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

23

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

Piratage de ses comptes sociaux : prévenir, repérer

et réagir | Denis JACOPINI

Piratage de ses comptes sociaux : prévenir, repérer et réagir !

Sur les réseaux sociaux, la plus grande vigilance est requise si l'on veut protéger ses données personnelles.

Les réseaux sociaux se multipliant de façon considérable, il convient de se montrer attentif à la protection des données personnelles, car ces dernières peuvent d'autant plus facilement être piratées.
A ce titre, la Commission nationale de l'informatique et des libertés (CNIL) publie une fiche pratique, agrémentée de liens directs vers les principaux réseaux sociaux, afin de mettre en oeuvre le contrôle des données personnelles.

Parmi les conseils donnés par la Commission, citons :
– le choix de mots de passe complexes, mais aussi différents les uns des autres, et avec un sens n'ayant aucun rapport avec une donnée personnelle relative à la vie privée du titulaire du compte (comme une date de naissance, etc…) ;
– l'absence totale de communication du mot de passe à une tierce personne ;
– l'activation d'un dispositif d'alerte en cas d'intrusion (dans ce cas, la personne titulaire du compte et qui se connecte depuis un poste informatique inconnu doit confirmer l'accès en entrant un code, reçu préalablement par sms ou par mail) ;
– la déconnexion à distance des terminaux encore liés au compte ;
– la désactivation des applications tierces encore connectées au compte ;
– le réglage précis des paramètres de confidentialité.
En outre, la CNIL donne des astuces pour repérer le piratage d'un compte. Des signes doivent en effet alerter l'utilisateur, par exemple un mot de passe invalide, ou des comportements inhabituels ayant lieu sur le compte, sans consentement préalable (comme suivre, se désabonner, ou encore bloquer…).

En cas de piratage, il convient donc :
– en premier lieu, de signaler le compte piraté auprès du réseau social ;
– cette première étape franchie, il convient alors de demander une réinitialisation du mot de passe. Si la réponse apportées par les modérateurs du réseau n'est pas satisfaisante, la CNIL peut être saisie.

Consultez la fiche pratique de la CNIL

Source : http://www.net-iris.fr/veille-juridique/actualite/34642/comment-prevenir-le-piratage-de-son-compte-en-ligne.php

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.
Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant… Les accès gratuits pullulent et se généralisent.
Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « **Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit** » assure-t-il. « **Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants…** »

Des sniffeurs de données

Il exagère ? Non. « **L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés !** » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« **Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter.** » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « **Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi** ».

Conseils

Alors quels conseils ? « **Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites.** » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.
Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Androïd.
Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]

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, contentieux, 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.

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

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ? | Denis JACOPINI

Mon employeur peut-il enregistrer ou écouter mes conversations téléphoniques à mon insu ?

Un employeur n'a le droit ni d'enregistrer ni d'écouter les conversations téléphoniques de ses employés s'ils n'en sont pas informés.S'il le fait, il commet un délit et risque des sanctions pénales.

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

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

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

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=4FBDF806985B62BC62EB3DEBC567BF6F?name=Mon+employeur+peut-il+enregistrer+ou+%C3%A9couter+mes+conversations+t%C3%A9l%C3%A9phoniques+%C3%A0+mon+insu+%3F&id=106

Comment savoir si je suis fiché au FNAEG (Fichier national des empreintes

génétiques) ? | Denis JACOPINI

Comment savoir si je suis fiché au #FNAEG (#Fichier national des empreintes génétiques) ?

Pour avoir ces informations, vous devez écrire (en joignant une copie d'une pièce d'identité) à l'adresse suivante :
Directeur central de la police judiciaire
Ministère de l'Intérieur
11 Rue des Saussaies
75800 Paris Cedex 08
Si vous n'avez pas de réponse dans un délai de 2 mois ou si votre demande est refusée, vous pouvez adresser une plainte à la CNIL ou porter plainte auprès des services de police, de gendarmerie ou du procureur de la République.

L'effacement de votre inscription est possible dans certains cas, en vous adressant au procureur de la République du Tribunal de grande instance compétent.

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

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

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

S o u r c e :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=65372FC5C6502D0A6ED2239F1706AE63?name=FNAEG+(Fichier+national+des+empreintes+g%C3%A9n%C3%A9tiques)+%3A+comment+savoir+si+je+suis+fich%C3%A9+%3F&id=256

Windows 10 : Identifier les applications malveillantes à partir des services par

défaut | Denis JACOPINI

Windows 10 : Identifier les applications malveillantes à partir des services par défaut

Afin de vérifier si votre ordinateur dispose d'applications malveillantes ou non, nous vous mettons en ligne la liste des service lancés par défaut de Windows 8.
Executez Services.msc

Name	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Manual	Local System
AllJoyn Router Service	Manual (Trigger Start)	Local Service
App Readiness	Manual	Local System
Application Identity	Manual (Trigger Start)	Local Service
Application Information	Manual (Trigger Start)	Local System
Application Layer Gateway Service	Manual	Local Service
Application Management	Manual	Local System
AppX Deployment Service (AppXSVC)	Manual	Local System
Auto Time Zone Updater	Disabled	Local Service
AVCTP service	Manual (Trigger Start)	Local Service
Background Intelligent Transfer Service	Automatic (Delayed Start)	Local System
Background Tasks Infrastructure Service	Automatic	Local System
Base Filtering Engine	Automatic	Local Service
BitLocker Drive Encryption Service	Manual (Trigger Start)	Local System
Block Level Backup Engine Service	Manual	Local System
Bluetooth Audio Gateway Service	Manual (Trigger Start)	Local Service
Bluetooth Support Service	Manual (Trigger Start)	Local Service
Bluetooth User Support Service	Manual (Trigger Start)	Local System
BranchCache	Manual	Network Service
Capability Access Manager Service	Manual	Local System
CaptureService	Manual	Local System
Certificate Propagation	Manual	Local System
Client License Service (ClipSVC)	Manual (Trigger Start)	Local System
Clipboard User Service	Manual	Local System
CNG Key Isolation	Manual (Trigger Start)	Local System
COM+ Event System	Automatic	Local Service
COM+ System Application	Manual	Local System
Computer Browser	Manual (Trigger Start)	Local System
Connected Device Platform Service	Automatic (Delayed Start)	Local Service
Connected Devices Platform User Service	Automatic	Local System
Connected User Experiences and Telemetry	Automatic	Local System
ConsentUX	Manual	Local System
Contact Data	Manual	Local System
CoreMessaging	Automatic	Local Service
Credential Manager	Manual	Local System
Cryptographic Services	Automatic	Network Service
Data Sharing Service	Manual (Trigger Start)	Local System
Data Usage	Automatic (Delayed Start)	Local Service
DCOM Server Process Launcher	Automatic	Local System
Delivery Optimization	Automatic (Delayed Start)	Network Service
Device Association Service	Automatic (Trigger Start)	Local System
Device Install Service	Manual (Trigger Start)	Local System
Device Management Enrollment Service	Manual	Local System
Device Management Wireless Application Protocol (WAP) Push message Routing Service	Manual (Trigger)	Local System
Device Setup Manager	Manual (Trigger Start)	Local System
DevicePicker	Manual	Local System
DevicesFlow	Manual	Local System
Devquery Background Discovery Broker	Manual (Trigger Start)	Local System
DHCP Client	Automatic	Local Service
Diagnostic Execution Service	Manual (Trigger)	Local System
Diagnostic Policy Service	Automatic	Local Service
Diagnostic Service Host	Manual	Local Service
Diagnostic System Host	Manual	Local System
DisplayEnhancementService	Manual (Trigger Start)	Local System
Distributed Link Tracking Client	Automatic	Local System
Distributed Transaction Coordinator	Manual	Network Service
DNS Client	Automatic (Trigger Start)	Network Service
Downloaded Maps Manager	Automatic (Delayed Start)	Network Service
Embedded Mode	Manual (Trigger Start)	Local System
Encrypting File System (EFS)	Manual (Trigger Start)	Local System
Enterprise App Management Service	Manual	Local System
Extensible Authentication Protocol	Manual	Local System
Fax	Manual	Network Service
File History Service	Manual (Trigger Start)	Local System
Function Discovery Provider Host	Manual	Local Service
Function Discovery Resource Publication	Manual	Local Service
GameDVR and Broadcast User Service	Manual	Local System
Geolocation Service	Manual (Trigger Start)	Local System
GraphicsPerfSvc	Manual (Trigger Start)	Local System
Group Policy Client	Automatic (Trigger Start)	Local System
Human Interface Device Service	Manual (Trigger Start)	Local System
HV Host Service	Manual (Trigger Start)	Local System
Hyper-V Data Exchange Service	Manual (Trigger Start)	Local System
Hyper-V Guest Service Interface	Manual (Trigger Start)	Local System
Hyper-V Guest Shutdown Service	Manual (Trigger Start)	Local System
Hyper-V Heartbeat Service	Manual (Trigger Start)	Local System
Hyper-V PowerShell Direct Service	Manual (Trigger Start)	Local System
Hyper-V Remote Desktop Virtualization Service	Manual (Trigger Start)	Local System
Hyper-V Time Synchronization Service	Manual (Trigger Start)	Local Service
Hyper-V Volume Shadow Copy Requestor	Manual (Trigger Start)	Local System
IKE and AuthIP IPsec Keying Modules	Manual (Trigger Start)	Local System
Infrared monitor service	Manual	Local System
Internet Connection Sharing (ICS)	Manual	Local System
IP Helper	Automatic	Local System
IPsec Policy Agent	Manual (Trigger Start)	Network Service
IP Translation Configuration Service	Manual (Trigger Start)	Local System
KtmRm for Distributed Transaction Coordinator	Manual (Trigger Start)	Network Service
Language Experience Service	Manual	Local System
Link-Layer Topology Discovery Mapper	Manual	Local Service
Local Profile Assistant Service	Manual (Trigger Start)	Local Service
Local Session Manager	Automatic	Local System
LxssManager	Manual	Local System
Messaging&Service	Manual (Trigger Start)	Local System
Microsoft (R) Diagnostics Hub Standard Collector Service	Manual	Local System
Microsoft Account Sign-in Assistant	Manual (Trigger Start)	Local System
Microsoft App-V Client	Disabled	Local System
Microsoft iSCSI Initiator Service	Manual	Local System
Microsoft Passport	Manual (Trigger Start)	Local System
Microsoft Passport Container	Manual (Trigger Start)	Local Service
Microsoft Software Shadow Copy Provider	Manual	Local System
Microsoft Storage Spaces SMP	Manual	Network Service
Microsoft Store Install Service	Manual	Local System
Microsoft Windows SMS Router Service	Manual (Trigger Start)	Local Service
Natural Authentication	Manual (Trigger Start)	Local System
Net.Tcp Port Sharing Service	Disabled	Local Service
Netlogon	Manual	Local System
Network Connected Devices Auto-Setup	Manual (Trigger Start)	Local Service
Network Connection Broker	Manual (Trigger Start)	Local System
Network Connections	Manual	Local System
Network Connectivity Assistant	Manual (Trigger Start)	Local System
Network List Service	Manual	Local Service
Network Location Awareness	Automatic	Network Service
Network Setup Service	Manual (Trigger Start)	Local System
Network Store Interface Service	Automatic	Local Service
Offline Files	Manual (Trigger Start)	Local System
OpenSSH Authentication Agent	Disabled	Local System
Optimum VGN Server	Manual	Local System
OpenSSH	Manual	Local System
Optimize drives	Manual	Local System
Payments and NFC/SE Manager	Manual (Trigger Start)	Local Service
Peer Name Resolution Protocol	Manual	Local Service
Peer Networking Grouping	Manual	Local Service
Peer Networking Identity Manager	Manual	Local Service
Performance Counter DLL Host	Manual	Local Service
Performance Logs & Alerts	Manual	Local Service
Phone Service	Manual (Trigger Start)	Local System
Plug and Play	Manual	Local System
PNRP Machine Name Publication Service	Manual	Local Service
Portable Device Enumerator Service	Manual (Trigger Start)	Local System
Power	Automatic	Local System
Print Spooler	Automatic	Local System
Printer Extensions and Notifications	Manual	Local System
PrintWorkflow	Manual	Local System
Problem Reports and Solutions Control Panel Support	Manual	Local System
Program Compatibility Assistant Service	Automatic	Local System
Quality Windows Audio Video Experience	Manual	Local Service
Radio Management Service	Manual	Local Service
Remote Access Auto Connection Manager	Manual	Local System
Remote Access Connection Manager	Automatic	Local System
Remote Desktop Configuration	Manual	Local System
Remote Desktop Services	Manual	Network Service
Remote Desktop Services UserMode Port Redirector	Manual	Local System
Remote Procedure Call (RPC)	Automatic	Network Service
Remote Procedure Call (RPC) Locator	Manual	Network Service
Remote Registry	Disabled	Local Service
Retail Demo Service	Manual	Local System
Routing and Remote Access	Disabled	Local System
RPC Endpoint Mapper	Automatic	Network Service
Secondary Logon	Manual	Local System
Secure Socket Tunneling Protocol Service	Manual	Local Service
Security Accounts Manager	Automatic	Local System
Security Center	Automatic (Delayed Start)	Local Service
Sensor Data Service	Manual (Trigger Start)	Local System
Sensor Monitoring Service	Manual (Trigger Start)	Local Service
Sensor Service	Manual (Trigger Start)	Local System
Server	Automatic	Local System
Shared PC Account Manager	Disabled	Local System
Shell Hardware Detection	Automatic	Local System
Smart Card	Manual (Trigger Start)	Local Service
Smart Card Device Enumeration Service	Manual (Trigger Start)	Local System
Smart Card Removal Policy	Manual	Local System
Spatial Data Service	Manual	Local Service
SNMP Service	Automatic	Local System
SNMP Trap	Manual	Local Service
Software Protection	Automatic (Delayed Start, Trigger Start)	Network Service
Spot Verifier	Manual (Trigger Start)	Local System
SSDP Discovery	Manual	Local Service
State Repository Service	Manual	Local System
Still Image Acquisition Events	Manual	Local System
Storage Service	Manual (Trigger Start)	Local System
Storage Tiers Management	Manual	Local System
Sync Host	Automatic (Delayed Start)	Local System
SysMain	Automatic	Local System
System Event Notification Service	Automatic	Local System
System Events Broker	Automatic (Trigger Start)	Local System
System Guard Runtime Monitor Broker	Automatic (Delayed Start)	Local System
Task Scheduler	Automatic	Local System
TCP/IP NetBIOS Helper	Manual (Trigger Start)	Local Service
Telephony	Manual	Network Service
Themes	Automatic	Local System
Time Broker	Manual (Trigger Start)	Local Service
Touch Keyboard and Handwriting Panel Service	Manual (Trigger Start)	Local System
Update Orchestrator Service	Automatic (Delayed Start)	Local System
UPnP Device Host	Manual	Local Service
User Data Access	Manual	Local System
User Data Storage	Manual	Local System
User Experience Virtualization Service	Disabled	Local System
User Manager	Automatic (Trigger Start)	Local System
User Profile Service	Automatic	Local System
Virtual Disk	Manual	Local System
Volume Shadow Copy	Manual	Local System
VolumeTrig Audio Inspector Service	Manual	Local Service
WDI Logging service	Manual	Local System
WalletService	Manual	Local System
WbioSrvSvc	Manual (Trigger Start)	Local Service
Web Account Manager	Manual	Local System
WebClient	Manual (Trigger Start)	Local Service
Wi-Fi Direct Services Connection Manager Service	Manual (Trigger Start)	Local Service
Windows Audio	Automatic	Local Service
Windows Audio Endpoint Builder	Automatic	Local System
Windows Backup	Manual	Local System
Windows Biometric Service	Manual (Trigger Start)	Local System
Windows Camera Frame Server	Manual (Trigger Start)	Local Service
Windows Connect Now - Config Registrar	Manual	Local Service
Windows Connection Manager	Automatic (Trigger Start)	Local Service
Windows Defender Advanced Threat Protection Service	Manual	Local System
Windows Defender Antivirus Network Inspection Service	Manual	Local Service
Windows Defender Antivirus Service	Automatic	Local System
Windows Encryption Provider Host Service	Manual (Trigger Start)	Local Service
Windows Error Reporting Service	Manual (Trigger Start)	Local System
Windows Event Collector	Manual	Network Service
Windows Event Log	Automatic	Local Service
Windows Defender Firewall	Automatic	Local Service
Windows Font Cache Service	Automatic	Local Service
Windows Image Acquisition (WIA)	Manual	Local Service
Windows Insider Service	Manual (Trigger Start)	Local System
Windows Installer	Manual	Local System
Windows License Manager Service	Manual (Trigger Start)	Local Service
Windows Management Instrumentation	Automatic	Local System
Windows Management Service	Manual	Local System
Windows Media Player Network Sharing Service	Manual	Network Service
Windows Mobile Hotspot Service	Manual (Trigger Start)	Local Service
Windows Modules Installer	Manual	Local System
Windows Perception Service	Manual (Trigger Start)	Local Service
Windows Perception Simulation Service	Manual	Local System
Windows Presentation Foundation Font Cache	Manual	Local Service
Windows Process Activation Service	Manual	Local System
Windows Push Notifications System Service	Automatic	Local System
Windows Push Notifications User Service	Automatic	Local System
Windows PushToInstall Service	Manual (Trigger Start)	Local System
Windows Remote Management (WS-Management)	Manual	Network Service
Windows Search	Automatic (Delayed Start)	Local System
Windows Security Service	Manual	Local System
Windows Time	Manual (Trigger Start)	Local Service
Windows Update	Manual (Trigger Start)	Local System
Windows Update Medic Service	Manual	Local System
WinHTTP Web Proxy Auto-Discovery Service	Manual	Local Service
Wired AutoConfig	Manual	Local System
WLAN AutoConfig	Automatic	Local System
WMI Performance Adapter	Manual	Local System
Work Folders	Manual	Local Service
Workstation	Automatic	Network Service
World Wide Web Publishing Service	Automatic	Local System
WWAN AutoConfig	Manual	Local Service
Xbox Accessory Management Service	Manual (Trigger Start)	Local System
Xbox Live Auth Manager	Manual	Local System
Xbox Live Game Save	Manual	Local System
Xbox Live Networking Service	Manual	Local System

[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 ?

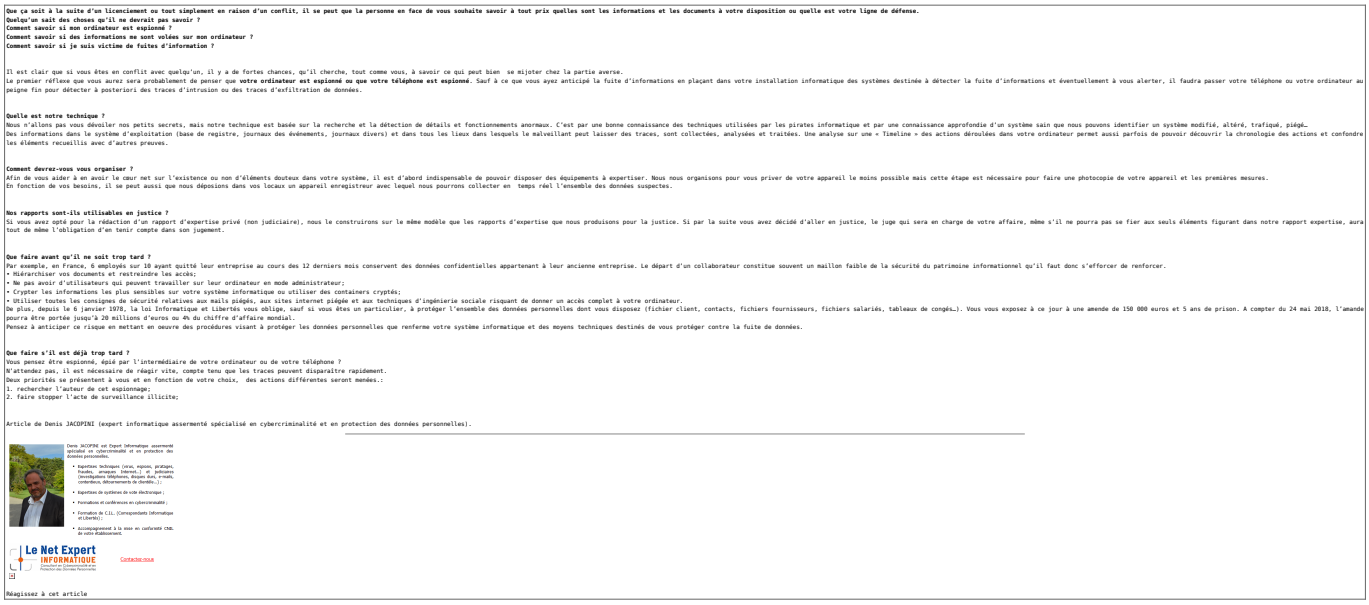
[block id="24760" title="Pied de page BAS"]

Source : https://www.winhelponline.com/blog/windows-10-default-services-configuration

---

Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ? | Denis JACOPINI


LE NET EXPERT
AUDITS & EXPERTISES
EXPERTISES DE SYSTÈMES DE VOTES ELECTRONIQUES
LENETEXPERT .fr
RGPD CYBER
LE NET EXPERT
MISES EN CONFORMITÉ
SPY DETECTION
Services de détection de logiciels espions
LE NET EXPERT
FORMATIONS
LE NET EXPERT
ARNAQUES & PIRATAGES
Denis JACOPINI
VOUS INFORME
LCI
Mon ordinateur ou mon téléphone est-il espionné ? Des informations me sont-elles volées ?



Que ça soit à la suite d'un licenciement ou tout simplement en raison d'un conflit, il se peut que la personne en face de vous souhaite savoir à tout prix quelles sont les informations et les documents à votre disposition ou quelle est votre ligne de défense.
Quelqu'un sait des choses qu'il ne devrait pas savoir ?
Comment savoir si mon ordinateur est espionné ?
Comment savoir si des informations ne sont volées sur mon ordinateur ?
Comment savoir si je suis victime de fuites d'information ?

Il est clair que si vous êtes en conflit avec quelqu'un, il y a de fortes chances, qu'il cherche, tout comme vous, à savoir ce qui peut bien se mijoter chez la partie averse.
Le premier réflexe que vous aurez sera probablement de penser que **votre ordinateur est espionné ou que votre téléphone est espionné**. Sauf à ce que vous ayez anticipé la fuite d'informations en plaçant dans votre installation informatique des systèmes destinée à détecter la fuite d'informations et éventuellement à vous alerter, il faudra passer votre téléphone ou votre ordinateur au peigne fin pour détecter à posteriori des traces d'intrusion ou des traces d'exfiltration de données.

Quelle est notre technique ?
Nous n'allons pas vous dévoiler nos petits secrets, mais notre technique est basée sur la recherche et la détection de détails et fonctionnements anormaux. C'est par une bonne connaissance des techniques utilisées par les pirates informatique et par une connaissance approfondie d'un système sain que nous pouvons identifier un système modifié, altéré, trafiqué, piégé…
Des informations dans le système d'exploitation (base de registre, journaux des événements, journaux divers) et dans tous les lieux dans lesquels le malveillant peut laisser des traces, sont collectées, analysées et traitées. Une analyse sur une « Timeline » des actions déroulées dans votre ordinateur permet aussi parfois de pouvoir découvrir la chronologie des actions et confondre les éléments recueillis avec d'autres preuves.

Comment devrez-vous vous organiser ?
Afin de vous aider à en avoir le cœur net sur l'existence ou non d'éléments douteux dans votre système, il est d'abord indispensable de pouvoir disposer des équipements à expertiser. Nous nous organisons pour vous priver de votre appareil le moins possible mais cette étape est nécessaire pour faire une photocopie de votre appareil et les premières mesures.
En fonction de vos besoins, il se peut aussi que nous déposions dans vos locaux un appareil enregistreur avec lequel nous pourrons collecter en temps réel l'ensemble des données suspectes.

Nos rapports sont-ils utilisables en justice ?
Si vous avez opté pour la rédaction d'un rapport d'expertise privé (non judiciaire), nous le construirons sur le même modèle que les rapports d'expertise que nous produisons pour la justice. Si par la suite vous avez décidé d'aller en justice, le juge qui sera en charge de votre affaire, même s'il ne pourra pas se fier aux seuls éléments figurant dans notre rapport expertise, aura tout de même l'obligation d'en tenir compte dans son jugement.

Que faire avant qu'il ne soit trop tard ?
Par exemple, en France, 6 employés sur 10 ayant quitté leur entreprise au cours des 12 derniers mois conservent des données confidentielles appartenant à leur ancienne entreprise. Le départ d'un collaborateur constitue souvent un maillon faible de la sécurité du patrimoine informationnel qu'il faut donc s'efforcer de renforcer.
• Hiérarchiser vos documents et restreindre les accès;
• Ne pas avoir d'utilisateurs qui peuvent travailler sur leur ordinateur en mode administrateur;
• Crypter les informations les plus sensibles sur votre système informatique ou utiliser des containers cryptés;
• Utiliser toutes les consignes de sécurité relatives aux mails piégés, aux sites internet piégés et aux techniques d'ingénierie sociale risquant de donner un accès complet à votre ordinateur.
De plus, depuis le 6 janvier 1978, la loi Informatique et Libertés vous oblige, sauf si vous êtes un particulier, à protéger l'ensemble des données personnelles dont vous disposez (fichier client, contacts, fichiers fournisseurs, fichiers salariés, tableaux de congés…). Vous vous exposez à ce jour à une amende de 150 000 euros et 5 ans de prison. A compter du 24 mai 2018, l'amande pourra être portée jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial.
Pensez à anticiper ce risque en mettant en œuvre des procédures visant à protéger les données personnelles que renferme votre système informatique et des moyens techniques destinés de vous protéger contre la fuite de données.

Que faire s'il est déjà trop tard ?
Vous pensez être espionné, épié par l'intermédiaire de votre ordinateur ou de votre téléphone ?
N'attendez pas, il est nécessaire de réagir vite, compte tenu que les traces peuvent disparaître rapidement.
Deux priorités se présentent à vous et en fonction de votre choix, des actions différentes seront menées.:
1. rechercher l'auteur de cet espionnage;
2. faire stopper l'acte de surveillance illicite;

Article de Denis JACOPINI (expert informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles).

Denis JACOPINE 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, contentieux, 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.
Le Net Expert INFORMATIQUE
Contactez-nous
Réagissez à cet article

Original de l'article mis en page : Comment se protéger contre la fuite d'informations avec le départ des collaborateurs ? — Lexsi Security Hub

---

Comment bien sécuriser ses e-mails ? | Denis JACOPINI

Peut-on encore se passer de l'e mail dans le cadre de nos activités professionnelles ? Je ne le crois pas. Il est pratique et instantané. Cependant, peu sécurisé en standard, sans précautions, il pourrait bien vous attirer des ennuis.

Selon une étude récente de SilverSky, Email Security Habits Survey Report, 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes, que 21 % des employés déclarent envoyer des données sensibles sans les chiffrer et que 22 % des entreprises sont concernées chaque année par la #perte de données via e-mail.

Inquiétant vous direz-vous ? Catastrophique quand on sait que tout détenteur de données à caractère personnel est tenu à la sécurisation de ces données, conformément à la loi informatique et libertés, encadrée par la CNIL.
Et c'est encore pire quand on prend en compte les informations soumises au secret professionnel ou revêtues de confidentialité que nous échangeons quotidiennement… (plus de 100 milliards d'e-mails sont échangées chaque jour…)
Un des derniers incidents en date : la récente #divulgation des numéros de passeport de 31 leaders mondiaux…
Malgré l'évolution du contexte législatif il est bien étonnant que les entreprises ne soient pas plus nombreuses à choisir de sécuriser leurs échanges par e-mail.

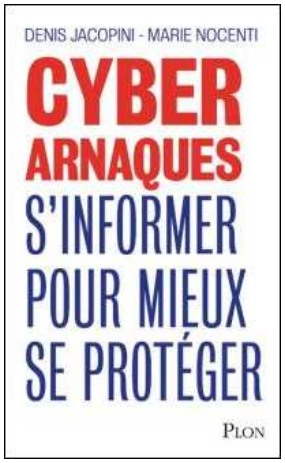
Des solutions ?
Oui, heureusement, et je vais partager avec vous mes conseils :
Mettez en place des procédés de signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message.
Vous éviterez ainsi que des données sensibles ne tombent dans de mauvaises mains.
Avantage pour le destinataire : l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
L'utilisation simultanée de ces procédés vous permettront ainsi de répondre à un besoin de Confidentialité (par le chiffrement) et un besoin d'Intégrité (par la signature électronique).

Enfin, aucun de ces deux procédés vous assurera une protection contre la fuite d'informations ou de données confidentielles à votre insu. POur cela, nous vous recommandons d'utiliser des système de « Protection contre la fuite des données » ou de « Data Leak Protection ».*

Plus d'info sur la confidentialité des e-mails ici

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

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

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 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité 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 risque ? 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.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

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 coécrit 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

Hotspot Shield le logiciel VPN pour Windows MacOs IOS

Android Apple Samsung pour accéder de manière sécurisée à un Wifi public | Denis JACOPINI

#Hotspot Shield le #logiciel VPN pour Windows MacOs IOS Android Apple Samsung pour accéder de manière sécurisée à un Wifi public

En période de vacances ou lors de déplacements professionnels, nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… En juillet 2015, nous vous avions publié un article « Est-il risqué de se connecter au wifi public ? » pour vous informer des principaux risques à partager ces accès sans fil à internet avec d'autres. Cette fois, nous allons parler des solutions pour surfer sécurisé en utilisant les réseaux Wifi publics.

RAPPEL DU PRINCIPAL RISQUE

Un pirate peut se connecter tout aussi facilement que vous sur un réseau Wifi Public et espionner les données qui y transitent.
Il peut ainsi, en fonction des données qu'il récupère, accéder à toutes les informations qui sortent et qui entrent de votre ordinateur (le protocole tcp/ip n'étant pas protégé par défaut).

LA SOLUTION ?

Utiliser une connexion Wifi qui sera cryptée au moyen d'un logiciel VPN (ce ctyptage n'a aucun rapport avec les clés Wifi) .
La connexion Wifi ainsi créée étant crypté, toutes les informations qui véhiculeront (identifiants, adresses email, mots de passe, numéros de cartes bancaires…) seront illisibles pour tous les pirates qui seront connectés sur le mêle point d'accès wifi.

Vous pouvez certes partager la connexion 3G ou 4G de votre smartphone, mais l'utilisation d'un logiciel VPN est recommandé.
Un logiciel « VPN » (Virtual Private Network) est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais elle est du coup sécurisée.

Nous utilisons régulièrement un logiciel VPN #HotSpotShield. C'est un logiciel qui coûte moins de 25 euros et qui vous rendra les connections Wifi publiques sécurisées.
HotSpot Shield existe pour Windows pour protéger par un logiciel VPN les connexions Wifi des ordinateurs assemblés, Acer, Asus, IBM, Dell ;
HotSpot Shield existe aussi pour MacOs X Lion pour protéger par un logiciel VPN les connexions Wifi des ordinateurs Apple ;
HotSpot Shield existe aussi pour Android pour protéger par un logiciel VPN les connexions Wifi des smartphones Samsung, HTC, Archos, LG, Acer, Wiko, Sony, Asus, Alcatel, ZTE… ;
Enfin, HotSpot Shield existe aussi pour IOs pour protéger par un logiciel VPN les connexions Wifi des smartphones Apple.

Téléchargez et testez gratuitement HotSpot Shield

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, contentieux, 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.

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

Contactez-nous

Réagissez à cet article

Denis JACOPINI interviewé par une journaliste de Ouest France | Denis JACOPINI

Est-il risqué de se connecter au wifi public ?
Nous sommes de plus en plus nombreux à utiliser les bornes wifi des lieux publics, gares, hôtels, restaurants… Mais y a-t-il un risque à partager ces accès sans fil à internet avec d'autres ? Peut-on se faire pirater ses données ? Le point avec Denis Jacopini, expert en cybercriminalité.

Avec les smartphones ou ordinateurs portables d'aujourd'hui, se connecter au réseau wifi d'une gare ou d'un hôtel, quand on est en déplacement, est devenu presque banal. À l'étranger, c'est même la solution la plus simple pour surfer sur internet et relever ses e-mails, sans risquer d'exorbitants frais de « roaming » (coûts de connexion au réseau mobile local, facturés ensuite par l'opérateur français).
Résultat, on a tendance à surfer sur ces réseaux wifi avec la même insouciance qu'à la maison, sans aucune précaution. Ce qui n'est pas bien malin. Denis Jacopini, expert judiciaire en sécurité informatique, nous explique pourquoi.

Denis Jacopini, créateur du site LeNetExpert.fr et correspondant Cnil (Commission nationale de l'informatique et des libertés), est aussi formateur en protection des données personnelles et en sécurité informatique. (Photo : DR)

À quoi faut-il faire attention, quand on se connecte à une borne wifi publique ou semi-publique, en ville ou dans un hôtel ?
Si possible, il faut choisir un réseau wifi où la connexion se fait avec un nom d'identifiant et un mot de passe personnalisés, différents pour chaque utilisateur. En cas d'utilisation malveillante du réseau par quelqu'un, cette identification fournit une piste, sur le plan judiciaire, pour remonter jusqu'à l'auteur. Avec les wifi qui proposent un identifiant et un mot de passe identiques pour tout le monde, on est moins protégé. Les réseaux wifi les plus dangereux sont ceux qui sont complètement ouverts, sans aucun mot de passe, où les utilisateurs sont impossibles à tracer.

Quel est le danger ? Se faire espionner ?
Tout à fait. À partir du moment où quelqu'un se trouve connecté au même point wifi que vous, il a techniquement la possibilité d'accéder aux informations qui transitent sur le réseau, il peut « voir » ce qui entre et qui sort. Les pirates utilisent pour cela des logiciels espions, appelés « sniffers », ou « renifleurs » en bon français. Ces programmes sont désormais très faciles à trouver et à télécharger sur internet. Plus ou moins sophistiqués, ils permettent de capter, trier et interpréter le « bruit » informatique qui transite par le wifi.

Le wifi public, c'est pratique, mais pas très sécurisé. (Photo : FlickR/Richard Summers)

La confidentialité de la navigation n'est donc pas garantie ?
En effet. Et pas uniquement sur les réseaux wifi, d'ailleurs. C'est ainsi depuis la création d'internet : les protocoles de communication du web ne sont pas cryptés. Mais de plus en plus de sites « sensibles » – par exemple les messageries électroniques, les banques, les boutiques en ligne, etc. – ont désormais des adresses commençant par « https » au lieu de « http ». Le « s », souvent associé avec un petit cadenas dans la barre du navigateur, signifie que les communications sont sécurisées. Quand on navigue sur internet via un wifi, il faut donc privilégier ces sites.

Le risque de se faire voler ses mots de passe, ou ses coordonnées bancaires, est donc bien réel ?
Oui, mieux vaut éviter de saisir des données confidentielles quand on navigue sur internet via un wifi public ou semi-public. On a ainsi vu des hommes d'affaires se faire voler des informations importantes, car ils utilisaient en toute confiance un wifi d'hôtel… sur lequel étaient aussi connectés des pirates !

Un café Starbucks à Londres, très apprécié pour sa connexion wifi gratuite. (Photo : Stefan Wermuth/Reuters)

Peut-on se faire abuser par une fausse borne wifi ?
Oui, c'est une raison supplémentaire de se méfier des réseaux complètement ouverts : certains pirates créent leur propre borne wifi à partir d'un simple ordinateur portable. Les passants se connectent dessus, par facilité, sans se douter qu'il ne s'agit pas du tout d'une « vraie » borne. Ensuite, la personne mal intentionnée n'a plus qu'à récupérer les informations qui transitent par le réseau qu'elle a créé… Aujourd'hui, c'est très facile de devenir pirate !

Comment se protéger ?
En s'abstenant de réaliser des opérations sensibles, comme des achats en ligne ou des opérations bancaires, sur un wifi public. Si on le peut, mieux vaut utiliser le réseau 3G ou 4G pour se connecter à internet en mobilité. Les informations qui transitent par cette voie sont beaucoup moins faciles à pirater. Il y a aussi la solution consistant à installer, sur son smartphone ou son ordinateur, ce qu'on appelle un « VPN ». C'est un logiciel qui crée un « réseau privé virtuel », une sorte de tunnel crypté pour vos communications internet. Cela ralentit un peu la connexion, mais c'est beaucoup plus sûr.

Zone de wifi gratuit à New York : en France comme à l'étranger, mieux vaut se connecter sur un nom de réseau connu, éventuellement signalé via l'affichage public. (Photo : Keith Bedford/Reuters)

[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.ouest-france.fr/leditiondusoir/data/492/reader/reader.html?t=1431534138729#!preferred/1/package/492/pub/493/page/7
Par Corinne Bourbeillon