

Victime d'un prélèvement frauduleux sur votre compte bancaire ? Que faire ? | Quelques conseils... | Denis JACOPINI

Victime d'un prélèvement frauduleux sur votre compte bancaire ? Que faire ?

Malgré toutes les actions que nous menons pour vous former au risque en cybercriminalité ou tous les efforts pour vous sensibiliser, vous êtes victime d'une arnaque sur Internet. Alors, que faire ?



Vous avez constaté un débit frauduleux sur votre compte bancaire ?

Les raisons peuvent être multiples. Carte bancaire copiés, votre numéro de carte bancaire généré aléatoirement, numéros de votre carte bancaire interceptés, virus ou logiciel d'espionnage informatique etc.



1) Tout d'abord, faites le plus vite possible opposition sur votre CB

en appelant le service interbancaire des cartes perdues ou volées qui est disponible 7 jours sur 7 au 08 92 705 705 (0,34€/min). Cela permettra d'éviter d'autres prélèvements frauduleux.



2) Contactez votre conseiller bancaire

pour lui expliquer l'arnaque dont vous avez été victime pour récupérer votre argent. La banque devrait vous proposer de vous rembourser sans délai. Si vous rencontrez des difficultés pour vous faire entendre, évoquez l'article de loi suivant :

L'Article L133-18 du code monétaire et financier précise :

» En cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues à l'article L. 133-24, le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans l'état où il se serait trouvé si l'opération de paiement non autorisée n'avait pas eu lieu. Le payeur et son prestataire de services de paiement peuvent décider contractuellement d'une indemnité complémentaire «

3) Portez plainte au commissariat ou à la gendarmerie la plus proche.

Le Défenseur des droits a pu constater que les policiers incitent les plaignants à ne déposer qu'une main courante, et non une plainte.

- La main courante est simplement déclarative; elle n'implique pas que la justice soit informée, ni qu'une investigation soit lancée; elle pourra seulement être versée à l'instruction si une procédure judiciaire a lieu.

- La plainte, en revanche, suppose une transmission au procureur de la République qui décide des suites à y donner.

Il est vrai que si les escrocs sont à l'autre bout du monde, il y a peu de chance que la police de notre pays réussisse à mettre un terme à leurs agissements... mais déposez plainte ! Ainsi votre cas sera connu des services de Police et cela pourra vous prévenir contre d'éventuelles complications suite à l'arnaque que vous avez subie. En effet les escrocs pourraient profiter des données qu'ils ont pour multiplier leurs méfaits. En portant plainte, vous montrez à la police que vous êtes bien une victime et que vous en subissez les conséquences.

Enregistrer votre plainte est une obligation des services de Police ou de Gendarmerie en vertu de l'article 15-3 du code de procédure pénale et de la Charte de l'accueil du public et de l'assistance aux victimes.

Ils sont censés enregistrer une plainte dès que la demande est émise, quels que soient le lieu où a été commise l'infraction et le lieu de résidence de la victime, et sans que cette dernière ait besoin d'apporter pour cela un quelconque élément de preuve (certificat médical, devis, etc).

Munissez-vous de tous les renseignements suivants :

- une pièce d'identité ;
- votre relevé bancaire sur lequel figure(nt) le (ou les) paiement(s) contesté(s) ;
- les coordonnées de votre banque ;
- les références de votre carte bancaire ;
- tout autre renseignement pouvant aider à l'identification de l'escroc.

Suite à ce dépôt de plainte, une enquête sera ouverte et transmise au procureur de la République.

4) Vous pouvez aussi appeler « Info Escroqueries »

N'oubliez pas le numéro « Info Escroqueries » 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0,06 €/minute depuis un téléphone mobile) à utiliser si à la base, vous avez été la cible d'un e-mail frauduleux ou d'une escroquerie.



5) Rechercher l'origine de l'escroquerie

Une fois les actions précédentes réalisées, afin d'éviter que le problème ne se reproduise, il est indispensable d'identifier l'origine du prélèvement frauduleux. Par exemple, si votre système informatique s'est fait pirater, l'arnaque se reproduira.

Pour cela, contactez un expert informatique spécialisé en cybercriminalité.

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

Consommateurs, exercez vos droits auprès de la CNIL | Denis JACOPINI



Participer à un concours, demander une carte de fidélité, remplir un formulaire sur internet, ou simplement poster sur les réseaux sociaux, nous transmettons très souvent des données personnelles à des organismes.

Grâce à la loi Informatique et Libertés, vous bénéficiez de droits spécifiques que vous pouvez – dans la plupart des cas – faire valoir vous-mêmes.

Droit d'accès

Droit de rectification

Droit d'opposition

Droit au déréférencement



Réagissez à cet article

Source : *Exercer vos droits – CNIL – Commission nationale de l'informatique et des libertés*

Comment se connecter de manière sécurisée à un wifi public ? | Denis JACOPINI



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) ;
- vous voler, crypter des documents ou exercer un chantage pour que vous puissiez les récupérer ;
- usurper votre identité et réaliser des actes illégaux ou terroristes sous votre identité ;
- accéder à des informations bancaires et vous spolier de l'argent.

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 même 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 et conseillons le logiciel VPN HotSpot Shield. Ce logiciel rendra vos connections Wifi publiques tranquilles. Téléchargez et découvrez gratuitement HotSpot Shield
Notre page de présentation de 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.

Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d'une cyberattaque ?



Rançongiciel
et
hameçonnage
: quelle
démarche
entreprendre
si vous êtes
là, cible
d'une
cyberattaque
?

Les ordinateurs contiennent des documents privés et données confidentielles (renseignements personnels, identifiants bancaires, codes secrets) qui peuvent être convoités par une tierce personne mal intentionnée. En cas de cyberattaque, il est important de savoir réagir vite pour se protéger d'une utilisation frauduleuse de vos données personnelles. Nous expliquons ici les principales cybermenaces qui planent sur les internautes, les recommandations de sécurité pour s'en prémunir et, surtout, comment agir si vous êtes la victime d'un cybercriminel.

Les recommandations de sécurité pour se protéger des cyber-escrocs

Selon l'ANSII (agence nationale de la sécurité des systèmes d'information), il vous est fortement conseillé de respecter quelques règles simples pour vous protéger contre les cyberattaques. Effectuer des sauvegardes régulières de vos fichiers importants sur des supports de stockage amovibles (CD, clé USB, disque dur externe). Mettre à jour régulièrement les principaux logiciels de vos appareils numériques (ex : Windows, antivirus, lecteur PDF, navigateur, etc.) en privilégiant leur mise à jour automatique. Ne pas avoir une confiance aveugle dans le nom de l'expéditeur de l'email. En cas de doute, n'hésitez pas à contacter directement l'expéditeur par un autre moyen de communication. Se méfier de courriel type « hameçonnage ciblé » qui vous propose un contenu personnalisé pour mieux tromper votre vigilance. Ne pas ouvrir les pièces jointes et ne pas suivre les liens des messages électroniques douteux (fautes d'orthographe, caractères accentués, nom des pièces jointes trop succinct). Ne jamais répondre à une demande d'information confidentielle par courriel.

En cas de cyber-attaque, il faut immédiatement déconnecter du réseau tout appareil susceptible d'être infecté et alerter au plus vite le responsable de sécurité ou le service informatique. Dans le cadre d'un rançongiciel, il est primordial de ne pas payer la rançon, car il n'est nullement garanti que la victime récupère la clé de déchiffrement qui lui permettra de récupérer l'accès à ses données personnelles.

Comment réagir si vous êtes victime d'un rançongiciel ou d'hameçonnage ?

Vous devez vous rendre dans un commissariat de police ou une brigade de gendarmerie pour déposer plainte, ou bien adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent.

Pour mener correctement l'enquête, il faudra fournir les renseignements suivants.

- Les références du (ou des) transfert(s) d'argent effectué(s).
- Les informations de la (ou des) personne(s) contactée(s) : pseudos utilisés, adresse de messagerie ou adresse postale, numéros de téléphone, fax, copie des courriels...
- Le numéro complet de la carte bancaire ayant servi au paiement, la référence de votre banque et de votre compte, et la copie du relevé de compte bancaire où apparaît le débit frauduleux.
- Tout autre renseignement utile à l'identification du cyber-escroc.

Vous pouvez également utiliser la plateforme de signalement Pharos ou le numéro de téléphone dédié : 0811 02 02 17 pour signaler les faits dont vous avez été victime. La suite de l'enquête sera prise en charge par des services spécialisés...[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, suivez nos formations ;

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

COLLECTE & RECHERCHE DE PREUVES : Nous mettrons 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 nombreuses formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration et vous accompagnons dans l'établissement d'une analyse d'impact et de votre mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettrons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assisterons 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))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRET n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Source : *Rançongiciel et hameçonnage : quelle démarche entreprendre si vous êtes la cible d'une cyberattaque ?*

RGPD dans les collectivités : Que faut-il mettre en oeuvre ?

Denis JACOPINI est Expert en Cybercriminalité et en Protection des Données à Caractère Personnel.

Notre métier :

Animation de formations et de conférences

Cybercriminalité (virus, espions, piratages, fraudes, arnaques Internet)

Protection des Données à Caractère Personnel (mise en conformité avec la CNIL et le RGPD)

Audits sécurité, Expertises techniques et judiciaires

Audit sécurité (ISO 27005) ;

ID Swatting

Recherche de preuves (Investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;

Expertises de systèmes de vote électronique ;

Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?

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

 LE NET EXPERT AUDITS & EXPERTISES	 EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES LENETEXPERT .fr	 RGPD CYBER	 SPY DETECTION Services de détection de logiciels espions	 LE NET EXPERT FORMATIONS	 LE NET EXPERT ARNAQUES & PIRATAGES
 Denis JACOPINI DENIS JACOPINI EXPERT INFORMATIQUE ASSESSMENT SPECIALISE EN CYBERCRIMINALITE vous informe		Formation en Cybercriminalité : Arnaques, virus et demandes de rançons, Comment s'en protéger ?			

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.

Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?

Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène.

OBJECTIF DE LA FORMATION EN CYBERCRIMINALITE :

La formation en cybercriminalité a pour but de créer des déclics chez les utilisateurs, mettre à jour les connaissances des informaticiens et faire prendre conscience aux chefs d'entreprises des risques en couvrant les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer le phénomène de la cybercriminalité.

PROGRAMME :

- Etat des lieux de la cybercriminalité en France et dans le monde;
- Les principaux cas de piratages et d'arnaques expliqués ;
- Les bonnes pratiques au quotidien pour limiter les risques ;
- Etude de vos témoignages, analyse de cas et solutions.
- PUBLIC CONCERNÉ : Utilisateurs, chefs d'entreprise, présidents d'associations, élus....

MOYENS PÉDAGOGIQUES :

- Support de cours pour prise de notes
- Résumé remis en fin de cours.
- Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

CONDITIONS D'ORGANISATION

- Formations individuelles ou en groupe
- Formations dispensées dans vos locaux ou organisées en salle de formation partout en France en fonction du nombre de stagiaires.

Téléchargez la fiche de présentation / Contactez-nous

QUI EST LE FORMATEUR ?

Denis JACOPINI est Expert Informatique assermenté, diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire et a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Il anime dans toute le France et à l'étranger des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles.

A ce titre, il intervient régulièrement sur différents médias et sur La Chaine d'Info LCI pour vulgariser les sujets d'actualité en rapport avec ces thèmes.

Spécialisé en protection des données personnelles, il accompagne les établissements dans leur mise en conformité CNIL en les accompagnant dans la mise en place d'un Correspondant Informatique et Libertés (CIL).

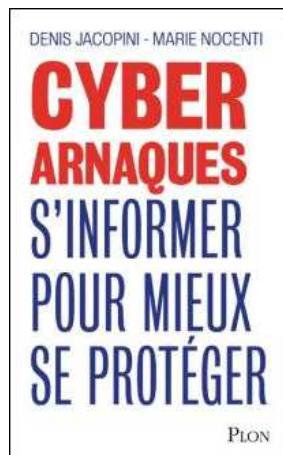
Enfin, il intervient en Master II dans un centre d'Enseignement et de Recherche en Informatique, en Master Lutte contre la Criminalité Financière et Organisée, au Centre National de la Fonction Publique Territoriale et anime le blog LeNetExpert.fr sur lequel il partage et publie de très nombreuses informations sur ses thèmes de prédilection.

Denis JACOPINI peut facilement être contacté sur :

<http://www.leNetExpert.fr/contact>

[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 Millions de victimes de la Cybercriminalité 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](https://www.fnac.fr)

Arnaque à la webcam : des conseils pour bien réagir –

Denis JACOPINI

 **#Arnaque à la webcam : des conseils pour bien réagir**

Alors que les arnaques à la webcam se multiplient et touchent chaque années des milliers de victimes, la CNIL publie un guide de ces pratiques.

Pour chaque situation particulière, l'arnaque semble se dérouler à peu près de la même façon : la victime se rend la plupart du temps sur un site de rencontre, et entame la conversation avec une jeune femme ou un jeune homme au physique plutôt attrayant. La victime se voit alors proposer de continuer la conversation par Webcam, et s'exécute. Le cyber-escroc fait une capture d'écran, et menace de diffuser la vidéo ou les images de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos, si la personne ne lui remet pas la somme de 200 euros sous 24/48h.

Afin de faire face à cette situation, la Commission nationale de l'informatique et des libertés (CNIL) a publié une fiche pratique, destinée à informer et accompagner les victimes de ces cyber escrocs. Il y est notamment indiqué :

- qu'il ne faut surtout pas répondre aux tentatives de chantage du cyber-escroc ;
- qu'il convient d'alerter les autorités compétentes, via la plateforme du Ministère de l'intérieur ;
- qu'il faut demander au site de dépublier le contenu gênant ;

Rappelons que des sociétés, spécialisées dans l'effacement des contenus gênants, existent. De plus, et depuis un arrêt rendu par la Cour de justice de l'Union européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leur nom et prénom.

Quel réflexe adopter ?

1. Ne répondez surtout pas à un cyber-escroc

Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, ne versez surtout pas d'argent quel que soit la somme demandée.

2. Verrouillez immédiatement vos comptes sociaux

Paramétrez vos comptes sociaux professionnels et vos comptes Facebook de manière à ce que le malfaiteur n'associe pas votre nom à une liste d'amis / de contacts. Ne rendez accessible votre profil Facebook qu'auprès de vos amis de confiance. Enfin, ne publiez rien de personnel sur votre mur. Des personnes mal intentionnées peuvent détourner ces informations à d'autres fins. Notre page Facebook délivre quelques conseils pour bien paramétrer vos comptes.

3. Alertez les autorités via la plateforme du Ministère de l'Intérieur

Effectuez des captures d'écran justifiant votre situation (messages reçus, contenus à effacer ...). Voir la fiche pratique

4. Signalez directement l'escroquerie sur la plateforme www.internet-signalement.gouv.fr

Renseignez-vous via le service Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile ; Du lundi au vendredi de 9h à 18h)

5. Parlez-en à une personne de confiance

La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance. Vous êtes mineur ? Des télé-conseillers sont gratuitement à votre écoute au 0800 200 000 de 9h à 19h en semaine. Voir le site Net écoute

6. Informez vos amis de l'escroquerie

Veillez à informer discrètement les personnes susceptibles d'être sollicitées par le cyber-escroc en mentionnant sobrement que vous êtes victime d'une escroquerie en ligne et qu'il ne faut ni ouvrir, ni partager, ni répondre à une éventuelle sollicitation provenant d'un inconnu.

7. Effectuez régulièrement des recherches à votre nom

Vous pouvez par exemple programmer une alerte à votre nom qui vous enverra un message sur votre webmail dès qu'un contenu associé à votre nom est mis en ligne. Certains services existent ici ou là. **Si la vidéo a été diffusée ...**

8. Demandez systématiquement au site de dépublier le contenu gênant

Exemple : si la vidéo a été mise en ligne sur Youtube : demandez à Youtube de supprimer cette vidéo. Si le site ne répond pas à votre demande sous deux mois, adressez vous à la CNIL en suivant la procédure de notre formulaire de plainte en ligne.

9. En parallèle, demandez au moteur de recherche de déréférencer le contenu en cause

Depuis un récent arrêt de la cour de justice européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leurs nom et prénom.

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

formateur n°93 84 03041 84



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, contenus, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondant Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Sources :

<http://www.net-iris.fr/veille-juridique/actualite/34611/arnaque-a-la-webcam-la-cnil-donne-des-conseils-pour-bien-reagir.php>

<http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/reagir-en-cas-de-chantage-a-la-webcam>

Vie privée en danger : pourquoi nous sommes tous concernés | Denis JACOPINI

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

 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
 Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité informatique - Cybercriminalité vous informe...	Vie privée en danger : pourquoi nous sommes tous concernés				

Est-il possible de rentrer chez nous, d'écouter nos conversations et de s'immiscer dans notre intimité sans y être invité ? Nous avons découvert qu'il suffit pour cela d'une simple connexion Internet. Ordinateur, téléphone portable, réseaux sociaux et même cartes bancaires : désormais nous sommes en permanence connectés les uns aux autres. Mais nos informations personnelles sont-elles réellement bien protégées ? Pas si sûr...

Chaque semaine, de nouveaux scandales éclatent comme, par exemple, le vol, il y a quelques jours, de milliers de photos intimes de stars américaines. Et cela nous concerne tous : « phishing », vol d'identité, harcèlement numérique, vols de compte bancaire : chaque seconde, 17 personnes sont victimes de cyber-escroqueries à travers le monde. Car Internet a créé une nouvelle génération d'escrocs 2.0. Leur butin s'élèverait l'année dernière à 400 milliards de dollars. Un chiffre en constante augmentation. Nous avons découvert les failles des nouvelles cartes bancaires NFC, sans contact. Désormais, les pickpockets n'ont plus besoin de mettre la main dans votre sac pour voler votre argent.

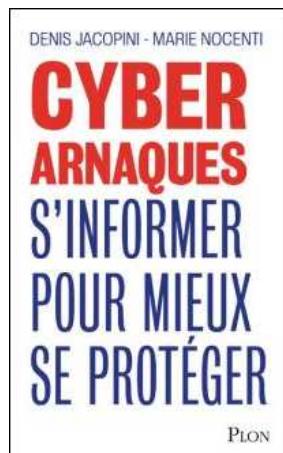
Nous allons vous raconter l'histoire de différentes victimes françaises. Celle de Laetitia, en proie au cyber-harcèlement, qui a failli mettre fin à ses jours. Stéphane, lui, pensait avoir rencontré l'amour sur la toile ; il était en fait entre les mains de brouteurs de Côte d'Ivoire. Nous avons remonté leurs traces à Abidjan.

Nous nous sommes également rendus en Roumanie dans une ville hors du commun que le FBI a surnommée Hacker-ville. Là-bas, une grande partie de la population vivrait des cyber-escroqueries. Certains escrocs ont accepté de nous rencontrer ; d'autres après avoir été arrêtés par les forces de l'ordre ont décidé de mettre leur génie informatique au service de la société.

Enfin, vous découvrirez que pour protéger leurs ados des dangers du web, des parents ont trouvé une solution radicale. Christophe est un papa espion : il contrôle les moindres faits et gestes de ses trois enfants. Grâce à une panoplie de logiciels et d'applications, il a accès à l'intégralité du contenu de leur téléphone et ordinateur. Internet est sans aucun doute la principale révolution de ces trente dernières années mais c'est peut-être aussi la fin de la vie privée.

[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 Millions de victimes de la Cybercriminalité 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

Source :
http://www.m6.fr/emission-zone_interdite/28-09-2014-vie_privee_en_danger_pourquoi_nous_sommes_tous_concernes/

Les 5 techniques de phishing les plus courantes | Denis JACOPINI

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



LE NET EXPERT
AUDITS & EXPERTISES

EXPERTISES DE SYSTÈMES DE VOTES ÉLECTRONIQUES
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

Les 5 techniques de phishing les plus courantes

L'ère des attaques ciblées est en marche

Le spam est aujourd'hui plus une nuisance qu'une réelle menace. En effet, les tentatives de vendre du viagra ou encore de recevoir l'héritage d'un riche prince d'une contrée éloignée ne font plus beaucoup de victimes. La majorité des solutions antispm bloquent ces emails et l'unique façon de les voir consiste à consulter votre dossier « courrier indésirable ». Toutefois, une menace bien plus sophistiquée et dangereuse atterrit dans votre boîte de réception. Vous ciblant vous et vos employés. Connus sous le nom de « phishing » ou « hameçonnage », ces emails cherchent à piéger vos employés. Comment ? Simplement en leur demandant d'effectuer une action. Dans la vie, il y a deux façons d'obtenir ce que l'on veut : soit le demander gentiment, soit être la bonne personne (et avoir l'autorité qui convient). Le phishing et son cousin le spear phishing, rassemblent ces deux conditions. Le principe du phishing consiste à usurper l'identité d'une personne ou d'une organisation et simplement demander d'exécuter une action (modification de mot de passe, vérification d'une pièce jointe, etc.). L'attaque est orchestrée autour de deux éléments : l'email et le site web ou une pièce jointe. L'email de phishing demande à ses victimes de se connecter à une page et d'entrer leurs identifiants afin d'effectuer une action qui semble légitime. Concrètement, il s'agit par exemple de faux emails de votre fournisseur d'électricité vous avertissant de régulariser votre facture... au plus vite !

L'impact du phishing en entreprise

Des milliers de phishing sont envoyés quotidiennement (contre des millions pour le spam) par des organisations de cybercriminels ou des gouvernements étrangers (ou les deux quand ce dernier « soustrait »). Cette menace n'est pas encore bien maîtrisée par la majorité des antispm et anti-virus sur le marché pour plusieurs raisons. Premièrement, le « faible » volume d'emails de phishing ne permet pas d'être détecté par la majorité des solutions reposant sur une base de signatures. Deuxièmement, l'email semble légitime et ne reprend pas les « codes » du spam. Le phishing est une réelle menace pour les entreprises, car il y a deux façons d'être victime : voir sa marque usurpée ou tomber dans le piège quand on reçoit l'email. Dans les deux cas, voici les 4 principaux dégâts que le phishing peut causer à votre entreprise :

Nuire à votre réputation si votre marque est utilisée pour dupper des internautes. Bien souvent, vous ne savez même pas que votre marque est utilisée à des fins malicieuses.

Perde de données sensibles, de propriétés intellectuelles ou encore de secrets industriels.

Divulgation de vos données clients et partenaires.

Des pertes financières directes liées au vol, à des amendes ou au dédommagement de tiers.

Selon une étude de l'américain Verizon, 11% des récepteurs de phishing cliquent sur le lien !

Les 5 techniques de phishing les plus répandues

Pas si évident que cela à identifier. Tout le monde peut se laisser duper par manque de vigilance par un email de phishing, car celui ci semble légitime et original.

Voici ci-dessous les 5 techniques qu'utilisent les phiseurs pour attaquer votre entreprise. Dans nos exemples, nous parlerons de Pierre, un salarié aux responsabilités moyennes, travaillant dans le service finance de son entreprise, et qui a des journées bien remplies.

Le premier exemple de la série correspond à un phishing de masse, alors que les 4 suivants seront plus ciblés, reprenant l'art du Spear Phishing, qui nécessite des recherches avancées sur les cibles afin d'être crédible et de présenter l'autorité qui convient. Dans ces cas là, Alain sera le patron de Pierre, information facilement trouvable sur le site internet de la société.

1. Abus de confiance

Pierre reçoit un email lui demandant de confirmer un transfert d'argent. L'email contient un lien envoyant vers un site qui se présente comme celui de sa banque... mais en réalité il s'agit d'une copie, éditée, contrôlée et hébergée par des pirates. Une fois sur la page, Pierre entre normalement ses identifiants mais rien ne se passe et un message disant que le site est « temporairement indisponible » apparaît. Pierre étant très occupé, se dit qu'il s'en occupera plus tard. En attendant, il a envoyé ses codes d'accès aux pirates.

2. Fausse loterie

Pierre reçoit un email lui indiquant qu'il a gagné un prix. Habituellement Pierre n'y prête pas attention, car bien trop occupé. Toutefois, cette fois ci, l'email est envoyé par Alain, mentionnant une organisation caritative qu'ils soutiennent mutuellement. Pierre clique alors sur le lien, rien ne se passe à l'écran, mais un malware s'est installé sur son poste de travail.

3. Mise à jour d'informations

Pierre reçoit un email d'Alain lui demandant de regarder le document en pièce jointe. Ce document contient un malware. Pierre ne s'est rendu compte de rien, en ouvrant le document, tout semblait correct bien qu'incohérent par rapport à son travail. Résultat, le malware enregistre tout ce que fait Pierre sur son poste (keylogger) depuis des mois, ce qui met en danger tout le Système d'Information de l'entreprise facilitant le vol de données.

4. Appel à donation

Pierre reçoit un email du frère d'Alain, lui disant qu'il est atteint d'un cancer et que sa couverture sociale s'est arrêtée. Voulant faire bonne impression auprès de son patron, Pierre clique sur le lien et se rend sur le site de donation dédié. Pierre décide de faire une donation de 100€ et entre ses informations bancaires. Le site précise même que le don est déductible des impôts... Trop tard, Pierre a donné ses informations et se fait débiter d'un montant bien supérieur ! Sans pouvoir le déduire de ses impôts...

5. Usurpation d'identité

Pierre reçoit un email d'Alain, lui demandant d'effectuer un virement auprès d'un fournisseur connu au sujet d'une avance concernant un dossier urgent. Pour Pierre, il s'agit d'une tâche de routine qu'il effectue aussitôt. L'argent est envoyé sur un compte étranger, impossible à tracer et ne sera jamais retrouvé.

Les attaques de phishing et spear phishing sont en augmentation, tant sur le nombre que sur leur niveau de sophistication. Si vos employés reçoivent ce type d'email il y a de forte chance qu'ils se fassent piéger.

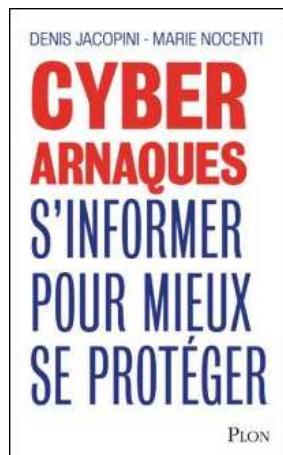
Qu'est ce qui peut être fait pour protéger vos employés ?

Pour se protéger contre phishing, la majorité des entreprises se contentent de leur antispm et d'autres logiciels anti-virus ou de blocage des sites web. Toutefois, face à l'augmentation et à la sophistication des attaques, cette menace nécessite une protection dédiée. Les solutions antispm et virus classiques ne sont plus suffisantes. Il reste la formation des employés, efficace mais trop peu utilisée et qui nécessite d'être régulière.

Les organisations ont besoin de solutions dédiées à cette menace qu'est le phishing qui nécessite une analyse particulière pour être identifiée et bloquée. Les cybercriminels font évoluer leurs techniques rapidement mais la riposte technologique s'organise également, et certaines solutions anti-phishing sont désormais capables de bloquer tous les types de phishing et spear phishing en analysant chaque lien ainsi que les habitudes des échanges. Mais au delà de ce socle technologique nouveau et efficace, l'arme ultime pour contrer les phishing reste l'humain, et sur ce point le travail de formation et d'éducation reste énorme !

[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 Millions de victimes de la Cybercriminalité 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

Source : *Les 5 techniques de phishing les plus courantes | Programmez!*

Mot de passe Wifi : trois

quarts des foyers français à la merci d'une attaque | Denis JACOPINI

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

#Mot de passe Wifi : trois quarts des foyers français à la merci d'une attaque

Trois ménages français sur quatre ne protègent pas correctement leur borne wifi, rendant leurs ordinateurs, téléphones et tablettes accessibles aux pirates informatiques.

Près de trois ménages français sur quatre ne protègent pas correctement leur borne wifi domestique, rendant leurs ordinateurs, téléphones et autres équipements connectés aisément accessibles aux pirates informatiques, selon une étude publiée jeudi par l'éditeur de logiciels antivirus Avast Software.

D'après cette enquête, menée en novembre auprès de plus de 16 000 internautes français équipés d'un réseau wifi domestique, « la vaste majorité des routeurs (...) ne sont pas sécurisés ».

Mot de passe inexistant... ou évident

Les Français sont ainsi 10% à déclarer ne pas utiliser de mot de passe pour protéger leur réseau wifi et 24% à utiliser comme mot de passe « leur adresse, leur nom, leur numéro de téléphone, le nom de leur rue ou d'autres mots faciles à deviner ».

En outre, plus de la moitié des routeurs sont « mal sécurisés par défaut », avec des combinaisons de codes d'accès « beaucoup trop évidentes, telles que 'admin/admin' ou 'admin/motdepasse' », selon Avast.

Selon l'éditeur d'antivirus, 5% des bornes wifi françaises sont même « accessibles de l'extérieur » du domicile. Une proportion identique de sondés admet d'ailleurs avoir utilisé le réseau d'un de leurs voisins à son insu.

Un Français sur cinq a déjà été piraté

Le manque de sécurité des routeurs en fait « des points d'entrée très faciles d'accès pour les hackeurs, qui sont dès lors capables de pirater des millions de réseaux domestiques en France », a affirmé Vince Steckler, directeur général d'Avast, lors d'un point de presse.

Un Français sur cinq rapporte avoir déjà subi un piratage informatique, et 34% redoutent un vol d'informations personnelles ou de données bancaires et financières. Cependant, 42% sont persuadés que leur réseau domestique est suffisamment sûr.

Rappelons qu'un mot de passe, pour être le plus efficace possible, doit comporter des caractères aplha-numériques (lettres minuscules, majuscules, chiffres) et, si possible, des caractères spéciaux.

Et que les mots de passe les plus utilisés l'an dernier – et donc les plus faciles à « craquer » – étaient les suivants :

123456
password
12345678
qwerty
abc123
123456789
111111
1234567
iloveyou
123123
Admin
1234567890
Un conseil : évitez-les !

[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/informatique-wifi-trois-quarts-des-foyers-francais-la-merci-dune-cyberattaque-3026280>