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 Incredimail.

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 mémorisé au fil de vos consultations de sites Internet sont également stockés dans vote 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

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

---

Quelles formalités une pharmacie doit déclarer à la CNIL ? | Denis JACOPINI

Quelles formalités une pharmacie doit déclarer à la CNIL ?

Les fichiers relatifs à la gestion d’une pharmacie doivent être déclarés à la CNIL :Par une déclaration simplifiée de conformité à la norme n°52 si le fichier correspond aux caractéristiques énoncées dans ce texte ;
Par une déclaration normale si le fichier sort du cadre de cette norme.

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

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://www.aide.cnil.fr/selfcnil/site/template.do;jsessionid=193E337DAA685A15B25C9E90E19E80BF?name=Activit%C3%A9+d%27une+pharmacie+%3A+quelles+formalit%C3%A9s+%C3%A0+la+CNIL+%3F&id=545

Votre boite e-mail a été piratée. Quelle attitude adopter ? | Denis JACOPINI

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?

Un choix s'offre à vous :
Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage
Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?
– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?
– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?
– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?
1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.
Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions… Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.
2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulèrement (e-mail, banque, blog, réseaux sociaux…).
Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

Rechercher l'auteur et porter plainte
Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.
Soit vous avez les éléments techniques pouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.
Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Source : Denis JACOPINI

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 X années l'est encore plus. Il est donc nécessaire de savoir comment le faire sans laisser de données professionnelles ou 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 probablement en état de marche. À moins d'avoir des circonstances ou des consignes particulières, vous devrez donc rendre cet appareil au moins dans l'état initial.
1. En premier lieu, pensez à identifier les données à sauvegarder dont il vous sera nécessaire de conserver copie. Attention aux données professionnelles frappées de confidentialité ou d'une clause de non concurrence, tel que les fichiers clients.
On pourrait bien vous reprocher d'en avoir conservé une copie et de l'utiliser contre votre ancien employeur.
2. Identifiez les données ayant un caractère confidentiel et qui nécessiteront une sauvegarde dans un format protégé par un procédé tel que le cryptage ou le hachage.
3. Identifiez les données devant être conservées pendant un grand nombre d'années tels que des justificatifs d'assurance, de sinistre…
4. Identifiez les données que vous ne devez absolument pas perdre car non reproductibles (contrats, photos de mariage, des enfants, petits-enfants…)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ça soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, identifiez 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 adaptée soit :
– à la confidentialité (tout support numérique en utilisant un logiciel de cryptage ou de hachage tel de Truecrypt, Veracrypt, ou AxCrypt…) ;
– à l'intégrité (multiplier le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à n'absolument pas perdre) ;
– à la longévité en utilisant des supports avec une durée de vie adapté à vos attentes. Sachez 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'altération des supports avec le temps, mais aussi de l'évolution des versions, des formations et des logiciels). Qui peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
– à la disponibilité sur plusieurs plateformes et sur plusieurs lieux, comme le proposent les solutions *cloud* qui sont éclos il y a quelques dizaines d'années seulement ;
– à la quantité (car vous devez rapidement stocker pour ensuite trier et choisir un support adapté) en choisissant par exemple un disque dur USB externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui ayant 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 tomberont un jour ou l'autre en panne. Pensez-y pour ne pas leur confier les documents de votre vie.
Idem pour les disques durs. 100% des disques durs tomberont un jour en panne. Cependant, contrairement aux clés USB ou aux cartes mémoire, les disques durs (mécaniques et non SSD) permettront plus facilement de récupérer leur contenu en cas de panne.
Les supports de type lecteurs ZIP, lecteur JAZ, lecteurs magnéto-optiques, lecteurs de bandes etc. sont de plus en plus rares. Conserver des données importantes sur de tels supports peut s'avérer dangereux. En effet, imaginez un instant jour ou vous souhaitez y 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 vies de vos données numériques entre les mains du *Bon Coin*…
Voila, en fonction de tous ces critères et à partir de ces conseils, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

Comparatif :
Disque dur : Quelques Go à quelques To – Bon marché, rapide mais fragile.
Clé USB : Quelques Go – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.
Cloud : Quelques Mo à quelques To – 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 perdrez tout.
Disques optiques (CD, DVD,Magnéto Optique) : Bonne tenue dans le temps si conservés dans de bonnes conditions mais utilisables (pérennité des lecteurs de disques) jusqu'à quand ?
Supports spéciaux (ZIP/Jazz/QIC/DAT/DLT/DDS/SDLT) : Supports fragiles, lecteurs trop rares pour garantir une lecture au delà de 5 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 ?
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 « %*s*% *AppData\Local\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
– les fichiers contenus dans '%*s*%\APPDATA%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird
– le dossier contenu dans « …\Local Settings\Application Data\Identities » pour le programme Incredimail.
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 (cartes 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 mémorisé 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 »…

Ne pas effacer ses données personnelles sur so ordinateur de fonction est-il dommageable ? 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.

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 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 : 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

---

Arnaques, spams, phishing, sextape. Comment se protéger ? | Denis JACOPINI

Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée ?Quelle attitude adopter ?

Un choix s'offre à vous :
Vous protéger et faire cesser le piratage, ou bien rechercher l'auteur et porter plainte.

Vous protéger et faire cesser le piratage
Il vous semble ou vous avez la certitude que votre boite e-mail a été piratée. Quels sont les éléments qui vous font penser ça ?
– Quelqu'un est au courant de choses dont il ne devrait pas être au courant qui n'apparaît que dans les e-mails ?
– Vous constatez que des e-mails que vous n'avez pas lu sont tout de même « lus » ?
– Vous avez constaté dans l'historique des connexions une connexion qui ne semble pas être la votre ?
1°/ Pour vous protéger contre ça et faire cesser tout piratage, la première chose à faire est de lancer des outils de détection de virus, d'espions, keyloggers et autres logiciels malveillants.
Vous fournir une liste serait très compliqué car ceci engagerait quelque part ma responsabilité de vous conseiller un outil plutôt qu'un autre, alors qu'il en existe un grand nombre et aucun n'est fiable à 100%. Je ne peux vous conseiller que de rechercher sur Internet des « Antivirus Online », des Anti-Malwares, des Anti-espions… Toutefois, pour nos propres besoins nous avons une liste de liens accessible sur www.antivirus.lenetexpert.fr.
2°/ Une fois votre ordinateur nettoyé, vous pouvez procéder aux changements de mots de passe des différents services que vous utilisez régulèrement (e-mail, banque, blog, réseaux sociaux…).
Une fois ces deux étapes réalisées, vous ne devriez plus être « espionné ».

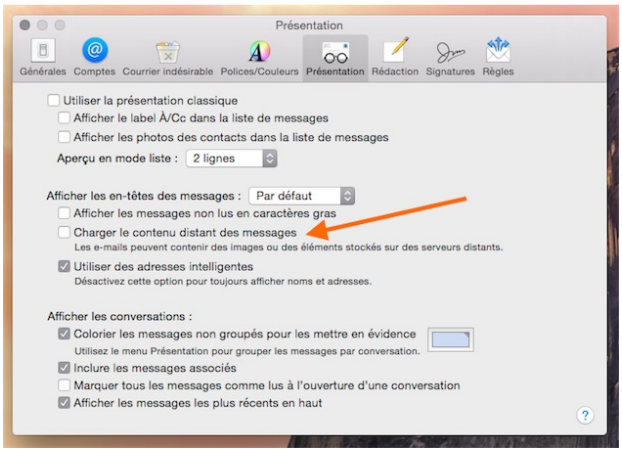
Rechercher l'auteur et porter plainte
Si vous suspectez une personne en particulier et que vous souhaitez l'attraper la main dans le sac, sachez que votre action doit prendre la voie de la justice.
Soit vous avez les éléments techniques prouvant l'action de l'auteur clairement identifié, et vous pouvez faire constater par huissier, soit, vous n'avez comme élément qu'une adresse IP, au quel cas, il sera nécessaire de se rapprocher d'un avocat conseil qui rédigera une requête auprès du Tribunal Adhoc afin d'obtenir une ordonnance nous permettant, en tant qu'expert, de réaliser les démarches auprès des fournisseurs de services concernés par le piratage.
Une autre solution plus économique car gratuite mais à l'issue incertaine est de signaler les actes de piratages dont vous êtes victime aux services de Gendarmerie ou de Police en commissariat, en brigade ou sur le site Internet www.internet-signalement.gouv.fr. Cependant, s'il n'y a pas de très grosses sommes en jeu, d'actes délictueux auprès de mineurs ou en rapport avec des entreprises terroristes, vous comprendrez aisément que votre demande ne sera pas considérée comme prioritaire. Sachat que les opérateurs conservent les traces qui vous permettront d'agir en justice quelques mois, quelques semaines ou quelques jours, votre demande par cette voie risque fortement d'être classée sans suite.

Denis JACOPINI est Expert Informatique assermenté, pratiquant à la demande de particuliers d'entreprises ou de Tribunaux. Il est consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

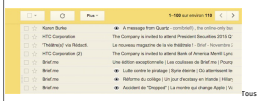
Comment se protéger des emails trop curieux | Denis JACOPINI



Comment se protéger des emails trop curieux

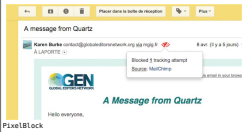
Sans même que vous visitiez un site web, les publicitaires peuvent récolter des informations vous concernant. L'une des techniques utilisées, très répandue et pas illégale, est le pixel tracking.

Une image transparente de 1 x 1 pixel liée à une URL est insérée dans un email. Quand l'email est ouvert, cette minuscule image est chargée et communique avec les serveurs du publicitaire qui a alors accès à des données personnelles, comme l'adresse IP, l'emplacement géographique (via l'IP), l'heure de la consultation et le terminal utilisé.
Les éditeurs ne font pas toujours preuve de tant de discrétion pour récolter des informations à partir des emails (une simple image, comme un logo d'entreprise, suffit), mais le résultat est le même ; des données sont récoltées sans le consentement de l'utilisateur.



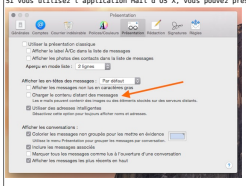
Tous les éditeurs n'utilisent pas le pixel tracking ou une autre technique de traçage à des fins publicitaires. Brief.me, un mini-journal disponible uniquement par email, l'exploite par exemple pour avoir des statistiques de consultation.

L'extension Chrome UglyEmail met en lumière les emails exploitant des techniques de traçage d'entreprises spécialisées (Streak, Yesware, Mandrill, MailChimp, Postmark, TinyLetter, Sidekick, MixMax et Bananatag). Quand UglyEmail repère dans la boîte de réception de Gmail un email trop curieux, il le signale avec une petite icône d'œil.
L'extension n'enregistre et ne transmet aucune donnée provenant de Gmail, assure son auteur à Wired. Des versions pour Firefox et Safari sont en développement.
PixelBlock, une autre extension Chrome réservée elle aussi à Gmail, va plus loin puisqu'elle bloque carrément le tracking. En cliquant sur l'œil rouge à côté du nom de l'expéditeur, on découvre la source du service de traçage.



PixelBlock

Si vous utilisez l'application Mail d'OS X, vous pouvez préserver votre confidentialité en désactivant le chargement des contenus distants des emails (l'option se trouve dans l'onglet Présentation des préférences). Cela fonctionne avec tous les fournisseurs de courrier électronique (Gmail, iCloud, Outlook, Yahoo…).



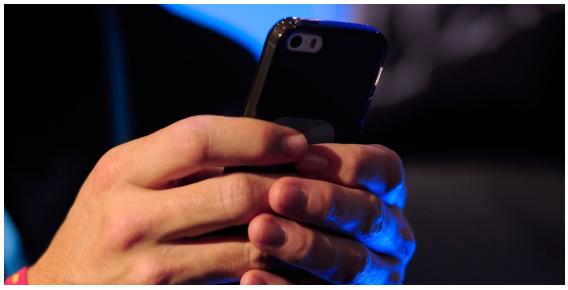
Puisque le lien avec le serveur distant est coupé, les informations personnelles ne sont pas divulguées. Cela a aussi pour effet de « casser » la mise en page des emails qui utilisent des images distantes, mais Mail permet très simplement de charger le contenu distant au cas par cas (un bouton est présent en haut du courrier quand le cas se présente).

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.macg.co/logiciels/2015/04/confidentialite-comment-se-proteger-des-emails-trop-curieux-88326
Par Stéphane Moussie

Les données personnelles des portables d'occasion toujours accessibles | Denis JACOPINI



Les données personnelles des portables d'occasion toujours accessibles

De nombreux smartphones reconditionnés contiennent toujours des informations sensibles sur leurs anciens propriétaires.

Avant de revendre votre portable, veillez à bien effacer toutes vos données personnelles. En effet, de nombreux smartphones reconditionnés – c'est-à-dire d'occasion et revendus dans les boutiques – contiennent toujours des informations de leurs anciens propriétaires, selon une étude réalisée par l'entreprise Avast, spécialisée dans les antivirus, et révélée en exclusivité par Europe 1.
Emails, photos, SMS, factures personnelles ou même clichés à caractère sexuel : ces téléphones renferment souvent des données extrêmement sensibles.

Un contrat de travail, des mails et des SMS retrouvés

Le problème concerne une part croissante du marché des téléphones portables. 10% des Français ont en effet acheté un mobile de seconde main en 2015. Avast a ainsi mené une expérimentation sur vingt anciens modèles de smartphone, achetés à New York, Paris, Barcelone et Berlin. Les résultats sont édifiants : sur cet échantillon test, de nombreuses données personnelles ont été retrouvées.
Avast a ainsi pu accéder à 2.000 photos, dont des clichés d'enfants, d'autres à caractère sexuel, mais aussi un contrat de travail ou encore 300 mails et SMS. Pire : deux propriétaires de téléphone avaient oublié de déconnecter leurs comptes Gmail, prenant le risque que les nouveaux acheteurs lisent ou envoient des mails en leur nom.

« Important de faire une démarche complète »

Bien que 40% des portables vendus dans les boutiques d'occasion soient reconditionnés, les anciens propriétaires réinitialisent souvent mal, voire pas du tout, leurs terminaux. Les revendeurs spécialisés le constatent ainsi tous les jours. « Ça arrive à un client sur deux : quand il nous propose son téléphone, il ne l'a pas effacé au préalable », explique Frédéric Bertinet, de Cash Express.
« Les téléphones ont été mal réinitialisés, donc on pense qu'on a fait le travail parce qu'on a enlevé les mots de passe et les réglages, mais le contenu lui n'a pas été effacé. Il est important de faire une démarche complète, un peu procédurière », conclut Frédéric Bertinet.

Des applications sécurisées pour effacer les données

Mais pour éviter tout risque, une simple réinitialisation ne suffit pas. « Lorsqu'un fichier est effacé, c'est seulement la référence de ce fichier qui disparaît. Pour que ces fichiers disparaissent complètement, il faut les remplacer par d'autres données quelconques, c'est-à-dire des 0 et des 1. Sinon, c'est théoriquement récupérable », détaille Arnaud Matthieu, représentant d'Avast pour la France.
Pour vider à jamais votre téléphone portable, des applications sécurisées sont disponibles gratuitement sur Internet. Mais attention : si vous n'écrasez pas correctement vos données personnelles, les risques sont immenses. Les anciens propriétaires de smartphones s'exposent à du chantage, à des photos personnelles publiées sur internet ou encore à de l'usurpation d'identité.

Réagissez à cet article

Source : *Les données personnelles des portables d'occasion toujours accessibles*

Télécharger tout votre historique Google est maintenant possible | Denis JACOPINI

	Télécharger tout votre h2istorique Google est maintenant possible

En attendant une fonction d'importation qui pourrait devenir standard pour tous les moteurs de recherche, Google propose aux internautes de télécharger une copie de tout leur historique de recherches effectuées depuis qu'ils utilisent un compte Google.

Google donnait depuis longtemps la possibilité aux internautes de consulter leur historique de recherches, à condition d'utiliser le moteur de recherche en étant identifié sur le service. Désormais, il est également possible de télécharger un archive qui contient l'ensemble des recherches effectuées depuis la création de votre compte. Il suffit de vous rendre sur la page de l'historique, et de cliquer sur l'icône des options tout en haut à droite :

Lors de la demande de téléchargement de l'historique, une pop-up s'ouvre qui prévient qu'un lien permettant de télécharger le fichier stocké sur l'espace personnel Google Drive de l'archive sera envoyé à l'adresse Gmail. Etant donnée la sensibilité des informations que peuvent contenir vos recherches (sans doute beaucoup plus nombreuses que vous ne l'imaginez), Google conseille tout de même de ne pas télécharger le fichier depuis un ordinateur public, et d'utiliser la validation en deux étapes de l'identification.
Alors que vous ne voyez sans doute pas l'intérêt de télécharger votre historique, l'intérêt est d'assurer la portabilité des données personnelles, au cas où vous souhaiteriez changer de moteur de recherche sans perdre toute la personnalisation des résultats et des suggestions créée à partir des milliers de requêtes effectuées précédemment. Il sera ainsi peut-être un jour possible d'importer son historique de recherches dans Yahoo, Bing, Qwant ou DuckDuckGo, et réciproquement, d'importer ses recherches vers Google. Ce n'est sans doute pas très utile vu d'Europe où Google écrase le marché des moteurs de recherche, mais ça peut avoir un intérêt aux Etats-Unis où Google représente autour de 65 % du marché.
Le fichier reçu est une archive .ZIP qui contient l'ensemble des recherches réunies dans un fichier par trimestre, au format JSON. Qui sait ce que les développeurs auront l'idée d'en faire ?

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.numerama.com/magazine/32852-telecharger-tout-votre-historique-google-est-maintenant-possible.html

---

Piratage informatique : bien plus sûre que le « mot de

passe », la « phrase de passe » (à condition que…)| Denis JACOPINI

	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 vérouille nos différents comptes.

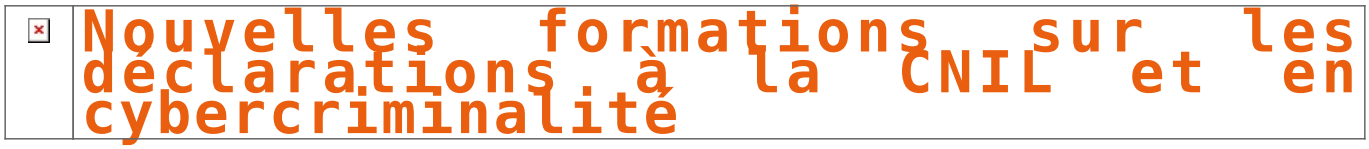
Enfin et surtout, je conseille de ne pas se focaliser uniquement sur la conception du mot de passe ou de la « phrase de passe », parce que c'est très loin d'être suffisant pour se prémunir du piratage informatique. Ouvrir par erreur un mail contenant un malware peut donner accès à toutes vos données 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 vérrouiller son ordinateur, etc…

Article original de Denis JACOPINI et Atlantico

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

Nouvelles formations sur les déclarations à la CNIL et en cybercriminalité | Denis JACOPINI



Pour information, Denis JACOPINI propose depuis quelques mois deux nouveaux sujets de formation à destination des chefs d'entreprise, de leurs salariés mais aussi des administrations et de leurs agents :

– La cybercriminalité, un vrai risque pour les chefs d'entreprises– Mettre son entreprise en conformité avec la CNIL, secrets et mode d'emploi
– Cybercriminalité, sécurité informatique et CNIL, bonnes pratiques et cadre juridique
– La cybercriminalité, un vrai risque pour administrations

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

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…