Simple Hack Lets Hackers Listen to Your Facebook Voice Messages Sent Over Chat

Simple Hack Lets Hackers Listen to Your Facebook Voice Messages Sent Over Chat

Most people hate typing long messages while chatting on messaging apps, but thanks to voice recording feature provided by WhatsApp and Facebook Messenger, which makes it much easier for users to send longer messages that generally includes a lot of typing effort.…[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 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.

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

Contactez-nous

Réagissez à cet article

Comment Windows 10 Anniversary Update a détourné deux attaques zero day

Comment Windows 10 Anniversary Update a détourné deux attaques zero day

Les attaques zero day ont la particularité d'exploiter des vulnérabilités non corrigées des éditeurs. Dans ces conditions, les utilisateurs et entreprises ciblées par ce type d'attaques doivent multiplier les couches de protection pour s'en prémunir au mieux.…[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 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.

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

Contactez-nous

Réagissez à cet article

Comment Windows 10 Anniversary Update a détourné deux attaques zero day

Comment Windows 10 Anniversary Update a détourné deux attaques zero day

Les attaques zero day ont la particularité d'exploiter des vulnérabilités non corrigées des éditeurs. Dans ces conditions, les utilisateurs et entreprises ciblées par ce type d'attaques doivent multiplier les couches de protection pour s'en prémunir au mieux.…[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 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.

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

Contactez-nous

Réagissez à cet article

La moitié des écoles de Bordeaux victimes d'un ransomware

La moitié des écoles de Bordeaux victimes d'un ransomware

Les ransomwares font de nouvelles victimes. Un établissement de santé gérant 5 hôpitaux de l'est de Londres et une quarantaine d'écoles de Bordeaux sont tombés dans leurs filets.
Selon nos confrères de Sud-Ouest, pas loin d'une école bordelaise sur deux a été la victime d'une attaque informatique. Le phénomène a démarré en septembre et s'est accéléré jusqu'aux vacances de Noël, pour toucher au total les serveurs d'environ 40 établissements sur les 101 écoles que compte la préfecture de la Gironde. Un audit est en cours pour tenter de déterminer l'origine de l'infection. L'adjointe au maire en charge de l'éducation, Emmanuelle Cuny, parle d'une attaque « *sans précédent* ».

S'il est encore trop tôt pour se montrer catégorique, l'infection semble provenir d'un ransomware qui s'est diffusé de machine en machine. Comme le note le site spécialisé DataSecurityBreach, l'Académie de Bordeaux dispose d'un contrat avec l'éditeur d'antivirus TrendMicro, pour le produit Internet Security. Reste à savoir si cette protection a été dupée par les cybercriminels ou si – comme c'est plus probable -, elle n'a pas été correctement installée dans les établissements victimes du fléau. Selon Sud-Ouest, les données pédagogiques sont menacées par cette épidémie…[lire la suite]

Denis JACOPINI : Nous allons rentrer en contact avec l'adjointe au maire en charge de l'éducationà la Mairie de Bordeaux pour voir comment nous pouvons leur venir en aide.

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 : La moitié des écoles de

Bordeaux victimes d’un ransomware

Que nous réserve la cybercriminalité dans les 12 prochains mois ?

	**Que nous réserve la cybercriminalité dans les 12 prochains mois ?**

Depuis ces dernières années, la cybercriminalité fait couler beaucoup d'encre ! Qui n'a pas été touché ou ne connaît pas un proche concerné par un e-mail douteux voire d'arnaque, un site Internet piégé, un programme aux intentions essentiellement malveillantes, un profil menteur-voleur ou même un petit prélèvement à l'étranger ?

Le développement de l'Internet et son nombre d'utilisateurs grandissant a aussi fait grimper le nombre de cyberdélinquants. Si quelques pirates informatiques peuvent être considérés comme de véritables génies, les plus nombreux trouvent sur Internet suffisamment d'informations techniques pour se comporter comme de simples émules et s'en mettre eux aussi plein les poches. Parce qu'un homme averti en vaut deux, venez découvrir au cours de notre conférence d'1h30, ce que la cybercriminalité va nous réserver dans les 12 prochains mois afin d'y être mentalement et techniquement préparé.

Objectif de la conférence

Améliorez votre confiance et adaptez votre stratégie digitale en tenant compte des tendances des prochaines années en matière de cybercriminalité.

Programme

• Etat des lieux en France et dans le monde;
• Les prochaines techniques utilisées par les pirates;
• Faisons évoluer nos bonnes pratiques ;

Durée

1h30 + 30min à 1h de questions / réponses.

Public concerné :

Clubs d'entreprises, chambres, fédérations, corporations, décideurs, dirigeants, élus, présidents d'associations.

Moyens techniques :

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

Animateur :

Denis JACOPINI
Expert Judiciaire en Informatique
Diplômé en cybercriminalité, sécurité de l'information
Droit de l'expertise judiciaire
Risk Manager ISO 27005
Spécialisé en protection des données personnelles
Correspondant CNIL
Gérant d'une SSII pendant 17 ans

Intéressé pour organiser cette conférence ? Contactez-nous

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

Le nombre de serveurs MongoDB infectés augmente chaque jour…

L'irruption d'un groupe de cybercriminels spécialisé dans le ransomware a encore dopé le nombre de piratages des bases MongoDB. Une quinzaine d'acteurs malveillants exploitent désormais le filon.

Déjà en nette expansion la semaine dernière, l'infection touchant les bases de données MongoDB laissées librement accessibles sur Internet tourne à l'épidémie. Alors que les deux chercheurs suivant cette attaque, Victor Gevers et Niall Merrigan, recensaient un peu plus de 10 000 serveurs pris en otage vendredi, le total dépasse désormais les 28 300. Cette soudaine inflation est en grande partie due à l'entrée d'une scène d'un groupe de cybercriminels spécialistes des ransomwares, Kraken. Ce dernier, responsable à lui seul de 16 000 infections, serait entré en lice vendredi dernier, après avoir probablement pris conscience de la simplicité d'exploitation de ce nouveau filon. Selon les éléments recensés par Victor Gevers et Niall Merrigan dans un tableau récapitulant les données relatives à la quinzaine de groupes impliqués dans des attaques de ce type, Kraken aurait déjà convaincu 67 organisations de lui verser une rançon de 0,1 Bitcoin (86 euros environ) ou, dans certains cas, de 1 Bitcoin.
Rappelons que l'attaque ne consiste pas à déployer un ransomware, mais exploite la (très discutable) configuration par défaut des bases MongoDB, au sein duquel l'accès n'est pas protégé par une authentification. Lorsque que ces bases sont librement accessibles sur Internet, les pirates se contentent d'exporter le contenu des bases non sécurisées, d'effacer les données du réceptacle originel et d'y déposer un fichier comportant les informations poussant à la victime à payer une rançon (entre 0,1 et 1 Bitcoin) afin de retrouver ses données. Notons que MongoDB a publié un billet de blog expliquant comment paramétrer sa solution pour éviter ce type de mésaventure.

Un défaut connu de longue date

Victor Gevers et Niall Merrigan signalent que certains groupes de cybercriminels se contentent d'effacer les données, sans les télécharger au préalable, rendant toute récupération de l'information illusoire pour les victimes. Selon Victor Gevers, 12 organisations ayant versé une rançon à Kraken n'ont pour l'instant obtenu aucune réponse du groupe de cybercriminels. Les deux chercheurs notent également que certains acteurs malveillants en concurrence sur ce segment n'hésitent pas à remplacer les fichiers de demande de rançon d'autres groupes de hackers. La conséquence ? Les victimes peuvent se retrouver à verser des bitcoins à des individus qui, de toute façon, ne détiennent pas leurs données…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Epidémie pour MongoDB : 28 000 serveurs pris en otage

---

Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook ?

Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook ?

Deux groupes ont été fermés pour avoir diffusé des photos volées de femmes nues…

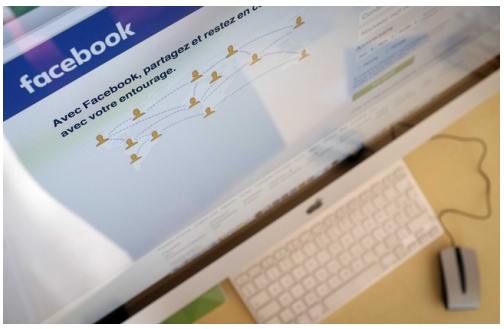


Illustration Facebook — LODI FRANCK/SIPA

Ils partageaient des photos de leurs copines nues assorties de commentaires graveleux ou insultants. Deux groupes secrets sur Facebook, « Babylone 2.0 » et « Garde ta pêche », ont été fermés en fin de semaine dernière après leur découverte par une journaliste belge. Pour pouvoir entrer dans ces groupes, il faut être coopté et personne d'autre que leurs membres ne peuvent en voir le contenu. Ce qui pose un problème au réseau social, dont le principe de modération est basé sur les signalements des utilisateurs.

« Banalisation de la violence »

« Chaque utilisateur a la possibilité de signaler tout contenu qu'il considère choquant, qu'il s'agisse d'un commentaire, d'un post, d'une page, d'un profil, etc. (…) Dès le premier signalement, le contenu est consulté et analysé par une équipe dédiée mobilisée 24 heures sur 24, 7 jours sur 7. Pour la France, nous disposons d'une équipe francophone », indique Facebook France. Il s'agit donc d'une modération *a posteriori*, qui n'intervient que lorsqu'un utilisateur du réseau alerte Facebook. Si tous les membres d'un groupe sont d'accord pour partager des contenus qui enfreignent « les standards de la communauté », il y a donc peu de chances pour que ceux-ci soient interdits.

« On sait que Facebook a des soucis de modération, estime Hélène Dupont, conseillère éditoriale sur le programme Internet sans crainte. On ne peut pas attendre de Facebook d'avoir la même vigilance qu'un média car ils n'ont pas de rédaction ou de comité éditorial. C'est pour cela que nous sommes favorables à l'éducation des utilisateurs en amont. » Chez les jeunes notamment, la connaissance des outils de signalement est importante. Mais lorsqu'ils voient un contenu qui les choque, ce n'est pas leur compétence technique qui fait défaut pour lancer une alerte : « On a vu que pour la cyberviolence ou le harcèlement, la tolérance est bien plus grande en ligne que dans la réalité, note Hélène Dupont. Il y a une banalisation de la violence sur Facebook et les jeunes en réfèrent peu à des adultes. »…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Cyberviolence: Comment sont contrôlés les groupes secrets sur Facebook

---

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

---

Agir contre les rançongiciels chiffrants !

Agir contre les rançongiciels chiffrants !

Le CECyF a rejoint en décembre 2016 avec enthousiasme le programme NoMoreRansom. Il regroupe, sous l'égide d'Europol, un certain nombre de partenaires publics et privés œuvrant dans la lutte contre les cryptolockers ou rançongiciels chiffrants.

Ainsi, sur le site NoMoreRansom vous trouverez des informations sur cette menace, la façon de s'en prémunir et surtout, **dès qu'une solution existe, des liens vers les outils vous permettant de déchiffrer les fichiers compromis** par le cryptolocker dont vous êtes victime…[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

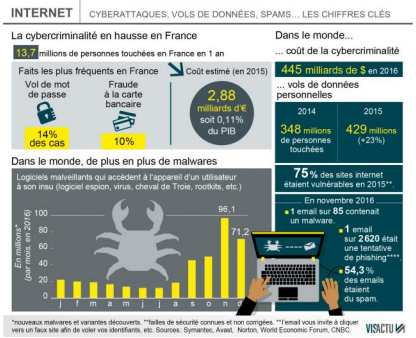
Original de l'article mis en page : No More Ransom – Agissons contre les rançongiciels chiffrants ! | CECyF

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 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