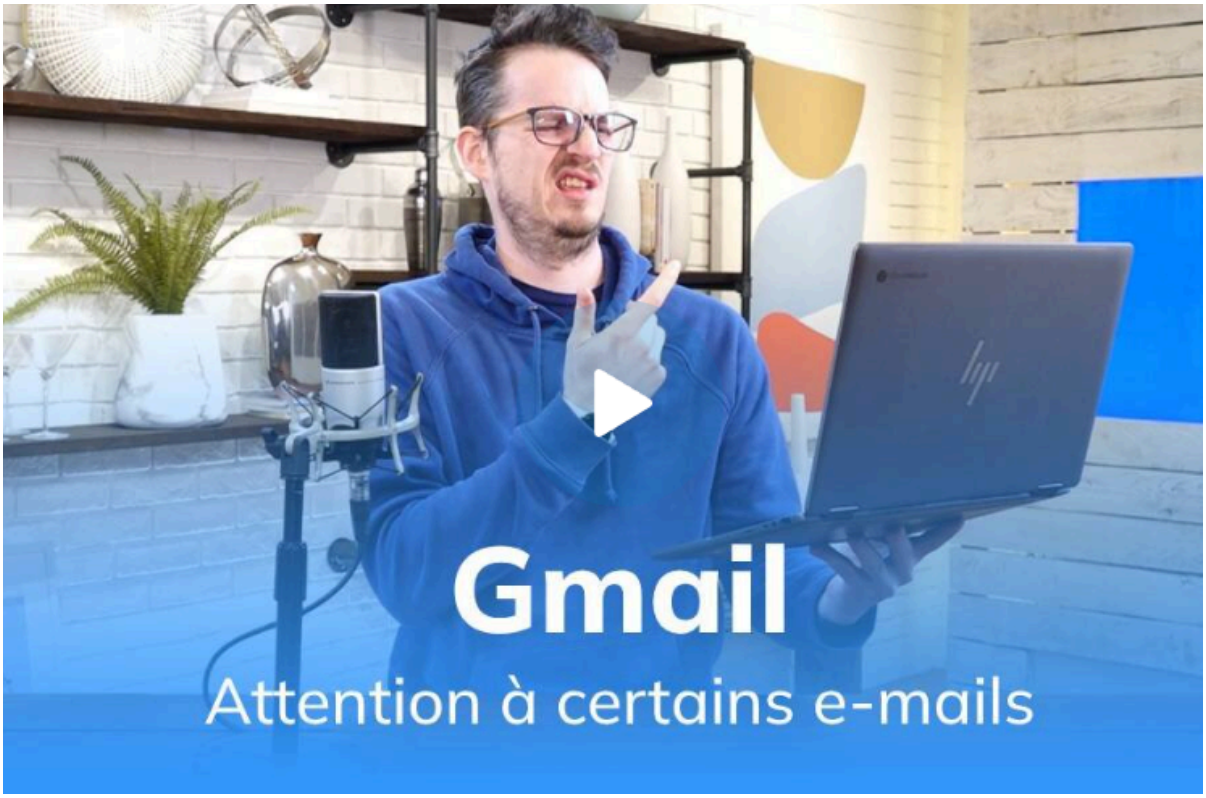
francoischarron.com /securite/fraude-et-arnaques-web/les-comptes-gmail-vises-par-une-vicieuse-tacti…

Les comptes Gmail visés par une vicieuse tactique de fraude



Capture d'écran, pour regarder la vidéo, cliquer le lien qui vous permet d'accéder au site Internet de François Charron:

Les comptes Gmail visés par une vicieuse tactique de fraude

Publié le 24 avril 2025 Vincent Paquette IA

Des pirates informatiques ont lancé une vague de courriels d'hameçonnage très sophistiquée visant les comptes Gmail. Le but est de subtiliser nos informations de connexion à notre compte Google pour en prendre le contrôle.

Les comptes Gmail sont visés par une campagne d'hameçonnage sophistiquée. - *francoischarron.com avec Dall-E.*

Des pirates informatiques ciblent actuellement les utilisateurs de Gmail avec une arnaque par hameçonnage (phishing) particulièrement sophistiquée.

Cette attaque est considérée comme très dangereuse, car elle exploite des failles dans l'infrastructure de Google et trompe les vérifications de sécurité habituelles.

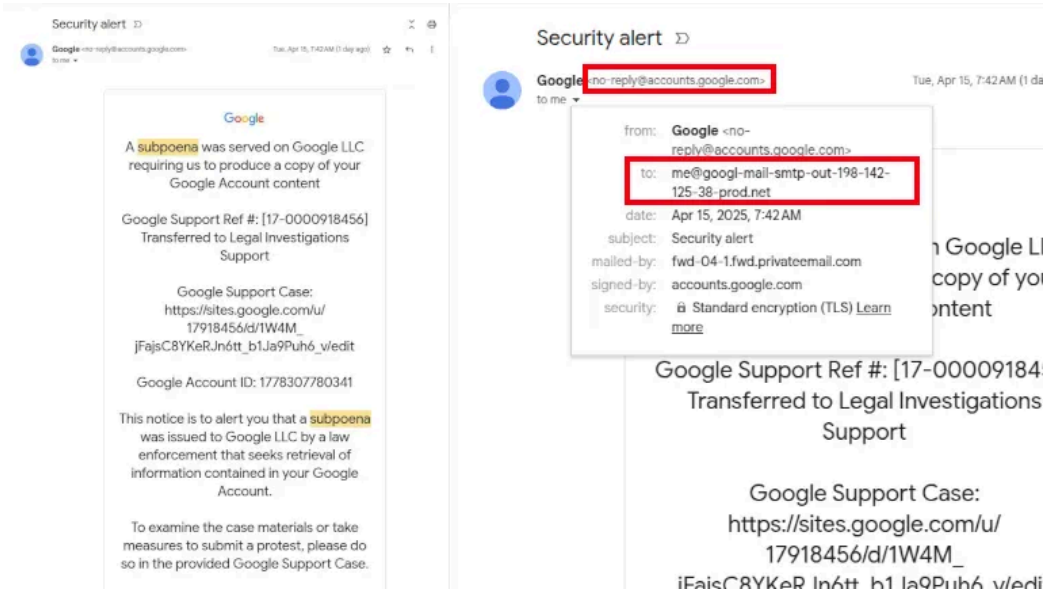
Comment l'arnaque fonctionne-t-elle?

C'est un développeur du nom de Nick Johnson qui a reçu le courriel problématique et a décortiqué la fraude.

L'attaque commence par un courriel qui semble provenir directement de Google.

Lorsqu'on vérifie l'adresse de l'expéditeur, celle-ci apparaît comme une adresse officielle. Il peut s'agir de l'adresse **no-reply@accounts.google.com** ou **no-reply@google.com**.

Mais en réalité, quand on regarde de plus proche, on se rend compte que le courriel ne nous est pas destiné, mais qu'il est destiné à une adresse me@.



Voici à quoi ressemble le faux courriel en question. - *Nick Johnson*

La procédure est assez complexe, mais toujours est-il que ces courriels sont conçus pour être presque parfaits. Ils passent les tests de sécurité, notamment la signature DKIM (un système qui vérifie l'authenticité des courriels).

Gmail affiche ces messages sans avertissement et peut même les placer dans la même conversation que d'autres alertes de sécurité légitimes de Google, ce qui les rend difficiles à distinguer des vrais.

Le courriel en question nous alerte d'une prétendue assignation à comparaître ou d'une injonction légale demandant de fournir une copie du contenu de notre compte Google.

Le courriel contient un lien nous invitant à examiner le dossier, à consulter les documents ou à s'y opposer.

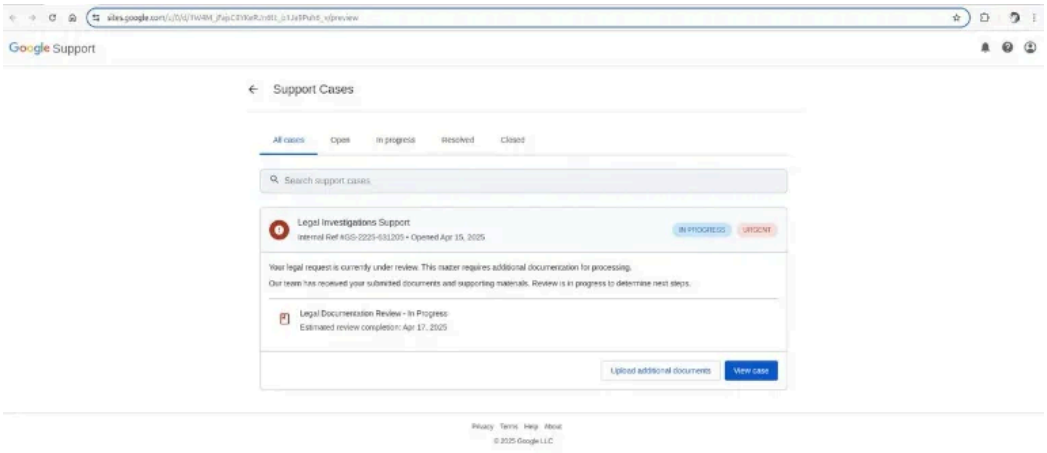
En cliquant sur le lien, on est redirigée vers une page hébergée sur: sites.google.com. Ce domaine appartient à Google, ce qui inspire confiance.

L'utilisation d'une page utilisant: sites.google.com est stratégique. Il s'agit d'une plateforme de Google qui nous permet d'héberger et créer des sites web avec un sous-domaine google.com.

C'est une opportunité pour les pirates de créer facilement des pages qui ressemblent à des portails d'assistance officiels de Google.

La page frauduleuse est conçue pour imiter la page de support officielle de Google.

Elle nous incite à télécharger des documents ou à consulter un dossier.



Voici la fausse page sur laquelle nous sommes redirigés. - *Nick Johnson*

Cependant, lorsqu'on tente d'accéder à ces éléments, on est invité à saisir nos identifiants Google.

En réalité, cette page est une page de connexion falsifiée hébergée sur: sites.google.com, et non sur le domaine officiel de Google qui est: accounts.google.com.

C'est à ce moment qu'on est piégé. En saisissant nos identifiants sur cette page, on les transmet directement aux pirates. Ils peuvent alors prendre contrôle de notre compte.

Google a reconnu le problème et travaille à déployer des protections pour bloquer cette voie d'abus.

Comment se protéger dès maintenant?

Google a confirmé être au courant de ce type d'attaque d'hameçonnage et déploie des protections, mais, en attendant, des mesures simples sont essentielles pour sécuriser notre compte.

Voici les étapes clés:

- **Se méfier des courriels suspects**. Google ne nous contactera jamais pour nous demander vos identifiants. Il faut rester très vigilant si un message nous demande de cliquer sur un lien ou de saisir nos identifiants, même s'il semble provenir de Google.
- **Vérifier l'URL avant de cliquer**. Si un courriel contient un lien, passer son curseur dessus (sans cliquer) permet de voir l'adresse complète. On doit s'assurer que les pages de connexion Google commencent bien par: **https://accounts.google.com**.
- **Activer l'authentification à deux facteurs (2FA)**. C'est une couche de sécurité supplémentaire qui exige une deuxième vérification (comme un code envoyé sur votre téléphone ou une clé de sécurité) en plus de votre mot de passe pour vous connecter. Même si un pirate obtient votre mot de passe, il ne pourra pas accéder à votre compte sans ce second facteur.

Comment ajouter l’authentification à double facteur sur son compte Gmail

- **Utiliser des méthodes d'authentification forte**. Activer la double authentification est déjà une bonne chose. Seulement, on devrait éviter de recevoir nos codes 2FA via messages texte SMS. Il est préférable d'utiliser une application 2FA générant ces fameux codes aux 30 secondes.
- **Configurer un numéro de téléphone et une adresse courriel de récupération** sur notre compte Google. Cela nous donne une période de **sept jours** pour récupérer notre compte si jamais il est piraté, même si l'attaquant a changé vos informations de récupération. Pendant cette semaine, Google peut toujours envoyer des codes de connexion à nos anciens contacts de récupération.

Définir un numéro de téléphone ou une adresse e-mail de récupération sur Google

- **Éviter d'utiliser les mêmes mots de passe pour se connecter.** Il va de soi qu'on a tout intérêt à ne pas réutiliser les mêmes mots de passe pour nos comptes. Autrement, si un tombe, tous les autres vont tomber. D'où l'idée d'utiliser un gestionnaire de mots de passe pour en obtenir des forts et diversifiés pour tous nos comptes.

Nos recommandations de gestionnaires de mots de passe

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20250424
"C'est ensemble qu'on avance"