées. Il affirme ne pas avoir subi d'intrusion sur ses serveurs.

[Consulter](#)

02/10/2014 : JP Morgan Chase a indiqué que 76 millions de foyers et 7 millions de PME parmi ses clients avaient été piratés lors d'une attaque informatique dans le courant du mois d'août.

[Consulter](#)

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](#)

08/09/2014 : Home Depot : finalement 56 millions de cartes bancaires piratées

[Consulter](#)

16/06/2014 : Payer une rançon ou voir les données de centaines de milliers de ses clients publiées sur Internet. C'est le choix auquel devait faire face jusqu'à lundi 16 juin au soir l'entreprise de livraisons de pizzas Domino's Pizza.

[Consulter](#)

21/05/2014 : Victime d'une attaque, eBay demande à ses utilisateurs de changer de mot de passe
Les vols de données se suivent et se ressemblent (Target, Orange...). Le spécialiste de l'e-commerce, eBay, vient de communiquer sur une attaque informatique qui aurait visé ses bases de données.

[Consulter](#)

20/05/2014 : Malware BlackShades : 100 arrestations dont 29 en France

A l'origine de l'infection de plus de 500.000 ordinateurs, le logiciel espion BlackShades a donné lieu à une opération de police internationale. En France, 29 personnes ont été placées en garde à vue, en majorité des adolescents ayant avoué avoir exploité le malware.

[Consulter](#)

15/04/2014 : Les deux premiers sites internet reconnaissant avoir subi une attaque liée à la Faille Heartbleed

Au Royaume Uni, le site parental Mumsnet a été attaqué via la vulnérabilité Heartbleed.

Au Canada, l'administration fiscale CRA a admis publiquement avoir été victimes de la faille de sécurité découverte dans l'outil de chiffrement OpenSSL. (900 numéros d'assurance sociale volés) .

[Consulter](#)

12/02/2014 : Une attaque par déni de service (DDoS) a frappé de multiples serveurs aux Etats-Unis et en Europe en début de semaine. Il s'agit de l'**attaque informatique de ce type la**

plus grande recensée à ce jour.

Consulter

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](#)

31/01/2014 : La messagerie de Yahoo! victime d'une attaque informatique massive

Des cybercriminels se sont introduits dans des comptes email, à la recherche de données personnelles. Les utilisateurs impactés sont invités à modifier leur mot de passe.

Consulter

27/11/2013 : La chaîne américaine de grande distribution Target a été victime de pirates informatiques qui se sont procuré les coordonnées bancaires de plus de 40 millions de ses clients entre le 27 novembre et le 15 décembre. Ce piratage tombe mal en pleine période des fêtes et ses conséquences sont potentiellement désastreuses pour les

clients ainsi que pour la marque.

Consulter

28/04/2013 : L'auteur présumé de la cyberattaque contre Spamhaus arrêté

Un Néerlandais de 35 ans a été interpellé en Espagne. Il est soupçonné d'être à l'origine d'une cyberattaque fin mars contre une entreprise basée en Suisse, Spamhaus, qui fournit aux messageries des listes permettant de bloquer les mails indésirables – les fameux spams.

Consulter

15/02/2013 : Facebook a subi une attaque informatique « sophistiquée »

Le réseau social Facebook a annoncé avoir subi, le mois dernier, une attaque informatique « sophistiquée », qui n'aurait toutefois pas compromis les données de ses utilisateurs.

« Nous avons remédié au problème dans tous les appareils infectés, nous avons informé la police et commencé une vaste enquête qui se poursuit à ce jour », a ajouté le réseau.

Consulter

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](#)

02/02/2013 : Twitter touché par des attaques informatiques
Le réseau social Twitter a annoncé, vendredi 2 février, que certains de ses utilisateurs avaient été victimes d'attaques informatiques similaires à celles portées contre des sociétés et des médias américains.

[Consulter](#)

28/12/2012 : Le groupe pétrolier d'Arabie Saoudite Aramco a révélé avoir fait l'objet d'une attaque informatique de grande ampleur au milieu du mois d'août. Ce sont ainsi 30.000 postes de travail de l'entreprise qui ont été infectés par un virus informatique, provenant de l'extérieur.

[Consulter](#)

21/08/2012 : Le nouveau virus Shamoona illustre une fois de plus la progression des attaques visant de 'nouvelles'

cibles. Le virus Shamoon (ou Disttrack) semble écraser des fichiers dans les PC Windows, puis les 'master boot records'. Il en résulte que ces fichiers ne peuvent être récupérés. Or le PC ne peut être redémarré sans qu'ils soient réinstallés.

Consulter

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

29/05/2012 : Flame, le virus le plus puissant de l'histoire du cyber-espiionage ?

Découvert au Proche-Orient, ce malware circulerait depuis plus de cinq ans et viserait, comme Stuxnet, des entreprises sensibles et des sites académiques. Une nouvelle arme pour la cyber-guerre ?

Consulter

27/04/2011 : Sony s'est fait pirater en mai 2011 12700 numéros de cartes de crédit non américaines issues d'une vieille base de données.

Consulter

07/03/2011 : Bercy et plus précisément **la direction du Trésor victime d'une vaste opération de piratage** informatique

Au total, plus de cent cinquante ordinateurs du ministère ont été infiltrés et de nombreux documents piratés. La méthode des espions est classique : à partir d'une adresse e-mail piratée, le « hacker » prend le contrôle de l'ordinateur de sa cible grâce à un cheval de Troie, en l'occurrence une pièce jointe. Chacun de ses correspondants au sein de l'administration peut à son tour être infiltré.

Ingénierie sociale a encore frappé. Crédulité ou excès de confiance ?

Consulter

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

21/11/2010 : Quand le piratage informatique s'en prend au Nucléaire

Les experts sont maintenant convaincus que le virus Stuxnet a été conçu pour s'attaquer aux centrifugeuses de Natanz utilisées par Téhéran pour enrichir l'uranium.

Consulter

Pour combattre cela, les états organisent 3 branches : Cyberdéfense (atteinte à la sécurité nationale), Cybersécurité (anticipation des risques numériques) et Cybercriminalité qui est la délinquance transposée dans le monde numérique.

Des organismes sont créés ou réorganisés et des hommes embauchés :

O.C.L.C.T.I.C. : Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

D.C.R.I. : Direction centrale du Renseignement intérieur qui depuis début Mai 2014 d'appelle :

D.G.S.I. : Direction Générale de la Sécurité Intérieure

Gendarmerie Nationale

A.N.S.S.I : Agence Nationale de la Sécurité des Systèmes d'Information (créé en juillet 2009)

Cyberdouanes

B.E.F.T.I. : Brigade d'enquête surles Fraudes aux Technologies de l'Information

**Cet article vous à plu ? Laissez-nous un commentaire
(notre source d'encouragements et de progrès)**

La webcam, Est-ce une vraie menace pour les utilisateurs d'ordinateurs

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

LE NET EXPERT
AUDITS & EXPERTISES

EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES
LENETEXPERT.fr
LE NET EXPERT
MISES EN CONFORMITE

RGPD CYBER

SPY DETECTION
Services de détection
de logiciels espions

LE NET EXPERT
FORMATIONS

LE NET EXPERT
ARNAQUES & PIRATAGES

La **webcam**, est-ce une vraie menace pour les utilisateurs d'ordinateurs

Après Mark Zuckerberg et sa webcam masquée par du scotch, voilà que c'est le directeur du FBI, James Comey, qui admet avoir adopté le même réflexe.

Une webcam cachée pour s'éviter bien des ennemis

A l'heure où les hackers multiplient les attaques contre les machines des entreprises et des particuliers, beaucoup se sont moqués de Mark Zuckerberg et de son bout de scotch sur la webcam et sur la prise jack, certains allant même jusqu'à le traiter de « parano ». Pourtant, il semblerait qu'il s'agisse d'un réflexe à prendre et ce pour tout le monde. En effet, un pirate talentueux peut assez simplement prendre le contrôle d'une webcam à distance et pousser ainsi l'utilisateur à télécharger un malware sur sa machine. Aussi, lors d'une interview, James Comey, le directeur du FBI, a défendu l'idée de masquer la webcam. Il a même précisé que ce devait être un réflexe de base en matière de sécurité. En prenant le contrôle de votre caméra, un pirate peut effectivement visionner vos saisies sur clavier et récupérer ainsi identifiants, mots de passe et coordonnées bancaires pour ne citer qu'eux... lire la suite]

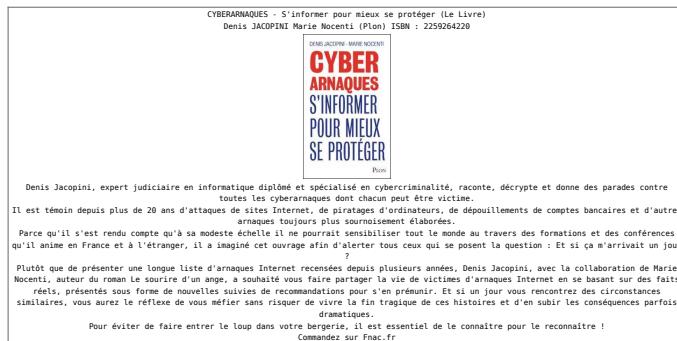
Conseils de Denis JACOPINI :

Les personnes averties croient utiliser la méthode miracle pour protéger leur vie privée en masquant leur Webcam.

Certes, je recommande toutefois de masquer votre Webcam car, même si, en l'absence de logiciel de sécurité adapté, le pirate peut la mettre en marche sans que vous rendiez compte de rien. Le pirate peut en effet voir votre tête en train de taper au clavier ou de jouer (ce qui en soit n'aura rien d'intéressant) mais selon l'orientation, voir le reste lorsque vous éloignez de l'ordinateur.

A l'instar des baby phones piratés, mettre en route le microphone de votre ordinateur est tout aussi facile que de mettre en route votre Webcam et même mieux d'ailleurs, car à ma connaissance, il n'existe pas de logiciel de sécurité qui empêche l'accès au microphone. Certes tout le monde n'est pas Mark Zuckerberg, mais tout professionnel devrait en plus de couper son téléphone pendant les réunions, penser aussi à boucher le microphone de son appareil ou mieux, enfincher une fiche Jack vide.

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



06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 Invités : 7 Millions de victimes de la Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risquer ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

<https://www.youtube.com/watch?v=vlDw3kI7ra2s>
12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet
Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coédité avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de Justice en Informatique spécialisé en Cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).
Commandez sur Fnac.fr

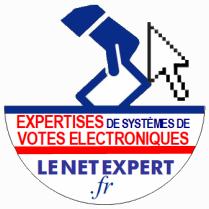
Original de l'article mis en page : La webcam, une vraie menace pour les utilisateurs d'ordinateurs

Comment retirer des publications gênante sur les réseaux sociaux ? Les conseils de la CNIL

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



LE NET EXPERT
AUDITS & EXPERTISES



EXPERTISES DE SYSTEMES DE
VOTES ELECTRONIQUES
LE NET EXPERT
.fr



RGPD CYBER
LE NET EXPERT
MISES EN CONFORMITE



SPY DETECTION
Services de détection
de logiciels espions



LE NET EXPERT
FORMATIONS



LE NET EXPERT
ARNAQUES & PIRATAGES



Comment retirer
des publications
génante sur les
réseaux sociaux
? Les conseils
de la CNIL

Sur les réseaux sociaux, vous pouvez être confronté à la diffusion d'informations personnelles publiée par d'autres internautes. Voici quelques liens utiles pour demander rapidement l'effacement de ces contenus

Une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable ». Sur une publication, vous pouvez être identifié :

- **directement** (exemple : nom, prénom, etc.)
- ou **indirectement** (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à votre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi votre voix ou votre image).

Votre identification peut être réalisée :

- **à partir d'une seule de vos données** (exemple : numéro de sécurité sociale, etc.)
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)

Avant de demander la suppression du contenu, assurez-vous que le compte ou l'information n'appartient pas à un homonyme.

En cas de doute raisonnable, le réseau social peut être en mesure de vous demander tout document permettant de prouver que ce contenu vous concerne. En revanche, **il ne peut pas vous demander des pièces justificatives qui seraient abusives, non pertinentes et disproportionnées par rapport à votre demande.**

1. Signaler la publication à effacer

En fonction du réseau social, vous devez vous rendre sur la page appropriée qu'il a mis à votre disposition à cet effet.

Twitter : Signaler la divulgation d'informations privées

Instagram : Signaler une photo ou vidéo pour violation de vos droits de confidentialité sur Instagram

Facebook : Utiliser le lien » Signaler »

situé à côté de la publication, de la photo ou du commentaire

Snapchat : Signaler la publication ou Utiliser ce formulaire en ligne ou Utiliser le formulaire de droit à l'image

LinkedIn : Signaler le harcèlement d'un utilisateur ou un problème de sécurité

Youtube : Réclamer une atteinte à la vie privée

Dailymotion : Sous chaque vidéo figure un bouton » Signaler cette vidéo »

en cliquant dessus, vous aurez à remplir un formulaire.

2. Si le réseau social ne fait pas partie de cette liste

- Rendez-vous vous en bas de la page d'accueil du réseau social ;
- Identifiez une page « politique de confidentialité » ou « données personnelles » ou « vie privée » ;
- Dans cette page, recherchez les coordonnées du service ou le formulaire qui répondra à votre demande ;
- Envoyez si besoin un modèle à personnaliser qui comprend les références aux textes de loi et vous permet d'indiquer un motif.

Quelle réponse attendre du réseau social ?

Le réseau social doit procéder à l'effacement dans les meilleurs délais et au plus tard dans un délai d'un mois, qui peut être porté à trois mois. Dans ce dernier cas, l'organisme doit vous informer des raisons de cette prolongation dans le délai d'un mois.

En parallèle de cette démarche d'effacement – et si ce contenu est référencé dans les moteur de recherche – exercez votre droit au déréférencement de manière à ce que ce contenu ne soit plus associé à votre nom et prénom dans les résultats d'un moteur de recherche.

En cas de réponse insatisfaisante – ou d'absence de réponse sous un mois – de la part du réseau social ou du moteur de recherche, vous pouvez saisir la CNIL.

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

Les 10 conseils pour ne pas se faire «hacker» pendant l'été

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

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

Source : *Publication gênante sur les réseaux sociaux : signalez pour supprimer ! | CNIL*

Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité | Denis JACOPINI



Des solutions pour la sensibilisation et formation des salariés face à la Cybercriminalité

La sensibilisation et l'éducation des utilisateurs jouent un grand rôle dans la réduction des risques.

Il importe donc pour les entreprises d'encourager leurs collaborateurs à se comporter de manière cohérente, en respectant des processus et procédures communiqués clairement, dont la conception et la surveillance sont centralisées et qui couvrent la totalité des équipements en usage. Cela n'évitera peut-être pas toute tentative d'attaque mais renforcera certainement la sécurité de l'entreprise.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI et

<http://www.globalsecuritymag.fr/Les-entreprises-revoient-leur,20150826,55304.html>

Ne relayez pas les spams, canulars, chaînes de lettres... | Denis JACOPINI

2



L'association Cléair Taïti (Club de la Sécurité de l'Informatique Région Tahiti, une jeune association de professionnels du secteur) continue de détailler les 12 commandements de la sécurité informatique dans nos colonnes. Après nous avoir appris comment choisir un mot de passe et comment sécuriser sa navigation sur le Web, l'association s'attaque au sujet pour eux troisième commandement.

Le piratage informatique n'aide pas à des techniques de hacking, il utilise aussi des manipulations qualifiées d'*«Ingenierie sociale»*, qui consistent à obtenir des informations confidentielles (identifiant un mot de passe par exemple) en trompant les victimes. C'est pourquoi, en complément de votre antivirus, il est indispensable de faire preuve de sens critique lors de la lecture de certains messages non sollicités.

Le spamer est un curieux malin, aussi appelé «pisseur». Ces messages proposent de tout : les réseaux d'un barbier, des éducateurs ou d'autres praticiens contraints, un prêt d'argent, voire des ressources sur Internet, etc.

Certains spams sont alors bien plus que de l'abus, mais certains peuvent encore plus d'aggraver depuis lors les réseaux sociaux. Les conseils restent pourtant les mêmes : pour éviter une utilisation de vos professionnels que nous ne connaissons pas l'expéditeur, il y a qu'une règle : détruire le message et ne répondre surtout pas.

Le SPAM

Definition d'un spam : «*cyber-escroquerie* généralement menée par courriel.

Malheureusement, il existe des personnes qui veulent servir toute sorte de compte pour vérifier votre identité / corriger un défaut / payer la commission du celu qui vous appelle la 'petite affaire'... » Ils peuvent aussi se présenter comme la nouvelle d'un gros gain à une loterie à laquelle vous n'avez jamais joué.

En Polynésie, ce sont les offres de « prises entre particuliers » par mail, sur Facebook et sur les forums qui sont utilisées de manière industrielle ces dernières années, faisant des centaines de victimes qui ne reverront jamais leur argent.

Le phishing ou homogénéage

Vous recevez un message qui ressemblerait en tout point à ce que pourrait vous enoyer un site officiel. Par exemple Yahoo, Google, Gmail, EDF, votre banque, etc. Les clients Mana subissent ces dernières semaines une grosse attaque de ce type, où des courriels ressemblant à ceux du fournisseur d'accès à internet vous demandent votre mot de passe, votre question secrète, mais une organisation vous facilitez un service et ont déjà toutes les informations qui leurs sont nécessaires sur vous. Donc il va de vous demander juste son identifiant ou ses informations bancaires de cette façon. Réfléchissez donc de ce qui semble être un message important mais qui n'est en réalité qu'un escroquerie.



23 adresses électroniques volées ! (partout dans ce message). Parfois il y en a beaucoup plus une véritable maladie pour les spammers toujours à la recherche de nouvelles adresses mail à polluer.

Comme dans le cas du Chef Mana, les chaînes manipulent le lecteur en jouant sur les sentiments. Mais les transmettre va-t-il réellement résoudre le problème ? Si vous velez aider, il existe des petitions en ligne (ou l'on peut compter le nombre de soutiens à une cause), des sites sécurisé pour faire des dons. Mais ne faites surtout pas cultiver une chaîne.

Parfois, les chaînes utilisent la superstition en prétendant qu'il se fait pas suivre, un cycle sera rompu et que des événements atroces se produiront. Ne vous laissez pas impressionner : aucun message n'a l'air de pouvoir. Par contre, le non-respect des consignes de cyber-sécurité peut avoir des effets dramatiques.

Qui fait-il faire ?

Si vous envoyez un message à de nombreuses personnes qui n'auront pas l'occasion de répondre à tout le groupe, comme une invitation à un évènement ou un appel à témoins, mettez toutes les adresses dans le champ « Cci » (=Copie Carbone Visible, appellé également copie cache). Certains logiciels en anglais nomment ce champ Bcc (Blind Carbon Copy). C'est à cause de personnes qui ne le font pas que vous pouvez parfois commencer à recevoir des spams sur votre courriel alors que vous n'avez rien fait de mal.

Parfois, les chaînes utilisent la superstition en prétendant qu'il se fait pas suivre, un cycle sera rompu et que des événements atroces se produiront. Ne vous laissez pas impressionner : aucun message n'a l'air de pouvoir.

Il devrait être possible de faire une demande de renseignements personnels au bancaire. N'envoyez jamais d'image de vos papiers d'identité à un tiers qui vous en fait la demande dans un message.

Enfin, garder à l'esprit que les cyber-escroquerie servent à financer des activités criminelle : si jamais vous êtes victime d'une escroquerie, allez porter plainte.

Même si les pirates se trouvent dans un pays lointain, il faut que l'on connaisse le plus précisément possible les chiffres de la cybersécurité pour mieux lutter contre elle.


Jean-Michel Lemoine, administrateur principal de l'association Cléair Taïti, membre du conseil d'administration de l'UICP et membre du conseil d'administration de l'UICP.
• Expert technique (info, cybersécurité, prévention, formation, conseil, audit, étude, recherche, développement, enseignement,...)
• Responsable de projets
• Coordinateur de réseaux
• Membre de comités (Comité national de sécurité, Comité de sécurité, Comité de prévention, Comité de formation, Comité de recherche,...)

Le Net Expert
Cyber-Sécurité

[Regarder à cet article](#)

Source

http://www.tahiti-infos.com/Clusir-Ne-relayez-pas-les-spams-ca-nulars-chaines-de-lettres_a121624.html

Nos ordinateurs ont-ils la mémoire courte ? Vidéo



Nos
ordinateurs
ont-ils la
mémoire
courte ?
Vidéo

Que trouveront les archéologues du futur, d'ici quelques siècles ou quelques milliers d'années ? Des pierres taillées du paléolithique, des hiéroglyphes, des rouleaux de parchemins probablement, des livres peut-être.

Quelles images, quels sons, quels écrits de notre société restera-t-il dans 2000 ans ? Auront-ils résisté aux épreuves du temps et aux mutations technologiques comme l'ont fait la première photo, le premier film, le premier enregistrement sonore. Mais que deviendront les milliards d'informations engrangées dans les disques durs qui se démagnétisent, et sur les CD ou DVD, qui redoutent la lumière du soleil ?[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 ;

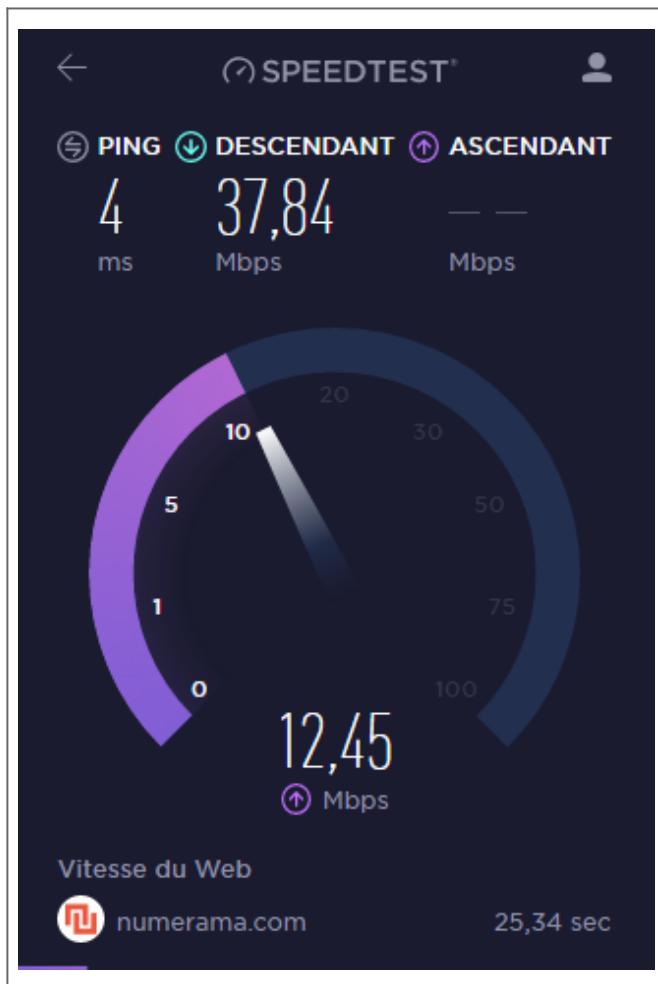
Source : *Nos ordinateurs ont-ils la mémoire courte ?*

Les objets connectés représentent-ils un risque ?

| Denis JACOPINI

 Les #objets connectés représentent-ils un risque ?

Comment mesurer et tester le débit de votre connexion internet | Denis JACOPINI



Comment mesurer
et tester le
débit de
votre connexion
internet

Internet c'est bien. Quand c'est rapide, c'est mieux. Nous vous avons listé quelques outils indispensables pour mesurer votre débit, que vous soyez chez Free, SFR, Orange, Numericable ou Bouygues.

On entend souvent dire qu'aujourd'hui on ne peut plus vivre sans Internet. Cette affirmation est fausse. Dire qu'on ne peut plus vivre sans **bonne** connexion Internet serait plus juste. Et justement, pour connaître la qualité de votre bande passante, il existe quelques outils extrêmement simple d'utilisation. Petit tour d'horizon des indispensables pour ceux qui ne les connaîtraient pas.

SPEEDTEST

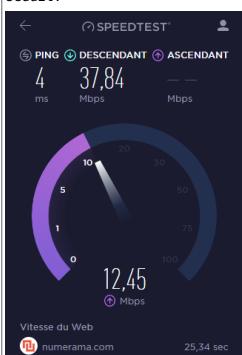
C'est le plus connu des outils présentés ici. Speedtest est complet et calcule votre débit montant et descendant ainsi que le temps de latence. Vous avez ainsi en main absolument toutes les informations en main pour connaître la vitesse de votre connexion. On regrette seulement le temps assez long que peut prendre un test (environ 47 secondes) et l'interface qui manque de sobriété.



Cela devrait bientôt changer grâce à la version HTML5 – encore en version beta – plus simple et efficace. Attention, celle-ci ne fonctionne pas lorsque le bloqueur de publicité est activé. Speedtest se décline également en application mobile pour profiter des mêmes fonctionnalités sur son smartphone.

EXTENSTON 00K1 A

EXTENSION OOKLA
Cet outil est extrêmement pratique. Ookla, l'entreprise qui a créé Speedtest, a sorti une extension Chrome rapide et ergonomique. À l'instar du site Internet, elle calcule le download, l'upload et le ping. Le test est réalisé en un peu moins de 30 secondes mais c'est surtout par son extrême simplicité d'utilisation que l'extension séduit.

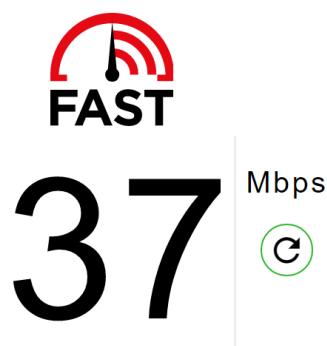


En effet, pas besoin de taper l'adresse d'un site ou de lancer une recherche Google. Un simple clic en haut à droite de votre navigateur suffit à y accéder. Ainsi, si vous remarquez certaines lenteurs de connexion, pas besoin d'attendre une éternité avant d'accéder à la page qui pourra vous confirmer que votre débit est pourri. Vous pouvez d'ailleurs fermer la fenêtre de l'extension, celle-ci continuera à faire le test de débit discrètement.

Malheureusement pour tous ceux qui n'utilisent pas le navigateur web de Google, l'addon Ookla est disponible uniquement sur Chrome.

Mathieu eusement
FAST.COM

En moins de dix secondes, Fast.com calcule votre vitesse de téléchargement (débit descendant uniquement). Si vous n'en avez rien à faire du temps de latence ou que vous n'avez rien à uploader, il s'agit du site idéal.



Ce site est en accord avec la vision de Netflix, son créateur, qui s'adresse plus aux internautes qui consomment plutôt qu'à ceux qui produisent. Ainsi, si vous ne surfez sur le web que pour consulter et télécharger des fichiers, Fast.com représente la meilleure solution. Le service en HTML 5 fonctionne aussi bien sur PC que sur mobiles, smart TV ou tablettes.

Article original de Omar Belkaab



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contenus, détournements de clientèle...);
 - Expertises de systèmes de vote électronique ;
 - Formations et conférences en cybercriminalité ;
 - Formation de C.I.L. (Correspondants Informatique et Libertés) ;
 - Accompagnement à la mise en conformité CNIL de votre établissement.

Attention, l'employeur peut lire les SMS des téléphones professionnels | Denis JACOPINI

23

Attention, l'employeur peut lire les SMS des téléphones professionnels

Une décision de la Cour de cassation permet désormais à une entreprise de lire les messages reçus et envoyés sur un téléphone professionnel. Comme elle pouvait déjà le faire avec les e-mails.
Gare aux sanctions si vous refusez l'accès à vos SMS à votre employeur.

Appelée à statuer sur le litige opposant deux sociétés de courtage, la Cour de cassation a pris une décision qui va concerner des centaines de milliers de salariés : elle a validé le principe selon lequel les SMS envoyés ou reçus par un téléphone mis à la disposition par une entreprise sont « présumés avoir un caractère professionnel ». Par conséquent, les employeurs sont autorisés à lire ces messages, même hors de la présence des salariés.

« Cet arrêt est dans la droite ligne de décisions prises depuis quelques années, nous explique Olivier Iteanu, avocat à la cour d'appel de Paris. Peu à peu la jurisprudence en vient à plus protéger l'entreprise que le salarié. »

L'avocat rappelle ainsi qu'en 2012, un employeur avait été autorisé à consulter le contenu de la clé USB d'un salarié car celui-ci l'avait branchée sur le système informatique de l'entreprise. Un an plus tard, la Cour de cassation confirmait que les employeurs pouvaient consulter les e-mails de la boîte professionnelle de leurs salariés, même hors de leur présence, s'ils n'étaient pas identifiés comme personnels.

Concrètement, grâce à la décision prise en ce mois de février 2015, un employeur ayant « un motif légitime » peut vérifier les SMS en prenant le téléphone de son salarié ou « placer, en passant par des outils de Mobile Device Management (gestion de terminaux mobiles), des logiciels qui vont monitorer ce qui se passe sur le smartphone, pour en extraire les SMS qui pourront être analysés », nous précise Jean Pujol, manager au sein de l'entité conseil en stratégie SI du cabinet Kurt Salmon. « Les SMS peuvent aussi être stockés sur des serveurs centraux, comme cela était le cas dans l'affaire jugée par la Cour de cassation. »

Refuser le contrôle entraînera une sanction

Pour Me Martine Ricouart-Maillet, vice-présidente de l'Association française des correspondants à la protection des données personnelles et associée au sein du cabinet BRM Avocats, « afin d'éviter tout litige, le salarié doit être informé de l'usage qu'il peut faire des outils mis à sa disposition dans la charte informatique de l'entreprise. Cette charte doit aussi l'avertir des moyens de surveillance dont dispose son employeur. »

« Et s'il refuse de se soumettre à ce contrôle, ajoute Me Iteanu, le salarié pourra être sanctionné. » La sanction « suprême » étant le licenciement. Pour lui, cette décision risque d'induire des comportements abusifs de la part de certains employeurs. « Les juges devront très probablement se saisir de cas pour rétablir l'équilibre entre les parties », estime-t-il.

La seule solution pour protéger certains SMS est de les identifier comme personnels. Même si cela n'interdit pas à l'employeur de les lire, cela l'empêche de les utiliser contre un employé. Autre méthode, plus radicale : disposer de deux appareils, un professionnel et un personnel.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source :

<http://www.01net.com/editorial/646337/attention-votre-employeur-va-pouvoir-lire-les-sms-de-votre-telephone-pro/>
Par Cécile Bolesse