

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

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

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

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

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

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

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

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

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

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

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


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



Réagissez à cet article

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

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

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

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

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

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

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

Aujourd'hui encore, on peut comparer le courrier électronique au courrier postal. Cependant, si l'utilisation du courrier postal est en constante diminution (-22% entre 2009 et 2014), l'usage des messages électroniques par logiciel de messagerie ou par messagerie instantanée a lui par contre largement augmenté. Parmi les messages reçus, il y a très probablement des réponses attendues, des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant de nos nouvelles et quelques autres messages que nous recevons avec plaisir de personnes connues et puis il y a tout le reste, les messages non attendus, non désirés qui s'appellent des spams.

En 2015, malgré les filtres mis en place par les fournisseurs de systèmes de messagerie, il y avait tout de même encore un peu plus de 50% de messages non désirés.

Parmi ces pourriels (poubelle « e-mail ») se cachent de nombreux messages ayant des objectifs malveillants à votre égard. Les risques les plus répandus sont les incitations au téléchargement d'une pièce jointe, au clic sur un lien renvoyant vers un site Internet piégé ou vous proposer d'échanger dans le but de faire « copain copain » et ensuite vous arnaquer.

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

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

Imaginez, vous recevez un message ressemblant à ça :

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

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

Un autre exemple d'e-mail ou similaire souvent reçu :

« Objet : Commande – CD2533
Expéditeur : Prénom et Nom d'une personne inconnue
Madame, Monsieur,
Nous vous remercions pour votre nouvelle « Commande – CD2533 ».
Nous revenons vers vous au plus vite pour les délais
Meilleures salutations,
VEDISCOM SECURITE »

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

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

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

A mon avis, le principal levier utilisé pour pousser les gens à cliquer sur les emails pour en voir l'objet, cliquer sur les pièces jointes pour en voir le contenu ou cliquer sur les liens pour découvrir la suite, est une des nombreuses failles humaine : la curiosité.

Cette curiosité peut nous faire faire des choses complètement irresponsables, car on connaît les dangers des pièces jointes ou des liens dans les e-mails. Malgré cela, si notre curiosité est éveillée, il sera difficile de résister au clic censé la satisfaire.

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

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°34 03041 84).

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

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

 Réglez à cet article

Original de l'article mis en page : One in two users click on links from unknown senders > FAU.EU

Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 | Denis JACOPINI

 Un oeil sur vous, citoyens sous surveillance – Documentaire 2015 2h24

Des milliards de citoyens connectés livrent en permanence – et sans toujours s'en rendre compte – des informations sur leur vie quotidienne à des sociétés privées qui les stockent dans de gigantesques serveurs. Ces informations sont rendues accessibles aux États et vendues aux entreprises. Dans ce monde sous étroite surveillance, jusqu'où irons-nous en sacrifiant nos vies intimes et nos droits à la liberté individuelle ?

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

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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 plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

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

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

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de trace sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé (effacer l'historique de ses comptes mails et personnelles, formatage complet, logiciel d'aide à la suppression etc...) ?

La première étape consiste à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur la plupart des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :

- Des programmes ajoutés ;
- Nos e-mails ;
- Nos traces de navigation ;
- Nos fichiers téléchargés ;
- Divers identifiants et mots de passe ;
- Les fichiers temporaires

Afin d'éviter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Concernant les programmes ajoutés

Facile sur Mac en mettant le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes sous Windows. La plupart des programmes apparaissent dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

- soit par le raccourcis de désinstallation que le programme a créé ;
- s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
- Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que RevoUninstaller (gratuit).

Concernant les e-mails

Selon le programme que vous utiliserez, la suppression du/des compte(s) de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

- fichiers « .pst » et « .ost » de votre compte et archives pour le logiciel « Outlook » ;
- fichiers dans « » »% »'AppDataLocalMicrosoftWindows Live Mail » pour le logiciel « Windows Live Mail » ;
- les fichiers contenus dans ' » »% »'APPDATA%ThunderbirdProfiles » pour le programme Mozilla Thunderbird
- le dossier contenu dans « ..Local SettingsApplication DataIMIdentities » pour le programme Incremail.

Concernant nos traces de navigation

En fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'Historique de Navigation » ou les « Données de Navigation ».

Concernant les fichiers téléchargés

En fonction de votre système d'exploitation l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Concernant divers identifiants et mots de passe

Du fait que le mot de passe de votre système d'exploitation stocké quelque part (certes crypté), si vous êtes le seul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un basic de type « utilisateur ».

Du fait que les mots de passe que vous avez mémorisés au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires

En utilisant la fonction adaptée dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).

En utilisant la fonction adaptée dans votre systèmes d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Pour finir

Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore »...

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

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

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



Réagissez à cet article

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

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

Quitter son travail est souvent difficile, mais effacer des données présentes sur un ordinateur professionnel sur lequel on a travaillé pendant 8 heures l'est encore plus. Il est donc nécessaire de savoir comment le faire sans laisser de données professionnelles ni personnelles derrière soi.

Atlantico : Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction ?

Denis Jacopini : L'ordinateur professionnel qui vous a été mis à disposition était généralement en état de sécurité. À moins d'être des circumlocutions ou des techniques particulières, vous devriez donc rendre cet appareil au mieux dans l'état initial. De manière à vous empêcher d'en avoir conscience une copie et de l'utiliser contre votre ancien employeur.

1. Identifier les données ayant un caractère confidentiel et qui nécessitent une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.
2. Identifier les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de assistance.
3. Identifier les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants.)
4. Identifier les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ce soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifier les fonctions de « Sauvegarde », « Enregistrer sous » ou d'« Export ». Vous pourrez alors choisir le support adapté.

Enfin, en fonction des critères de sécurité choisis, vous pourrez sauvegarder sur des supports adaptés soit :

- à la confidentialité (tout support numérique ne utilisant que logiciel de cryptage de type TrueCrypt, PGP, ou autre) ;
- à l'intégrité (utiliser le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à l'abandonner pas perdre) ;
- à la longévité (utiliser des supports avec une durée de vie adaptée à vos attentes. Saché qu'à ce jour, il est difficile de garantir la lecture d'une information numérique au-delà de plusieurs dizaines d'années (en raison de l'évolution des versions, des formats et des logiciels). On peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
- à la disponibilité (plusieurs plateformes ou plusieurs lieux, comme le proposent les solutions cloud qui sont déjà il y a quelques dizaines d'années seulement) ;
- à la disponibilité (plusieurs plateformes ou plusieurs lieux, comme le proposent les solutions cloud qui sont déjà il y a quelques dizaines d'années seulement) ;
- à la quantité (car vous devez rapidement stocker pour ensuite tirer et choisir un support adapté en choisissant par exemple un disque dur USB externe actuellement (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui qui le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

Les risques :

Les clés USB sont des outils permettant de conserver une copie facilement accessible et aisément transportable. 100% des clés USB tombent un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.

Si on ne les disques durs, 100% des disques durs tombent un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettent plus facilement de récupérer leur contenu en cas de panne.

Les supports de type lecteurs ZIP, lecteurs DVD, lecteurs Blu-ray, lecteurs de bande etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginer un instant pour de vous soustraire et accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vie de vos données numériques entre les mains de Son Ciel.

Enfin, en fonction de vos choix, il se peut que vous n'avez plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Commentaires :

Discussion sur : Quelque chose à quelconque de - Son marché, rapide mais fragile.

Claire USB - Quelque chose - Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.

Cloud - Quelque chose à quelconque de - Accessible de n'importe où mais aussi par tous ceux qui ont le mot de passe (risqué) - Dépend du fonctionnement et de la rapidité d'Internet - Les services de cloud gratuits peuvent s'arrêter du jour au lendemain et vous perdre tout.

Disques optiques (CD, DVD, Blu-ray, etc.) - Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (paramètres des lecteurs de disques) jusqu'à quand ?

Supports externes (ZIP, lecteurs DVD, lecteurs Blu-ray, lecteurs de bande etc.) - Supports fragiles, lecteurs trop rares pour garantir une lecture au-delà de 10 ans.

Est-il possible d'effacer toutes nos données présentes sur un ordinateur de fonction lorsque l'on quitte son travail et que l'on ne souhaite pas laisser de traces sur celui-ci ? Si oui, quels moyens préconisez-vous pour être sûr que ce type de données soit bien effacé ?

Le procédé étape consistant à identifier les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur le logiciel des ordinateurs professionnels, parfois sans le savoir, en plus de nos documents de travail nous stockons :

- Des programmes installés ;
- Nos e-mails ;
- Nos traces de navigation ;
- Nos fichiers téléchargés ;
- Divers identifiants et mots de passe ;
- Les fichiers temporaires.

Afin d'écarter l'accès à ces informations par le futur locataire / propriétaire / donataire de votre ordinateur, il sera important de procéder à leur suppression minutieuse.

Commentez les programmes installés :

Facile sur Mac et surtout le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes ou Windows. (Le support des programmes apparaît dans la liste des programmes installés. Pour procéder à leur suppression, nous vous conseillons de procéder :

- soit par le raccourci de désinstallation que le programme a créé ;
- si il n'y a pas de raccourci prévu à cet effet, passer par la fonction « Ajout et Suppression de Programmes » ou « Paramètres » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;

Commentez les e-mails :

Selon le programme que vous utilisez, la suppression d'un e-mail de messagerie dans le programme en question suffit pour supprimer le ou les fichiers contenant les e-mails. Sinon, par précaution, vous pouvez directement les localiser et les supprimer :

- Fichiers « .ost » et « .pst » de votre compte et archives pour le logiciel « Outlook » ;
- Fichiers dans « %AppData%\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
- Les fichiers contenus dans « %localappdata%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird.

Le dossier contenu dans « %localappdata%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird.

Commentez nos traces de navigation :

De fonction de votre navigateur Internet et de sa version, utilisez, dans les « Options » ou les « Paramètres » la fonction supprimant l'« Historique de Navigation » ou les « Données de Navigation ».

Commentez les fichiers téléchargés :

De fonction de votre système d'exploitation et l'emplacement de stockage par défaut des fichiers téléchargés change. Pensez toutefois à parcourir les différents endroits de votre disque dur, dans les lecteurs réseau ou les lecteurs externes à la recherche de fichiers et documents téléchargés que vous auriez pu stocker.

Commentez divers identifiants et mots de passe :

De fait que le mot de passe de votre système d'exploitation stocke quelque part (certes crypté), il vous échoit le veul à le connaître et souhaitez en conserver la confidentialité, pensez à le changer et à en mettre un autre de type « utilisateur ».

De fait que les mots de passe que vous avez mémorisés au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passe et les informations qui pré remplissent les champs.

Commentez les fichiers temporaires :

En utilisant la fonction adéquate dans vos navigateurs Internet, pensez à supprimer les fichiers temporaires liés à la navigation Internet (images, cookies, historiques de navigation, autres fichiers).

En utilisant la fonction adéquate dans votre système d'exploitation, supprimez les fichiers temporaires que les programmes et Windows génèrent automatiquement pour leur usage.

Peut-être :

Parce qu'un fichier supprimé n'est pas tout à fait supprimé (il est simplement marqué supprimé mais il est toujours présent) et dans bien des cas toujours récupérable, vous pourrez utiliser une application permettant de supprimer définitivement ces fichiers supprimés mais pourtant récupérables telle que « Eraser », « Clean Disk Security », « Prevent Restore ».

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

- Accéder à vos documents et déjouer les informations qui peuvent être professionnelles et être utilisées contre vous, mais personnelles permettant à un usage de les utiliser contre vous tout en vous demandant de l'argent contre son silence ou pour avoir le paix ;
- Accéder aux identifiants et mots de passe des comptes Internet que vous utilisez (même pour des sites Internet commençant par https) et ainsi accéder à nos comptes Facebook, Twitter, Dropbox... ;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement apposer des commentaires ou envoyer des e-mails en utilisant votre identité.

Auteur : Denis JACOPINI

Denis Jacopini anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 04 03041 04).

Nous animons conférences et formations pour sensibiliser décideurs et utilisateurs aux risques de information, découvrir comment les entreprises et les stratégies informatiques pour mieux s'en protéger et se mettre en conformité avec la CNIL et le maître de Protection des Données Personnelles. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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

10

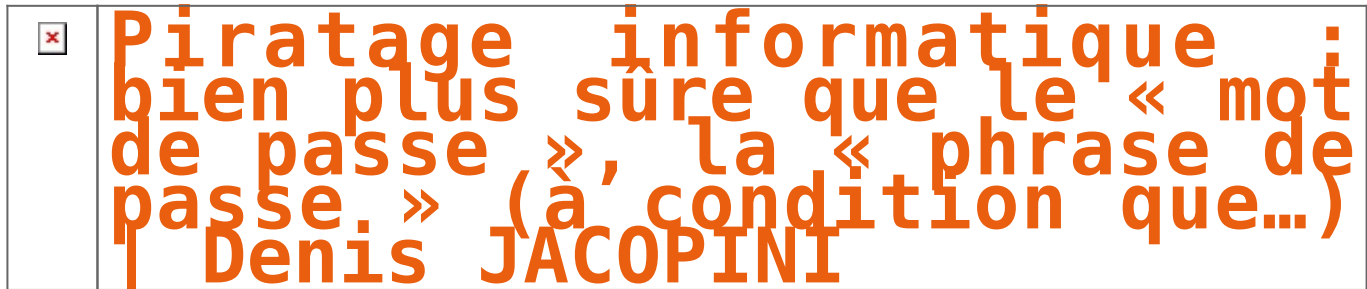
11

Rejoignez à cet article

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

Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...)

Denis JACOPINI



Une « phrase de passe » est beaucoup plus difficile à pirater qu'un « mot de passe ». Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Atlantico : Selon de nombreuses études menées par des chercheurs de l'Université américaine Carnegie-Mellon, un long mot de passe facile à retenir tel que « *ilfaitbeaudanstoutelafrancesaufdanslebassinparisien* » serait plus difficile à pirater qu'un mot de passe relativement court mais composé de glyphes de toutes sortes, tel que « *p8)J#&=89pE* », très difficiles à mémoriser. Pouvez-vous nous expliquer pourquoi ?

Denis Jacopini : La plupart des mots de passe sont piratés par une technique qu'on appelle « la force brute ». En d'autres termes, les hackers vont utiliser toutes les combinaisons possibles des caractères qui composent le mot de passe.

Donc, logiquement, plus le mot de passe choisi va avoir de caractères (majuscule, minuscule, chiffre, symbole), plus il va être long à trouver. Pour donner un ordre d'idée, les pirates du Web mettent quelques heures à quelques jours pour trouver un mot de passe de huit caractères complexes via la technique de « la force brute », et mettraient... plusieurs millions d'années pour décoder un mot de passe complexe de 12 caractères.

Un long mot de passe est donc plus difficile à pirater qu'un mot de passe court, à une condition cependant : que **la phrase choisie comme mot de passe ne soit pas une phrase connue de tous**, qui sort dès qu'on en tape les premiers mots dans la barre de recherche de Google. Les pirates du Net ont en effet des bases de données où ils compilent toutes les phrases, expressions ou mots de passe les plus couramment utilisés, et essayent de hacker les données personnelles en les composant tous les uns derrière les autres. Par exemple, mieux vaut avoir un mot de passe court et complexe plutôt qu'une « phrase de passe » comme « *Sur le pont d'Avignon, on y danse on y danse...* ».

Il faut également bien veiller à ce que cette « phrase de passe » ne corresponde pas trop à nos habitudes de vie, car les pirates du Web les étudient aussi pour arriver à leur fin. Par exemple, si vous avez un chien qui s'appelle « Titi » et que vous habitez dans le 93, il y a beaucoup de chance que votre ou vos mots de passe emploient ces termes, avec des associations basiques du type : « *jevaispromenermonchienTITIdansle93* ».

De plus, selon la Federal Trade Commission, changer son mot de passe régulièrement comme il est habituellement recommandé aurait pour effet de faciliter le piratage. Pourquoi ?

Changer fréquemment de mot de passe est en soi une très bonne recommandation, mais elle a un effet pervers : plus les internautes changent leurs mots de passe, plus ils doivent en inventer de nouveaux, ce qui finit par embrouiller leur mémoire. Dès lors, **plus les internautes changent fréquemment de mots de passe, plus ils les simplifient, par peur de les oublier, ce qui, comme expliqué plus haut, facilite grandement le piratage informatique.**

Plus généralement, quels seraient vos conseils pour se prémunir le plus efficacement du piratage informatique ?

Je conseille d'avoir une « phrase de passe » plutôt qu'un « mot de passe », qui ne soit pas connue de tous, et dont on peut aisément en changer la fin, pour ne pas avoir la même « phrase de passe » qui verrouille nos différents comptes.

Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données personnelles, sans avoir à pirater aucun mot de passe. Il faut donc rester vigilant sur les mails que l'on ouvre, réfléchir à qui on communique notre mot de passe professionnel si on travail sur un ordinateur partagé, bien verrouiller son ordinateur, etc...

Article original de Denis JACOPINI et Atlantico

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

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

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



Réagissez à cet article

Original de l'article mis en page : Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...) | Atlantico.fr

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques



Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

Quelques conseils pratiques pour assurer la sécurité de vos systèmes informatiques

1. CHOISISSEZ AVEC SOIN VOS MOTS DE PASSE

Entrer un mot de passe permettant de s'authentifier pour accéder à son ordinateur, sa tablette ou son téléphone portable est un geste quotidien de sécurité.

Choisir un mot de passe difficile à décoder par une tierce personne ou par du piratage informatique est ainsi un rempart efficace pour protéger ses données personnelles contre les intrusions frauduleuses.

Comment bien choisir son mot de passe ?

Définissez des mots de passe composés d'au moins 12 caractères

- mélangeant majuscules, minuscules, chiffres et caractères spéciaux
- n'ayant aucun lien avec vous comme votre nom, date ou lieu de naissance
- ne formant pas de mots figurant dans le dictionnaire

Comment faire en pratique ?

Pour cela 2 méthodes simples :

- la méthode phonétique : « J'ai acheté 5 CD pour cent euros cet après-midi » : ght5CDn€7am
- la méthode des premières lettres : « Un tiens vaut mieux que deux tu l'auras » : ltvnQ2tl'A

Quelques recommandations supplémentaires

- n'utilisez pas le même mot de passe pour tout, notamment pour accéder à votre banque en ligne et votre messagerie personnelle ou professionnelle
- méfiez-vous des logiciels qui vous proposent de stocker vos mots de passe

2. ENTRETENEZ RÉGULIÈREMENT VOS APPAREILS NUMÉRIQUES

En mettant à jour régulièrement les logiciels de vos appareils numériques

Dans chaque système d'exploitation (Android, MacOS, Linux, Windows,...), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité.

Sachant que bon nombre d'utilisateurs ne procèdent pas à ces mises à jour, les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations longtemps encore après leur découverte ou même leur correction. Il donc **nécessaire de procéder aux mises à jour régulières des logiciels.**

Comment faire ?

- configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible
- ou téléchargez les correctifs de sécurité disponibles en utilisant pour cela exclusivement les sites Internet officiels des éditeurs
- en effectuant couramment des sauvegardes

3. Effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple) permet de disposer de ses données après un dysfonctionnement ou une panne d'ordinateur

Comment faire ?

- utilisez des supports externes tels qu'un disque dur externe, un CD ou un DVD enregistrable pour enregistrer et sauvegarder vos données.

4. PRENEZ SOIN DE VOS INFORMATIONS PERSONNELLES ET DE VOTRE IDENTITÉ NUMÉRIQUE

Les données que vous laissez sur Internet vous échappent instantanément.

Des personnes malveillantes récoltent vos informations personnelles, le plus souvent frauduleusement et à votre insu, afin de déduire vos mots de passe, d'accéder à votre système informatique, voire d'usurper votre identité et de conduire des activités d'espionnage industriel.

Une grande prudence est conseillée dans la diffusion de vos informations personnelles sur Internet.

Voici quelques recommandations générales :

- soyez vigilant vis-à-vis des formulaires que vous êtes amenés à remplir : ne transmettez que les informations strictement nécessaires et pensez à décocher les cases qui autoriseraient le site à conserver ou à partager vos données, par exemple avec des partenaires commerciaux
- ne donnez accès qu'à un minimum d'informations personnelles sur les réseaux sociaux
- utilisez plusieurs adresses électroniques dédiées à vos différentes activités sur Internet : une adresse réservée aux activités dites sérieuses (banques, recherches d'emploi, activité professionnelle...) et une adresse destinée aux autres services en ligne (forums, jeux concours...)

5. PROTÉGEZ VOS DONNÉES LORS DE VOS DÉPLACEMENTS

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite le quotidien lors des déplacements professionnels. Pourtant, voyager avec ces appareils nomades peut mettre en péril des informations sensibles sur l'entreprise ou vous travaillez.

Précautions à prendre avant de partir en mission

- utilisez le matériel dédié à la mission prêté par votre entreprise (ordinateur, clefs USB, téléphone)
- sauvegardez aussi vos données sur un support amovible pour les retrouver en cas de perte
- si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur
- apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport

Pendant la mission

- gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel)
- si vous êtes contraint de vous séparer de votre téléphone, retirez la carte SIM et la batterie
- en cas d'inspection ou de saisie de votre matériel par des autorités étrangères, informez votre organisation
- n'utilisez pas les équipements que l'on vous offre si vous ne pouvez pas les faire vérifier par un service de sécurité de confiance
- évitez de connecter vos équipements à des postes qui ne sont pas de confiance. Par exemple, si vous avez besoin d'échanger des documents lors d'une présentation

6. SÉCURISEZ VOTRE WI-FI

Si l'utilisation du Wi-Fi est une pratique attractive, elle permet, lorsque le point d'accès n'est pas sécurisé, à des personnes malintentionnées d'intercepter vos données et d'utiliser votre connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes.

C'est pour cette raison que l'accès à Internet par un point d'accès Wi-Fi est à éviter dans le cadre de l'entreprise.

Le Wi-Fi, solution pratique et peu coûteuse, peut cependant être le seul moyen possible d'accéder à Internet, il convient dans ce cas de sécuriser l'accès en configurant votre box. Pour ce faire, n'hésitez pas à contacter l'assistance technique de votre fournisseur d'accès.

Quelques recommandations générales :

- modifiez le nom d'utilisateur et le mot de passe par défaut (généralement « admin » et « 0000 ») de votre page de configuration accessible via votre navigateur Internet
- vérifiez que votre box dispose du protocole de chiffrement WPA2 et activez-le. Sinon, utilisez la version précédente WPA-AES (ne jamais utiliser le chiffrement WEP cassable en quelques minutes)
- modifiez la clé de connexion par défaut avec une clé (mot de passe) de plus de 20 caractères de types différents (cf. Choisissez des mots de passe robustes)
- ne divulguez votre clé de connexion qu'à des tiers de confiance et changez-la régulièrement
- activez et configurez les fonctions pare-feu / routeur.
- désactivez le Wi-Fi de votre borne d'accès lorsqu'il n'est pas utilisé

7. SÉPAREZ VOS USAGES PERSONNELS DES USAGES PROFESSIONNELS

Monsieur Paul, directeur commercial, rapporte souvent du travail chez lui le soir. Sans qu'il s'en aperçoive son ordinateur personnel a été attaqué. Grâce aux informations qu'il contenait, l'attaquant a pu pénétrer le réseau interne de l'entreprise de Monsieur Paul. Des informations sensibles ont été volées puis revendues à la concurrence.

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, ordiphone,...) personnels et professionnels.

Dans ce contexte, il est recommandé de séparer vos usages personnels de vos usages professionnels :

- ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
- ne stockez pas de données professionnelles sur vos équipements communicants personnels

En savoir plus sur le AVEC ou BYOD :

Le AVEC (Apportez Votre Equipement personnel de Communication) ou BYOD (Bring Your Own Device) est une pratique qui consiste, pour les collaborateurs, à utiliser leurs équipements personnels (ordinateur, ordiphone, tablette) dans un contexte professionnel. Si cette solution est de plus en plus utilisée aujourd'hui, elle est cependant très problématique pour la sécurité des données personnelles et professionnelles (vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur).

De la même façon, il faut éviter de connecter des supports amovibles personnels (clés USB, disques durs externes) aux ordinateurs de l'entreprise.

8. SOYEZ AUSSI PRUDENT AVEC VOTRE ORDIPHONE (SMARTPHONE) OU VOTRE TABLETTE QU'AVEC VOTRE ORDINATEUR

Alexandre possède un ordiphone. Lors de l'installation d'une application, il n'a pas désactivé l'accès de l'application à ses données personnelles. Désormais, les éditeurs peuvent accéder à tous les SMS présents sur son téléphone.

Bien que proposant des services innovants, les ordiphones (smartphones) sont aujourd'hui très peu sécurisés. Il est donc indispensable d'appliquer certaines règles élémentaires d'hygiène informatique :

• n'installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l'accès à des données qui ne sont pas nécessaires à leur fonctionnement : il faut éviter de les installer

• en plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l'accès à votre terminal et configurez votre téléphone pour qu'il se verrouille automatiquement

• effectuez des sauvegardes régulières de vos contenus sur un support externe pour pouvoir les retrouver en cas de panne de votre ordinateur ou ordiphone

9. SOYEZ PRUDENT LORSQUE VOUS OUVREZ VOS MESSAGES ÉLECTRONIQUES

Suite à la réception d'un courriel semblant provenir d'un de ses amis, Madame Michel a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Madame Michel le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants diffusant des images pédopornographiques.

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées,...).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

- l'identité d'un expéditeur n'est en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message
- n'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoyez habituellement vos contacts
- si un lien ou plusieurs figurent dans un courriel, vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. L'adresse complète du site s'affichera alors dans la barre d'état en bas de la page ouverte. Si vous avez un doute sur l'adresse affichée, abstenez-vous de cliquer
- ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
- n'ouvrez pas et ne retapez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.

10. SOYEZ VIGILANT LORS D'UN PAIEMENT SUR INTERNET

Lorsque vous réalisez des achats en ligne, vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants, directement sur votre ordinateur.

Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs)
- assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet
- vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple

Si possible, lors d'un achat en ligne, privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.

De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire.

11. TÉLÉCHARGEZ LES PROGRAMMES, LOGICIELS SUR LES SITES OFFICIELS DES ÉDITEURS

Si vous téléchargez du contenu numérique sur des sites Internet dont la confiance n'est pas assurée, vous prenez le risque d'enregistrer sur votre ordinateur des programmes ne pouvant être mis à jour, qui le plus souvent contiennent des virus ou des chevaux de Troie. Cela peut permettre à des personnes malveillantes de prendre le contrôle à distance de votre machine pour espionner les actions réalisées sur votre ordinateur, voler vos données personnelles, lancer des attaques, etc.

• C'est la raison pour laquelle il est vivement recommandé de télécharger vos programmes sur les sites officiels des éditeurs

• Enfin, désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir, afin de vérifier qu'ils ne sont pas infectés par un quelconque virus ou spyware.



Réagissez à cet article

Comment sécuriser Firefox efficacement en quelques clics de souris ?

 Comment sécuriser Firefox
efficacement en quelques
clics de souris ?

Vous utilisez Firefox est vous souhaitez que cet excellent navigateur soit encore plus sécurisé lors de vos surfs sur Internet ? Voici quelques astuces qui supprimeront la géolocalisation, le profilage de Google ou encore que vos données offline disparaissent du regard d'espions locaux.

C'est sur le blog des Télécoms que j'ai vu pointer l'information concernant le réglage de plusieurs paramètres de Firefox afin de rendre le navigateur de la fondation Mozilla encore plus sécurisé. L'idée de ce paramétrage, empêcher par exemple Google de vous suivre à la trace ou de bloquer la géolocalisation qui pourrait être particulièrement big brotherienne.

Commençons par du simple. Il suffit de taper dans la barre de navigation de votre Firefox la commande `about:config`. Une alerte s'affiche, pas d'inquiétude, mais lisez là quand même. recherchez ensuite la ligne `security.tls.version`. Les valeurs affichées doivent osciller entre 1 et 3. Ensuite, recherchez la ligne `geo.enabled` pour annuler la géolocalisation. Passez le « true » en « False ». Pour que les sites que vous visitiez ne connaissent pas la dernière page que vous avez pu visiter, cherchez la ligne `network.http.sendRefererHeader` et mettez la valeur 1. Elle est naturellement placée à 2. Passez à False la ligne `browser.safebrowsing.malware.enabled`.

Ici, il ne s'agit pas d'autoriser les malwares dans Firefox, mais d'empêcher Google de vous tracer en bloquant les requêtes vers les serveurs de Google. Pour que Google cesse de vous profiler, cherchez la ligne `browser.safebrowsing.provider.google.lists` et effacez la valeur proposée.

Pour finir, vos données peuvent être encore accessibles en « offline », en mode hors connexion. Cherchez les lignes `offline-apps.allow_by_default` et `offline-apps.quota.warn`. La première valeur est à passer en False, la seconde valeur en 0.

Il ne vous reste plus qu'à tester votre navigateur via le site de la CNIL ou celui de l'Electronic Frontier Foundation.

Article original de Damien Bancal



Réagissez à cet article

Original de l'article mis en page : Sécuriser Firefox efficacement en quelques clics de souris – Data Security BreachData Security Breach

**Victime d'une arnaque sur
Internet ? Faites-nous part
de votre témoignage**

✕	Victime d'une arnaque sur Internet ? Faites-nous part de votre témoignage
---	--

**Vous êtes victime d'une arnaque ou d'un piratage sur Internet ?
Votre témoignage nous permettra peut-être de vous aider.**

Devant une explosion de cas d'arnaques et de piratages par Internet et des pouvoirs publics débordés par ce phénomène, nous avons souhaité apporter notre pierre à l'édifice. Vous souhaitez nous faire part de votre témoignage, contactez-nous.

Vous devez nous communiquer les informations suivantes (tout message incomplet et correctement rédigé ne sera pas traité) :

- une présentation de vous (qui vous êtes, ce que vous faites dans la vie et quel type d'utilisateur informatique vous êtes)
;
- un déroulé chronologique et précis des faits (qui vous a contacté, comment et quand et les différents échanges qui se sont succédé, sans oublier l'ensemble des détails même s'ils vous semblent inutiles, date heure, prénom nom du ou des interlocuteurs, numéro, adresse e-mail, éventuellement numéros de téléphone ;
- Ce que vous attendez comme aide (je souhaite que vous m'aidiez en faisant la chose suivante :)
- Vos nom, prénom et coordonnées (ces informations resteront strictement confidentielles).


Contactez moi

Conservez précieusement toutes traces d'échanges avec l'auteur des actes malveillants. Ils me seront peut-être utiles.



Réagissez à cet article

La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n'est pas trop tard !

	<p>La sensibilisation des utilisateurs est la principale clé pour se protéger des pirates informatiques. Il n'est pas trop tard !</p>
---	--

La sensibilisation des utilisateurs est la clé pour se protéger des pirates informatiques

L'avis de Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité (arnaques, virus, phishing...) en Direct sur LCI le 23 mai 2016 dans l'émission « Ca nous Concerne » de Valérie Expert.

En mai 2016, Denis JACOPINI nous sensibilisait encore et déjà aux **cyber risques**.

Nos formations / nos sensibilisations
Toutes nos vidéos

LE NET EXPERT ET DENIS JACOPINI FONT DÉSORMAIS PARTIE DES PRESTATAIRES DE CONFIANCE DE LA PLATEFORME



LE NET EXPERT

- **ACCOMPAGNEMENT RGPD (ÉTAT DES LIEUX ⇒ MISE EN CONFORMITÉ)**
 - ANALYSE DE VOTRE ACTIVITÉ
 - CARTOGRAPHIE DE VOS TRAITEMENTS DE DONNÉES
 - IDENTIFICATION DES RISQUES
 - ANALYSE DE RISQUE (PIA / DPIA)
 - MISE EN CONFORMITÉ RGPD de vos traitements
 - SUIVI de l'évolution de vos traitements
 - **FORMATIONS / SENSIBILISATION :**
 - CYBERCRIMINALITÉ
 - PROTECTION DES DONNÉES PERSONNELLES
 - AU RGPD
 - À LA FONCTION DE DPO
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - ORDINATEURS (**Photos / E-mails / Fichiers**)
 - TÉLÉPHONES (récupération de **Photos / SMS**)
 - SYSTÈMES NUMÉRIQUES
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
 - **SÉCURITÉ INFORMATIQUE**
 - SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article