Attaque informatique par Clé USB piégée, plus fréquente qu’il n’y parraît

	Attaque informatique par Clé USB piégée, plus fréquente qu’il n’y parraît

Attaque informatique via votre boîte aux lettres ! La police Australienne alerte les citoyens de Melbourne après la découverte de clés USB piégées distribuées dans des boites aux lettres.

Voilà une attaque informatique, couplée à du social engineering, qui laisse songeur. La police fédérale de l'État de Victoria [Australie] a mis en garde les habitants de la banlieue de Pakenham (région de Melbourne) de ne surtout pas utiliser la clé USB qui a pu leur être proposée. Une clé USB diffusée dans un courrier, placé directement dans leur boite aux lettres. L'avertissement que j'ai repéré dans le site officiel de la Police locale indique que « ***Les lecteurs USB sont considérés comme extrêmement dangereux et le public est invité à ne pas les brancher sur leurs ordinateurs ou d'autres appareils informatiques.***«
Il a été constaté que la clé USB mystérieuse lançait des processus dans les ordinateurs comme l'installation d'outils dédiés à des abonnements malveillants. Même si les clés USB ont été détectées dans un seul quartier, la police de Victoria a néanmoins jugé bon d'émettre une alerte à l'échelle de l'État…[lire la suite]

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 : ZATAZ Attaque informatique : Clé USB piégée dans votre boîte aux lettres – ZATAZ

Enfin une idée pour suivre en temps réel la localisation des avions

Enfin une idée pour suivre en temps réel la localisation des avions

Une constellation de satellites pour pister les avions où qu'ils soient. Tel est le projet de deux sociétés américaines qui vont placer des récepteurs dans des satellites qui seront mis en orbite très prochainement.

C'est une question qui taraude systématiquement l'industrie aéronautique à chaque fois qu'un avion disparaît mystérieusement sans laisser la moindre trace : comment aurait-on pu améliorer le suivi de l'appareil ? À cette question, les progrès techniques ont déjà fourni au fil du temps des réponses qui ont fortement amélioré la qualité du contrôle du trafic aérien.
Mais ce n'est évidemment pas suffisant. Il y a à peine plus de deux ans, le vol MH370 de la Malaysia Airlines sortait de son plan de vol initial – l'avion, un Boeing 777, devait relier Kuala Lumpur à Pékin – pour s'abîmer quelque part dans l'océan Indien. La carcasse principale n'a jamais été retrouvée. Seuls quelques débris charriés au gré des courants ont fini par échouer sur les côtes.

DES SATELLITES EN ORBITE BASSE À LA RESCOUSSE

C'est pour éviter la répétition de ce scénario que deux sociétés américaines œuvrent sur un dispositif consistant à placer des récepteurs ADS-B (automatic dependent surveillance-broadcast) dans des satellites situés en orbite terrestre basse, à une altitude d'environ 780 km. Les deux entreprises, FlightAware et Aireon, anticipent une mise en service aux alentours de 2018.
« *Cela n'aura pas d'importance que le vol se trouve au-dessus de l'océan, d'un désert ou du Pôle Nord, nous saurons où est l'avion* », commente, très confiant, Daniel Baker, le patron de FlightAware à Reuters. Selon les instigateurs du projet, il sera possible d'avoir un suivi des avions en quasi-temps réel, de manière à éviter que ne subsistent de trop longues plages de temps entre deux contacts automatiques de l'avion.

IRIDIUM NEXT

Ce sont des satellites de la future constellation Iridium NEXT qui seront utilisés pour accueillir les récepteurs ADS-B. Ces satellites, qui doivent être au nombre de 70 (66 actifs et 4 de réserve), doivent être mis en orbite par SpaceX au cours de sept missions distinctes devant décoller de la base de l'Air Force Vandenberg en Californie.
C'est la fusée Falcon 9 qui sera utilisée. Au départ, il était prévu que les vols démarrent à la fin 2016. Toutefois, les premiers décollages risquent d'être reportés à cause de l'explosion d'un lanceur au début du mois de septembre. Le groupe a toutefois une piste sur l'origine de la catastrophe et se dit persuadé de pouvoir reprendre ses missions dès novembre… pile pour les vols des satellites Iridium NEXT.
Le cas du vol MH370 n'a pas uniquement nourri la réflexion de FlightAware et Aireon. Du côté du conseil de l'organisation de l'aviation civile internationale (OACI), une série de modifications a été proposée ce printemps pour pister plus efficacement un aéronef en détresse dans des zones isolées. Il est en particulier question de pouvoir obtenir la localisation de l'avion toutes les minutes…[lire la suite]

Réagissez à cet article

Original de l’article mis en page : Des satellites pour suivre en permanence la localisation des avions – Tech – Numerama

---

Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

Alerte, découverte d’un virus qui se propage principalement via les Réseaux Sociaux

---

Afin de voler leurs données, le malware utilise une campagne de diffusion massive ciblée en renvoyant les victimes vers un site gouvernemental libyen compromis et contenant le malware

Malgré le manque de sophistication du malware et un mécanisme de propagation rudimentaire, les auteurs de cette menace ont démontré qu'ils étaient capables de compromettre des sites gouvernementaux avec succès.
Au cours de leurs recherches, les **experts ESET** ont découvert que les attaquants compromettent des profils de réseaux sociaux (Facebook, Twitter…) et postent des liens amenant au téléchargement de logiciels malveillants. Le post est rédigé en arabe et explique : « le premier ministre a été capturé à deux reprises, dont cette fois-ci dans une bibliothèque ».

Ce message texte relativement court est suivi d'un lien vers le site gouvernemental compromis.

Figure 1 : Post sur Facebook renvoyant vers un lien comportant le malware

En plus de la diffusion massive de cette campagne, les cybercriminels mènent des attaques ciblées par l'envoi d'e-mail contenant une pièce jointe malveillante de type spearphishing. Pour convaincre les victimes d'exécuter le code malveillant, des astuces d'ingénierie sociale sont mises en œuvre, comme l'utilisation d'icônes MS Word et PDF à la place de celles des exécutables et de techniques de double extension dans les noms de fichier, comme .pdf.exe. Dans certains cas, le malware peut afficher un document leurre.
Les experts ESET ont identifié le malware comme appartenant à la famille des Chevaux de Troie qui tentent de recueillir diverses informations par le vol de données classiques. Il peut être déployé sous plusieurs configurations. **La version complète du logiciel malveillant peut enregistrer les frappes de clavier, collecter des fichiers de profil des navigateurs Mozilla Firefox et Google Chrome, enregistrer des sons à partir du microphone, réaliser des captures d'écran depuis la webcam, et recueillir des informations sur la version du système d'exploitation et du logiciel antivirus installé.** Dans certains cas, le logiciel malveillant peut télécharger et exécuter des outils tiers de récupération de mots de passe enregistrés à partir d'applications installées.
« Nous avons analysé un échantillon de ce malware qui est actif depuis au moins 2012 dans des régions spécifiques du globe. Par le passé, les auteurs de cette cybermenace utilisaient ce malware pour une diffusion massive. Il convient de noter qu'il est encore utilisé dans des attaques de spearphishing », explique Anton Cherepanov, malware researcher chez ESET.
Pour plus de détails sur ce malware, cliquez ici.
Source : ESET

Réagissez à cet article

Original de l’article mis en page : Boîte de réception (10) – denis.jacopini@gmail.com – Gmail

---

Un utilisateur de Yahoo! poursuit le groupe pour « négligence »

Un utilisateur de Yahoo! poursuit le groupe pour « négligence »

Le plaignant regrette que les mesures de sécurité du groupe n'aient pas été renforcées. Il s'autoproclame représentant des utilisateurs lésés par le vol de données.

Après l'annonce, jeudi 22 septembre, du piratage d'au moins 500 millions de comptes d'utilisateurs de Yahoo!, le groupe est désormais poursuivi pour « *négligence grave* » à la suite de la plainte d'un utilisateur. Le groupe de Sunnyvale (Californie) fait face à un certain nombre de questions relatives à sa gestion de l'incident.
La plainte a été déposée vendredi auprès du tribunal fédéral de San Jose (Californie), par Ronald Schwartz, un résident de New York qui entend représenter tous les utilisateurs américains de Yahoo! affectés par le vol de leurs informations personnelles.
L'opérateur de services Internet a annoncé, la veille, que les données volées pourraient inclure des noms, des adresses emails, des numéros de téléphone, des dates de naissance et des mots de passe cryptés. Il a exclu à ce stade le vol de données bancaires dans ce qu'il présente comme une attaque menée par un « *agent piloté par un Etat* », sans apporter de preuve de cette hypothèse. L'action en justice vise le statut de recours collectif (« *class action* ») et entend réclamer des dommages et intérêts.
Selon le plaignant, le piratage aurait pu être évité si le groupe avait renforcé ses mesures de sécurité après plusieurs précédentes tentatives d'effraction. Il déplore également la lenteur de Yahoo!, qui aurait, selon lui, mis trois fois plus de temps que ses concurrents pour faire état du piratage…[lire la suite]

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

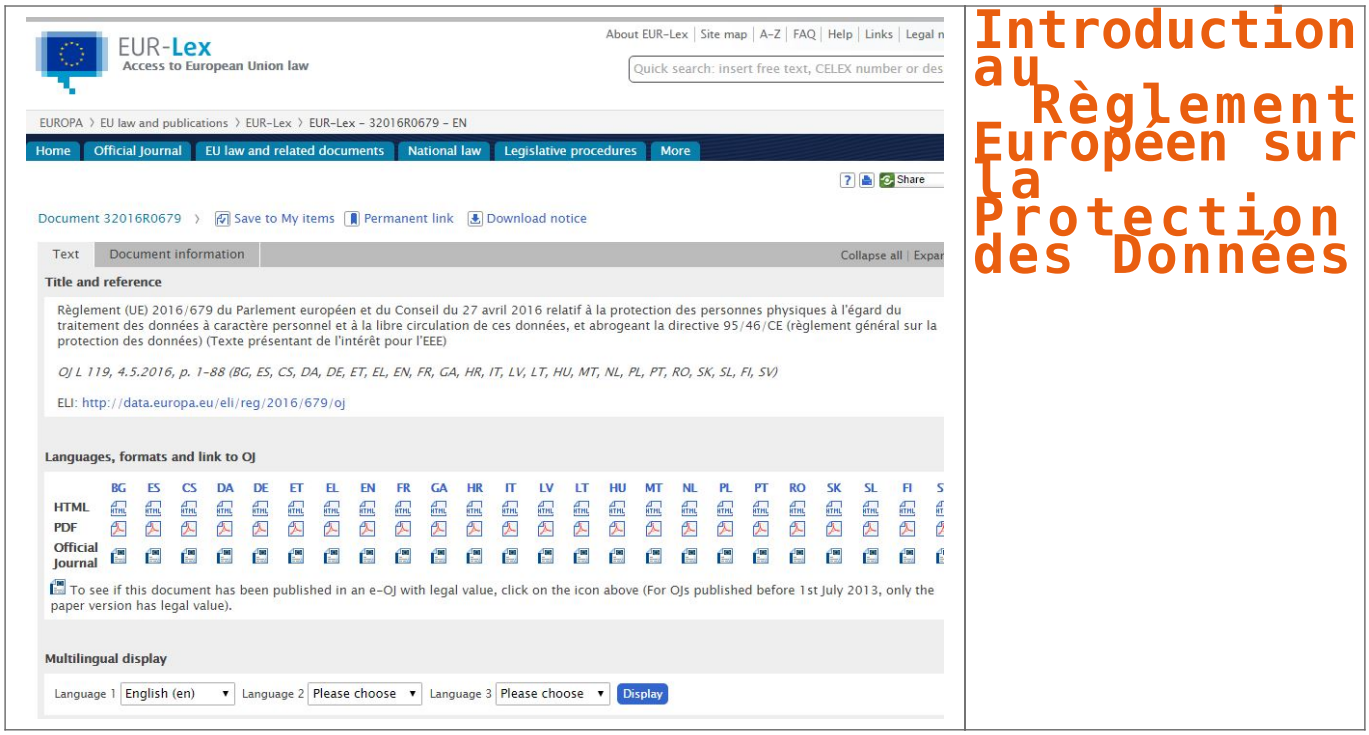
Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Piratage massif : Yahoo!

poursuivi pour « négligence » par un utilisateur

Introduction au Règlement Européen sur la Protection des Données



Introduction au Règlement Européen sur la Protection des Données

Le Règlement Général de l'Union Européenne sur la Protection des Données (RGPD) impose aux entreprises d'effectuer un suivi de toutes les occurrences des données à caractère personnel des clients au sein de leur organisation, d'obtenir le consentement des clients concernant l'utilisation de leurs informations personnelles (y compris le « droit à l'oubli ») et de documenter l'efficacité de cette gouvernance des données pour les auditeurs.

Deux tiers (68 %) des entreprises, selon Compuware, risquent de ne pas être en conformité avec le RGPD, en raison d'une augmentation de la collecte des données, de la complexité informatique grandissante, de la multiplicité des applications, de l'externalisation et de la mobilité. Ce risque tient aussi aux politiques laxistes concernant le masquage des données et l'obtention d'une autorisation explicite des clients en matière de données. Les entreprises européennes comme américaines doivent, par conséquent, adopter une série de bonnes pratiques, notamment un masquage plus rigoureux des données de test et de meilleurs pratiques concernant le consentement des clients, afin d'éviter des sanctions financières et une altération possible de leur image de marque résultant d'une non-conformité.
Le RGPD de l'Union européenne a été adopté en avril 2016, afin d'unifier des obligations auparavant réparties à travers différentes juridictions européennes concernant l'utilisation, la gestion et la suppression des informations personnellement identifiables (IPI) des clients par les entreprises. Toutes les entreprises dans l'UE, aux États-Unis et ailleurs, qui collectent des IPI relatives à des citoyens de l'UE, ont jusqu'en mai 2018 pour se conformer à ces dispositions. Tout non-respect du RGPD expose les entreprises à des amendes pouvant atteindre 20 millions € ou 4 % du chiffre d'affaires mondial….[lire la suite]

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

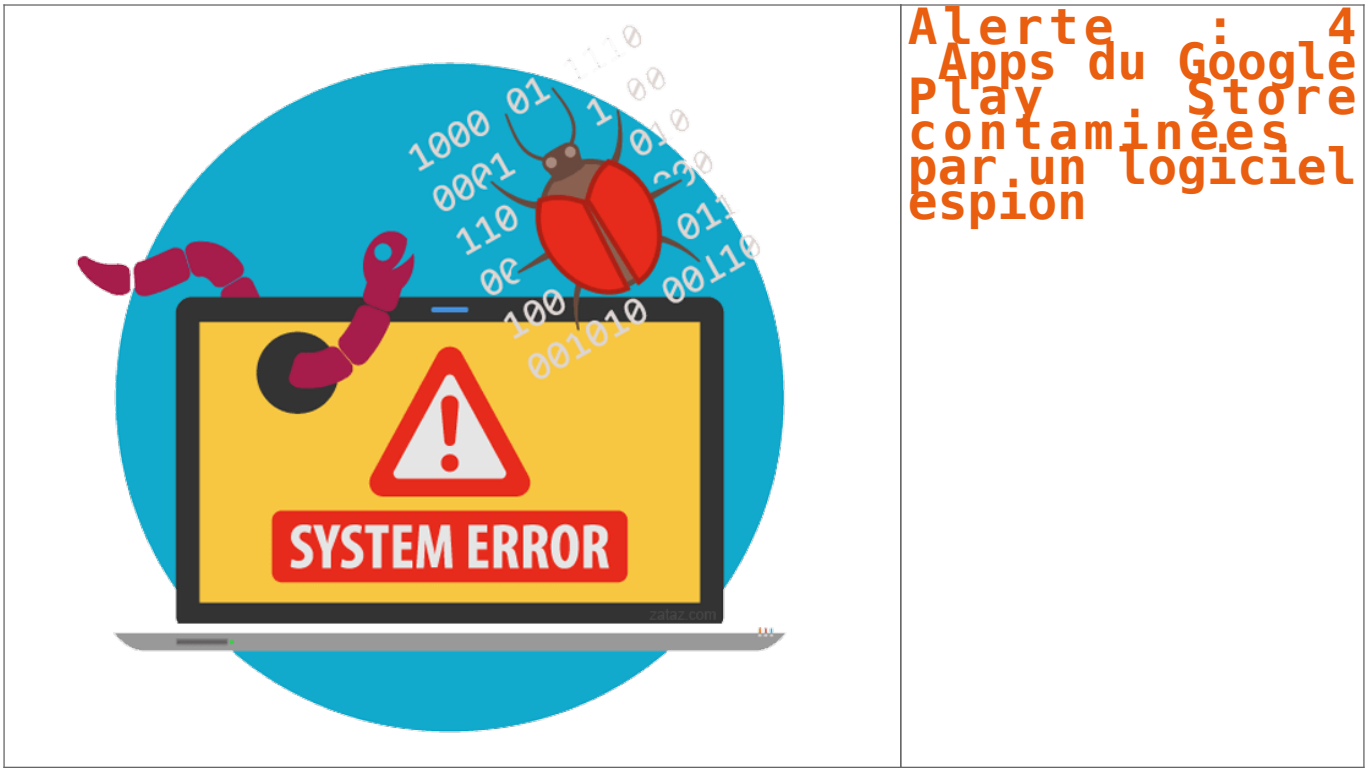
Contactez-nous

Réagissez à cet article

Original de l’article mis en page : Retour sur le RGPD, le Règlement Général de l’Union Européenne sur la Protection des Données – Data Security BreachData Security Breach

---

Alerte : 4 Apps du Google Play Store contaminées par un logiciel espion



Alerte : 4 Apps du Google Play Store contaminées par un logiciel espion

---

Quelques semaines seulement après avoir alerté Apple sur le logiciel espion PEGASUS qui avait trouvé une faille TRIDENT pour s'infiltrer sur IOS, l'équipe de veille et de recherche de Lookout Mobile Security, annonce avoir découvert un logiciel espion qui a attaqué plusieurs Apps sur Google Play Store.

Le spyware appelé OVERSEER, a été identifié sur quatre applications, dont une, Embassy, qui permettait aux voyageurs de rechercher des Ambassades à l'étranger. Ce malware a aussi été injecté sous forme de Trojan dans des applications de diffusion actualités Russes et Européennes. Google a promptement retiré les quatre applications infectées après avoir été prévenu par Lookout.
OVERSEER est un spyware qui cible par exemple grâce à Embassy, les grands voyageurs avec la fonction principale d'effectuer des recherches d'adresses d'Ambassades à travers le monde. Les personnes en voyages d'affaires, qui voyagent régulièrement, peuvent être particulièrement vulnérables à une telle attaque en installant sur leur téléphone l'application…[lire la suite]

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 : Un nouveau logiciel espion OVERSEER s'attaque aux Apps du Google Play Store – Data Security BreachData Security Breach

Signes indiquant qu’un compte a été piraté et procédure à suivre

Signes indiquant qu’un compte Yahoo a été piraté et procédure à suivre

Nous espérons que vous n'aurez jamais à craindre qu'une autre personne accède à votre compte sans votre autorisation, mais vous ne pouvez jamais être sûr à 100 % de la sécurité de votre compte. Voici comment déterminer si une autre personne s'est connectée à votre compte Yahoo et les étapes à suivre pour récupérer l'accès à celui-ci.

Quelle que soit la situation, si vous pensez qu'une autre personne a accédé à votre compte sans votre autorisation, **changez votre mot de passe immédiatement**. Si vous n'avez pas accès à votre compte, utilisez l'aide relative aux mots de passe pour le récupérer.

Signes indiquant que votre compte a été piraté

• Vos informations de compte ont été modifiées à votre insu.
• Des connexions ont été établies depuis des endroits que vous ne reconnaissez pas sur la page de vos activités de connexion.
• Vous ne recevez pas des e-mails que vous attendiez.
• Votre compte Yahoo Mail envoie des spams

Ce que vous devez faire

Bloquer l'envoi de spam depuis votre compte

Recevoir des spams est une chose. Recevoir des rapports de spam provenant de votre compte en est une autre. Si votre compte a été piraté de sorte qu'il envoie des spams, vous pouvez résoudre ce problème ! Le moyen le plus rapide de bloquer l'envoi de spams depuis votre compte consiste à sécuriser votre compte en créant un nouveau mot de passe fiable ou activer la clé de compte.

Signaler un mail falsifié (usurpé)

Les messages falsifiés sont des mails qui semblent avoir été envoyés depuis votre adresse mail, mais qui en réalité ont été envoyés depuis un compte de messagerie complètement différent. Si votre Yahoo Mail est sécurisé, mais que vos contacts reçoivent toujours des spams qui semblent provenir de votre adresse, il s'agit probablement d'un mail falsifié ou « usurpé ».

1. Affichez l'en-tête complet du mail en question.
2. Dans la dernière ligne Reçu de l'en-tête complet, notez l'adresse IP d'où provient le mail.
– Cela correspond au fournisseur d'accès Internet (FAI) de l'expéditeur.
3. Effectuez une recherche par adresse IP sur un site tel que WhoIs.net pour déterminer le fournisseur d'accès Internet de l'expéditeur.
4. Contactez le fournisseur d'accès Internet de l'expéditeur pour demander que l'action appropriée soit entreprise.

Les fournisseurs de messagerie ne peuvent pas empêcher ces contrefaçons, mais si la fraude est identifiée, il est possible d'entreprendre une action.

Examinez les paramètres Yahoo Mail

• Supprimez les contacts mail inconnus.
• Supprimez les comptes Mail liés que vous ne reconnaissez ou ne contrôlez pas.
• Changer votre mot de passe sur les comptes liés que vous contrôlez.
• Vérifiez que votre réponse automatique de congés est désactivée.
• Découvrez si une autre personne a accédé à votre compte.

Autres paramètres de compte Yahoo Mail habituellement modifiés :

• Signature
• Nom d'expéditeur
• Adresse de réponse
• Transfert de mails
• Filtres
• Adresses interdites

Restaurer les mails, messages instantanés et contacts manquants

Si des mails, des messages instantanés ou des contacts sont manquants, vous pouvez restaurer les mails ou messages instantanés perdus ou supprimés. Vous pouvez également récupérer les contacts perdus.

Empêchez d'autres personnes d'accéder à nouveau à votre compte, même après avoir modifié votre mot de passe. Assurez-vous que votre compte reste protégé.

Recherchez la présence de logiciel malveillant sur votre ordinateur

Les logiciels malveillants peuvent corrompre votre système et collecter des informations sensibles, telles que des mots de passe et des coordonnées bancaires. Plusieurs programmes anti-logiciel malveillant sont disponibles sur Internet et permettent de détecter et de supprimer les logiciels malveillants sur les Mac et PC.

Réagissez à cet article

Original de l'article mis en page : Signes indiquant qu'un compte a été piraté et procédure à suivre | Yahoo Aide – SLN2090

Toutes les 4 secondes, un nouveau malware téléchargé

Toutes les 4 secondes, un nouveau malware est téléchargé

Selon Check Point, les téléchargements de logiciels malveillants inconnus ont été multipliés par 9 dans les entreprises. La faute aux employés ?

Dans leur rapport de sécurité 2016, les chercheurs de Check Point ont analysé plus de 31 000 incidents cyber touchant plusieurs milliers d'entreprises dans le monde. Résultat des courses : les téléchargements de logiciels malveillants explosent dans les entreprises.
L'an dernier, les téléchargements de malwares encore « inconnus » des systèmes de sécurité d'organisations ont été multipliés par 9, passant de 106 à plus de 970 téléchargements par heure, selon Check Point. En moyenne, un nouveau programme malveillant inconnu est téléchargé toutes les quatre secondes. Et les employés sont présentés comme le maillon faible dans ce domaine.

Maillon faible

Les malwares « connus » font également des dégâts (un téléchargement toutes les 81 secondes en moyenne) lorsque les systèmes sont irrégulièrement mis à jour et que les correctifs de sécurité font défaut. Une variante d'un programme malveillant peut aussi confondre un antivirus, au risque d'exposer les systèmes et réseaux d'une entreprise à l'espionnage et au vol de données…[lire la suite]

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 : Un nouveau malware téléchargé toutes les 4 secondes

Comment Facebook manipule le contenu qu’il nous affiche ?

Comment Facebook manipule le contenu qu’il nous affiche ?

Censure d'une photo historique, choix d'articles qui renforcent les partis pris: les centaines de millions d'internautes qui s'informent via leurs «amis» sur Facebook, plutôt que par les médias classiques, courent le risque d'une information biaisée, selon des experts.

Dernier exemple en date, la censure par Facebook la semaine dernière de la célèbre photo d'une petite Vietnamienne nue brûlée au napalm, au nom de sa politique contre la nudité des enfants. Critiqué dans le monde entier, le groupe américain a rétabli la photo et promis de tenir compte à l'avenir du «statut d'icône» des clichés historiques.
Cette polémique a révélé l'importance prise par Facebook comme source d'information pour une majorité d'internautes dans le monde.
Un sondage international du Reuters Institute montre que 51% des personnes interrogées dans 26 pays s'informent par les réseaux sociaux, dont 44% par Facebook, et que 12% en ont fait leur première source d'information. En France, un Français sur deux consulte Facebook, surtout sur mobile, et peut y passer plusieurs heures par semaine.
Aucun des 1,7 milliard d'utilisateurs ne voit les mêmes informations dans son «newsfeed» (fil d'actualités), qui compile les messages de ses «amis»: un mélange de commentaires personnels et d'articles partagés, provenant aussi bien de grands médias que de blogues inconnus.
Entre les milliers de messages produits par ses amis, impossible de tout lire: c'est l'algorithme de Facebook qui, pour chacun, classe ceux placés en haut de page. Et donc ceux qui seront vus, car en moyenne l'utilisateur ne lit que 200 des 2000 messages de son fil.
Les utilisateurs ignorent le plus souvent l'existence et les critères de ce tri, qui ont changé sans cesse en 10 ans d'existence. En juin, Facebook a brusquement décidé de privilégier les messages personnels au détriment des partages d'articles, diminuant la place des médias classiques…[lire la suite]

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 : Comment Facebook filtre notre connaissance du monde | Laurence BENHAMOU | Internet

---

Yahoo victime de millions de comptes volés

Yahoo victime de millions de comptes volés

Selon la presse américaine, le portail web pourrait bientôt confirmer le vol de plus de 200 millions de comptes. Un hiatus dans la phase de rachat de Yahoo par Verizon.

L'année 2012 a bel et bien été une annus horribilis pour les services web. Beaucoup de vols de données ont eu lieu cette année-là. Mais à l'époque, la plupart des services touchés avait relativisé, voire minimisé le nombre de comptes compromis.
Depuis quelques mois, le passé les rattrape et un pirate du nom de « Peace » égrène sur le Dark Web des paquets contenant des données sur des millions de comptes issues de vols de 2012. On pense notamment aux 167 millions de comptes de Linkedin, 360 millions de comptes pour MySpace et 65 millions de Tumblr. Des doutes subsistent sur Dropbox qui a demandé à ses abonnés antérieurs à 2012 de changer leur mot de passe.
Mais au mois d'août dernier, Motherboard avait repéré sur le Dark Web une nouvelle vente de « Peace » concernant 200 millions de comptes Yahoo. Ces données vendus 3 bitcoins (soit environ 1800 dollars) peuvent contenir les noms d'utilisateurs, les mots de passe hachés avec l'algorithme MD5. Mais aussi les dates de naissance et, parfois, une adresse e-mail de secours…[lire la suite]

Réagissez à cet article

Original de l'article mis en page : Yahoo va-t-il reconnaître le vol de 200 millions de comptes ?