Vidéoprotection / vidéosurveillance : le public doit-il être informé qu'il est filmé ? | Denis JACOPINI

Vidéoprotection / vidéosurveillance : le public doit-il être informé qu'il est filmé ?

Les personnes filmées dans un espace public (rue, administration, gare, centre commercial, banque etc.) doivent en être informées, au moyen de panneaux affichés de façon visible comportant :
• Un pictogramme représentant une caméra
• Le nom ou la qualité et le numéro de téléphone du responsable
Ces panneaux doivent être affichés en permanence dans les lieux concernés et doivent être compréhensibles par tous les publics.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.
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 plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=514319E089C032799DD14161D6197C4C?name=Vid%C3%A9oprotection%2Fvid%C3%A9osurveillance+%3A+le+public+doit-il+%C3%AAtre+inform%C3%A9+qu%27il+est+film%C3%A9+%3F&id=409

Attaque informatique TV5 Monde – Denis JACOPINI

interviewé par un journaliste de Canal Plus pour le JT de Direct8 | Denis JACOPINI

	Attaque informatique TV5 Monde - Denis JACOPINI interviewé par un journaliste de Canal Plus pour le JT de Direct8

A la suite de l'attaque informatique ayant visé TV5 Monte, le 9 avril dernier, pendant qu'il se trouvait à un Colloque international sur la Cybercriminalité à Montpellier organisé par Adel JOMNI, Denis JACOPINI a été interviewé par un journaliste de Canal Plus et certains propos retenus pour le JT de 20h45 sur Direct 8.

D'après-vous, pourquoi les pirates ont choisi la chaîne de télévision TV5 Monde comme cible de leur attaque informatique ?Lorsque des pirates ou des cybercriminels décident d'attaquer un système informatique, il le font principalement pour les raisons suivantes :- A la suite d'une sorte de défi qu'ils se sont lancés afin de prouver leur capacité à pirater un système qui s'est par exemple déclaré comme système inviolable…- Afin de récolter de l'argent soit en menaçant de diffuser des informations secrètes, soit en vendant les informations piratées, soit en prenant en otage un serveur en le bloquant et tout cela, contre rançon.

– Ou bien, dans le but de diffuser un message idéologique, prônant un message politique, religieux… Dans ce cas, l'objectif premier des cyber-attaquants est la diffusion à grande échelle d'un message (c.f. les deffaçages de plus de 25000 sites Internet à la suite des attentats contre Charlie Hebdo). Que le plus de personnes possibles puisse prendre connaissance d'un message en y associant une sensation de puissance, tel a été le type d'attaque contre TV5 Monde. Cette attaque, a été destinée avant tout à diffuser un message idéologique, en touchant un média à couverture mondiale pour qu'on parle le plus possible des attaquant et de leur symbole.

Quelle a été la technique utilisée lors de l'attaque des serveurs de TV5 Monde ?

Les cybercriminels utilisent généralement 2 types de méthodes pour pénétrer dans un système informatique :

– la recherche de failles

– la naïveté d'un destinataire à un e-mail

C'est un voire même plusieurs e-mails, de type phishing qui semblent être à l'origine, depuis probablement plusieurs semaines ou mois, de l'intrusion du système informatique de TV5 monde par les cybercriminels. Une fois introduits dans le système informatique, l'accès invisible ou silencieux à des informations confidentielles ou secrètes permet ensuite de trouver les clefs autorisant de se répandre dans un réseau et contaminer ainsi le plus possibles d'organes sensibles ou stratégiques.

Une fois tous ces accès ainsi possibles, il suffit de coordonner une attaque simultanée de tous ces fruits devenus véreux pour donner l'impressionnante vision d'un arbre prêt à tomber.

« Il suffit d'envoyer tous les jours un email avec un virus auprès de différentes personnes de différents services et à un moment ou un autre il va bien y a voir quelqu'un qui va l'ouvrir.

Son vrai travail va commencer lorsque quelqu'un aura mordu à l'hameçon »

Peut-on conclure que n'importe quelle chaines de télévision peuvent être victime de cyber-attaques telles que celle dont a été victime TV5 monde ?

La faille qu'ont exploité les cybercriminels dans le cadre de l'attaque informatique de TV5 monde est une faille humaine. En effet, recevoir un e-mail nous incitant à cliquer sur un lien qui va contre notre volonté et de manière complètement invisible changer dans son ordinateur un logiciel malveillant chargé, de manière tout aussi silencieuse, de prendre le contrôle de notre ordinateur est devenu le moyen d'attaque le plus utilisé.

Les systèmes informatiques des chaines de télévision sont certes équipées de moyens de protection techniques contre les virus, les codes malveillants et autres types d'attaques, mais les cybercriminels auront toujours un coup d'avance en exploitant la faille humaine, principalement par manque de connaissance ou manque de formation de la part des utilisateurs.

Existe t-il un moyen de se protéger contre ce type d'attaque ?

Les organismes et entreprises ont prix trop de retard pour mettre en place des politiques de sécurité informatique. Quand on voit qu'en 2013, moins de 100 000 entreprises en France s'étaient mises en conformité avec la CNIL, excellent point de départ pour mettre en place des mesures de sécurité sur les données personnelles, il y a de quoi s'inquiéter sur la manière dont nos données (mot de passe y compris) sont sécurisées.

Commencer par se mettre en conformité avec la CNIL serait un bon début…

http://www.lenetexpert.fr/wp-content/uploads/2015/04/Denis-JACOPINI-interviewé-par-journaliste-Canal-plus-pour-JT-de-Direct-8.mp4

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 protection juridique du chef d'entreprise.

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://www.bfmtv.com/culture/l-attaque-contre-tv5monde-enclenchee-des-fin-janvier-877334.html

Comment gérer les licences des logiciels installés par les salariés ? | Denis JACOPINI

Comment gérer les licences des logiciels installés par les salariés ?

Dès que l'on souhaite accueillir les terminaux personnels des collaborateurs dans l'entreprise, il faut absolument se pencher sur la question des licences logicielles pour éviter de cuisantes déconvenues.

Dès qu'un logiciel est présent, les risques liés aux licences sont forcément tapis dans l'ombre. Si l'on souhaite accueillir les terminaux personnels des collaborateurs avec un projet BYOD (Bring Your Own Device), il faut donc se pencher sur la question pour éviter de cuisantes déconvenues. Il en va de même avec les petits logiciels gratuits que les employés peuvent installer sur les équipements fournis par l'entreprise, qu'ils en soient ou non administrateurs.

Ces deux exemples, aussi concrets que courants, offrent quelques clefs pour mieux maîtriser un phénomène dont la complexité et l'ampleur ne cessent de croître.

Bring your own licence illégale

Si l'on ne parvient pas à endiguer un phénomène, autant en tirer profit. C'est notamment le cas avec ces équipements informatiques personnels que les employés introduisent discrètement dans les systèmes d'information d'entreprise depuis des années. Las de lutter, les DSI cèdent à une nouvelle mode : le BYOD (Bring Your Own Device).

Certains se contentent de canaliser ces terminaux hétéroclites en veillant à la survie des équipes de support et à la sécurité de l'information : pas de support technique, connexion sur les accès Wi-Fi pour visiteur, etc. D'autres vont plus loin, comme dans cette grande organisation du secteur tertiaire dont je tairai le nom :

· Les collaborateurs peuvent utiliser leur matériel préféré à la place de celui fourni par la DSI ;
· Ils doivent alors y installer l'antivirus homologué dont une licence leur est allouée ;
· S'ils restituent le PC de la compagnie pour n'utiliser que le leur, ce dernier est subventionné ;
· En pareil cas, ils sont livrés à eux-mêmes en termes d'assistance et de logiciels ;
· Ils peuvent cependant bénéficier de l'accord passé avec Microsoft pour acquérir une licence Office à 13 €.

Remarquable exemple de modernité et d'ouverture, qui permet au passage de réduire les coûts de matériel, de logiciel et de support. Le tout est savamment enrobé d'une communication du plus bel effet vantant les mérites d'une transformation digitale soucieuse des collaborateurs et de leur bien-être.

Comme d'habitude, le diable est dans les détails, en l'occurrence dans les conditions d'utilisation de la licence Microsoft Office à 13 €. En effet, elle couvre l'usage secondaire du logiciel sur un PC personnel si une licence entreprise est octroyée à l'utilisateur. Dans notre cas, l'utilisateur n'a plus de licence entreprise puisqu'il l'a restituée en même temps que son PC.

Voilà comment une organisation peut pousser ses collaborateurs à agir illégalement, sans s'exposer directement puisque les logiciels et les terminaux incriminés ne lui appartiennent pas. Les employés mis en défaut par Microsoft pourront cependant prouver qu'ils ont respecté les préconisations relayées par leur hiérarchie. Il n'est pas certain que cela engendre l'atmosphère voulue : décontractée et propice au travail.

La gratuité peut coûter cher

Une autre situation classique, en apparence anodine, peut faire des remous si l'on n'y prend pas garde : les logiciels gratuits, si pratiques et si sympathiques.

Ainsi, un collègue m'a récemment présenté les bienfaits d'un petit freeware qui le comblait d'aise. Il m'a vivement conseillé de l'installer sur mon PC professionnel. Je l'ai donc téléchargé depuis le site de l'éditeur. Avant de lancer l'installation, j'ai lu les conditions d'utilisation (vous auriez évidemment fait la même chose à ma place). Au milieu de cette prose, j'ai découvert que le produit ne devait pas être utilisé en entreprise. Que l'on travaille sur un terminal personnel ou mis à disposition par la DSI ne change rien puisqu'il s'agit toujours d'un usage « en entreprise ». Utiliser ainsi la version gratuite du logiciel est donc illégal.

Disposer des droits d'administrateur sur son ordinateur n'est pas forcément nécessaire pour installer un tel produit. L'entreprise peut donc se retrouver dans une posture inavouable, même si elle a correctement sécurisé son parc informatique. Pour mettre un peu de piment, ajoutons que ces installations occultes passent inaperçues lors des inventaires logiciels, puisqu'ils sont le plus souvent conçus pour détecter ce qui est connu, et non pour découvrir l'inconnu.

De nos jours, les logiciels communiquent presque tous avec leur éditeur via Internet au moyen de protocoles réseau qui franchissent allègrement les dispositifs de sécurité. Il peut s'agir de rechercher des mises à jour ou de fournir des données vous concernant. C'est légal puisque spécifié dans le contrat de licence accepté *de facto* lors de l'installation, qu'il ait été lu ou non. Il suffit alors d'un nombre significatif de PC communiquant depuis votre réseau d'entreprise pour mettre la puce à l'oreille de l'éditeur. Il a alors tout le loisir de vous retrouver grâce à vos adresses IP publiques et de réclamer le manque à gagner en faisant jouer la clause d'audit inscrite, elle aussi, aux conditions générales d'utilisation. Elle lui offre en effet la possibilité de contrôler votre système d'information pour vérifier que les logiciels utilisés sont dûment payés.

Les petits logiciels gratuits peuvent ainsi coûter fort cher à des DSI qui en ignoraient jusqu'à l'existence car les grands éditeurs ne sont plus les seuls à développer leurs ventes par un nouveau canal : l'audit.

L'effort fait les forts

Ces deux cas d'école montrent que la compréhension des contrats de licences est indispensable pour éviter des complications désagréables. C'est par ailleurs un préalable à la gestion des actifs logiciels (Software Asset Management, SAM). Comment, en effet, maîtriser le droit d'usage contractuel d'un produit dont on ignore le contrat ?

En ces temps de crise, la chasse au manque à gagner est ouverte pour de nombreux éditeurs. Tout changement impliquant l'informatique concerne forcément des composants logiciels. Il convient donc d'être prudent et de prendre en considération leur dimension contractuelle. Bien des projets ont vu leur retour sur investissement réduit à néant, voire inversé, après un audit d'éditeur.

En définitive, qu'il s'agisse d'adopter le BYOD, d'utiliser un freeware ou de transformer le système d'information, le SAM renforce la position du client face aux éditeurs de logiciels car, comme disait Marcel Pagnol : « Comme on est faible quand on est dans son tort ! »… [Lire la suite]

Réagissez à cet article

Source : *BYOD et freewares : quid des licences ? – JDN*

Les TPE et les PME, cibles privilégiées des cybercriminels | Denis JACOPINI

Les TPE et les PME, cibles privilégiées des cybercriminels

Selon le spécialiste de la sécurité Symantec, 71 % des TPE et les PME qui font l'objet d'une cyber-attaque ne s'en remettent pas. Pourtant, la sécurité du système informatique ne fait pas partie des priorités des petites et moyennes entreprises, même si c'est un enjeu majeur pour leur survie.

Face à des systèmes d'information de plus en plus ouverts, un usage généralisé d'internet et des terminaux mobiles connectés, les entreprises doivent mettre en œuvre des politiques de sécurité informatique de plus en plus exigeantes. Pourquoi les cybercriminels s'en prennent d'avantage aux TPE et aux PME ? Explication.

La cybercriminalité n'est pas un fait nouveau. Pourtant depuis quelques années, nous sommes tous devenus ultra-connectés et multi-équipés. Ce constat n'épargne pas les entreprises qui ont vu apparaître de nouveaux outils qui permettent aux salariés de rester connecter en étant plus mobile et plus productif. Ces nouveaux modes de travail, sont aujourd'hui autant de failles de sécurité possibles et donc d'attaques possibles. Cette forme de criminalité ne concerne plus les grandes entreprises qui ont majoritairement mis en place des moyens coûteux pour lutter contre le piratage. La nouvelle cible privilégiée des hackers serait les TPE et les PME qui seraient plus simple à attaquer.

Des cibles plus accessibles

Les enquêtes le confirment : les gérants de TPE et PME ont une vision assez exacte du piratage informatique, mais ils se sentent peu concernés. Selon eux, cette forme moderne de criminalité menace surtout les grandes entreprises. Pourtant, les délits constatés contredisent cette perception. Plus encore, le pourcentage des attaques vers les entreprises de moins de 250 salariés progressent. Selon le rapport Symantec Security Threat, elles seraient passées de 18% à 31% en 4 ans. Or ce sont justement les entreprises de moins de 250 salariés qui doivent protéger leurs données. Le constat est le suivant : 40% de la valeur des entreprises est issue des informations qu'elles détiennent. Ce qui intéresse les cybercriminels : dossiers clients, listes de contacts, renseignements sur le personnel et informations bancaires de l'entreprise, cartes de crédit comprises et propriétés intellectuelles. Elles représentent aussi des passerelles d'accès à leurs partenaires.

Un frein pour travailler avec les grandes entreprises

Loin des considérations financières et ne se sentant pas concernées, les TPE et PME s'estiment à l'abri de ces attaques. En conséquence, leurs infrastructures ne sont pas adaptées. Elles sont alors des cibles idéales permettant d'attaquer leurs différents partenaires qui sont parfois des grandes entreprises ou des administrations. Elles deviennent alors un moyen d'accéder à leurs systèmes d'information. Et cela peut constituer un frein à la compétitivité. Les Grandes Entreprises, ne pouvant contrôler le système d'information de leurs partenaires, exigent alors de leurs sous traitants un matériel informatique similaire afin de contrôler les flux.

Des attaques virales invisibles

Les attaques les plus fréquentes sont de natures virales. A l'insu des utilisateurs, elles visent à installer de petits programmes capables d'identifier les mots de passe (via des enregistreurs de frappe), d'accéder aux services bancaires en ligne de l'entreprise (Chevaux de Troie bancaires), de contrôler à distance les ordinateurs de l'entreprise pour lancer des attaques commandées (réseaux de zombies ou botnet) ou d'espionner les employés pour connaître leurs habitudes, leurs mots de passe ou leurs préférences (Spyware)…

De nouvelles attaques plus structurées

Les techniques de piratages évoluent et le matériel n'est plus l'unique faille. On voit apparaître de nouveaux types d'attaques basées sur les failles humaines et sociales. Les environnements de travail des salariés sont ciblés à travers les postes de travail des salariés. A titre d'exemple, les hackers identifient le lien entre les entreprises et leurs partenaires. Des mails sont envoyés depuis les réseaux sociaux type Linkedin ou Viadéo au nom du partenaire. L'email sera donc ouvert sans réel méfiance de la part du salarié. Cette technique, appelée « social engineering », permet alors au pirate d'accéder au poste de travail de l'utilisateur en premier lieu pour ensuite évoluer dans le système d'information de l'entreprise.

Des règles simples de cyber-stratégie

Il n'est pas rare qu'en entreprise les salariés utilisent des outils réservés aux particuliers. Ce type de pratique multiplie les dangers d'intrusion car les systèmes peuvent être piratés. Ils pointeraient vers l'installation de « maliciels » (logiciels malveillants conçus pour infiltrer un ordinateur et y réaliser des activités non autorisées). Il en est de même pour tous les outils connectés. Malheureusement, ce n'est souvent qu'une question de temps avant qu'un hacker arrive à ses fins. Il est donc primordial de faire preuve de plus de rigueur pour gagner du temps afin de décourager l'intrusion. Une entreprise qui connait les risques et montre qu'elle a pris des mesures de sécurité simples, décourage les pirates. Il existe aujourd'hui des services de sécurité informatiques adaptés aux TPE/PME. A titre d'exemple, des prestataires proposent des offres sous forme de machine virtuelle, un proxy complet et simple. Le service permet de filtrer les pages internet en se basant sur des listes préétablies.

Mais bien avant de se consacrer à la sécurisation du matériel de travail, la première mesure à prendre concernera celle des bonnes pratiques des salariés. Des mesures de protection humaines sont nécessaires. « Il est surtout important de sensibiliser ses collaborateurs aux bonnes pratiques », assure Philippe Trouchaud, associé PricewaterhouseCoopers, spécialiste de la cyber sécurité. Le gouvernement met à disposition un Guide d'Hygiène et de Sécurité de l'ANSSI, il fournit les bases de la sécurité pour les utilisateurs au sein des entreprises.

Aussi une politique de sécurité consistera tout d'abord à mener de front trois actions :
• Identifier les points de vulnérabilité généralement utilisés par les criminels informatiques pour s'introduire dans les systèmes d'information,
• Définir les règles de prudence à appliquer au quotidien par l'entreprise et son personnel,
• Mettre en œuvre systèmes de protection électroniques adéquats. Le tout devant être organisé et planifié dans la durée.

Comment recevoir moins d’appels téléphoniques publicitaires ? | Denis JACOPINI

Comment recevoir moins d’appels téléphoniques publicitaires ?

Règle n° 1 : ne communiquez pas votre numéro de téléphone lors d'un achat ou d'un contact commercial sauf si c'est indispensable (par exemple, pour la livraison).Règle n° 2 : signaler au commerçant que vous ne souhaitez pas que votre numéro soit réutilisé à des fins publicitaires.

Il existe également des listes d'opposition sur lesquelles vous pouvez vous inscrire gratuitement :

• La liste rouge :

Vos coordonnées ne sont pas publiées dans l'annuaire et ne sont pas communiquées par les services de renseignement téléphonique. Contactez votre opérateur télécom.

• La liste orange ou « anti prospection » :

Vos coordonnées sont publiées dans l'annuaire et sont communiquées par les services de renseignement téléphonique. En revanche, elles ne peuvent pas être utilisées pour du démarchage publicitaire. Contactez votre opérateur télécom.

• Liste anti annuaire inversé :

Elle empêche que l'on puisse trouver votre nom ou votre adresse à partir de votre numéro de téléphone fixe ou mobile. Contactez votre opérateur télécom.

A savoir : Votre opérateur telecom peut vous adresser des appels commerciaux sur ses produits et services, même si vous êtes inscrits sur liste rouge ou anti prospection. Pour vous y opposer, contactez votre opérateur.

La liste PACITEL

Vous ne serez plus démarché par les sociétés adhérantes à l'association Pacitel.

MISE A JOUR DU 13/10/2016 :

La liste PACITEL n'existe plus depuis le 1er janvier 2016, elle a été remplacée par BLOCTEL en juin 2016.

Consultez nos infos sur Bloctel : https://www.lenetexpert.fr/bloctel-la-nouvelle-liste-rouge-contre-les-spams-telephoniques

Autre lien : https://www.service-public.fr/particuliers/actualites/A10590

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. 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

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 plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : http://www.aide.cnil.fr/selfcnil/site/template.do?id=112&back=true

Que faire en cas de fraude sur sa carte bancaire ?

Que faire en cas de fraude sur sa carte bancaire ?

De plus en plus d'usagers de la banque sont victimes de l'utilisation frauduleuse de leur carte alors même qu'ils ne l'utilisent pas pour leur achat sur le net. Pourtant il arrive de plus en plus fréquemment que certains d'entre eux constatent des sommes prélevées sur leur compte bancaire en consultant leur relevé bancaire.

Que faire en cas de fraude sur sa carte ? Quelles sont les démarches pour déclarer une utilisation frauduleuse de sa carte bancaire ?

Selon les disposition de l'article L 133-24 du Code Monétaire et Financier, la responsabilité du propriétaire d'une carte bancaire n'est pas engagée dans le cas où la carte a été contrefaite ou si l'achat contesté n'a pas été effectué avec l'utilisation physique de la carte.

Les titulaires de carte victimes d'une utilisation frauduleuse sur Internet ont un délai de 13 mois pour contester les sommes prélevées sur leur compte bancaire. Ils doivent se rendre auprès de sa banque et s'opposer formellement aux transactions effectuées ou au paiement des opérations en question.

Quelles sont les démarches à faire auprès de sa banque ?

En cas d'usurpation des données de sa carte bancaire, il faut :

• Appeler sa banque le plus rapidement possible pour le signaler par téléphone.

• Envoyer à sa banque une lettre qui confirme la mise en opposition de la carte utilisée frauduleusement,

– Un document qui décrit toutes les opérations contestées, les coordonnées bancaires et le motif de l'opposition de la carte,

– Une attestation (AFFIDAVIT) certifiant que la carte a toujours été en sa possession et qu'elle n'a jamais été cédée ou prêtée.

La loi de 2001 sur la protection du consommateur n'exige pas de dépôt de plainte auprès de la gendarmerie. Il n'est donc pas nécessaire de porter plainte pour que la banque procède aux remboursement des sommes usurpées.

Selon les articles L133-19 et L 133-20, la banque doit rembourser toutes les sommes prélevées à compter de la date d'opposition ainsi que tous les frais liés à l'opposition de la carte bancaire.

Pour éviter une usurpation de sa CB, voici quelques conseils et certaines mesures de sécurité à prendre :

– ne jamais laisser la carte bancaire à la vue d'un quelconque public (ex :
– exposée la CB dans la voiture ou sur un bureau),

– penser à reprendre sa carte bancaire dans les terminaux de paiement après chaque achat,

– détruire les tickets de paiement avant de les jeter car ils comportent le code de la carte bancaire,

– ne jamais dire le numéro ni le code secret de la carte bancaire à quiconque,

– ne pas oublier de signer au dos de la carte bancaire.

Source : Banque-en-ligne.fr *Que faire en cas de fraude sur sa carte bancaire ?*

LE NET EXPERT

• ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)

- **ANALYSE DE VOTRE ACTIVITÉ**
- **CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES**
- **IDENTIFICATION DES RISQUES**
- **ANALYSE DE RISQUE (PIA / DPIA)**
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements

• FORMATIONS / SENSIBILISATION :

- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**

• RECHERCHE DE PREUVES (outils Gendarmerie/Police)

- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES

• EXPERTISES & AUDITS (certifié ISO 27005)

- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

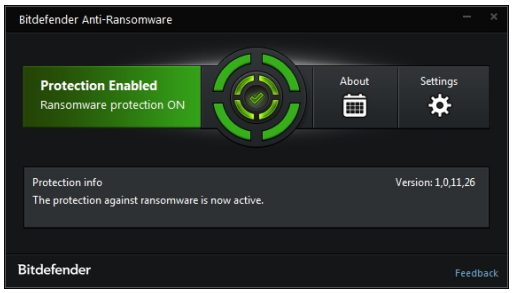
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

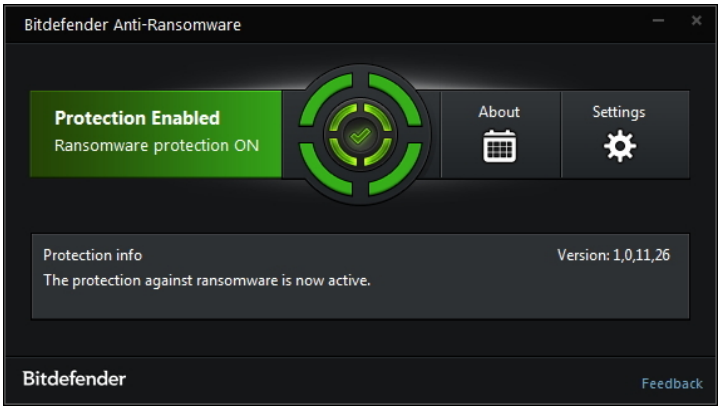
Comment protéger votre

ordinateur du virus Locky avec un outil Gratuit ? | Denis JACOPINI



Comment protéger votre ordinateur du virus Locky avec un outil Gratuit ?

Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.



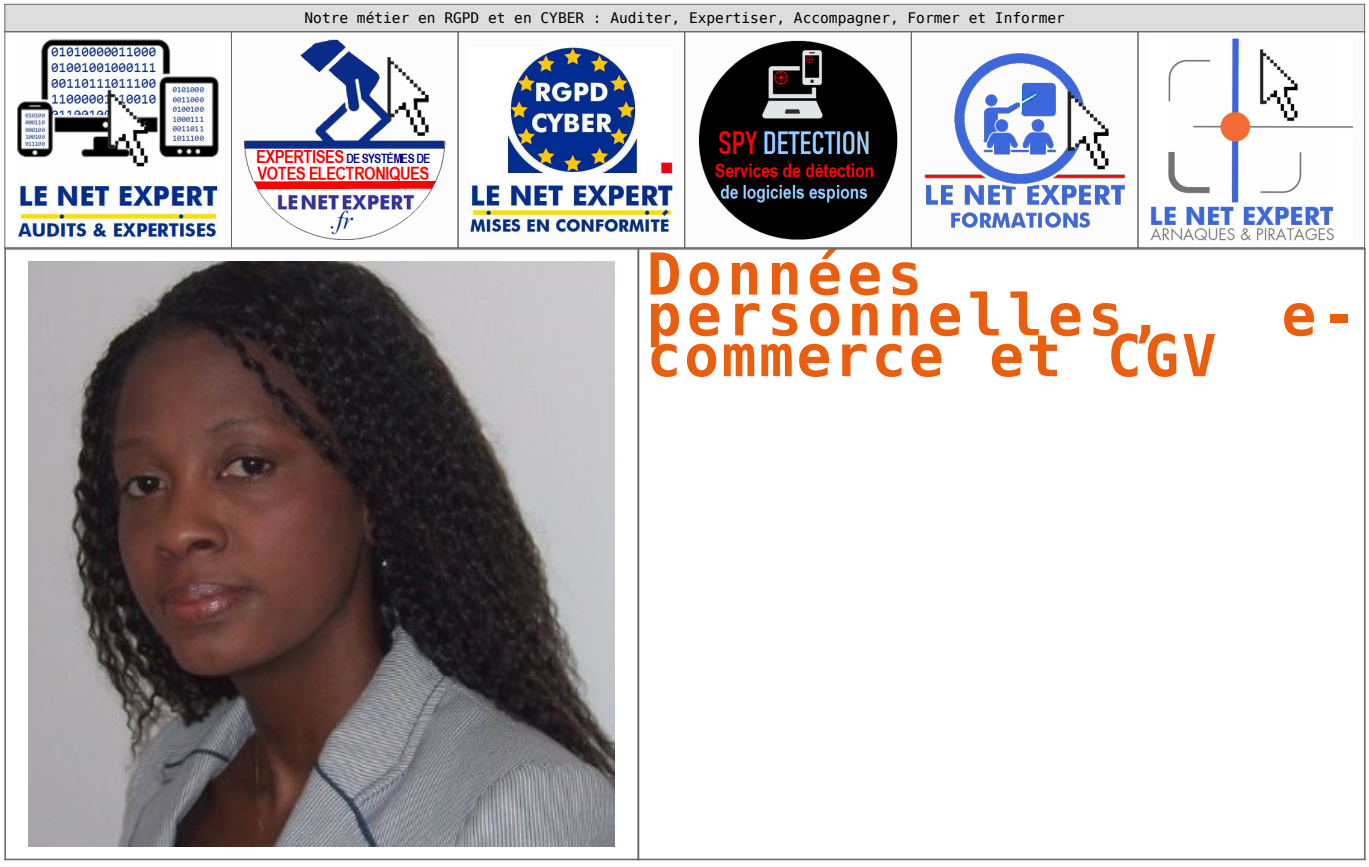
Antivirus firm Bitdefender has released a free tool that can prevent computers from being infected with some of the most widespread file-encrypting ransomware programs: Locky, TeslaCrypt and CTB-Locker.

The new Bitdefender Anti-Ransomware vaccine is built on the same principle as a previous tool that the company designed to prevent CryptoWall infections. CryptoWall later changed the way in which it operates, rendering that tool ineffective, but the same defense concept still works for other ransomware families.
While security experts generally advise against paying ransomware authors for decryption keys, this is based more on ethical grounds than on a perceived risk that the keys won't be delivered.
In fact, the creators of some of the most successful ransomware programs go to great lengths to deliver on their promise and help paying users decrypt their data, often even engaging in negotiations that result in smaller payments. After all, the likelihood of more users paying is influenced by what past victims report.
Many ransomware creators also build checks into their programs to ensure that infected computers where files have already been encrypted are not infected again. Otherwise, some files could end up with nested encryption by the same ransomware program.
The new Bitdefender tool takes advantage of these ransomware checks by making it appear as if computers are already infected with current variants of Locky, TeslaCrypt or CTB-Locker. This prevents those programs from infecting them again.
The downside is that the tool can only fool certain ransomware families and is not guaranteed to work indefinitely. Therefore, it's best for users to take all the common precautions to prevent infections in the first place and to view the tool only as a last layer of defense that might save them in case everything else fails.
Users should always keep the software on their computer up to date, especially the OS, browser and browser plug-ins like Flash Player, Adobe Reader, Java and Silverlight. They should never enable the execution of macros in documents, unless they've verified their source and know that the documents in question are supposed to contain such code.
Emails, especially those that contain attachments, should be carefully scrutinized, regardless of who appears to have sent them. Performing day-to day activities from a limited user account on the OS, not from an administrative one, and running an up-to-date antivirus program, are also essential steps in preventing malware infections.
« While extremely effective, the anti-ransomware vaccine was designed as a complementary layer of defense for end-users who don't run a security solution or who would like to complement their security solution with an anti-ransomware feature, » said Bogdan Botezatu, a senior e-threat analyst at Bitdefender, via email… [Lire la suite]

Réagissez à cet article

Source : *Free Bitdefender tool prevents Locky, other ransomware infections, for now | Computerworld*

Données personnelles, e-commerce et CGV. Par Sarah Garcia, Avocate. | Denis JACOPINI



Considérées comme le socle de la relation contractuelle, les #conditions générales de vente (CGV) désignent l'ensemble des clauses qui constituent l'offre émise par un vendeur professionnel à destination des acquéreurs potentiels de ses produits.

Avec le développement du commerce en ligne, la protection des données personnelles devient un enjeu important en termes d'image de l'entreprise, mais aussi et surtout en termes de confiance que l'utilisateur a dans le site. Comme le souligne la présidente de la CNIL, « la protection des données personnelles est un avantage concurrentiel pour les entreprises ».
La protection des données personnelles est au cœur du fonctionnement du site e-commerce, à travers le recueil d'informations relatives à l'identification des personnes (nom, adresse, numéro de téléphone, numéro de carte bancaire…)
La loi informatique et libertés du 6 janvier 1978 modifiée assure à travers une série de règles la protection de ces données personnelles. La création et le traitement de données à caractère personnel sont soumis à des obligations destinées à protéger la vie privée des personnes des prospects et les libertés individuelles.
Sans être exhaustif, nous allons aborder les règles qu'impose la CNIL dans le cadre du respect des #droits des clients, la durée de conservation de ces données personnelles, les règles applicables dans le cadre de la prospection commerciale, qui sont autant de domaines qui touchent à la protection des données personnelles.

1. Le respect des droits des clients
Les conditions générales de vente lorsqu'elles recueillent des données personnelles doivent mentionner les droits des personnes dont les données sont recueillies.
Les CGV doivent donc mentionner les procédés mis en œuvre par le site de e-commerce afin de garantir les droits de ces personnes.

Le droit d'être préalablement informé (article 32 de la loi Informatique et Libertés).
Le droit de consentir (article 7 de la loi informatique et libertés).
Le #droit d'accès (article 39, I, 4° de la loi informatique et libertés)
Le #droit de rectification (article 40 de la loi informatique et libertés)
Le #droit d'opposition (article 38 de la loi informatique et libertés).
En règle générale, une clause de ces conditions générales doit renvoyer aux conditions de mise en œuvre. Il est également possible de rédiger séparément une #politique de protection des données personnelles sur le site.

2. La #durée de conservation des données
La loi informatique et libertés prévoit qu'un traitement ne peut porter que sur des données à caractère personnel qui sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées (article 6, 5°).

En pratique, la CNIL recommande de respecter les durées suivantes :
Concernant les éléments d'identité des clients habituels et occasionnels : 5 ans à compter de la clôture du compte ou de la relation commerciale.
Concernant les documents et informations relatifs aux opérations faites par les clients. Il peut s'agir du dépôt, du retrait, des virements, des prélèvements, des opérations concernant les cartes. La durée de conservation est de 5 ans à compter de l'exécution de l'opération.
Toutes ces informations peuvent figurer aussi bien dans les conditions générales de vente que dans un document intitulé « politique de protection des données personnelles » et mis à la disposition des utilisateurs sur le site internet.

3. Le #recueil du consentement dans le cadre de la prospection commerciale et du parrainage
Cette prospection commerciale se fait généralement par voie électronique, appel téléphonique ou centre d'appel.
Le recueil du consentement du prospect est important. Le site d'e-commerce peut en effet s'exposer à payer une amende ou une peine d'emprisonnement.

En cas de prospections commerciales effectuées par voie postale, ou par appel téléphonique depuis un centre d'appel, l'envoi de publicité par voie postale est possible sous réserve que la personne soit, au moment de la collecte de ses coordonnées informée de leur utilisation à des fins de prospection et en mesure de s'opposer à cette utilisation de manière simple et gratuite. Telle est la préconisation de la CNIL. C'est le système de l'op out.

En matière de publicité par voie électronique, le principe en la matière est de recueillir l'accord préalable du destinataire. C'est le système de l'op in. La CNIL a ainsi récemment condamnée la Société Prisma Media a payé une amende de 15.000 euros pour envoi sans le consentement des prospects de lettres d'information électronique contenant de la prospection [1]

En effet, la CNIL subordonne l'envoi de publicité à des prospects par la voie électronique à un consentement. Dans la pratique, ce consentement doit être matérialisé par une case à cocher.

Toutefois des exceptions demeurent :
Si la personne prospectée est déjà cliente de l'entreprise et si la prospection concerne des produits ou des services analogues à ceux déjà fournis par l'entreprise.
Si la prospection n'est pas de nature commerciale.

Dans ces deux cas, la personne doit, au moment de la collecte de son adresse de messagerie :
– être informée que son adresse électronique sera utilisée à des fins de prospection,
– être en mesure de s'opposer à cette utilisation de manière simple et gratuite.

En ce qui concerne les professionnels, le principe est celui de l'information préalable et le droit d'opposition. Il faut ainsi que la personne soit informée que son adresse électronique est utilisée à des fins de prospection commerciale, et être en mesure de s'opposer à cette utilisation de manière simple et gratuite.

Le consentement doit être recueilli sans aucune ambiguïté. Ainsi, l'utilisation d'une case pré-cochée est à proscrire.
Le non-respect de ces dispositions est sanctionné par une amende de 750 euros par message expédié et 5 ans d'emprisonnement et 300.000 euros d'amende.

4. Le parrainage et les jeux concours
La recherche de nouveaux prospects, le site e-commerce peut organiser un système de parrainage ou des jeux concours. Ils ne sont pas interdits, mais il est nécessaire de respecter la protection des données personnelles.

a. Le parrainage
Qu'est-ce que le parrainage ? Il a pour objet de demander à une personne de renseigner les coordonnés d'un tiers qui peut être intéressé par une offre commerciale.
Comment respecter le droit relatif à la protection des données personnelles ? La CNIL précise que le destinataire de l'offre doit connaître l'identité de son parrain lorsqu'il est contacté par l'entreprise. Ensuite, les données du parrainé ne peuvent être utilisées qu'une seule fois pour lui adresser l'offre commerciale, l'article de presse ou l'annonce suggéré par le parrain. Enfin, l'entreprise ne pourra conserver les données du parrainé pour lui adresser d'autres messages que si elle a obtenu son consentement exprès.
Tout comme l'organisation des jeux concours, le parrainage ne doit pas être dilué dans les conditions générales de vente.

b. Les jeux concours
L'organisation des jeux concours est attractive et peut permettre de capter la clientèle. L'internaute doit pouvoir participer à un jeu concours sans être obligé de recevoir de la prospection.
La CNIL précise que les informations recueillies concernant le joueur ne peuvent être utilisées que dans le cadre du jeu et la remise du lot. Les coordonnées électroniques du participant ne peuvent pas être utilisées à des fins publicitaires, sauf consentement exprès de sa part.
Il est essentiel que le responsable du fichier reprenne les mentions de la loi « informatique et libertés » sur le formulaire de participation au jeu-concours. Il doit être remis au participant le règlement du jeu concours dans lequel figurera une rubrique « vie privée ».
La CNIL précise par ailleurs que le consentement préalable doit être recueilli par un moyen simple et gratuit, comme une case à cocher par exemple. Pour que le consentement soit valide, la case ne doit pas être « pré-cochée ».

5. La #gestion des cookies
a. Le cadre juridique applicable.
Le législateur européen a posé le principe (directive 2009/136/CE) d'un consentement préalable de l'utilisateur avant le stockage d'informations sur son équipement ou l'accès à des informations déjà stockées. Ce consentement préalable n'est pas nécessaire si les actions sont strictement nécessaires pour la délivrance d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

b. Quels sont les cookies concernés et nécessitant un consentement préalable ?
Sont concernés les traceurs déposés et lus par exemple lors de la consultation d'un site internet, de la lecture d'un courrier électronique, de l'installation ou de l'utilisation d'un logiciel ou d'une application mobile et ce, quel que soit le type de terminal utilisé tels qu'un ordinateur, un smartphone, une liseuse numérique et une console de jeux vidéos connectée à Internet. Il s'agit par exemple de cookies http, ou de cookie flash…
Ces obligations sont requises que les cookies collectent des données à caractère personnel ou non.
Pour les cookies nécessitant une information préalable et une demande de consentement, on peut notamment citer ceux liés aux opérations relatives à la publicité ciblée ; certains cookies de mesure d'audience ou encore les cookies des réseaux sociaux engendrés notamment par leurs boutons de partage lorsqu'ils collectent des données personnelles sans consentement des personnes concernées. Cette liste n'est pas exhaustive.
Il convient de souligner que le cookie de mesure d'audience est exempté dans certains cas de consentement de l'internaute.

c. La mise en conformité du site
L'obligation est donc double pour le site : une information préalable et un consentement préalable.
En règle générale, l'internaute doit avoir un affichage d'un bandeau d'information sur la première page du site visité.

Un modèle pourrait être libellé comme suit :
« En poursuivant votre navigation sur ce site, vous acceptez l'utilisation de [Cookies ou autres traceurs] pour vous proposer [par exemple, des publicités ciblées adaptés à vos centres d'intérêts] et (par exemple, réaliser des statistiques de visites]. »
Pour en savoir plus et paramétrer les traceurs : Source la CNIL.

En définitive, la politique de protection des données personnelles est un élément que le site e-commerce doit prendre en compte dans la rédaction des conditions générales de vente et dans la gestion de son site. Éléments essentiels et incontournables, les sites de e-commerce doivent intégrer cette réalité. Car un respect de ces obligations légales est aussi un outil marketing pour le développement de ces sites.

[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 : http://www.village-justice.com/articles/Donnees-personnelles-commerce-CGV,20003.html
Par Sarah Garcia, Avocate

Procédure à suivre pour demander l'aide juridictionnelle | Denis JACOPINI

	**Comment demander l’aide juridictionnelle** Il vous semble qu’un logiciel espion se cache dans votre iphone, votre smartphone, votre ordinateur, ou votre téléphone ? Vous soupçonnez être victime d’espionnage informatique ? Vous souhaitez utiliser les services d’un #expert informatique pour faire analyser votre appareil ? Avant d’engager les services d’un expert informatique,vérifiez si vous n’avez pas droit à une prise en charge par l’état de vos frais juridiques.

Vous êtes ou il vous semble être victime d’espionnage de votre ordinateur, de votre téléphone ou de votre smartphone ?

Vous souhaitez utiliser les services d’un expert informatique pour faire analyser votre appareil ?

Vous pouvez probablement bénéficier de l’aide juridictionnelle.

L’aide juridictionnelle, c’est quoi ?

L’aide juridictionnelle vous permet, si vous avez de faibles ressources, de bénéficier d’une prise en charge totale ou partielle par l’État des honoraires et frais de justice (avocat, huissier, expert, etc.).

Si la prise en charge par l’état est totale

Tous vos frais sont pris en charge, à l’exception du droit de plaidoirie fixé à **13 €** dû devant certaines juridictions et à payer à votre avocat.

Attention
Les sommes engagées avant la demande d’aide juridictionnelle ne sont pas remboursées.

Si la prise en charge par l’état est partielle

L’État ne prend en charge qu’une partie des honoraires d’avocat. Vous devez lui verser des honoraires complémentaires à fixer avec lui avant le procès.

Les autres frais relatifs aux instances, procédures ou actes pour lesquels l’aide juridictionnelle partielle vous a été accordée (frais d’expertise, d’enquête sociale, droit d’enregistrement, etc.) sont totalement pris en charge par l’État.

Remarque
L’aide juridictionnelle (totale ou partielle) ne couvre pas les frais auxquels vous pouvez éventuellement être condamné à l’issue du procès (condamnation aux dépens, dommages et intérêts).

Comment demander l’aide juridictionnelle ?

Formulaire de demande d’aide juridictionnelle – Cerfa n°12467*01

Site Internet sur l’aide juridictionnelle du site Service-Public.fr

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

Références :

Loi n°91-647 du 11 juillet 1991 relative à l’aide juridique

Décret n°91-1266 du 19 décembre 1991 relatif à l’aide juridique

Arrêté du 23 novembre 2011 sur les procédures visées par le décret du 15 février 1995 relatif aux droits de plaidoirie

---

Qui peut le consulter le fichier des impayés de la téléphonie mobile Préventel ? | Denis JACOPINI

Qui peut le consulter le fichier des impayés de la téléphonie mobile Préventel ?

Le fichier peut être consulté par le GIE Preventel et par les les services des membres du GIE Préventel chargés de la gestion des abonnements et des recouvrements.
Le fichier est consulté pour chaque nouvelle demande d'abonnement mobile par les services chargés de l'ouverture de ligne.
Les vendeurs en boutique n'ont pas directement accès au fichier PREVENTEL.

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
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

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4A1F561B7B702AD8312BAF603CB6F9F0?name=Pr%C3%A9ventel+(fichier+des+impay%C3%A9s+de+la+t%C3%A9l%C3%A9phonie+mobile)+%3A+qui+peut+le+consulter+%3F&id=378