PSC INFO

4 | 2016

Dossier
Cybercriminalité

Chère lectrice, cher lecteur,


PSC

L'énergie qu'il faut déployer pour pratiquer le vol et et le mensonge sur Internet, pour y simuler des sentiments ou pour y déverser sa haine, semble sans limites.

Les propos tenus par Stéphane Koch dans notre interview m'ont fait prendre une nouvelle fois conscience que l'éducation est l'une des clés pour prévenir efficacement la criminalité sur Internet. Détenir une compétence médiatique est décisif pour savoir comment se protéger, ne pas croire tout ce qu'on voit ou ce qu'on lit, et pour comprendre comment fonctionnent les dispositifs de communication numériques. Cette protection passe par l'amélioration du niveau de connaissances des utilisatrices et des utilisateurs.

La police municipale de Zurich a engagé un dialogue soutenu avec la population, en se servant systématiquement des médias sociaux. Depuis quelque temps, la population peut suivre le travail policier des deux iCoPs Jean Patrick et Eleni Moschos, en se servant des média sociaux. Tous les deux sont en contact étroit avec des jeunes et des jeunes adultes de Zurich et environs, et se font ainsi l'écho de la population, qui souhaite davantage de transparence et de confiance.

Nos meilleurs vœux pour
la nouvelle année 2017.

Martin Boess
Directeur PSC

Situation actuelle et tendances de la cybercriminalité

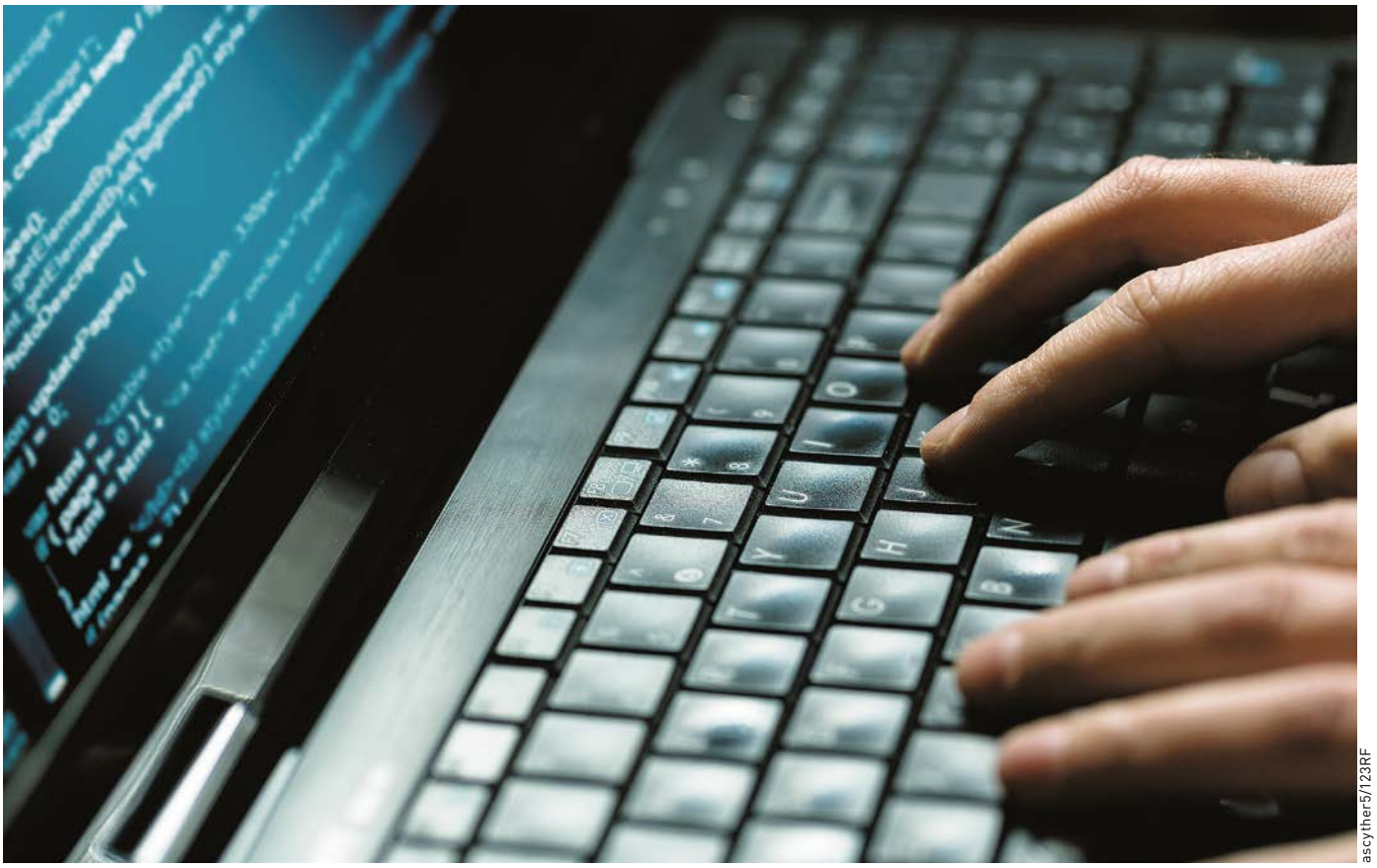
Interview de Stéphane Koch

Monsieur,
Sur votre site www.intelligentzia.ch, vous résumez vos services de la façon suivante : « Conseil & formation en intelligence économique et gestion stratégique de l'information, stratégies numériques et réseaux sociaux, sécurité de l'information ». Les éléments de votre formation sont également impressionnants et se rapportent tous aux médias numériques sous les aspects les plus divers. Vous êtes donc pour nous l'interlocuteur idéal pour une interview visant à présenter à nos lecteurs la thématique « Criminalité sur et via Internet », mettant bien sûr l'accent sur les mesures de prévention de la criminalité et les poursuites pénales.
Mais tout d'abord une question générale en introduction :

Quelle est la différence entre la criminalité « normale » et la cybercriminalité, et comment le Web a-t-il modifié la criminalité ?
La différence se situe principalement au niveau de la dématérialisation de notre société. Dès lors, la cybercriminalité représente globalement une continuité ou une adaptation des formes de criminalité que l'on trouve dans le monde physique. Nombre d'actions criminelles qui se déroulent par le biais de l'utilisation des TIC (technologies de l'information et de la communication), respectivement d'internet, ont une base ancrée dans le monde physique (que ce soit au niveau de l'utilisation d'un serveur, ou d'un ordinateur ou encore d'un périphérique mobile), donc en relation avec un potentiel « for juridique » (base légale liée à l'emplacement d'un serveur/ordinateur dans le monde physique). Les principales différences résident dans l'asymétrie entre le peu de moyens nécessaires pour mettre en œuvre une action cybercriminelle et l'impact important que celle-ci peut avoir, tant au niveau financier que par rapport au nombre de personnes ou d'entreprises qui peuvent être touchées par une action unique. Une autre forme d'asymétrie se situe au niveau de la lutte contre les actions cybercriminelles, même si l'organisation et la diffusion de ces actions (fraude en ligne, cyberattaque, cyberextorsion, etc.) demandent peu de moyens aux cybercriminels. Ce que les autorités concernées vont devoir entreprendre pour lutter contre ces formes de cybercriminalité va – à l'inverse – demander énormément de ressources, que ça soit au niveau humain, en temps, ou au niveau technique. De plus, c'est aussi extrêmement contraignant au niveau de la justice. Les lieux physiques entre l'organisation et la mise en œuvre d'une action cybercriminelle, ainsi que ceux liés à l'emplacement des victimes de cette action ne sont pas nécessairement les mêmes et peuvent être répartis dans différentes zones géographiques du monde qui ne bénéficieront


DR

Stéphane Koch, conseiller et formateur en communication et stratégie numérique, spécialiste de la sécurité de l'information, spécialiste de réputation numérique et réseaux sociaux.



ascyther5/123RF

« La cybercriminalité adapte des formes de criminalité que l'on trouve dans le monde réel. »

pas nécessairement d'accords d'entraide judiciaire. Un autre changement majeur est qu'aujourd'hui les cybercriminels peuvent toucher leurs victimes potentielles chez elles, sans pour autant avoir à fracturer leurs appartements. Et il en va de même pour les entreprises. Le cybercriminel n'est qu'à un clic de souris de sa victime. Et dans le cas de fraude en ligne, les dommages causés peuvent facilement dépasser la valeur des biens qui se trouveraient physiquement dans un domicile donné. Dans un cas de sextorsion, par exemple, la victime pourrait ressentir un traumatisme psychologique identique à celui d'une agression physique, sans pour autant avoir directement été physiquement agressée. De plus, paradoxalement et en opposition aux sciences forensiques classiques, domaine dans lequel l'évolution des technologies a facilité l'investigation (recherche de traces, utilisation de l'ADN, reconstitution et numérisation en 3D des scènes de crime, par exemple), l'évolution du domaine des TIC a compliqué d'autant l'investigation numérique. Des cybercriminels chevronnés sont tout à fait capable de modifier, d'altérer, voire d'effacer des traces numériques. Et si on prend en compte que chaque ordinateur impliqué dans une activité cybercriminelle peut représenter une scène de crime en tant que tel, et qu'un certain nombre d'ordinateurs concernés par « cette activité » appartiendront à des particuliers innocents (leurs ordinateurs mal protégés, ou infectés, ayant été utilisés à l'insu de leurs propriétaires), on prend alors toute la mesure de la complexité de l'investigation numérique. Donc, oui, le web a fondamentalement modifié la criminalité, d'autant plus que les gens n'ont pas été formés à détecter le pendant « cybernétique » des formes de la criminalité classique, alors que « l'intervention » de la police, elle, est devenue beaucoup plus compliquée.

Quels sont, d'après votre estimation, les principaux secteurs de délits sur Internet, ou plus précisément, quels sont selon vous les délits basés sur Internet qui entraînent les plus grands dommages dans notre pays ?

Il n'est pas facile de répondre, car tous les délits ne sont pas signalés, que ça soit au niveau des individus ou celui des entreprises. Parfois on hésite à signaler que l'on a été victime d'une fraude en ligne, d'un chantage, ou d'un vol de données. Mais actuellement les tentatives de phishing visant à injecter un ransomware dans les ordinateurs des particuliers et des entreprises semblent occuper la première place du podium (90% des attaques par phishing contiennent un logiciel de rançon). Europol a d'ailleurs annoncé que ces logiciels de rançon sont considérés comme une menace prioritaire au niveau européen. Les « fraudes au président » occupent aussi une place importante par rapport au montant des

wk1003mike/Shutterstock.com

« 90% des attaques par phishing contiennent un logiciel de rançon. »

fonds détournés. D'autres types de fraudes, aussi basées sur l'usurpation d'identité et l'ingénierie sociale, sont fortement présentes sur les réseaux sociaux. A ce titre, l'usurpation d'identité n'étant pas, en tant que telle un délit pénal, ça facilite le travail des cybercriminels.

Y a-t-il des délits qui touchent plus particulièrement la Suisse et si oui, comment peut-on l'expliquer ?

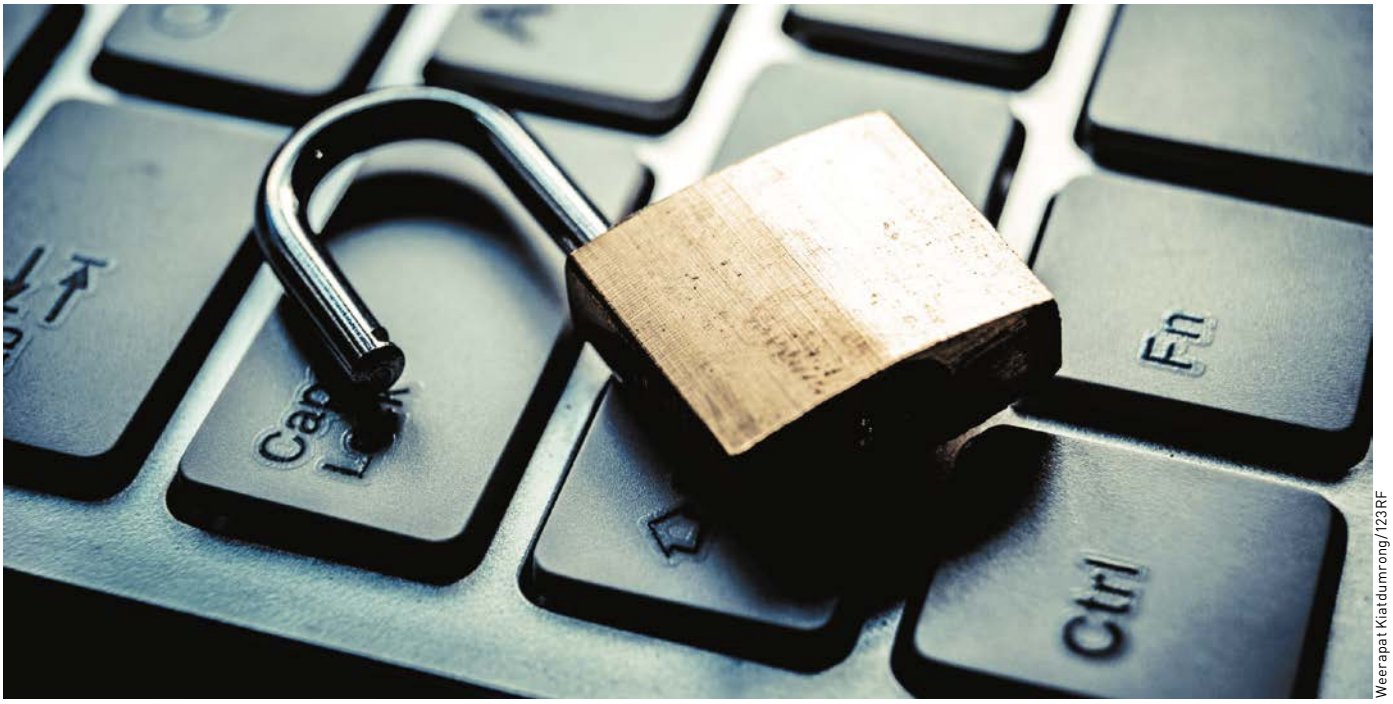
La Suisse est considérée comme un pays riche, dont les citoyens ont un bon niveau de vie. Dès lors, elle est globalement plus ciblée que d'autres pays : attaques sur les infrastructures critiques, attaques par déni de services distribué (DDOS), qui, même quand elles se déroulent à l'étranger, affectent les entreprises et les utilisateurs en Suisse, étant donné la répartition mondiale des infrastructures internet et leur interdépendance en terme de connectivité. Ce type d'attaque (DDOS), suivant son importance, est à même de freiner voire de bloquer l'accès à de multiples services qui dépendent de l'accès à internet, que ça soit à un niveau local ou global. En mars 2016, des sites Web suisses de banques et de commerces en ligne avaient été victimes d'un groupe cybercriminel nommé Armada, qui avait réussi à bloquer l'accès à leurs services suite au refus des entreprises concernées de payer la rançon demandée par les cybercriminels. En septembre 2016, « Internet » a connu l'attaque par DDOS la plus importante jamais observée (Mirai botnet). Sa particularité résidait dans le fait que pour mener à bien leur offensive, les cybercriminels se sont servis d'environ 400 000 caméras connectées à travers le monde, dont les « accès administrateurs » par défaut n'avaient pas été modifiés par leurs propriétaires. Une attaque similaire, dont les effets se sont aussi fait ressentir en Suisse, a eu lieu le mois suivant. Mais ce n'est là qu'un exemple, auquel on peut ajouter les attaques par tentative de phishing, le blocage de l'accès aux fichiers numériques – des particuliers ou des entreprises – par des « logiciels de rançon » (ransomwares, qui bloquent l'accès aux fichiers jusqu'à ce que la rançon soit payée), les vols de données d'entreprises (bancaires ou autres), etc. Ce qui fait la différence entre un pays et un autre, ce sont les moyens que ce pays va mettre en œuvre pour lutter contre la cybercriminalité ou d'autres formes d'attaques initiées par le biais des réseaux connectés, ainsi que le niveau de « conscience » de ses citoyens et des entreprises. Et dans ce domaine la Suisse est à la traîne ! Il y a des manquements considérables dans les moyens de lutte contre la cybercriminalité, et le niveau de connaissance et de réactivité des entreprises et des individus est largement insuffisant. En ce qui concerne les moyens, c'est un problème politique. La Suisse est victime de son fédéralisme, à l'heure où le monde est interconnecté, et fait peu de cas des frontières physiques, culturelles et linguistiques. Seule Zurich possède une brigade autonome de lutte contre la cybercriminalité (les autres cantons ont dans la majorité des cas une unité de lutte contre la criminalité informatique, qui opère en soutien des autres services de polices), et la majorité des magistrats ne sont pas formés aux TIC (technologies de l'information et de la

communication) et les dossiers s'empilent. Pour ce qui est des entreprises et des particuliers, le manque de conscience et de connaissances fait que la Suisse représente – en toute logique – un terrain privilégié pour les cybercriminels. Le 22e rapport semestriel de MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information) illustrait bien cette situation, son thème prioritaire était « la gestion des lacunes de sécurité ». Comme le disait récemment Guillaume Poupard, directeur général de l'Agence nationale française de la sécurité des systèmes d'information, l'Anssi : *« Au sein des entreprises, il y a évidemment un responsable de la sécurité des systèmes d'information : il est indispensable, mais pas suffisant. L'idée, c'est vraiment de se dire que chacun est acteur de cette cybersécurité : le PDG, le directeur juridique, le directeur financier… Chacun a un rôle à jouer, y compris l'intérimaire, généralement oublié dans les procédures, alors qu'il a souvent accès aux systèmes. »* Cette situation, qui fragilise l'économie du pays, respectivement sa compétitivité et donc sa croissance, ne changera pas, tant que les mentalités n'évolueront pas. A l'heure actuelle, il n'y a quasiment rien dans l'enseignement scolaire primaire, secondaire, ou dans celui des hautes écoles, qui puisse permettre à tout un chacun d'intégrer les connaissances nécessaires pour comprendre, assimiler et maîtriser la transformation numérique de notre société (l'ensemble de ces connaissances est regroupée sous la dénomination de « littératie numérique », l'Europe quant à elle a mis en place le programme de formation en culture numérique « DLit2.0 Curriculum »).

http ://www.digital-literacy2020.eu/content/sections/index.cfm/secid.59

Y a-t-il en Suisse des catégories spécifiques de victimes ? Y a-t-il des personnes, des groupes ou des institutions particulièrement menacés par la cybercriminalité ?

Le comportement des cybercriminels est assez logique : ils cherchent à optimiser le rendement de leurs actions criminelles et vont donc s'attaquer au plus faible. En terme de cybercriminalité, ça signifie que les attaques viseront en premier lieu les ordinateurs - ou autres outils ou périphériques informatiques – les moins bien protégés. Pour reformuler la question, on pourrait dire que c'est le potentiel de profit qui définit la cible. Les entreprises seront donc une cible importante, mais l'accumulation de petits profits par la multiplication des attaques sur les particuliers génère beaucoup de revenu tout en créant un risque minime pour les cybercriminels (chaque ordinateur individuel touché étant une nouvelle affaire pour la police et la justice). Il est important de comprendre néanmoins que la majorité des fraudes demandent une intervention ou une « collaboration » de la victime. Dès lors le facteur de réussite d'un grand nombre de ces fraudes en ligne repose sur le manque de connaissance ou l'inconscience de l'utilisateur. Il ne faut pas non plus négliger le fait que certains gouvernements (ou groupes soutenus par des gouvernements) ont parfois des comportements cybercriminels et, qu'à ce titre, les institutions ou certains pôles stratégiques peuvent représenter des cibles de choix. La récente attaque sur la société RUAG en est un bel exemple : les attaquants ont utilisé un logiciel espion (un malware) pour s'infiltrer dans les serveurs de RUAG et piller son patrimoine



Weerapat Kiatdumrong/123RF

« Les cybercriminels tentent d'optimiser leur rendement et vont donc s'attaquer au plus faible. »

neydt/123RF

«Les Hacktivists sont une sorte de Black Blocs numériques, tel que le mouvement Anonymous, avec des revendications d'ordre sociétal et politique.»

intellectuel et industriel. Les instigateurs de cette cyberattaque – qui n'ont toujours pas été formellement identifiés à ce jour – ont pu agir plusieurs mois avant que l'on finisse par détecter leur présence.

Avez-vous des connaissances sur les criminels ? S'agissant de la «criminalité hors ligne», il existe des groupes de criminels spécialisés et des mobiles bien définis. Peut-on observer la même chose au niveau de la cybercriminalité et si oui, sous quelles formes ?

Il n'est pas évident de dresser un «état des lieux» de la cybercriminalité qui soit exhaustif, car c'est un domaine polymorphe qui se compose de nuance de gris. Par exemple, il n'y a pas les «hackers» et le reste du monde. Tout un ensemble de «courants» sont présents et il est important de les définir et de les catégoriser: il y les **«Black Hats»** (comportement criminel); les **«White Hats»** (comportement éthique, hackers éthiques, utiles à la société, ils font remonter des failles de sécurité); les **«Grey Hats»** (un peu des deux); les **«State sponsored hackers»** (comportements criminels – officieusement – soutenus par un Etat, ou nationalistes soutenant de facto leur pays par des actions offensives); les **«Hacktivists»** (forme de Black Blocs numériques, tel que le mouvement **Anonymous,** avec des revendications d'ordre sociétal et politique. A la base, ce ne sont pas des criminels, mais la nature de leurs comportements peut l'être); les **«Cybercriminels»** (extension et développement des activés criminelles classiques dans le monde cybernétique); les **«Script kiddies»** (adolescents généralement, ou personnes utilisant des programmes informatiques créés par d'autres – et possédant un potentiel d'attaques – car eux-mêmes ne possèdent pas le niveau d'expertise pour les développer); les **«Cyber-mercenaires»** (personnes monnayant leurs connaissances informatiques. «L'affaire Giroud» en est un exemple. En 2014, cet encaveur valaisan a été accusé d'avoir embauché un cyber mercenaire pour aller voler des documents l'incriminant sur les ordinateurs de deux journalistes). En résumé, tout ce petit monde représente à la fois la diversité et la complexité des acteurs du monde numérique. Cette complexité est encore accrue par le fait qu'aujourd'hui, les cybercriminels ont des comportements d'entrepreneurs, et certains entrepreneurs (ou des gouvernements) ont parfois des comportements de cybercriminels. On observe aussi la présence de «cybercriminels à temps partiel», qui agissent épisodiquement dans l'obscurité, tout en étant au grand jour employés par des entreprises, car ils évaluent que la prise de risque est minime par rapport aux gains potentiels (théorie des opportunités en criminologie, Walsh, 1986). Il y a aussi ceux qui cherchent des failles de sécurité pour les revendre – entre autres – sur le Darknet (marché gris de la cybercriminalité). Ils ne commettront pas de crimes eux-mêmes, mais fourniront les «armes et les munitions», respectivement les ressources nécessaires à leur mise en œuvre à des cybercriminels (entre autres). C'est un marché très lucratif, et peu risqué. Certaines failles de sécurité peuvent se

revendre plusieurs centaines de milliers de francs. A ce titre, le marché gris des failles de sécurité fournit non seulement les cybercriminels, mais aussi des entreprises, des gouvernements et leurs services de renseignements. Certains gouvernements ont alloué un budget spécifiquement dédié à l'achat de ce type de ressources (failles de sécurité, ou vulnérabilités inconnues des concepteurs des logiciels, pour lesquelles il n'existe pas de parade ou de correctif, et qui par leur nature permettent d'accéder à des programmes, respectivement des ordinateurs en contournant les mesures de sécurité présentes. Ce type de faille est aussi appelé 0Day, ou vulnérabilité Zero day).

En 2012, le Dr Michael McGuire, du John Grieve Centre, a tenté de dresser un portrait de la relation potentielle entre le crime organisé et la cybercriminalité, dans une étude nommée: «Organised Crime in the Digital Age». Selon cette étude, 80% des groupes cybercriminels reposeraient sur une forme de structure organisée, sans pour autant que ces groupes organisés appartiennent tous à une organisation criminelle classique. 43% des membres de ces organisations cybercriminelles avaient plus de 35 ans, et 29% moins de 25 ans. La moitié des groupes comprennent une structure de six personnes ou plus, avec un quart comprenant 11 ou plus. 25% des groupes actifs ont agi pendant moins de six mois.

www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Vous avez également une formation en lutte contre la criminalité économique. Pouvez-vous nous parler de la lutte contre la criminalité économique sur Internet ? Quels en sont les points forts ou quels devraient-ils être ? De quels moyens dispose-t-on pour les poursuites pénales et lesquels font défaut ?

Avec la montée en puissance de l'utilisation des TIC, la dématérialisation croissante des services et l'émergence de l'internet des objets (de plus en plus de connexions et d'échanges de données entre des périphériques connectés à des éléments de notre quotidien, où le frigo connecté ne pose pas trop de problème, mais une pompe à insuline, un pacemaker, une voiture, ou encore la serrure d'un appartement, eux, oui), on assiste à une augmentation importante des cas de criminalité économique en rapport avec le domaine du numérique. Le problème est que – comme expliqué à la question 3 – la police et la justice n'arrivent pas à obtenir les ressources qui leur seraient nécessaires pour être en mesure de traiter la multitude de cas qui se présentent à eux. Et les cas suisses ne se limitent pas aux frontières de la Suisse, ils nécessitent la plupart du temps une collaboration au niveau européen ou mondial. Cette collaboration est souvent soumise à des demandes d'entraide judiciaire qui vont prendre du temps, et cette latence profite pleinement aux cybercriminels. Il existe bien la Convention sur la cybercriminalité du Conseil de l'Europe, qui est entrée en vigueur en Suisse en 2012, mais tous les pays ne l'on pas signée, et les cybercriminels exploitent logiquement ce genre de failles. Ils chargent des spécialistes du domaine juridique d'évaluer quelles seront – légalement – les meilleures bases arrière pour lancer leurs attaques.

Si vous deviez conseiller à un avocat spécialisé dans la protection des données des stratégies dans le domaine de la cybercriminalité, quelles seraient vos recommandations pour les actions de poursuite pénale en Suisse ?

Il doit y avoir une vraie réflexion au niveau pénal, et elle ne doit pas être l'œuvre uniquement de juristes et de la «politique». Dans le domaine des TIC, le système de milice a atteint ses limites. Il est nécessaire que les professionnels – du secteur public et du secteur privé – qui, dans leur pratique, luttent contre la cybercriminalité, puissent exposer les problèmes auxquels ils sont confrontés. Les connaissances lacunaires des politiques en matière de société de l'information (y compris dans les commissions spécialisées), impactent extrêmement négativement sur leur capacité à comprendre les problèmes liés à la lutte contre la cybercriminalité. Par exemple, début 2013, Me François Charlet, un avocat spécialisé dans la protection des données, et moi-même, avions été invités par un parti politique pour partager quelques réflexions sur les problématiques liées aux TIC. Suite à cette réunion, il était ressorti que la pénalisation de l'usurpation d'identité était un dossier prioritaire. En 2016, ce qui a progressé, c'est uniquement le nombre de victimes! Il

rangizzz/123RF

«La police et la justice nécessitent une collaboration au niveau européen ou mondial, et des demandes d'entraide judiciaire qui vont prendre du temps; les cybercriminels le savent.»

en va de même avec les fuites de données : l'Europe a mis en place la Directive NIS « Network Security and Information » qui entrera en vigueur en 2018 (www.riskinsight-wavestone.com/2016/03/8822/). Elle contient une obligation de déclaration aux autorités compétentes en cas de piratage d'infrastructures considérées comme étant critiques, d'intrusion dans les systèmes informatiques, ainsi que l'obligation, pour les entreprises victimes de fuite de données, de signaler leur cas aux régulateurs nationaux, et aux personnes touchées, sous trois jours. Elle impose aussi aux acteurs concernés de prendre les mesures nécessaires pour assurer une sécurité efficace de leurs infrastructures. La Suisse – que certains présentent comme le futur coffre numérique du monde – se doit d'appliquer au plus vite de telles directives.

Au niveau des particuliers, là aussi la justice est à la traîne et nombre de magistrats ne semblent pas être connectés avec les réalités de notre société… connectée. J'ai traité des cas de *sextorsion* et de *revenge porn* (pratique qui consiste à diffuser des images intimes, à caractère sexuel, du conjoint sans le consentement de celui-ci), et dans le cas du *revenge porn,* selon le code pénal suisse, la victime – suivant son âge – pourrait être potentiellement considérée comme coupable de création et de diffusion de contenus à caractère pornographique. Non seulement on ne reconnaît pas son statut de victime, mais l'agresseur ne risque pas grand-chose non plus. Dans le canton de Vaud, en 2013, un homme reconnu coupable de la diffusion de vidéos intimes de son ex-copine, sur un site pornographique, n'a été condamné qu'à 50 jours amende avec sursis (les femmes représentent plus de 80% des victimes). Il en va de même lorsque qu'une femme se fait violer : si les agresseurs filment la scène et la partagent dans un groupe WhatsApp – comme c'est déjà arrivé – ou sur le Net, le ou les agresseurs seront éventuellement condamnés pour le viol, mais le juge ne prendra pas en compte le fait d'avoir filmé et partagé le viol, alors que le fait de filmer un viol en vue de partager devrait – dans l'intention – être considéré pénalement comme un acte de cruauté ! Le jugement devrait aussi prendre en compte une obligation légale de retrait des contenus incriminés du Net, sous peine d'une autre sanction en cas d'échec. En résumé, pour que la loi évolue, il faut que les mentalités évoluent. Il est nécessaire que les autorités concernées développent une conscience de la victime et des traumatismes potentiels qui résultent d'une agression en ligne, et du stress posttraumatique dû au risque de réapparition des contenus humiliants pour la victime. Cette évolution des mentalités est aussi nécessaire pour que les magistrats comprennent mieux les contraintes liées au travail d'enquête de la police en rapport avec le Net. Par exemple « l'investigation secrète », qui autorise l'utilisation d'une identité d'emprunt (dont la réglementation a été harmonisée au niveau fédéral et est entrée en vigueur en 2005), doit être plus facile à mettre en œuvre.

De quelle manière la criminalité sur Internet va-t-elle évoluer ? Peut-on s'attendre à de nouveaux types de délits ?
Le spécialiste en criminologie Michael McGuire définit la cybercriminalité comme étant la quatrième ère de la criminalité. Pour ma part, je pourrais résumer la question par « plus de crimes et moins de moyens pour les combattre ». Il ne faut néanmoins pas accepter l'augmentation de la cybercriminalité comme une fatalité. Mais il faut se donner les moyens de la combattre. Et plus encore que les moyens financiers, légaux et policiers, c'est la « connaissance » qui est et sera toujours le « nerf de la guerre » contre ces formes de criminalité. Au final, les cybercriminels utilisent les mêmes technologies que nous. Une grande majorité des cyberattaques et des fraudes en ligne reposent sur la méconnaissance des utilisateurs. Si on prend le phishing, par exemple, ça fait près d'un quart de siècle que le Web existe, et on n'a toujours pas appris aux utilisateurs à lire correctement un lien internet (URL), dont la manipulation est l'élément de base sur lequel repose la fraude.

Quel est le rôle du Darknet dans la cybercriminalité ? La police a-t-elle une chance de détecter les crimes dans le Darknet ou faudrait-il modifier la législation ?
La problématique représentée par ce que l'on nomme le Darknet n'est pas uniquement un problème de législation. Les outils qui permettent l'anonymat, et que l'on associe généralement au Darknet sont les mêmes outils que ceux utilisés par les défenseurs des droits humains ou par des journalistes dans des pays non démocratiques pour rapporter des cas d'atteintes aux libertés individuelles, ou pour dénoncer les mauvais agissements de certains gouvernements ou des cas de corruption. Pour résumer, ces outils sauvent aussi des vies. Donc la solution ne passe pas par un affaiblissement des technologies (de chiffrement par exemple), elle passe par l'amélioration du niveau d'expertise et une meilleure collaboration et un meilleur échange d'informations entre les différents services de police et de justice, tant au niveau national qu'international. De plus, les faits nous ont prouvé que le Darknet n'est pas un espace impénétrable : en 2013, le FBI a réussi à fermer « Silk Road » une des plus grandes places de commerce illégal du Darknet. Puis il a réussi à infiltrer – dès le début de son lancement – Silk Road 2.0 pour le fermer en 2014. Aujourd'hui, une nouvelle version du site existe, et connaît un développement florissant, surtout dans la vente de drogues. Mais quoi de différent avec le monde physique ? On n'a pas réussi à y éradiquer la vente de drogue non plus. Ce que je veux dire, c'est qu'avec les moyens et le niveau d'expertise adéquat, la police est en mesure de lutter sur tous les fronts technologiques.

scanrail/123RF

«Avec les moyens et le niveau d'expertise adéquat, la police est en mesure de lutter sur tous les fronts technologiques.»

Quels sont les principaux conseils pour se protéger de la cybercriminalité ?
Quitte à me répéter : l'utilisateur, qu'il s'agisse d'un individu ou d'une personne morale, doit fondamentalement améliorer son niveau de connaissance. Rien ne pourra se faire sans cela. L'Etat, quant à lui, doit lui mettre à disposition les moyens pour pouvoir le faire. Que cela passe par l'instruction publique, les entreprises, et pourquoi pas l'armée (on pourrait imaginer une formation dispensée pendant l'école de recrue). En France, par exemple, l'Institut national des hautes études de la sécurité et de la justice (INHESJ) et la Délégation interministérielle à l'intelligence économique (D2IE) se sont engagés dans une démarche partenariale visant à former des «Conférenciers en sécurité économique» issus du monde économique : entreprises, pôles, clusters, consultants, etc. L'objectif est de délivrer un message général, uniformisé et cohérent sur la sécurité économique et de promouvoir les outils existants ou à venir. Il est aussi de la responsabilité de l'Etat d'identifier les menaces que les entreprises et les citoyens ne peuvent pas être en mesure d'identifier. Il faut mettre en place des structures gouvernementales, qui utiliseraient les ressources disponibles dans le secteur privé, pour proactivement rechercher les menaces à venir (failles 0-day / vulnérabilité Zero day), évaluer le matériel utilisé dans les infrastructures stratégiques du pays (hardware, software, firmware). Le futur de la sécurité économique de la Suisse, de sa capacité d'innovation et de croissance, est à ce prix. Au niveau légal, les entreprises qui ne protègent pas suffisamment leurs données doivent être pénalisées.

L'utilisateur, quant à lui, a pour responsabilité de comprendre les outils qu'il utilise. Il n'est plus acceptable d'être dans cette forme de déni de responsabilité vis-à-vis de technologies que l'on utilise au quotidien. Alors que dans notre société physique, la grande majorité des gens acceptent la responsabilité de devoir s'informer sur les médicaments qu'on leur aura prescrit, ou sur la composition des aliments qu'ils vont consommer, ou encore sur le mode d'utilisation et le fonctionnement du véhicule qu'ils vont utiliser. Ils rechignent, mais acceptent néanmoins de s'adapter au tri des déchets et aux «nouvelles règles» liées à l'évolution et aux changements qui surviennent dans notre monde physique. Ce n'est pourtant pas différent avec les TIC ! Elles sont à la base de la transformation numérique de notre société, et le monde virtuel n'en est que la «réalité» dématérialisée. Ça reste quand même la société, notre société, celle dans laquelle on vit, et non un «espace virtuel» à part de celle-ci, comme l'a dit Edgard Morin : «dans une société complexe, il faut adopter une pensée complexe». Je me permettrais de reformuler son propos par «prendre le temps d'apprendre à vivre avec son temps, pour ne pas exister hors du temps».

Qui lutte contre la cybercriminalité et protège les structures numériques en Suisse ?

La stratégie du Conseil fédéral pour une Suisse numérique et son impact sur la sécurité de la population

Le Conseil fédéral a adopté en avril 2016 la stratégie «Suisse numérique», qui doit permettre de tirer pleinement parti de l'expansion du numérique. Il est capital, dans une société informée et démocratique, que les habitants de notre pays puissent utiliser les technologies de l'information et de la communication modernes de manière compétente et sûre dans leur vie quotidienne.

Dans le cadre de cette stratégie doivent notamment être mises en œuvre différentes mesures ayant trait à la sécurité :

- Organisation d'une consultation sur une révision de la loi sur les télécommunications visant à doter la Confédération d'instruments pour protéger les jeunes contre les risques inhérents aux services de télécommunication. Les fournisseurs d'accès Internet seront tenus de conseiller leur clientèle sur les mesures visant à protéger la jeunesse et de bloquer les contenus pornographiques pédophiles (mise en œuvre d'ici fin 2016).
- Examen des possibilités pour protéger la sphère privée des consommateurs de médias numériques, spécialement les enfants et les jeunes, dans le cadre de la révision de la loi sur la protection des données (mise en œuvre d'ici fin 2016)
- Nouvelle loi visant à renforcer la protection de la jeunesse contre les contenus inappropriés qui oblige à fixer des limites d'âge et à établir des restrictions pour la remise de vidéos et de jeux électroniques (mise en œuvre d'ici fin 2017)
- Analyse de l'évolution de la sécurité et du traitement des données (big data), évaluation des conséquences pour la société et réexamen du cadre légal actuel (mise en œuvre d'ici mi-2018)

Pour plus d'informations :
www.bakom.admin.ch/bakom

Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)

Le SCOCI est rattaché à une division principale de l'Office fédéral de la police (fedpol) : la Police judiciaire fédérale.

Le SCOCI effectue des recherches actives non ciblées sur Internet. Les dossiers créés sont analysés et les cas relevant du pénal sont transmis aux autorités de poursuite compétentes en Suisse et à l'étranger. Les contenus sur Internet sont considérés comme relevant du pénal dans différents cas de figure (liste non exhaustive) :

- Pornographie dure (actes sexuels avec des enfants ou des animaux, actes sexuels violents)
- Pornographie légale accessible aux mineurs et proposée sans mesure de protection des enfants ni contrôle d'âge
- Représentation de la violence
- Racisme, extrémisme
- Atteinte à l'honneur, menaces
- Escroquerie, criminalité économique
- Intrusion non autorisée dans un système informatique
- Diffusion de virus informatiques, détérioration de données

Les contenus suspects repérés sur Internet peuvent être signalés sur le site www.cybercrime.ch (formulaire).

Le SCOCI est un centre de compétences à disposition du public, des autorités et des fournisseurs d'accès Internet pour toute question juridique ou technique concernant la cybercriminalité. En tant que service national chargé de coordonner la lutte contre la cybercriminalité, il est aussi l'interlocuteur des services étrangers homologues.

Pour plus d'informations :
www.cybercrime.admin.ch

Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI)

MELANI fonctionne en tant que modèle de coopération entre le Département fédéral des finances (DFF), représenté par l'Unité de pilotage informatique de la Confédération (UPIC), et le Département fédéral de la défense, de la protection de la population et des sports (DDPS), représenté par le Service de renseignement de la Confédération (SRC).

MELANI s'adresse à deux groupes de clients : Le **cercle ouvert** est à disposition des particuliers utilisant un ordinateur et Internet ainsi que des PME en Suisse.

Son offre :

- Informations sur les dangers et les mesures possibles en rapport avec l'utilisation des technologies de l'information et de la communication modernes (p. ex. : Internet, banque en ligne) ;
- Rapports sur les tendances et les évolutions principales dans le domaine

des technologies de l'information et de la communication en relation avec les incidents et les événements observés ;
- Formulaire permettant aux utilisateurs de signaler les incidents dont ils sont victimes.

Le **cercle fermé** est réservé à différents exploitants d'infrastructures critiques à l'échelon national (p.ex. : fournisseurs d'énergie, entreprises de télécommunication, banques). MELANI a vocation à protéger ces infrastructures vitales, en particulier quand ces dernières dépendent du bon fonctionnement des infrastructures d'information et de communication.

Pour plus d'informations :
www.melani.admin.ch

Le rapport « Sûreté de l'information – Situation en Suisse et sur le plan international » est établi semestriellement. Le dernier numéro en date (2016/I) a été publié fin octobre. Il présente les principaux incidents survenus au cours du premier semestre au plan national et international. Il consacre son point fort à l'expansion de la cyber-extorsion.

www.melani.admin.ch → Documentation → Rapports → Rapports sur la situation → Rapport semestriel 2016/1

Formes fréquentes de cyberdélinquance

Du fait de sa longue expérience en la matière, la PSC est souvent le premier interlocuteur des citoyens préoccupés. Agissant aussi comme conseiller de premier recours et de guichet virtuel pour les victimes d'un délit sur Internet, la PSC passe en revue les éléments qui pourraient constituer une plainte ou indique à qui s'adresser auprès de la police. En parlant avec les victimes, elle peut en outre collecter de précieux renseignements sur les stratégies des malfaiteurs, ce qui lui permet ensuite d'actualiser ses messages de prévention en fonction des diverses formes de cyberdélinquance.

La PSC décrit ici les délits qui lui sont le plus souvent rapportés par la population, soit parce que les personnes qui appellent sont elles-mêmes lésées, soit parce qu'elles soupçonnent qu'un de leurs proches, parent ou ami, pourrait l'être.

Désir et amour font le bonheur des vautours

On sait que les filous utilisent la Toile pour prendre les pigeons dans leurs filets. Pour qu'une personne tombe dans le panneau, il suffit qu'elle avale tous les bobards qu'on lui raconte et rien n'est plus simple lorsque la victime est prête à y croire. Cette disposition à se faire avoir naît d'un manque, donc d'un besoin subjectif. Un besoin d'argent, de prestige, de proximité physique ou psychique.

Les deux formes d'escroquerie ou de chantage décrites ici fonctionnent avec ces besoins et visent par conséquent des personnes à la recherche de chaleur humaine ou de plaisir physique, même si elles présentent chacune des profils très différents.

Romance scam

Le mensonge de l'amour des escrocs au mariage sur Internet

Les expressions anglaises de *romance scam* et de *love scam* désignent un certain type de fraude sur Internet. Cette arnaque vise des personnes qui recherchent ardemment un ou une partenaire. Elle est particulièrement sournoise parce qu'en plus d'aller jusqu'à ruiner une victime, elle la laisse le cœur brisé. Comment ça marche ?

Mode opératoire

Sur des sites de rencontre et des réseaux sociaux, les escrocs se présentent comme des soupirants transis d'amour (hommes ou femmes), et ce, bien évidemment sous de fausses identités. Ils couvrent leurs victimes de compliments et de serments puis essaient de leur soutirer de l'argent avec des histoires bouleversantes. Prenons un exemple : sur un site de rencontres, un certain Bob Tyler[1] se présente comme ingénieur, bien de sa

1 Noms fictifs

stokkete/123RF

Romance scam : ce cyberdélit est particulièrement sournois, parce que la victime se retrouve ruinée et le cœur brisé.

personne et avec une belle situation. C'est ainsi qu'il entre en contact avec Danièle Chappuis[2], vivant à N. Après quelques échanges, il devient très insistant et lui déclare toute sa flamme : à le lire, elle est la femme de sa vie. Madame Chappuis n'est pas très méfiante sur Internet et ne sait peut-être pas combien il est facile de créer des profils inventés de toutes pièces. Elle n'imagine pas non plus que des adresses électroniques et des numéros de téléphone ne peuvent en rien garantir le pays d'origine de leurs interlocuteurs. Par ailleurs, Madame Chappuis a envie d'une relation et aime cet échange romantique comme elle n'en a pas connu depuis longtemps. Ainsi donc, la chance lui sourit enfin et elle est convaincue de vivre désormais un grand amour ! Les *love scammers* (littéralement auteurs d'escroqueries à l'amour) sont passés maîtres dans l'art de séduire, de complimenter et d'embobiner. Ainsi, plus Mme Chappuis tchatte et téléphone avec M. Tyler, plus elle se convainc de l'authenticité des sentiments de son correspondant. Pourquoi sinon quelqu'un se donnerait autant de peine ? On dit que l'amour rend aveugle, mais pas seulement. Avec l'arnaque à l'amour s'ajoute le fait que les mécanismes spécifiques de mystification et de tromperie sur Internet ne sont souvent pas connus, raison pour laquelle les mensonges sont encore plus difficiles à reconnaître.

Une fois l'escroc certain d'avoir créé une dépendance émotionnelle suffisamment forte chez sa victime et que la perspective d'une rencontre dans la vie réelle se concrétise, il commence à raconter tous ses problèmes : accidents, maladies, difficultés avec des autorités, urgences familiales et professionnelles. Alors que M. Tyler affirme être en route pour la Suisse, il annonce qu'il doit impérativement faire un détour par Dubaï pour des raisons professionnelles. Or, il ne peut conclure un marché dans cette ville que s'il est en mesure d'avancer une certaine somme d'argent. Hélas, pour toutes sortes de raisons, M. Tyler ne peut disposer immédiatement de cet argent. Mme Chappuis aurait-elle la gentillesse de lui virer ce montant le plus rapidement possible afin qu'il puisse ensuite enfin venir la retrouver ? Il n'est pas rare que de tels mensonges permettent à ces filous d'encaisser plusieurs centaines de milliers de francs avant que leurs victimes réalisent que ce n'était pas leur cœur qui était convoité, mais leur argent.

Et comme les courriels, les numéros de téléphone et les profils sont falsifiés ou anonymisés, que les paiements ont été faits par Western Union ou Moneygram, les opérations financières perdent toute traçabilité et l'argent est perdu. La confiance des victimes a été totalement ébranlée et elles éprouvent un vif sentiment de honte.

Mode opératoire de type « haute école de l'escroquerie »

Et comme si cela ne suffisait pas déjà, les mensonges et les tromperies vont plus loin ! La victime qui ne paie pas ou qui ne veut plus payer est assaillie de fausses lettres de la police ou de la justice qui lui font croire que l'auteur du délit va pouvoir être arrêté. Elle est convaincue que pour cela, il lui faut de nouveau avancer de l'argent. On lui fait croire qu'un enquêteur spécialisé d'Interpol a identifié Bob Tyler et qu'il sait ainsi que Danièle Chappuis a été sa victime. Pour récupérer son argent, cette dernière doit procéder à tels paiements à la douane et au ministère de la Justice de Dubaï. Il arrive ainsi que la victime soit escroquée deux fois et qu'au lieu de recevoir de l'aide, elle s'endette encore davantage. Les auteurs de ces délits sont inventifs, innovants, persévérants, patients, rompus à toutes les astuces et très au fait de toutes les possibilités qu'offrent Internet. En dernière analyse, comme nous l'avons dit, cette activité criminelle peut s'avérer extrêmement rentable.

Mesures de prévention contre le romance scam

Avoir confiance, c'est bien mais il vaut parfois mieux être sur ses gardes. Dans les escroqueries commises par Internet, la prévention est d'autant plus importante que les auteurs des délits ne courent quasiment aucun risque d'être identifiés. Les personnes informées qui sont à la recherche d'un ou une partenaire identifient assez bien une arnaque parce que le mode opératoire de celle-ci est très standard. C'est la raison pour laquelle il est important de faire connaître cette forme d'escroquerie. Et dans tous les cas, ce conseil vous évitera bien des déconvenues :

Ne remettez jamais de l'argent à des gens que vous ne connaissez pas

2 Noms fictifs

personnellement, c'est-à-dire que vous n'avez pas rencontrés dans la vie réelle. Aussi émouvante et belle que soit l'histoire qui a ravi votre cœur !

La sextortion, un chantage avec des photos et des vidéos compromettantes

Le frisson de plaisir avant… la gueule de bois

On dit que pour appâter un homme, il vaut mieux le faire saliver avec les plaisirs de la chair qu'avec de grands serments d'amour. Or, dans la réalité, ce sont plutôt des femmes (mais pas seulement !) qui sont victimes d'arnaques à l'amour, tandis que les hommes sont plus la cible de *Sextortion.* « Sextortion » est un mot-valise qui associe sexe et extorsion. Sa signification tombe sous le sens puisqu'il s'agit d'un délit dans lequel des gens, hommes le plus souvent, sont abordés de manière particulièrement directe par des femmes très sexy sur les réseaux sociaux (Facebook, WhatsApp, etc.). Après un rapide chat, la personne est invitée à mettre sa webcam en route et à continuer sur Skype. Là, la discussion prend rapidement une tournure plus excitante et prometteuse. L'interlocutrice propose un petit show érotique et demande à son nouveau partenaire d'en faire de même. A deux, tout est plus rigolo. Mais la partie de plaisir ne dure pas longtemps et les choses se gâtent. En effet, l'interlocutrice dévoile son jeu dès le moment où elle dispose de matériel compromettant. Elle réclame alors de l'argent sans quoi elle publiera les images et les vidéos sur YouTube ou les enverra directement à toute la liste d'amis de sa victime.

loganban/123RF

Les victimes de sextorsion sont surtout des hommes.

Payer ne règle rien !

Les victimes en éprouvent une honte incommensurable et n'osent même pas parler à leurs proches de ce chantage. Par peur que leur famille, des amis ou des collègues de travail les découvrent dans leur intimité, quelques-unes paient la rançon exigée, en général quelques centaines d'euros, de dollars ou de francs suisses.

Dans ce cas comme dans le précédent, il est important d'être bien informé, ce qui n'est en l'occurrence pas très difficile : Ne le faites pas ! Pas de cybersexe avec une webcam si vous ne connaissez pas votre interlocutrice! Tout ce qui est transmis sur Internet présente un potentiel d'abus. Des photos et des vidéos intimes sont le matériel par excellence pour des abus.

Le niveau d'excitation que suscite le vidéochat fait oublier les règles de prudence les plus élémentaires, du genre « Pensez avant de poster ». En clair, si un homme, dans un moment de faiblesse, en est venu à croire que son interlocutrice était vraiment folle de lui et n'en voulait pas à son argent, les premières mesures à prendre sont les suivantes :

- rester calme, mettre un terme à tout contact, bloquer l'adresse et annoncer le faux compte de l'extorqueuse au webmaster du site ;
- ne céder en aucun cas au chantage et ne pas envoyer d'argent ! Le fait de payer ne protège en rien contre une publication du matériel collecté. Au contraire, les extorqueuses lâchent encore moins facilement prise et réclament plus d'argent dès le moment où elles savent qu'elles peuvent faire chanter leur victime.
- Cette dernière peut par exemple mettre en place une alerte Google personnelle. De cette manière, elle est informée dès que de nouvelles vidéos, photos ou autres données avec son nom sont mises en ligne.
- Au cas où des photos ou des vidéos seraient mises en ligne (et ce n'est de loin pas toujours le cas !), les exploitants des sites doivent être informés. Les réseaux sociaux comme Facebook effacent en général rapidement les « contenus inappropriés ».

Et même si la police n'a que très peu de chance de pouvoir enquêter sur ces délits et identifier les personnes qui tirent les ficelles puisque tout se fait dans l'anonymat le plus complet, il est important de les dénoncer. En effet, les informations fournies permettent à la police de mesurer l'ampleur des arnaques, d'établir des liens avec d'autres plaintes et, éventuellement, de trouver des moyens d'enquêter.

Pour cela, il faut conserver les moyens de preuve qui démontrent le chantage ou l'escroquerie : captures d'écran des faux comptes utilisés, enregistrements des conversations et des courriels échangés. Une plainte peut être déposée auprès de la police cantonale. Le chantage et l'escroquerie sont des délits poursuivis d'office, c'est-à-dire pour lesquels la justice intervient dès qu'elle en a connaissance.

Une dernière remarque importante pour conclure : n'ayez pas peur des situations gênantes : la police est là pour sanctionner des délits, pas pour juger des faiblesses que chacun peut avoir.

Fraude à la commission

De quoi s'agit-il ?

Les fraudes à la commission sont connues depuis plus de 30 ans. Leur principe est simple : un escroc essaie d'obtenir que sa victime (potentielle) lui fasse un paiement anticipé pour un

produit ou un service qu'il ne livrera ou n'effectuera jamais. Ce phénomène a été révélé notamment par les fausses loteries («Vous avez gagné 2 millions d'euros en Espagne, venez encaisser votre gain!») ou les faux héritages («Un oncle richissime, que vous ne connaissez pas personnellement, est décédé en Namibie. Nous vous envoyons votre héritage.») dont les victimes ont été avisées par courrier postal, fax ou courriel. Aujourd'hui, les fraudes à la commission s'exercent presque exclusivement par courriel ou via des sites Internet.

Quelle est la forme la plus fréquente de fraude à la commission ?

La PSC a un vaste aperçu des formes les plus fréquentes de fraude à la commission, car elle est alertée par les médias, les associations de consommateurs, ainsi que par des personnes directement victimes d'une escroquerie ou venues s'informer pour un tiers. Il semble que les cibles privilégiées soient des personnes âgées peu habituées aux médias numériques et persuadées que l'argent qu'elles ont investi à mauvais escient leur sera remboursé un jour. De fait, c'est très souvent que la PSC doit répondre aux proches d'une personne âgée sur la meilleure façon de la convaincre qu'elle est victime d'une arnaque.

La PSC informe principalement sur quatre formes de fraude à la commission :

1. Fausses loteries


zentilia/123RF

Les fraudeurs informent leurs victimes, en général par courriel, qu'elles ont gagné le gros lot d'une loterie à l'étranger. La «Loteria primitiva», très populaire en ce moment, existe bel et bien. Elle est située en Espagne et a beaucoup de succès. La victime est informée que son gain est prêt à être versé sous réserve de quelques formalités à remplir (impôt anticipé, honoraires d'avocat, frais de banque, de transfert et de recherche) pour lesquelles elle doit verser une substantielle avance de frais via une société de transfert de fonds (Western Union, Money Gram, etc.).

Evidemment, le gros lot n'est jamais versé et les avances ne sont jamais restituées. Les fraudeurs en revanche trouvent toujours de nouveaux prétextes pour exiger un paiement de leur victime, par exemple au moyen de faux documents et lettres provenant d'entreprises renommées (la plupart du temps des instituts bancaires) et d'autorités importantes (Europol, Interpol). Les sommes ainsi escroquées se montent rapidement à plusieurs milliers de francs : la PSC a même connaissance de cas où des avances à hauteur de 250000 francs ont été transférées à l'étranger.

Formes similaires : fraude à la commission sur des héritages à l'étranger ou sur un transfert de fortune de grands potentats via des comptes en Suisse insoupçonnables.

2. Fausses locations


Vitaly Krivosheev/123RF

Les fraudeurs publient sur des sites immobiliers connus des annonces crédibles pour la location bon marché de beaux logements magnifiquement situés. Mais ces objets ne sont pas à louer à ce moment-là : les fraudeurs ont copié ces annonces sur le portail lors d'une précédente tentative de location et les ont conservées afin de les utiliser ensuite dans le cadre d'une fraude à la commission. Il est possible aussi que l'objet en question n'existe même pas.

En réponse au locataire intéressé (et futur lésé), l'escroc explique qu'étant actuellement à l'étranger, il n'a pas besoin de son appartement et souhaite le louer à des personnes dignes de confiance. La victime pourra visiter l'appartement toute seule, mais par sécurité elle devra avancer au minimum un mois de loyer en guise de caution. Le fraudeur peut aussi exiger une caution pour la clé. Ni le loyer avancé, ni la caution pour la clé ne seront jamais remboursés et il est impossible de louer l'appartement.

Formes similaires : fraude à la commission sur la location de maisons individuelles et de bureaux.

3. Fausses locations de vacances


Martin Valigursky/123RF

Les fraudeurs publient sur des sites Internet connus des annonces pour des appartements et maisons de vacances qui n'existent même pas. Ces escrocs essaient d'attirer leur proie hors du site Internet, afin d'éviter que celui-ci ne surveille la transaction. Ils lui font donc miroiter des loyers très bon marché, et lui demandent de verser son loyer non pas via le site Internet mais directement par virement bancaire ou en utilisant un service de transfert de fonds. Ils peuvent aussi exiger une caution pour la clé. Ni le loyer payé d'avance, ni la caution pour la clé ne seront jamais remboursés. Et bien sûr, la victime se retrouve sur son lieu de villégiature sans aucun hébergement, ce qui est particulièrement dramatique durant la haute saison.

4. Fausses ventes de véhicule

Les fraudeurs publient sur un site Internet connu une annonce proposant la vente d'un véhicule. Lorsque la victime contacte l'escroc pour lui acheter


DR

sa voiture, celui-ci l'informe qu'il mandatera une entreprise de transport pour lui livrer le véhicule. L'entreprise de transport, qui fait également partie du réseau de l'escroc, contacte alors l'acheteur pour lui réclamer son adresse ainsi que diverses informations le concernant. Ensuite, il lui demande encore de verser un acompte sur la livraison, voire parfois la somme de vente totale, avant la livraison du véhicule. Bien entendu, la voiture n'est jamais livrée, et ni les frais de transport, ni l'argent versé ne sont jamais remboursés.

Formes similaires : fraude à la commission sur d'autres articles vendus sur des sites Internet.

Les fraudes à la commission sont-elles fréquentes ?

Il n'existe aucune donnée statistique sur la fréquence des fraudes à la commission. Les statistiques ne recensent que les cas qui ont été rapportés à la police. La plupart du temps, la victime d'une fraude à la commission renonce à porter plainte car, de prime abord, il semble impossible de pouvoir jamais retrouver le malfaiteur, surtout que, dans la majorité des cas, il opère depuis l'étranger. Il arrive souvent aussi que les victimes renoncent à porter plainte parce qu'elles ont honte et ne comprennent pas comment elles ont pu tomber dans le panneau. Dans le même ordre d'idée, les tentatives d'escroquerie sont elles aussi rarement dénoncées à la police. Pour toutes ces raisons, il est impossible de déterminer la fréquence des fraudes à la commission. Etant donné le nombre élevé de citoyennes et citoyens qui se renseignent sur la possibilité d'enquêter sur une fraude à la commission, la PSC est en droit de penser que le chiffre noir est gigantesque. En outre, la somme des délits doit être astronomique si l'on fait une estimation du total des montants escroqués qui ont été signalés.

Problématique spécifique aux fraudes à la commission

Comme les malfaiteurs changent souvent d'astuces, il est très difficile d'avoir une vue d'ensemble de toutes les formes de fraudes à la commission. De plus, ils se font souvent passer pour des entreprises sérieuses et connues pour tromper leurs victimes et leur soutirer toutes sortes d'informations personnelles.

Une chose est sûre : quelle que soit la forme de la fraude à la commission, une fois que l'argent a été versé, il est presque impossible de le récupérer. Dans la majorité des cas, les lésés l'ont définitivement perdu.

En général, la poursuite des fraudeurs à la commission est inutile pour les raisons suivantes :

- Ils opèrent le plus souvent depuis l'étranger, sous des noms d'emprunt, et leurs numéros de téléphone et adresses de courriel ne sont pas répertoriés. Les malfaiteurs ne sont pas connus.
- S'ils sont connus à l'étranger et s'ils devaient y répondre de leurs actes, il se pourrait qu'un mauvais fonctionnement du système judiciaire dans le pays empêche toute poursuite (corruption).
- Si, avant l'escroquerie, les lésés avaient pu se protéger ou éviter leur erreur avec un minimum de prudence, alors il n'y a pas escroquerie au sens du code pénal ; on ne peut ainsi pas reprocher au fraudeur d'avoir usé d'une astuce. (Cf. ATF 126 IV 165).

Cela dit, il est indispensable que la police détermine dans chaque cas si l'agissement du fraudeur à la commission est effectivement punissable. Selon les cas, il s'agit d'une escroquerie au sens de l'article 146 du code pénal.

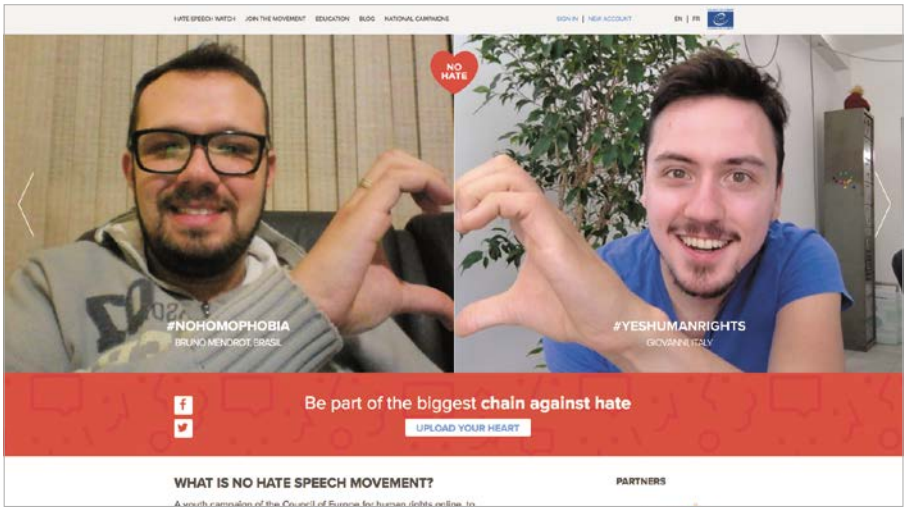
Mesures préventives contre la fraude à la commission

- Ne versez jamais d'acomptes pour des biens ou des services.
- Insistez pour payer la somme due au moment de la remise de la marchandise. Le mieux c'est de convenir d'un rendez-vous avec le vendeur pour recevoir la marchandise et la payer sur-le-champ.
- Utilisez le service d'un tiers de confiance (comme p. ex. sur eBay).
- Méfiez-vous des offres trop alléchantes (prix très avantageux, livrable de suite, « bonnes affaires »).
- Méfiez-vous aussi lorsqu'un vendeur vous pousse à conclure le marché le plus rapidement possible, voire immédiatement, « sans quoi l'objet en question risque d'être vendu à un autre intéressé ». Le stress ainsi occasionné peut faire oublier certaines règles de prudence élémentaires.

Discours de haine *(hate speech)*

Qu'entend-on par discours de haine ?

La notion de discours de haine englobe toutes les déclarations ou représentations qui insultent d'autres personnes, les ostracisent ou appellent à la violence contre une personne ou un groupe de personnes. Les déclarations ou représentations offensantes se basent souvent sur le sexe, la religion, l'origine, certains attributs physiques ou encore l'orientation sexuelle d'une personne ou d'un groupe ou encore la combinaison de plusieurs de ces caractéristiques. La diversité des discours de haine ne connaît aucune limite. Le discours de haine peut tout aussi bien viser une personne, par exemple une jeune fille en surpoids ou une personne en fauteuil roulant, que des groupes, par exemple des musulmans ou des personnes de couleur. On observe que les discours de haine sont portés à l'encontre d'un nombre croissant de personnes ou de groupes. D'un autre côté, tout individu qui s'expose dans la société, que ce soit professionnellement ou comme particulier, ou qui fait une déclaration



Le site « No Hate Speech » : une campagne du Conseil de l'Europe. https://www.nohatespeechmovement.org

publique à caractère polémique devient la victime de discours haineux.

Les conséquences des discours de haine sont multiples. Pour l'individu comme la jeune fille obèse, ces attaques sont émotionnellement très dures à supporter. Lorsque le discours de haine se fait sur le dos d'un groupe, il en résulte une stigmatisation de ce dernier avec la mise en évidence de stéréotypes éventuellement négatifs.

Quelle est la fréquence des discours de haine ?

C'est sur Internet que les discours de haine se propagent le plus rapidement. Les réseaux sociaux, les blogs ou les espaces réservés aux commentaires permettent aux internautes de s'exprimer librement et de discuter des sujets les plus divers. Malheureusement, un certain nombre d'entre eux abusent de cette liberté d'expression virtuelle en propageant sur les réseaux sociaux des déclarations extrêmes ou discriminantes contre des personnes ou des groupes. En outre, l'absence de contact physique et le relatif anonymat de la Toile ont pour effet de diminuer les inhibitions dans nombre de communautés en ligne (sans charte d'utilisation). Du coup, les gens osent subitement écrire des choses qu'ils n'oseraient jamais dire en face à quelqu'un.

L'anonymat des auteurs combiné aux mécanismes de diffusion d'Internet complique la recherche des sources de discours de haine, empêchant ainsi l'accumulation de preuves des délits et la fréquence des dénonciations. Certaines enquêtes ont néanmoins pu montrer que le discours de haine était un phénomène répandu. Il a ainsi été possible de dire quels étaient les groupes et les personnes concernés. En 2015, par exemple, le Conseil de l'Europe a mené une enquête en ligne sur les discours de haine. Les résultats du sondage ont montré que 83 % des personnes interrogées avaient déjà été confrontées à des discours de haine sur Internet. Il en est ressorti que les principaux groupes de victimes de ces discours étaient : les jeunes LGBTI[3], les musulmans et les femmes.

Mesures de prévention contre les discours de haine

Le discours de haine est avant tout un problème parce qu'il contribue à la propagation de la haine. L'émergence des réseaux sociaux a rendu cette diffusion très simple. Toute personne sachant écrire peut faire connaître son opinion sur Internet et volontairement ou non, devenir un propagateur de haine. Pour cette raison, on devrait toujours se demander si les commentaires ou déclarations que l'on veut mettre en ligne sont susceptibles d'insulter ou d'ostraciser des personnes ou encore d'entraîner des déclarations négatives à leur encontre. Par ailleurs, on ne devrait jamais partager des opinions ou des contenus irréfléchis ou extrêmes, voire interdits tels que des appels à la violence (Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure) ou le soutien à des organisations interdites telles qu'Al-Qaïda ou l'Etat islamique (Loi fédérale interdisant les groupes Al-Qaïda et Etat islamique et les organisations apparentées).

Il existe toutefois aussi divers moyens pour agir a posteriori contre les discours de haine. Il n'importe pas seulement que les victimes se défendent mais aussi que les témoins manifestent un courage civique et s'engagent résolument contre les diffamations et les discriminations.

- Pendant ou après un incident, adressez-vous à votre famille, à vos connaissances ou à un centre de consultation pour discuter des insultes qui vous ont été adressées ou qui ont été diffusées par des tiers.
- Bloquez les utilisateurs qui diffusent sur Internet des déclarations diffamantes ou discriminatoires pour empêcher les possibilités de diffusion.
- Envoyez un rapport aux fournisseurs de plateformes comme Facebook ou Instagram sur la diffusion de déclarations discriminantes ou diffamantes.
- Si vous voulez déposer une plainte pénale contre une personne ou un groupe, faites-le auprès de votre police cantonale. Il est toutefois recommandé de voir avec un centre de consultation si cette mesure est vraiment utile.

3 LGBTI est un sigle anglophone pour désigner les personnes homosexuelles, bisexuelles, transgenres ou intersexes : lesbiennes, gays, bisexuels, transgenres et intersexes.

- Conservez impérativement vos preuves, par exemple des captures d'écran avec la date et l'heure, ainsi que l'URL, les procès-verbaux des chats ou des images qui documentent l'événement.

Pour plus d'informations sur ce sujet :

Jeunes et médias – Plateforme nationale de promotion des compétences médiatiques : http://www.jeunesetmedias.ch/fr/opportunites-et-risques/risques/extremisme.html

Campagne No Hate Speech du Conseil de l'Europe en Belgique et au Québec : http://www.nonalahaine.be/ et https://www.mouvementnonalahaine.org/

Vol et usurpation d'identité

Aujourd'hui en Suisse, plus guère personne ne voudrait renoncer à Internet. La plupart d'entre nous disposent d'au moins une adresse électronique privée. Nous l'utilisons pour partager des nouvelles avec nos parents et amis. De plus en plus de personnes règlent leurs factures via e-banking et s'épargnent ainsi de devoir passer au moins une fois par mois à la banque et à la poste. Nous sommes aussi de plus en plus nombreux à apprécier les achats en ligne en Suisse et à l'étranger et à nous connecter pour nos activités professionnelles. En un mot comme en cent, la numérisation de notre quotidien avance à grands pas et a pour conséquence que l'on trouve toujours plus de données nous concernant sur Internet.

Le plus souvent pour de l'argent, mais parfois aussi pour nuire à une réputation

Si des données privées arrivent entre les mains d'inconnus et sont utilisées sans notre consentement, on parle de vol ou d'usurpation d'identité. Rien d'étonnant qu'une très grande quantité de données soient volées et usurpées dans un but d'enrichissement illégitime. Il suffit de penser aux données des cartes de crédit avec lesquelles on peut très simplement payer des chambres d'hôtel en ligne, acheter des habits, du vin ou d'autres produits et les faire livrer à n'importe quelle adresse. Mais il arrive aussi que des données soient volées pour nuire à la réputation de la victime : l'auteur se présente ensuite sur Internet comme étant la personne volée, crée dans son dos de faux comptes sur les réseaux sociaux ou propose des prestations sexuelles sur des sites coquins.

everythingpossible/123RF

On peut facilement se servir de données bancaires volées pour payer sa chambre d'hôtel en ligne ou commander des habits, du vin, ou tout autre produit.

Collecter ou s'emparer de données

Le vol ou l'usurpation d'une identité peut parfois être un jeu d'enfant pour le délinquant. Certaines données n'ont même pas besoin d'être chassées ou volées, il suffit de les collecter. Certains utilisateurs sont si insouciants et confiants qu'ils rendent accessibles à tout un chacun sur les réseaux sociaux leur adresse et leur numéro de téléphone, les noms des membres de leur famille et de leur employeur. D'autres n'autorisent l'accès à ces données qu'à leurs amis mais acceptent de devenir amis avec des gens qu'ils n'ont jamais rencontrés dans la vie réelle. L'accès aux données des cartes de crédit et des coordonnées bancaires est beaucoup plus difficile. Pourtant, des criminels parviennent souvent à se les faire communiquer par des personnes naïves, par exemple au moyen de courriels d'hameçonnage (phishing).

La prudence la plus élémentaire ne suffit pas

Il ne suffit malheureusement pas de croire que l'on peut se protéger contre le vol et l'usurpation d'identité en renonçant à utiliser Internet. Aujourd'hui, un grand nombre de données sensibles concernant chacun de nous circule sur Internet ou à proximité immédiate de la Toile. Certes, nos données bancaires, les données sur notre santé et autres sont bien protégées. Toutefois, une simple négligence (stocker un paquet de données sur le mauvais serveur) ou la persévérance d'un hacker font que nos données vont être utilisées à mauvais escient sans que nous puissions empêcher quoi que ce soit.

Mesures de prévention

Même si l'utilisation d'Internet présente toujours un certain risque, chacun peut réduire le risque d'être la victime d'un vol d'identité en adoptant certains comportements et en prenant un certain nombre de mesures :

- Sur la page de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (www.melani.admin.ch), vous trouverez nombre de conseils et de recommandations pour protéger vos données du vol ainsi que votre PC et votre téléphone portable contre des attaques.
- Sur la page du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), vous obtiendrez des informations sur les modes opératoires les plus fréquemment utilisés par les malfaiteurs sur Internet. La page www.cybercrime.admin.ch donne également des informations sur l'actualité des faux courriels et des faux sites Internet,

Le vol ou l'usurpation d'identités n'est pas explicitement réprimé dans le code pénal suisse (CP). Ces délits sont toutefois toujours assimilés à des actes délictueux prévus par le code pénal. Suivant qu'il s'agit d'un vol ou d'une usurpation, ce seront la soustraction de données (art. 143 CP), l'accès indu à un système informatique (art. 143 bis et 126 CP) et les infractions contre l'honneur et contre le domaine secret ou le domaine privé (art. 173 ss CP) qui seront appliqués.

La Police municipale de Zurich et sa stratégie en matière de médias sociaux: d'ICoP à Instagram

Interview de Michael Wirz, chef du secteur Communication de la Police municipale de Zurich

Monsieur Wirz, la Police municipale de Zurich se sert depuis des années des médias numériques pour donner des informations actuelles à la population de la ville. Pourquoi la Police municipale a-t-elle décidé de devenir active dans les médias sociaux ?

En 2008, de nombreuses personnes se sont donné rendez-vous via Facebook pour un botellón à Zurich. Plus d'un millier d'adolescents et de jeunes adultes ont ensuite participé à cette beuverie de masse et ont généré des coûts de plusieurs centaines de milliers de francs pour l'ensemble de l'administration municipale. C'est là que nous avons compris que nous devions nous pencher sur Facebook. Le commandant m'a alors chargé d'élaborer une stratégie, ce que j'ai fait de 2009 à 2011 à l'aide d'une enquête menée dans la communauté en ligne. J'ai été surpris de voir à quel point les réactions étaient positives: les personnes interrogées étaient très intéressées par une communication avec la police via les médias sociaux. Aujourd'hui, nous sommes actifs sur Facebook, Twitter, YouTube et Instagram.

Quelle stratégie et quels buts poursuivez-vous en utilisant les canaux des médias sociaux ?

Tout d'abord, nous voulons avoir un dialogue avec la population au lieu d'utiliser simplement les médias sociaux comme canaux de distribution supplémentaires pour nos communiqués de presse, etc. De nombreux citoyens et citoyennes utilisent aujourd'hui les médias sociaux, il faut donc que la police y soit présente également. Cela veut dire que nous mettons en œuvre systématiquement en ligne la philosophie et la culture que nous avons par ailleurs. Au fond, le travail de la police est le même, que ce soit sur Internet ou en dehors. Nous poursuivons notre stratégie de communication existante, nous l'avons juste complétée. Ainsi, nous restons authentiques, ciblés et générons la confiance. Au début, nous prévoyions nos contenus à l'avance *(content plan)*, mais cela nous bridait trop. Aujourd'hui, nous «postons» lorsqu'il se passe quelque chose et nous avons constaté que ce n'est pas un problème pour nos amis et abonnés Facebook si rien de nouveau n'apparaît pendant deux semaines.

Quel canal convient à quel usage ?

Nous utilisons Twitter pour une information rapide et directe. Nous atteignons ainsi en particulier les leaders d'opinion tels que journalistes ou hommes et femmes politiques, mais aussi diverses organisations. Twitter nous permet dans certains cas d'influencer l'agenda dans une certaine mesure. Comme le ton y est plus «familier», on peut parfois lancer un thème plus difficile à aborder autrement.

Facebook fonctionne très bien pour des récits plus longs et plus approfondis, souvent accompagnés de photos. Nous y récoltons aussi l'avis et les sentiments de la population et proposons un regard dans les coulisses du travail de la police.

Du point de vue thématique, nous utilisons également nos canaux et leur grande portée pour diffuser nos messages de prévention.

Peut-on gagner la confiance de la population par le biais des médias sociaux ?

Bien sûr pas uniquement, le comportement au contact direct est tout aussi important. Mais lorsque j'observe les réactions et les nombreuses demandes que nous recevons sur ces canaux, je suis certain que cet engagement contribue à améliorer la confiance ! Nous sommes extrêmement soucieux de la confiance qui nous est accordée et nous répondons aux questions très sérieusement et en détail. Nous veillons aussi à ne diffuser que des contenus fiables à 100%.


DR

Michael Wirz, 40 ans, policier de formation, est chef du secteur Communication de la Police municipale de Zurich. Ces dernières années, il s'est penché de manière intensive sur la thématique «Numérisation et travail policier». Dans le cadre de son travail de master, il a en particulier étudié les chances et risques de l'utilisation des médias sociaux par les services d'urgence et il a planifié la stratégie et introduit l'usage des nouveaux médias par la Police municipale de Zurich. Entre-temps, ce corps de police est leader dans ce domaine en Europe germanophone. Michael Wirz enseigne en outre la communication administrative dans différentes hautes écoles.

Patrick Jean est le premier ICoP de Suisse. Comment avez-vous eu cette idée d'un policier de proximité sur Internet ?
En cas de souci, on préfère toujours avoir affaire à un être humain qu'à une organisation anonyme. C'est pareil en ligne et hors ligne. Lors d'une conférence du Collège européen de police (cepol), nous avons rencontré Marko Forrs, «nettipoliisi» finlandais. C'est un collègue d'Helsinki qui travaille sur Internet depuis des années. Cette idée de police de proximité en ligne m'a

Patrick Jean, profession ICoP.

fasciné et je me suis demandé si cela fonctionnerait aussi dans la ville de Zurich. Nous nous sommes donc mis en quête d'un collègue adéquat… Patrick Jean faisait à l'époque un stage dans notre division et il semblait très bien convenir à cette mission. Il est communicatif, ouvert, il écrit bien et il a du doigté. Nous l'avons formé pour ce travail avant de lancer tout d'abord un projet pilote de six mois. L'intérêt et la confiance dont on lui a témoigné en tant qu'ICoP étaient énormes, il a vite eu de nombreux «amis» et abonnés ! Aujourd'hui, des adolescents et des jeunes gens le reconnaissent souvent et l'abordent dans la rue. Il travaille à 50% comme policier de quartier à Zurich-Hottingen et à 50% en tant que ICoP.

Quels sont les prochains projets prévus ou déjà en cours ?
Depuis juillet de cette année, Eleni Moschos est le pendant féminin de Patrick Jean. D'une part, cela le décharge d'une partie du travail, d'autre part, il y a des sujets et des domaines auxquels une femme a un meilleur accès. Il ne faut pas oublier que Patrick et Eleni travaillent surtout en arrière-plan: ils traitent des messages directs qui leur parviennent via Facebook, de sorte qu'ils peuvent conseiller et arbitrer de manière non bureaucratique. Ils représentent souvent la porte d'entrée pour les jeunes qui s'adressent à eux via Facebook ou Instagram. Par exemple, ils organisent souvent des rendez-vous auprès du service des jeunes ou indiquent un service de conseil adéquat. Si elles ont le choix, les femmes et les jeunes filles préfèrent parler de certains sujets à une femme.

S'agissant de l'utilisation de nouveaux canaux et plates-formes, nous nous tenons toujours au courant. Nous surveillons actuellement des plates-formes telles que Snapchat et Periscope et nous nous occupons souvent de vidéos en ligne.

A quels problèmes avez-vous déjà été confrontés ? Y a-t-il eu des flots d'insultes (shitstorm), des menaces contre la police municipale, des atteintes à la personnalité ou autres choses de ce genre ?
Nous n'avons jamais eu de flots d'insultes de type *shitstorm*. Mais il nous est arrivé d'avoir 50 commentaires négatifs à un message sur un concept de sécurité pour un match de football. Jusqu'à présent, nous avons pu gérer tout cela plutôt bien et nous avons pris le temps de répondre à chaque commentaire.

Par contre, il y a parfois des atteintes à la personnalité, par exemple des usagers qui chargent une photo d'une voiture en stationnement interdit devant chez eux. Nous leur expliquons ce qu'il en est et leur demandons de supprimer la photo.

Quelle conclusion tirez-vous après plusieurs années de travail de votre corps de police sur et avec les médias sociaux ? Ces médias facilitent-ils le travail de la police ou cet engagement représente-t-il surtout une tâche supplémentaire ?
Mon bilan est globalement positif, je suis sûr que cela facilite notre travail. Ce que nous faisons dans les médias sociaux va nettement au-delà des relations publiques, c'est de la police de proximité. En fait, c'est du travail policier normal, mais en ligne. Nous procédons de manière tout aussi pragmatique en ligne que hors ligne. Je me souviens par exemple d'un cas où nous avons retrouvé plus ou moins par hasard sur Facebook quelqu'un qui était porté disparu. Nous lui avons envoyé un message, il a répondu que tout allait bien, qu'il était à l'étranger et allait contacter immédiatement ses proches. Dans un tel cas, le réseau social nous facilite vraiment le travail et nous décharge même de certaines tâches. Bien sûr, la présence sur les médias sociaux est aussi une promesse de transparence et donc une mesure qui renforce la confiance, ce que nous montrent les nombreuses questions qui nous parviennent. Il arrive assez souvent que des gens laissent entendre qu'ils ne sont pas de grands amis de la police, mais qu'ils trouvent ça bien que nous soyons là.

Je trouverais intéressant que d'autres corps de police aient aussi à l'avenir des policiers en ligne car nos ICoPs ont aussi des amis hors de la ville et du canton de Zurich et il serait parfois utile de pouvoir leur indiquer un collègue. Nous sentons en tout cas déjà que d'autres corps de police s'intéressent à nos activités. Suivant le principe des médias sociaux, nous sommes heureux de partager notre expérience avec d'autres. N'oublions pas que le savoir est le seul bien qui ne diminue pas, mais au contraire se multiplie quand on le partage !

Facebook www.fb.com/StadtpolizeiZH
Twitter @StadtpolizeiZH

ICoPs
Patrick Jean
Facebook www.fb.com/stapojean
Instagram @stapojean
Eleni Moschos
Facebook www.fb.com/eli.stapo
Instagram @eli.stapo

Brochures d'information et de prévention de la PSC

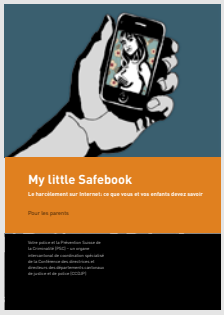
Une prévention spécialement dédiée aux médias numériques est importante et utile pour diverses raisons. A l'heure actuelle, les enfants et les adolescents grandissent à la fois dans le monde réel et dans le monde virtuel et il est donc important qu'ils acquièrent des compétences en ligne comme en dehors. De nombreux types d'escroquerie sur Internet sont relativement faciles à déceler à condition de les connaître. L'information est donc souvent une mesure de prévention satisfaisante. Et si les citoyen-ne-s apprennent et comprennent Internet et le fonctionnement des «trucs» et des arnaques, il est beaucoup plus probable qu'ils repèreront les agissements criminels. C'est pourquoi la PSC a élaboré plusieurs brochures et dépliants qui abordent ces sujets par groupes cibles.

Les différents produits sont disponibles sur le site Web www.skp psc.ch (à télécharger) ou auprès des polices cantonales et municipales.

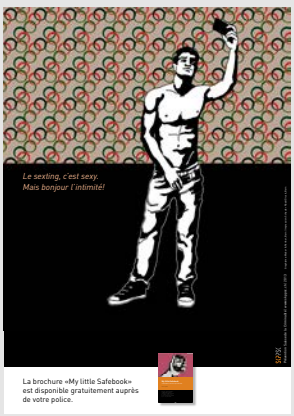
Brochure «My little Safebook»
pour les jeunes

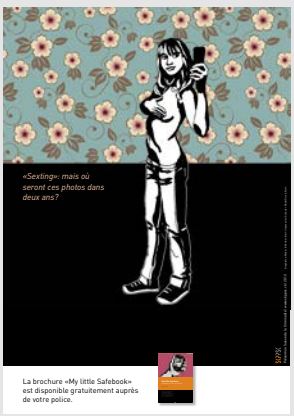
«My little Safebook» s'adresse aux jeunes à partir de 12 ans et a pour but de leur expliquer tout ce qu'il faut savoir sur le harcèlement sur Internet. La brochure explique en outre comment les jeunes peuvent se protéger contre les attaques de cyberharcèlement, les délits sexuels et les abonnements abusifs. De plus, elle les incite à réfléchir sur leur propre comportement dans les médias et sur la différence entre le monde réel et le monde virtuel. Cette brochure est complétée par une courte présentation de la situation juridique et une liste de liens vers des informations complémentaires.

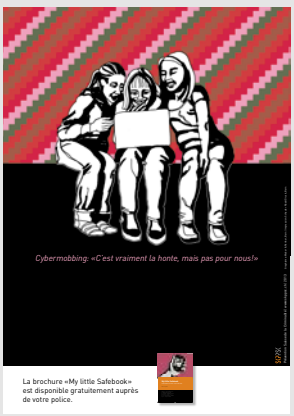
Brochure «My little Safebook»
pour les parents



«My little Safebook» s'adresse aux parents et responsables d'éducation de jeunes à partir de 12 ans. La brochure a pour but de les aider à mieux comprendre pourquoi l'Internet est tellement important dans la vie des jeunes d'aujourd'hui et comment ils peuvent les accompagner efficacement dans les réseaux sociaux. Elle informe également en détail sur le cyberharcèlement, les délits sexuels et les abonnements abusifs, et explique comment les jeunes peuvent se protéger. D'autres thèmes, comme la consommation et les compétences médiatiques sont également abordés et complétés par des conseils sur le comportement que peuvent adopter les adultes sur Internet pour servir de modèles aux jeunes. Cette brochure comporte en outre une courte présentation de la situation juridique et une liste de liens pour des informations complémentaires.







Poster A3
«Sexting» et «Cybermobbing»

«Le sexting, c'est sexy. Mais bonjour l'intimité!»

«Sexting: mais où seront ces photos dans deux ans?»

«Cybermobbing: C'est vraiment la honte, mais pas pour nous!»

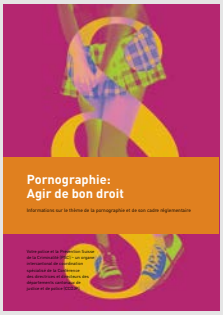
Brochure «Il était une fois… Internet»

Les enfants découvrent de plus en plus tôt l'Internet. C'est pourquoi la brochure «il était une fois… Internet» s'adresse aux parents d'enfants de moins de 12 ans.
De manière amusante et humoristique, cinq contes modernes abordent les cinq principales problématiques: La dépendance à Internet, la pédocriminalité, le cyberharcèlement, le shopping en ligne et les abonnements-pièges, ainsi que la protection des données: les contes joliment illustrés peuvent être lus à haute voix ou lus eux-mêmes par les enfants en âge scolaire. Les petits chapitres «et la morale de l'histoire» expliquent aux parents les enjeux de chaque problématique et leur donnent des conseils de comportement.

«Cyberharcèlement: Agir de bon droit»

Le fascicule «Cyberharcèlement: Agir de bon droit» fournit des renseignements sur les principaux articles de loi concernant le cyberharcèlement. Deux exemples de cas ont pour but de montrer comment le harcèlement est pratiqué dans les nouveaux médias et sept conseils illustrent comment se protéger contre ce phénomène. Le fascicule poursuit en outre le but de permettre aux jeunes de faire la différence entre une dispute et une attaque de cyberharcèlement. Quant aux parents et responsables d'éducation, il les conseille afin qu'ils maîtrisent le sujet avant de l'aborder avec les jeunes.

«Pornographie: Agir de bon droit»

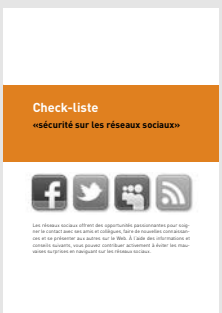


Le fascicule «Pornographie: Agir de bon droit» fournit des renseignements sur les principaux articles de loi concernant la pornographie. Il a pour but de contribuer à ce que les jeunes apprennent à satisfaire leur curiosité et la découverte de leur sexualité de manière tout à fait légale. Le fascicule détaille la situation juridique dans le domaine et fournit aux jeunes et aux adultes des informations utiles sur l'âge de protection, le sexting et la pornographie illégale. Quant aux parents et responsables d'éducation, il les conseille afin qu'ils maîtrisent le sujet avant de l'aborder avec les jeunes.

«Mon image: Agir de bon droit»

Le fascicule «Mon image: Agir de bon droit» montre, à l'aide d'exemples de cas, dans quelles conditions le droit à sa propre image peut être compromis et aide ainsi à éviter toute violation de la loi. Il contient également des explications sur le cadre juridique et explique les cas dans lesquels les juges partent du principe d'un accord tacite. Le fascicule informe en outre sur ce qu'il faut savoir lorsque l'on prend des photos d'enfants ou de jeunes, afin de ne pas enfreindre leur droit à l'image.

Check-liste «Sécurité sur les réseaux sociaux»



Cette check-liste, présentée sur une double page, comporte cinq conseils d'ordre général sur la manière dont les réseaux sociaux fonctionnent, ainsi que quatre conseils sur la façon de se comporter pour éviter les mauvaises surprises et profiter pleinement et sereinement des avantages de ces nouveaux réseaux.

Carte postale «Cybercriminalité» et «Escroquerie»

Changement à la Commission de direction PSC

La Commission de direction approuve la planification annuelle et les comptes PSC et les campagnes de prévention que le service spécialisé PSC a proposé d'élaborer et de mettre en œuvre.

Mme la Conseillère d'Etat Maya Büchi-Kaiser (canton d'Obwald) ayant changé de département, elle a quitté la commission le 30 juin 2016. Lui succède M. le Conseiller d'Etat **Christoph Amstad,** désormais à la tête du Département de la justice et de la sécurité. M. Amstad représentera également le concordat de police Suisse centrale au sein de la Commission de direction.

Adrian Lobsiger, directeur suppléant fedpol, a été nommé préposé fédéral à la protection des données. Il a quitté la commission au printemps 2016. C'est le directeur suppléant **René Bühler** qui représentera désormais fedpol au sein de la Commission de direction.

Changement à la Commission de projet PSC

La Commission de projet analyse la situation en matière de criminalité et propose des thèmes de campagne qu'elle défend devant la Commission de direction avant de les transmettre à la CCDJP.

Robert Steiner était le plus ancien membre de la Commission de projet. Délégué de la commission, il prenait part aux réunions de la Commission de direction PSC. Il était un maillon essentiel entre les deux commissions.

Chef de la police de sûreté du canton du Valais, il a pris sa retraite an 2016. La Commission de projet a pris congé de lui lors de sa réunion de printemps. Son successeur et homologue du canton de Fribourg, **Florian Walser,** a participé à la réunion d'automne. Florian Walser assumera aussi la représentation des chefs de la police de sûreté du concordat de police Suisse romande.

fedpol/Gaëtan Bally

Christoph Amstad

DR

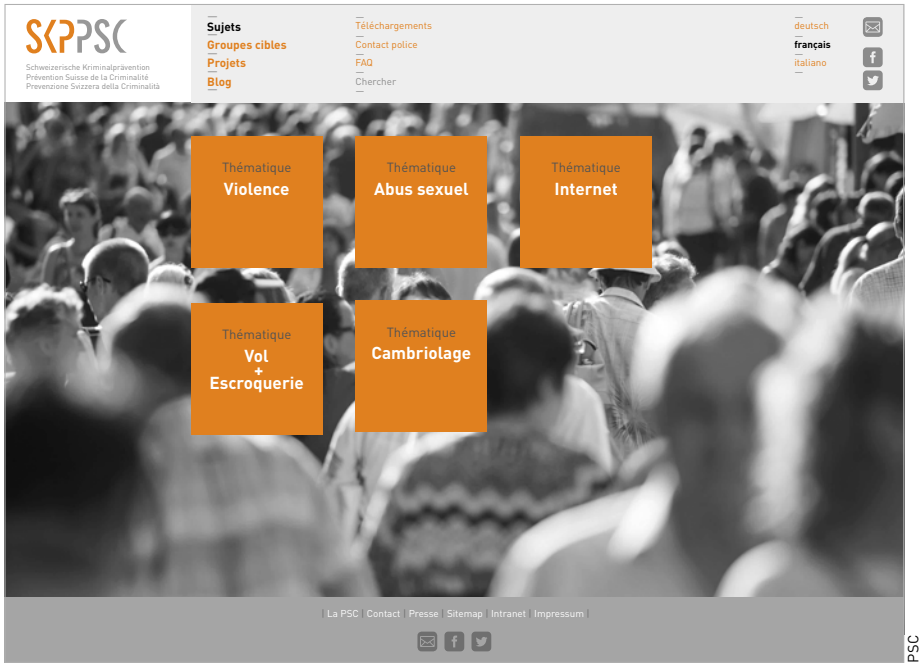
René Bühler

DR

Florian Walser

Refonte du site Internet PSC (www.skppsc.ch)

Le 1er janvier 2017 aura lieu le lancement du nouveau site Internet de la PSC. La façon de présenter les sujets étant dépassée, il a fallu envisager un remaniement complet. Ceci aura pour effet que tous les liens renvoyant au site Internet PSC, situés sur les sites de ses partenaires, seront désactivés et devront être remplacés. La PSC fera son possible pour que ses partenaires soient renseignés sur les principaux liens du nouveau site avant sa mise en service.



PSC

Plan d'action national (PAN) contre la radicalisation et l'extrémisme violent

Le Réseau national de sécurité (RNS) a été chargé par le Conseil fédéral, les cantons, les villes et les communes d'élaborer un PAN. Il a pour but de prévenir toutes les formes de radicalisation et d'extrémisme violent. Le PAN comprend quatre domaines d'action : prévention, répression, protection et prévention des crises. Les axes thématiques, appelés champs thématiques, sont rattachés à ces domaines d'action. Les champs sont au nombre de neuf, chacun d'eux incombant à une organisation responsable. Il s'agit des champs éducation, intégration, reconnaissance/formation, domaine social, sécurité, collaboration interdisciplinaire, sensibilisation, déradicalisation/réhabilitation et coopération internationale.

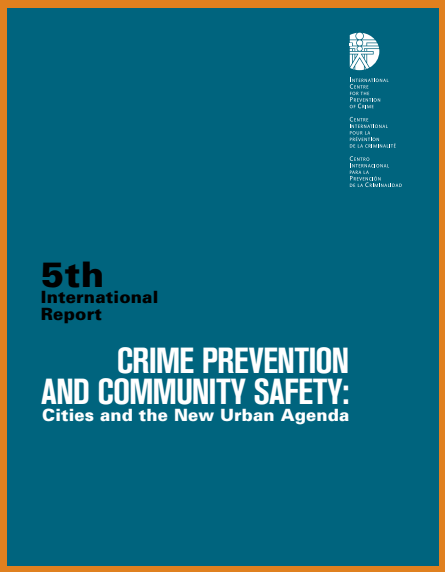
L'élaboration du PAN devrait être achevée au plus tard début septembre 2017. La consultation des autorités et instances concernées se déroulera en juin 2017.

Pour plus d'informations : www.svs.admin.ch

Cinquième rapport international sur la prévention de la criminalité et la sécurité quotidienne

Début novembre, le Centre international pour la prévention de la criminalité (CIPC) a publié son 5e rapport international. Intitulé « Les villes et le Nouvel Agenda Urbain », il comprend cinq chapitres : « Tendances en matière de prévention de la criminalité et de prévention », « Sécurité urbaine », « Villes, territoire et politiques de sécurité publique, une perspective latino-américaine », « Prévention de la criminalité dans les transports publics urbains », « Prévention de la criminalité liée à la consommation de drogue en milieu urbain », « Les villes et la prévention de la radicalisation violente ».

Le rapport s'adresse principalement à trois secteurs clés : les décideurs et les élus politiques en charge de la sécurité, les experts en sécurité urbaine et les milieux scientifiques qui recherchent de bonnes pratiques, les évalue et les commente. Le rapport en anglais et son résumé en français sont disponibles en téléchargement sur le site Internet du CIPC.



Pour plus d'informations :
www.crime-prevention-intl.org/fr

22es Journées de la prévention 2017, Hanovre, Allemagne

Les 22es Journées de la prévention (DPT) auront lieu les 19 et 20 juin 2017 à Hanovre. Elles seront consacrées au sujet « Prévention & Intégration ». Les partenaires organisateurs de la manifestation sont le Land de Niedersachsen, sa capitale Hanovre et le Conseil de la prévention du Land de Niedersachsen (LPR). Les inscriptions sont ouvertes.

Nouveau cours de l'Institut suisse de police (ISP) Sécurité urbaine (6.40.00.d)

Groupe-cible

- Collaborateurs des corps de police municipaux et communaux chargés de délivrer, d'examiner ou de traiter des autorisations, ou qui seront appelés à le faire.
- Membres des corps de police cantonaux (chefs de postes, p. ex.), qui offrent aux autorités communales des prestations de conseil sur les questions ayant trait aux autorisations et aux manifestations.
- Collaborateurs de l'administration qui traitent de questions de sécurité ayant trait aux manifestations et aux autorisations.

Objectifs

Les participants :

- Etablissent le déroulement d'une procédure d'autorisation pour les manifestations dans l'espace public, semi-public et privé, et sont capables d'expliquer et de délivrer des formulaires d'autorisation et de demande ;
- Sont en mesure, sur la base de check-lists et d'autres documents de traiter correctement et efficacement les différents types d'autorisation, d'assumer des tâches de réseautage et de définir des interfaces ;
- Sont sensibilisés, sur la base d'un cas type, étudié en groupe, à certains enjeux et problèmes spécifiques survenant lors de manifestations, et sont en mesure d'élaborer des approches de solution de manière autonome ;
- Acquièrent des compétences dans les domaines demandes et autorisations, droit administratif, surveillance technique dans l'espace public et sécurité urbaine, et sont en mesure de les mettre en œuvre.

Contenus

Sécurité urbaine ; procédure d'autorisation pour les manifestations ; formulaires d'autorisation et de demande ; droit administratif ; responsabilité incombant à l'autorité habilitée à délivrer des autorisations ; autorisations d'exploiter un établissement occasionnel ; alcool & protection des mineurs ; Crowd Management ; normes de la police du feu ; charges des responsables CO ; surveillance technique de l'espace public ; concepts d'événements.

Le cours est dispensé en allemand.

www.edupolice.ch → kurse → kursangebot → 6.40.00.d Urbane Sicherheit

Reto Habermacher est le nouveau directeur de l'ISP

Succédant à Pius Valier, **Reto Habermacher** est entré en fonction le 1er octobre 2016. L'Institut suisse de police a été chargé par la CCDJP de gérer le projet CGF 2020 et de procéder en parallèle aux remaniements requis au sein de l'organisation. Mener de front ce projet de réorganisation, le CGF 2020 et la direction de l'ISP occuperait un poste à plus de 100%. Reto Habermacher se chargera donc de la direction et de la réorganisation, tandis que Pius Valier a accepté de conduire le projet CGF en tant que directeur opérationnel. C'est la direction de projet stratégique qui lui a confié ce mandat, qu'il exercera en externe et à temps partiel.

DR

Pour plus d'informations :
www.institut-police.ch

« eBanking – en toute sécurité ! »

Le site Internet www.ebankingabersicher.ch informe les internautes intéressés par les questions de sécurité informatique sur les précautions à prendre lorsqu'on effectue des opérations bancaires en ligne. La Haute école de Lucerne, section Informatique, a été chargée par les grands instituts financiers suisses de créer ce site destiné au grand public. Le site est actuellement soutenu par plus de 70 instituts basés en Suisse et dans la Principauté de Liechtenstein.

Pour plus d'informations :
www.ebankingabersicher.ch

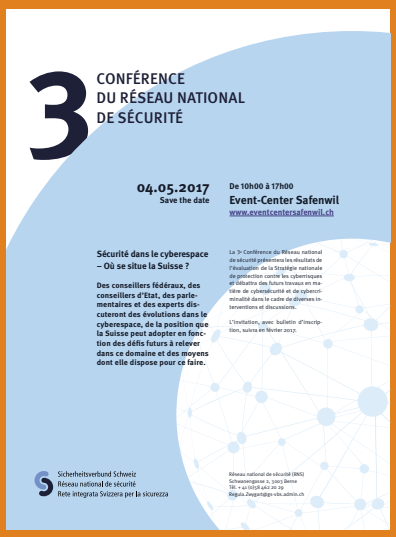
Jeunes et médias – le portail d'information dédié à la promotion des compétences médiatiques

Protéger les enfants, c'est aussi les accompagner à travers le monde numérique. Le portail d'information dispense des conseils aux parents, aux enseignants et à tout adulte intéressé, afin que les jeunes utilisent les médias numériques en toute sécurité et de manière adaptée à leur âge.

Pour plus d'informations :
www.jeunesetmedias.ch

Date à retenir en 2017

La 3e Conférence du Réseau national de sécurité Suisse présentera les résultats de l'évaluation de la Stratégie nationale de protection contre les cyberrisques et permettra aux participants de débattre des travaux prévus en matière de cybersécurité et de cybercriminalité. Date : 4 mai 2017.



Pour plus d'informations : www.svs.admin.ch

SKPPSC

Prévention Suisse de la Criminalité
Maison des cantons
Speichergasse 6
Case postale
CH-3000 Berne 7

www.skppsc.ch

Editeur et commande
Prévention suisse de la criminalité PSC, Berne
Courriel : info@skppsc.ch, tél. +41 31 320 29 50

Responsable		Martin Boess, directeur PSC
Rédacteur		Wolfgang Wettstein, Zurich
Traduction	**fr**	ADC, Martigny
	it	Annie Schirrmeister, Massagno
Mise en pages		Weber & Partner, Berne
Impression		Vetter Druck SA, Thoune
Tirage		fr: 300 ex. | all: 1350 ex. | it: 100 ex.
Date de parution		Numéro 4 | 2016, décembre 2016

PSC Info 4 | 2016 est téléchargeable en format PDF, à l'adresse : www.skppsc.ch/skpinfo.
PSC Info 4 | 2016 est aussi parue en allemand et en italien.

vectomart/123RF