

Cybersécurité : les 10 chiffres qui font peur – Silicon

✖	Cybersécurité : les 10 chiffres qui font peur
---	---

L'explosion du trafic Internet et des activités numériques est un progrès incontestable. Mais il fait aussi courir des risques grandissants en matière de sécurité. La preuve avec ces dix exemples, qui doivent alerter sur les mesures à prendre.

3 minutes pour pirater un nouvel objet connecté

Caméras de surveillance, imprimantes, thermostats intelligents... Les milliards d'objets reliés au web sont extrêmement mal sécurisés. Les utilisateurs omettent la plupart du temps de changer le mot de passe par défaut et, d'autre part, les fabricants n'intègrent pas de réel système de sécurité dans leurs dispositifs. Résultat : moins de 3 minutes sont nécessaires à un hacker pour prendre le contrôle d'un objet connecté, selon l'éditeur de sécurité ForeScout, partenaire de Malwarebytes.

1,1 million de victimes de fraude à la carte bancaire par an

Le nombre de ménages victimes d'une fraude à la carte bancaire a plus que doublé en 5 ans, passant de 500.000 en 2011 à 1,1 million en 2015,...[lire la suite]

+83 % de smartphones infectés au 2e semestre 2016

65 vols de données par seconde

41 % : le taux de succès d'un ransomware

201 jours pour découvrir une cyberattaque

1,7 milliard de publicités fraudueuses en 2016

140 attaques de phishing par heure

Les particuliers deux fois plus infectés que les professionnels

Une entreprise subit 29 cyberattaques par an

[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Cybersécurité : les 10 chiffres qui font peur* –

Un demi-million de pacemakers menacés de piratage informatique rappelés

✕	Un demi-million, de pacemakers menacés de piratage informatique rappelés
---	--

L'administration américaine a rappelé 465.000 stimulateurs cardiaques menacés d'un piratage potentiel à cause d'une vulnérabilité informatique. Un correctif « vital » de leur logiciel devra être installé en hôpital. Explications.

Jamais le terme « vital » ne s'était autant appliqué à un correctif logiciel. Un léger vent de panique souffle dans les départements de cardiologie des hôpitaux américains, car ils doivent se préparer à recevoir la visite de presque un demi-million de patients pour une mise à jour logicielle de leur stimulateur cardiaque.

La puissante US Food and Drugs Administration (FDA) est à l'origine de ce rappel. Son **alerte officielle** concerne 465.000 pacemakers exposés à une attaque informatique éventuelle en raison d'un « faille » décelée a posteriori.

Cette « vulnérabilité » permettrait à un pirate très mal intentionné se trouvant à proximité d'en altérer le fonctionnement en agissant à distance par onde radio pour, par exemple, vider la batterie ou modifier la fréquence cardiaque. Et mettre en danger la vie du porteur du stimulateur cardiaque...[lire la suite]

NOTRE MÉTIER :

- **FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO**
- **EXPERTISES TECHNIQUES / RECHERCHE DE PREUVES**
- **AUDITS RGPD, AUDIT SECURITE ET ANALYSE D'IMPACT**
 - **MISE EN CONFORMITE RGPD / FORMATION DPO**

FORMATIONS EN CYBERCRIMINALITE, RGPD ET DPO : En groupe dans la toute la France ou individuelle dans vos locaux sous forme de conférences, ou de formations, de la sensibilisation à la maîtrise du sujet, découvrez nos formations ;

EXPERTISES TECHNIQUES : Pour prouver un dysfonctionnement, dans le but de déposer plainte ou de vous protéger d'une plainte, une expertise technique vous servira avant procès ou pour constituer votre dossier de défense ;

COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

AUDITS RGPD / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-nous

NOS FORMATIONS


: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : Un demi-million de pacemakers menacés de piratage informatique rappelés

**FIC 2018 les 23 et 24 janvier
à Lille : à l'ère de
l'hyperconnexion, comment
s'organise la cyber-
résilience ?**

	FIC 2018 les 23 et 24 janvier à Lille : à l'ère de l'hyperconnexion, comment s'organise la cyber-résilience ?
---	--

Organisé conjointement par la Gendarmerie Nationale, CEIS et EuraTechnologies, et co-financé par la Région Hauts-de-France, la 10^è édition du Forum International de la Cybersécurité entre dans l'ère de l'hyperconnexion.

« Les individus et les machines sont connectés en permanence et communiquent sans discontinuer entre eux et les uns avec les autres. Cette imbrication de réseaux expose le système aux effets dominos sur l'une de ses composantes et pose d'abord la question de la résilience, c'est à dire la capacité du système à faire face aux conséquences d'une attaque ou d'une défaillance sur l'un des maillons de la chaîne, et à récupérer ses aptitudes à opérer normalement. Cette nouvelle configuration bouleverse aussi les modes de fonctionnement et d'organisation de nos sociétés, et nécessitera d'adapter nos comportements, pratiques, technologies de sécurité et corpus législatifs et règlementaires. A l'ère de l'hyperconnexion, la cyber-résilience suppose donc une approche systémique de la sécurité impliquant à la fois les individus, les processus et les techniques » explique le Général Marc Watin-Augouard, fondateur du Forum International de la Cybersécurité...[lire la suite]

Denis JACOPINI :

C'est sur ce thème que le FIC 2018 ouvrira. Conférences, démonstrations, ateliers seront au rendez-vous. Le FIC 2018 est aussi le point de rencontre international des principaux acteurs de la cybersécurité. Donnons-nous donc rendez-vous les 23 et 24 janvier à Lille Grand Palais. Consultez le Pré Programme du FIC 2018 au 02/09/2017.

NOTRE MÉTIER :

FORMATIONS EN CYBERCRIMINALITE / RECHERCHE DE PREUVES / EXPERTISES INFORMATIQUES / AUDITS RGPD / MISE EN CONFORMITE RGPD / FORMATION DPO

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : 23 et 24 janvier Lille – FIC 2018 : à l'ère de l'hyperconnexion, comment s'organise la cyber-résilience ? – Global Security Mag Online

Intelligence artificielle: y a-t-il un pilote dans la maison ?

	Intelligence artificielle: y a-t-il un pilote dans la maison ?
---	---

C'est un véritable chef d'orchestre qui vient d'arriver dans le secteur des nouvelles technologies. Les assistants personnels commandent les objets connectés, la domotique mais aussi répondent à vos questions. Dernier arrivé en France : Google Home qui allie la puissance de son moteur de recherche à un boîtier qui promet de modifier nos vies à la maison, voire nos habitudes futures avec les nouvelles technologies.

Mais de quoi s'agit-il exactement ? Les boîtiers truffés de micros (des micros ultrasensibles et un système de traitement du langage naturel perfectionné pour Google Home) et d'un haut-parleur sont connectés au Wifi de la maison. Ils vont pouvoir ainsi tirer tout leur potentiel dès que vous les déclenchez avec des mots magiques comme « OK Google » ou « Alexa ».

Vous dialoguez alors en direct avec une intelligence artificielle. Chacune a les caractéristiques de sa marque : Apple, Google, Amazon ou Microsoft. C'est cette dernière qui va s'efforcer de répondre à toutes vos questions ou vos demandes domotiques. Le marché des nouvelles technologies est depuis quelques années dopé par ces intelligences artificielles qui promettent désormais d'intervenir directement dans votre vie de tous les jours...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Intelligence artificielle: y a-t-il un pilote dans la maison?* – Hebdo – RFI

Attention aux fausses sociétés d'assistance informatique !

✖	Attention aux fausses sociétés d'assistance informatique !
---	--

Les cybercriminels présentent la particularité d'être inventifs et très opportunistes. La médiatisation de la cyberattaque Wannacry a créé une peur que des hackers mal intentionnés ont parfaitement su utiliser.

Ainsi, les spams (courriels indésirables, généralement publicitaires) ont augmenté de 57% au deuxième trimestre 2017 d'après Kaspersky Lab. Avec une particularité : de nombreux courriels contenaient « *des offres de services de lutte contre Wannacry, des conseils pour éviter d'infection ainsi que des invitations à des séminaires de formation* ». Les escrocs en ont profité pour envoyer de fausses notifications, au nom d'éditeurs connus de logiciels, qui signalaient au destinataire que son ordinateur avait été infecté et qu'il fallait cliquer sur un lien pour installer une mise à jour. Problème : ce lien menait sur une page de *phishing*, c'est-à-dire un formulaire incitant les victimes à entrer des informations personnelles, utilisées ensuite pour effectuer une usurpation d'identité...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Cyberattaques, spams, malwares : les cybercriminels n'ont pas chômé au deuxième trimestre*

Une faille dangereuse découverte sur les hoverboards



Des experts chez Alibaba Security se sont penchés sur le niveau de sécurité des hoverboards. Résultat, ils sont parvenus à mettre à jour une faille qui pourrait être dangereuse pour les utilisateurs. Les tests menés par les spécialistes ont démontré qu'il était possible de brouiller les capteurs de mouvement des hoverboards. L'utilisateur pourrait alors tomber et se blesser.

Les démonstrations, faites lors de la conférence Black Hat Security en juillet, ont révélé que la faiblesse des hoverboards n'était autre que les ondes sonores. Projetées sur les capteurs, elles peuvent perturber les mesures et données collectées par ces derniers, déséquilibrant du même coup l'hoverboard et son utilisateur...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à votre disposition une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Les hoverboards ont un talon d'Achille, les ondes sonores*

Trouver une faille de sécurité peut rapporter jusqu'à 500 000 dollars

✕	Trouver une faille de sécurité peut rapporter jusqu'à 500 000 dollars
---	---

La société Zerodium, spécialisée dans le commerce de failles zero-day, revient avec un nouvel appel d'offre : un demi million de dollars à quiconque apportera sur un plateau une vulnérabilité inconnue dans les applis de messagerie WhatsApp et Signal.

Quel est le prix de votre vie privée ? 499 999 dollars, ça vous semble correct ? Parce qu'à vrai dire, elle pourrait être bientôt être vendue pour seulement un dollar de plus. L'entreprise Zerodium, spécialisée dans l'achat et la revente de vulnérabilités zero-day, vient de proposer la rondelette somme de 500 000 dollars à celui qui sera capable mettre au point les outils nécessaires au piratage des applications de messagerie cryptée Signal et WhatsApp. Déjà, en octobre 2016, elle avait proposé 1,5 millions de dollars pour une faille dans iOS 10...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : Une entreprise offre 500 000 dollars à celui qui trouvera une faille de sécurité exploitable sur WhatsApp et Signal

Un nouveau ransomware, Defray, cible l'éducation et la santé

✕	Un nouveau ransomware, Defray, cible l'éducation et la santé
---	--

Les chercheurs Proofpoint ont récemment analysé un nouveau ransomware, nommé Defray. Durant le mois d'août, ils ont observé plusieurs attaques ciblées, visant notamment les secteurs de la santé, de l'éducation, de l'industrie et de l'informatique.

« Defray » a été choisi en rapport avec le nom d'hôte du serveur de commande et de contrôle (C&C) de la première attaque observée :

defrayable-listings[.]000webhostapp[.]com Par coïncidence, le terme « defray » signifie fournir de l'argent pour payer une partie d'un coût, bien que ce dont les victimes doivent s'acquitter ne soit pas tout à fait clair.

La distribution de Defray présente plusieurs caractéristiques :

- Defray est diffusé via des documents Word dans des pièces jointes d'emails
 - Les pièges sont conçus sur mesure pour attirer toutes les victimes potentielles
 - Les destinataires sont des individus ou bien des groupes d'individus, par exemple, group@ ou websupport@
 - Les pays les plus touchés sont le Royaume-Uni et les États-Unis
- [Global Security Mag Online]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Defray, le nouveau ransomware qui cible l'éducation et la santé – Global Security Mag Online*

**Mots de passe Wifi des
espaces Lounges des
principaux aéroports à travers
le monde. Les conseils de
Denis JACOPINI**



**Mots de passe Wifi des
espaces Lounges des
principaux aéroports à
travers le monde. Les
conseils de Denis
JACOPINI**

Une base de donnée de nombreux codes d'accès Wifi des principaux aéroports à travers le monde accessible librement sur une carte Google Maps. Toutefois, même si le service paraît très utile, il peut aussi devenir un piège à voyageurs. Denis JACOPINI nous en dit plus

Même si pour beaucoup les vacances sont terminées, pour d'autres le réflexe à peine descendu d'un vol lors d'une escale ou arrivé à destination est de vérifier ses mails pour certains, ses j'aime, ses stats ou flash pour d'autres.

Autant anticiper en consultant cette carte et récupérer les identifiants et mots de passe des aéroports qui seront visités (avant de partir).
[Accéder à la carte avec la liste des aéroports]

Attention toutefois à prendre vos précautions lorsque vous utiliserez ces réseaux Wifi inconnus, publics ou libres ! Des pirates peuvent traîner par là et récupérer vos codes, vos informations ou pire, infecter leurs voisins numériques. Protégez bien votre ordinateur avec un système de sécurité à jour et utilisez un VPN pour accéder à des informations sensibles.

Maintenant, si c'est trop tard pour les utiliser lors des vacances de cette année pour certains, conservez précieusement ces informations pour l'année prochaine ☐

Denis JACOPINI

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Wireless Passwords From Airports And Lounges Around The World*

La stéganographie pour cacher des informations volées dans les images

x	La stéganographie pour cacher des informations volées dans les images
---	---

En analysant de multiples campagnes de cyberespionnage et de cybercriminalité, les chercheurs de Kaspersky Lab ont identifié une nouvelle tendance inquiétante : des pirates emploient de plus en plus la stéganographie, une version numérique d'un stratagème ancien consistant à dissimuler des messages à l'intérieur d'images, afin de masquer les traces de leur activité malveillante sur un ordinateur attaqué. Un certain nombre de malwares espions ainsi que plusieurs autres destinés au vol d'informations financières ont récemment été repérés utilisant cette technique.

Dans le cadre d'une cyberattaque ciblée type, un acteur malveillant – une fois infiltré dans le réseau attaqué – établit une tête de pont puis collecte des informations de valeur afin de les transférer par la suite à un serveur de commande et de contrôle (C&C). Dans la plupart des cas, des solutions de sécurité ou des outils analytiques professionnels éprouvés sont en mesure de détecter la présence de l'intrus sur le réseau à chaque phase d'une attaque, notamment au moment de l'exfiltration des données volées. En effet, cette exfiltration laisse généralement des traces, par exemple l'enregistrement de connexions à une adresse IP inconnue ou inscrite en liste noire. Or le recours à la stéganographie rend cette détection difficile...[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques ;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficacité maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliserons un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Réagissez à cet article

Source : *Plusieurs groupes de pirates utilisent de plus en plus la technique de la stéganographie pour cacher des informations volées dans les images – Global Security Mag Online*