Webcams et objets connectés

Ce qu'il faut savoir pour se protéger contre le piratage

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

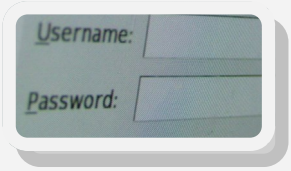
CASES

En novembre 2014, des milliers d'accès à des webcams privées ou publiques ont été divulgués par des pirates. En cause leurs fonctionnalités de contrôle à distance, qui n'étaient pas correctement protégées. La problématique ne se limite toutefois pas seulement aux webcams. N'importe quel objet connecté à Internet est potentiellement piratable.

Comment protéger ma webcam et mes objets connectés?

UTILISER UN MOT DE PASSE SOLIDE

Un mot de passe faible est un des moyens les plus faciles pour les cybercriminels d'accéder à vos objets connectés



Utiliser au moins 10 signes
****

Un mot de passe avec moins de caractères est considéré comme faible

Modifier le mot de passe par défaut
0000 1111

Après l'achat d'un nouveau produit, modifier le mot de passe par défaut qui est souvent facile à deviner

Choisir des caractères inhabituels
ABC abc 123 @€#

Utiliser une suite de chiffres, de lettres majuscules et minuscules ainsi que des caractères spéciaux

Changer régulièrement de mot de passe
1 fois/an

Prévoir de changer tous les mots de passe au moins une fois par an

Facile à mémoriser mais difficile à deviner
P.ex. Ja1meMOnCh13n

Le mot de passe doit être mémorisable sans avoir à le noter sur un support externe

Ne pas utiliser des informations publiques
Noms, anniversaires, etc.

Les pirates peuvent récolter beaucoup d'informations, p.ex. le nom de votre chien via les réseaux sociaux

Utiliser différents mots de passe pour différents usages
Internet banking, Facebook, Twitter, Amazon, etc.

En cas d'intrusion, les pirates n'auront pas accès à tous les comptes (réseaux sociaux, e-commerce, etc.)

Ne pas choisir un mot repris dans les dictionnaires
A-Z

Les pirates utilisent des logiciels de déchiffrement qui passent en revue tous les termes figurant dans les dictionnaires, en y ajoutant même des variantes

À EVITER: LES MOTS DE PASSE LES PLUS UTILISÉS EN 2013

1)	123456	6)	123456789	11)	123123	16)	1234	21)	password1
2)	password	7)	111111	12)	admin	17)	monkey	22)	princess
3)	12345678	8)	1234567	13)	1234567890	18)	shadow	23)	azerty
4)	qwerty	9)	iloveyou	14)	letmein	19)	sunshine	24)	trustno1
5)	abc123	10)	adobe123	15)	photoshop	20)	12345	25)	000000

CONSEILS EN FONCTION DU TYPE DE MATÉRIEL

Il faut distinguer 3 types:

La webcam autonome (souvent utilisée à des fins de surveillance domestique)

⇒ **Modifiez les paramètres d'usine** pour l'administration à distance;
⇒ **protégez le réseau Wi-Fi:**
  ⇒ par un mot de passe solide;
  ⇒ en activant le chiffrement de la connexion sans fil;
  ⇒ en protégeant l'accès aux paramètres du routeur par un mot de passe solide;
  ⇒ en désactivant le Wi-Fi lorsqu'il n'est pas nécessaire;
  ⇒ en modifiant le nom (SSID) du point d'accès Wi-Fi de manière à ce qu'il ne donne aucune indication sur son propriétaire;
  ⇒ en rendant le point d'accès Wi-Fi invisible;
  ⇒ en désactivant la possibilité de l'accès à la caméra depuis l'Internet;
⇒ **installez un VPN** (Virtual Private Network).

La webcam intégrée à un ordinateur portable ou connectée par USB

⇒ **Utilisez un antivirus à jour** pour éviter de vous faire infecter par des logiciels malveillants, qui arrivent à prendre le contrôle de la caméra (Le voyant rouge peut même être désactivé);
⇒ **désactivez votre caméra** si vous ne l'utilisez pas couramment;
⇒ **obstruez votre webcam** en y collant un sparadrap ou bien tout autre film opaque;
⇒ **soyez vigilants aux messages d'alerte** que votre ordinateur peut vous envoyer lorsque vous utilisez des services ou des programmes qui veulent activer votre webcam.

La caméra intégrée à un smartphone ou à une tablette

⇒ N'installez pas les applications si vous ne savez pas précisément **à quel moment et sous quelles conditions elles peuvent activer la caméra**;
⇒ soyez vigilant concernant les applications de sécurité qui permettent par exemple de **tracer un ordinateur, une tablette ou un smartphone volé par son adresse IP et/ou sa position GPS**. Ces applications ont parfois des fonctions de surveillance très étendues qui ne sont pas toujours conformes aux réglementations sur le respect de la vie privée.

Comment savoir si j'ai été piraté?

Savoir si on a été piraté peut s'avérer très complexe, surtout si le pirate prend des précautions pour éviter de se faire repérer. Dans le cadre de l'usage de webcams, vous pouvez toutefois **porter attention aux indices suivants qui pourraient indiquer un potentiel piratage:**

1) La **lumière de la caméra s'allume** alors que vous n'êtes pas en train de l'utiliser;
2) Vous disposez d'une caméra avec un **moteur de mouvement et celui-ci s'active tout seul**;
3) Le **logiciel de sécurité** installé sur votre terminal vous **signifie des alertes ou tentatives d'intrusion.**

Que faire si j'ai été piraté?

1 ADOPTER LES BONS RÉFLEXES

Si vous êtes victime d'un piratage informatique, il peut être utile de suivre, dans un premier temps, les recommandations suivantes :

1) Relever les indices / éléments du piratage : faire des copies d'écrans, prendre des photos, faire une copie des éléments à disposition sur une clé USB ;

2) Appliquer les bonnes pratiques de protection citées dans la section précédente ;

3) Si votre PC a été infecté par un logiciel malveillant, le moyen le plus sûr de s'assurer de la suppression de tout élément malicieux est de réinstaller votre système d'exploitation (ex : Windows) à neuf ;

4) Porter plainte à la police (plus d'informations ci-dessous).

2 S'ADRESSER AUX INSTANCES RESPONSABLES

En ce qui concerne le piratage de caméras de surveillance, votre interlocuteur change en fonction des cas de figures suivants :

Cas de figure	Qui s'expose à des peines?	A qui s'adresser?
Caméras utilisées dans un cadre personnel *Ex: moniteurs-bébé, caméras de surveillance opérées par des particuliers, webcams personnelles*	L'auteur de l'intrusion ou de la tentative d'accès → *article 509-1 du Code pénal*	Il est recommandé de porter plainte auprès de la police
Vidéosurveillance sur le lieu du travail *Ex: surveillance des salariés sur le lieu du travail et des non salariés qui passent dans le champ de vision des caméras (p.ex. dans les établissements commerciaux ou administrations)*	L'auteur de l'intrusion ou de la tentative d'accès → *article 509-1 du Code pénal* L'employeur pour ne pas avoir pris les mesures nécessaires pour sécuriser ses traitements → *articles 22 et 23 de la loi modifiée du 2 août 2002*	Ces caméras sont soumises à autorisation de la CNPD. Il est recommandé de porter plainte auprès de la CNPD et/ou de la police.
Vidéosurveillance dans les lieux publics *Zones de sécurité opérés par la Police grand-ducale ("Visupol")*	L'auteur de l'intrusion ou de la tentative d'accès → *article 509-1 du Code pénal*	Ces caméras doivent être autorisées par voie de règlement grand-ducal et arrêté ministériel. La surveillance de ces traitements relève de la compétence d'une autorité de contrôle spécifique. → *article 17 de la loi modifiée du 2 août 2002*

La loi sur la protection des données ne s'applique pas aux équipements d'enregistrement vidéo dont les images **ne permettent pas d'identifier directement ou indirectement des personnes**, étant donné que dans cette hypothèse il n'y a pas de traitement de données à caractère personnel et une autorisation de la CNPD n'est donc pas requise (*p.ex. les webcams destinées à filmer l'avancement d'un chantier, des webcams à finalité touristique, etc).*

Sources: CASES (https://www.cases.lu/fr/mot-de-passe.html); splashdata.com; icons8.com.

Contact

Commission nationale pour la protection des données (CNPD)

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette

Tél. : (+352) 26 10 60 -1
Fax. : (+352) 26 10 60 - 29
Courriel: info@cnpd.lu
Internet: www.cnpd.lu

Cyberworld awareness & security enhancement services (CASES)

19-21, boulevard Royal
L-2449 Luxembourg

Courriel: help@cases.lu
Internet: www.cases.lu