Arnaque à la Webcam - Attention aux brouteurs du WEB

Fiche pratique publié le **22/06/2016**, vu **7277 fois**, Auteur : Alexandre Chombeau

L'arnaque à la webcam ou chantage à la webcam est une pratique de plus en plus courante qui consiste à piéger un internaute afin de lui soutirer de l'argent. Qu'est-ce que l'arnaque à la webcam ? Comment ceux que l'on appelle les « brouteurs » choisissent leurs proies et quelles sont les solutions lorsque l'on subit ce genre d'attaque ? Alexandre Chombeau, responsable de l'agence digitale CSV vous répond.

L'arnaque à la webcam ou chantage à la webcam est une pratique de plus en plus courante qui consiste à piéger un internaute afin de lui soutirer de l'argent. Qu'est-ce que l'arnaque à la webcam ? Comment ceux que l'on appelle les « brouteurs » choisissent leurs proies et quelles sont les solutions lorsque l'on subit ce genre d'attaque ? Alexandre Chombeau, responsable de l'agence digitale CSV vous répond.

Qu'est-ce que l'arnaque à la webcam ?

La victime d'une arnaque à la webcam se laisse approcher voire séduire sur Internet par une personne mal intentionnée. Le premier contact se fait généralement sur Skype, Facebook ou sur un site de rencontres. Le brouteur instaure un climat de confiance avec sa proie jusqu'à réussir à obtenir un rendez-vous par webcam. Si la victime se déshabille ou adopte un comportement équivoque, le brouteur capture des images/la vidéo et obtient ainsi l'objet de son futur chantage. En possession de ces documents, le malfaiteur se permet de réclamer de l'argent à sa proie en la menaçant de tout dévoiler en cas de refus (à ses proches, ses collègues, son employeur, etc.).

Comment les brouteurs choisissent-ils leurs proies ?

Pour que leur futur chantage soit efficace, les brouteurs choisissent des personnes dont les éléments de la vie privée sont faciles à trouver sur la toile. Un individu qui indique son statut marital, le nom de son époux(se), la société dans laquelle il/elle travaille ainsi que son lieu de résidence sera beaucoup plus facile à convaincre qu'un individu ne laissant rien apparaître. En effet, une fois que le brouteur aura obtenu les documents gênants, il sera extrêmement facile pour lui de menacer la proie qui n'a pas pris ses précautions (en lui promettant de les divulguer à son entourage).

Pour éviter d'être la cible d'un brouteur, il est important de verrouiller ses profils sur les réseaux sociaux (en évitant le mode « public ») et de vérifier régulièrement quelles sont les informations personnelles divulguées sur Internet.

Comment savoir si l'on a affaire à un arnaqueur ?

Les brouteurs ne sont pas de jolies jeunes femmes qui cherchent l'amour mais plutôt des groupes d'hommes, généralement situés en Afrique noire. Ils sévissent à plusieurs. Les photos qu'ils

choisissent pour leurs profils sont donc fausses et ont souvent été volées sur la toile (clichés de jolies femmes).

- La première chose à faire est de vérifier si la photo de profil est unique en la copiant et la collant dans la barre de recherche de Google Images. Si plusieurs réponses apparaissent et ne concernent pas la personne avec laquelle vous discutez, ce sera un premier indice de malhonnêteté.

Avant d'effectuer la manipulation, demandez à votre contact si sa photo de profil le/la représente.

- La deuxième chose à faire est de lui poser des questions, de noter les réponses puis de reposer les mêmes questions quelques jours plus tard. Si les réponses sont différentes d'un jour à l'autre, ce sera un deuxième indice important.

Pensez également à observer son profil afin de voir si tout vous paraît normal : voyez si vous avez accès à sa date d'inscription, s'il/elle a de nombreux amis, s'il y a de l'interaction sur son mur (sur Facebook par exemple), etc.

Les brouteurs proposent souvent des phrases toutes faites et assez bien écrites (copiées/collées) pour les réponses « banales ». Ils répondent en revanche dans un français approximatif lorsqu'ils doivent improviser : c'est encore un signe.

Astuces pour éviter l'escroquerie

Paramétrages

Paramétrez tous vos comptes de manière à ne laisser apparaître qu'un minimum d'informations sur votre vie personnelle (et même professionnelle).

Les rencontres

Pour faire des rencontres sans avoir peur des représailles, vous pouvez tout simplement demander un rendez-vous téléphonique à votre contact. A cette occasion, vous pourrez détecter un éventuel accent étranger et voir si votre interlocuteur semble fiable.

Si vous décidez de réaliser une entrevue par webcam, demandez à votre contact de se montrer en premier et de vous parler ou de vous faire un signe (pour vous assurer que la vidéo n'est pas un enregistrement).

Premiers réflexes en cas d'arnaque à la webcam

1 – Ignorer

Ignorez l'arnaqueur, ne lui répondez plus, si vous avez peur, ne le montrez pas.

2 – Bloquer tous ses comptes

Vous aviez laissé vos différents profils en mode « public » ? Vous devrez rapidement bloquer l'accès à tous vos comptes de manière à ce que le brouteur ne puisse pas accéder à vos listes d'amis, à l'adresse de la société dans laquelle vous travailler, etc. Sur Facebook par exemple, cliquez sur l'onglet « amis » puis sur « gérer » et « modifier la confidentialité », une nouvelle fenêtre apparaît, faites en sorte d'être le seul à pouvoir voir votre liste d'amis en sélectionnant « moi uniquement » dans le menu déroulant. Vous avez des abonnés ? Faites de même avec la liste des personnes qui vous suivent.

3 – Diffuser un message à l'intégralité de ses contacts

Très rapidement, préparez un message que vous enverrez à l'intégralité de vos contacts (qu'ils soient professionnels ou personnels). Dans cet e-mail, expliquez que vos comptes ont été piratés et qu'il ne faut en aucun cas ouvrir de message vous concernant, surtout s'il y a des pièces jointes, au risque de recevoir un virus.

Grâce à ce message, vos contacts effaceront le message du brouteur (s'il venait à l'envoyer) avant même de l'avoir ouvert.

4 – Réunir des preuves

Retournez sur les logiciels ou sites que vous utilisiez avec le brouteur pour communiquer et faites des copies d'écran afin de réunir les preuves de l'arnaque. Vous pourrez ensuite les envoyer au Ministère de l'Intérieur.

Notez également que l'escroc tente parfois de se faire passer pour la police, pour Dailymotion ou Youtube : analysez chaque document que vous recevrez avec attention et ne paniquez pas.

Si le malfaiteur publie la vidéo compromettante et qu'il vous envoie le lien pour vous prouver sa démarche, sachez que vous pouvez contacter les sites concernées afin de leur demander de retirer la vidéo le plus rapidement possible. Pour accélérer le processus, vous pouvez également faire appel à des nettoyeurs du net.

Ne donnez jamais d'argent à un brouteur : s'il reçoit le mandat, rien ne prouve qu'il ne continuera pas à exploiter la vidéo ; de plus, les personnes qui se laissent manipuler participent à l'entretien de ce genre de pratiques.

Peut-on porter plainte pour chantage à la webcam ?

Il est possible de porter plainte pour escroquerie mais il est rare que les autorités réussissent à démanteler ce genre de réseau. En effet, les escrocs se connectent depuis des cybercafés, sur d'autres continents, ils utilisent aussi des adresses IP cachées.

Pour signaler l'abus, rendez-vous sur la page officielle du Ministère de l'Intérieur prévue à cet effet : https://www.internet-signalement.gouv.fr/. Vous pouvez également déposer plainte dans le commissariat ou le poste de gendarmerie le plus proche.

Enfin, gardez toujours à l'esprit qu'un malfaiteur n'aura aucun intérêt à diffuser vos documents si vous refusez fermement de coopérer (c'est-à-dire, de lui envoyer de l'argent). Son objectif est de convaincre ses proies, s'il comprend que cela ne fonctionnera pas avec vous, il ne perdra pas son temps et continuera ses escroqueries ailleurs. Ne laissez jamais de place au doute ou à l'hésitation, montrez-vous sûr de vous et ferme, c'est ainsi que vous pourrez vous protéger au mieux.