

Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?



Pourquoi supprimer vos données personnelles si vous rendez votre ordinateur professionnel à votre employeur ?

Ne pas effacer ses données personnelles sur son ordinateur de fonction est-il dommageable (risque d'accès à nos données personnelles, vol d'identité ou accès frauduleux etc...)? Si oui, pourquoi ?

Imaginez, votre ordinateur, protégé ou non, tombe entre les mains d'une personne malveillante. Il pourra :

- Accéder à vos documents et découvrir les informations qui peuvent soit être professionnelles et être utilisées contre vous, soit personnelles permettant à un voyou de les utiliser contre vous soit en vous demandant de l'argent contre son silence ou pour avoir la paix ;
- Accéder aux identifiants et mots de passe des comptes internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes facebook, twitter, dropbox... ;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement déposer des commentaires ou envoyer des e-mails en utilisant votre identité. Même si l'article 226-4 du code pénal complété par la loi LOPPSI du 14 mars 2011 d'un article 226-4-1, l'usurpation d'identité numérique est un délit puni de deux ans d'emprisonnement et de 20 000 euros d'amende, il sera fastidieux d'une part pour vous, de prouver que vous n'êtes pas le véritable auteur des faits reprochés, et difficile pour les enquêteurs de retrouver le véritable auteur des faits.

Ne pas effacer ses données personnelles sur l'ordinateur que l'on rend, donne, vend, c'est laisser l'opportunité à un inconnu de fouiller dans vos papiers, violer votre intimité et cambrioler votre vie.

Pire ! vous connaissez bien le donataire de votre matériel et vous savez qu'il n'y a aucun risque qu'il ait des intentions répréhensibles. Mais êtes vous certain qu'il sera aussi prudent que vous avec son matériel ?

Êtes-vous prêt à prendre des risques s'il perdait ce matériel ?

Dormiriez-vous tranquille si vous imaginiez que votre ancien ordinateur est actuellement sous l'emprise d'un pirate informatique prêt à tout pour tricher, voler et violer en utilisant votre identité ?

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus sur
d'informations
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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.

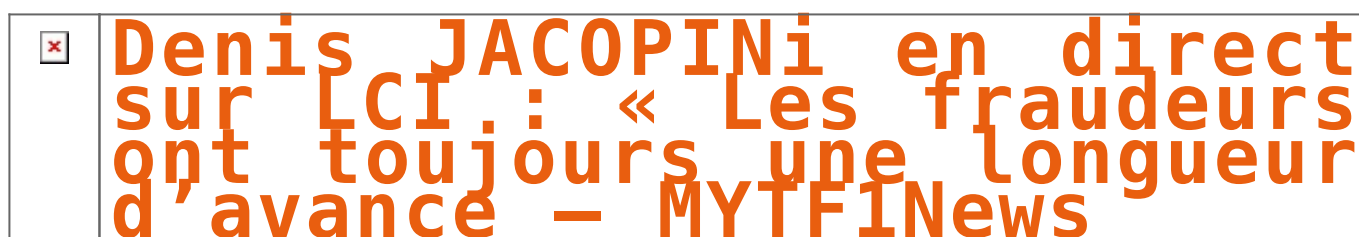


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : 5 applications pour effacer des données de façon sécurisée – ZDNet

Denis JACOPINI en direct sur LCI : « Les fraudeurs ont toujours une longueur d'avance – MYTF1News | Denis JACOPINI



Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent sur les techniques des cybercriminels pour vous pirater votre CB.



<http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html>

Réagissez à cet article

Source : *Cartes bancaires : « Les fraudeurs ont toujours une longueur d'avance » – Société – MYTF1News*

**Pourquoi, malgré le danger
connu, cliquons nous sur des
e-mails d'expéditeurs
inconnus ?**



**Pourquoi,
malgré le
danger connu,
cliquons nous
sur des e-
mails
d'expéditeurs
inconnus ?**

Selon une enquête de la FAU (University of Erlangen-Nuremberg), près de la moitié des utilisateurs cliqueraient sur des liens d'expéditeurs inconnus (environ 56% d'utilisateurs de boîte mails et 40% d'utilisateurs de Facebook), tout en étant parfaitement conscient des risques de virus ou d'autres infections.

Le site d'information Français Pure Player Atlantico a interrogé à ce sujet Denis JACOPINI, Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles

Atlantico :
Pourquoi donc, selon vous, le font-ils malgré tout ? Qu'est-ce qui rend un mail d'un inconnu si attirant, quitte à nous faire baisser notre garde ?

Denis JACOPINI :
Ça vous est très probablement déjà arrivé de recevoir un e-mail provenant d'un expéditeur anonyme ou inconnu. Avez-vous résisté à cliquer pour en savoir plus ? Quels dangers se cachent derrière ces sollicitations inhabituelles ? Comment les pirates informatiques peuvent se servir de nos comportements incontrôlables ?

Aujourd'hui encore, on peut comparer le courrier électronique au courrier postal. Cependant, si l'utilisation du courrier postal est en constante diminution (-22% entre 2009 et 2014), l'usage des messages électroniques par logiciel de messagerie ou par messagerie instantanée a lui par contre largement augmenté. Parmi les messages reçus, il y a très probablement des réponses attendues, des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant de nos nouvelles et quelques autres messages que nous recevons avec plaisir de personnes connues et puis il y a tout le reste, les messages non attendus, non désirés qui s'appellent des spams. En 2015, malgré les filtres mis en place par les fournisseurs de systèmes de messagerie, il y avait tout de même encore un peu plus de 50% de messages non désirés. Parmi ces pourriels (spambot + e-mail) se cachent de nombreux messages ayant des objectifs malveillants à votre égard. Les risques les plus répandus sont les incitations au téléchargement d'une pièce jointe, au clic sur un lien renvoyant vers un site Internet piégé ou vous proposer d'échanger dans le but de faire « copain copain » et ensuite vous arnaquer.

La solution : ne pas cliquer sur un e-mail ou un message provenant d'un inconnu, de la même manière qu'on apprend aux enfants de ne pas parler à un inconnu. Pourtant, des millions de personnes en France se font piéger chaque année. Pourquoi ?

A mon avis, les techniques d'ingénierie sociale sont à la base de ces correspondances. L'ingénierie sociale est une pratique qui exploite les failles humaines et sociales. L'attaquant va utiliser de nombreuses techniques dans le but d'abuser de la confiance, de l'ignorance ou de la crédulité des personnes ciblées.

Imaginez, vous recevez un message ressemblant à ça :
« Objet : changements dans le document 01.08.16
Expéditeur : Prénom et Nom d'une personne inconnue
Bonjour,
Nous avons fait tous les changements nécessaires dans le document.
Malheureusement, je ne comprends pas la cause pour la quelle vous ne recevez pas les fichier jointes.
J'ai essayé de remettre les fichier jointes dans le e-mail. »

Dans cet exemple, on ne connaît pas la personne, on ne connaît pas le contenu du document, mais la personne sous-entend un nouvel envoi qui peut laisser penser à une ultime tentative. Le document donne l'impression d'être important, le ton est professionnel, il n'y pas trop de faute d'orthographe. Difficile de résister au clic pour savoir ce qui se cache dans ce mystérieux document.

Un autre exemple d'e-mail ou similaire souvent reçu :
« Objet : Commande - CD2533
Expéditeur : Prénom et Nom d'une personne inconnue
Madame, Monsieur,
Nous vous remercions pour votre nouvelle « Commande - CD2533 ».
Nous revenons vers vous au plus vite pour les délais
Meilleures salutations,
VEDISCOM SECURITE »

En fait, bien évidemment pour ce message aussi, la pièce jointe contient un virus et si le virus est récent et s'il est bien codé, il sera indétectable par tous les filtres chargés de la sécurité informatique de votre patrimoine immatériel. Auriez-vous cliqué ? Auriez-vous fais partie des dizaines ou centaines de milliers de personnes qui auraient pu se faire piéger ?


Un autre exemple : Vous recevez sur facebook un message venant à première vue d'un inconnu mais l'expéditeur à un prénom que vous connaissez (par exemple Marie, le prénom le plus porté en France en 2016). Serait-ce la « Marie » dont vous ne connaissez pas le nom de famille, rencontrée par hasard lors d'un forum ou d'une soirée qui vous aurait retrouvé sur Facebook ? Dans le doute vous l'acceptez comme amie pour en savoir plus et engager pourquoi pas la conversation. C'est un autre moyen utilisé par les pirates informatiques pour rentrer dans votre cercle d'amis et probablement tenter des actes illicites que je ne détaillerai pas ici.

Vous rappelez-vous avoir accepté une demande de mise en contact provenant d'un inconnu sur Facebook ? Peut-être que vous ne connaissiez pas les risques, mais qu'est-ce qui vous a poussé à répondre à un inconnu ? La politesse ? La curiosité ?


A mon avis, le principal levier utilisé pour pousser les gens à cliquer sur les emails pour en voir l'objet, cliquer sur les pièces jointes pour en voir le contenu ou cliquer sur les liens pour découvrir la suite, est une des nombreuses failles humaine : la curiosité. Cette curiosité peut nous faire faire des choses complètement irresponsables, car on connaît les dangers des pièces jointes ou des liens dans les e-mails. Malgré cela, si notre curiosité est éveillée, il sera difficile de résister au clic censé la satisfaire.

Il est clair que la curiosité positive est nécessaire, mais dans notre monde numérique où les escrocs et pirates oeuvrent en masse le plus souvent en toute discrétion et en toute impunité, la pollution des moyens de communication numériques grand public est telle que le niveau de prudence doit être augmenté au point de ne plus laisser de place au hasard. Le jeu vaut-il vraiment la chandelle face aux graves conséquences que peut engendrer un simple clic mal placé ?

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03841 84).
Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques en informatique, découvrir et comprendre les arnaques et les piratages informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL en matière de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

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

- Expertises techniques (virus, espion, piratage, fraude, arnaques Internet, et logiciels d'investigation numériques, bases de données, e-mail, contenus, documents de clients...)
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Clients) ;
- 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 : One in two users click on links from unknown senders > FAU.EU

10 techniques de cybercriminels pour vous pirater votre carte bancaire | Denis JACOPINI

Denis JACOPINI



10 techniques de
cybercriminels
pour
vous pirater
votre carte
bancaire



Sources :

<http://www.agefi.fr/banque-assurance/actualites/hebdo/20160210/oberthur-technologies-lance-carte-a-cvv-dynamique-155903>

<http://www.challenges.fr/economie/20130912.CHA4249/la-verite-sur-les-fraudes-a-la-carte-bancaire.html>

<https://www.jegardecapourmoi.com>

<http://www.challenges.fr/economie/20130912.CHA4249/la-verite-sur-les-fraudes-a-la-carte-bancaire.html>

<http://www.bienpublic.com/actualite/2013/10/10/dijon>

<http://www.lanouvelletribune.info/societe/vie-societale/technologie/25616-greendispenser-un-nouveau-virus-voleur-de-billets-de-banque>

<https://securelist.com/analysis/quarterly-spam-reports/69932/spam-and-phishing-in-the-first-quarter-of-2015>

Règlement européen sur la protection des données : Renforcement des droits des personnes

✖	Règlement européen sur la protection des données : Renforcement des droits des personnes
---	--

Le règlement européen renforce les droits des personnes et facilite l'exercice de ceux-ci. Consentement renforcé et transparence

Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.

L'expression du consentement est définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. La matérialisation de ce consentement doit être non ambiguë.

De nouveaux droits

Le droit à la portabilité des données : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers. Il s'agit ici de redonner aux personnes la maîtrise de leurs données, et de compenser en partie l'asymétrie entre le responsable de traitement et la personne concernée.

Des conditions particulières pour le traitement des données des enfants : Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. L'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale. Les États membres peuvent abaisser cet âge par la loi, sans toutefois qu'il puisse être inférieur à 13 ans. Devenu adulte, le consentement donné sur un traitement doit pouvoir être retiré et les données effacées.

Introduction du principe des actions collectives : Tout comme pour la législation relative à la protection des consommateurs, les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles.

Un droit à réparation des dommages matériel ou moral : Toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable du traitement ou du sous-traitant réparation du préjudice subi.

source : CNIL



Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



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 téléphoniques, 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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Règlement européen sur la protection des données : ce qui change pour les professionnels | CNIL

Victime d'une arnaque vous

demandant de régler par coupons recharges PCS ? Pas de panique !

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES <i>fr</i></p>	 <p>LE NET EXPERT RGPD CYBER MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de détection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
<p>Denis JACOPINI</p>  <p>vous informe</p>	<p>Victime d'une arnaque demandant de régler par coupons recharges PCS ? Pas de panique !</p>				

Les escroqueries à la Carte prépayée et aux coupons recharges PCS Mastercard (ou Transcash ou Tonéo) se développent de plus en plus et ont tendance à remplacer certaines arnaques plus anciennes, mais désormais mieux détectées par les internautes

Par mail ou via Facebook, ils envoient tout d'abord soit un appel au secours venant d'une personne proche ou toute autre raison aboutissant à un chantage.

Ils demandent ensuite de recharger leur carte de crédit par ce nouveau moyen très moderne qu'est la carte prépayée PCS Mastercard. Souvent les personnes ne connaissent même pas le principe de rechargement de carte de crédit mais lorsque l'interlocuteur nous explique qu'il suffit simplement de descendre au bureau de tabac en bas de chez nous, d'acheter 1, 2, 3 ou 4 tickets de rechargement (coupons recharges), puis de lui envoyer les codes pour répondre à sa demande, beaucoup commencent à flairer le piège.

Ce moyen de paiement vient en remplacement des mandats cash ou des versement par Western Union qui ont aujourd'hui une telle mauvaise réputation que leur nom seul éveille des soupçons pour la plupart d'entre nous.. Il permet de rendre impossible de remonter jusqu'au destinataire par la voie judiciaire habituelle.

Ainsi, que ça soit quelqu'un qui se fait passer pour un ami qui vous signale avoir perdu ses papiers ou son téléphone en vous suppliant de l'aide par ce moyen de paiement ou une personne qui exerce sur vous un chantage :

- N'hésitez pas à porter plainte en commissariat de Police ou en Brigade de Gendarmerie (en fonction de votre résidence) ;
- Vous pouvez utiliser un site internet de pré-plainte sur Internet (<https://www.pre-plainte-en-ligne.gouv.fr>)
- Ne répondez plus à ses messages ;
- Signalez ses agissements sur www.internet-signalement.gouv.fr ;

Si vous avez du temps à perdre, vous pouvez aussi vous amuser à les mener en bateau, **les capacités de nuisance de ces arnaqueurs du dimanche étant très limitées** à seulement pouvoir vous envoyer des e-mails ou vous téléphoner si vous avez commis l'imprudence de leur communiquer votre numéro. Vous pouvez rétorquer en leur faisant croire que vous allez les payer ou que vous avez vous aussi besoin d'un coupon de recharge PCS pour vous déplacer pour aller en acheter un !

Attention :

Si vous êtes en contact avec une personne se présentant comme victime s'étant faite arnaquer par un escroc et que cette dernière vous communique ensuite les coordonnées d'un contact chez Interpol présenté comme son sauveur, fuyez ! Il s'agit aussi d'une arnaque.

Interpol ne rentre jamais en contact directement avec les victimes !

Ceux qui vous soutiennent le contraire ou qui vous contactent directement en se faisant passer pour Interpol ont malheureusement aussi pour objectif de vous soutirer de l'argent.

Plus d'infos sur : <https://www.lenetexpert.fr/contacter-interpol-en-cas-darnaque-est-une-arnaque/>

Remarque :

Il est possible qu'au moment où vous êtes sur le point de déposer plainte, la personne en face de vous cherche à vous dissuader. C'est normal, face aux faibles chances de retrouver l'auteur de l'acte délictueux, ils considèrent comme une perte de temps le fait de devoir traiter votre demande sous forme de plainte et vous inviteront à déposer une main courante.

Insistez pour déposer plainte car sans cette acte citoyen qu'on ne peut vous refuser (en faisant bien attention de le faire en mentionnant la bonne qualification juridique), vous ne laisserez pas passer la moindre chance (même si elle est minime) de faire arrêter l'escroc.

Pour information

- Les délits d'usurpation d'identité, pouvant être associé au phishing selon l'article 226-4-1 du code pénal sont punis d'un an d'emprisonnement et de 15 000 € d'amende.
- Selon l'article Article 312-1 du code pénal, le délit d'extorsion ou de tentative d'extorsion (demande d'argent en échange de ne pas supprimer des données ou de ne pas divulguer des secrets volés) est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.
- Les délits d'escroquerie ou tentative d'escroquerie, selon les articles 313-1, 313-2 et 313-3 du code pénal, sont punis de cinq ans d'emprisonnement et de 375 000 euros d'amende.

[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 : *Comment fonctionne une escroquerie à la Carte prépayée et aux coupons recharges PCS Mastercard, Transcash ou Tonéo? | Ms2i On Air*

Quoi et comment supprimer vos données si vous rendez votre ordinateur professionnel à votre employeur ?



Quoi et comment
supprimer vos
données si vous
rendez votre
ordinateur
professionnel à
votre employeur ?

stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) ?



Étape par
étape :
comment bien
effacer et
conserver vos
données
informatiques
stockées sur
votre
ordinateur
professionnel
si vous
changez de
travail à la
rentrée (et
pourquoi
c'est très
important) ?

Original de l'article mis en page : Étape par étape : comment bien effacer et conserver vos données informatiques stockées sur votre ordinateur professionnel si vous changez de travail à la rentrée (et pourquoi c'est très important) | Atlantico.fr

Déplacements professionnels. Attention au Wi-Fi de l'hôtel...



Déplacements
professionnels.
Attention au Wi-
Fi de l'hôtel...

De nos jours, qui réussirait à se passer d'Internet plus d'une journée, en vacances, en déplacement, lors d'une conférence ou au travail ? Nos vies aujourd'hui digitalisées nous poussent à nous connecter quasi automatiquement au premier réseau Wi-Fi disponible, quitte à mettre la confidentialité de nos données en danger.

Cela devient d'autant plus problématique lorsque nous voyageons : une étude Kaspersky Lab révélait récemment que 82% des personnes interrogées se connectent à des réseaux Wi-Fi gratuits non sécurisés dans des terminaux d'aéroports, des hôtels, des cafés ou des restaurants.

Dans la tribune ci-dessous, Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord analyse les vulnérabilités des réseaux Wi-Fi dans les hôtels, une mine d'or pour des cybercriminels en quête de données personnelles ou d'informations confidentielles.

Depuis 10 ans, le cyber crime s'est largement professionnalisé pour devenir une véritable industrie, portée sur la rentabilité. Les cybercriminels sont en quête permanente de victimes qui leur assureront un maximum de gains pour un minimum d'investissements techniques.

De son côté, l'industrie hôtelière a passé la dernière décennie à se transformer pour répondre aux nouvelles attentes digitales de ses clients. Alors que plus d'un quart d'entre eux annoncent qu'ils refuseraient de séjourner dans un hôtel ne proposant pas de Wi-Fi, la technologie n'est plus un luxe mais bien une question de survie pour les établissements hôteliers. Face aux ruptures liées à la numérisation, il a donc fallu repenser les modèles existants et s'équiper, parfois en hâte, de nouvelles technologies mal maîtrisées. Il n'était donc pas surprenant de voir émerger rapidement des problèmes de sécurité, dans les hôtels bon marché comme dans les 5 étoiles.

Par Tanguy de Coatpont, Directeur général de Kaspersky Lab France et Afrique du Nord

Le paradoxe du Wi-Fi à l'hôtel : privé mais public

Ils ont beau être déployés dans des établissements privés, les Wi-Fi d'hôtels restent des points d'accès publics. Ils sont même parfois complètement ouverts. Le processus de connexion, qui nécessite le plus souvent de confirmer son identité et son numéro de chambre, limite l'accès au réseau mais ne chiffre pas les communications. Il ne garantit pas non plus leur confidentialité. Est-ce que cela signifie que nos informations sont à la portée de tous ? La réalité n'est pas aussi sombre, mais elles sont à la portée de n'importe quel criminel équipé d'un logiciel de piratage, dont certains sont disponibles gratuitement en ligne, et disposant de connaissances techniques de base.

Concrètement, il suffit à un criminel de se positionner virtuellement entre l'utilisateur et le point de connexion pour récupérer toutes les données qui transitent par le réseau, qu'il s'agisse d'emails, de données bancaires ou encore de mots de passe qui lui donneront accès à tous les comptes de l'internaute. Une approche plus sophistiquée consiste à utiliser une connexion Wi-Fi non sécurisée pour propager un malware, en créant par exemple des fenêtres pop-up malveillantes qui invitent faussement l'utilisateur à mettre à jour un logiciel légitime comme Windows.

Le mythe de la victime idéale

En 2014, le groupe de cybercriminels Darkhotel avait utilisé une connexion Wi-Fi pour infiltrer un réseau d'hôtels de luxe et espionner quelques-uns de leurs clients les plus prestigieux. Un an plus tard, les activités de ce groupe étaient toujours en cours, continuant d'exfiltrer les données des dirigeants d'entreprises et dignitaires. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisateurs continuent de penser qu'ils ne courent aucun risque car les informations qu'ils partagent sur Internet ne méritent pas d'être piratées. C'est oublier que la rentabilité d'une attaque repose aussi sur le nombre de victimes. Parmi les 30 millions de clients pris en charge par l'hôtellerie française chaque année, seuls 20% sont des clients d'affaires. Les 80% de voyageurs de loisirs représentent donc une manne financière tout aussi importante pour des cybercriminels en quête de profit.

Dans certains cas, une faille Wi-Fi peut même exposer l'hôtel lui-même, en servant de porte d'entrée vers son réseau. Si l'on prend le cas d'une chaîne d'hôtellerie internationale qui disposerait d'un système de gestion centralisé et automatisé, une intrusion sur le réseau pourrait entraîner le vol à grande échelle d'informations confidentielles et bancaires sur les employés, le fonctionnement de l'hôtel et ses clients.

Hôtels indépendants vs. chaînes hôtelières : des contraintes différentes pour un même défi

Pour une industrie aussi fragmentée que celle de l'hôtellerie, la sécurité est sans aucun doute un défi. Les hôtels indépendants ont une capacité d'accueil réduite et traitent donc moins de données. Le revers de la médaille est qu'ils disposent souvent d'une expertise informatique limitée et leur taille ne permet pas de réaliser les économies d'échelle qui rentabiliseraient un investissement important dans la sécurité informatique. Quant aux grands groupes, qui comptent des ressources humaines et financières plus importantes, ils sont mis à mal par l'étendue de leur écosystème, qui rend difficile l'harmonisation d'une politique de sécurité sur des centaines, voire des milliers de sites.

Il est important que tous les hôtels, quelle que soit leur taille ou leur catégorie, respectent quelques règles simples à commencer par l'isolation de chaque client sur le réseau, l'utilisation de technologies de chiffrement et l'installation de solutions de sécurité professionnelles. Enfin, le réseau Wi-Fi offert aux clients ne doit jamais être connecté au reste du système informatique de l'hôtel, afin d'éviter qu'une petite infection ne se transforme en épidémie généralisée. En respectant ces règles, la sécurité pourrait devenir un argument commercial au moins aussi efficace que le Wi-Fi.

Article original de Robert Kassouf

Denis JACOPINI est Expert Informatique et aussi **formateur en Cybercriminalité** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Nous pouvons vous animer des **actions de sensibilisation ou de formation** à la Protection des Données Personnelles, au risque informatique, à l'hygiène informatique et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Plus d'informations sur : <https://www.Lenetexpert.fr/formations-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI



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.

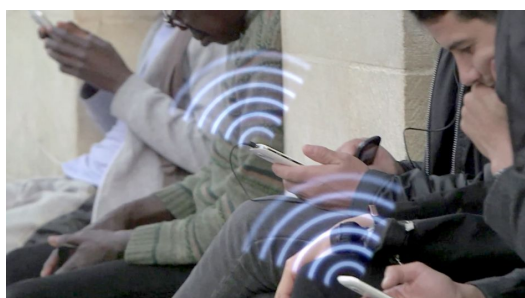


[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Etude Kaspersky sur le Wi-Fi à l'hôtel... | InfoTravel.fr

Comment se comporte notre cerveau surchargé par le numérique



Comment se
comporte notre
cerveau
surchargé par le
numérique

**Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées :
« HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».**

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être. Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression... : si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52'), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours !
si vous ne voyez pas la vidéo, le lien



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.



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Hyperconnectés : le

cerveau en surcharge