Piratage adresse mail

Votre adresse mail ou celle d'une de vos connaissances peut être piratée et personne n'est à l'abri. Lorsqu'un pirate accède au compte mail de sa victime, cela signifie qu'il en connaît le mot de passe. Il peut ainsi librement consulter les mails de la boîte de réception, le carnet d'adresses et les éventuels services complémentaires.

Qui pirate et comment ?

Pour la pirater, votre adresse mail doit être identifiée. A force de **laisser nos adresses mail sur le web** (sites commerciaux, sites marketing, réseaux sociaux, forums, messageries instantanées, etc.), elles finissent par tomber **entre de mauvaises mains**. Une autre cause est l'envoi de message en groupe où les adresses mail figurent en clair dans la liste des destinataires ou dans le contenu des messages. Pour connaître votre mot de passe, le pirate a alors plusieurs possibilités, soit vous envoyer un mail vous incitant à le donner, soit tenter de le découvrir.

Exemple d'Invitation

De: STAFF GESTION <sal.accardi@alice.it>
Objet: Chers Utilisateurs Facebook
Date: 12 novembre 2015 04:23:14 UTC+1
Répondre à: v_gestion.staff@yahoo.fr

Chers Utilisateurs,
Dans le cadre de l'installation définitive des nouveaux paramètres Facebook et de la réinitialisation de toutes nos adresses facebook, Il est procédé à un marquage de tous les comptes actifs à ce jour. Afin de ne pas risquer de perdre votre compte Facebook ! lors de l'expiration de notre précédant service de messagerie, vous êtes donc prié de bien vouloir remplir impérativement la grille d'information ci-dessous.
Passé le délai de 72 heures, nous procéderons à la suppression de toutes les comptes non encore enregistrées.
Informations obligatoires :
Nom Prénoms: ....
Date de naissance:.....
Sexe:.....
Adresse courriel :.....
Mot de passe:.....
Confirmation Mot de passe:.....
Adresse Secours:.....
Mot de passe:.....
Question sécrète:.....
Réponse sécrète:.....
…
Après avoir répondu au questionnaire et après vérification par nos services votre compte continuera de fonctionner normalement.
Nous vous remercions pour votre bonne compréhension et nous exerçons à améliorer nos services pour nos utilisateurs. Tout en nous excusant pour ces désagréments.
L'équipe Facebook.com ! Maintenance

Dans le précédent message, il s'agit de sécurité, cela peut être aussi l'annonce d'un gain. Attention aux messages qui contiennent aussi un lien vous invitant à vous connecter sur votre compte de messagerie ou votre banque, comme le suivant.

O-PEN NOUVELLE FONCTIONNALITE

Après plusieurs plaintes de multiples abonnées, toute l'équipe o-pen a décidé de procéder à une demande d'activité sur chaque compte afin de pouvoir supprimer les plus défaillants et infects.

Afin de bénéficier aussi de nos nouvelles fonctionnalités.Dans le but de mieux vous servir et toujours garder la confidentialité de vos données et messages .

Nous vous informons qu'un contrôle est dès à présent disponible.

Pour mener à bien cette opération veuillez vous rendre sur cette page > Clientèle.O'range pour votre authentification.

Conseils

- Regardez l'adresse de l'expéditeur et celle à laquelle la réponse sera envoyée, ces contacts n'ont en général aucun rapport avec le service qu'ils sont censés représenter.
- Ne vous connectez pas en utilisant les liens de ces mails suspects. Et si vous cliquez sur un lien, vérifiez que l'adresse du site correspond au bon domaine.
- Pour les sites sensibles tels que votre opérateur ou votre banque, utilisez directement votre navigateur et les procédures de connexion sécurisées prévues par le site.

Robot

Le pirate n'est pas forcément une personne à part entière, mais peut être un **robot logiciel** (bot). Ce robot utilisera **une attaque par dictionnaire pour rapidement identifier le code d'accès**.

Il s'agit d'une méthode utilisée pour trouver/deviner un mot de passe. Via un logiciel spécialisé, elle consiste à tester à grande vitesse tous les mots de dictionnaires (français, anglais, espagnol, etc.) en espérant qu'un des mots soit utilisé comme mot de passe. Auquel cas celui-ci est vite démasqué, notamment s'il est court. Les mots de passe tels que « maison », « skyscraper », « abanico », etc. sont donc à éviter pour protéger son ordinateur, sa boite mail, sa box, etc.

Comment savoir ?

Une fois le compte identifié, le pirate n'a plus qu'à rechercher dans le compte mail **toutes sortes d'informations** qu'il pourra réutiliser ou revendre : contacts mail, informations personnelles, identifiants, messages sauvegardés, etc.

La plupart du temps, ce sont vos proches qui vont vous alerter car ils recevront des mails de détresse souvent mal orthographiés et émis soit disant de votre part.

Exemples de messages de détresse

Bonjour,
J'espère que tu vas bien? Moi, je vais très mal, je suis au Portugal où j'ai eu de grave soucis (attaque physique)
Donne suite à mon mail dès que tu l'auras reçu stp. Je reste connecté, j'ai également perdu mon tel
Surtout garde ce mail pour toi stp.
J'ai besoin d'un service, peux tu te rendre chez un buraliste ce matin?
Réponds rapidement stp. Jean

Bonjour,
Dis-moi où es-tu? J'ai besoin que tu me rendes un service.
Contacte-moi par e-mail rapidement car c'est impossible de me joindre au téléphone.
René

Le but des pirates est d'obtenir une aide financière qu'il ne faut bien sûr pas donner.

Si vous recevez un message de ce genre, n'y répondez pas. Il est de grandes chances que le mot de passe du compte ait été modifié et votre ami ne pourra plus se connecter à sa messagerie.

Informez la personne par téléphone.

Que faire ?

Malheureusement, ce qui est fait est fait et vous ne pouvez pas revenir en arrière et empêcher le vol de vos informations.

Il est par contre possible de limiter la casse, et de prévenir tout autre piratage.
Il faut absolument faire en sorte que :

1. Le pirate ne se reconnecte plus au compte mail
2. Que les données volées ne puissent pas lui servir
3. Que d'autres pirates n'accèdent pas à votre espace personnel

Changer le mot de passe

Si possible, changez le mot de passe via les options de votre compte. Ainsi, vos anciens identifiants seront caduques, et le pirate ne pourra plus se reconnecter. Si vous ne pouvez plus accéder à votre compte, contactez l'opérateur qui vous communiquera un nouveau mot de passe par courrier.
Si vous modifiez le mot de passe, n'optez pas pour un mot de passe court et issu d'un dictionnaire. Il a toutes les chances d'être démasqué rapidement s'il est attaqué. Et ajouter un 01 pour le complexifier n'est pas très efficace. Choisissez plutôt un mot de passe long et complexe (mélange de majuscules, minuscules, chiffres, caractères de ponctuation).
Consultez les sites :

- 10 conseils pour un mot de passe solide
- Les mots de passe à éviter

Changer les mots de passe des comptes mentionnés dans les mails piratés

Peut-être que dans vos mails figurent des messages d'autres comptes, Paypal, CDiscount, Facebook, La Banque Postale ou divers forums par exemple. Or, sur ces plateformes, la plupart des utilisateurs choisissent comme identifiant leur adresse mail, et comme mot de passe, le **même code que pour leur compte mail** ! Ainsi, le mot de passe compromis du compte mail pourra servir au pirate pour se connecter à son compte Paypal… Changez donc rapidement tous vos mots de passe potentiellement corrompus.

Autres actions

- Envoyez un mail à tous vos contacts en CCI pour leur raconter votre mésaventure (éventuellement vous excuser), et leur conseiller d'adopter des mots de passe solides au plus vite : leur compte mail sera certainement une future cible.
- Utilisez un **logiciel de messagerie** qui vous permettra de stocker les adresses de vos contacts indépendamment de votre fournisseur de compte de messagerie.
- Supprimez les messages inutiles et videz la corbeille.
- Supprimez les contacts qui ne sont pas primordiaux pour vous.
- Réfléchissez à la manière dont vous gérez votre/vos mot(s) de passe, diversifiez-les en fonction de vos différents comptes (Facebook, Twitter, mail, sites commerciaux, etc.), et appliquez une **politique d'accès à vos espaces privés** plus sévère, même si cela doit être plus contraignant.
- Ne stockez pas les mots de passe dans vos mails, notez les si besoin dans un espace sécurisé.

A lire Votre identité numérique vaut de l'or !

Support des opérateurs

La plupart des opérateurs mettent en ligne les procédures à suivre lors de piratage d'adresse mail. Quelques sites :

- Google Récupérer un compte Gmail piraté
- Yahoo https://fr.aide.yahoo.com/kb/SLN2090.html
- Outlook http://windows.microsoft.com/fr-fr/windows/outlook/hacked-account

Informations sur le phishing ou hameçonnage :

- Assistance Orange
- Assistance SFR

Envoi en CCI (Copie Carbone Invisible)

Pour tout envoi de mails à un groupe de personnes, utilisez le champ **CCI** qui permet de respecter la vie privée de vos contacts (diffusion non voulue des adresses e-mail).
En effet, si tous les noms des destinataires sont affichés, A va récupérer l'adresse de B alors que B ne souhaitait pas parler à A. Ou pire, si D est un spammeur, il recevra toutes les adresses de vos contacts, et n'hésitera pas à s'en resservir (envoi de spam).

Dans tout site WebMail ou client de messagerie (Microsoft Outlook, Mozilla Thunderbird, Eudora Mail, Pegasus Mail, etc.) il est possible d'envoyer un mail à un grand nombre de destinataires tout en masquant à chacun d'entre eux la liste des personnes à qui vous écrivez.

Pour ce faire, il suffit de saisir la liste de vos destinataires **non pas** dans le champ "***A***" (en anglais "*To*") ou "**CC**" (Copie Carbone), mais dans le champ "**CCI**" (*Copie Carbone Invisible*, appelée également *copie cachée*) ou en anglais **BCC** (*Blind Carbon Copy*).

Transfert de message

Quelques conseils lorsque vous transférez un message :

- Utilisez le **CCI** pour les adresses des différents destinataires
- **Effacez du corps du mail les adresses** que l'expéditeur précédent aurait pu laisser visibles
- Pensez à **effacer** tous les "**Tr. Fw...**" dans le champ *Sujet*

SPAM

Le ***spam***, **courriel indésirable** ou **pourriel** (terme recommandé au Québec par l'OQLF) est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.