



Quoi faire avant de paniquer en cas de chantage à la webcam piratée

*6 mesures de protection et
7 choses à faire en cas d'attaque*



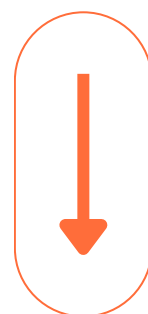


Définition 1/2

Le chantage à l'ordinateur ou à la webcam **prétendus piratés** (ou « cryptoporno ») désigne un type d'escroquerie qui vise à vous faire croire que vos équipements ont été piratés. Il prend généralement la forme d'un **message reçu**, essentiellement par courriel (mail), de la part d'un inconnu qui se présente comme un pirate informatique.

Ce « hacker » prétend avoir pris le contrôle de l'ordinateur de la victime suite à la consultation d'un site pornographique et annonce **avoir obtenu des vidéos compromettantes** avec sa webcam.

Source : cybermalveillance.gouv.fr

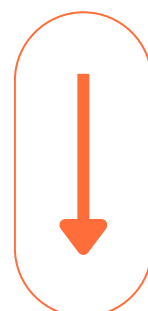




Définition 2/2

Le cybercriminel **menace de les publier aux contacts** (personnels et/ou professionnels) de la victime **si elle ne lui paie pas une rançon**, souvent réclamée en monnaie virtuelle (généralement en Bitcoin). Parfois, pour attester de la prise de contrôle de l'ordinateur auprès de la victime, les cybercriminels vont jusqu'à **lui écrire avec sa propre adresse mail** ou lui dévoiler l'un de ses mots de passe.

Source : cybermalveillance.gouv.fr



Prévention

1. Faites régulièrement les **mises à jour** de sécurité de tous vos appareils.
2. **Utilisez un antivirus** et tenez-le à jour.
3. **Évitez les sites non sûrs** ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.).
4. Utilisez des mots de passe suffisamment complexes et **changez-les au moindre doute.**



Prévention

5. **N'ouvrez pas les messages suspects**, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.

6. **Masquez votre webcam** quand vous ne vous en servez pas (un simple morceau de ruban adhésif opaque sur l'objectif peut suffire). Pour info : le fondateur de Facebook, Mark Zuckerberg, et l'ancien directeur du FBI, James Comey, le font...



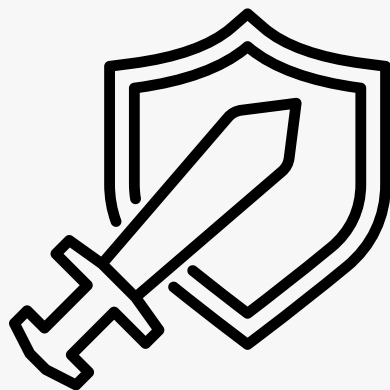
Défense si vous êtes victime

1. NE PANIQUEZ PAS.

En effet, vous n'avez sans doute rien de réellement compromettant à vous reprocher.

2. NE RÉPONDEZ PAS.

Il ne faut jamais répondre à de telles menaces de chantage qui montrent aux cybercriminels que votre adresse de messaging est « valide » et que vous portez de l'intérêt au message de chantage qu'ils vous ont envoyé.



Défense si vous êtes victime

3. NE PAYEZ PAS LA RANÇON.

Et ce, même si vous aviez un doute.

4. CONSERVEZ LES PREUVES.

Faites des captures d'écran, conservez les messages qui pourront vous servir pour signaler cette tentative d'extorsion aux autorités.

5. CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE partout où vous l'utilisez s'il a été divulgué ou au moindre doute et choisissez-en un solide.



Défense si vous êtes victime

6. CONTACTEZ VOTRE BANQUE si vous avez payé la rançon pour essayer de faire annuler la transaction.

7. DÉPOSEZ PLAINTÉ au commissariat de police ou à la gendarmerie ou en adressant votre plainte au procureur de la République du tribunal judiciaire dont vous dépendez.

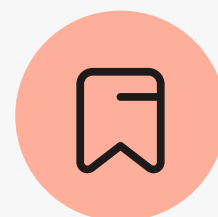
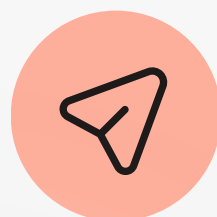
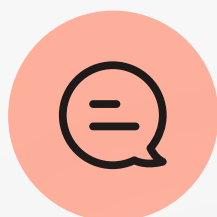


Besoin d'aide ?

Écrivez-moi!

Peur d'oublier ?

Enregistrez et partagez à vos collègues.



@loicsecuritenumerique 



YouTube

À partir des infos de

