Comment bien sécuriser ses e-mails ? | Denis JACOPINI

Peut-on encore se passer de l'e mail dans le cadre de nos activités professionnelles ? Je ne le crois pas. Il est pratique et instantané. Cependant, peu sécurisé en standard, sans précautions, il pourrait bien vous attirer des ennuis.

Selon une étude récente de SilverSky, Email Security Habits Survey Report, 53 % des employés ont déjà reçu des données sensibles d'entreprise non cryptées par e mail ou en pièces jointes, que 21 % des employés déclarent envoyer des données sensibles sans les chiffrer et que 22 % des entreprises sont concernées chaque année par la #perte de données via e-mail.

Inquiétant vous direz-vous ? Catastrophique quand on sait que tout détenteur de données à caractère personnel est tenu à la sécurisation de ces données, conformément à la loi informatique et libertés, encadrée par la CNIL.
Et c'est encore pire quand on prend en compte les informations soumises au secret professionnel ou revêtues de confidentialité que nous échangeons quotidiennement… (plus de 100 milliards d'e-mails sont échangées chaque jour…)
Un des derniers incidents en date : la récente #divulgation des numéros de passeport de 31 leaders mondiaux…
Malgré l'évolution du contexte législatif il est bien étonnant que les entreprises ne soient pas plus nombreuses à choisir de sécuriser leurs échanges par e-mail.

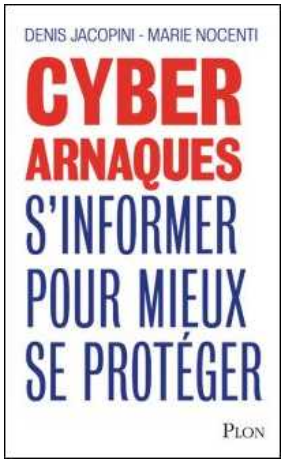
Des solutions ?
Oui, heureusement, et je vais partager avec vous mes conseils :
Mettez en place des procédés de signature numérique et le chiffrement des e-mails garantissent la confidentialité d'un message.
Vous éviterez ainsi que des données sensibles ne tombent dans de mauvaises mains.
Avantage pour le destinataire : l'assurance de l'identité réelle de l'expéditeur de l'e-mail et que le contenu du message n'a pas été modifié après son envoi.
L'utilisation simultanée de ces procédés vous permettront ainsi de répondre à un besoin de Confidentialité (par le chiffrement) et un besoin d'Intégrité (par la signature électronique).

Enfin, aucun de ces deux procédés vous assurera une protection contre la fuite d'informations ou de données confidentielles à votre insu. POur cela, nous vous recommandons d'utiliser des système de « Protection contre la fuite des données » ou de « Data Leak Protection ».*

Plus d'info sur la confidentialité des e-mails ici

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

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)
Denis JACOPINI Marie Nocenti (Plon) ISBN : 2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !

Commandez sur Fnac.fr

https://www.youtube.com/watch?v=lDw3kI7ra2s

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger",Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Milions de victimes de la Cybercirminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

---

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"
Comment se protéger des arnaques Internet

Commandez sur amazon.fr

Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.
Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.
J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur Fnac.fr

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 !

Cybersécurité : les 10 chiffres qui font peur – Silicon

Cybersécurité : les 10 chiffres qui font peur

L'explosion du trafic Internet et des activités numériques est un progrès incontestable. Mais il fait aussi courir des risques grandissants en matière de sécurité. La preuve avec ces dix exemples, qui doivent alerter sur les mesures à prendre.

3 minutes pour pirater un nouvel objet connecté

Caméras de surveillance, imprimantes, thermostats intelligents… Les milliards d'objets reliés au web sont extrêmement mal sécurisés. Les utilisateurs omettent la plupart du temps de changer le mot de passe par défaut et, d'autre part, les fabricants n'intègrent pas de réel système de sécurité dans leurs dispositifs. Résultat : moins de 3 minutes sont nécessaires à un hacker pour prendre le contrôle d'un objet connecté, selon l'éditeur de sécurité ForeScout, partenaire de Malwarebytes.

1,1 million de victimes de fraude à la carte bancaire par an

Le nombre de ménages victimes d'une fraude à la carte bancaire a plus que doublé en 5 ans, passant de 500.000 en 2011 à 1,1 million en 2015,…[lire la suite]

+83 % de smartphones infectés au 2e semestre 2016
65 vols de données par seconde
41 % : le taux de succès d'un ransomware
201 jours pour découvrir une cyberattaque
1,7 milliard de publicités fraudeuses en 2016
140 attaques de phishing par heure
Les particuliers deux fois plus infectés que les professionnels
Une entreprise subit 29 cyberattaques par an
[lire la suite]

NOTRE MÉTIER :

EXPERTISES / COLLECTE & RECHERCHE DE PREUVES : Nous mettons à votre disposition notre expérience en matière d'expertise technique et judiciaire ainsi que nos meilleurs équipements en vue de collecter ou rechercher des preuves dans des téléphones, ordinateurs et autres équipements numériques;

PRÉVENTION : Nous vous apprenons à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;

SUPERVISION : En collaboration avec votre société de maintenance informatique, nous assurons le suivi de la sécurité de votre installation pour son efficience maximale ;

AUDITS CNIL / AUDIT SÉCURITÉ / ANALYSE D'IMPACT : Fort de notre expérience d'une vingtaine d'années, de notre certification en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005) et des formations suivies auprès de la CNIL, nous réaliseront un état des lieux (audit) de votre installation en vue de son amélioration, d'une analyse d'impact ou de sa mise en conformité ;

MISE EN CONFORMITÉ CNIL/RGPD : Nous mettons à niveau une personne de votre établissement qui deviendra référent CNIL et nous l'assistons dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : les 10 chiffres qui font peur – Silicon*

Rapport 2017 sur la Cyber

Sécurité de F-Secure

Rapport 2017 sur la Cyber Sécurité de F-Secure

F-Secure vient de publier son Rapport 2017 sur la Cyber Sécurité qui décrit et analyse l'état actuel de la cyber sécurité dans le monde. Ce rapport s'attarde en particulier sur les problèmes que rencontrent les entreprises, dans un contexte où les pirates délaissent les malware conventionnels au profit d'attaques plus sophistiquées, et donc encore plus dangereuses.
« Les menaces actuelles peuvent déjouer les approches unilatérales classiques de la sécurité, même les plus efficaces. En ayant recours au phishing (avec désormais des listes, vendues en ligne, de comptes ou réseaux pré-exposés) ou via d'autres méthodes, les pirates peuvent beaucoup plus facilement viser un gouvernement ou une entreprise du Fortune 500 », explique Sean Sullivan, Security Advisor chez F-Secure. « Nous vivons dans un monde post-malware, où le piratage s'est industrialisé. Et les cyber criminels ne comptent plus seulement sur les malware les plus communs pour se faire de l'argent. »

Ce rapport offre une analyse détaillée des problèmes majeurs diagnostiqués par les chercheurs et experts sur le plan de la cyber sécurité. Parmi les principaux résultats :
• Une grande partie du trafic de reconnaissance active en 2016 était liée à des adresses IP majoritairement situées dans 10 pays, et notamment la Russie, les Pays-Bas, les États-Unis, la Chine ou encore l'Allemagne.
• Les versions obsolètes d'Android sont de plus en plus nombreuses et rendent les appareils mobiles particulièrement exposés. L'Indonésie possède le nombre le plus important d'appareils Android non mis à jour, la Norvège, le plus faible.
• La plupart des cyber attaques font appel à des techniques basiques et s'en prennent à des infrastructures peu robustes.
• 197 nouvelles familles de ransomware ont été découvertes en 2016, contre seulement 44 en 2015.
• Le recours aux exploit kits a diminué au cours de 2016.
Ce rapport relate également les évènements marquants et les tendances de l'année 2016. Au programme : des informations sur les botnets de type Mirai, sur les attaques préparées en amont, sur le cyber crime et sur les dernières tendances globales en matière de cyber menaces. Certaines organisations comme l'Autorité finlandaise de régulation des communication, le Virus Bulletin ou encore AV-Test, ont contribué à ce rapport à travers plusieurs articles…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Nouveau Rapport F-Secure sur la Cyber Sécurité : un monde « post-malware » – Global Security Mag Online*

Protéger son identité contre le vol sur Internet devrait être une priorité

Protéger son identité contre le vol sur Internet devrait être une priorité

Selon une étude concernant le vol d'identité et menée aux États-Unis par l'entreprise spécialisée dans la cybersécurité mobile Lookout auprès de 2000 clients, les délits concernant les données personnelles sont en pleine expansion. Ils constituent l'un des principaux soucis des usagers d'Internet et de la téléphonie mobile, qu'ils soient particuliers ou entreprises. Actuellement, le vol… Lire la suite

Actuellement, le vol d'identité est considéré comme un phénomène inéluctable d'après les enquêtes réalisées par Lookout. Les résultats démontrent que près de 35 % des sondées ont été victimes de vol d'identité. 41 % affirment que leurs données personnelles ne peuvent plus être sécurisées et, à un moment donné, elles seront inévitablement volées. D'ailleurs, aux États-Unis, le pourcentage d'infraction sur les identités des personnes a augmenté de près de 20 % depuis octobre 2015.

Internet : principal moyen de vol

Lookout affirme que le vol de données personnelles ne se passe plus par les méthodes classiques telles que la fouille des ordures dans les rues ou encore le vol de courrier dans les boîtes aux lettres ou il est très facile d'y trouver des informations permettant d'accéder aux numéros de carte de crédit ou de comptes divers. De nos jours, les criminels sont plus malins et bien plus discrets en usant de moyens sophistiqués et d'Internet comme les techniques de « phishing ».

Cette méthode profite de la faille humaine et non de l'informatique. Les voleurs se font passer pour une banque, un opérateur téléphonique ou une entreprise pour pousser la victime à se connecter sur leur site à travers un faux lien hypertexte. De cette manière, ils peuvent récolter des informations personnelles (des coordonnées bancaires surtout) qu'ils vont utiliser pour réaliser des achats ou des transferts d'argent vers leur compte.

En effet, l'étude menée par Lookout démontre que 60 % des Américains ont effectué à leur insu, des achats à de grandes entreprises de vente en ligne ou des transactions bancaires à cause d'une cyberattaque via de courriels frauduleux d'hameçonnage (phishing).

Les chiffres démontrés par l'étude de Lookout

D'autres chiffres révèlent aussi que les personnes ne se sentent pas en sécurité : 77 % craignent de perdre leur numéro de sécurité sociale, 74 % leurs données bancaires, 71 % leur code et carte de crédit et 56 % leurs données personnelles.

Par ailleurs, la plus grande peur des gens concerne le fait qu'ils ne soient pas immédiatement au courant du vol de leur identité au moment des actes de fraudes commises par les criminels. Selon l'enquête faite par Lookout, une personne victime d'un vol d'identité ne le découvrira que par une lettre postale (33 %), une information télévisée ou radio (31 %) ou un mail inattendu (31 %). Cela résulte du fait que les factures sur les crimes commis lui sont toujours renvoyées plus tard par mail ou par la poste.

Toujours d'après l'étude, 65 % des personnes ayant subi un vol ou une usurpation de leur identité via un site sur lequel elles se sont inscrites n'en seront averties qu'un mois après la cyberattaque. De même, 75 % des usurpés ne connaissent pas les actions à entreprendre dans de telles situations.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous accompagner dans vos démarches de mise en conformité avec la réglement Européen relatif à la protection des données à caractère personnel (RGPD).

Denis JACOPINI est Expert Judiciaire en Informatique, Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), Diplômé en Droit de l'Expertise Judiciaire et Risk Manager ISO 27005, spécialisé en Cybercriminalité et en protection des Données à Caractère Personnel.

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

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Le vol d’identité en nette progression : les données personnelles ne sont plus sécurisées

---

80 % des entreprises françaises ont constaté au moins une cyberattaque dans l’année

80 % des entreprises françaises ont constaté au moins une cyberattaque dans l’année

---

Dans son baromètre annuel fraîchement publié, le Club des experts de la sécurité de l'information et du numérique (CESIN) qui regroupe 280 responsables d'entreprises françaises, notamment celles du CAC 40, relate que 52% des responsables sécurité des systèmes d'information d'entreprises françaises (RSSI) avouent être optimistes dans la capacité de leur structure à faire obstacle aux risques d'intrusions en 2016, soit une hausse de 5% par rapport à 2015. Mais pourtant.

Le verre à moitié vide ou à moitié plein donc, puisque même si la moitié des RSSI se disent faire confiance à leur système de sécurité, la hausse perpétuelle des attaques ne fait aucun doute. D'après le CESIN, elles ont augmenté pour 46% des RSSI entre 2015 et 2016 alors que 53% s'estiment stables. Plus frappant encore, le pourcentage d'entreprises françaises recensant au moins une cyberattaque entrante dans leurs serveurs sur les 12 derniers mois, s'élève à 80%. Et c'est là que le bas blesse, il leur faut généralement en moyenne une à six heures pour détecter l'attaque et entre 3 jours et trois semaine pour corriger le système.

Des moyens de protection jugés peu efficaces

Afin d'assurer leur cyber-sécurité, 84% des entreprises vont acquérir de nouvelles solutions techniques, 55% jugeront utile d'augmenter leur budget et 44% vont accroître leur effectif, comme le rappelle La Tribune.

Si les pare-feux (91%), le VPN (89%) et le filtrage web (78%) sont jugées efficaces, les sondes de sécurité conseillées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sont jugées peu efficace (54%) ainsi que le chiffrement de base de données (60%). A ce propos, Olivier Ligneul, vice président du CESIN martèle : « Les RSSI ne peuvent plus se contenter d'être les ultra-spécialistes qui gérent les règles des pare-feux des entreprises .»

En résumé, 40% des entreprises affirment que les solutions techniques proposées par le marché ne sont pas adaptées aux différents types de menaces.

Les types d'attaques

Toujours selon le CESIN, l'attaque en tête de classement est de loin le « ransomware » soit la demande de rançon (80%), en seconde position arrive l'attaque par déni de service (40%), complète le podium les attaques virales générales (36%).

D'ailleurs à l'avenir et avec la transformation numérique, l'exposition aux attaques se multipliera notamment avec les mobiles, cloud et objets connectés, les entreprises devront ainsi revoir leur priorité en terme de protection et améliorer leur défense. Il y a du pain sur la planche.

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

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

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
  (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Baromètre CESIN : 80 % des entreprises françaises ont constaté au moins une cyberattaque dans l’année

---

13,7 millions de Français ont été confrontées à la cybercriminalité en 2016

13,7 millions de Français ont été confrontées à la cybercriminalité en 2016

La nouvelle édition du rapport Norton sur les cyber risques montre le laxisme des utilisateurs français quant à leur sécurité en ligne tandis que les cyber-attaquants ne cessent de développer leurs compétences et la sophistication de leurs attaques.

France *vs* Monde		
TOP FINDINGS	FRANCE	GLOBAL (21 pays)
Individus confrontés à la cybercriminalité au cours de l'année écoulée	**13,7 millions (24 %)**	689,4 millions (31 %)
Coût financier total lié à la cybercriminalité au cours de l'année écoulée	**1,789 milliards d'euros**	125,9 milliards de dollars (environ 117 milliards d'euros)
Temps moyen passé à gérer les conséquences d'un acte de criminalité en ligne	**9,6 heures**	19,7 heures
Profils d'individus les plus touchés par la cybercriminalité au cours de l'année écoulée	**Voyageurs fréquents : 31 % Millennials : 29 % Parents : 26 %**	Voyageurs fréquents : 40 % Millennials : 40 % Parents : 40 %
Personnes ne sachant pas identifier un e-mail de phishing ou évaluer la validité d'un e-mail	**31 %**	41 %
Victimes d'un acte de cybercrime après avoir répondu à un potentiel e-mail de phishing	**90 %**	80 %
Individus ensant savoir déterminer si le réseau Wi-Fi utilisé est sécurisé	**56 %**	48 %
Individus se sentant dépassés par la quantité d'informations dont ils ont besoin pour se protéger en ligne au quotidien	**33 %**	39 %
Individus estimant que les appareils domestiques connectés offrent aux pirates de nouvelles façons de voler des données	**81 %**	72 %
Individus n'utilisant des mots de passe sécurisés que lorsqu'ils sont requis	**26 %**	42 %
Individus possédant au moins un terminal non protégé	**35 %**	35 %

En France, 13,7 millions de personnes ont été confrontées à la cybercriminalité en 2016

Norton by **Symantec**, a publié les résultats de son rapport annuel sur les cyber risques : au cours de l'année écoulée, 13,7 millions de Français ont été victimes d'actes de cybercriminalité. Les attaquants continuent de profiter d'un manque de vigilance de la part des utilisateurs. Le rapport montre que le coût financier lié au cyber crime s'élève à près d' 1,8 milliard d'euros en France (environ 117 milliard d'euros au niveau mondial). Quant au « coût temps », les Français victimes d'acte de cyber crime passent en moyenne 9,6 heures à en gérer les conséquences.
L'enquête, réalisée auprès d'un échantillon représentatif de 20 907 personnes répartis dans 21 pays, dont 1 008 Français, illustre l'impact de la cybercriminalité et révèle qu'alors que la prise de conscience commence à s'intensifier, de nombreuses personnes restent trop laxistes quant à la protection de leurs informations personnelles. Plus des trois-quarts des Français (77 %) savent qu'ils doivent activement protéger leurs informations en ligne, mais sont toujours enclins à cliquer sur des liens ou à ouvrir des pièces jointes douteuses provenant d'expéditeurs inconnus.
Les catégories les plus affectées par le cybercrime sont les 18-34 ans – 29% d'entre eux en ont été victimes l'an passé. Par ailleurs, 31% des voyageurs fréquents, 26% des parents et 21% des hommes ont reconnu avoir été concernés par le sujet au cours de l'année passée.
Si les comportements qui ne respectent pas les règles élémentaires de sécurité en ligne sont mis en évidence par le rapport, 81% des Français savent reconnaitre un email de phishing, ce qui les place au premier rang européen et mondial. Ce score élevé résulte probablement des efforts de pédagogie des institutions gouvernementales et financières sur le sujet.
*« La conclusion de notre rapport 2016 est sans appel : les internautes ont de plus en plus conscience qu'il est indispensable de protéger leurs informations personnelles en ligne mais n'ont pas envie de prendre les précautions adéquates pour assurer leur sécurité », déclare **Laurent Heslault**, expert en cyber-sécurité Norton by Symantec. « La paresse des utilisateurs n'évolue pas, mais dans le même temps, les cyber-attaquants affinent leurs compétences et adaptent leurs fraudes pour profiter davantage des internautes. Le besoin d'éducation n'a jamais été aussi fort et il est donc crucial de prendre des mesures appropriées. »*

Les internautes savent que le risque est réel
La cybercriminalité est aujourd'hui si courante et répandue que les internautes la considèrent comme un risque équivalent à ceux du monde réel :
• Près de la moitié des internautes (46 %) déclare qu'il est devenu plus difficile d'assurer sa sécurité en ligne que dans le monde physique et réel ;
• Presque la moitié (47 %) estime que saisir ses informations financières sur Internet, en étant connecté à un réseau Wi-Fi public, serait plus risqué que de lire à voix haute son numéro de carte dans un lieu public ;
• Un Français sur 2 pense qu'il est plus probable que quelqu'un accède frauduleusement à leurs appareils domestiques connectés plutôt qu'à leur logement.

Et les risques sont bien réels
Les actes de cybercriminalité les plus fréquents en France sont le vol de mot de passe (14 %) et la fraude à la carte de crédit (10 %). Les deux reflètent un besoin encore présent de sensibilisation du public sur la sécurité en ligne ; en effet :
• Les Français ne vérifient pas toujours le niveau de sécurité des sites Web lors de leurs achats en ligne ;
• 1 Français sur 5 partage ses mots de passe ;
• Près d'1 Français sur 2 utilise le même sur plusieurs plates-formes et comptes.
Parmi les autres actes de cybercriminalité, le rapport sur les cyber risques Norton by Symantec a identifié le piratage électronique (11 %) et le piratage des réseaux sociaux (9 %). Alors que le ransomware représentait seulement 4 % des actes de cybercriminalité, soit environ 548 000 au cours de l'année passée ; 30 % des victimes de ransomware ont payé la rançon et 41 % ne pouvaient plus accéder à leurs fichiers.

Les mauvaises habitudes en ligne ont la vie dure
La cybercriminalité est un risque intrinsèque à notre monde connecté, mais les utilisateurs manquent toujours de vigilance et manifestent des habitudes en ligne risquées lorsqu'il s'agit de protéger leurs informations personnelles en ligne. Parmi les faits marquants de l'étude Norton by Symantec :
• L'email, ce fléau – 65 % des Français ont ouvert une pièce jointe provenant d'un expéditeur inconnu, mais seulement 35 % d'entre eux ont ouvert la porte à un étranger : il existe donc une dichotomie des comportements de sécurité entre le monde physique et le monde virtuel. Par ailleurs, 19% ne savent toujours pas identifier un email de phishing.
• Le gap générationnel – La génération Y montre des habitudes étonnement peu sérieuses en ligne et partage facilement ses mots de passe, mettant ainsi en danger sa sécurité en ligne (35 %). C'est probablement pour cette raison que les jeunes restent les victimes les plus fréquentes puisque 29 % des Français de la génération Y ont été victimes de cybercriminalité l'année dernière ;
• La faille du mot de passe – Même si une majorité des utilisateurs (58 %) affirme utiliser un mot de passe sécurisé sur chaque compte, quasiment un internaute sur 5 (20 %) partage ses mots de passe avec d'autres personnes et nombre d'entre eux (42 %) ne voient pas le danger d'utiliser les mêmes mots de passe sur plusieurs comptes ;
• Le manque de protection – 35 % des Français ont au moins un appareil non protégé, ce qui les rend vulnérables face aux ransomware et phishing, aux sites malveillants et aux attaques zero-day. Parmi eux, 1 tiers (31 %) l'explique par le fait qu'il ne pense pas que l'appareil ait besoin d'être protégé et 27 % affirment ne rien faire de « risqué » en ligne, les rendant vulnérables à une attaque ;
Une connexion permanente à quel prix ? – L'envie de rester connecté en permanence fait que 25 % des Français préféreraient installer un programme tiers pour accéder à un Wi-Fi public plutôt que de s'en passer…[lire la suite]

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.*
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l’article mis en page : En France, 13,7 millions de personnes ont été confrontées à la cybercriminalité en 2016 – No Web Agency

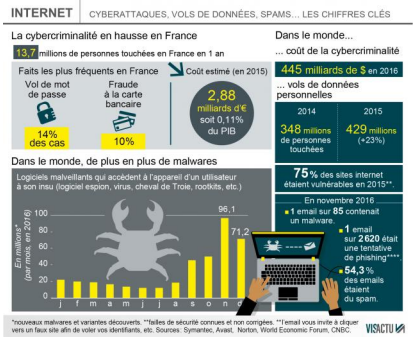
---

Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

Comment a évolué la cybercriminalité en 2016 par rapport à 2015 ?

Il y a les cyberattaques à l'échelle des états et il y a la cybercriminalité qui peut toucher chaque citoyen. Vols de mots de passe, demandes de rançon, vols de données personnelles… Les chiffres sont en hausse partout dans le monde mais aussi en France.

Les chiffres de la cybercriminalité ont de quoi faire peur. 13,7 millions de personnes ont été confrontées à la cybercriminalité en France en 2016, selon Norton, entreprise spécialisée dans la sécurité en ligne.
Vente de faux papiers d'identité, apologie du terrorisme, vols de mots de passe, de données personnelles, extorsion de fonds ou encore trafic d'armes : le terme cybercriminalité couvre de multiples activités illicites.



Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. | Visactu

Vol de mots de passe

En France, les actes les plus fréquents sont les vols de mots de passe (14 % des cas) et la fraude à la carte bancaire (10 % des cas). Mais entre les faits recensés et la réalité, il est très difficile de mesurer l'ampleur exacte du phénomène…
Certaines victimes ne savent tout simplement pas (encore) qu'elles ont été volées, d'autres n'ont pas porté plainte et ont préféré payer une rançon (parfois quelques centaines d'euros) pour récupérer des photos intimes par exemple.
Selon Symantec, célèbre pour ses logiciels antivirus, le nombre de cyberattaques dans le monde a diminué ces derniers mois. Elle en a recensé 291 000 pour le seul mois de novembre 2016 contre 1 461 000 en janvier 2015.

Gare aux malwares

Par contre, le nombre de nouveaux malwares explose. Ces logiciels malveillants qui accèdent à l'appareil d'un utilisateur à son insu (logiciel espion, virus, cheval de Troie, rootkits, etc.) dans le but de dérober des données sont partout.
Symantec dénombrait 20 millions de nouveaux malwares (et variantes) chaque mois début 2016, un chiffre qui a bondi en fin d'année pour atteindre les 96,1 millions en novembre et 71,2 millions de nouveaux malwares détectés en décembre.

Les vols de données de personnelles en hausse

En novembre 2016, Symantec estimait qu'un email sur 85 contenait un malware, qu'un email sur 2 620 était une tentative de phishing (l'email vous invite à cliquer vers un faux site afin de voler vos identifiants, mots de passe, etc.) et que plus de la moitié des emails (54,3 %) étaient non sollicités (spam).
En 2015, elle estimait que 429 millions de personnes dans le monde s'étaient faites voler des données personnelles, un chiffre en hausse de 23 % par rapport à l'année précédente.

Original de l'article : La cybercriminalité en hausse en France et dans le monde

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRECCTE n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : La cybercriminalité en hausse en France et dans le monde

---

Une entreprise touchée toutes les 40 secondes par une

attaque par Ransomware en 2016

Une entreprise touchée toutes les 40 secondes par une attaque par Ransomware en 2016

Entre janvier et septembre 2016, la fréquence des attaques de ransomware contre les entreprises a triplé, passant d'une toutes les deux minutes une toutes les 40 secondes. Pour les particuliers, cet intervalle s'est réduit de 20 à 10 secondes. Avec l'apparition de plus de 62 nouvelles familles de logiciels rançonneurs au cours de l'année, le ransomware est la menace désignée comme fait marquant de l'année 2016. La rubrique Story of the Year fait partie de l'édition annuelle du Kaspersky Security Bulletin retraçant les principales menaces et statistiques de l'année écoulée et établit des prévisions sur ce que nous réserve 2017.

Le ransomware est devenu un réel business

Entre autres choses, 2016 a révélé à quel point le modèle RaaS (Ransomware as a Service) séduit désormais les criminels qui ne possèdent pas les compétences ou les ressources nécessaires pour développer leur propre malware ou n'en ont tout simplement pas envie. Le principe consiste pour les créateurs du code malveillant à offrir celui-ci « à la demande », en se bornant à vendre des versions modifiées à leurs clients qui les diffusent via du spam ou des sites web et reversent une commission à l'auteur, le principal bénéficiaire financier. « Le modèle classique de l'affiliation paraît aussi efficace pour le ransomware que pour les autres types de malware. Les victimes paient souvent la rançon, de sorte que l'argent coule à flots. Inévitablement, cela a conduit à l'apparition quasi quotidienne de nouveaux logiciels de cryptage », commente Fedor Sinitsyn, analyste senior en malware chez Kaspersky Lab.

L'évolution du ransomware en 2016

En 2016, le ransomware a poursuivi ses ravages à travers le monde, devenant de plus en plus élaboré et diversifié pour renforcer son emprise sur les données, les appareils, les particuliers et les entreprises :

• Les attaques sur les entreprises ont nettement augmenté. Selon l'étude Kaspersky Lab, une entreprise sur cinq au niveau mondial a subi un incident de sécurité informatique à la suite d'une attaque de ransomware et une petite entreprise sur cinq n'a jamais récupéré ses fichiers, même après avoir versé une rançon.

• Si certains secteurs d'activité ont été plus durement touchés que d'autres, notre étude indique que personne n'est véritablement épargné par le risque : le plus fort taux d'attaques frappe l'enseignement (de l'ordre de 23 %) et le plus faible, la grande distribution et les loisirs (16 %).

• Le ransomware « éducatif », conçu pour donner aux administrateurs système un outil permettant de simuler des attaques de ce type, a été rapidement et impitoyablement exploité par des criminels, donnant notamment naissance à Ded_Cryptor et Fantom.

• Parmi les méthodes de rançonnage observées pour la première fois en 2016 figure le cryptage de disque, consistant pour les auteurs des attaques à bloquer l'accès, non pas à quelques fichiers, mais à la totalité d'entre eux simultanément. Petya Dcryptor, alias Mamba, va encore plus loin en verrouillant l'ensemble du disque dur, grâce à des attaques de mots de passe par force brute pour accéder à distance aux appareils des victimes.

• Le ransomware Shade a montré sa capacité à changer d'approche vis-à-vis d'une victime si l'ordinateur infecté s'avère appartenir à des services financiers, pour télécharger et installer un spyware au lieu de crypter les fichiers.

• Les codes malveillants ont sensiblement perdu de leur qualité : c'est ainsi que de simples chevaux de Troie rançonneurs, présentant des erreurs de programmation et des fautes grossières dans les demandes de rançon, multiplient les risques pour les victimes de ne jamais récupérer leurs données…[lire la suite]

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

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

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

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Ransomware : Kaspersky Lab recense une attaque toutes les 40 secondes contre les entreprises en 2016 — Global Security Mag Online

Explosion de la cybercriminalité en 2016

	**Explosion de la cybercriminalité en 2016**

En 2016, les peur des attentats s'est multipliée par six, selon une étude sur l'insécurité en France. Autre donnée importante : en cinq ans, les personnes victimes de retraits frauduleux sur leurs comptes bancaires ont doublé.

Notre métier : Au delà de nos actions de sensibilisation, nous répondons à vos préoccupations en matière de cybersécurité par des audits sécurité, par des actions de sensibilisation sous forme de formations ou de conférences. Vous apprendrez comment vous protéger des pirates informatiques et comment vous mettre en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur 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 réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) 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 : Explosion de la cybercriminalité en 2016 — Fdesouche