

# Guide du Cloud Computing et des Datacenters à l'attention des collectivités locales | Denis JACOPINI

 Guide du Cloud Computing et des Datacenters à l'attention des collectivités locales

## A l'attention des collectivités locales

Les concepts de Cloud Computing et de Datacenters suscitent un fort intérêt de la part des collectivités locales, mais soulèvent également de nombreuses questions.

La Direction Générale des Entreprises, la Caisse des Dépôts et le Commissariat Général à l'Egalité des territoires proposent un guide pratique pour orienter les collectivités locales dans leurs réflexions.

- Comment répondre aux nouveaux besoins et disposer rapidement de nouvelles ressources informatiques ?
- Comment gérer et administrer facilement les ressources nécessaires à l'ensemble des services ?
- Comment assurer la disponibilité en continu de ces services ?
- Comment garantir l'interopérabilité des plateformes et la pérennité des solutions technologiques ?
- Comment gérer les problématiques de confidentialité et de sécurité des données ?
- Comment maîtriser les coûts de construction et d'exploitation des solutions ?
- Quels changements ces solutions imposent-elles dans le fonctionnement des Dsi et des services numériques ?
- Comment contractualiser avec les fournisseurs de services et maîtriser la relation client – fournisseur ?
- Quelles sont les contraintes liées à la construction et à la maintenance d'un Datacenter ?
- Comment mesurer la rentabilité d'un Datacenter ?
- Quelle est la pérennité des investissements dans les Datacenters locaux ou Datacenters de proximité implantés sur le territoire ?
- Quelle stratégie adopter pour mutualiser les projets et conserver la maîtrise des coûts ?

Ce guide a ainsi pour mission d'apporter un éclairage sur les différents concepts et de proposer aux collectivités un ensemble de solutions et de moyens pour réussir leurs projets.

Il s'adresse à la fois aux élus locaux, aux responsables du développement économique des territoires, aux responsables informatiques, aux opérationnels au sein des collectivités, associations et structures de mutualisation , ainsi qu'à tous les acteurs publics et privés de ces écosystèmes.

---

Nous organisons régulièrement, en collectivité ou auprès des CNFPT des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité 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 !

Source

<http://www.entreprises.gouv.fr/secteurs-professionnels/guide-du-cloud-computing-et-des-datacenters>

# Comment bien choisir ses mots de passe ?



**Les mots de passe sont une protection incontournable pour sécuriser l'ordinateur et ses données ainsi que tous les accès aux services sur Internet. Mais encore faut-il en choisir un bon. Un bon mot de passe doit être difficile à deviner par une personne tierce et facile à retenir pour l'utilisateur.**

### **Qu'est ce qu'un bon mot de passe ?**

Un bon mot de passe est constitué d'au moins **12 caractères** dont :

- des lettres majuscules
- des lettres minuscules
- des chiffres
- des caractères spéciaux

Un mot de passe est d'autant plus faible qu'il est court. L'utilisation d'un alphabet réduit ou de mot issu du dictionnaire le rend très vulnérable.

Les mots du dictionnaire ne doivent pas être utilisés.

Aussi à proscrire, les mots en relation avec soi, qui seront facilement devinables : nom du chien, dates de naissances...

Réseaux sociaux, adresses mail, accès au banque en ligne, au Trésor public, factures en ligne.

Les accès sécurisés se sont multipliés sur internet.

Au risque de voir tous ses comptes faire l'objet d'utilisation frauduleuse, il est impératif de **ne pas utiliser le même mot de passe** pour des accès différents.

Alors, choisir un mot de passe pour chaque utilisation peut vite devenir un vrai casse-tête.

### **Comment choisir et retenir un bon mot de passe ?**

Pour créer un bon mot de passe, il existe plusieurs méthodes :

#### **La méthode phonétique**

Cette méthode consiste à utiliser les sons de chaque syllabe pour créer une phrase facilement mémorisable.

Exemple : « j'ai acheté huit cd pour cent euros ce après-midi » donnera : ght8CD%E7am

#### **La méthode des premières lettres**

Utiliser les premières lettres d'une phrase en variant majuscules, minuscules et caractères spéciaux.

Exemple : « un tiens vaut mieux que deux tu l'auras » donnera : 1TvmQ2tl@

#### **Diversifier facilement les mots de passe**

Opter pour une politique personnelle avec, par exemple, un préfixe pour chaque type d'activité. Comme BANQUE-MonMotDePassz pour la banque, IMP-MonMotDePasse pour les impôts. Quelque chose de très facile à mémoriser qui complexifie votre mot de passe et, surtout, vous permet de le diversifier.

#### **Diminuer les imprudences**

Pour finir, il est utile de rappeler de **ne pas stocker ses mots de passe à proximité de son ordinateur** si il est accessible par d'autres personnes. L'écriture sur le post-it déposé sous le clavier est à proscrire par exemple, de même que le stockage dans un fichier de la machine.

En règle général, les logiciels proposent de **retenir les mots de passe**, c'est très **tentant mais imprudent**. Si votre ordinateur fait l'objet d'un piratage ou d'une panne, les mots de passe seront accessibles par le pirate ou perdus.

#### **Que faire en cas de piratage ?**

Il est recommandé de préserver les traces liées à l'activité du compte.

Ces éléments seront nécessaires en cas de dépôt de plainte au commissariat de Police ou à la Gendarmerie.

Exemple

#### **Compte email piraté**

Vos contacts ont reçu des messages suspects envoyés de votre adresse.

Contactez-les pour qu'ils conservent ces messages.

Ils contiennent des informations précieuses pour l'enquêteur qui traitera votre dépôt de plainte.

Récupérez l'accès à votre compte afin de changer le mot de passe et re-sécurisez l'accès à votre compte.

#### **Changer de mots de passe régulièrement**

Cette dernière règle est contraignante mais assurera un niveau supérieur de sécurité pour vos activités sur Internet.

Un **bon mot de passe doit être renouvelé plusieurs fois par an** et toujours en utilisant les méthodes décrites ci-dessus.

---

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 **arnachages et les piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.

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



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

# **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>



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

---

# Lutte contre les cyberattaques : bien choisir son mot de passe | Denis JACOPINI



Lutte contre les  
cyberattaques : bien  
choisir son mot de passe

**Chaque année, les cyberattaques coûtent plus de 400 milliards de dollars à l'économie mondiale.**

Pour renforcer la sécurité sur internet, il est important de bien choisir ses mots de passe : huit caractères avec au moins une majuscule et un mélange de chiffres et de lettres. Le mot de passe doit être le plus compliqué possible et différent pour chaque compte afin d'être le plus sécurisé. Il reste tout de même de plus en plus facile à déceler pour les hackers et difficile à mémoriser pour les utilisateurs. Résultat : on opte pour la facilité. En 2014, le mot de passe le plus utilisé sur internet était la suite de chiffres : 1 2 3 4 5 6.

#### **Un enjeu de taille**

Le mot de passe serait à l'origine de 31% des cyberattaques avec un coût de 445 milliards de dollars chaque année pour l'économie mondiale. L'enjeu économique est de taille. Un consortium d'entreprises et d'États planche sur de nouvelles techniques d'authentification : scan de l'iris, empreinte digitale, reconnaissance vocale ou faciale... Des éléments propres au véritable utilisateur et donc plus sécurisés.

---

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

[http://www.francetvinfo.fr/monde/lutte-contre-les-cyberattaques-bien-choisir-son-mot-de-passe\\_968535.html](http://www.francetvinfo.fr/monde/lutte-contre-les-cyberattaques-bien-choisir-son-mot-de-passe_968535.html)

# **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 cliquaient sur des liens d'expéditeurs inconnus (environ 56% d'utilisateurs de boîte mails et 40% d'utilisateurs de Facebook), tout en étant parfaitement conscient des risques de virus ou d'autres infections.

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

Attention :

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

Denis JACOPINI :

« Il 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 également des informations souhaitées, des messages de personnes ou d'organismes connus nous envoyant une information ou souhaitant que nous nouvelles et quelques autres messages que nous recevons avec plaisir de personnes connues.

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 (spam + e-mail) se cachent de nombreux message 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 : 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

Auteur : 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 laquelle 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 a 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

Auteur : 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 détails

Mille bonnes 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 fait 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 d'une personne inconnue 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 événement d'une soirée que vous auriez rencontré sur Facebook ?

Dans le doute vous l'acceptez comme auteur pour en savoir plus et engager l'arbitrage pour la conversation.

C'est un autre moyen utilisé par les pirates informatiques pour rentrer dans votre cercle d'amis et probablement tenter des actes illicites que je ne détaillerai pas ici.

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

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

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

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

Denis Jacopini anime des conférences et des formations et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux CyberRisques (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03841 84).

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

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



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

- Expertises : arnaques (virus, spyware, phising, fraude, arnaques financières...) et piratages (informatiques, débrouilleurs de données, cryptomonnaies, etc.)
- Expertises en systèmes de vote électronique
- Formations et conférences en cybersécurité
- Formation de C.I.L. (Correspondant Informatique de la CNIL) à votre établissement
- Accompagnement à la mise en conformité CNIL de votre établissement

**Le Net Expert**  
INFORMATIQUE  
Conseil en Cybercriminalité et  
Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

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

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

**Un œil 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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

---

# 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 raccourci 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 RevõInstall (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 « %AppData%\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
- les fichiers contenus dans « %APPDATA%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird
- le dossier contenu dans « ..\Local Settings\Application Data\IMIdentities » 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 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.

#### 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>



[Contactez-nous](#)

Réagissez à cet article

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

# 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. A 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 devrez 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 adaptée 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 éclatés 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 des 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 vie de vos données numériques entre les mains du Bon Coin...

Voilà, 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.

Cle 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 le 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/OIC/DAT/DLT/DOS/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 raccourci 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 « %AppData%\Microsoft\Windows Live Mail » pour le logiciel « Windows Live Mail » ;
- les fichiers contenus dans « %AppData%\Thunderbird\Profiles » pour le programme Mozilla Thunderbird
- le dossier contenu dans « Local Settings\Application Data\IMIdentities » 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 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 système 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 son 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>

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

- Expertise techniques (virus, espions, pirates, fraudes, arnaques Internet et judiciaires (évasion fiscale, déguisement d'identité, malwares, conteneurs, détournements de clientèle...));
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

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

---

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



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

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

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

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

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

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

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

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

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

#### Le mythe de la victime idéale

En 2014, le groupe de cybercriminels Darkhotel avait utilisé une connexion Wi-Fi pour infiltrer un réseau d'hôtels de luxe et espionner quelques-uns de leurs clients les plus prestigieux. Un an plus tard, les activités de ce groupe étaient toujours en cours, continuant d'exfiltrer les données des dirigeants d'entreprises et dignitaires. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisateurs continuent de penser qu'ils ne courrent aucun risque car les informations qu'ils partagent sur Internet ne méritent pas d'être piratées. C'est oublier que la rentabilité d'une attaque repose aussi sur le nombre de victimes. Parmi les 30 millions de clients pris en charge par l'hôtellerie française chaque année, seuls 20% sont des clients d'affaires. Les 80% de voyageurs de loisirs représentent donc une manne financière tout aussi importante pour des cybercriminels en quête de profit. Dans certains cas, une faille Wi-Fi peut même exposer l'hôtel lui-même, en servant de porte d'entrée vers son réseau. Si l'on prend le cas d'une chaîne d'hôtellerie internationale qui disposerait d'un système de gestion centralisé et automatisé, une intrusion sur le réseau pourrait entraîner le vol à grande échelle d'informations confidentielles et bancaires sur les employées, le fonctionnement de l'hôtel et ses clients.

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

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

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

Article original de Robert Kassous

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

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

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

Denis JACOPINI



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, conteneurs, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Liberté) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

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

---

# **Sensibilisations et Formations à la Cybercriminalité et au RGPD (Protection des données personnelles) – Redirect**

**Parce que la Cybercriminalité et la Protection des données personnelles sont liés, nous couvrons ces sujets concomitamment (Intervention en France et étranger)**

Nos formations sont personnalisées en fonction du type de publics présent (Dirigeants, cadres, informaticiens, responsable informatique, RSSI, utilisateurs).

[Contactez-nous](#)

## **PROGRAMME**

**CYBERCRIMINALITÉ**  
**COMMENT PROTÉGER VOTRE ORGANISME DE LA CYBERCRIMINALITÉ**

[Présentation](#)

La France a rattrapé son retard en matière d'équipement à Internet mais à en voir les dizaines de millions de français victimes chaque année, les bonnes pratiques ne semblent toujours pas intégrées dans vos habitudes.

Piratages, arnaques, demandes de rançons sont légions dans ce monde numérique et se protéger au moyen d'un antivirus ne suffit plus depuis bien longtemps.

Avons-nous raison d'avoir peur et comment se protéger ?

Cette formation couvrira les principaux risques et les principales solutions, pour la plupart gratuites, vous permettant de protéger votre informatique et de ne plus faire vous piéger.

### Objectifs

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant de naviguer sur Internet en toute sécurité.

Demande d'informations

## **CYBERCRIMINALITÉ** **LES ARNAQUES INTERNET A CONNAÎTRE POUR NE PLUS SE FAIRE AVOIR**

### Présentation

Que vous vous serviez d'Internet pour acheter, vendre, télécharger ou communiquer, un arnaqueur se cache peut-être derrière votre interlocuteur.

Quels sont les signes qui ne trompent pas ? Comment les détecter pour ne pas vous faire piéger ?

### Objectifs

Découvrez les mécanismes astucieux utilisés par les arnaqueurs

d'Internet dans plus d'une vingtaine cas d'arnaques différents. Une fois expliqués, vous ne pourrez plus vous faire piéger.

### Demande d'informations

## **PROTECTION DES DONNÉES** **RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION** **DES DONNÉES) – CE QU'IL FAUT SAVOIR POUR** **NE PAS LE PAYER CHER**

### Présentation

Le Règlement Général sur la Protection de Données (RGPD) est entré en application le 25 mai 2018 et toutes les entreprises, administrations et associations ne se sont pas mises en conformité. Or, quelle que soit leur taille, elles sont toutes concernées et risqueront, en cas de manquement, des sanctions financières jusqu'alors inégalées.

Au delà de ces amendes pouvant atteindre plusieurs millions d'euros, de nouvelles obligations de signalement de piratages informatiques risquent désormais aussi d'entacher votre réputation. Quelle valeur lui donnez vous ? Serez-vous prêt à la perdre pour ne pas avoir fais les démarches dans les temps ?

Cette formation non seulement répondra la plupart des questions que vous vous posez, vous offrira des éléments concrets non seulement pour initier la mise en conformité de votre établissement mais surtout pour transformer ce qui peut vous sembler à ce jour être une contrainte en une véritable opportunité.

### Objectifs

Cette formation a pour objectif de vous apporter l'essentiel pour comprendre et démarrer votre mise en conformité avec le

RGPD dans le but à la fois de répondre à la réglementation et de prévenir en cas de contrôle de la CNIL.

## Informations complémentaires

### Demande d'informations

## PROTECTION DES DONNÉES

### RGPD (RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES) – ANALYSONS CE QUE VOUS AVEZ COMMENCÉ

#### Présentation

Après avoir suivi notre formation vous permettant de comprendre l'intérêt d'une telle réglementation et de savoir ce qu'il faut mettre en place pour bien démarrer, vous souhaitez aller plus loin dans la démarche de mise en conformité avec le RGPD.

Après un retour éclair sur les règles de base, nous ferons un point sur la démarche de mise en conformité que vous avez initiée ces derniers mois dans votre établissement. Nous détaillerons ensuite les démarches à réaliser en cas de détection de données sensibles et d'analyse d'impact. Enfin, nous approfondirons des démarches périphériques essentielles pour répondre à vos obligations.

#### Objectifs

Après avoir déjà découvert l'essentiel pour comprendre et démarrer votre mise en conformité avec le RGPD, cette formation aura pour objectif de vous perfectionner afin de devenir référent protection des données ou DPO (Data Protection Officer = Délégué à la Protection des Données).

### Demande d'informations

# **CYBERSÉCURITÉ**

## **DÉTECTER ET GÉRER LES CYBER-ATTAQUES**

### Présentation

Que vous ayez déjà été victime d'une cyber-attaque ou que vous souhaitiez l'anticiper, certaines procédures doivent absolument être respectées pour conserver un maximum de preuves et pouvoir les utiliser.

### Objectifs

Que votre objectif soit de découvrir le mode opératoire pour savoir quelles sont les failles de votre système ou si vous avez été victime d'un acte ciblé avec l'intention de vous nuire, découvrez les procédures à suivre.

Demande d'informations

# **CYBERSÉCURITÉ**

## **APPRENEZ À RÉALISER DES AUDITS SÉCURITÉ SUR VOTRE SYSTÈME INFORMATIQUE**

### Présentation

Votre système informatique a très probablement de nombreuses vulnérabilités présentées aux pirates informatiques comme de nombreux moyens de nuire à votre système informatique.

Avant de procéder à un test d'intrusion, apprenez à réaliser l'indispensable audit sécurité de votre système informatique afin d'appliquer les mesures de sécurité de base présentes dans les référentiels internationalement utilisés.

### Objectifs

**Vous apprendrez au cours de cette formation la manière dont doit être mené un audit sécurité sur un système informatique, quelques référentiels probablement adaptés à votre organisme et nous étudierons ensemble le niveau de sécurité informatique de votre établissement.**

**Demande d'informations**

## **CYBERSÉCURITÉ**

### **APPRENEZ À RÉALISER DES TESTS D'INTRUSION SUR VOTRE SYSTÈME INFORMATIQUE**

#### Présentation

Cette formation vous apporte l'essentiel de ce dont vous avez besoin pour adopter l'approche du Hacker pour mieux s'en protéger en élaborant vos tests de vulnérabilité, mettre en place une approche offensive de la sécurité informatique permettant d'aboutir à une meilleure sécurité et réaliser des audits de sécurité (test d'intrusion) au sein de votre infrastructure.

La présentation des techniques d'attaques et des vulnérabilités potentielles sera effectuée sous un angle « pratique ».

#### Objectifs

Cette formation vous apportera la compréhension technique et pratique des différentes formes d'attaques existantes, en mettant l'accent sur les vulnérabilités les plus critiques pour mieux vous protéger d'attaques potentielles.

**Demande d'informations**

## QUI EST LE FORMATEUR ?

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

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

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

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

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

Denis JACOPINI peut facilement être contacté sur :  
<http://www.leNetExpert.fr/contact>

