

Arnaque à la webcam ... que faire ?

Vous venez de recevoir un message vous indiquant que votre dernière conversation vidéo en ligne a été enregistrée alors que vous pensiez être en situation d'intimité avec la personne avec qui vous échangez ? On vous menace de diffuser cette vidéo si vous ne payez pas une certaine somme d'argent ? Comment faut-il réagir ?

En parcourant Internet (CNIL¹, Arnaque-chantage-webcam, ...), les conseils suivants peuvent être bien utiles.

**Quelle attitude adopter ?**

- **ne répondez pas** au cyber-escroc,
Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, **ne versez surtout pas d'argent** quelle que soit la somme demandée.
- **verrouillez tous vos comptes sociaux** (Facebook) de façon à ce que le malfaiteur n'associe pas votre nom à une liste d'amis ou de contacts,
Paramétrez vos comptes sociaux professionnels et vos comptes Facebook de manière à ce que le malfaiteur n'associe pas votre nom à une liste d'amis / de contacts. Ne rendez accessible votre profil Facebook qu'àuprès de vos amis de confiance. Enfin, ne publiez rien de personnel sur votre mur. Des personnes mal intentionnées peuvent détourner ces informations à d'autres fins.
Voir aussi *Comment régler ses paramètres Facebook*² et *Comment protéger sa vie privée sur Facebook en 15 étapes*³.
- **effectuez des captures d'écran** des messages et d'alerter les autorités,
N'hésitez pas à vous rendre auprès du bureau de police, vous pouvez déposer une plainte et serez entendu par des policiers totalement compréhensifs. N'oubliez pas que ce qui vous arrive est actuellement courant.
- **avertissez vos ami(e)s** afin qu'ils ne répondent pas à d'éventuelles sollicitations,
Veillez à informer discrètement les personnes susceptibles d'être sollicitées par le cyber-escroc en mentionnant sobrement que vous êtes victime d'une escroquerie en ligne et qu'il ne faut ni ouvrir, ni partager, ni répondre à une éventuelle sollicitation provenant d'un inconnu
- **parlez-en à une personne de confiance..**
Cette arnaque est une intrusion violente dans votre vie privée. N'hésitez pas à en parler à un proche qui pourra vous aider à franchir ce moment. Si vous en ressentez le besoin et si vous souhaitez anticiper les suites éventuelles de cette arnaque, n'hésitez pas à consulter une personne compétente (thérapeute, ...).
- **réalisez** régulièrement des **recherches sur votre nom** dans les moteurs afin de savoir si un contenu en ligne y est associé.
Vous pouvez par exemple programmer une alerte à votre nom qui vous enverra un message sur votre messagerie électronique dès qu'un contenu associé à votre nom est mis en ligne. Certains services existent⁴.

¹ Sources : <https://www.service-public.fr/particuliers/actualites/007952> et <https://www.cnil.fr/fr/reagir-en-cas-de-chantage-la-webcam>

² http://www.internetsanscrainte.fr/pdf/Comment_reglar_ses_parametres-Facebook.pdf

³ <http://www.phonandroid.com/vie-privee-sur-facebook-les-15-reglages-de-confidentialite-pour-etre-invisible.html>

⁴ Voir <http://www.talkwalker.com/fr/alerts> et <https://www.google.fr/alerts>

Si en plus de Facebook, votre compte Skype a été utilisé⁵.

Coupez le contact sur Skype lors d'une arnaque à la webcam, en **supprimant purement et définitivement votre compte Skype**.

Si l'escroc connaît votre compte Skype, comme pour votre adresse email : le moyen le plus simple et le plus efficace est de supprimer votre compte . Ainsi, si l'escroc tente de vous joindre, il ne vous retrouvera plus, il ne pourra plus vous ajouter ou vous contacter sur Skype, que ce soit avec son compte ou un autre.

Si vous ne supprimez pas votre compte, si vous « bloquez » simplement l'escroc ce ne sera pas suffisant. En effet l'escroc pourra très facilement créer un autre compte, vous retrouver sur Skype et vous harceler avec un autre compte. Afin de couper définitivement les menaces sur Skype, la solution est donc la **suppression totale** du compte skype

Attention : Il ne s'agit pas simplement de désinstaller Skype de votre ordinateur ou de votre smartphone mais bien de supprimer définitivement votre compte. Le fait de désinstaller le compte ne change rien. L'escroc peut toujours croire qu'il peut vous contacter. S'il pense qu'il peut vous joindre, vous augmentez la période de risque et de surveillance.

Pourquoi supprimer le compte Skype et ne pas supprimer le compte Facebook ?

Sur Skype, la menace sur vos amis et relations ne tient pas ! Il est impossible pour l'escroc de connaître vos relations Skype. Du coup contrairement à Facebook, on ne risque pas une usurpation d'identité, ni un partage de la vidéo à nos amis "Skype".

Pour supprimer définitivement votre compte Skype, consultez l'article suivant : *Comment puis-je fermer mon compte Skype ?*⁶ et suivez les étapes suivantes :

1. Vous devez avoir accès à l'adresse de courriel associée à votre compte Skype. Le service technique vérifiera votre identité en vous faisant parvenir un code de vérification.
2. Contactez le service clientèle Skype à l'adresse suivante : <http://www.skype.com/go/contactcs>
3. Entrez votre pseudo et votre mot de passe
4. Sélectionnez : Compte et mot de passe.
5. Sélectionnez : Suppression d'un compte.
6. Cliquez sur suivant
7. Cliquez sur Discuter par écrit avec le support
Ceci vous permettra de discuter avec un technicien du support technique
8. Cliquez sur le bouton Commencer le Chat.
9. Quelques minutes de patience et vous êtes en contact avec un technicien. Expliquez-lui que vous êtes victime d'une arnaque à la webcam via votre compte Skype. Il comprendra très bien, ... n'oubliez pas qu'il s'agit d'une arnaque fréquente.
10. Afin de vérifier votre identité, le technicien vous invitera à consulter un code de vérification envoyé à votre adresse de courriel. Consultez vos courriels et transmettez-lui le code.
11. Suivez ensuite les instructions du technicien. En quelques minutes votre compte sera effacé.

N'oubliez pas qu'il peut falloir jusqu'à 30 jours pour que votre nom disparaisse de l'annuaire, mais ensuite, personne ne pourra vous trouver dans Skype. Votre nom s'affiche encore dans les listes de contacts de vos amis tant qu'ils ne le suppriment pas, mais ils ne peuvent pas vous contacter⁷.

⁵ Sources : <http://www.arnaque-chantage-webcam.com/protégez-vous/supprimer-skype/>

⁶ <https://support.skype.com/fr/faq/FA142/comment-puis-je-fermer-mon-compte-skype>

⁷ Source : idem

Si la vidéo est déjà diffusée ...

Si la vidéo a déjà été diffusée, vous pouvez demander au site de la dépublier et aux moteurs de recherche de déréférencer le contenu en cause.

- Pour une vidéo diffusée sur Youtube voir le formulaire *Procédure relative aux réclamations pour violation de la vie privée de YouTube*⁸.
Voir aussi : Centre de signalement des abus et de mise en application des règles⁹
- En parallèle, demandez au moteur de recherche de déréférencer le contenu en cause¹⁰.
Depuis un récent arrêt de la cour de justice européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leurs nom et prénom.
 - Formulaire Google du droit à l'oubli (Demande de suppression de résultat de recherche au titre de la législation européenne en matière de protection des données) :
https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=fr
 - Formulaire Bing du droit à l'oubli (Si vous êtes résident européen et souhaitez que Microsoft bloque les résultats sur Bing des recherches portant sur votre nom) : <https://www.bing.com/webmaster/tools/eu-privacy-request>

D'autres solutions existent

- Créer du contenu bien référencé à votre nom
*Vous pouvez créer rapidement des contenus valorisants associés à votre nom et donc bien référencés. Il peut s'agir d'un blog consacré à une passion ou d'une page de curation de contenus (outil qui permet de sélectionner, éditer et partager des pages/liens web sur un sujet précis).
Attention à ne pas communiquer d'éléments personnels.*
- Faire appel à une agence spécialisée
Certains cas peuvent nécessiter l'intervention d'une agence spécialisée dans l'effacement de contenus gênants. Soyez néanmoins vigilant sur les compétences vantées dans l'annonce.
N'hésitez pas à vous rendre sur des forums pour vous renseigner sur la réputation de ces agences.

Pour en savoir plus ...

Pour de la prévention, consultez aussi : <https://soundcloud.com/fedpol-belgium/>

⁸ Voir : <https://support.google.com/youtube/contact/privacy2>

⁹ <https://www.youtube.com/yt/policyandsafety/fr/reporting.html>

¹⁰ Voir : Le droit au déréférencement (<https://www.cnil.fr/fr/le-droit-au-dereferencement>)