

Quelles sont les messageries qui protègent le mieux vos données personnelles ?



Apple, Google, Snapchat, BlackBerry, ou encore le Chinois Tencent, tous ces géants du web proposent à leurs utilisateurs des messageries instantanées. Aujourd’hui, ce sont plusieurs milliards de personnes qui les utilisent quotidiennement. Au sein de ceux-là, des minorités opprimées, des militants pour les droits de l’Homme, des dissidents politiques, des lanceurs d’alertes... Mais comment ces messageries protègent-elles nos données ?

Amnesty International a rendu un rapport accablant sur la question, dans lequel elle effectue un classement des messageries privées.

Classement des messageries privées

Quelle messagerie privée est la plus sécurisée selon le classement d’Amnesty International ?

Entreprises ▼	Messageries	Siège	Nombre d'utilisateurs	Classement Amnesty (sur 100)
Apple	iMessage, Facetime	USA	Inconnu, mais 1 milliard d'iPhone vendus	67
Blackberry	Blackberry Messenger	Canada	100 millions	20
Facebook	Facebook Messenger, WhatsApp	USA	1 milliard chacune	73
Google	Allo, Duo, Hangouts	USA	Inconnu, mais plus de deux milliards d'utilisateurs Google	53
Kakao Inc	Kakao Talk	Corée du Sud	49 millions	40
Line	Line	Japon	218 millions	47
Microsoft	Skype	USA	300 millions	40
Snapchat	Snapchat	USA	200 millions	26
Telegram	Telegram Messenger	Allemagne	100 millions	67
Tencent	QQ, We Chat	Chine	697 millions, 853 millions	0
Viber media	Viber	Luxembourg	250 millions	47

Source: Amnesty Internationale [Récupérez les données](#) Créé avec [Datawrapper](#).

Classement Amnesty International

Les onze grandes entreprises évaluées affichent toutes des engagements écrits en termes de protection de la vie privée. Et pourtant, aucune n’est irréprochable, toutes ne respectent pas les normes internationales en vigueur et peu proposent un niveau élémentaire de protection. Facebook, Apple ou Google sont en haut du classement, quand Microsoft, Snapchat, ou Tencent font figure de mauvais élèves. L’ONG a mis au point un barème.

Les critères du classement

Amnesty International attribue une note de 0 à 100 aux entreprises, selon leur résultat sur cinq critères provenant des normes internationales en la matière. Trois sont primordiaux pour assurer la sécurité des données personnelles.

Les entreprises sont jugées sur leur capacité à reconnaître les menaces contre la vie privée et la liberté d’expression. En clair, que mettent-elles en place pour protéger les droits de leurs utilisateurs ?

Elles doivent ensuite appliquer par défaut le chiffrement de bout en bout. Une question au cœur des préoccupations d’Amnesty International. L’ONG estime que seul le chiffrement de bout en bout est apte à protéger la vie privée. Ici, seul l’émetteur et le receveur détiennent la clef de chiffrement. Les acteurs intermédiaires du processus (fournisseur d’accès, entreprise de messagerie) n’ont donc pas accès au contenu de la conversation.

Les messageries doivent enfin rendre publiques les informations sur les demandes de données d’utilisateurs par des gouvernements et refuser de contourner les clefs de chiffrements.

Facebook, Apple, Telegram et Google en tête

La messagerie de Facebook est la mieux classée, avec un score de 73 points. Le bébé de Mark Zuckerberg totalise environ un milliard de fidèles quotidiens. C’est lui qui offre le plus de garanties à ses utilisateurs. Mais ses deux messageries ne sont pas équivalentes. Si WhatsApp propose un chiffrement de bout en bout par défaut (l’utilisateur n’a pas à choisir, c’est automatique), cette option récente de Facebook Messenger doit être activée.

Apple cumule 67 points. La marque à la pomme offre un chiffrement de bout en bout sur ses deux messageries (iMessenger et Facetime). Mais Amnesty International relève qu’elle « devrait adopter un protocole de chiffrement plus ouvert qui permette une vérification indépendante complète ».

Telegram est deuxième ex aequo, avec 67 points aussi. Ce nom vous dit quelque chose ? C’est normal, cette messagerie a beaucoup defrayé la chronique car elle est l’application de messagerie instantanée la plus prisée des milieux djihadistes. Elle perd des points car son système de chiffrement n’est pas automatique et doit être activé.

Vient ensuite Google avec un score de 53. Le moteur de recherche est critiqué par Amnesty International car ses trois messageries instantanées ne proposent pas toutes des systèmes de chiffrement.

Les quatre entreprises qui caracolent en tête se sont toutes publiquement prononcées contre les moyens de contournement des clés de chiffrement par les États. Et toutes, à l’exception de Telegram, préviennent leurs utilisateurs des demandes faites par les gouvernements.

Skype, Snapchat et Tencent, les mauvais élèves

Snapchat, c’est cette messagerie qui permet de s’envoyer une photo ou un texte sur un temps très court. Skype, propriété de Microsoft, c’est celle qui vous permet de faire des appels vidéo. Les deux applications sont mauvaises élèves aux quatrième et troisième plus mauvaises places.

Aucun chiffrement de bout à bout n’est proposé par les deux géants, qui présentent tous deux un système « très vulnérable », selon Amnesty. Les deux sont utilisées par des millions de jeunes quotidiennement, un public très menacé et très exposé à la cybercriminalité.

BlackBerry occupe l’avant-dernière place. La messagerie privée canadienne n’offre pas un système de chiffrement de bout en bout, elle le vend. Ainsi, si on ne paie pas, on n’est pas protégé sur BlackBerry. Qui plus est, d’après le site américain Vice, BlackBerry aurait donné sa clef de chiffrement à la police canadienne qui a alors pu intercepter des messages.

À la dernière place, on retrouve Tencent, le mastodonte chinois. L’entreprise accuse un score de 0 point. Aucun des critères n’est rempli et les données personnelles de plus d’un milliard et demi de personnes ne sont absolument pas protégées, conséquence de la censure que subit l’Internet chinois. En 2013, un développeur de Tencent confiait au journal *Le Monde* , « Les autorités ont le privilège d’accéder aux historiques, donc elles savent tout sur vous dès lors que vous utilisez nos services. » Le ton est donné…[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l’Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l’étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d’un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

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



Le Net Expert
INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Quelles sont les messageries qui protègent le mieux vos données personnelles ?
– La Voix du Nord

Que prévoit la loi pour les Hackers éthiques ?



Que
prévoit
la loi
pour les
Hackers
éthiques
?

La loi pour une République numérique protège les hackers éthiques et confirme le rôle central de l'Anssi dans le signalement de failles informatiques. Les explications de l'avocat François Coupez.

En complétant le code de la défense, la loi du 7 octobre 2016 pour une République numérique entérine la protection des hackers éthiques. En tout cas ceux qui signalent une faille informatique découverte par leurs soins à l'Agence nationale pour la sécurité des systèmes d'information (Anssi). La législation confirme ainsi le rôle central de cette dernière dans le signalement des vulnérabilités.

« Ce texte va surtout permettre une officialisation », explique à *Silicon.fr* François Coupez, avocat associé du cabinet Atipic. « L'Anssi apparaît bien comme le second point de contact officiel, en plus du responsable du système d'information objet des vulnérabilités ». Ce point de contact « est utile pour les cas où les 'hackers éthiques' supposeraient qu'ils ne peuvent joindre directement l'entité dont le SI est vulnérable, quelle qu'en soit la raison : responsable supposé peu réceptif, responsable déjà contacté en vain, etc. ».

Protéger le hacker dit « éthique »

Pour distinguer le hacker éthique du pirate (l'article 323-1 du code pénal sanctionne le piratage frauduleux d'au moins deux ans d'emprisonnement et de 60 000 euros d'amende), l'article 47 de la loi numérique complète le code de la défense par un article L2321-4 ainsi rédigé :

« Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données.

L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée.

L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

Sécuriser les agents de l'Anssi

Rappelons que l'article 40 du code pénal cité dans cet article L2321-4 indique : « Toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs. »

Or, dans la loi portée par Axelle Lemaire, cette obligation prévue à l'article 40 ne s'applique pas aux *white hats*. Ce qui arrivait déjà, en fait, avant la promulgation du texte. « D'après ce qu'a pu indiquer à certaines occasions l'Anssi elle-même, la pratique interne était déjà de ne pas appliquer l'article 40 dans les hypothèses similaires à celles visées par cet article L2321-4 du code de la défense nouvellement créé. Et ce afin de faciliter les remontées d'informations. Ce que la loi République numérique légitime dorénavant via cet article, et c'est une très bonne chose pour la sécurité juridique des agents de l'Anssi », ajoute François Coupez...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Original de l'article mis en page : Hacker éthique : la législation française enfin claire ?

Cash investigation ne comprend rien à la cybersécurité



Cash
investigation
ne comprend
rien à la
cybersécurité

La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que Cash Investigation a tenté de montrer.

La cybersécurité est un sujet suffisamment sensible pour qu'il mérite d'être traité par les journalistes avec rigueur et sérieux. En la matière, l'approximation et la sous-estimation de sa complexité conduisent inévitablement à des contre-vérités médiatiques et à des biais de représentation. C'est précisément ce que l'émission de France 2 Cash Investigation Marchés publics : le grand dérapage nous a fourni le mardi 18 octobre à 20h55, tant les approximations et les contre-vérités se succédaient à grande vitesse tout au long du reportage sur le système d'exploitation des ordinateurs du Ministère de la Défense.

Je dois avouer qu'il en faut en général beaucoup pour me choquer mais que ce beaucoup a été très vite atteint par l'équipe de Cash Investigation ! Jamais réalité n'avait été à ce point tordue et déformée dans l'unique but d'entrer par le goulot étroit du format préfabriqué de la désinformation. En clair, on a voulu se payer les balourds du Ministère de la Défense et les militaires qui ont choisi le système d'exploitation Windows (Microsoft) pour équiper leurs machines...

Un piratage en trois clics ?

Pensez donc, Madame, en trois clics et deux failles de sécurité, Élise Lucet nous démontrait qu'elle pouvait prendre le contrôle des ordinateurs du Ministère de la Défense pour déclencher dans la foulée la troisième guerre mondiale... Il est vrai qu'elle venait de pirater sans pression l'ordinateur de l'un de ses collègues, avec l'aide de deux experts en cybersécurité de l'ESIEA. Et comme chacun le sait, si l'opération fonctionne avec la machine Windows de madame Michu, ça marchera tout pareil avec les machines de la Grande Muette.

Dans le cadre d'un renouvellement de contrat, Microsoft a remporté en 2013 le marché public du Ministère de la Défense concernant l'équipement en systèmes d'exploitations du parc informatique des Armées. Windows est donc installé sur 200 000 ordinateurs de l'armée française.

Partant de cette réalité, Élise Lucet et son équipe en ont déduit que cela constituait un choix risqué en matière de cybersécurité & cyberdéfense tant ce système d'exploitation est truffé de vulnérabilités et de Back Doors (portes dérobées) installées par les méchants espions américains de la NSA.

Le « piège » de Microsoft

En conclusion, toujours selon Élise Lucet, les militaires français sont tombés dans le piège tendu par Microsoft qui dispose désormais de toutes les entrées possibles pour la prise de contrôle à distance des ordinateurs sensibles du Ministère et de leurs secrets Défense. La théorie du complot n'est pas très éloignée dans tout cela, surtout lorsque l'hypothèse d'Élise Lucet se trouve plus ou moins confirmée par les déclarations de l'expert cryptologue Éric Filiol, retraité des services de renseignement et actuellement directeur du centre de recherche en cybersécurité de l'ESIEA.

Ce que dit Éric Filiol durant ses courtes interventions n'est pas contestable : il effectue une démonstration de prise de contrôle à distance d'un ordinateur équipé du système Windows 7 à la suite d'un clic de l'utilisateur (la cible) sur un lien malveillant transmis par mail. La démonstration qu'il donne d'une prise de contrôle n'appelle aucune critique puisqu'elle est un classique du genre, connue de tous les étudiants préparant un Master en cybersécurité.

Quelle preuve des failles de sécurité ?

C'est l'usage qui en est fait qui devient très contestable : puisque la manipulation fonctionne sur l'ordinateur doté de Windows de mon collègue journaliste (qui, au demeurant, a le clic facile et l'antivirus laxiste), c'est qu'elle fonctionne également avec l'ensemble du parc informatique relevant du Ministère de la Défense (cqfd). Preuve est donc faite de l'incompétence des services de l'État, de services chargés de la cybersécurité des infrastructures militaires et de l'ensemble des experts, ingénieurs et chercheurs qui œuvrent chaque jour en France pour sécuriser les systèmes...

Le reportage pousse encore un peu plus loin sa courageuse investigation en allant interroger très brièvement l'Officier Général Cyberdéfense, le vice Amiral Coustillière. Ce dernier est interrogé entre deux portes sur le choix improbable d'installer Windows sur des machines qui font la guerre.

White Hat au grand cœur

N'écoutez que leur sagacité et leur expertise autoproclamée, nos journalistes hackers « White Hat » au grand cœur (donc toujours du bon côté de la Force) donnent pour finir une leçon de cyberstratégie à l'Amiral responsable de la sécurité des infrastructures numériques militaires, tout en le faisant passer pour un amateur déconnecté des réalités informatiques... C'est à ce point que l'on touche au paroxysme de la désinformation du spectateur que l'on considère comme un consommateur compulsif de dysfonctionnements et malversations étatiques...

Et bien non, Madame Lucet, non, le choix de Windows n'est pas plus ou moins défendable que celui d'un système open source. Linux et ses dérivés souffrent également de vulnérabilités, subissent des attaques et des correctifs. C'est le triste destin de tout système complexe que d'avoir été créé imparfait, ouvert aux agressions extérieures exploitées par des individus mal intentionnés ou en quête d'information.

On ne clique pas tous sur les malware

Non, Madame Lucet, ce n'est pas parce qu'un de vos collègues journalistes clique facilement sur un lien malveillant que tout le monde le fait. Ce n'est pas parce que son antivirus ne détecte pas un malware qu'aucun autre antivirus ne le détectera. Ce n'est pas parce que Windows possède des vulnérabilités que les autres systèmes d'exploitation n'en possèdent pas.

Ce n'est pas parce que Microsoft a pu transmettre ou vendre certaines données aux services gouvernementaux américains que cette firme cherche obsessionnellement à piéger l'armée française. Enfin, non chère Élise, l'armée française ne découvre pas les problématiques de sécurité numérique avec votre reportage et ne sous-estime pas les risques de vol de données sensibles. C'est quelque part faire injure aux spécialistes civils et militaires qui œuvrent quotidiennement à la défense des intérêts numériques de la nation.

La cybersécurité est une science complexe qui croise les compétences techniques et la compréhension des mécanismes humains. L'art de la guerre numérique dépasse de très loin ce que ce triste reportage a tenté de montrer.

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contenus, 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 : Cash investigation ne comprend rien à la cybersécurité | Contrepoints

Quelques détails sur la cyberattaque massive dont ont été victime les états unis

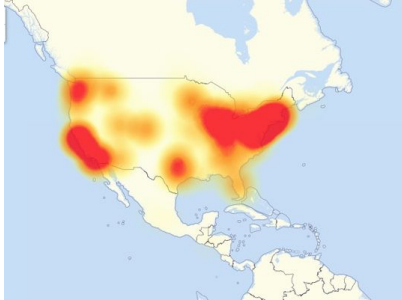


Quelques
détails sur
la cyberattaque
massive dont
ont été victime
les états unis

Pendant plusieurs heures, une vaste attaque informatique a paralysé de nombreux sites internet outre-Atlantique, vendredi 21 octobre.

En se réveillant vendredi 21 octobre, plusieurs millions d'Américains ont la désagréable surprise de se voir refuser l'accès à leurs sites préférés. Pendant de longues heures, impossible en effet de se connecter à **Twitter**, **Spotify**, **Amazon** ou **eBay**. Mais aussi à des grands médias, tels que le *New York Times*, **CNN**, le *Boston Globe*, le *Financial Times* ou encore le célèbre quotidien anglais *The Guardian*. En cause : une **cyberattaque massive** menée en plusieurs vagues qui a fortement perturbé le fonctionnement d'internet outre-Atlantique.

Le fait que tous ces sites mondialement connus soient hors d'accès ne révèle toutefois que la partie émergée de l'iceberg. En effet, les pirates **s'en sont pris en réalité à la société Dyn**, dont la notoriété auprès du grand public est beaucoup plus faible. Le rôle de la firme est de **rediriger les flux internet vers les hébergeurs** et traduit en quelque sorte des noms de sites en adresse IP. À 22h17, Dyn a indiqué que l'incident était résolu.



Le département de la sécurité intérieure (DHS) ainsi que le FBI ont annoncé dans la foulée **l'ouverture d'une enquête** « sur toutes les causes potentielles » de ce gigantesque piratage à l'envergure inédite. Des investigations qui s'annoncent de longue haleine, tant cette attaque se déplaçant de la côte est vers l'ouest du pays semble sophistiquée. « **C'est une attaque très élaborée**. À chaque fois que nous la neutralisons, ils s'adaptent », a expliqué Kyle Owen, un responsable de Dyn, cité sur le site spécialisé *Techcrunch*.

Qui est à l'origine de l'attaque ?

Pour l'heure, l'identité et l'origine des auteurs demeurent inconnues. Mais l'ampleur du piratage éveille les soupçons. « Quand je vois une telle attaque, je me dis que c'est un État qui est derrière », a estimé Eric o'Neill, chargé de la stratégie pour la société de sécurité informatique Carbon Black et ex-chargé de la lutte contre l'espionnage au FBI. Les regards se tournent inévitablement vers des pays comme la Russie ou la Chine, qui pourraient avoir intérêt à déstabiliser le géant américain, alors que les élections approchent.

Mais d'autres hypothèses circulent. Le site Wikileaks, qui a publié des milliers d'emails du directeur de campagne de la candidate démocrate à la présidentielle Hillary Clinton, a cru déceler dans cette attaque une marque de soutien à son fondateur Julian Assange, réfugié dans l'ambassade d'Équateur à Londres et dont l'accès à internet a été récemment coupé. « Julian Assange est toujours en vie et Wikileaks continue de publier. Nous demandons à nos soutiens d'arrêter de bloquer l'internet américain. Vous avez été entendus », a tweeté le site.

Comment les pirates ont-ils procédé ?

La technique utilisée vendredi pour plonger le web américain dans le chaos est dite de déni de service distribué (DDoS). Cette dernière consiste à rendre un serveur indisponible en le surchargeant de requêtes. Elle est souvent menée à partir d'un réseau de machines zombies – des « botnets » – elles-mêmes piratées et utilisées à l'insu de leurs propriétaires. En l'occurrence, les pirates ont hacké des objets connectés, tels que des smartphones, machines à café, des téléviseurs ou des luminaires.

« Ces attaques, en particulier avec l'essor d'objets connectés non sécurisés, vont continuer à harceler nos organisations. Malheureusement, ce que nous voyons n'est que le début en termes de 'botnets' à grande échelle et de dommages disproportionnés », prédit Ben Johnson, ex-hacker pour l'agence américaine de renseignement NSA et cofondateur de Carbon Black.

Quelles peuvent être les conséquences ?

La société Dyn était préparée à ce type d'attaque et a pu résoudre le problème dans des délais relativement brefs. Mais **les conséquences pourraient être bien plus graves** dans les secteurs de la finance, du transport ou de l'énergie, bien moins préparés, selon Eric o'Neill. Quelle qu'en soit l'origine, l'attaque a en effet mis en lumière **les dangers posés par l'utilisation croissante des objets connectés**, qui peuvent être utilisés à l'insu de leurs propriétaires pour bloquer l'accès à un site...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contenus, 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 : Trois questions pour comprendre la cyberattaque massive

Faut-il avoir peur des ransomwares ?



Faut-il avoir
peur des
ransomwares ?

Depuis le premier virus détecté en 1986, le nombre d'attaque n'a cessé d'augmenter, devenant la menace la plus importante pour les entreprises.

En effet, cette forme d'attaque profite aux cybercriminels qui ont trouvé le bon filon pour gagner de l'argent. En constante mouvance, les formes d'attaques sont de plus en plus redoutables et ont généré un trafic de données important : les informations détenues par les entreprises sont désormais toutes disponibles en environnement virtuel et constituent l'élément essentiel pour l'économie de la société (données sensibles, fichiers clients, etc). Leur perte est inconcevable et cela, les cybercriminels l'ont bien compris. Au fil des ans, leurs techniques ont changé jusqu'à l'arrivée des ransomwares. Ce type d'attaque se révèle être la plus rentable pour les attaquants qui multiplient les variantes. La tendance est d'ailleurs à l'augmentation sur tous types de support connecté.

Parce que la perte de données en entreprise peut avoir des conséquences irréversibles sur son activité si l'on prend en compte les paramètres suivants : perte de productivité, perte de données et la réputation liée à ces deux pertes, le non-paiement de factures émises, perte de confiance des salariés dans leur entreprise ; l'impact d'un ransomware peut être catastrophique. Le succès et les méthodes pour obtenir un paiement rapide de la rançon ont permis aux cybercriminels d'attirer l'attention des médias et d'entretenir ce climat de tension.

Il y a quelques mois, ESET a averti les utilisateurs qu'un nombre impressionnant d'e-mails infectés propageaient des ransomwares, submergeant ainsi les boîtes de réception dans le monde entier. Feignant de ne contenir que des fichiers inoffensifs, JS/TrojanDownloader.Nemucod essayait en réalité de forcer les victimes à télécharger et à installer des ransomwares tels que TeslaCrypt ou Locky. Cette stratégie fut efficace puisque les cybercriminels l'ont répété plusieurs fois, multipliant également les variantes utilisées tels que CTBLocker ou Filecoder.DG.

Heureusement les ransomwares ne sont pas toujours aussi dangereux que ceux cités ci-dessus. Beaucoup de cybercriminels amateurs surfent sur cette tendance et développent leur propre ransomware dont l'exécutable, de faible qualité, est facile à contrer. Ceci fut le cas de Petya et Jigsaw qu'ESET a analysé : tous deux contenaient des défauts de mise en œuvre qui ont permis aux victimes touchées de récupérer leurs fichiers sans payer un centime.

Comment vaincre cette peur du ransomware ?

Avoir peur du ransomware ne vous en protégera pas pour autant et payer la rançon ne résoudra pas forcément vos problèmes. Si vous en arrivez à ce stade, c'est que vous n'avez pas appliqué toutes les précautions nécessaires.

La meilleure façon de ne plus avoir peur des ransomwares est de se protéger avec une solution efficace et reconnue, et de s'assurer de couvrir 3 domaines complémentaires : technologique, politique de sécurité et éducation des employés. Sous l'impulsion de l'Etat et des agences de sécurité, les entreprises sont encouragées à adopter des mesures de protection. Les textes, dont le RGPD, étant là pour cadrer l'utilisation et la sécurité des données détenues par les entreprises. En particulier, les investissements dans la recherche et le développement de nouvelles technologies nécessitent un plan de sécurité permettant d'évaluer et de décrire leur sécurité.

Par conséquent, avec des attaques de plus grande envergure et l'émergence de nouvelles vulnérabilités, le plus grand défi de 2016 est de mettre l'accent sur la protection des réseaux et l'accès aux données. Les meilleures pratiques de sécurité doivent donc être appliquées pour protéger les données, les informations et la vie privée. Il s'agit là d'un travail transversal qui exige une participation active des plus hautes fonctions de l'entreprise.

Faut-il avoir peur des ransomwares ? La réponse est non pour tout dirigeant préparé à cette éventualité.

Source : Benoît Grunemwald – Directeur des Opérations ESET France

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

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



[Contactez-nous](#)

Réagissez à cet article

Les jeunes ne seraient pas plus prudents sur le web que leurs grands-parents



Selon une enquête Ipsos, Les 18 – 34 ans sont les premiers touchés par les arnaques en ligne, bien devant leurs grands-parents.

Les natifs du numérique ne sont pas tout à fait aussi prudents sur le net qu'on pourrait le supposer nous disent Microsoft et Ipsos. Même s'ils sont plus à l'aise avec les nouvelles technologies que leurs aînés, les 18 – 34 ans sont également les premiers touchés par les arnaques en ligne, les fameux scams.

VOUS ÊTES LE 1 000 0000 0000E VISITEUR ! ! ! ! !

La moitié des victimes d'arnaque en ligne ont en effet moins de 35 ans selon une étude publiée par Ipsos. Derrière les jeunes gens, on retrouve les 36 – 54 ans qui représentent 34 % des victimes et enfin les plus vieux, plus de 55 ans, ne représentent eux que 17 % du total des victimes.



Le sondage d'Ipsos porte sur une population internationale de 12 000 personnes, dans plus de 12 pays et a été réalisée pour Microsoft.

Les arnaques du web sont aussi vieilles que la technologie, néanmoins leur prolifération ne semble guère être ralentie par les nouveaux usages. Les mails d'arnaque sont devenus des profils Facebook, des messages d'erreurs sur mobile ou d'autres hameçons modernes que l'on retrouve au fil des modes sur différentes plateformes. Si les usages changent, la présence des arnaques, elle, ne fait que s'adapter indéfiniment.

Le rapport met en lumière une des plus importantes arnaques de notre siècle, dans laquelle la victime reçoit un message prétendument adressé par Microsoft, Apple, Dell ou HP, ou d'autres firmes reconnues de la tech grand public. Il explique invariablement que l'appareil du possesseur est infecté, et que l'installation d'un logiciel tiers est nécessaire...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

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



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphoniques, digipsi d'envi, e-mail, contournement de clientèle...);

- Expertises de systèmes de vote électronique ;

- Formations et conférences en cybercriminalité ;

- Formation de CIL (Correspondants Informatique et Libertés) ;

- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contacter nous](#)

Réagissez à cet article

Original de l'article mis en page : Les jeunes ne seraient pas plus prudents sur le web que leurs grands-parents – Tech – Numerama

Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus ?



Données
personnelles en
danger
pourquoi il est
très important
de supprimer vos
comptes en ligne
que vous
n'utilisez plus
?

Atlantico : Le 22 septembre dernier, Yahoo ! révélait que 500 millions de boîtes emails avaient été piratées à la fin de l'année 2014. Quels sont les risques de se voir piraté par une intrusion via des comptes emails dont on ne se sert plus, mais toujours actifs ?

Les actions énoncées ci-dessous que pourraient mener d'éventuels pirates informatiques sont illicites et ne constituent en rien une incitation. Les communiquer a pour seul objectif de sensibiliser des utilisateurs mal informés.

Denis Jacopini : On néglige trop souvent les conséquences d'un piratage de sa propre boîte e-mail.

Donnez vos identifiants et vos mots de passe à un pirate Informatique, vous verrez tout ce qu'il peut en faire...

Tout d'abord, il est possible que vous utilisiez la fonction de carnet d'adresse, notamment parce qu'elle est généralement fournie en même temps que la boîte à courriers électroniques et parce que c'est du coup bien pratique. Un pirate peut alors par exemple, en votre nom (usurpation d'identité), faire croire au destinataire que c'est vous qui écrivez. Ceci pourra avoir pour effet d'inciter la victime à ouvrir une pièce jointe piégée, cliquer sur un lien piégé ou lui venir en aide à la suite d'un vol de papiers, de téléphone etc. Forcément, si vous recevez un e-mail de la part d'un de vos contacts, puisque vous le connaissez, vous n'allez pas vous méfier de la pièce jointe à ouvrir, ni du lien à cliquer et ni de la demande invoquée. Trop tard vous êtes piégé. Le pirate informatique pourra alors injecter un petit malware (programme malveillant) dans votre ordinateur, et s'adonner à de multiples occupations dont scruter la totalité des informations que votre ordinateur, vos ordinateurs ou réseaux, renferment, et pourquoi pas espionner leurs frappes clavier, faire des captures d'écran, écouter votre microphone, activer et consulter de manière invisible votre webcam...

Ensuite, il pourra par exemple consulter les e-mails que vous avez soigneusement conservés ou que vous avez délicatement classés afin d'en savoir un petit peu plus sur votre vie et votre potentiel financier.

Il pourra également probablement demander à des sites Internet encore liés à cette adresse e-mail, de renvoyer des mots de passe oubliés et pourra alors recevoir des liens pour les réinitialiser.

Enfin, si le pirate connaît votre identifiant et votre mot de passe, il tentera d'utiliser ces informations sur d'autres sites Internet sur lesquels vous auriez pu également vous inscrire tels que Facebook, Twitter, Linked-in, ou d'autres sites bancaires ou de vente en ligne.

Quels signes doivent nous pousser à nous inquiéter d'un éventuel « hacking » de nos boîtes mails inactives ? Quelles sont les solutions permettant de se prémunir face à de telles intrusions ?

Si votre boîte e-mail n'est plus active parce que vous ne l'utilisez plus, les signes d'un éventuel « hacking » sont multiples.

D'abord, le signe qui me paraît le plus important est celui d'une personne qui soit vous signale le piratage de votre boîte e-mail, soit qui fait référence à un e-mail que vous n'avez jamais envoyé.

Ensuite, la presse et les médias spécialisés n'hésitent pas à relayer les annonces de piratages de boîtes.

Vous pouvez alors conserver une oreille attentive en vous abonnant à l'un d'eux. Attention aux lanceurs d'alertes de failles de sécurité tels que leakedsource.com. Ce site était rapidement devenu la référence et le meilleur lanceur d'alerte en cas de fuites de données massives suite à un piratage (leak). Bien que créé dans un but louable à la base, le business semble avoir pris le dessus et ce site peut devenir une véritable base de données en libre accès pour les cybercriminels.

Enfin, si vous connaissez encore l'identifiant et le mot de passe de vos boîtes email, en général les fournisseurs de services vous permettent de visualiser un historique d'utilisation. Le consulter vous permettra de vérifier si ce compte soi-disant inutilisé l'est vraiment.

Avec Hotmail (ou Outlook.com), cliquez sur « Vérifier l'activité récente » dans la section « Sécurité et confidentialité ».

Si on utilise Gmail, accédez à vos activités récentes sur Google en allant sur le site <https://security.google.com/settings/security/activity> ou consultez vos dernières activités sur votre compte Gmail en allant sur la page d'accueil de votre messagerie. Vous aurez un lien « Détails » en bas à droite.

Avec Yahoo, survolez avec la souris votre nom / pseudo en haut à droite, et dans le menu déroulant qui apparaît, cliquez sur « Infos compte ». Votre mot de passe est à nouveau demandé : saisissez-le. Dans la rubrique « Connexion et sécurité », cliquez sur le dernier lien : « Consulter vos connexions récentes ».

En général de telles intrusions sont possibles soit si vous avez malencontreusement communiqué votre mot de passe à quelqu'un, soit s'il vous l'a volé en se faisant passer pour un tiers de confiance par la technique de phishing, soit, si le fournisseur de services s'est fait voler, pirater sa base de données, comme dans le cas présent avec plus de 500 millions de comptes Yahoo !

Pour se prémunir face à de telles intrusions, il est aujourd'hui essentiel de renforcer sa politique de gestion des mots de passe. Il y a à peine plus d'un mois, dans un article sur Atlantico je donnais toute une série de conseils sur la manière avec laquelle nous devons aujourd'hui choisir les mots de passe ou plutôt des phrases de passe. Ainsi, en cas de piratage d'un service Internet, vous n'aurez aucune inquiétude en cas de réutilisation de votre mot de passe sur d'autres services.

Enfin, vous pouvez aussi activer des fonctions de sécurité renforcée que certains services proposent. Vous recevrez alors soit un SMS qui vous avertira si un accès anormal à votre compte est détecté, soit un code reçu par SMS à saisir sur la page de connexion en plus de l'identifiant et du mot de passe.

Comment réagir si on s'aperçoit que nos boîtes mails obsolètes ont bel et bien été piratées ? Plus globalement, est-il préférable de supprimer nos comptes en ligne lorsque nous ne les utilisons plus ? Si oui, pourquoi et comment s'y prendre ?

Si on s'aperçoit que nos boîtes mails obsolètes ont bel et bien été piratées, à mon avis, c'est trop tard. Votre adresse e-mail et le mot de passe ont probablement déjà été partagés sur de nombreuses plateformes et ont même certainement fait plusieurs fois le tour du monde.

Demandez-vous d'abord quelle est votre priorité : vous protéger ou retrouver l'auteur du piratage ?

Pour retrouver l'auteur du piratage, l'objectif sera de toucher le moins de choses possibles afin de recueillir un maximum de preuves. Si votre priorité s'oriente vers la protection de vos comptes, suivez les conseils ci-dessous.

A ce stade, il est important de savoir si le mot de passe de votre boîte e-mail piratée est utilisé ailleurs. Si c'est le cas, il faut changer les mots de passe de la boîte e-mail piratée et le mot de passe de chaque service sur lequel ce mot de passe a aussi été utilisé, bien évidemment en veillant à choisir un mot de passe différent pour chaque service.

Ensuite, sans plus attendre, il est important de consulter le contenu de cette boîte e-mail piratée et vérifier qu'elle ne renferme pas des informations sensibles tels que des informations bancaires ou des identifiants d'autres comptes internet.

Soit vous ne souhaitez pas conserver la boîte e-mail, il faudra alors demander la suppression de votre compte, soit vous comptez la conserver, appliquez votre nouvelle politique de gestion des mots de passe.

Enfin, partez du principe que si votre compte a été volé, la réponse à la question secrète aussi. Prenez désormais l'habitude de choisir pour chaque service Internet des questions secrètes différentes car, piraté et disponible dans le DarkNet (Le Web sombre et illégal) et associée à votre adresse e-mail, ce secret pourrait aussi bien représenter une bonne porte d'entrée pour un futur pirate.

Sachez que la suppression du compte n'annule pas le piratage et n'efface pas réellement toutes les informations associées à votre compte.

Propos recueillis par Chloé Chouraqui

Notre métier : Sensibiliser les décideurs et les utilisateurs aux risques liés à la **Cybercriminalité** et à la **Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement).

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



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

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, conteneurs, détournements de clientèle...);

- Expertises de systèmes de vote électronique ;

- Formations et conférences en cybercriminalité ;

- Formation de C.I.L. (Correspondants Informatique et Libertés) ;

- Accompagnement à la mise en conformité CNIL de votre établissement.

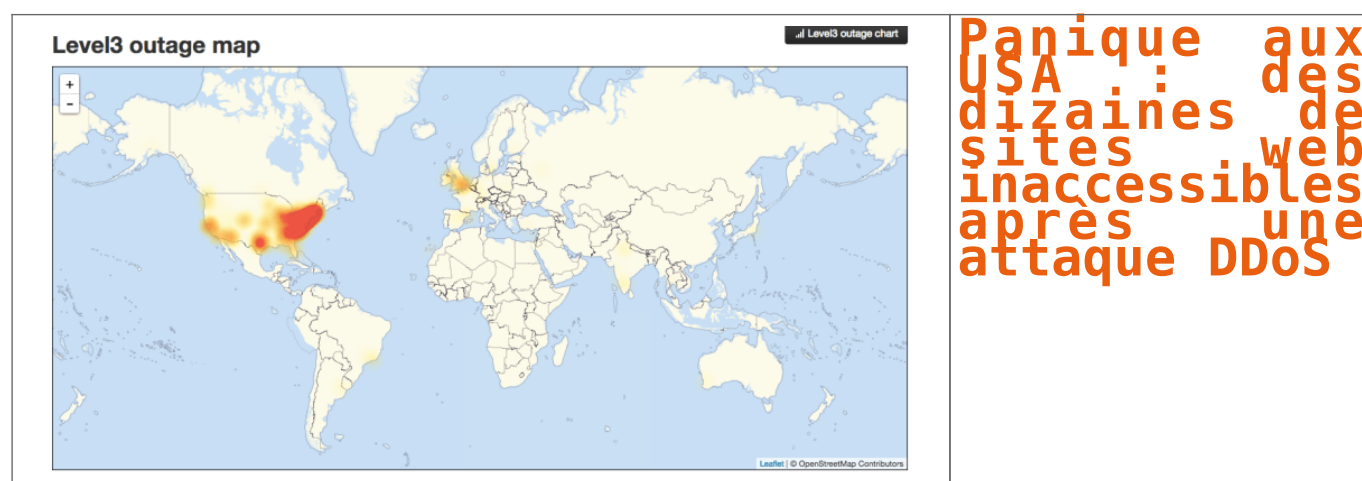


[Contacter-nous](#)

Réagissez à cet article

Original de l'article mis en page : Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n'utilisez plus (et pas seulement de les fermer) | Atlantico.fr

Panique aux USA : des dizaines de sites web inaccessibles après une attaque DDoS



Une attaque par déni de service aurait rendu une grande partie des sites web inaccessibles aux utilisateurs Américains. Le service Dyn, qui a subi l'attaque, est héberge un service de DNS particulièrement utilisé...[Lire la suite]

Denis JACOPINI anime des conférences, des formations en Cybercriminalité et est régulièrement invité à des tables rondes en France et à l'étranger pour sensibiliser les décideurs et les utilisateurs aux Dangers liés à la Cybercriminalité (Arnaques, Piratages...) pour mieux s'en

protéger (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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

Le fonctionnement d'une centrale nucléaire perturbé par une cyberattaque



Le fonctionnement d'une centrale nucléaire perturbé par une cyberattaque

C'est à l'occasion d'un déplacement en Allemagne que Yukiya Amano, patron de l'agence internationale de l'énergie atomique (AIEA) a indiqué qu'une attaque informatique avait, il y a deux ou trois, selon nos confrères de Reuters, affecté le fonctionnement d'une centrale nucléaire...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** en Cybercriminalité et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **Dangers liés à la Cybercriminalité (Arnaques, Piratages...)** pour mieux s'en **protéger** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur sur cette page.



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.

Cloud Microsoft – Les Etats-Unis bien décidés à accéder à des données en Europe

Cloud Microsoft – Les Etats-Unis bien

Législation : Le gouvernement US estime être en droit d'exiger de Microsoft qu'il livre les données d'un utilisateur étranger stockées sur un serveur en Irlande. Un tribunal avait dit non, mais le Département de la Justice revient à la charge....[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Plus d'informations sur notre page 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