

Emails de chantage et sextorsion : le bluff qui rapporte des millions

« Je vous ai filmé, payez en bitcoin » : anatomie d'un chantage presque toujours bidon — et des cas rares où il ne l'est pas.

7 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/sextorsion-chantage

L'email fait froid dans le dos : « J'ai piraté votre ordinateur et vous ai filmé sur des sites pour adultes ; payez en bitcoin ou j'envoie la vidéo à vos contacts. » Il cite parfois un de vos vrais mots de passe — glaçant. Dans l'immense majorité des cas, tout est faux : pas de piratage, pas de vidéo, juste un vieux mot de passe issu d'une fuite et un envoi en masse. Comprendre le mécanisme désamorce la panique — et permet de reconnaître les rares chantages réels, qui se traitent autrement.

1. Le chantage de masse : pur bluff

- Le « piratage » : inexistant — l'escroc a acheté des couples email + mot de passe issus de fuites de données et envoie le même texte à des millions d'adresses
- Le vieux mot de passe cité est LA preuve inversée : il date d'une fuite ancienne — s'il vous surveillait vraiment, il citerait l'actuel
- Variantes du même moule : « votre webcam », « vos recherches », la fausse convocation de police pour « pédopornographie », la bombe dans les locaux — même industrie, même bluff
- L'usurpation de votre propre adresse en expéditeur (« je vous écris depuis votre boîte ! ») : un artifice technique banal, pas une preuve d'accès — que DMARC rend d'ailleurs plus difficile

ATTENTION

La règle absolue : ne jamais payer, ne jamais répondre. Payer ne fait pas disparaître une vidéo qui n'existe pas — mais inscrit votre adresse sur la liste « payeurs », revendue et re-ciblée sans fin. Répondre confirme que l'adresse est lue. Le bon traitement : signaler (signal-spam), supprimer, et changer le mot de passe cité s'il sert encore quelque part.

2. Les bons gestes face au chantage de masse

- Respirer : le scénario est un modèle industriel connu, documenté par toutes les autorités
- Si un mot de passe est cité : vérifier où il sert encore et le changer partout — c'est l'unique information vraie du message, et elle mérite ce traitement
- Signaler puis supprimer ; pas de paiement, pas de réponse, pas de clic
- En entreprise : prévenir l'équipe qu'une vague circule — la personne qui reçoit ça en silence peut paniquer, voire payer ; en parler tue l'arnaque

3. Les cas réels : rares, mais sérieux

- La vraie sextorsion : après un échange intime réel en ligne (piège tendu sur les réseaux ou applications), l'escroc possède effectivement des images — cible privilégiée : hommes, y compris des dirigeants, et adolescents
- Le chantage aux données volées : après une vraie intrusion (ransomware avec vol de données), la menace de publication est réelle et se gère comme un incident majeur
- Le signe distinctif du réel : des éléments précis et récents impossibles à connaître autrement (captures de VOTRE échange, VOS fichiers) — pas un mot de passe de 2019

4. Face à un chantage réel

- Ne pas payer non plus : le paiement déclenche l'escalade (« encore un peu ou je publie ») — les autorités sont unanimes
- Couper tout contact, tout capturer AVANT (messages, profils, références de paiement demandées)
- Plainte immédiate : les sections cyber traitent ces dossiers couramment, avec des leviers réels (signalements de comptes, coopération des plateformes)
- Sur les plateformes : signaler le profil maître-chanteur ; pour les images intimes, des dispositifs dédiés bloquent la diffusion (StopNCII et outils des plateformes)
- S'entourer : proche de confiance, association d'aide aux victimes (France Victimes, 116 006) — la honte isole, et l'isolement est l'arme du chanteur

L'essentiel à retenir

- 01 Ne jamais payer ni répondre à un chantage par email
- 02 Changer tout mot de passe cité encore en usage
- 03 Signaler (signal-spam, THESEE) puis supprimer
- 04 Prévenir l'équipe quand une vague circule
- 05 Chantage réel : tout capturer, plainte, zéro contact
- 06 Orienter les victimes vers les dispositifs d'aide dédiés

Questions fréquentes

L'email vient de MA propre adresse. N'est-ce pas la preuve d'un piratage ?

Non : falsifier l'adresse d'expéditeur affichée est trivial sans aucun accès à votre boîte — comme écrire un faux nom d'expéditeur au dos d'une enveloppe. Le test utile : les connexions récentes de votre compte et l'absence de messages envoyés inconnus. Et une configuration DMARC stricte de votre domaine rend l'artifice bien plus difficile.

Le message cite mon mot de passe ACTUEL. Que faire ?

Là, on agit sérieusement : ce mot de passe est compromis quelque part (fuite récente, infostealer, réutilisation). Changement immédiat partout où il sert, MFA activée, analyse du poste au moindre doute, et vérification des connexions aux comptes principaux. Le chantage reste du bluff — mais l'indice de compromission, lui, est réel et se traite.

Un collaborateur victime d'une vraie sextorsion : quel rôle pour l'entreprise ?

L'humanité d'abord : orienter vers la plainte et les dispositifs d'aide, sans jugement — le pire scénario est la victime isolée qui paie en silence, voire puise dans la caisse. Côté entreprise : vérifier que la pression ne cible pas aussi des accès professionnels, et rappeler que le soutien existe. Les chartes qui mentionnent « en cas de chantage, parlez-en, sans conséquence » débloquent des situations.

Pour aller plus loin

Cybermalveillance.gouv.fr — le chantage à la webcam — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/chantage-ordinateur-webcam-pretendue-piratee

France Victimes — 116 006, aide aux victimes — www.france-victimes.fr

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr