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

La Commission Européenne facilite l’accès aux preuves électroniques

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

La Commission propose de nouvelles règles visant à permettre aux autorités policières et judiciaires d'obtenir plus facilement et plus rapidement les preuves électroniques, comme les courriels ou les documents se trouvant sur le cloud, dont elles ont besoin pour mener à bien leurs enquêtes, ainsi que pour poursuivre et condamner les criminels et les terroristes.

Les nouvelles règles permettront aux services répressifs des États membres de l'UE de mieux rechercher des pistes en ligne et par-delà les frontières, tout en offrant des garanties suffisantes pour les droits et les libertés de tous les intéressés.

M. **Frans Timmermans**, premier vice-président de la Commission, a déclaré à ce propos: *«Les preuves électroniques revêtent une importance croissante en matière pénale. Nous ne pouvons pas accepter que les criminels et les terroristes exploitent les technologies de communication électroniques modernes pour dissimuler leurs actes et se soustraire à la justice. Les criminels et les terroristes ne doivent pouvoir trouver aucun refuge en Europe, que ce soit en ligne ou hors ligne. Les propositions présentées aujourd'hui visent non seulement à mettre en place de nouveaux instruments qui permettront aux autorités compétentes de recueillir des preuves électroniques rapidement et efficacement par-delà les frontières, mais aussi à assurer des garanties solides pour les droits et les libertés de toutes les personnes concernées.»*

Les propositions visent à:

• créer une injonction européenne de production ;

• empêcher l'effacement de données au moyen d'une injonction européenne de conservation ;

• mettre en place des garanties solides et des voies de recours ;

• contraindre les prestataires de services à désigner un représentant légal dans l'Union ;

• procurer une sécurité juridique aux entreprises et aux prestataires de services ;

[L'article original complet]

[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 : *Commission Européenne – COMMUNIQUES DE PRESSE – Communiqué de presse – Union de la sécurité: la Commission facilite l'accès aux preuves électroniques*

Des drones-pigeons pour espionner ses habitants

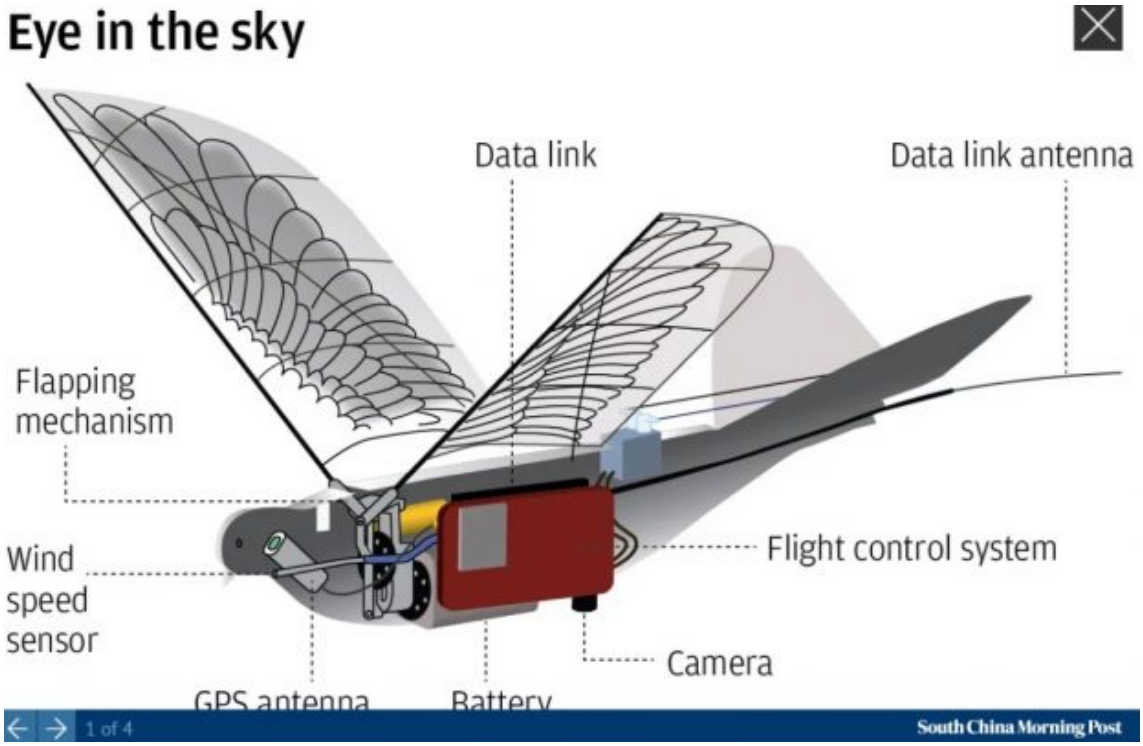
Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Des drones-pigeons pour espionner ses habitants

La technologie des drones est mise au service de la surveillance de la population en Chine, déguisée en oiseaux.

La surveillance de sa population semble toujours plus poussée en Chine. La nouvelle trouvaille est l'utilisation de drones camouflés en pigeons pour suivre ses habitants. Développés par une équipe de chercheurs de l'Université Polytechnique de Shaanxi, les pigeons-robots imitent près de 90% du comportement et des mouvements d'un véritable oiseau.

Ces petits « bijoux » de technologies sont utilisés par une trentaine d'agences gouvernementales et militaires chinoises dans au moins 5 provinces différentes du pays, comme le rapporte le **South China Morning Post**. La région du Xinjiang semble être l'une des plus survolées – donc surveillée – par ces drones-oiseaux. Cette région regroupe la communauté musulmane ouïghoure, qui fait l'objet d'une surveillance accrue de la part du gouvernement chinois.



Ces pigeons-robots mesurent environ 50 centimètres et pèsent 200 grammes. Avec une autonomie de 30 minutes, les drones-oiseaux peuvent aller à une vitesse de 40 km/h et sont contrôlés à distance grâce à une caméra haute définition et un GPS intégrés...[lire la suite]

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Source et illustrations : *La Chine utilise des drones-pigeons pour espionner ses habitants – Geeko*

Interpol peut maintenant reconnaître votre voix grâce au Big Data

Interpol peut désormais identifier la voix d'un locuteur inconnu grâce à une base de données regroupant des échantillons vocaux en provenance d'agences gouvernementales du monde entier.…[Lire la suite]

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Interpol peut maintenant reconnaître votre voix grâce au Big Data

Interpol peut désormais identifier la voix d'un locuteur inconnu grâce à une base de données regroupant des échantillons vocaux en provenance d'agences gouvernementales du monde entier.…[Lire la suite]

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Interpol peut maintenant reconnaître votre voix grâce au Big Data

Interpol peut désormais identifier la voix d'un locuteur inconnu grâce à une base de données regroupant des échantillons vocaux en provenance d'agences gouvernementales du monde entier.…[Lire la suite]

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Interpol peut maintenant reconnaître votre voix grâce au Big Data

Interpol peut désormais identifier la voix d'un locuteur inconnu grâce à une base de données regroupant des échantillons vocaux en provenance d'agences gouvernementales du monde entier.…[Lire la suite]

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Interpol peut maintenant reconnaître votre voix grâce au Big Data

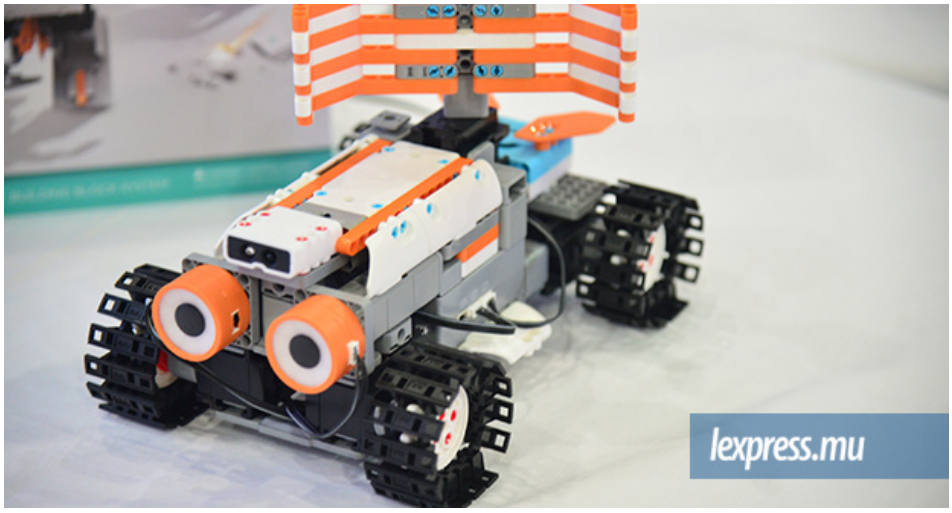
Interpol peut désormais identifier la voix d'un locuteur inconnu grâce à une base de données regroupant des échantillons vocaux en provenance d'agences gouvernementales du monde entier.…[Lire la suite]

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

[block id="24881" title="Pied de page Contenu Cyber"]

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

Objets connectés: attention, on vous espionne…



Objets connectés: attention, on vous espionne…

Montre connectée. Enceintes connectées. Casque connectée. Jouets connectés… Autant d'appareils qui ont besoin d'Internet pour fonctionner correctement. Sauf qu'ils sont susceptibles d'être des espions. La plupart sont, en effet, vulnérables aux menaces.

En France, l'Association européenne de défense des consommateurs a pris les devants pour demander que les poupées connectées soient retirées des étagères pour Noël. Ces poupées connectées, d'un fabricant réputé, répond aux enfants. Les conversations ont été enregistrées au préalable. Toutefois, cela n'est pas conforme aux règles de protection des données des mineurs. En effet, n'importe qui peut s'y connecter à travers le Bluetooth et ainsi intercepter des conversations

Selon un informaticien, les parents ne réalisent pas ce qu'ils achètent. *«Ils ignorent les dangers des poupées ou des jouets connectés. Ils vont en acheter sans réaliser qu'il y a des failles de sécurité»,* fait-il valoir.

Pas de vérifications

Le fait est que tous les objets qui ont des fonctions Bluetooth et sont équipés de micros sont de parfaits espions. Grâce à des logiciels espions, des pirates peuvent écouter les conversations. Wikileaks a rendu public des documents, en mars dernier, prouvant que la *National Security Agency*, aux États-Unis, peut effectuer des écoutes…[lire la suite]

Réagissez à cet article

Source : *Objets connectés: attention, on vous espionne… | lexpress.mu*

Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs

Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs

---

Une étude menée par des chercheurs de l'université de Princeton montre que des sites très populaires recourent à des scripts qui enregistrent le moindre mouvement de souris.

La pratique s'appelle session replay, littéralement « rejouer une session ». Elle consiste à enregistrer l'intégralité des actions d'un visiteur sur un site Web : les endroits où il clique bien sûr, mais aussi ses mouvements de souris, ce qu'il ou elle tape dans un formulaire de série et à quelle vitesse… Des données qui permettent de « revoir », en vidéo, comment un internaute s'est comporté en reproduisant l'intégralité de sa session sur le site…[lire la suite]

Source : *Plusieurs centaines de sites enregistrent l'intégralité des actions de visiteurs*