

# Comment bien se protéger contre les Cyberattaques ?



Comment bien se protéger  
contre les Cyberattaques ?

---

**On l'a encore vu récemment, aucun système informatique n'est à l'abri d'une faille...**

Et en matière de cybercriminalité, les exemples nous montrent que l'attaque semble toujours avoir un coup d'avance sur la défense. L'enjeu, pour les institutions et les entreprises, est d'anticiper et de se préparer à ces situations de crise en développant, en amont, une stratégie à-même de minorer au maximum leurs conséquences.

Demande de rançons, fraudes externes, défiguration de sites web, vols ou fuites d'informations, cyber-espionnage économique ou industriel..., en 2016 huit entreprises françaises sur dix ont été victimes de cybercriminels, contre six en 2015. La tendance n'est malheureusement pas à l'amélioration et l'actualité récente regorge d'exemples frappants : le logiciel malveillant WannaCry qui vient de frapper plus de 300 000 ordinateurs dans 150 pays avec les conséquences désastreuses que l'on connaît, l'attaque du virus Adylkuzz qui ralentit les systèmes informatiques, le vol de la copie numérique du dernier opus de la saga « Pirates des Caraïbes » quelques jours avant sa sortie mondiale..., les exemples de cyberattaques ne cessent de défrayer la chronique.

Pour bien se protéger contre les Cyberattaque, nous vous conseillons de suivre les étapes suivantes :

1. Faire ou faire faire un état des lieux des menaces et vulnérabilités risquant de mettre en danger votre système informatique ;
2. Faire ou faire faire un état des lieux des failles aussi bien techniques qu'humaines ;
3. Mettre en place les mesures de sécurité adaptées à vos priorités et aux moyens que vous souhaitez consacrer ;
4. Assurer une surveillance des mesures de sécurité et s'assurer de leur bon fonctionnement et de leur adaptation au fil de vos évolutions aussi bien techniques que stratégiques.

- Vous souhaitez faire un point sur l'exposition de votre entreprise aux risques cyber ?
- Vous souhaitez sensibiliser votre personnel aux différentes arnaques avant qu'il ne soit trop tard ?
- Vous recherchez une structure en mesure de mettre en place une surveillance de votre réseau, de votre installation, de vos ordinateurs ?

Contactez-vous

---

**Notre métier :** Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur

: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *Cyberattaque, comment faire pour limiter les risques ?*

---

# Alerte Virus ! Rombertik détruit le PC lorsqu'il est détecté | Denis JACOPINI



Alerte Virus !  
Rombertik détruit le PC lorsqu'il  
est détecté

**La menace a de quoi faire froid dans le dos. Les équipes de chercheurs de Talos (Cisco) viennent de repérer un nouveau type de malware capable de mettre à genoux un PC et les données qu'il contient. Rien de neuf, me direz-vous...**

Mais Rombertik, c'est son petit nom, a été pensé pour contourner les protections mises en place, qu'elles soient système ou liées à un anti-virus. Pire, il devient particulièrement agressif lorsqu'il est chatouillé ou en phase d'être repéré.

Comme d'habitude, Rombertik se loge dans votre PC via un mail (spam ou phishing) contenant un lien piégé, souvent un faux PDF. Une fois exécuté, le malware fait le tour du propriétaire et s'assure de ne pas être enfermé dans une sandbox. Après s'être déployé, il est ensuite capable de s'insérer dans le navigateur utilisé pour collecter des données personnelles, même sur un site en https, et les expédier vers un serveur distant. Classique.

Dans le même temps, et c'est à ce moment qu'il est le plus dangereux, le malware vérifie qu'il n'est pas en cours d'analyse mémoire. Si c'est le cas, il va alors tenter de détruire le Master Boot Record (MBR), endommageant gravement le PC. Ce composant est essentiel pour démarrer une machine Windows.

S'il ne parvient pas à ses fins, il s'attaquera alors aux fichiers présents dans le dossier utilisateurs, fichiers qui seront alors cryptés avec une clé RC4 aléatoire. La machine est alors rebootée mais entre dans une boucle infinie. Bref, les dégâts sont majeurs. Et une analyse anti-virus aura les mêmes effets. La réinstallation du système est alors le seul moyen d'accéder à sa machine.

« Ce qui est intéressant avec ce malware, c'est qu'il n'a pas une fonction malveillante, mais plusieurs », souligne les experts de Talos. « Le résultat est un cauchemar », ajoutent-ils.

Comment alors se protéger ? « Etant donné que Rombertik est très sensible à la traditionnelle sandboxing réactive, il est crucial d'utiliser des systèmes de défense modernes – prédictifs. Des systèmes qui n'attendent pas qu'un utilisateur clique pour déclencher un téléchargement potentiel de Rombertik. », explique Charles Rami, responsable technique Proofpoint..

« De plus, comme le malware peut être expédié via de multiples vecteurs – comme Dyre, via des URL ou des fichiers .doc ou .zip/exe etc. – il est crucial d'utiliser des systèmes qui examinent l'ensemble chaîne destructrice, et bloquent l'accès des utilisateurs aux URL et pièces jointes envoyées par emails avant ceux-ci ne cliquent dessus. Enfin, les aspects « autodestruction » de Rombertik état susceptibles d'être déclenchés par les technologies telles que les antivirus, il est crucial que les entreprises utilisent des systèmes automatisés de réponse aux menaces – des systèmes qui peuvent localiser et bloquer l'exfiltration de données par Rombertik – sans – déclencher d'action sur le PC, et alerter les équipes de sécurité pour répondre rapidement aux dommages pouvant être causés », poursuit-il.

---

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

---

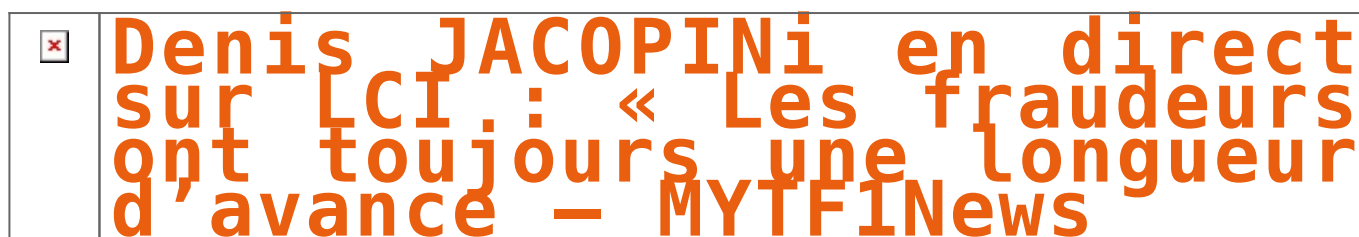
Cet article vous plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source :

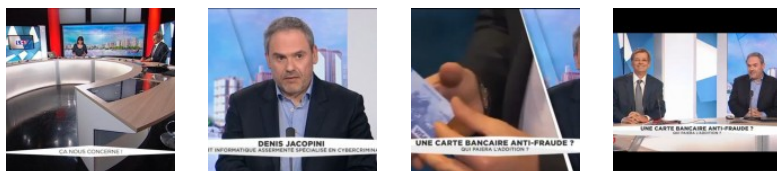
<http://www.zdnet.fr/actualites/rombertik-un-virus-qui-detruit-le-pc-lorsqu-il-est-detecte-39818978.htm>

# Denis JACOPINI en direct sur LCI : « Les fraudeurs ont toujours une longueur d'avance – MYTF1News | Denis JACOPINI



Denis Jacopini, expert informatique assermenté spécialisé en cybercriminalité, explique que quoi que l'on fasse, les fraudeurs auront une longueur d'avance. Néanmoins, il y a des failles dans le système, et en particulier au niveau du cryptogramme visuel.

En direct sur LCI avec Serge Maître Maître, président de l'AFUB (Association Française des Usagers des Banques) et Nicolas CHATILLON, Directeur du développement-fonctions transverses du groupe BPCE et Denis JACOPINI, Expert informatique assermenté spécialisé en cybercriminalité débattent sur les techniques des cybercriminels pour vous pirater votre CB.



<http://lci.tf1.fr/france/societe/cartes-bancaires-les-fraudeurs-ont-toujours-une-longueur-d-avance-8722056.html>



Réagissez à cet article

Source : *Cartes bancaires : « Les fraudeurs ont toujours une longueur d'avance » – Société – MYTF1News*

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

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

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

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la #cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

---

Expert Informatique assermenté et formateur spécialisé en #sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.

Contactez-nous


---

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

---

**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) ?**

	<p><b>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) ?</b></p>
---	--

---



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

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

Denis Jacquot, l'organisateur professionnel qui vous a été mis à disposition d'ici jusqu'à la fin de l'année, vous décrit donc minute par minute ce qu'il faut faire 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. Ne oubliez pas votre recherche d'un poste conservé une copie et de l'utiliser contre votre ancien employeur.
2. Identifiez les données ayant un caractère confidentiel et qui nécessitent une sauvegarde dans un format protégé par un mot de passe 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 assistance.
4. Identifiez les données que vous ne devez absolument pas perdre car non remplaçables (contrats, photos de mariage, des enfants, petits-enfants.)
5. Identifiez les données que vous souhaitez rendre accessibles sur plusieurs plateformes (ordinateurs, téléphones, tablettes) que ce soit au bureau à la maison, en déplacement ou en vacances. Ensuite, en fonction des logiciels permettant d'accéder à vos données, 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 adaptés soit :

- à la confidentialité (soit support numérique utilisant un logiciel de cryptage de type TrueCrypt, PGP, ou autre) ;
- à l'intégrité (utiliser le nombre de sauvegardes en réalisant plusieurs exemplaires de vos données à l'abandon dans un lieu sûr) ;
- à la traçabilité (utiliser 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 formats et des logiciels). On peut vous garantir de pouvoir visualiser vos photos numériques dans cinquante ans ?
- à la disponibilité (sur plusieurs plateformes et plateformes liées, comme le proposent les solutions cloud qui sont d'ici il y a quelques dizaines d'années seulement) ;
- à la suppression (sur plusieurs plateformes et plateformes liées, comme le proposent les solutions cloud qui sont d'ici il y a quelques dizaines d'années seulement) ;

Le point à noter (car vous devez rapidement stocker pour ensuite l'effacer) est de choisir un support adapté en choisissant par exemple un disque dur SSD externe auto-alimenté (si le port USB de votre ordinateur l'autorise), ce support est actuellement celui avec le meilleur rapport capacité / prix avec une bonne rapidité d'écriture.

**Les risques :**

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

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

Les supports de type lecteurs ZIP, lecteurs DVD, lecteurs Blu-ray, lecteurs de bande etc. sont de plus en plus rares. Conservez des données importantes sur de tels supports pour l'avenir. Cependant, en effet, imaginez un instant pour de votre ordinateur et accéder mais que vous n'avez plus le lecteur pour les consulter et que le lecteur ne se vend même plus. Ne laissez pas la vie de vos données numériques entre les mains de son Créa.

Enfin, en fonction de tous ces paramètres, il ne vous reste plus qu'à sauvegarder vos données importantes avant de les effacer de l'appareil que vous allez rendre.

**Comment :**

Disque dur : Quelque Soit à quelconque To – Son marché, rapide mais fragile.

Clé USB : Quelque Soit – Rapide, léger mais quasiment impossible de récupérer des données en cas de panne.

Cloud : Quelque Soit à quelconque To – Accessible de n'importe où mais aussi pas tous ceux qui ont le net de passe (risqué) – Dépend du fonctionnement et de la rapidité d'Internet – Les services de cloud gratuits peuvent arriver du jour au lendemain et vous perdre tout.

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

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

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

La procédure élimine totalement les données à supprimer et celles à sauvegarder avant de procéder au nettoyage. Sur le plus grand des ordinateurs professionnels, voici les moyens de travail nous suggérons :

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

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

**Concernant les programmes ajoutés :**

Facile sur Mac et nettement le dossier d'un programme à la corbeille, n'utilisez surtout pas la corbeille pour supprimer des programmes 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 ;
- si il n'y a pas de raccourci grave 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) ;

**Concernant les e-mails :**

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

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

Le dossier contenu dans « %Local Settings%\Application Data\Identific » pour le programme InternetMail.

**Concernant nos traces de navigation :**

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

**Concernant les fichiers téléchargés :**

De 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 :**

De fait que le mot de passe de votre système d'exploitation stocke 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 bas de type « utilisateur ».

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

**Concernant les fichiers temporaires :**

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

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

**Pour finir :**

Pensez 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 déjouer les informations qui peuvent être professionnelles et être utilisées contre vous, mais personnelles permettant à un copain de les utiliser contre vous en vous demandant de l'argent contre son silence ou pour avoir le plaisir ;
- 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 vos comptes Facebook, Twitter, Dropbox... ;
- Avec vos identifiants ou en accédant à votre système de messagerie, le pirate pourra facilement appeler des commentaires ou envoyer des e-mails en utilisant votre identité.

Auteur : Denis JACQUOT

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

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

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

02  
03

Rejoignez ce site

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 réussit 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'actualité plus problématique lorsque nous voyageons : une étude Kaspersky Lab révélait récemment que 52% 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 rubrique de sécurité, Tammy de Costant, Directeur général de Kaspersky Lab France et dirige du Nord analyse les vulnérabilités des réseaux Wi-Fi dans les hôtels, une mise d'ur pour des cybercriminels en quête de données personnelles ou d'informations confidentielles.

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

De son côté, l'industrie hôtelière a pu et se transforme pour répondre aux nouvelles attentes digitales de ses clients. Alors que plus d'un quart d'entre eux annoncent qu'ils refuseront de séjourner 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 remettre les modèles existants et s'équiper, parfois en tête, 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 Tammy de Costant, Directeur général de Kaspersky Lab France et Afrique de Nord

**Le paradoxe de Wi-Fi à l'hôtel : privé mais public**

Il a été très décrié dans les médias récemment, les Wi-Fi hôtels devant 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 simple, mais elles sont à la portée de ce que l'on appelle un pirate. Les cybercriminels sont en quête permanente de victimes qui leur assurent un maximum de gains pour un minimum d'investissements techniques.

Concrètement, il suffit à un criminel de se positionner physiquement entre l'utilisateur et le point de connexion pour récupérer toutes les données qui transitent par le réseau, qu'il s'agisse d'emails, de données bancaires ou encore de notes de route de passe qui lui donneront accès à tous les comptes de l'Internet. Une approche plus sophistiquée consiste à utiliser une connexion Wi-Fi non sécurisée pour piéger un utilisateur, 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'hôtel 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'exploiter les données des dirigeants d'entreprises et digitales. Pour autant, les cybercriminels ne ciblent pas que des victimes à hauts profils. Beaucoup d'utilisateurs continuent de penser qu'ils ne courent 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 masse financière tout aussi importante pour des cybercriminels en quête de profits.

Dans certains cas, une faille Wi-Fi peut même espionner 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 la vol à grande échelle d'informations confidentielles et bancaires sur les employés. 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'échelle 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 Nasson

Denis JACOPINI est Expert Informatique et aussi formateur en Cybercriminalité (Autorisation de la Direction du travail de l'Église et de la Formation Professionnelle n°03 84 03041 04).

Nous pouvons vous aider des actions de sensibilisation 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.limemexpert.fr/formation-en-cybercriminalite-et-en-protection-des-donnees-personnelles>

Denis JACOPINI

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 attendre 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 fait 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>



---

**Comment se comporte notre**

# cerveau surchargé par le numérique



## Comment se comporte notre cerveau surchargé par le numérique

**Samedi 3 septembre, ARTE a diffusé un excellent reportage sur la manière dont notre cerveau se comporte face à nos vies de plus en plus hyper connectées : « HYPERCONNECTÉS : LE CERVEAU EN SURCHARGE ».**

Grâce aux smartphones, ordinateurs et autres tablettes, nous sommes reliés au monde en continu. Mais ce déluge d'informations menace notre bien-être.

Alliant témoignages de cadres victimes de burn out et explications de chercheurs en neurosciences, en informatique ou en sciences de l'information et de la communication, ce documentaire captivant passe en revue les dangers de cette surcharge sur le cerveau. Il explore aussi des solutions pour s'en prémunir, des méthodes de filtrage de l'information aux innovations censées adapter la technologie à nos besoins et à nos limites.

Chaque jour, cent cinquante milliards d'e-mails sont échangés dans le monde. Les SMS, les fils d'actualité et les réseaux sociaux font également partie intégrante de notre quotidien connecté, tant au bureau qu'à l'extérieur. Nous disposons ainsi de tout un attirail technologique qui permet de rester en contact avec nos amis, nos collègues, et qui sollicite sans cesse notre attention. Comment notre cerveau réagit-il face à cette avalanche permanente de données ? Existe-t-il une limite au-delà de laquelle nous ne parvenons plus à traiter les informations ? Perte de concentration, stress, épuisement mental, voire dépression... : si les outils connectés augmentent la productivité au travail, des études montrent aussi que le trop-plein numérique qui envahit nos existences tend à diminuer les capacités cognitives.

Un documentaire de Laurence Serfaty (France, 52'), diffusé sur ARTE le samedi 3 septembre à 22h20

A voir et à revoir sur Arte +7 pendant encore quelques jours !  
si vous ne voyez pas la vidéo, le lien



Réagissez à cet article

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

✕	<b>Piratage informatique : bien plus sûre que le « mot de passe », la « phrase de passe » (à condition que...)  Denis JACOPINI</b>
---	--

---

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

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

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

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

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

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

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

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

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

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

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

Article original de Denis JACOPINI et Atlantico

---

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

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

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



Réagissez à cet article

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

---

**Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur**

✕	<b>Etapes à suivre si vous comptez rendre votre ordinateur professionnel à votre employeur</b>
---	--

---

**Quelles étapes faut-il suivre avant d'effacer nos données personnelles présentes sur notre futur ancien ordinateur de fonction (sauvegarder des fichiers importants et personnelles (contacts importants, copier des fichiers et tout ce qui nous concerne (photo, pdf, CV etc...)) sur un disque dur ou un système de Cloud etc...)?**

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 hashage.
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 hashage 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 informations 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...

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

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.

---

Denis JACOPINI anime des conférences et des formations pour sensibiliser les décideurs et les utilisateurs aux CyberRisques.

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

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

<https://twitter.com/lenetexpert>

<https://www.linkedin.com/in/lenetexpert>

---



Réagissez à cet article

Original de l'article mis en page : Supprimer vos données personnelles avant de donner ou recycler un ordi – FrancoisCharron.com