



CAMPAGNE DE PHISHING EN COURS

Date : 17 septembre 2025

Objet : Identification d'une campagne de phishing usurpant des comptes internes

Niveau d'alerte : **ÉLEVÉ**

1. Situation

L'équipe informatique a identifié une campagne de phishing active ciblant notre organisation. Des e-mails malveillants sont envoyés depuis les comptes internes suivants qui ont été compromis :

- eric.le-saux@mnhn.fr
- tep-vanrith.ung@mnhn.fr

L'objectif de ces e-mails est de vous inciter à cliquer sur un lien frauduleux pour voler vos identifiants de connexion.

2. Comment identifier l'e-mail frauduleux ?

L'e-mail se présente comme une alerte de connexion et contient les éléments suivants :

Expéditeur usurpé : Service d'Authentification <adresse.compromise@mnhn.fr>

Objet : Deux Messages

"Bonjour, Une authentification avec votre compte académique a été détectée... Veuillez CLIQUEZ-ICI pour la vérification... Si vous ne procédez pas à la vérification sous 48h, nous serons dans l'obligation de le suspendre..."

3. Que faire si vous recevez cet e-mail ?

- **Ne cliquez sur AUCUN lien** et n'ouvrez aucune pièce jointe.
- **Ne répondez pas** à l'expéditeur.
- **Signalez immédiatement l'e-mail** en le transférant à alerte-ssi@mnhn.fr.
- **Supprimez l'e-mail** de votre boîte de réception après l'avoir signalé.

4. Rappels des bonnes pratiques

La vigilance est notre meilleure protection. Soyez particulièrement attentif aux signes suivants :

- **Caractère d'urgence** : Méfiez-vous des messages qui vous menacent ou vous pressent d'agir.
- **Liens suspects** : Survolez toujours les liens avec votre souris pour vérifier la destination réelle avant de cliquer.
- **Expéditeur inattendu** : Un service officiel ne vous contactera jamais depuis le compte d'un collègue.