Abus des moyens de télécommunication et réseaux sociaux

Sommaire

Généralités

Il existe certaines mesures dissuasives d'ordre technique ou judiciaire pour mettre fin aux désagréments entraînés par l'utilisation abusive de moyens de télécommunication.

Descriptif

Refus des appels masqués

S'agissant du téléphone fixe, l'opérateur auquel est affilié l'abonné propose généralement des procédures permettant de refuser les appels anonymes, c'est-à-dire ceux dont le numéro ne s'affiche pas sur le combiné (en lien: procédure chez Swisscom). S'agissant du téléphone portable, certains appareils ont une fonction permettant de configurer le blocage des appels anonymes. Cela peut parfois poser des difficultés, notamment parce que certaines administrations publiques utilisent des numéros masqués. L'appelant est cependant avisé du refus des numéros masqués.

Demander le nom de la personne

En cas d'appels abusifs, vous pouvez demander à votre opérateur le nom et l'adresse du titulaire du numéro. Vous devez néanmoins prouver que ces données sont nécessaires pour démontrer un abus et dès lors indiquer l'heure et la durée des appels que votre opérateur pourra vérifier.

Obtenir un nouveau numéro de téléphone et disparaître de l'annuaire

Il est par ailleurs possible d'obtenir la mise à disposition d'un nouveau numéro de téléphone, qui ne sera pas communiqué par le numéro des renseignements. Il n'est plus obligatoire de figurer dans l'annuaire et l'abonné peut choisir de figurer dans l'une des listes suivantes:

- blanche: le numéro figure dans l'annuaire, sur internet (également auprès d'éditeurs qui acquièrent ces données), DVD et aux

renseignements;
- verte: le numéro est donné par le numéro des renseignements et sur internet;
- rouge: l'adresse est communiquée, mais pas le numéro de téléphone;
- noire: aucune information n'est divulguée.

Choisir de figurer dans la liste noire pour échapper à des appels anonymes peut toutefois ne pas être judicieux. En effet, l'abonné peut avoir communiqué son numéro à des tiers qui eux-mêmes l'auront donné, etc., ce qui rend le secret tout relatif. Surtout, il risque de ne pas pouvoir être atteint en cas d'urgence. Il est cependant possible de faire installer une seconde ligne qui elle sera sur liste noire. Il est aussi possible d'avoir son numéro de téléphone sous un autre nom, par exemple celui d'un membre de sa famille ou d'une société.

Démarchage téléphonique

Afin de se prémunir contre les appels indésirables, il est possible de faire ajouter un astérisque à côté du numéro inscrit dans l'annuaire (procédure chez Swisscom). Depuis avril 2012, le non-respect de l'astérisque est considéré être une pratique déloyale (art. 3 let. u LCD). Les appels indésirables peuvent être annoncés au Secrétariat d'Etat à l'économie (SECO). Pour les questions relatives à la présence dans l'annuaire, voir le site du Préposé fédéral à la protection des données et à la transparence (PFPDT)

Spam

L'envoi en masse par voie de télécommunication (fax, courriels, sms) de messages publicitaires sans l'autorisation des destinataires est interdit (art. 3 let. o LCD). Les fournisseurs doivent disposer d'un service pour recevoir les annonces de spam. En pratique, il s'agit surtout de suivre les règles de prudence lorsque l'on donne ses coordonnées, protéger les données de ses correspondants, filtrer ses messages et protéger son ordinateur.

En cas d'appel préenregistré ou de sms demandant de composer un certain numéro, il est recommandé de ne rappeler que si le numéro ou son titulaire paraît digne de confiance. Il est recommandé de ne pas répondre à des appels ou des sms de caractère publicitaire pour exprimer son mécontentement, mais de noter les informations importantes et de les signaler à l'opérateur téléphonique.

Concernant les courriels, il est recommandé de supprimer les spams sans les ouvrir, de n'ouvrir en aucun cas les pièces jointes, et de n'acceptez aucune offre commerciale. Il est également conseillé de ne jamais répondre au spam, afin d'éviter de confirmer au spammeur que votre adresse est valide. Celle-ci sera à nouveau utilisée pour vous envoyer davantage de courriels non sollicités et elle pourrait même être revendue. De plus, il est fortement déconseillé de cliquer sur les liens hypertextes des spams!

Vous pouvez informer votre fournisseur de services des télécommunications (p.ex. votre fournisseur d'accès à Internet) des spams reçus et demandez-lui de vous indiquer leur provenance. Selon le PFPDT : « vous devez rendre vraisemblable, par écrit, que vous avez reçu de la publicité de masse déloyale (p.ex. envoyez une copie des spams que vous avez reçus). Pour autant que ces données soient encore disponibles, votre fournisseur devra vous indiquer la date, le moment et la durée de la communication ou du message, l'élément d'adressage ainsi que les noms et l'adresse de l'expéditeur. Selon que le message a été envoyé depuis la Suisse ou depuis l'étranger, vous disposez de plusieurs moyens ».

Pour plus d'informations :
SECO "Réclamation pour toute autre pratique commerciale déloyale"
FEDPOL

Réseaux sociaux

Le PFPDT relève deux aspects nouveaux des réseaux sociaux, s'agissant de la protection des données :

- Ce sont les utilisateurs eux-mêmes qui enregistrent les informations personnelles en question dans les profils Internet et qui donnent donc ainsi leur propre consentement.
- Les particuliers sont ainsi en mesure d'accéder aisément aux données personnelles d'autres particuliers, ce qui peut engendrer des risques. »

Le PFPDT recommande notamment :

- Prenez des précautions avant de publier sur un réseau social vos coordonnées (nom, adresse, numéro de téléphone) ainsi que toute autre donnée ou information personnelle (p.ex. convictions politiques). Utilisez des pseudonymes.
- Avant de publier des données, demandez-vous toujours si, lors d'un entretien d'embauche, vous souhaiteriez être confronté aux données/images en question, et cela, même dans dix ans.
- Respectez la sphère privée de tierces personnes, ne publiez pas leurs données personnelles et ne mettez pas leur nom sur des photos.
- Informez-vous au sujet des fournisseurs du portail et de la manière dont ils assurent la protection de la sphère privée des utilisateurs. Le service en question dispose-t-il d'un label de qualité en matière de protection des données ou de sécurité? Soyez critique à l'égard du comportement du fournisseur.
- Choisissez dans la configuration de votre profil les options permettant de préserver votre vie privée. Limitez l'accès à vos informations et photos à un cercle de personnes déterminé. Ne mettez jamais de contenus délicats sur Internet.
- N'employez pas le même nom d'utilisateur ni le même mot de passe pour tous les services.

Pour plus d'informations :

PFPDT- rubrique « médias sociaux »
Jeunes et médias

Chantage par webcam (sextorsion)

Le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) décrit le phénomène de la manière suivante : « l'auteur se fait passer en général pour une femme très attrayante et prend contact avec des personnes (en majorité des hommes) sur un réseau social. Il tente ensuite de les amener à discuter via un service tel que Skype, afin d'obtenir d'elles des actes à caractère sexuel, qu'elles effectuent devant une webcam. L'auteur enregistre tout et menace ensuite la victime de publier les images ou les vidéos sur Internet si elle ne paie pas une certaine somme d'argent ». Voir aide-mémoire FEDPOL

Conseils de la Prévention Suisse de la Criminalité:

- ne pas céder pas au chantage
- rompre tout contact avec le maître chanteur
- changer d'adresse e-mail
- contacter immédiatement YouTube ou Facebook afin qu'ils puissent supprimer la vidéo/l'image.

Autres recommandations :

- si un versement a déjà été effectué, signaler l'incident à votre poste de Police cantonale
- contacter le Centre LAVI de votre région. Le Centre LAVI (Loi sur l'aide aux victimes d'infractions) vient en aide aux victimes d'infractions, par le biais de l'écoute, de conseils, d'une assistance financière limitée et d'une orientation vers les professionnels qualifiés (voir fiche « Aide aux victimes d'infractions ».
- modifier vos paramètres de sécurité sur vos comptes de réseaux sociaux (Facebook, Google+, Skype, etc…)

Romance Scam

« Dans ce type d'arnaque, la victime croit rencontrer l'âme sœur, par exemple sur un site de dialogue en direct ou un site de rencontres. Une complicité se noue au fil des discussions. En réalité, la victime est en train de dialoguer avec un escroc, qui utilisera cette relation pour lui demander de l'argent. Les justifications à cette demande peuvent être diverses, mais la plupart du temps les escrocs expliquent connaître des difficultés financières passagères. Ces derniers utilisent bien souvent de fausses photos et font diverses promesses (mariage, rencontre future, etc.) pour mieux manipuler leur victime. » (Service national de coordination de la lutte contre la criminalité sur Internet).

Conseils : Il est recommandé de se méfier de son interlocuteur si celui-ci vous promet le grand amour après quelques discussions seulement. De même si ce dernier parle de problèmes financiers et vous demande de l'aide. Il faut également être prudent sur l'identité de l'interlocuteur car il peut facilement tromper la victime sur son identité (nom, photo, etc…).

Harcèlement

Le cyberharcèlement est une forme de harcèlement dont la particularité est de se produire sur Internet. On parle aussi de cyberintimidation ou de cybermobbing. La victime est la cible d'agressions répétées via les médias numériques, par exemple par SMS, sur le tchat et sur Facebook, pendant une longue période.

Il est conseillé d'en parler avec des personnes de confiance, et notamment pour les jeunes d'avoir un dialogue au sein de la famille et avec le corps enseignant. Il est également conseiller de bloquer sans attendre la personne à l'origine du harcèlement et la signaler au réseau social ou au forum de tchat concerné.

Pour plus d'informations :
Jeunes et médias - cyberharcèlement
Prévention Suisse de la Criminalité - brochure d'information

Stalking

Le stalking (de l'anglais « to stalk » = traquer) est une forme particulière de cyberharcèlement où une personne porte une attention obsessionnelle envers une autre et peut inclure le fait de suivre ou de surveiller la victime.

Conseils de la Prévention Suisse de la Criminalité (brochure en pdf) :

- couper radicalement contact avec la personne qui vous harcèle et rester ferme
- refuser les cadeaux et articles commandés à votre nom
- informer l'entourage (pour avoir du soutien, être protéger et leur éviter de divulguer des informations)
- documenter tous les faits et gestes de la personne qui vous harcèle (tenir un journal des événements, conserver les emails, sms, lettres

etc, photographier les cadeaux avant de les rendre, etc...)
- contacter le Centre LAVI de votre région
- contacter la police pour évaluer ensemble les mesures à prendre.

Pour plus d'informations :
Prévention Suisse de la Criminalité > Stalking
Bureau fédéral de l'égalité entre femmes et hommes > Stalking

Procédure

Comme vu plus haut, la personne peut s'adresser à son opérateur pour enquêter sur la provenance des appels ou messages. Lorsque l'auteur d'appels abusifs est identifié, l'opérateur, ou la personne importunée peut adresser à l'auteur une lettre d'avertissement signalant la possibilité de porter plainte en vertu de l'article 179septies précité.

Plainte pénale

Selon l'article 179septies du Code pénal: "celui qui, par méchanceté ou par espièglerie, aura utilisé abusivement une installation de télécommunication pour inquiéter un tiers ou pour l'importuner sera, sur plainte, puni d'une amende". Il est donc possible de porter plainte contre la personne qui abuse du téléphone (pour la procédure de plainte et ses suites, voir la fiche Plainte pénale).

Pour les cas de Romance scam (ou Love scam) : « si vous avez déjà procédé à des versements, il est recommandé de s'adresser à la police cantonale et éventuellement de déposer plainte pour escroquerie. » (Service national de coordination de la lutte contre la criminalité sur Internet).Il n'y a toutefois pas d'escroquerie au sens du droit pénal si la victime aurait pu se protéger avec un minimum d'attention.

Pour plus d'informations :
Office fédéral de la police – rubrique «Les différentes formes d'escroquerie »
Prévention Suisse de la criminalité – rubrique "Escroquerie"

Mesures de protection de la personnalité

En cas de violence, de menaces ou de harcèlement, on peut demander au juge d'interdire à l'auteur de l'atteinte, en particulier, de s'approcher ou d'accéder à un périmètre déterminé autour de son logement (art. 28b ch. 1 CC), de fréquenter certains lieux, notamment des rues, places ou quartiers (ch. 2), de prendre contact avec soi, notamment par téléphone, par écrit ou par voie électronique, ou de causer d'autres dérangements (ch. 3) (voir la fiche Protection de la personnalité).

Recours

Se référer aux fiches cantonales correspondantes.

Sources

Responsable rédaction: ARTIAS

Adresses

Aucune adresse trouvée en lien avec cette fiche

Lois et Règlements

Loi fédérale sur la protection des données
Ordonnance sur les services de télécommunications
Loi sur les télécommunications
Code pénal suisse du 21 septembre 1937 art. 179 septies (CP) (RS 311)

Sites utiles

Office fédéral de la police fedpol
Secrétariat d'Etat à l'économie (SECO)

Prévention Suisse de la Criminalité
Préposé fédéral à la protection des données et à la transparence
Plateforme "Jeunes et médias"
Aide aux victimes en Suisse