Tout ce que vous ne savez pas sur les clés USB | Denis JACOPINI



Tout ce que vous ne savez pas sur les clés USB La majorité des personnes savent très bien que la clé USB est un support de stockage amovible, c'est ce qui leur fait penser qu'une clé USB permet uniquement de stocker des fichiers à partir de tout système disposant de prises USB ou de transférer des données entre ordinateur.Or la clé USB peut être utilisée de plusieurs manière différentes.



Aujourd'hui, je vais vous montrer qu'il existe d'autres fonctions plus intéressante qu'on peut les utiliser à l'aide d'une simple clé USB.

1.Transformer votre clé USB à une barrette mémoire RAM

Une clé USB peut être utiliser pour améliorer les performances de votre ordinateur et augmenter la vitesse de son fonctionnement. L'astuce consiste à utiliser une clé USB pour augmenter la mémoire de votre ordinateur et booster ses performances à l'aide de logiciel eBoostr. Pour en savoir plus, je vous invite à lire cet article: l'utilisation de clé USB en tant que barrette.

2.Sécuriser votre PC avec une clé USB

On peut aussi utiliser une clé USB pour sécuriser son PC. L'utilitaire Rohos Logon Key fera en sorte que votre ordinateur s'ouvrira automatiquement au moment où vous insérerez la clé USB et se verrouillera lorsque vous la retirerez. Vous pourrez donc quitter votre ordinateur en toute sérénité. Pour en savoir plus, je vous invite à lire l'article suivant: la sécurité de votre pc avec une clé USB

3.Création d'une clé USB rootkit

Une autre fonction qu'on peut l'utiliser avec une clé USB, c 'est la récupération des mots de passe d'un ordinateur. La clé USB s'exécute automatiquement et récupère la plupart des mots de passe stockés sur votre ordinateur. Il est vraiment très utile surtout quand on perd les mots de passe. Pour en savoir les étapes pour créer une clé USB rootkit, je vous invite à lire cet article: création d'une clé USB rootkit.

4.Injecter une backdoor dans une machine Windows avec une clé USB

On peut aussi utiliser une clé USB pour accéder à votre PC à distance depuis n'importe quelle machine. Pour créer votre USB backdoor suivez les étapes de notre article: injection d'une backdoor dans une machine Windows avec une clé USB.

5.Emporter dans une clé USB vos logiciels préférés sans avoir besoin de les installer

Enfin, une autre fonction qui pourrait vous intéresser: c'est d'utiliser des logiciels stockés sur votre clé USB sans avoir besoin de les installer. Pour cela, il faut installer le programme gratuit **PortableApps** .

Il devient alors très facile d'ajouter vos logiciels préférés au lanceur d'applications portable « PortableApps ». Un outil principalement destiné aux développeurs qui enrichit et complète la suite logicielle référence en la matière. Le logiciel Open Source PortableApps propose déjà un panel très large d'applications portables : Firefox, LibreOffice, Google Chrome, Skype ou encore Dropbox. Ce lanceur vous permet d'utiliser les logiciels stockés sur la clé USB depuis un autre PC sans avoir à les installer.

Comme nous l'avons vu précédemment, une clé USB peut servir à autre chose qu'à stocker des données. Elle possède d'autres avantages. Si vous avez d'autres fonctions d'une clé USB, n'hésitez pas de les partager avec nous dans un commentaire .

Article original de Ahmed



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

Original de l'article mis en page : Tout ce que vous ne savez pas sur les clés USB | FunInformatique

Fraude sur Internet : comment éviter les pièges | Denis JACOPINI



Les fraudes sur Internet sont de plus en plus fréquentes. Apprenez à éviter les pièges tendus par ces pirates qui se font passer pour EDF, la Caf ou encore l'Assurance maladie.

Si vous bénéficiez d'une aide de la Caf, êtes client EDF ou assuré social, il est possible que vous soyez victimes d'arnaques sur Internet appelées phishing.

Des pirates envoient des e-mails frauduleux pour récupérer vos données personnelles, vous soutirer de l'argent, voire usurper votre identité.

En quoi consiste le phishing ?

Le phishing (ou hameçonnage) est une fraude pratiquée par des pirates informatiques. Ils envoient en masse et de manière aléatoire de faux e-mails en prenant l'identité de grandes sociétés ou organismes.

Leur objectif : recueillir vos données personnelles afin de vous escroquer. Ils peuvent tenter de récupérer :

- les données d'accès à votre espace personnel ;
- le numéro de votre carte bancaire, votre RIB ;
- votre adresse postale…

Le plus souvent, les messages frauduleux vous informent d'un retard de paiement, d'un remboursement, ou proposent de mettre à jour vos informations personnelles.

Ne cliquez pas sur les liens présents dans ces e-mails car ils peuvent contenir des virus et rediriger vers des sites non sécurisés.

Comment identifier une tentative de phishing ?

EDF, la Caf et l'Assurance maladie ne demandent jamais de coordonnées bancaires par e-mail (numéro de compte, numéro de carte bancaire, cryptogramme).

Ces données sont strictement confidentielles et sont uniquement requises dans votre espace personnel pour le paiement d'une éventuelle facture par carte bancaire ou par prélèvement automatique.

Afin de ne pas être victime d'une arnaque sur Internet, il est conseillé de regarder :

- l'adresse du site Internet dans la barre de navigation : sécurisée, elle commence toujours par « https » (et non pas « http ») ;
- l'adresse Internet de votre espace personnel. Elle est aussi sécurisée et commence par « https » ;
- l'exactitude de vos informations dans l'espace personnel (numéro de facture EDF, par exemple qui n'est certainement pas le même que celui qui apparaît sur votre véritable facture) ;
- l'orthographe et la syntaxe des messages que vous recevez. Les messages frauduleux comportent souvent des fautes de français.

Comment se protéger des arnaques sur Internet ?

Si vous avez des doutes concernant l'origine d'un e-mail, il est recommandé de :

- ne pas y répondre ;
- ne pas fournir les données qui vous sont demandées ;
- ne pas cliquer sur les liens ou les boutons présents dans l'e-mail, ne pas ouvrir ses pièces-jointes ;
- signaler le message frauduleux en le transmettant aux adresses suivantes :
- pour EDF : message-frauduleux@edf.fr ;
- pour la CAF : www.phishing-initiative.com ;
- pour l'Assurance maladie : plateforme Pharos ;
- mettre à jour le système de sécurité de votre ordinateur ou de votre smartphone ;
- éviter de consulter des pages Internet contenant vos données confidentielles depuis des ordinateurs installés dans des lieux publics.

Que faire si vous êtes victime d'une fraude sur Internet ?

Si vous avez cliqué involontairement sur le lien d'un e-mail frauduleux ou si vous avez fourni des informations confidentielles, suivez ces étapes :

- contactez immédiatement votre établissement bancaire et faites opposition ;
- modifiez votre mot de passe directement dans votre espace personnel. Si vous ne parvenez plus à vous connecter, demandez un nouveau mot de passe par e-mail ;
- · mettez à jour votre antivirus et procéder à une analyse de votre ordinateur ;
- vérifiez que votre pare-feu est bien activé ;
- sélectionnez l'e-mail frauduleux dans votre boîte de réception et signalez-le comme « indésirable ».

Le phishing, même une seule tentative, est un délit pénal contre lequel vous pouvez porter plainte au commissariat ou à la gendarmerie la plus proche.

Pour cela, munissez-vous de tout document permettant d'en identifier l'auteur (copie des e-mails, adresse e-mail ou postale, référence du transfert d'argent effectué…).

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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source :

http://www.dossierfamilial.com/fraude-sur-internet-comment-evi

ter-les-pieges-20905.html Auteur : Ysabelle Silly

10 bonnes pratiques pour des soldes sur Internet en sécurité



Pour réaliser vos achats en ligne en toute sécurité, ESET vous donne des conseils pour éviter de se faire pirater sa carte bancaire.

- Faites attention aux sites Internet que vous ne connaissez pas. Au moindre doute, n'effectuez pas vos achats, car il peut s'agir d'un faux site Internet qui tente de récupérer les informations de votre carte bancaire.
- Préparez-vous aux attaques par phishing. Elles se diffusent massivement par e-mail lors des soldes, car c'est à cette période que les internautes passent le plus de temps sur les sites Internet de vente en ligne. ESET a réalisé une courte vidéo pour vous expliquer comment éviter le phishing par e-mail.
- Utilisez des méthodes de paiement sécurisé. Vérifiez que l'URL mentionne HTTPS. Effectuez toujours vos paiements sur des sites Internet chiffrés.
- Attention aux annonces sur Facebook. Les plateformes des réseaux sociaux abondent de fausses annonces et sites Internet proposant des offres intéressantes. Évitez également de partager les détails de votre carte bancaire par message : vous ne pouvez pas vérifier l'identité des personnes qui ont accès au compte et qui recevront ces informations.
- Effectuez toujours vos achats sur des appareils sécurisés et évitez de vous connecter à un Wi-Fi public. Ce genre d'arnaque, appelé Man-in-the-Middle (MiTM) est très répandu. En 10 minutes, le pirate peut voler toutes les informations vous concernant.
- Utilisez des mots de passe forts ou un gestionnaire de mots de passe. Plusieurs études ont montré que les utilisateurs ayant plus de 20 comptes en ligne et étant actifs sur Internet sont plus susceptibles de réutiliser les mêmes mots de passe pour plusieurs accès. Selon le rapport de recherche et de stratégie Javelin, cette méthode augmente de 37% le risque de voir ses comptes compromis. Aussi, les experts ESET recommandent d'utiliser des mots de passe forts mélangeant des minuscules et des majuscules à des symboles et chiffres. Les gestionnaires de mots de passe peuvent être utilisés pour ne pas avoir à les apprendre par cœur. Retrouvez les erreurs les plus courantes lors de l'utilisation d'un mot de passe en cliquant ici.
- Soyez prudent avec votre smartphone. Le nombre de cybermenaces sur cette plateforme a considérablement augmenté. Pour commencer, faites vos achats uniquement via des applications certifiées et supprimez les applications dont vous ne vous servez pas. Pensez à désactiver le Wi-Fi lorsque vous faites votre shopping dans un lieu public, privilégiez les données cellulaires, ceci permettra d'empêcher les cybercriminels de vous diriger vers un faux Wi-Fi afin de voler vos informations bancaires.
- Utilisez une e-carte bleue. Non seulement elle est déconnectée de vos comptes bancaires et est également assurée contre les fraudes.
- Respectez les règles de sécurité de base. Cela peut paraître évident, mais avant de faire vos achats, assurez-vous d'être correctement protégé : installez une solution de sécurité efficace et mise à jour. Optez pour une solution qui offre une navigation sécurisée pour les transactions bancaires. Enfin, ajoutez des mots de passe à votre écran de verrouillage ou un code PIN à votre smartphone.
- Évitez de réaliser vos achats sur différents appareils (1 à 2 maximum). Plus vous entrerez les informations de votre carte de crédit sur des appareils différents (PC, tablette, smartphone...), plus vous multipliez le risque d'être victime d'une fraude.

[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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Article original de ESET

9 erreurs fréquentes à ne pas

commettre dans la ligne d'objet d'un e-mail | Denis JACOPINI



Voici les écueils à éviter lors de la rédaction de l'intitulé de votre message électronique. Que vous postuliez pour un emploi, que vous présentiez votre business ou que vous communiquiez avec un collègue, la ligne d'objet de votre e-mail est l'un des meilleurs outils à votre disposition pour attirer l'attention de votre interlocuteur. C'est aussi l'un des outils les plus mal-compris. Errire une ligne d'objet trop verbeuse, vague ou qui semble trop insistante est le meilleur moyen de ne jamais obtenir de réponse.

Nous avons interrogé des spécialistes sur la question de la ligne d'objet. Voici les écueils à éviter:

1. Ne pas en écrire une

Ne pas inclure une ligne d'objet à un e-mail est l'une des pires erreurs que vous pouvez commettre. Amanda Augustine, experte au cabinet de recrutement, TheLadders, souligne le fait qu'il n'y a rien de plus important dans un e-mail que la ligne d'objet. Un e-mail sans ligne d'objet sera probablement supprimé ou perdu. De plus, celà agacera immédiatement le destinataire, qui se voit forcé de l'ouvrir pour en comprendre le sujet.

« Une messagerie de bureau montre environ 60 caractères dans la ligne d'objet d'un e-mail. Un téléphone mobile n'en révèle quant à lui que 25 ou 30 », précise Amanda Augustine. D'après Dimitri Leonov, Vice Président de SaneBox, spécialiste du tri d'e-mail, 50% des e-mails sont désormais lus sur téléphone mobile. Si vous écrivez plus de six à huit mots en oubliant de placer les plus importants en tête de la ligne d'objet, vous risquez de perdre l'attention du destinataire.

La ligne d'objet doit faire comprendre le contenu exact de l'e-mail afin que son destinataire puisse en déterminer l'importance sans avoir à l'ouvrir. Amandine Augustine précise qu'écrire « As-tu une minute ? » est, par exemple, trop vague parce que cela force son destinataire à ouvrir l'e-mail ou à y répondre pour savoir ce dont il s'agit. Ne forcez pas votre lecteur à jouer aux devinettes. Soyez direct et précis. Utilisez des mots-clés logiques qui rendront votre e-mail facilement retrouvable par la suite.

Comme vous ne disposez que d'un espace restreint, ne le gâchez pas avec des mots inutiles tels que « bonjour », « enchanté » ou « merci », qui peuvent très simplement être inclus dans le corps de l'e-mail.

Si vous postulez pour un emploi:

N'écrivez pas: Bonjour, puis-je en savoir plus sur une ouverture de poste ? Ecrivez plutôt: Recommandé par Jane Brown, pour poste de rédacteur technique.

Mettre tous les mots en majuscules

Ecrire la ligne d'objet en majuscules peut attirer l'attention de quelqu'un, mais de la mauvaise manière puisqu'il s'agit de l'équivalent digital de crier. « Votre but est de rendre la lecture de votre e-mail aussi facile que possible, et non de provoquer de l'angoisse chez votre correspondant », rappelle Dimitri Leonov. A la place, utilisez de la ponctuation comme un tiret pour séparer vos idées, mais tâchez d'éviter les caractères spéciaux comme le point d'exclamation.

6. Commencer une phrase dans la ligne d'objet et la terminer dans le corps de l'e-mail

Si vous introduisez une idée ou une question dans la ligne d'objet pour la conclure dans le corps de l'e-mail, le lecteur sera obligé d'ouvrir celui-ci pour comprendre ce dont il s'agit. C'est un procédé agaçant, et puisque la clarté et le respect du temps du destinataire sont des priorités, cela n'apporte pas grand-chose. Demandez vous si, dans ce cas là, une messagerie instantanée ou un appel ne conviendrait pas mieux

Amandine Augustine rapporte que les erreurs de copier-coller sont bien trop fréquentes. Il est fréquent que quelqu'un qui envoie un e-mail similaire à plusieurs personnes oublie d'adapter son message à chaque lecteur, et se trompe ainsi de nom ou de titre dans la ligne d'objet. Le meilleur moyen de s'épargner cette erreur est de relire la ligne d'objet avant d'envoyer l'e

8. Ne pas préciser l'importance

« Les gens veulent savoir ce qu'ils ont réellement besoin de lire et s'ils doivent répondre », résume Amandine Augustine. Si vous avez besoin d'une réponse, faites le savoir clairement dans la ligne d'objet et fixez une deadline. Vous pourriez par exemple dire: « Répondez d'ici à vendredi svp ».

Si quelqu'un que vous connaissez tous les deux vous a recommandé au destinataire de l'e-mail, n'attendez pas le corps dudit e-mail pour le préciser, ou vous risquez que celui-ci soit jeté corbeille sans avoir été ouvert, rappelle Amandine Augustine. Elle suggère d'écrire le nom complet de la personne qui vous a recommandé en tête de la ligne d'objet, dans le d'attirer l'attention de votre lecteur.

[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.journaldunet.com/management/efficacite-personnelle/ 1150433-erreurs-objet-mail

Article de Jenna Goudreau. Traduction par Shane Knudson, JDN. Voir l'original: The 9 Worst Mistakes People Make In Email Subject Lines

Mise en conformité RGPD, privilégiez l'accompagnement sur mesure

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)

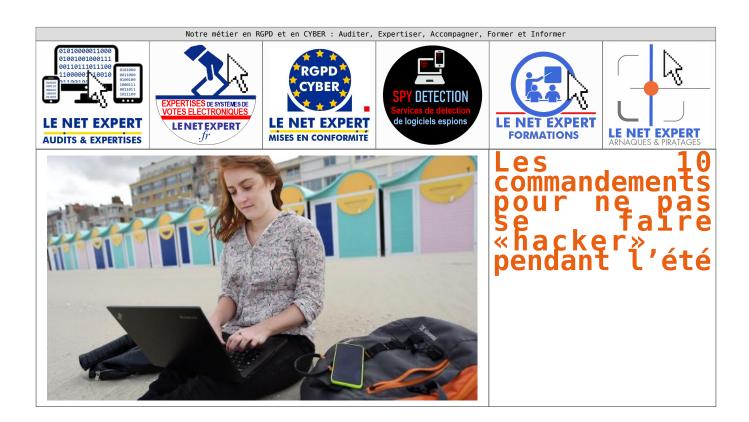
Protection des Données à Caractère Personne (mise en conformité avec la CNIL etle RGPD)

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 ;

Les 10 conseils pour ne pas se faire «hacker» pendant l'été | Denis JACOPINI



Toutes les secondes, un internaute sur deux dans le monde est victime d'un acte malveillant. La cybersécurité est aujourd'hui un enjeu majeur pour les entreprises comme les particuliers. Voici dix bonnes pratiques pour vivre un été connecté en toute sécurité, sans parano, ni naïveté...

Quand on part de chez soi, on ferme la porte. Pour nos vies numériques et ultraconnectées c'est pareil. « On doit se comporter sur Internet comme dans la vie réelle, sans parano, mais aussi sans naïveté », estime Raouti Chehih, directeur général d'Euratechnologies. Des entreprises spécialisées (Incloudio, Runiso, Suricat Concept et Zataz) nous ont fait la liste de quelques erreurs à ne pas commettre.

- 1. Je n'indique pas mes dates et destinations de vacances sur les réseaux sociaux. Facebook, c'est comme une place publique. Ne communiquez vos informations personnelles qu'aux personnes que vous connaissez.
- 2. Je ne laisse pas mon ordinateur/smartphone sur la plage pendant que je vais me baigner. À moins que vous ne souhaitiez vraiment vous en « débarrasser ».
- 3. Je restreins l'accès à mes appareils. Ne laissez pas la porte ouverte, sécurisez votre appareil en ajoutant un mot de passe pour accéder aux contenus.
- 4. Je ne me connecte pas à mon adresse mail habituelle à partir de mon lieu de vacances. Les ordinateurs publics des hôtels et campings ne sont pas toujours sécurisés. Si l'on ne veut pas laisser sa boîte mail personnelle ouverte à tous les vents, mieux vaut se créer une adresse temporaire dédiée à ses vacances.
- 5. Je ne prends pas mon ordinateur avec tous mes papiers, photos et documents sur mon lieu de vacances. En vacances, on n'emporte que l'essentiel, ce qui est confidentiel doit rester à la maison.
- 6. Je ne me connecte pas sur les « hotspots » gratuits à portée de Wi-Fi. Le Wi-Fi gratuit n'est pas sécurisé. Si vous n'avez rien à protéger, pas de problème. Mais pas question de consulter vos comptes bancaires n'importe où.
- 7. Je ne consulte pas mes mails sans utiliser de filtre antispam. Pour éviter de recevoir des mails infectés de virus, il existe plein de filtres gratuits, comme LoveYouremail, développé dans notre région.
- 8. Je n'utilise pas un mot de passe simple et identique pour tous mes comptes. N'hésitez pas à ajouter chiffres, majuscules, symboles dans vos mots de passe. Pour les retenir tous, il existe des coffres-forts virtuels, comme Keepass.
- 9. Je n'utilise pas l'ordinateur de l'hôtel ou du camping pour accéder à mes mails privés. N'utilisez ces ordinateurs que pour des informations non sensibles et n'oubliez pas de fermer la connexion après consultation.
- 10. J'anticipe une perte ou un vol de mon ordinateur. Il existe des antivols qui permettent de localiser votre appareil, protéger vos données et même prendre une photo de celui qui utilise votre ordinateur (type Beebip).

Enfin, si vous voulez vraiment passer des vacances tranquilles, déconnectez-vous tout simplement, et laissez votre ordinateur au bureau…

[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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Source

http://www.lavoixdunord.fr/economie/les-10-commandements-pour-ne-pas-se-faire-hacker-ia0b0n2975946

Piratage massif sur Twitter : voici comment protéger votre compte (et le récupérer en cas de besoin) | Denis JACOPINI



Pas moins de 32 millions d'identifiants Twitter seraient actuellement mis en vente en ligne à la suite d'un piratage massif : des adresses e-mails, des identifiants et des mots de passe, dérobés directement sur les navigateurs des intenautes. Voici nos astuces pour mieux protéger votre compte, et le récupérer en cas de piratage.



Le réseau social américain s'est empressé de rassurer ses utilisateurs après les révélations par le site LeakedSource de la mise en vente en ligne de plus de 32 millions d'identifiants Twitter dérobés par des hackeurs. A la différence de MySpace, victime d'une fuite de données identique en mai dernier, Twitter n'a pas été directement infiltré par les pirates.

D'après LeakedSource, les données dérobées — des adresses e-mail, des identifiants, et des mots de passe — l'ont été directement sur les navigateurs des victimes grâce à des malwares. Evidemment, le risque zéro n'existe pas, néanmoins, des solutions simples peuvent contribuer à compliquer un peu plus l'action de ces hackeurs malintentionnés. Voici comment procéder.

► Optez pour le bon mot de passe

Bien qu'on rechigne souvent à le faire, de peur de l'oublier, le choix du mot de passe est une étape cruciale pour s'assurer un niveau de protection suffisant. Utilisez autant que possible chiffres, lettres, minuscules, capitales et symboles.

La Commission nationale de l'informatique et des libertés (Cnil) recommande d'utiliser un moyen mnémotechnique : par exemple, la phrase « un Utilisateur d'Internet averti en vaut deux » correspond au mot de passe « 1Ud'Iaev2 ».

► Ajoutez votre numéro de téléphone

En associant un numéro de téléphone à votre compte, vous pourrez profiter de fonctionnalités de sécurité telles que la vérification de connexion (grâce à la réception d'un SMS). Pour ce faire, il suffit de se rendre dans le menu, en haut droite, en cliquant sur votre image de profil. Puis, allez dans la section « Mobile ».

► Comment savoir que votre compte a été piraté

Toujours dans le menu « Réglages », cette fois, rendez-vous dans la section « Vos données Twitter ». Vous pourrez ainsi consulter l'historique des connexions, ainsi que les appareils qui s'y sont connectés. Si, comme dans l'exemple cidessous, vous constatez une anomalie (dans notre cas, une connexion depuis le Mexique), cela signifie que votre compte Twitter est compromis.

Twitter pour iPhone	14 janv. 2016 09:44	France
Twitter pour iPhone	14 janv. 2016 09:28	France
Twitter pour iPhone	14 janv. 2016 07:49	France
Twitter.com	14 janv. 2016 02:53	201.173.172.72 Mexique
Twitter.com	14 janv. 2016 02:53	201.172.27.30 Mexique
Twitter pour iPhone	14 janv. 2016 00:20	France
Twitter.com	13 janv. 2016 20:23	France

► Que faire quand son compte est hacké

Le diagnostic classique : vous n'arrivez plus à vous connecter et votre compte se met à tweeter tout seul ou vos amis reçoivent du spam en message privé. Si vous pouvez accéder à votre compte, changez votre mot de passe immédiatement. Twitter propose une réinitialisation du mot de passe en entrant votre email ou bien votre numéro de téléphone (mais pour cela, il faut l'avoir associé comme expliqué plus haut).

Enfin, si aucune de ces solutions ne marche, vous pouvez demander l'assistance de Twitter. Pour terminer, n'oubliez pas de révoquer l'autorisation de toutes les apps utilisant Twitter. Pour ce faire, allez dans « Réglages », puis dans « Applications ».

Article original de MATTHIEU DELACHARLERY

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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

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

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

Original de l'article mis en page : Piratage massif sur Twitter : voici comment protéger votre compte (et le récupérer en cas de besoin) — metronews

Victime d'un piratage informatique, quelles sont les bonnes pratiques ?



Les cas de piratages informatiques ne se comptent plus depuis bien longtemps. Cependant, si vous vous êtes retrouvés victimes, il est urgent de mettre en pratique des règles de base.

Les 3 axes vers lesquels votre structure devra progresser seront

- Technique, par une amélioration des mesures de sécurité en place ;
- Juridique, par une présentation, auprès des principaux acteurs de votre structure pour une meilleure acceptation, des principales mesures de mise en conformité avec les règles françaises et européennes relatives à la protection des données personnelles ;
- Humain, par une meilleure prise de conscience des dangers numériques, pour une évolution des comportements vers une utilisation plus responsable des outils numériques.

Face à vos besoins d'accompagnement, nos formateurs ont élaboré un parcours destinés aux équipes de direction de votre structure, à l'équipe informatique et aux utilisateurs susceptibles d'être piégés.

En vous accompagnant sur ces 3 axes et auprès de ces 3 profils, vous pourrez alors comprendre comment les pirates informatiques vous ont piégé, découvrir s'ils pourront encore vous piéger et surtout, le plus important, quelles changements mettre en place pour limiter les risques à l'avenir.

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 (Symantec) 13,8 Milions de victimes Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

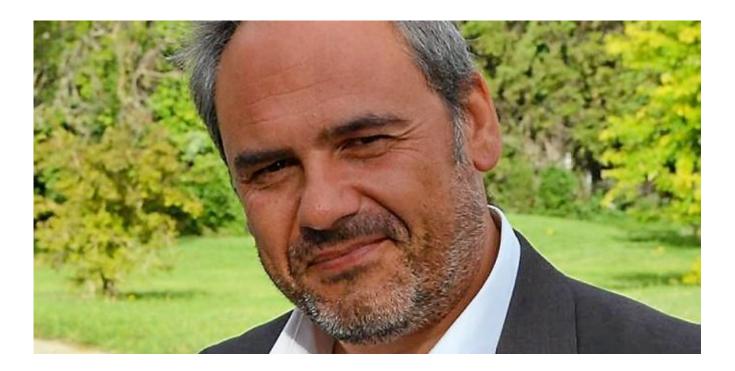
Commandez sur Fnac.fr

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

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

RGPD : Quelles actions sont à mettre en œuvre aujourd'hui

pour assurer la mise en conformité des pratiques avec les nouvelles règles ?



Le Règlement Général sur la Protection de Données (RGPD) est entré en application au 25 mai 2018 et <u>toutes les entreprises</u>, <u>administrations et associations</u> et leurs <u>soustraitants</u> ne s'y sont toujours pas préparés. Or, <u>quelle que soit leur taille</u>, <u>elles sont toutes concernées</u> et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées. Quelles actions sont à mettre en œuvre aujourd'hui pour assurer la mise en conformité des pratiques avec les nouvelles règles ?

Il importe d'auditer dès aujourd'hui les pratiques internes des différents services de l'entreprise (marketing, RH, IT...), mais également celles de ses partenaires.

Une étude des outils contractuels en place est également nécessaire, s'agissant en particulier des contrats avec les prestataires, des chartes internes, CGU, mentions d'information lors de la collecte des données… pour s'assurer de leur pertinence.

Une fois cet audit réalisé, les actions de mise en conformité seront identifiées et pourront être initiées : mise en place d'un registre, désignation d'un DPO, modification des contrats ou clauses contractuelles, sécurisation des traitements, refonte des CGU et formules d'information, etc. Une cartographie des traitements et la mise au point d'un référentiel des finalités et des traitements permettront de comprendre l'état des pratiques, d'alimenter le suivi des formalités et les évolutions nécessaires, et d'établir l'existence de pratiques conformes et à jour au regard du RGPD en cas de contrôle des autorités.

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



DÉSIGNATION N° DPO-15945





Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :





Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

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

Source : Le RGPD en 10 questions. Par François-Xavier Boulin, Avocat.

63% des Français redoutent de donner des informations personnelles sur Internet | Denis JACOPINI



Selon une enquête réalisée par Dashlane et Opinionway, en France, au Royaume-Uni et aux États-Unis, les internautes français sont ceux qui se méfient le plus. 14% ne communiquent jamais leurs données personnelles, contre 4 % des Britanniques et 5% des Américains.

En fonction de leur identité culturelle, les internautes n'abordent pas la saisie des données personnelles sur la toile de la même manière. Selon un sondage Opinionway, réalisé en octobre 2015, les Français se montrent bien plus frileux que leurs homologues anglo-saxons: 63% d'entre eux avouent leur méfiance quand il s'agit de donner des informations personnelles sur le web contre 35 et 34% chez les Britanniques et les Américains. 14% des Français refusent de communiquer leurs informations personnelles, un chiffre qui tombe à 4 et 5% en Grande-Bretagne et aux États-Unis.

Quel que soit le pays, la donnée la plus sensible est le numéro de carte bancaire. Là encore, ce sont les Français qui arrivent en tête. 72% d'entre eux avouent leur crainte quand il s'agit de stocker cette information sur un site, contre 48% des Anglais et 41% des Américains.

Les critères qui rassurent ne sont pas les mêmes d'un pays à l'autre, selon l'enquête. Les Français se sentent en priorité protégés par le petit cadenas à côté de l'adresse qui indique une connexion sécurisée (68%), puis par l'assurance que les données ne seront pas transmises (36%). Les Britanniques et les Américains se fient, eux, à la marque ou au site Internet (53% et 47%).

En revanche, le mot de passe fait consensus. Il rime avec sécurité dans le cas de transactions pour 1/3 des Français, des Britanniques et des Américains.

Globalement, les internautes se posent beaucoup de questions quand il s'agit de payer en ligne. La vigilance reste de mise à l'égard de certains sites, de peur d'être piratés. 65% des Français évitent alors d'y utiliser leur carte. 66% des Britanniques et 70% des Américains s'abstiennent également.

Interrogés sur les systèmes sensés améliorer leur confiance, les participants se disent prêts à utiliser leur carte bancaire plus souvent, si l'utilisation une carte temporaire infalsifiable rend le piratage impossible. À cette condition, 70% des Français, 76% des Britanniques et 77% des Américains passeraient à l'acte. Autre critère jugé rassurant: une étape d'authentification supplémentaire (63% en France, 54% en Grande-Bretagne et 50% aux États-Unis).

Méthodologie : pour réaliser cette enquête, un échantillon représentatif a été constitué en fonction des critères de sexe, d'âge, de catégorie socioprofessionnelle en France, de catégorie sociale Esomar au Royaume-Uni et de revenus aux Etats-Unis. 1014 Français, 1004 Britanniques et 1009 Américains ont été soumis à un questionnaire en ligne sur système CAWI (Computer Assisted Web interview).

```
[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.boursorama.com/actualites/63-des-francais-redoutent-de-donner-des-informations-personnelles-sur-internet-419faf4a01d101ef73283fcf315c7a50