

Rapport d'enquête

Tentative de sextorsion par courriel — analyse personnelle

Date du courriel	30 mai 2026	Date du rapport	30 mai 2026
Vecteur	Outlook / programme anti-spam Microsoft	Type d'arnaque	Sextorsion de masse

1. Contexte

Réception d'un courriel de chantage classique (« sextorsion ») prétendant qu'un logiciel espion aurait filmé le destinataire via sa webcam, et exigeant un paiement en Bitcoin sous peine de diffusion d'une vidéo compromettante. Le message a été reçu via le programme de lutte contre le courrier indésirable de Microsoft, qui l'a présenté pour classification.

Objectif de l'enquête : comprendre le mécanisme de l'usurpation, vérifier l'absence de compromission réelle du compte, et explorer une éventuelle piste de traçage — dans une posture strictement défensive (renseignement à signaler, sans aucune action offensive).

2. Analyse technique de l'en-tête

L'élément récupéré était l'enveloppe du programme Microsoft (expéditeur SpamFightersProgram@hotmail.com), et non l'en-tête brut du courriel frauduleux. Toute la chaîne de serveurs traversés appartenait à l'infrastructure Microsoft. L'en-tête original du message malveillant (chaîne Received, résultats SPF / DKIM / DMARC) n'était donc pas exploitable depuis cette copie.

Le courriel frauduleux affichait l'adresse du destinataire dans le champ « De », avec la mention « je l'ai envoyé depuis votre propre compte ». Il s'agit d'une simple falsification du champ From au niveau SMTP — technique de masse, triviale à réaliser — et non d'une preuve d'intrusion.

Constat : aucune compromission du compte. L'usurpation de l'adresse est un effet d'affichage, pas un accès réel. Le message ne citait aucun mot de passe : variante de bluff la plus faible, ne reposant sur aucune donnée personnelle.

3. Traçage de l'adresse Bitcoin

Adresse de paiement indiquée dans le message :

1Gpu4hxcqpLZyjQ4JHZ6ieojyVBFj81Y3K

Consultation publique via l'explorateur (mempool.space), sans création de compte ni manipulation de fonds. Résultats relevés :

Indicateur	Valeur	Lecture
Total reçu	0,00000000 BTC	L'adresse n'a jamais rien encaissé
Solde confirmé	0,00000000 BTC	Rien à suivre
Transactions / UTXO	0	Aucun flux à remonter

Rapport d'enquête

Tentative de sextorsion par courriel — analyse personnelle

Type d'adresse	P2PKH (legacy)	Information neutre
Conclusion de la piste on-chain : impasse. On ne peut pas tracer un argent qui n'a jamais circulé. Le wallet n'ayant rien reçu, la chaîne s'arrête au point de départ. C'est l'issue la plus banale de ces campagnes : leur rentabilité repose sur le volume d'envois, et la majorité des adresses restent vides. À noter : un total reçu nul sur cette adresse ne dit rien du gain global de la campagne, qui utilise souvent une adresse différente par victime.		

4. Actions de signalement

- Adresse Bitcoin et gabarit du message signalés sur Chainabuse.
- Canaux complémentaires disponibles : PHAROS (internet-signalement.gouv.fr), signal-spam.fr pour le courriel, et THESEE pour un dépôt de plainte en ligne.
- Posture maintenue : observation et signalement uniquement, sans contact avec l'auteur, sans tentative d'accès, sans publication d'identité.

5. Recommandations de sécurité

- Ne jamais payer ni répondre à ce type de message.
- Méfiance face aux courriels « LastPass » pressant de sauvegarder son coffre ou de saisir son mot de passe maître (campagne de phishing active depuis janvier 2026) : ne saisir le mot de passe maître que dans l'application officielle, jamais via un lien reçu.
- Maintenir un mot de passe maître long et unique, et activer la double authentification sur le gestionnaire de mots de passe.

Bilan : tentative de sextorsion sans fondement réel (aucune intrusion, aucun enregistrement). Piste blockchain en cul-de-sac, ce qui constitue une conclusion d'enquête valide. La valeur résiduelle est le renseignement transmis, exploitable si l'adresse réapparaît ailleurs.