

Comment réagir en cas de chantage à la webcam ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

x

x

x

x

x

x

x

Comment réagir en cas de chantage à la webcam ?

L'arnaque à la webcam touche chaque année des milliers de victimes. Cette série de conseils vous aidera à adopter les bonnes pratiques si vous devez faire face à ce type de chantage.

A quoi ressemble un cas typique de chantage à la webcam ?
La victime se rend sur un site de rencontre puis entame la conversation avec une jeune femme ou un jeune homme au physique attrayant. Après lui avoir posé quelques questions sur sa vie privée, cette personne l'invite à approfondir les échanges via une conversation vidéo plus intime. Quelque temps plus tard, un courriel ou un message Facebook apprendra à la victime que cette rencontre a été enregistrée. Le cyber-escroc menace de diffuser la vidéo de cet échange sur le compte Facebook d'un proche ou sur un site de partage de vidéos si la victime ne lui remet pas la somme de 200 euros sous 24h/48h.

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 quelle que soit la somme demandée.
- 2. Verrouillez immédiatement vos comptes sociaux**
Paramétrez vos comptes sociaux professionnellement 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. 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
 - Signalez directement l'escroquerie sur la plateforme www.internet-signalement.gouv.fr
 - Appelez le service Info Escroqueries au 8811 62 62 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)
- 4. 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 200 800 de 9h à 19h en semaine. Voir le site Net écoute
- 5. Informez vos amis de l'escroquerie**
Veillez à informer discrètement les personnes susceptibles d'être sollicitées par le cyber-escroc en mentionnant brièvement 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.
- 6. Effectuez régulièrement des recherches à votre nom**
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 existent ici ou là.

Si la vidéo a été diffusée –

- 7. 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.
- 8. 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. Le droit au déréférencement ☑
- 9. D'autres solutions existent**
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.
- 10. 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.

Réagissez à cet article

CYBERARNAQUES - S'informer pour mieux se protéger (Le Livre)

Denis JACOPINI Marie Nocenti (Plon) ISBN :
2259264220



Denis Jacopini, expert judiciaire en informatique diplômé et spécialisé en cybercriminalité, raconte, décrypte et donne des parades contre toutes les cyberarnaques dont chacun peut être victime.

Il est témoin depuis plus de 20 ans d'attaques de sites Internet, de piratages d'ordinateurs, de dépouillements de comptes bancaires et d'autres arnaques toujours plus sournoisement élaborées.

Parce qu'il s'est rendu compte qu'à sa modeste échelle il ne pourrait sensibiliser tout le monde au travers des formations et des conférences qu'il anime en France et à l'étranger, il a imaginé cet ouvrage afin d'alerter tous ceux qui se posent la question : Et si ça m'arrivait un jour ?

Plutôt que de présenter une longue liste d'arnaques Internet recensées depuis plusieurs années, Denis Jacopini, avec la collaboration de Marie Nocenti, auteur du roman Le sourire d'un ange, a souhaité vous faire partager la vie de victimes d'arnaques Internet en se basant sur des faits réels, présentés sous forme de nouvelles suivies de recommandations pour s'en prémunir. Et si un jour vous rencontrez des circonstances similaires, vous aurez le réflexe de vous méfier sans risquer de vivre la fin tragique de ces histoires et d'en subir les conséquences parfois dramatiques.

Pour éviter de faire entrer le loup dans votre bergerie, il est essentiel de le connaître pour le reconnaître !
Commandez sur Fnac.fr

<https://www.youtube.com/watch?v=lDw3kI7ra2s>

06/04/2018 A l'occasion de la sortie de son livre "CYBERARNAQUES : S'informer pour mieux se protéger", Denis JACOPINI répond aux questions de Valérie BENHAÏM et ses 4 invités : 7 Millions de victimes de la Cybercriminalité en 2010 (Symantec) 13,8 Millions de victimes de la

Cybercriminalité en 2016 (Symantec) 19,3 Millions de victimes de la Cybercriminalité en 2017 (Symantec) Plus ça va moins ça va ? Peut-on acheter sur Internet sans risque ? Si le site Internet est à l'étranger, il ne faut pas y aller ? Comment éviter de se faire arnaquer ? Comment on fait pour renifler une arnaque sur Internet ? Comment avoir un coup d'avance sur les pirates informatiques ? Quelle est l'arnaque qui revient le plus souvent ? Denis JACOPINI vous répond sur C8 avec Valérie BENHAÏM et ses invités.

Commandez sur Fnac.fr

https://youtu.be/usg12zkRD9I?list=UUoHqj_HKcbzRuvIPdu3FktA

12/04/2018 Denis JACOPINI est invité sur Europe 1 à l'occasion de la sortie du livre "CYBERARNAQUES S'informer pour mieux se protéger"

Comment se protéger des arnaques Internet

Commandez sur amazon.fr



Je me présente : Denis JACOPINI. Je suis l'auteur de ce livre coécrit avec Marie Nocenti, romancière.

Pour ma part, je suis Expert de justice en informatique spécialisé en cybercriminalité depuis 1996 et en protection des Données à Caractère Personnel.

J'anime des formations et des conférences sur le RGPD et la Cybercriminalité pour aider les organismes à se protéger des pirates informatiques et à se mettre en conformité avec la réglementation autour du numérique (dont le RGPD : Règlement Général sur la Protection des Données).

Commandez sur [Fnac.fr](https://www.fnac.fr)

Original de l'article remis en page : Réagir en cas de chantage à la webcam | CNIL