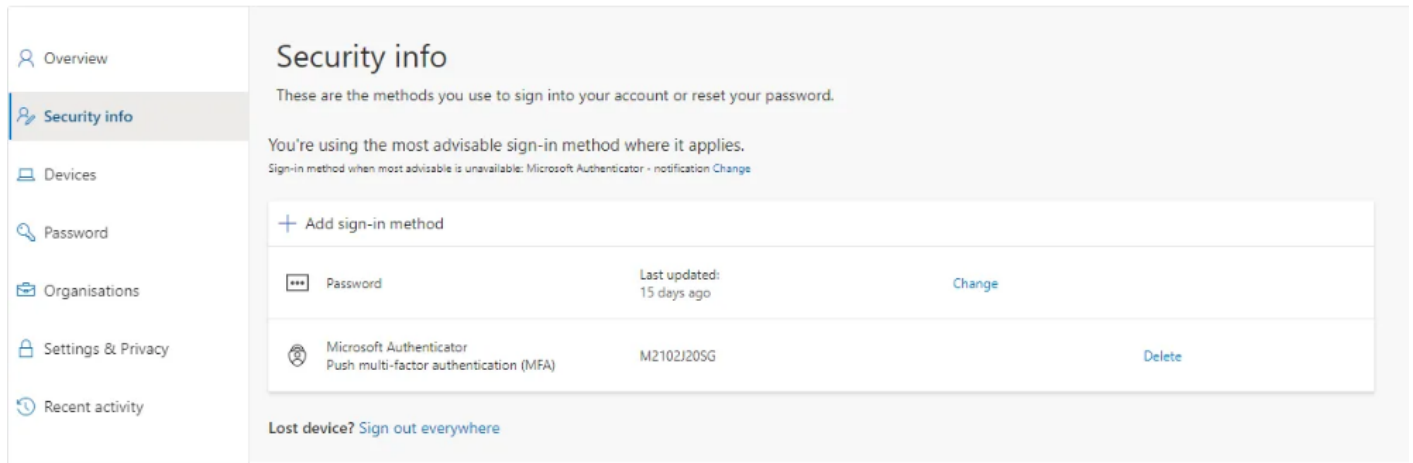


# Compte 365 compromis

Connexion sur le poste de l'utilisateur

Reset du mot de passe depuis le centre d'administration O365

Depuis le compte de l'utilisateur (via le web) ⇒ déconnexion de tous les appareils



Connexion au compte Outlook de de l'utilisateur.

Vérifier que des règles (obscurs) n'aient pas été appliquées.

Analyse antivirus sur le poste.

Pistes trouvées sur un site.

- Ne pas saisir de données
- Se déconnecter de l'internet
- Effectuez une analyse complète de votre machine à l'aide d'un logiciel antivirus/anti-malware.
- Changez vos mots de passe
- Assurez-vous d'avoir sauvegardé vos fichiers dans un endroit sûr.
- Supprimez le cache et les comptes supplémentaires de votre navigateur.
- Signaler un e-mail comme spam

## Qu'est-ce que l'hameçonnage ?

L'**hameçonnage** est une pratique qui consiste à envoyer des courriels nuisibles aux utilisateurs d'Internet afin de les escroquer. Il s'agit d'un type d'**ingénierie sociale** où les escrocs tirent parti des aspects psychologiques des individus pour les amener à agir de manière irrationnelle. L'objectif est d'obtenir l'accès à des informations privées sur les utilisateurs, notamment des données financières, des identifiants de système, des numéros de carte de crédit, etc.

# Comment fonctionne le phishing ?

Pour ce faire, un lien malveillant est inséré dans un courriel d'hameçonnage. Si vous cliquez sur ce lien, un **logiciel malveillant** infectera votre appareil et commencera à voler vos données.

Dans une **étude** réalisée en **2018** sur plus de 700 000 courriels d'hameçonnage, près de la moitié des destinataires ont ouvert le courriel et environ un tiers ont cliqué sur le lien d'hameçonnage. Alors, quels sont les problèmes qui peuvent survenir après avoir cliqué sur ce lien, et que pouvez-vous faire pour limiter les dégâts ?

## PROCEDURE

1. Réinitialiser le mot de passe de l'utilisateur (si l'utilisateur est un utilisateur géré dans le nuage, sinon sur l'ad local)
2. Activer l'authentification multifactorielle
3. Révoquer tous les jetons de rafraîchissement, ce qui oblige l'utilisateur à se reconnecter. (Depuis le portail azure)
4. Désactiver les règles de transfert (encore mieux modifiez la politique antispam outbound et désactiver les transferts auto a l'extérieur pour tous)
5. Désactiver le partage anonyme de calendriers
6. Supprimer les options de transfert de boîte aux lettres

Un script existe pour faire cela en powershell :

[Scripts/Remediate-BreachedAccount.ps1 at master · O365AES/Scripts · GitHub](#)

Pour plus chez Microsoft :

[Réponse à un compte de messagerie compromis - Office 365 | Microsoft Learn](#)

---

Revision #1

Created 25 November 2024 12:47:45 by Johann

Updated 25 November 2024 12:50:30 by Johann