PasDePiège

RAPPORT DE SÉCURITÉ · RISQUE CRITIQUE

DANGER

HAMEÇONNAGE AVÉRÉ

NE CLIQUEZ SUR RIEN

NE RÉPONDEZ PAS · NE PAYEZ PAS

NE DONNEZ AUCUNE INFORMATION

SIGNALEZ LE MESSAGE COMME PHISHING
PUIS SUPPRIMEZ-LE

Verdict 100/100 · Étude réelle fortement anonymisée · PDP-DEMO-001

Analyse d’un courriel usurpant une grande marque

Rapport technique fondé sur le message original, ses en-têtes complets et son code HTML.

RÉFÉRENCE	DATE DU MESSAGE	DESTINATAIRE
PDP-DEMO-001	Août 2026	Adresse masquée

RISQUE CRITIQUE · ACTION IMMÉDIATE

HAMEÇONNAGE AVÉRÉ

100 / 100

STOP — NE CLIQUEZ PAS

Ne cliquez sur aucun bouton, aucune image et aucun lien de désinscription. Ne répondez pas. Ne transmettez aucune donnée. Signalez le message comme hameçonnage, puis supprimez-le.

POURQUOI : le message usurpe deux grandes marques et dirige vers un hébergement tiers sans rapport avec elles. SPF, DKIM et DMARC authentifient seulement le domaine technique d’envoi — jamais l’identité commerciale affichée.

Synthèse technique

Expéditeur et identités observées

Nom affiché : [GRANDE MARQUE AUDIOVISUELLE]. Adresse effective et Return-Path : t**********@gmail.com. Adresse d'origine déclarée : r*****@d********.com. Message-ID terminé par un domaine tiers masqué. Aucune de ces adresses n'établit un lien avec la marque usurpée.

Chaîne d'acheminement reconstituée

Un serveur tiers [nom masqué], présenté par une infrastructure cloud et l'adresse 13.51.***.*** au moment de l'envoi, s'est connecté au service de messagerie au moyen d'une session ESMTPSA authentifiée. Le fournisseur a ensuite transmis le message depuis 209.85.***.*** vers la boîte du destinataire.

L'authentification SMTP et la signature Google démontrent que le compte Gmail a réellement servi à l'envoi. Elles ne démontrent pas que l'offre est légitime.

Lecture correcte de SPF, DKIM et DMARC

1. **SPF : PASS** — INFORMATIF

   L'enveloppe utilise une adresse Gmail masquée et le dernier relais est autorisé pour gmail.com. SPF ne contrôle pas la marque commerciale affichée.

2. **DKIM : PASS pour gmail.com** — INFORMATIF

   Google a signé le message après son injection dans Gmail. La signature garantit l'intégrité du contenu signé pendant le transport, pas l'honnêteté de son auteur.

3. **DMARC : PASS pour gmail.com** — INFORMATIF

   Le domaine visible et les mécanismes d'authentification sont alignés sur gmail.com. Il n'existe aucun alignement avec un domaine de la marque usurpée.

Infrastructure du lien

L'image et le bouton pointent vers https://[SOUS-DOMAINE-MASQUÉ].[STOCKAGE-CLOUD]/[FICHIER-MASQUÉ].html. Le jeton individuel a été intégralement supprimé. Ce domaine de stockage objet n'appartient visiblement à aucune des marques invoquées. L'adresse n'a pas été ouverte pendant l'analyse.

Indices de fraude relevés

1

Usurpation manifeste d’une grande marque

CRITIQUE

Le nom d’affichage annonce une marque connue, mais l’expéditeur réel est une adresse grand public sans relation visible avec elle.

2

Mélange d’identités incompatibles

CRITIQUE

Le message combine plusieurs marques, fournisseurs cloud, domaines tiers et identifiants de plateformes sans rapport entre eux. Cet assemblage n’est pas cohérent avec une campagne officielle.

3

Destination externe dissimulée

CRITIQUE

L’intégralité du visuel et le bouton conduisent vers un objet HTML hébergé sur un stockage cloud tiers. La destination officielle attendue devrait appartenir à la marque ou être clairement documentée.

4

Objet sans rapport avec la promesse

CRITIQUE

L’objet « Vérification de l’adresse e-mail » ne correspond pas au sondage promettant un produit électronique coûteux.

5

Récompense et urgence artificielle

CRITIQUE

La promesse d’un téléviseur, la sélection prétendument limitée et la mention de stocks réduits cherchent à provoquer une action impulsive.

6

Personnalisation défectueuse

CRITIQUE

Le lien de désinscription contient une autre adresse, entièrement retirée de cette démonstration. Ce défaut révèle une base ou un modèle réutilisé et interdit de considérer le lien comme fiable.

7

Bourrage de texte antispam

CRITIQUE

Le HTML contient des extraits législatifs, coordonnées, noms, textes universitaires et pharmaceutiques sans rapport. Ce « word salad » est compatible avec une tentative de perturbation des filtres antispam.

8

Structure MIME et HTML dégradée

CRITIQUE

Les limites multipart, balises et blocs résiduels sont incohérents. Le fichier noname.txt affiché par Gmail paraît être un artefact de cette construction incorrecte plutôt qu’une pièce jointe métier légitime.

Scénario probable et mesures

Parcours frauduleux vraisemblable

Après un clic, la victime est probablement conduite vers un faux sondage. Une récompense lui est ensuite annoncée, puis ses coordonnées et éventuellement de prétendus frais de livraison sont demandés. Le parcours peut viser la collecte de données personnelles, de coordonnées bancaires ou l'inscription à un abonnement caché.

Si aucun clic n'a eu lieu

- **Signaler le message comme hameçonnage dans Gmail.**
- **Ne pas utiliser le lien de désinscription, qui peut confirmer que l'adresse est active.**
- **Supprimer le message après le signalement.**

Si le lien a été ouvert

- **Fermer la page et ne rien télécharger.**
- **Retirer toute autorisation de notification accordée au site.**
- **Contrôler les téléchargements et les extensions récemment ajoutées.**

Si un mot de passe a été saisi

- **Modifier immédiatement le mot de passe depuis le site officiel saisi manuellement.**
- **Changer les autres comptes utilisant le même mot de passe et activer la double authentification.**
- **Contrôler les sessions, règles de transfert de courrier et applications autorisées.**

Si des données bancaires ont été saisies

- **Contacter immédiatement la banque et demander les mesures de protection adaptées.**
- **Surveiller les opérations et abonnements, puis conserver toutes les preuves.**
- **Effectuer les signalements officiels appropriés.**

Limites de l'analyse

L'analyse permet de conclure avec un très haut niveau de confiance au caractère frauduleux du courriel. Elle ne permet pas d'identifier juridiquement son auteur ni de déterminer si le compte d'envoi a été créé pour la fraude, compromis ou utilisé par un service tiers. Les fournisseurs techniques ne sont pas mis en cause : leurs infrastructures peuvent être détournées par des utilisateurs malveillants.

PasDePiège fournit un second avis informatif et probabiliste fondé sur les éléments disponibles. Ce rapport ne constitue ni une certification, ni une expertise juridique, financière ou judiciaire. Le client reste responsable de ses vérifications, de ses démarches et de sa décision finale.