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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Propos recueillis par Chloé Chouraqui

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

Denis JACOPINI anime dans toute 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 : Données personnelles en danger : pourquoi il est très important de supprimer vos comptes en ligne que vous n’utilisez plus (et pas seulement de les fermer) | Atlantico.fr