Les fiches conseils du Cypiée

Attention aux faux mails - Compte email piraté : que faire ?

L'e-mail reste l'un des outils les plus prisés des pirates sur Internet. Voici quelques conseils pour repérer les messages malveillants et ne pas être victime de tentatives de Phishing.

Un e-mail malveillant est un message électronique frauduleux qui a pour but d'inciter le destinataire à effectuer un transfert de fonds ou à se rendre sur un site frauduleux où lui seront demandés ses identifiants, ses mots de passe ou ses données bancaires. C'est la technique de l'hameçonnage, ou **Phishing** en anglais. On peut être invité à ouvrir une pièce jointe dans laquelle se cache un programme capable de voler des données présentes sur l'ordinateur, tablette ou smartphone.

Les indices qui doivent vous alerter

La présentation

Ne vous faites pas abuser par la présence de logos officiels, de liens vers des sites connus ou d'informations vous concernant. La présence de fautes d'orthographe ou de grammaire doit aussi vous mettre la puce à l'oreille.

L'expéditeur

Les pirates n'hésitent pas à se faire passer pour une banque, une administration (Caf, service des impôts…), une entreprise (EDF, Orange…) voire une personne de votre connaissance pour gagner votre confiance.

Le message

Il joue le plus souvent sur l'empathie (une personne a besoin d'aide), l'urgence (votre électricité sera coupée si vous ne réagissez pas vite), la peur (vous risquez d'être poursuivi si vous ne payez pas), fait miroiter une promesse d'argent ou un remboursement ou vous annonce qu'un colis vous attend ...

Le lien hypertexte

Vérifiez que l'adresse du site officiel vers laquelle il est censé renvoyer soit la bonne (www.microsoft.com et pas www.security-microsoft.com ou www.micosoft.com par exemple).

Les bons réflexes

- Ne répondez pas au message, ne cliquez sur aucun lien y compris celui censé permettre de se désabonner, n’ouvrez pas de pièce jointe et ne remplissez aucun formulaire.
- Faites preuve de bon sens : aucun organisme ne vous demandera par e-mail de lui communiquer des informations personnelles, et encore moins vos coordonnées bancaires.
- En cas de doute, contactez l’organisme censé vous avoir envoyé l’e-mail par téléphone ou en passant par la page d’accueil de son site Internet et non par le lien proposé dans l’e-mail.
- Signalez l’e-mail sur la plateforme gouvernementale Internet-signalement.gouv.fr.
- Supprimez-le et videz la corbeille.
- Pour une protection au quotidien, certains éditeurs d’antivirus proposent des suites complètes comprenant diverses fonctions protectrices, dont l’antiphishing.

Signaler les e-mails d'hameçonnage

Lorsque nous détectons un e-mail susceptible d'être une attaque par hameçonnage, nous pouvons afficher un message d'avertissement ou transférer l'e-mail dans les spams. Si un e-mail a été incorrectement marqué comme tentative d'hameçonnage ou, au contraire, n'a pas été détecté comme tel, suivez les étapes ci-dessous pour corriger son statut.

Remarque : Lorsque vous placez manuellement un e-mail dans le dossier "Spam", Google en reçoit une copie afin de l'analyser et de protéger ainsi les autres utilisateurs contre ce type d'e-mail et contre les abus.

Éviter les attaques par hameçonnage

Soyez prudent lorsque vous recevez un e-mail d'un site vous demandant des informations personnelles. Si cela se produit :

1. Ne cliquez sur aucun lien et ne fournissez aucune information personnelle tant que vous n'avez pas vérifié l'authenticité du message.
2. Si l'expéditeur dispose d'une adresse Gmail, signalez l'abus à Google.

Remarque : Gmail ne vous demandera jamais d'envoyer des informations personnelles, telles que votre mot de passe.

Lorsque vous recevez un message suspect, vérifiez les points suivants :

- Vérifiez que l'adresse e-mail et le nom de l'expéditeur correspondent.
- Vérifiez si le-mail est authentifié.
- Passez la souris sur les liens avant de cliquer dessus. Si l'URL du lien ne correspond pas à sa description, il se peut qu'il vous dirige vers un site d'hameçonnage.
- Vérifiez les en-têtes de message pour vous assurer que le nom indiqué dans l'en-tête "from" est correct.

Compte Email piraté : que faire ?

Lorsque votre compte Email a été piraté, des données sensibles peuvent rapidement tomber entre de mauvaises mains : les cybercriminels ont notamment accès à vos services de paiement en ligne, comme Paypal, ils peuvent faire des achats à votre place, obtenir des informations confidentielles sur votre entreprise ou même escroquer d'autres internautes. Les conséquences peuvent être graves. Ne cédez toutefois pas à la panique et appliquez nos conseils de crise : en effet, dans la majorité des cas, on peut récupérer le contrôle de son compte avant que quoi que ce soit de grave ne se passe.

Quels sont les signes qui prouvent que votre boite est piratée

Avant de paniquer, il est important de **savoir si votre boite mail a été piratée**, en repérant les petits signes d'activités suspectes.

- Vos données personnelles ont été modifiées (nom, date de naissance, paramètres de compte)
- Des proches se plaignent / vous informent qu'ils reçoivent des messages *étranges* de votre part
- Vous ne recevez plus aucun mail, car une redirection a été mise en place par le hacker. Il pourra lire vos communications et ainsi profiter des informations qu'elles contiennent
- Vous avez l'impression que des messages Non Lus sont Lus, alors que vous ne les avez pas ouverts
- On vous signale des connexions depuis des appareils que vous ne connaissez pas ou depuis des lieux ou vous n'êtes pas allés.

Sommaire

Comment fonctionne le piratage d'un compte mail ?

Pour résumer, l'étape la plus importante pour protéger son compte Email du piratage et des abus, c'est la **prévention**. C'est pourquoi il est important de savoir comment fonctionne le piratage d'un compte Email, afin de s'en protéger au mieux. Les cybercriminels utilisent plusieurs méthodes pour accéder aux adresses Email et aux mots de passe qui leur sont attribués. Un type de piratage particulièrement répandu consiste à attaquer les serveurs de sites Web importants afin de voler les données des utilisateurs. Le *phishing* ou les attaques de malware sont d'autres attaques fréquentes.

Le vol de données par attaque de serveur

Les **attaques en ligne** à grande échelle dont sont victimes les entreprises font souvent les gros titres. De cette façon, les criminels capturent les données de connexion de millions de clients. Dans la mesure où de nombreux utilisateurs utilisent le même mot de passe pour plusieurs sites différents, les pirates qui attaquent un site Web accèdent à d'innombrables comptes de messageries et sites Internet. Il est facile de se prémunir contre ce problème en créant pour chaque inscription un mot de passe unique et sécurisé. Dans la mesure où les piratages de compte Email sont découverts lorsqu'il est déjà trop tard, il est nécessaire d'agir rapidement et de changer ses mots de passe immédiatement.

Le phishing via des emails frauduleux

Le second moyen de dérober des données confidentielles est le P*hishing*. Il s'agit d'un piège par lequel un logiciel malveillant **envoie massivement de faux Emails**, incitant les destinataires à entrer leurs données personnelles de connexion sur des sites factices.

Le plus souvent, ces Emails frauduleux prétendent émaner de sites originaux, et demandent au destinataire de donner son mot de passe pour de prétendues raisons de sécurité. Il est alors redirigé vers un faux site, qui ressemble à l'original. Les mots de passe qui y sont entrés ne sont pas contrôlés pour leur sécurité, mais immédiatement transmis aux cybercriminels.

Le fait est que les sites sérieux, les services de messagerie, de paiement ou les boutiques en ligne **ne demandent jamais leurs mots de passe à leurs utilisateurs par Email**.

Il est donc important de ne jamais communiquer ces données simplement parce qu'elles nous sont demandées. En cas de doute sur l'authenticité d'un Email, n'hésitez pas à prendre contact avec l'assistance du site Web en question.

L'attaque au moyen de malwares

La troisième technique utilisée par les cybercriminels pour récolter des données confidentielles est l'attaque de malwares. La plupart des logiciels malveillants arrivent sous la forme d'Emails frauduleux ou de fausses pièces jointes : si ces fichiers sont ouverts, un logiciel malveillant est immédiatement installé sur l'ordinateur du destinataire : il s'agit d'un programme espion ou d'une sous-catégorie de type *keylogger* (enregistreur de frappe).

Ce sont des programmes qui fonctionnent en silence à l'arrière-plan et capturent les données sensibles, les mots de passe notamment. Les *keyloggers* enregistrent chaque frappe effectuée sur le

clavier de l'ordinateur infecté, et les transmettent aux cybercriminels. La meilleure protection contre ces logiciels malveillants consiste à installer sur son ordinateur **un antivirus récent et un pare-feu actif**. Mais il est aussi de la responsabilité de chacun d'être prudent : restez méfiant face aux Emails provenant d'inconnus, et vérifiez toujours l'authenticité d'un Email avant d'ouvrir ses pièces jointes.

Que faire quand son compte Email a été piraté

Vous pensez que votre compte Email a été piraté ? Il faut d'abord vous en assurer : Nous allons voir en détail tous les outils pour savoir si vous êtes victime de piratage.

Il existe pour cela un moyen simple : il suffit de rentrer votre adresse Email dans le moteur de recherche de cette page web, qui compile plusieurs adresses Emails piratées. Si votre adresse Email apparaît dans les résultats, suivez pas à pas notre « plan de crise » :

- Essayez d'abord de vous connecter à votre compte : si vous y arrivez sans problème, cela signifie que votre mot de passe n'a pas encore été changé par les pirates. Vous devez le faire vous-même aussi vite que possible : rendez-vous dans les paramètres de votre messagerie et **modifiez le mot de passe**. Choisissez un mot de passe à la sécurité élevée (voir ci-dessous), que vous utiliserez exclusivement pour votre messagerie. Si vous utilisez votre ancien mot de passe sur d'autres sites Web, changez-les aussi immédiatement, et choisissez un mot de passe unique pour chaque site. Vous devez ensuite enregistrer votre nouveau mot de passe de messagerie sur vos autres appareils (Smartphone, tablette, etc.), faute de quoi vos Emails entrants n'arriveront plus.

Pour tester votre mot de passe : *https://howsecureismypassword.net/*

Conseil :

Utilisez un mot de passe unique pour chaque compte (Email, réseaux sociaux, boutiques en ligne, etc.) Les mots de passe doivent de préférence être longs, et composés d'une combinaison aléatoire de lettres minuscules et majuscules, de chiffres et de caractères spéciaux. Il peut être utile de s'aider d'un gestionnaire de mots de passe pour les garder à portée de main.

- Si votre mot de passe a déjà été modifié par les pirates, vous pouvez toujours accéder à votre compte grâce à **une ou plusieurs questions confidentielles de sécurité**, un service proposé par la plupart des fournisseurs de messagerie. Pour ceci, cliquez sur le bouton ***« mot de passe oublié »***. En fonction des informations que vous avez fournies lors de votre inscription, le service vous demandera par exemple de rentrer le nom de jeune fille de votre mère, ou celui de votre premier animal de compagnie. Ce sont des questions qui sont posées à l'utilisateur lors de l'ouverture du compte : les réponses sont enregistrées et en principe connues de lui seul. Certains services proposent aussi de vérifier si l'accès au compte est autorisé grâce à un numéro de téléphone portable ou une seconde adresse Email. Si les réponses sont justes et que vous pouvez confirmer votre contact de vérification, un nouveau mot de passe vous sera envoyé par Email. Afin d'éviter tout risque de piratage ne le gardez pas, changez-le immédiatement en suivant les conseils ci-dessus.