Arnaque à la webcam : des conseils pour bien réagir – Denis JACOPINI

#Arnaque à la webcam : des conseils pour bien réagir

Alors que les arnaques à la webcam se multiplient et touchent chaque années des milliers de victimes, la CNIL publie un guide de ces pratiques.

Pour chaque situation particulière, l'arnaque semble se dérouler à peu près de la même façon : la victime se rend la plupart du temps sur un site de rencontre, et entame la conversation avec une jeune femme ou un jeune homme au physique plutôt attrayant. La victime se voit alors proposer de continuer la conversation par Webcam, et s'exécute. Le cyber-escroc fait une capture d'écran, et menace de diffuser la vidéo ou les images de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos, si la personne ne lui remet pas la somme de 200 euros sous 24/48h.
Afin de faire face à cette situation, la Commission nationale de l'informatique et des libertés (CNIL) a publié une fiche pratique, destinée à informer et accompagner les victimes de ces cyber escrocs. Il y est notamment indiqué :
• qu'il ne faut surtout pas répondre aux tentatives de chantage du cyber-escroc ;
• qu'il convient d'alerter les autorités compétentes, via la plateforme du Ministère de l'intérieur ;
• qu'il faut demander au site de dépublier le contenu gênant ;
Rappelons que des sociétés, spécialisées dans l'effacement des contenus gênants, existent. De plus, et depuis un arrêt rendu par la Cour de justice de l'Union européenne, les internautes peuvent saisir les moteurs de recherche d'une demande de déréférencement d'un contenu associé à leur nom et prénom.

Quel réflexe adopter ?
1. **Ne répondez surtout pas à un cyber-escroc**
Soyez parfaitement hermétique à toute tentative de chantage : ne communiquez aucune donnée personnelle, ne versez surtout pas d'argent quel que soit la somme demandée.
2. **Verrouillez immédiatement vos comptes sociaux**
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'auprès 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. Notre page Facebook délivre quelques conseils pour bien paramétrer vos comptes.
3. **Alertez les autorités via la plateforme du Ministère de l'Intérieur**
Effectuez des captures d'écran justifiant votre situation (messages reçus, contenus à effacer …). Voir la fiche pratique
4. **Signalez directement l'escroquerie sur la plateforme www.internet-signalement.gouv.fr**
Renseignez-vous via le service Info Escroqueries au 0811 02 02 17 (prix d'un appel local depuis un poste fixe ; ajouter 0.06 €/minute depuis un téléphone mobile ; Du lundi au vendredi de 9h à 18h)
5. **Parlez-en à une personne de confiance**
La violence des termes employés par l'escroc et le risque d'exposition de votre vie privée peuvent être vécus comme un traumatisme. Il est conseillé d'en parler avec une personne de confiance.Vous êtes mineur ? Des télé-conseillers sont gratuitement à votre écoute au 0800 200 000 de 9h à 19h en semaine. Voir le site Net écoute
6. **Informez vos amis de l'escroquerie**
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.
7. **Effectuez régulièrement des recherches à votre nom**
Vous pouvez par exemple programmer une alerte à votre nom qui vous enverra un message sur votre webmail dès qu'un contenu associé à votre nom est mis en ligne. Certains services existent ici ou là.**Si la vidéo a été diffusée …**
8. **Demandez systématiquement au site de dépublier le contenu gênant**
Exemple : si la vidéo a été mise en ligne sur Youtube : demandez à Youtube de supprimer cette vidéo. Si le site ne répond pas à votre demande sous deux mois, adressez vous à la CNIL en suivant la procédure de notre formulaire de plainte en ligne.
9. **En parallèle, demandez au moteur de recherche de déréférencer le contenu en cause**
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.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Sources :
http://www.net-iris.fr/veille-juridique/actualite/34611/arnaque-a-la-webcam-la-cnil-donne-des-conseils-pour-bien-reagir.php

http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/reagir-en-cas-de-chantage-a-la-webcam