

Les grands principes de la cryptologie et du chiffrement

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



Denis JACOPINI



Les grands principes de la cryptologie et du chiffrement

Historiquement, la cryptologie correspond à la science du secret, c'est-à-dire au chiffrement. Aujourd'hui, elle s'est élargie au fait de prouver qui est l'auteur d'un message et s'il a été modifié ou non, grâce aux signatures numériques et aux fonctions de hachage. À l'occasion du mois européen de la cybersécurité, la CNIL vous explique ce que c'est et à quoi ça sert.

Étymologiquement, la cryptologie est la science (λόγος) du secret (κρυπτός). Elle réunit la cryptographie (« écriture secrète ») et la cryptanalyse (étude des attaques contre les mécanismes de cryptographie).

La cryptologie ne se limite plus aujourd'hui à assurer la confidentialité des secrets. Elle s'est élargie au fait d'assurer mathématiquement d'autres notions : assurer l'authenticité d'un message (qui a envoyé ce message ?) ou encore assurer son intégrité (est-ce qu'il a été modifié ?).

Pour assurer ces usages, la cryptologie regroupe quatre principales fonctions : le hachage avec ou sans clé, la signature numérique et le chiffrement.

Pour expliquer la cryptologie, nous utiliserons dans nos exemples les personnages traditionnels en cryptographie : Alice et Bob.

Pour découvrir les grandes phases de l'histoire de la cryptologie, rendez-vous sur le webdocumentaire réalisé par l'ANSSI.

Pourquoi la cryptologie existe-t-elle ?

1.

Pour assurer l'intégrité du message : le hachage

La cryptologie permet justement de détecter si le message, ou l'information, a été involontairement modifié. Ainsi, une « fonction de hachage » permettra d'associer à un message, à un fichier ou à un répertoire, une empreinte unique calculable et vérifiable par tous. Cette empreinte est souvent matérialisée par une longue suite de chiffres et de lettres précédées du nom de l'algorithme utilisé, par exemple « SHA2 » ou « SHA256 ».

Il ne faut pas confondre le chiffrement, qui permet d'assurer la confidentialité, c'est-à-dire que seules les personnes visées peuvent y avoir accès (voir « Pour assurer la confidentialité du message »), et le hachage qui permet de garantir que le message est intègre, c'est-à-dire qu'il n'a pas été modifié.

Le hachage, pour quoi faire ?

Pour sauvegarder vos photos sur votre espace d'hébergement (de type « cloud » par exemple) et vérifier que votre téléchargement s'est bien déroulé ?

Pour synchroniser vos dossiers et détecter ceux qu'il faut sauvegarder à nouveau et ceux qui n'ont pas été modifiés ?

Il existe aussi des « fonctions de hachage à clé » qui permettent de rendre le calcul de l'empreinte différent en fonction de la clé utilisée. Avec celles-ci, pour calculer une empreinte, on utilise une clé secrète. Pour deux clés différentes l'empreinte obtenue sur un même message sera différente. Donc pour qu'Alice et Bob calculent la même empreinte, ils doivent tous les deux utiliser la même clé.

C'est parmi ces fonctions de hachage à clé que l'on trouve celles utilisées pour stocker les mots de passe de façon sécurisée.

Le hachage à clé, pour quoi faire ?

Votre service préféré reconnaît votre mot de passe quand vous vous connectez ?

Vous voulez pouvoir détecter si quelqu'un modifie des documents sans vous le dire ?

2.

Pour assurer l'authenticité du message : la signature

Au même titre que pour un document administratif ou un contrat sur support papier, le mécanisme de la « signature » – numérique – permet de vérifier qu'un message a bien été envoyé par le détenteur d'une « clé publique ». Ce procédé cryptographique permet à toute personne de s'assurer de l'identité de l'auteur d'un document et permet en plus d'assurer que celui-ci n'a pas été modifié.

La signature numérique, pour quoi faire ?

Vous voulez garantir être l'émetteur d'un courriel ?

Vous voulez vous assurer qu'une information provient d'une source sûre ?

Pour pouvoir signer, Alice doit se munir d'une paire de clés :

- l'une, dite « publique », qui peut être accessible à tous et en particulier à Bob qui est le destinataire des messages qu'envoie Alice ;
- l'autre, dite « privée », qui ne doit être connue que d'Alice.

En pratique, Alice génère sa signature avec sa clé privée qui n'est connue que d'elle. N'importe quelle personne ayant accès à la clé publique d'Alice, dont Bob, peut vérifier la signature sans échanger de secret.

3.

Pour assurer la confidentialité du message : le chiffrement

Le chiffrement d'un message permet justement de garantir que seuls l'émetteur et le(s) destinataire(s) légitime(s) d'un message en connaissent le contenu. C'est une sorte d'enveloppe scellée numérique. Une fois chiffré, faute d'avoir la clé spécifique, un message est inaccessible et illisible, que ce soit par les humains ou les machines.

Le chiffrement, pour quoi faire ?

Vous voulez vous assurer que seul le destinataire ait accès au message ?

Vous souhaitez envoyer ces informations sous enveloppe numérique et non lisible par tous comme sur une carte postale ?

Il existe deux grandes familles de chiffrement : le chiffement symétrique et le chiffement asymétrique.

Le **chiffement symétrique** permet de chiffrer et de déchiffrer un contenu avec la même clé, appelée alors la « clé secrète ». Le chiffement symétrique est particulièrement rapide mais nécessite que l'émetteur et le destinataire se mettent d'accord sur une clé secrète commune ou se la transmettent par un autre canal. Celui-ci doit être choisi avec précautions, sans quoi la clé pourrait être récupérée par les mauvaises personnes, ce qui n'assurerait plus la confidentialité du message.

Le **chiffement asymétrique** suppose que le (futur) destinataire est muni d'une paire de clés (clé privée, clé publique) et qu'il a fait en sorte que les émetteurs potentiels aient accès à sa clé publique. Dans ce cas, l'émetteur utilise la clé publique du destinataire pour chiffrer le message tandis que le destinataire utilise sa clé privée pour le déchiffrer.

Parmi ses avantages, la clé publique peut être connue de tous et publiée. Mais attention : il est nécessaire que les émetteurs aient confiance en l'origine de la clé publique, qu'ils soient sûrs qu'il s'agit bien de celle du destinataire.

Autre point fort : plus besoin de partager une même clé secrète ! Le chiffement asymétrique permet de s'en dispenser. Mais il est malheureusement plus lent.

Pour cette dernière raison, il existe une technique combinant chiffements « symétrique » et « asymétrique », mieux connue sous le nom de « **chiffement hybride** ».

Cette fois, une clé secrète est déterminée par une des deux parties souhaitant communiquer et celle-ci est envoyée chiffrée par un chiffement asymétrique. Une fois connue des deux parties, celles-ci communiquent en chiffrant symétriquement leurs échanges. Cette technique est notamment appliquée lorsque vous visitez un site dont l'adresse débute par « **https** ».

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

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

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source :
<https://www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>

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



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 sur
d'informations
: <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.



[Contactez-nous](#)

Réagissez à cet article

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

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

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

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

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

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

Contactez-nous

Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

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



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

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

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

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

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

Concernant les programmes ajoutés

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

- soit par le raccourcis de désinstallation que le programme a créé ;
- s'il n'y a pas de raccourci prévu à cet effet, passez par la fonction « Ajout et Suppression de Programmes » ou « Programmes et fonctionnalités » (ou fonction équivalente en fonction de votre système d'exploitation de sa version) ;
- Enfin, vous pouvez utiliser des programmes adaptés pour cette opération tels que Revoluninstaller (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 « » « %AppDataLocal\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 mémorisés au fil de vos consultations de sites Internet sont également stockés dans votre ordinateur, nous vous recommandons d'utiliser les fonctions dans ces mêmes navigateurs destinées à supprimer les mots de passes et les informations qui pré remplissent les champs.

Concernant les fichiers temporaires

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

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 83041 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 cybersécurité et en protection des données personnelles.

- Expertises techniques (vols, exploits, attaques, fraudes, arnaques Internet...) et judiciaires (investigation numérique, traque dark, e-mails, contenus, déblocage de clients...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybersécurité ;
- Formation de C.I.L. (Correspondants Informatique et Content) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

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

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



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 Coatpont, 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 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 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 Coatpont, 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 transitent 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 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 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 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'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 Kassouf

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, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

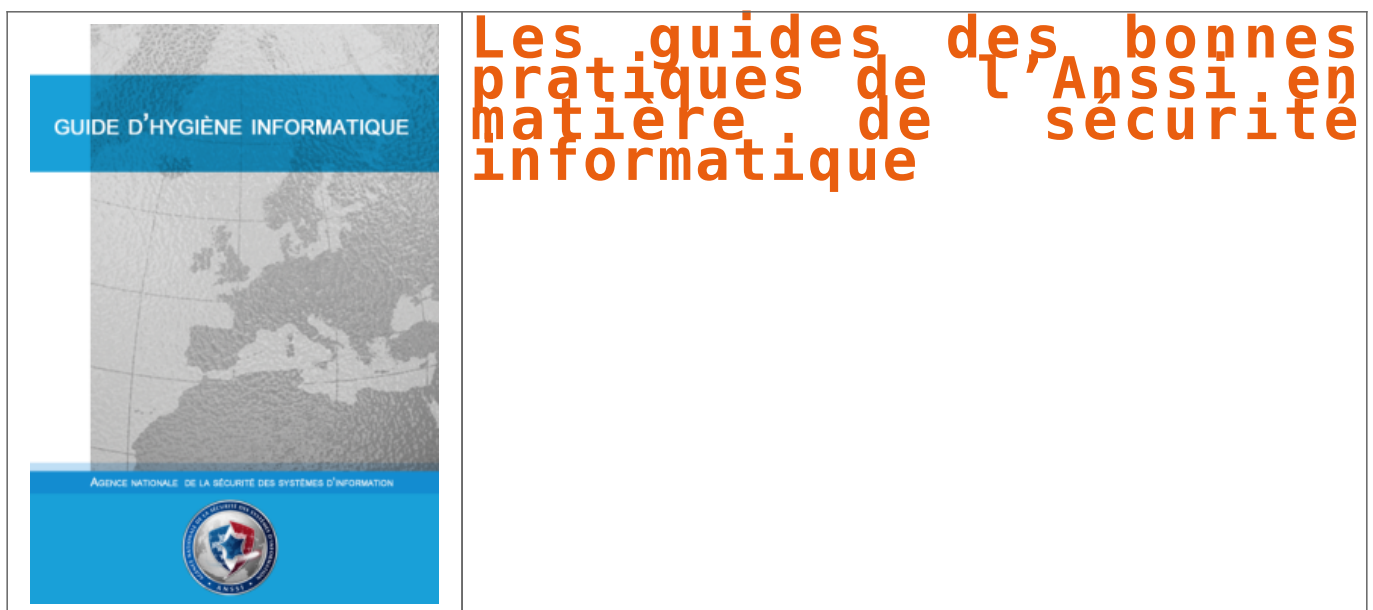


[Contactez-nous](#)

Réagissez à cet article

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

Les guides des bonnes pratiques de l'Anssi en matière de sécurité informatique | Denis JACOPINI



Vous voulez éviter que le parc informatique soit utilisé pour affaiblir votre organisation ? L'un des guides publiés par l'ANSSI vous aidera à vous protéger.

Initialement destinés aux professionnels de la sécurité informatique, les guides et recommandations de l'ANSSI constituent des bases méthodologiques utiles à tous. Vous trouverez sans peine votre chemin en utilisant les mots-clés, qu'un glossaire vous permet d'affiner, ou le menu thématique.

LISTE DES GUIDES DISPONIBLES

- Guide pour une formation sur la cybersécurité des systèmes industriels
- Profils de protection pour les systèmes industriels
- Sécuriser l'administration des systèmes d'information
- Achat de produits de sécurité et de services de confiance qualifiés dans le cadre du rgs
- Recommandations pour le déploiement sécurisé du navigateur mozilla firefox sous windows
- Cryptographie – les règles du rgs
- Recommandations de sécurité concernant l'analyse des flux https
- Partir en mission avec son téléphone sa tablette ou son ordinateur portable
- Recommandations de sécurité relatives à active directory
- Recommandations pour le déploiement sécurisé du navigateur microsoft internet explorer
- l'homologation de sécurité en neuf étapes simples,
- bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine,
- recommandations pour le déploiement sécurisé du navigateur google chrome sous windows,
- usage sécurisé d'(open)ssh,
- la cybersécurité des systèmes industriels,
- sécuriser une architecture de téléphonie sur ip,
- mettre en œuvre une politique de restrictions logicielles sous windows,
- prérequis à la mise en œuvre d'un système de journalisation,
- vulnérabilités 0-day, prévention et bonnes pratiques,
- le guide des bonnes pratiques de configuration de bgp,
- sécuriser son ordiphone,
- sécuriser un site web,
- sécuriser un environnement d'exécution java sous windows,
- définition d'une politique de pare-feu,
- sécuriser les accès wi-fi,
- sécuriser vos dispositifs de vidéoprotection,
- guide d'hygiène informatique,
- la sécurité des technologies sans contact pour le contrôle des accès physiques,
- recommandations de sécurité relatives à ipsec,
- la télé-assistance sécurisée,
- sécurité des systèmes de virtualisation,
- sécurité des mots de passe,
- définition d'une architecture de passerelle d'interconnexion sécurisée,
- ebios – expression des besoins et identification des objectifs de sécurité,
- la défense en profondeur appliquée aux systèmes d'information,
- externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques,
- archivage électronique... comment le sécuriser ?
- pssi – guide d'élaboration de politiques de sécurité des systèmes d'information,
- tdbssi – guide d'élaboration de tableaux de bord de sécurité des systèmes d'information,
- guide relatif à la maturité ssi,
- gissip – guide d'intégration de la sécurité des systèmes d'information dans les projets

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

Contactez-nous

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.ssi.gouv.fr/entreprise/bonnes-pratiques/>

Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits | Denis JACOPINI



Wi-Fi
Attention
au
piratage
sur les
vrais et
faux
réseaux
gratuits

Ce sont les vacances mais nombre de touristes ne se séparent pas de leurs smartphones, tablettes ou ordinateurs portables. Et pour se connecter à l'internet, quoi de mieux qu'attraper un wi-fi gratuit. Une pratique qui peut se révéler très dangereuse. Des proies faciles pour les « sniffeurs » de données. Explications de Laurent Heslault, expert sécurité chez Symantec.

Vous êtes sur votre lieu de vacances et vous avez envie de vous connecter à l'internet. Pour consulter votre messagerie ou vos réseaux sociaux, envoyer des photos à vos proches, surfer sur le net ou consulter votre compte en banque ou faire une réservation.

Solution la plus simple : se connecter à un réseau Wi-Fi gratuit. Dans votre hôtel, camping, à la terrasse d'un café ou d'un restaurant... Les accès gratuits pullulent et se généralisent.

Expert en sécurité à Symantec, Laurent Heslault tire le signal d'alarme. « Rien de plus simple que de pirater les données qui transitent sur un réseau Wi-Fi gratuit » assure-t-il. « Par exemple, je m'installe à la terrasse d'un café et je crée un vrai faux point d'accès gratuit en empruntant le nom du café. Des gens vont s'y connecter et je n'ai plus qu'à récupérer toutes les données qui m'intéressent. Des mots de passe, des identifiants... »

Des sniffeurs de données

Il exagère ? Non. « L'expérience a été faite à la terrasse d'un café. Nous avons installé un logiciel qui permet de sniffer tous les appareils qui se branchaient sur le Wi-Fi. Ensuite, des complices, qui se faisaient passer pour des magiciens, allaient voir les gens en disant que par magie, ils avaient réussi à changer le code de leur téléphone ou leur image sur Facebook. Ils étaient étonnés ! » Rien de magique mais des logiciels de piratage qui se trouvent facilement sur le net.

Les données sur le Wi-Fi ne sont pas chiffrées

« Les données qui transitent sur le Wi-Fi ne sont pas chiffrées. Sauf quand vous vous connectés à un site sécurisé avec le protocole HTTPS. Donc ce sont des données faciles à intercepter. » Danger sur les vrais faux points d'accès Wi-Fi mais aussi sur les vrais qui ne sont, dans la grande majorité des cas, pas chiffrés non plus. « Par contre pas de problème pour une connexion 3G ou 4G qui sont chiffrées. Mais pour économiser leur forfait, les gens préfèrent se connecter au Wi-Fi ».

Conseils

Alors quels conseils ? « Ne jamais, sur un Wi-Fi public, entrer un mot de passe. D'autant que la plupart des internautes utilisent le même mot de passe pour tous leurs sites. » En clair, limiter les dégâts en ne consultant que des sites qui ne demandent aucune identification.

Autre solution : protéger son smartphone ou sa tablette en y installent un logiciel qui va chiffrer toutes les données qui vont en sortir. Plusieurs types de logiciels existent dont le Wi-Fi Privacy de Norton qui est gratuit pendant 7 jours et peut s'installer sur des périphériques fonctionnant sous Ios et Android.

Article original de Samuel NOHRA.

Nous prodiguons une multitude d'autres conseils durant les formations que nous animons à destination des élus, chef d'entreprises, agents publics et salariés. [Consultez la liste de nos formations]



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Wi-Fi. Attention au piratage sur les vrais et faux réseaux gratuits

Bonnes pratiques face à une tentative de cyber-extorsion

| Denis JACOPINI



Bonnes pratiques
face à une
tentative de
cyber-extorsion

Bonnes pratiques face à une tentative de cyber-extorsion

1. Typologie des différents cas de cyber-extorsion

Le type le plus répandu de cyber-extorsion est l'attaque par crypto-ransomware. Ce dernier est une forme de malware qui chiffre les fichiers présents sur la machine infectée. Une rançon est par la suite demandée afin d'obtenir la clef qui permet de déchiffrer les données compromises. Ces attaques touchent autant les particuliers que les acteurs du monde professionnel. Il existe cependant deux autres types de cyber-extorsion auxquels doivent faire face les sociétés.

Le premier cas est celui du chantage faisant suite à un vol de données internes. L'exemple le plus marquant de ces derniers mois est celui du groupe Rex Mundi : ce dernier dérobe des informations sensibles/confidentielles – comme une base clientèle – puis demande une rançon à sa victime sous peine de divulguer son butin et par conséquent de rendre public l'acte de piratage; ce qui peut être fortement compromettant pour la société ciblée comme pour sa clientèle. De nombreuses entreprises comme Dexia, Xperthis, Voo ou encore Labio ont été victimes des chantages du groupe Rex Mundi.

La deuxième pratique est celle du DDoS contre rançon, spécialité des pirates d'Armada Collective. Le modus operandi est simple et efficace : la cible reçoit un email l'invitant à payer une rançon en Bitcoin afin de ne pas se voir infliger une puissante attaque DDoS qui rendrait son site web indisponible à ses utilisateurs. La plupart des victimes sont des sociétés de taille intermédiaire dont le modèle économique est basé sur le principe de la vente en ligne – produits ou services – comme le fournisseur suisse de services de messagerie ProtonMail en novembre 2015.

2. Bonnes pratiques à mettre en place

En amont de la tentative de cyber-extorsion

Un ensemble de bonnes pratiques permet d'éviter qu'une attaque par ransomware se finalise par une demande de rançon.

Il convient de mettre en place une stratégie de sauvegarde – et de restauration – régulière des données. Ces back-ups doivent être séparés du réseau traditionnel des utilisateurs afin d'éviter d'être chiffrés en cas de déploiement d'un crypto-ransomware. Dans ce cas de figure, le système pourra être restauré sans avoir besoin de payer la rançon exigée.

La propagation d'un malware peut également être évitée par l'installation d'outils/solutions de cybersécurité notamment au niveau du client, du webmail et du système d'exploitation (antivirus). Ceci doit obligatoirement être couplé à une mise à jour régulière du système d'exploitation et de l'ensemble des logiciels installés sur le parc informatique.

L'être humain étant toujours le principal maillon faible de la chaîne, il est primordial de sensibiliser les collaborateurs afin qu'ils adoptent des comportements non-risqués. Par exemple : ne pas cliquer sur les liens et ne pas ouvrir les pièces-jointes provenant d'expéditeurs inconnus, ne jamais renseigner ses coordonnées personnelles ou bancaires à des opérateurs d'apparence légitimes (banques, fournisseurs d'accès Internet, services des impôts, etc.).

Ces bonnes pratiques s'appliquent également dans le cas d'un chantage faisant suite à un vol de données internes. Ces dernières sont en général dérobées via l'envoi dans un premier temps d'un spam contenant une pièce jointe malicieuse ou une URL redirigeant vers un site web compromis. Une fois le système d'information compromis, un malware est déployé afin de voler les informations ciblées.

La menace provient également de l'intérieur : un employé mal intentionné peut aussi mettre en place une tentative de cyber-extorsion en menaçant de divulguer des informations sensibles/confidentielles. Ainsi, il est important de gérer les accès par une hiérarchisation des droits et un cloisonnement.

Pendant la tentative de cyber-extorsion

Lors d'un chantage faisant suite à un vol de données internes, il est important de se renseigner sur la véracité des informations qui ont été dérobées. Certains groupes de pirates se spécialisent dans des tentatives de cyber-extorsion basées sur de fausses informations et abusent de la crédulité de leurs victimes. Il en va de même concernant l'origine du corbeau : de nombreux usurpateurs imitent le style du groupe Armada Collective et envoient massivement des emails de chantage à des TPE/PME. Ces dernières cèdent fréquemment à ces attaques qui ne sont pourtant que des canulars.

Il est vivement recommandé de ne jamais payer une rançon car le paiement ne constitue pas une garantie. De nombreuses victimes sont amenées à payer une somme bien plus conséquente que la rançon initialement demandée. Il n'est pas rare de constater que les échanges débutent de manière très cordiale afin de mettre la cible en confiance. Si cette dernière cède au premier chantage, l'attaquant n'hésite pas à profiter de sa faiblesse afin de lui soutirer le plus d'argent possible. Il abuse de techniques basées sur l'ingénierie sociale afin d'augmenter ses profits. Ainsi, l'escroc gentil n'existe pas et le paiement de la rançon ne fait que l'encourager dans sa démarche frauduleuse.

De nombreuses victimes refusent de porter plainte et cela pour plusieurs raisons. Elles estiment à tort que c'est une perte de temps et refusent également de communiquer sur les résultats et conséquences d'une attaque qui ne feraient que nuire à leur image auprès des clients, fournisseurs ou partenaires. Pourtant cette mauvaise stratégie ne fait que renforcer le sentiment d'impunité des attaquants, les confortent dans le choix de leurs modes opératoires et leur permet de continuer leurs actions malveillantes. Il est ainsi vital de porter plainte lors de chaque tentative de cyber-extorsion. L'aide de personnes qualifiées permet de faciliter ce genre de démarches.

En cas d'attaque avérée, il est essentiel pour la victime de s'appuyer sur un panel de professionnels habitués à gérer ce type de situation. La mise en place d'une politique de sauvegarde ou bien la restauration d'un parc informatique n'est pas à la portée de toutes les TPE/PME. Il est nécessaire de faire appel à des prestataires spécialisés dans la réalisation de ces opérations complexes.

Par ailleurs, en cas de publication de la part de l'attaquant de données sensibles/confidentielles, il convient de mettre en place un plan de gestion de crise. La communication est un élément central dans ce cas de figure et nécessite l'aide de spécialistes.

Article original de Adrien Petit



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Bonnes pratiques face à une tentative de cyber-extorsion [Par Adrien Petit, CEIS] | Observatoire FIC

Formation en cybercriminalité : Virus, arnaques et piratages informatiques, Solutions pour nos entreprises

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
 <p>LE NET EXPERT AUDITS & EXPERTISES</p>	 <p>LE NET EXPERT EXPERTISES DE SYSTEMES DE VOTES ELECTRONIQUES</p>	 <p>LE NET EXPERT MISES EN CONFORMITE</p>	 <p>SPY DETECTION Services de detection de logiciels espions</p>	 <p>LE NET EXPERT FORMATIONS</p>	 <p>LE NET EXPERT ARNAQUES & PIRATAGES</p>
<p>Denis JACOPINI</p>  <p>vous informe</p>		<p>Formation en cybercriminalité : Virus et arnaques et piratages informatiques, Solutions pour nos entreprises</p>			

Présentation

Le contexte de l'Internet et l'ampleur du phénomène de la cybercriminalité, nous poussent à modifier nos comportements au quotidien.

Avons-nous raison d'avoir peur ? De quoi doit-on avoir peur ? Comment se protéger ?

Les réponses évidentes sont techniques, mais il n'en est pas moins vrai que des règles de bonnes pratiques et des attitudes responsables seront les clés permettant d'enrayer le phénomène...

Objectif

Découvrez les règles de bonnes pratiques et des attitudes responsables qui sont les clés permettant d'enrayer ce phénomène.

Durée

1 journée

ou conférence de 2 heures.

Public concerné

Chefs d'entreprise, présidents d'associations, élus, décideurs, employés, agents, ...

Moyens pédagogiques

Vidéo projecteur et sonorisation souhaitée selon la taille de la salle.

Animateur

Denis JACOPINI

Expert Judiciaire en Informatique diplômé en Cybercriminalité, Droit, Sécurité de l'information, informatique Légale et en Droit de l'Expertise Judiciaire. Spécialisé en Protection des données personnelles et certifié ISO 27005, il a été pendant une vingtaine d'année à la tête d'une société spécialisée en sécurité Informatique.

Son métier : Aider les professionnels à se protéger des pirates informatiques, et à se mettre en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles.

Il intervient dans la France entière et à l'étranger pour former ou sensibiliser les décideurs, informaticiens et utilisateurs sur les techniques utilisées par les Pirates informatiques pour piéger leurs victimes et sur les obligations en matière de protection des données à caractère personnel.

Différentes interventions pour :

- Le **Conseil de l'Europe** ;
- Un **Centre d'Enseignement et de Recherche en Informatique** ;
- Le **Centre d'Etudes des Techniques Financières** et d'Ingénierie d'Aix en Provence ;
- Des **écoles d'avocats** ;
- Des **Compagnies d'Experts Judiciaires** ;
- De nombreux clubs ou associations de chefs d'entreprises dans la **France entière et à l'étranger** ;
- Le **Centre National de la Fonction Publique Territoriale (CNFPT)** pour des élus, des S.G. et des agents publics.

(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle – Numéro formateur : 93 84 03041 84)

Plus d'informations sur

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

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

[Les 10 conseils pour ne pas se faire «hacker» pendant l'été](#)

[Les meilleurs conseils pour choisir vos mots de passe](#)

[Victime d'un piratage informatique, quelles sont les bonnes pratiques ?](#)

[Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?](#)

[Attaques informatiques : comment les repérer ?](#)

[block id="24760" title="Pied de page BAS"]

DU en Investigation Numérique Pénale – Denis JACOPINI témoigne

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer



DU en
Investigation
Numérique Pénale
– Denis JACOPINI
témoigne

Vous souhaitez connaître le droit, les éléments théoriques ainsi que les outils liés au métier d'investigateur numérique en matière pénale ? Cette formation de 130 heures qui débouche sur le premier Diplôme Universitaire en Investigation Numérique Pénale de France est faite pour vous. Attention, les places sont limitées.

Contenu de la formation :

- Acquisition des bases et des fondamentaux en matière informatique dans le cadre d'une expertise pénale ;
- Connaissance de la Procédure pénale ;
- Connaissance des missions, de l'organisation professionnelle et des bonnes pratiques d'un enquêteur numérique ;
- Acquisition des méthodes et pratiques d'extraction de données post mortem :
- *Extraction de données à partir de supports physiques*
- *Extraction de données à partir de terminaux mobiles*
- *Extraction de traces internet*
- *Manipulation d'objets multimédia*
- Acquisition des méthodes de fouille de données



2019 06 14 Plaquette INPA5 v12

Cette formation est réalisée en partenariat avec :

- UFIN (Union Française de l'Investigation Numérique)
- CNEJITA (Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées)
- AFSIN (Association Francophone des Spécialistes de l'Investigation Numérique)
- Gendarmerie nationale



Denis JACOPINI, Expert de Justice en Informatique spécialisé en Cybercriminalité et en Protection des Données Personnelles (RGPD) témoigne :

C'est avec grand plaisir que je vous témoigne ma grande satisfaction à l'issue de cette formation. Même si j'avais déjà une expérience en tant qu'Expert de Justice en Informatique, étalée sur 8 mois, le contenu de cette formation m'a permis d'être désormais mieux équipé (mentalement, organisationnellement et techniquement) et en plus grande confiance pour les futures expertises pénales qui me seront confiées.

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

Quelques articles sélectionnés par notre Expert qui pourraient aussi vous intéresser :

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

Les meilleurs conseils pour choisir vos mots de passe

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

Victime d'usurpation d'identité sur facebook, tweeter ? Portez plainte mais d'après quel article de loi ?

Attaques informatiques : comment les repérer ?

[block id="24760" title="Pied de page BAS"]

Source : *Diplôme d'Université : Investigation Numérique Pénale*
– Ametys