Gestion des mots de passe : Où en sont nos comportements ?

	Gestion des mots de passe : Où en sont nos comportements ?

Les internautes ont conscience du risque. Malgré tout, 61 % réutilisent les mêmes mots de passe sur différents comptes, selon une enquête internationale de Lab42 pour LastPass.

Malgré les recommandations en faveur de l'utilisation de mots de passe robustes, malgré la médiatisation de violations de données à grande échelle (Yahoo, LinkedIn…), la réutilisation de mots de passe aisément mémorisables est une pratique courante. C'est le principal enseignement d'un sondage réalisé par la société d'études Lab42 pour le gestionnaire de mots de passe LastPass.
L'enquête a été menée en mai dernier auprès d'un échantillon de 2000 internautes majeurs dans 6 pays : France, Allemagne, Royaume-Uni, États-Unis, Nouvelle Zélande et Australie.

Déni et prise de risque

Malgré la compréhension du risque (pour 91 % du panel), 61 % des internautes interrogés réutilisent les mêmes mots de passe sur différents comptes, sites et services en ligne. Autre enseignement du sondage : l'oubli d'un mot de passe est la principale raison à l'origine d'un changement. Seulement 29 % des personnes interrogées changent de mot de passe pour des raisons de sécurité.
La majorité rationalise le fait d'utiliser des mots de passe « *faibles* ». Près de la moitié des répondants (identifiés comme des personnalités de Type A par le Lab42) veulent garder le contrôle et mémoriser les mots de passe utilisés. Ils pensent ainsi ne pas être directement menacés.
En revanche, plus de 50 % des répondants (identifiés comme des personnalités de type B) disent limiter leur activité en ligne par crainte d'une violation de mots de passe. Ils parviennent à se convaincre que leurs données n'ont pas de valeur pour les hackers. Et maintiennent ainsi une approche distante, voire négligente en ce qui concerne la sécurité des mots de passe…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Mots de passe : le déni et la prise de risque exposés

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI

Yahoo a accepté sans combattre d'installer un logiciel sur ses serveurs, qui regarde le contenu des e-mails qui arrivent et transmet aux services de renseignement américains ceux qui peuvent les intéresser. Il est plus que temps de fermer son compte Yahoo.

L'agence Reuters a révélé mardi que les ingénieurs en charge du service des e-mails de Yahoo ont développé et mis en place en 2015 un logiciel qui scanne le contenu de tous les messages envoyés vers les centaines de millions de comptes Yahoo, pour copier et mettre à la disposition des autorités américaines ceux qui contiennent certaines chaînes de caractères intéressant les services de renseignement. L'ordre confidentiel, qui émanerait de la NSA ou du FBI et a été confirmé par quatre sources dont trois anciens employés de Yahoo, a été suivi sans que la direction de Yahoo le conteste.
C'est la découverte du bout de code qui aurait conduit le chef de la sécurité de Yahoo, Alex Stamos, à démissionner et partir chez Facebook en juin 2015. Ses équipes n'avaient pas été informées et il jugeait que le code mettait en danger la sécurité des utilisateurs…[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 le 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 : Yahoo espionne tous vos e-mails pour le compte de la NSA ou du FBI – Tech – Numerama

Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData Security Breach

Campagne de fraude ciblant les utilisateurs American Express

On n'apprend jamais des erreurs des autres, en tout cas, c'est qu'il faut croire après le nombre élevé d'utilisateurs American Express victimes de la plus récente attaque de phishing.

Les attaques de phishing ciblées deviennent de plus en plus difficiles à détecter. Voilà pourquoi il est important de toujours redoubler de vigilance dans la vérification d'adresses des expéditeurs, même si elles peuvent sembler venir de sources sûres. Dans l'escroquerie American Express, les pirates ont envoyé des e-mails en se faisant passer pour la société, et en reproduisant un modèle fidèle de mail de l'entreprise, ils sont allés jusqu'à créer un faux processus de configuration, pour installer une « clé personnel de protection personnel American Express.
Les e-mails frauduleux exhortent les clients à créer un compte pour protéger leur ordinateur contre les attaques de phishing -quelle ironie !-. Lorsque les utilisateurs cliquent sur le lien dans le mail, la page vers laquelle ils sont redirigées, leur demande des informations privées telles que le numéro de sécurité sociale, date de naissance, nom de jeune fille de la mère, date de naissance, e-mail et tous les détails de leurs cartes American Express, y compris les codes et la date d'expiration.
L'augmentation massive des attaques de ce type devrait sensibiliser les utilisateurs à ne jamais répondre à des e-mails suspects, mais il est toujours difficile de distinguer le vrai du faux, surtout si l'utilisateur n'est pas doué en informatique ou s'il ne maitrise pas bien l'Internet…[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 le 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

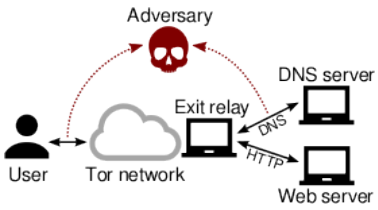
Original de l'article mis en page : Campagne de fraude ciblant les utilisateurs American Express – Data Security BreachData

Désanonymiser Tor. Possible ?

Désanonymiser Tor. Possible ?

Des chercheurs ont étudié la variante d'une attaque par corrélation permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. « DefecTor » est centrée sur les requêtes DNS.

Des chercheurs de Princeton, aux État-Unis, et des universités Karlstad et KTH, en Suède, ont étudié la faisabilité d'une méthode permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. Leurs travaux orientés sur le DNS sont en ligne (*« The Effect of DNS on Tor's Anonymity »*).
L'attaque nommée DefecTor est une variante d'une attaque par corrélation centrée sur les requêtes DNS (Domain Name System). Elle est possible car Tor Browser, le navigateur qui permet aux internautes d'accéder au réseau Tor, regroupe et chiffre le trafic HTTP et le trafic DNS. Ensuite la requête DNS est traitée au niveau du noeud de sortie, et le trafic HTTP est envoyé vers sa destination…[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 le 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.

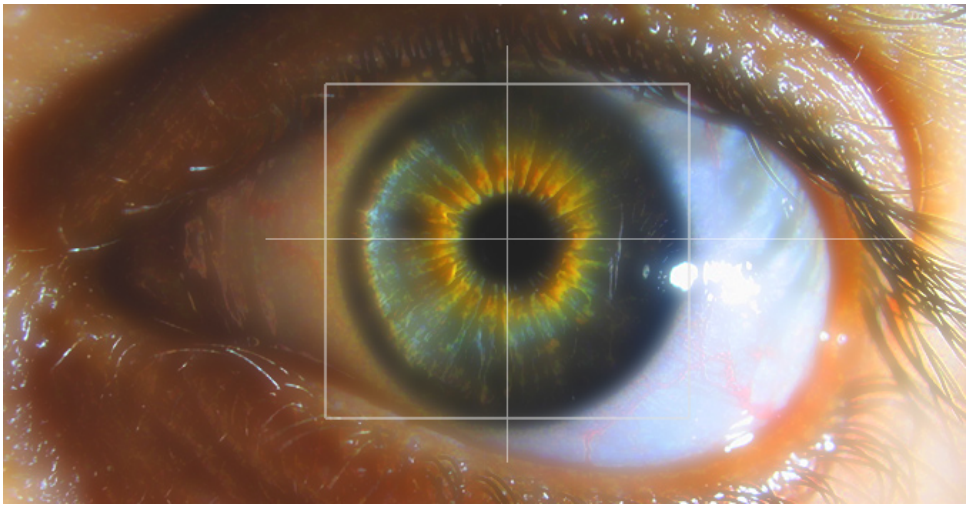
Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : DefecTor : s'appuyer sur

MasterCard déploie le paiement par selfie



MasterCard déploie le paiement par selfie

Après une phase de test dans quelques pays, le paiement par selfie imaginé par MasterCard se déploie en Europe.

C'est une procédure que vous connaissez forcément si vous avez déjà eu l'occasion d'effectuer un achat en ligne. Au moment du paiement, la boutique vous demande de renseigner les informations de votre carte bancaire (son numéro, sa date d'expiration et son cryptogramme visuel).
Une fois ces informations envoyées, votre banque est censée vous envoyer un SMS de confirmation contenant un code qu'il faut inscrire sur le site du marchand afin de valider définitivement la transaction. Cette mesure est nécessaire en cas de vol de la carte, afin de neutraliser toute tentative d'utilisation frauduleuse.
Avec l'envoi d'un code par texto (ou par mail), le client limite déjà beaucoup le risque de se faire avoir. Mais la méthode ne contre pas 100 % des menaces. Des fraudeurs très motivés et compétents peuvent modifier le numéro de téléphone censé recevoir le code ou accéder à la boîte mail pour y recevoir le courrier de validation. C'est en ayant ces problématiques en tête que MasterCard tente une autre approche, avec l'utilisation du selfie.

Évidemment, des interrogations apparaissent : que se passe-t-il si on utilise une photo de moi ? MasterCard dit avoir trouvé une parade en demandant à l'usager, pendant le selfie, de cligner des yeux. Et si une vidéo de moi est utilisée alors ? La parade pourrait être plus difficile à trouver, mais encore faut-il que le fraudeur puisse obtenir une vidéo de la victime, de face, en train de cligner des yeux. Or, elle n'existe peut-être pas.
Et quid des données biométriques qui sont par nature hautement sensibles ? MasterCard assure au Figaro qu'aucune information de cette nature n'est récupérée par le groupe sous sa forme originale. Manifestement, l'image est convertie en une sorte de signature numérique, qui est ensuite transmise à l'entreprise sans que celle-ci ne soit en mesure de faire le chemin inverse pour reconstituer le visage…[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 le 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 : Le paiement par selfie de MasterCard se déploie en Europe – Tech – Numerama

---

Alerte : Des bases MySQL menacées par une faille zero-day

Alors que les vulnerabilités zero-day sont de plus en plus fréquentes, voilà que l'une d'elles a été découverte pas n'importe où mais bel et bien dans la célèbre base de données MySQL. Rendue publique il y a quelques heures seulement, cette faille zero-day, si elle est exploitée, peut permettre à un attaquant d'exécuter du code malveillant.

Les serveurs MySQL exposés aux menaces

Il y a quelques heures, c'est le chercheur en sécurité Dawid Golunski qui a rendu public une drôle de découverte, à savoir une faille zero-day dans les bases de données MySQL.

Aussi, tous les serveurs MySQL paramétrés en configuration par défaut et les bases de données MariaDB et PerconaDB sont potentiellement exposés à des menaces. Eh oui, l'exploitation de la faille peut permettre assez simplement de modifier le fichier de configuration MySQL et donc d'exécuter une bibliothèque dont le pirate a préalablement pris le contrôle grâce aux privilèges « root ».

Cet exploit peut être exécuté dès lors que l'attaquant dispose d'une connexion authentifiée au service MySQL ou bien par injection SQL. Pourtant, il semblerait que la faille soit connue d'Oracle, qui a en charge le développement et le support de cette base de données, depuis maintenant plus d'un mois et demi.

Une faille zero-day véritablement dangereuse ?

Comme à chaque fois qu'une faille zero-day est découverte, la première préoccupation est de savoir si la menace qu'elle fait naître est importante ou non. A cette question, les réponses divergent.

Il faut dire que tout le monde ne semble pas d'accord sur la nature même de la faille. Pour certains, il s'agirait d'une vulnérabilité par escalade de privilèges et pas, comme l'a décrit Dawid Golunski, d'une vulnérabilité par exécution de code à distance.

Ainsi, il semble exister des solutions temporaires pour protéger au moins partiellement les bases de données mais tout le monde est unanime pour dire que la livraison de correctifs par Oracle, et ce dans le meilleur délai possible, se fait attendre avec beaucoup d'impatience du côté des administrateurs serveurs…[lire la source]

Réagissez à cet article

Original de l’article mis en page : Des bases MySQL menacées par une faille zero-day

---

Une série de clics suffisent à vous identifier

Une série de clics suffisent à vous identifier

Corréler l'historique des pages Web visitées aux profils Twitter permet d'identifier les internautes, expliquent des chercheurs de Princeton et de Standford. Ou quand le Big Data vient lever ce qui restait d'anonymat sur le Web.

L'anonymat sur Internet, un vœu pieux ? C'est en somme la démonstration d'une équipe de chercheurs des universités de Princeton et Standford. Ces derniers ont imaginé une extension pour le navigateur Chrome qui permet aux utilisateurs de prendre conscience de l'intérêt des traces qu'ils laissent sur le Net pour des publicitaires ou des espions. L'utilitaire, appelée Footprints, collecte les liens cliqués par l'utilisateur au cours des 30 derniers jours et, à partir de ces seules informations, renvoie une liste de 15 profils Twitter susceptibles de coller à cet usage. Ensuite, l'extension s'efface d'elle-même, assurent les chercheurs.
Professeur assistant à l'université de Standford, Sharad Goel explique que l'objectif de cet outil est avant tout éducatif : « *nous n'envisageons pas de rendre cet outil accessible à d'autres, il s'agit avant tout de réveiller les consciences.* » Un outil de ce type permettrait par exemple à une entreprise traçant déjà ses utilisateurs – soit la totalité des sites marchands notamment – de deviner l'identité des internautes, par corrélation avec leur usage d'un réseau social. En effet, si les publicitaires ou les spécialistes du marketing analysent déjà les traces laissées par les utilisateurs pour personnaliser l'expérience des clients online, ils ne sont en général pas en mesure de remonter jusqu'à l'identité réelle de l'internaute. Les chercheurs montrent que cette anonymat déjà tout relatif pourrait en pratique être levé, grâce à des analyses statistiques et au Big Data.

Dis-moi ce que tu cliques, j'en déduirai qui tu es

Dans un billet de blog, une étudiante de Standford ayant participé à la conception de Footprints, Jessica Su, explique le principe de la méthode : « *Partant de la combinaison unique de pages Web qu'un individu a visitées, nous déterminons les fils de réseau social similaires à cet historique, calculant une liste d'utilisateurs qui ont toutes les chances d'avoir produit cette série de clics. De cette façon, nous pouvons relier l'identité réelle d'une personne à un jeu de liens visités, y compris les liens qui n'ont jamais été postés publiquement sur aucun réseau social.* »…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Une série de clics et Twitter suffisent à vous identifier

---

Le code source d’un puissant programme d’attaques informatiques rendu public

Le code source d’un puissant programme d’attaques informatiques rendu public

---

Jeudi 22 septembre, le blog d'un célèbre spécialiste en sécurité informatique, Brian Krebs, était victime d'une des attaques informatiques les plus puissantes jamais recensées. Samedi 1er octobre, celui-ci a annoncé que le code source du programme ayant permis cette attaque avait été publié en ligne. « Ce qui garantit quasiment qu'Internet sera bientôt inondé d'attaques », prévient-il sur son site.

L'attaque en question était de type DDoS, ou « déni de service ». Elle consiste à saturer un serveur de requêtes afin que celui-ci ne soit plus en mesure de répondre. Celle subie en septembre par Brian Krebs était exceptionnelle par son ampleur : le volume de trafic envoyé vers son site a été estimé à environ 620 gigabits par seconde, alors que les attaques les plus violentes de ces dernières années culminaient à 300 Gbits/s.

Pour parvenir à un tel résultat, les auteurs de l'attaque ont utilisé un « botnet », un réseau de machines ne leur appartenant pas qu'ils ont piratées afin de les faire agir à leur guise. Une méthode classique, mais celle-ci a une particularité : les machines en question n'étaient pas, comme souvent, des ordinateurs, mais des objets connectés, comme des caméras de surveillance. Une cible relativement facile pour les pirates puisque ces objets, connectés en permanence, sont souvent mal sécurisés.

i m a g e :
http://s2.lemde.fr/image/2016/10/03/534x0/5007349_6_8042_2016-10-03-6ab49ca-14116-wlu2v0_5182276b854a344ebf95edab19e0b1b8.png

De nouvelles attaques à prévoir

Le code source du programme ayant permis de constituer et de piloter ce botnet a été divulgué vendredi 30 septembre sur un forum fréquenté par des hackeurs, par un utilisateur se faisant appeler *« Anna-Senpai »*, affirme Brian Krebs. *« Quand je me suis lancé dans le DDoS, je n'avais pas l'intention d'y rester longtemps*, écrit cet utilisateur dans le message accompagnant son geste. *J'ai fait de l'argent, de nombreux regards se tournent désormais vers l'Internet des objets, il est donc temps de GTFO »* (*« Get The Fuck Out »*, à savoir : partir)…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Le code source d'un puissant programme d'attaques informatiques rendu public

La Métropole de Lyon touchée par un virus informatique

La Métropole de Lyon touchée par un virus informatique

Les services du Grand Lyon sont touchés depuis jeudi, en fin d'après-midi, par un virus informatique. Un mail reçu, comportant un fichier Excel, serait à l'origine du problème.Il est demandé aux usagers d'être vigilants et de ne pas ouvrir de mails suspects.Le nettoyage est en cours et tout devrait être rétabli dans la journée.

Denis Jacopini anime des **conférences et des formations** et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **CyberRisques** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).
Nous animons **conférences et formations** pour sensibiliser décideurs et utilisateurs **aux risques en informatique**, découvrir et comprendre les **arnaques** et les **piratages informatiques** pour mieux s'en protéger et se **mettre en conformité avec la CNIL** en matière de **Protection des Données Personnelles**. Nos actions peuvent être personnalisées et organisées dans votre établissement.
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

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 : Lyon | La Métropole touchée par un virus informatique

---

4.5 MILLION PEOPLE FORCED TO

CANCEL CREDIT & DEBIT CARDS IN THE LAST YEAR DUE TO ONLINE FRAUD

One in ten people have been the victim of a cyber-attack on their credit or debit card in the last year, according to new research from comparethemarket.com. In 62% of cases, money was successfully removed from the account with an average of £475 stolen. At a national level this equates to 4.…[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.

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

Contactez-nous

Réagissez à cet article