PSC INFO

1 | 2021

LE MAGAZINE DE LA PRÉVENTION SUISSE DE LA CRIMINALITÉ

Dossier
Cybersécurité

La cybersécurité, c'est

S-U-P-E-R.ch

Chère lectrice, cher lecteur,


PSC

Pas un jour ne passe en Suisse sans qu'une personne ne tombe dans les filets d'un escroc en ligne. La victime aura reçu un courriel de hameçonnage qui lui enjoint de verser de l'argent pour recevoir un paquet, ou un courriel la menaçant de diffuser des photos intimes si elle ne paye pas la somme demandée. Des sites Internet truqués proposent des marchandises ou des biens immobiliers à des prix défiants toute concurrence et, en plus, cautionnés par des célébrités ou des entreprises connues, afin de mieux cacher leur origine criminelle. Des entreprises et des organisations entières se font pirater et subissent ensuite un chantage. La liste des escroqueries est malheureusement sans fin, comme l'imagination de leurs instigateurs, une situation dont les autorités de poursuite pénale doivent se contenter de prendre acte, la plupart du temps. Ce qu'elles ne font certes pas de gaieté de cœur, mais parce qu'en leur qualité d'instances nationales il leur est (encore) difficile de mettre un terme aux agissements de criminels qui opèrent la plupart du temps à l'échelle internationale. Raison pour laquelle la prévention revêt une importance toute particulière pour ce type d'infraction.

La PSC et tous les corps de police se sont alliés avec le Centre national pour la cybersécurité (NCSC), la Swiss Internet Security Alliance (SISA) et « eBanking – en toute sécurité ! » (EBAS) pour lancer une campagne de prévention de grande envergure qui entend sensibiliser la population suisse et attirer son attention sur les gestes simples que chacune et chacun peut faire pour se protéger efficacement sur Internet : les « 5 règles pour votre sécurité numérique ».

Ce numéro de PSC Info vous en dit plus sur ce projet commun et sur les autorités et organisations qui se consacrent à la prévention des cyberdélits. Ainsi, le NCSC présente ses nouvelles orientations et champs d'action. SISA, une association regroupant des représentants des cercles de l'économie et de l'administration, exploite une plateforme dédiée à la sécurité sur Internet, avec la marque en ligne « iBarry.ch ». Mandatée par des instituts financiers suisses et mise sur pied par la Haute école de Lucerne, EBAS est elle aussi une plateforme indépendante. Quant à l'agence chargée de réaliser les idées de cette campagne, elle expose son point de vue dans une interview et parle des enseignements qu'elle retire de son travail avec les responsables du projet. Enfin, la PSC et « Votre police » expliquent pourquoi elles ont mis en place ce projet commun. Il est aussi question de NEDIK (le réseau de soutien aux enquêtes dans la lutte contre la criminalité informatique) et de ses nouveaux champs d'action.

Si nous vous avons mis l'eau à la bouche et que vous souhaitez savoir ce qui se passera exactement pendant la semaine du 3 au 7 mai 2021, suivez-nous sur les canaux des médias sociaux. Le top départ sera donné le 3 mai !

Je vous souhaite une agréable lecture !

Fabian Ilg
Directeur suppléant PSC et responsable de projet Cybercriminalité

IMPRESSUM

Editeur et commande
Prévention Suisse de la Criminalité
Maison des cantons
Speichergasse 6
3001 Berne

Courriel : info@skppsc.ch
tél. 031 511 00 09

PSC Info 1 | 2021 est téléchargeable en format PDF, à l'adresse : www.skppsc.ch/skpinfo.
PSC Info 1 | 2021 paraît aussi en allemand et en italien.

Responsable		Chantal Billaud, directrice PSC
Rédaction		Volker Wienecke, Berne
Traduction	**fr**	ADC, Vevey
	it	Annie Schirrmeister, Massagno
Mise en pages		Weber & Partner, Berne
Impression		Länggass Druck SA, Berne
Tirage		fr: 300 ex. | all: 1350 ex. | it: 250 ex.
Date de parution		Numéro 1 | 2021, avril 2021

La cybersécurité, c'est S-U-P-E-R – semaine d'action en mai

Du 3 au 7 mai 2021, la Prévention Suisse de la Criminalité mène campagne en ligne pour sensibiliser les citoyennes et citoyens à la sécurité numérique. Montée en partenariat, cette action doit surprendre, intéresser et informer, et permettre à tout un chacun d'y trouver son compte grâce à un dispositif à entrées multiples. La cheffe de projet Beatrice Kübli nous emmène dans les coulisses, et « c'est S-U-P-E-R ».

DR

S-U-P-E-R sert d'aide-mémoire pour les cinq règles de sécurité numérique et il est aussi l'URL de la page de renvoi.

Qui ne connaît pas ce sentiment diffus à l'approche de la visite chez le dentiste ? Comme à chaque fois, il demandera combien de fois on a utilisé son fil dentaire. Et comme à chaque fois, on se dira qu'il aurait fallu, mais… Il en va de même avec beaucoup de mesures de prévention, et la sécurité numérique ne fait pas exception. Avez-vous bien sauvegardé récemment vos données privées ? Parfois, il suffit d'un petit rappel de l'extérieur pour donner un nouvel élan, les déconvenues d'un collègue par ex. dont le portable est tombé dans l'Aar et qui a perdu toute sa collection de photos. Puisque nous ne souhaitons à personne de voir tomber ses photos, voire pire, à l'eau, nous nous chargeons de faire ce petit rappel de l'extérieur en lançant une semaine d'action.

« Nous », ce sont la PSC, les corps de police réunis sous le label « Votre police », le Centre national pour la cybersécurité (NCSC), la Swiss Internet Security Alliance (SISA) et sa plateforme *iBarry* ainsi que la plateforme « eBanking – en toute sécurité ! » (EBAS) de la Haute école de Lucerne. La campagne de sensibilisation qui aura lieu du 3 au 7 mai 2021 présentera aux citoyennes et citoyens les fameuses cinq règles qui leur permettent de protéger leurs données et accès à Internet. La réalisation en a été confiée à l'agence « Partner & Partner » de Winterthour.

« Pourquoi avoir choisi de parler de sécurité numérique ? », pourrait-on légitimement se demander. Le paysage de la prévention a bien d'autres sujets importants auxquels il faudrait sensibiliser la population. Il est certain que chacun de ces sujets mériterait qu'on lui consacre une semaine d'action. Mais commencer par la sécurité numérique a toute sa raison d'être.

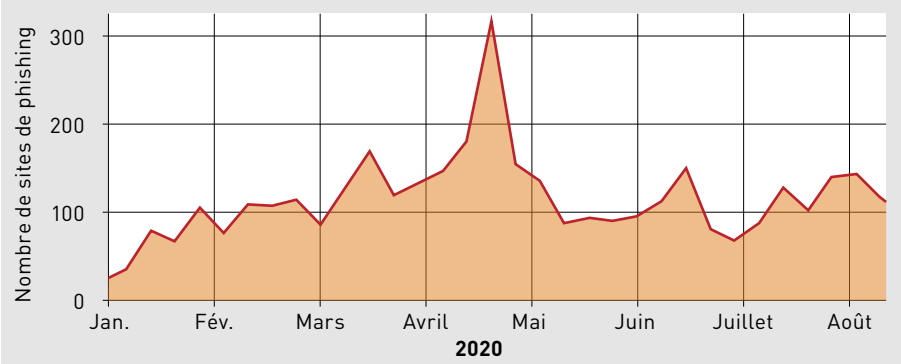
Prévenir est plus facile que mener l'enquête

Internet offre aux criminels un terrain d'action idéal où utiliser toutes sortes d'arnaques pour s'enrichir : sans que leurs utilisateurs ne s'en aperçoivent, les ordinateurs peuvent servir à mettre la main sur leurs codes bancaires, s'emparer de leur identité ou bloquer l'accès à leurs données. Enquêter n'est pas une mince affaire, d'autant que les résultats sont rarement au rendez-vous, car les escrocs sont basés à l'étranger et utilisent les ressources d'Internet pour garder l'anonymat et dissimuler leurs activités. Enquêter et effectuer des recherches suppose une coopération internationale, ce qui n'est pas aisé à mettre en place avec tous les pays, ainsi que des connaissances solides en informatique et une infra-

Auteure

Beatrice Kübli
Responsable de projet à la Prévention Suisse de la Criminalité

PSC



Nombre de sites Internet de hameçonnage signalés et confirmés par semaine sur antiphishing.ch au premier semestre 2020[1]

structure adaptée. La part des cyberdélits rapportée à l'ensemble des infractions pénales est en constante augmentation, avec une prépondérance pour les fraudes en ligne et le hameçonnage. Plus de la moitié des signalements recueillis ces dernières années par fedpol concernaient ces deux formes de délit.[2] Et pour les six premiers mois de l'année 2020, la centrale du NCSC a recensé chaque semaine une centaine de sites s'adonnant au hameçonnage.

Or toutes les victimes de cyberattaques ne contactent pas la police, loin s'en faut. Certaines éprouvent de la honte d'être tombées dans le piège. D'autres sont résignées et ne croient pas que le délit pourra être élucidé ; elles ne portent donc pas plainte. Le nombre de cas non déclarés est élevé et les dégâts personnels et économiques considérables. Miser sur la prévention vaut donc la peine, précisément en matière de sécurité numérique. On évitera bien des déboires avec peu de moyens, assez simples, en utilisant par exemple des mots de passe sûrs, en mettant régulièrement à jour ses logiciels ou en installant un antivirus. Il importe aussi que les citoyennes et citoyens connaissent bien la nature des dangers, de manière à user de sens critique en présence de courriels ou de SMS de provenance douteuse. Celle ou celui qui connaît le fonctionnement d'une attaque de hameçonnage ou de piratage sera moins tenté de commettre un acte inconsidéré ou de répondre sans hésiter à une sollicitation, aussi tentante soit-elle. Prendre la mesure du risque individuel permet aussi de prévenir les attaques d'envergure qui visent les entreprises, car l'employé averti ne cliquera plus sur le premier lien venu. Certes, certains actes de piratage sont perpétrés sur un plan purement technique, mais la plupart des délinquants tablent sur le maillon le plus faible, qui est l'humain. C'est le levier de notre campagne.

Une semaine – c'est faisable !

A l'origine, nous pensions évoquer dans notre campagne l'idée du nettoyage de printemps, qui permet de faire – enfin ! – régner l'ordre, de dépoussiérer et de se délester des dossiers qui traînent. En cours de route, nous avons pourtant trouvé que l'idée du nettoyage n'était pas tout à fait adéquate, car il s'agit davantage de sécurité que de propreté. Seul est resté le principe d'une semaine d'action, au fil de laquelle les participants font successivement de l'ordre. Le projet « cinq règles pour la sécurité numérique » que nous avions mis au point en 2020 avec EBAS s'avéra un concept tout trouvé. A chaque jour sa règle. La semaine est une unité de temps claire et gérable, qui permet de garder sa motivation à participer et promet un grand impact du fait de sa densité.

La campagne vise avant tout à sensibiliser les citoyennes et citoyens à l'importance que revêt la sécurité numérique. Il s'agit de prendre conscience que les appareils que tout un chacun utilise, de l'ordinateur au téléphone portable en passant par la tablette, doivent être protégés. Chacun peut et doit être responsable de sa sécurité numérique, savoir comment y parvenir et comment se prémunir contre une attaque. Ensuite, il faut être capable de passer à l'étape de la mise en pratique. Ces trois phases sont au cœur du message de notre campagne.

Créer une prise de conscience

L'élément primordial d'une campagne de prévention est sa visibilité. Les meilleures affiches et messages postés ne servent à rien si personne ne les regarde. Nous misons donc sur l'humour et la surprise. Il nous importait aussi que le lien avec le sujet soit évident de façon que chacun comprenne au premier coup d'œil de quoi il s'agit. L'agence a conçu cinq sujets : on voit un appareil, qui peut être tour à tour un ordinateur, une tablette ou un téléphone portable, combiné à un élément que chacun associe à la sécurité dans sa vie de tous les jours. Puisque ces combinaisons n'existent pas dans la vie réelle, elles étonnent, surprennent ou perturbent, et ont un effet comique.

1 Source : Centre national pour la cybersécurité NCSC/MELANI : « Sûreté de l'information. Situation en Suisse et sur le plan international. Rapport semestriel 2020/I (de janvier à juin) », 29 octobre, sur Internet, à l'adresse : www.ncsc.admin.ch → Documentation → Rapports → Rapports sur la situation → Rapport semestriel 2020/1

2 National Risk Assessment (NRA) : « Escroquerie et hameçonnage en vue de l'utilisation frauduleuse d'un ordinateur en tant qu'infractions préalables au blanchiment d'argent, Rapport du Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF) », janvier 2020, sur Internet, à l'adresse : www.sif.admin.ch → Politique et stratégie en matière de marchés financiers → Intégrité de la place financière → Rapports

DR

Sauvegarder ses données est l'une des cinq règles de sécurité numérique. Chaque règle a son propre sujet d'illustration.

Ainsi, on voit un ordinateur portable nager avec une bouée, ou du dentifrice étalé sur une tablette. Un simple coup d'œil suffit à capter intuitivement le message : « protéger les appareils numériques ». En y regardant à deux fois, on en apprend davantage.

Acquérir des connaissances

Les sujets sont accompagnés d'un bref commentaire qui explique le lien qu'entretient l'image avec la cybersécurité. Chaque sujet illustre l'une des cinq règles. Ainsi, le commentaire de l'image de la bouée est : « Sécurisez vos données, et évitez le naufrage ». On comprend aisément que ce geste est une règle pour garantir sa sécurité. Pour bien mémoriser les cinq règles, l'agence a créé le mot S-U-P-E-R ! S comme sauvegarder, U comme utiliser ses mises à jour, P comme protéger avec un antivirus, E comme équiper ses accès d'un mot de passe fort et R comme réduire les risques. L'acronyme est aussi l'URL ouvrant l'accès au site Internet qui contient toutes les informations et les consignes utiles.

Doter d'une capacité d'action

Pour avoir davantage d'informations sur la façon de protéger ses appareils, une page de renvoi expliquera comment mettre en pratique les différentes règles. Chacune d'elles est accompagnée d'un bref texte explicatif. Et pour en savoir encore davantage, des liens redirigent vers les organisations partenaires, qui permettent d'approfondir tous les sujets ou de participer à des webinaires du NCSC.

Grâce à son dispositif à entrées multiples, l'offre s'adresse aux citoyennes et citoyens selon leur niveau de connaissances. Via la page de renvoi, l'utilisateur avancé accédera à des informations de spécialistes tandis que le béotien trouvera un accès simple à la thématique.

Diffuser en s'appuyant sur un réseau

Afin de réaliser une diffusion à large échelle, en trois langues, dans toute la Suisse, nous pouvons compter sur nos réseaux. Car il est essentiel que soient transmis les contenus du plus grand nombre possible de partenaires pour que la campagne réalise ses objectifs. Les corps de police et différentes banques nous ont déjà confirmé leur participation, divers partenaires économiques de SISA sont intéressés. Coordonner les efforts de toutes les parties prenantes constitue un défi, mais la PSC n'en est pas à son coup d'essai. Nous avons déjà mené à bien de nombreuses actions avec notre réseau et sommes donc confiants. Il s'agit de montrer à la collectivité combien notre réseau est solide. En effet, l'enjeu de cette action n'est pas seulement la sécurité numérique, mais aussi de faire en sorte que la police et les organisations partenaires se positionnent comme des interlocuteurs compétents, et de montrer la densité et la souplesse du réseau suisse qui veille sur la cybersécurité. Ce sera certainement S-U-P-E-R !

« eBanking – en toute sécurité ! »

La plate-forme « eBanking – en toute sécurité ! » (EBAS) du département Informatique de la Haute école spécialisée (HES) de Lucerne, a pour but d'aider les particuliers et les banques à assurer leur sécurité informatique, notamment lors de leurs opérations d'e-banking.

C'était en avril 2017. La police zougoise avait organisé une rencontre sur le thème de la prévention. A l'apéritif qui a suivi (oui, c'était chose courante avant le Covid !) j'ai fait la connaissance du cyber-enquêteur zougois qui m'a parlé de la Prévention Suisse de la Criminalité (PSC) avec laquelle il avait travaillé. J'ai tout de suite vu les avantages réciproques d'une collaboration et le contact s'est établi peu après.

De fait, ça n'a pas traîné et au mois de juin nous nous retrouvions dans les locaux du tout nouveau département Informatique de la HES Lucerne. Une analyse croisée des objectifs de la PSC et de « eBanking – en toute sécurité » a vite montré que la collaboration serait possible dans plusieurs domaines. L'intérêt s'est notamment porté sur les excellentes brochures et dépliants réalisés par la PSC et c'est en automne/hiver 2017 déjà qu'a paru notre première brochure commune : « Les 5 règles pour votre sécurité numérique ». D'autres ont suivi, et à ce jour nous comptons sept dépliants issus de la collaboration PSC-EBAS :

- Les 5 règles pour votre sécurité numérique
- Travailler comme passeur d'argent (Money Mule) pour le compte de criminels ?
- Phishing
- Arnaques par téléphone : les faux services d'assistance
- Mobile Banking et Mobile Payment
- Médias sociaux en toute sécurité
- Rendements de rêve ? Gare au réveil !

Ce matériel d'information est distribué par la PSC, mais aussi par l'EBAS, soit directement dans le cadre de formations, cours et manifestations, soit indirectement via le service « eBanking – en toute sécurité ! » des banques partenaires.

Retour vers le futur immédiat : la Prévention Suisse de la Criminalité organise du 3 au 7 mai 2021 une semaine d'action nationale pour la cybersécurité. Cette campagne permettra en quelque sorte de nouer la gerbe avec notre première brochure commune, puisqu'elle détaillera chaque jour une des « 5 règles pour votre sécurité numérique ». Nous sommes ravis d'avoir participé, en tant qu'une des quatre organisations faîtières, à l'élaboration de cette campagne, et nous allons poursuivre cette fructueuse collaboration en faveur de la prévention et de la sensibilisation du public suisse aux dangers du cyberespace.

« eBanking – en toute sécurité ! »

« eBanking – en toute sécurité ! » (EBAS) est une campagne de sensibilisation qui, depuis plus de dix ans, incite efficacement la population suisse et les acteurs du secteur financier à pratiquer un e-banking sécurisé. Lancée en 2009 avec trois banques partenaires pilotes (Crédit Suisse, PostFinance et Zürcher Kantonalbank), elle peut compter aujourd'hui sur le soutien de près de 50 banques dans toute la Suisse. Multilingue, cette campagne repose sur quatre piliers :

1. Le site Internet
(pour tout public)
Afin que les particuliers puissent protéger efficacement et durablement leurs appareils numériques, ils ont besoin d'aide et de conseil. Le but de ce soutien est aussi de les rendre plus vigilants et circonspects lors de leurs transactions bancaires sur Internet.

Le département Informatique de la HES Lucerne met à disposition sur son site www.ebas.ch des informations claires et pratiques sur les mesures à suivre et les comportements à adopter pour assurer la sécurité numérique, notamment lors d'opérations d'e-banking.

2. Formations pour clients
(pour tout public)
Notre site Internet propose chaque année des cours très accessibles, ouverts aux clients de différents horizons. Dispensés dans divers lieux de Suisse, ils comprennent un cours de base, un cours pratique avec des exercices sur des dispositifs fournis, un cours spécial en ligne destiné aux moins de 30 ans et un cours pour PME. Le cours de base, par exemple, dure deux heures et demie et informe sur la sécurité numérique en général et sur la sécurisation

Auteur


DR

Oliver Hirschi
Informaticien de formation, il est chargé de cours pour la sécurité de l'information numérique à la Haute école spécialisée de Lucerne depuis 2013. Il dirige notamment la plate-forme « eBanking – en tout sécurité ! » (www.ebas.ch). Il est coauteur d'un manuel de sécurité numérique en allemand (www.sihb.ch) et fait partie du groupe de sécurité suisse SGRP (www.sgrp.ch).

DR

Le site Internet www.ebas.ch de la Haute école de Lucerne diffuse des informations pratiques sur les mesures de sécurité élémentaires et le comportement à adopter.

des opérations d'e-banking en particulier. Toute l'offre du moment sur www.ebas.ch → Formations

3. Suivi des médias
(pour instituts membres seulement)
Les médias ont une influence sur la confiance et le comportement de l'utilisateur final. L'un ou l'autre article sur l'e-banking peut inquiéter et susciter de nombreuses questions auxquelles le service clients ou le conseiller à la clientèle devra répondre. Un suivi régulier de l'activité du paysage médiatique suisse, la préparation de prises de position à l'intention des diverses instances de conseil, ainsi qu'une base de données comprenant les articles publiés et les prises de position y relatives augmentent nettement la qualité de ce service.

En collaboration avec Argus Data Insights Suisse, la HES Lucerne surveille quotidiennement la production médiatique suisse (journaux, médias en ligne, radio et télévision). Tous les articles concernant de près ou de loin l'e-banking et la sécurité numérique sont collectés. Pour ceux qui le nécessitent, une prise de position est ensuite rédigée et mise à disposition des banques partenaires. De la sorte, les collaborateurs bancaires sont en mesure de répondre de façon documentée et compétente aux questions de leurs clients en matière de sécurité.

4. Formation pour conseillers à la clientèle
(pour instituts membres seulement)
Il est essentiel que les conseillers à la clientèle et les services clients soient à même de répondre de façon claire, documentée et compétente à toutes les questions ayant trait à la sécurité informatique. La HES Lucerne propose donc aux instituts financiers un cursus de formation ciblé à cette fin.

A noter enfin que le site Internet de la HES Lucerne comptabilise près de 40000 vues par mois, et que plus de 1200 collaborateurs d'instituts financiers partenaires et 4800 particuliers ont à ce jour suivi une formation EBAS pour un e-banking en toute sécurité.

Sensibiliser aux risques numériques – une tâche primordiale du NCSC

La sécurité numérique occupe une place centrale au sein de la politique étrangère et de la politique de sécurité, que ce soit au plan national ou au plan international. Elle est aussi un facteur essentiel pour la place économique suisse. Le Centre national pour la cybersécurité est le premier interlocuteur des particuliers, des milieux économiques, de l'administration et des établissements d'enseignement pour toute question relative aux cyberrisques.

Auteure

Dominique Trachsel
lic.phil., MAS, MSc FCCI, est responsable sensibilisation et prévention NCSC.

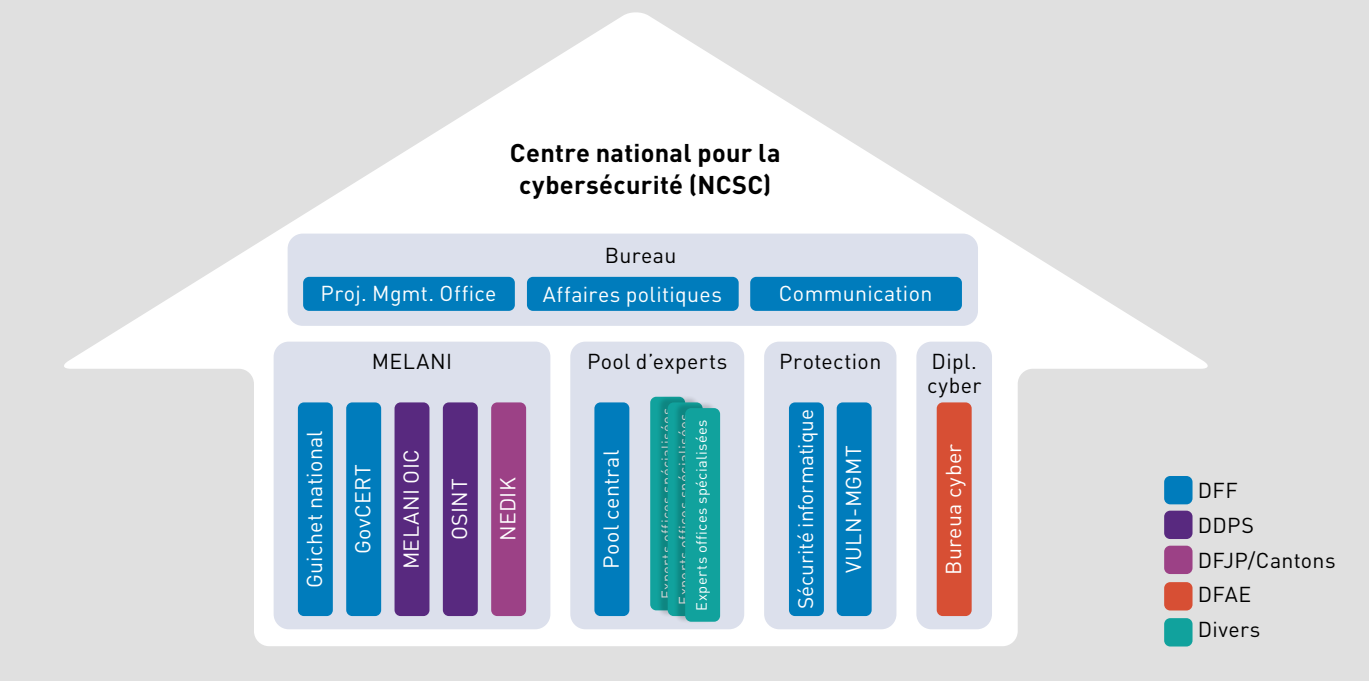
DR

Le Centre national pour la cybersécurité (National Cyber Security Centre – NCSC), qui est dirigé par le délégué fédéral à la cybersécurité, Florian Schütz, est notamment chargé de mettre en œuvre de manière coordonnée la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Cette stratégie fixe les objectifs et mesures qui fondent aussi l'action des acteurs des cantons, de l'économie, de la société et des hautes écoles. Le NCSC se base légalement sur l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (OPCy), qui règlemente la structure, les tâches et les compétences des autorités impliquées. L'OPCy prescrit de plus la réalisation d'un travail de sensibilisation et de prévention[1], un domaine dans lequel il est essentiel pour le NCSC de pouvoir collaborer et échanger avec les services de l'administration fédérale et d'autres acteurs.

Sensibilisation et prévention

La cybersécurité étant l'affaire de chacun et chacune d'entre nous, l'une des tâches du NCSC est d'informer le public des cyberrisques afin de le sensibiliser aux dangers de l'espace numérique. En étroite collaboration avec des entités internes et externes à l'administration fédérale, il met au point des règles de prévention et formule des recommandations sur la manière dont les victimes de cyberdélits peuvent réagir. Le NCSC soutient dans ce cadre la semaine nationale d'action lancée par la Prévention suisse de la criminalité (PSC),

1 Art. 12, lettre h, de l'ordonnance sur les cyberrisques



Source: NCSC

qui présente à un large public des mesures concrètes permettant de se mouvoir en toute sécurité dans le monde virtuel. Cette semaine d'action est financée et organisée en partenariat par la plateforme indépendante «eBanking – en toute sécurité!» de la Haute école de Lucerne, l'Alliance suisse pour la sécurité sur Internet (SISA/iBarry), la PSC et le NCSC.

Organisation

Le NCSC comprend un Bureau, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), un pool d'experts, un secteur dédié à l'autoprotection de l'administration et un secteur dédié à la diplomatie cyber.

La centrale MELANI, créée en 2004, est devenue en 2020 le service technique du NCSC, qu'elle a intégré avec l'équipe d'intervention en cas d'urgence informatique (GovCERT). Ses capacités ont été étendues à cette occasion et elle se charge depuis de la coordination avec le Service de renseignement de la Confédération et les instances de poursuite pénale, afin de garantir la transmission des informations concernant les menaces. La centrale MELANI comprend également le guichet unique suisse mandaté pour centraliser les notifications concernant les cyberincidents émanant de la population et des milieux économiques, les examiner et donner aux personnes ou aux services à l'origine du signalement une évaluation de l'incident concerné ainsi que des recommandations pour la suite de la procédure.

Le NCSC met aussi à disposition des divers acteurs un pool d'experts. Ces derniers les assistent dans le développement et la mise en œuvre de normes en matière de cybersécurité. Le pool d'experts se charge aussi du domaine de la sensibilisation et de la prévention.

En ce qui concerne l'autoprotection de l'administration fédérale, le NSCS édicte des directives sur la cybersécurité, vérifie qu'elles soient respectées et aide les fournisseurs de prestations à remédier aux failles détectées. Également à l'échelon de la Confédération, le *«Vulnerability Management»* développe des processus et des outils d'aide; il publie aussi des rapports sur les failles de sécurité.

Quant au Bureau Cyber du Département fédéral des affaires étrangères (DFAE), il assure la collaboration et la coordination avec la politique extérieure de la Suisse.

Swiss Internet Security Alliance – une association d'utilité publique pour la protection contre les dangers de l'Internet

La Swiss Internet Security Alliance (SISA) regroupe des représentants de l'économie et des pouvoirs publics, unis pour engager des actions de cyberprévention. Avec le site iBarry.ch, la SISA met à disposition un outil dédié que les corps de police peuvent aussi recommander dans le cadre de leurs activités de prévention.

Pour faire de la Suisse le pays à l'Internet le plus sûr au monde

La SISA – ou alliance suisse pour la sécurité sur Internet – a été fondée en 2014 par de hauts responsables économiques. Parmi eux figuraient les principaux fournisseurs d'accès à Internet de Suisse: ceux-ci ont accepté de ne pas se faire concurrence lorsqu'il s'agit de protéger la population des dangers d'Internet et de son utilisation. La SISA a mis en avant sa vision, qui est de faire de la Suisse le pays le plus sûr au monde en matière d'Internet. En conséquence, elle se donne pour but de rendre les utilisateurs vigilants quant aux risques que représente la vulnérabilité de leurs appareils connectés à Internet, de leur indiquer des solutions à ces problèmes, et de les sensibiliser aux dangers potentiels. Autrement dit, la SISA fait de la cyberprévention.

Auteur


DR

Daniel Nussbaumer est président de l'Alliance suisse pour la sécurité sur Internet depuis 2019. Avant cela, il a été responsable de la cybercriminalité à la police cantonale de Zurich pendant quatre ans et a dirigé NEDIK – le réseau intercantonal de police chargé de la répression et de la prévention dans le domaine de la cybercriminalité dans toute la Suisse.

La cyberprévention est une lourde tâche – tirons parti des synergies !

La cyberprévention est une lourde tâche. La création et la diffusion de campagnes de prévention, le développement et la maintenance de sites web ou encore la préparation et la réalisation de présentations nécessitent des ressources. Nombre d'entreprises et de pouvoirs publics le savent mais elles peinent à en mobiliser, compte tenu de leurs objectifs de gestion.

Or le volume de la cybercriminalité est estimé à environ 600 milliards de dollars par an, ce qui signifie que la cybercriminalité génère davantage d'argent que le commerce mondial de la drogue. Dès lors, faire de la cyberprévention, c'est se battre contre une industrie qui pèse 600 milliards de dollars.

Il est donc judicieux d'exploiter les synergies dans ce domaine afin d'éviter de faire le travail à double ou à triple, et afin d'échanger les contenus et produits développés, mais aussi – idéalement – de développer conjointement des stratégies, des campagnes et des pages d'accueil tout en conjuguant les efforts de mise en œuvre.

Le partenariat public-privé Swiss Internet Security Alliance

Aujourd'hui, la SISA regroupe non seulement des représentants de l'économie, mais aussi de l'administration publique et des hautes écoles. En tant qu'association d'utilité publique, SISA offre ainsi à ses membres et partenaires la possibilité de développer et de diffuser conjointement des produits de prévention.

Dans ce cadre, son activité comporte principalement deux volets : d'une part, son comité consultatif, au sein duquel siègent les membres et les partenaires de l'association, détermine les contenus. De l'autre, elle exploite la plate-forme iBarry.ch, qui fournit des conseils concrets à la population sur tous les phénomènes cybernétiques actuels. Le site web propose également des outils que les citoyens peuvent utiliser gratuitement pour vérifier le degré de protection de leur ordinateur contre les cyberattaques.

Le comité consultatif

Le comité consultatif est composé d'experts en matière de sensibilisation issus des organismes membres ou partenaires de la SISA ; il consiste en une plate-forme où sont élaborés conjointement des contenus pour des campagnes ciblées. Les messages de prévention correspondants doivent être coordonnés de manière à ce que tous les partenaires utilisent la même formulation lors de la diffusion des messages de prévention.

Actuellement, le comité consultatif comprend des représentants des fournisseurs d'accès à Internet, des instituts financiers, des pouvoirs publics et des hautes écoles. Ils assurent ainsi le développement conjoint de messages de prévention pour le secteur privé et le secteur public, et donc aussi la coordination des efforts de prévention.

Pour sa part, la SISA lance chaque année au moins quatre campagnes de sensibilisation élaborées par le comité consultatif ; ainsi, elle contribue activement – en coordonnant les efforts de tous les partenaires – à la sensibilisation du public.

iBarry.ch – une plate-forme pour le travail de prévention des corps de police

Les cyberattaques, de plus en plus complexes et diversifiées, ciblent les personnes et/ou les failles numériques. Cependant, les cybercriminels sont de plus en plus nombreux à revenir toujours à la charge avec des méthodes qu'ils renouvellent sans cesse, destinées à abuser de la bonne foi des gens. Exemple typique, les courriels contenant des liens ou des pièces jointes qui peuvent déclencher l'installation sur l'ordinateur d'un logiciel malveillant si on les ouvre ou que l'on y accède par mégarde. Ou les courriels frauduleux, tels que les escroqueries sentimentales ou les arnaques au président. Non contentes de cibler la personne, ces attaques cherchent les failles informatiques afin de se frayer un chemin jusqu'aux appareils.

Prendre des mesures ciblées pour protéger la population est d'autant plus difficile que ces cyberattaques sont multiples et diverses, et que les mesures de prévention doivent donc l'être aussi. Or, leur mise en place demande beaucoup de temps et de ressources.

En 2019, la SISA a lancé la marque iBarry.ch – un site de cyberprévention de grande envergure qui dispense des conseils sur le comportement à adopter en ligne sur tous les sujets cybernétiques actuels. En exploitant ce site, entretenu en continu, les membres de la SISA financent une plate-forme de sensibilisation à large portée pour la population suisse. Ainsi, il n'est plus nécessaire que les autres institutions investissent, chacune de son côté, des ressources dans le développement de sites Internet dédiés. Les entreprises privées ou les institutions telles que les corps de police peuvent ainsi ren-

DR

voyer à iBarry.ch au lieu de concevoir chacune leur propre matériel de prévention.

Coopération nationale – campagne en cinq étapes en mai

Outre les activités susmentionnées, la SISA participe également à la prochaine campagne en cinq étapes, que la PSC, le NCSC, la SISA et l'EBAS ont élaborée conjointement et qui sera lancée en mai. Cette collaboration est également issue du constat que nous pouvons avoir davantage d'impact si les entreprises et les pouvoirs publics mettent leurs ressources en commun et agissent ensemble. Nous avons tous – que nous soyons un fournisseur d'accès à Internet, un institut financier, une haute école ou un organisme public – un intérêt commun à sensibiliser la population aux dangers du web et à lui donner des conseils concrets sur le comportement adéquat – c'est ce dont nous tenons compte en mettant en œuvre la campagne en cinq étapes.

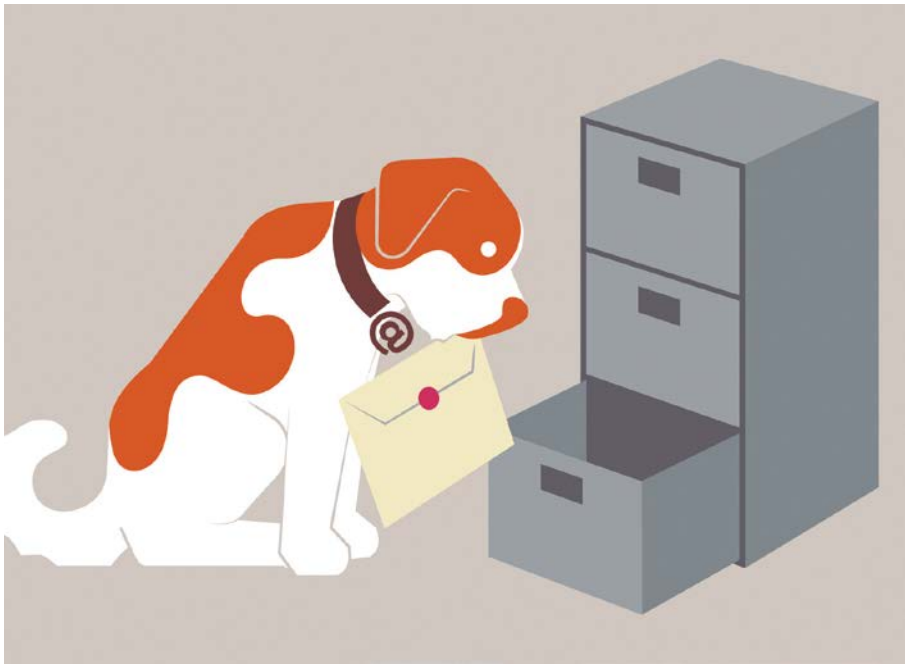
La SISA se donne pour mission de promouvoir les partenariats public-privé, et de continuer à mener des campagnes nationales conjointes. L'objectif de ces campagnes est d'atteindre le plus grand nombre possible de citoyens et de les sensibiliser, afin que la Suisse devienne un pays où l'Internet est plus sûr.

Devenez membre

La SISA accueille de nouveaux membres et partenaires. Elle offre notamment aux corps de police de Suisse la possibilité de devenir gratuitement partenaire de l'association. L'idée d'un tel partenariat est de se soutenir mutuellement et, en particulier, d'utiliser et de diffuser activement les produits de la SISA, tels que le matériel de prévention d'iBarry.ch. Plusieurs corps de police en Suisse profitent déjà de cette possibilité, ce qui leur permet de préserver ainsi leurs propres ressources. Prenez contact avec nous, de préférence sur iBarry.ch (ibarry.ch → À propos de nous → Contact).

iBarry.ch – le chien au pelage blanc et orange qui vous guidera à travers le Net en toute sécurité

Poussé par la curiosité, il risque souvent de tomber dans les arnaques en ligne. C'est ainsi qu'iBarry – notre sympathique saint-bernard – attire notre attention sur un sujet que peu de gens aiment aborder : en flairant les pièges sur Internet.



DR

iBarry a des traits humains dans les nombreuses images comme celle-ci, qui évoque la sauvegarde de données. Mais parfois il se comporte comme un chien et aboie lorsqu'il flaire un danger, ou renifle avec curiosité quand quelque chose l'intrigue.

Auteure

DR

Annette Hirschberg est responsable de la communication et du marketing pour iBarry, collabore avec Swiss Internet Security Alliance depuis août 2019.

Barry a existé ; et il aurait sauvé de l'avalanche plus de 40 vies au début du XIXe siècle. iBarry est son successeur virtuel qui, au début du XXIe siècle, veut suivre ses traces pour la navigation sur Internet. Le rôle du chien virtuel a certes quelque peu changé : puisqu'il ne peut pas localiser directement les victimes et les sortir de la neige comme le faisait son prédécesseur, il donne le


DR

Sécurité des smartphones : iBarry, très curieux, s'introduit à l'intérieur du portable et renifle les icônes des applications – le téléchargement de logiciels malveillants étant l'un des dangers de l'utilisation des appareils mobiles.


DR

Achats en ligne : comment les escrocs s'évertuent à induire leurs victimes en erreur, et comment reconnaitre les faux sites de vente en ligne.

bon exemple et met toute sa belle énergie à explorer les moindres recoins du Net afin d'en déceler les embûches. Naïf et crédule, il rencontre toutes sortes de dangers, sans pour autant tomber dans les pièges tendus par les escrocs.

Des règles simples pour une technologie complexe

iBarry incarne en quelque sorte l'internaute moyen. Un chien – même un chien de secours – n'est pas particulièrement calé en informatique et ne connaît pas grand-chose aux astuces des escrocs. Par cette caractéristique et par son air de toutou câlin, il véhicule l'idée que n'importe qui est en mesure de reconnaître les dangers sur Internet. iBarry a donc pour tâche de faciliter, en toute sécurité, l'utilisation des appareils électroniques et la navigation sur Internet.

Voilà qui est important pour sensibiliser aux cyberrisques : aujourd'hui, la quasi-totalité de la population, des élèves de l'école enfantine aux centenaires, utilise Internet pour échanger des messages, faire des achats, rechercher des informations ou discuter. En arrière-fond, pourtant, se cache un monde virtuel qui est si complexe et difficile à comprendre que la plupart des gens se sentent impuissants, ballottés à la merci de la technologie. Telle est la raison d'être de ce saint-bernard qui, à l'aide d'images sympathiques et en utilisant un langage simple, montre au public que la sécurité en ligne est moins compliquée qu'il n'y paraît.

iBarry sensibilise le public grâce à des conseils clairs et simples

Dans la plupart des cas, iBarry commence par fournir, sur ses pages d'information, quelques conseils simples à propos de divers sujets, par exemple sur le thème de la sécurité des appareils mobiles. S'adressant directement à son lectorat, il énonce cinq règles simples avec lesquelles chacun peut rendre son smartphone et sa navigation plus sûrs :

1 **On verrouille son téléphone :** on bloque l'accès à son smartphone pour le protéger des intrus.
2 **On vérifie les applis :** on n'installe que des applications issues des app-stores officiels et on ne consent qu'aux autorisations indispensables.
3 **On installe les mises à jour :** on recherche les dernières mises à jour des logiciels et des applications et on les installe dès que possible.
4 **On se méfie des offres faites par téléphone, par texto ou en ligne :** on ne tombe pas dans le panneau et on se méfie des offres alléchantes.
5 **On se montre prudents avec les réseaux Wi-Fi :** on n'oublie pas que, lorsque l'on emprunte un réseau local sans fil public, chacun de nos actes accomplis sur le Net peut être intercepté par des tiers.

Ceux qui souhaitent en savoir davantage peuvent s'informer en détail à travers les textes et explications que fournit la plateforme.

Il s'y trouve aussi des captures d'écran illustrant des exemples réels pour expliquer comment reconnaître les faux sites de vente en ligne ou les courriels de hameçonnage. L'objectif étant d'aider les utilisateurs et utilisatrices à se transformer en internautes avertis : plus on est informé, moins on risque de devenir soi-même une victime.

Davantage de sécurité sur le Net en s'amusant et à l'aide de tests

Le site web est divisé en trois sections : « Dispositifs sécurisés », « Sécurité sur Internet » et « Risques sur Internet ». On y trouve des pages d'information sur les sujets les plus importants en matière de sécurité numérique, tels que l'utilisation des appareils intelligents (Internet des objets), la protection des données sur les médias sociaux, ou

encore le hameçonnage et l'escroquerie sentimentale.

iBarry ne se contente pas de promouvoir un comportement sûr à l'aide de rubriques faciles à comprendre : depuis peu, les utilisatrices et utilisateurs ont la possibilité de tester leurs connaissances d'Internet tout en s'amusant. Par exemple, ils peuvent, grâce au quiz sur la sécurité des mots de passe, tester leur savoir en matière de règles de sécurité usuelles pour les mots de passe. D'autres tests suivront prochainement au sujet de la sécurité des smartphones, de la protection des données, de la navigation en toute sécurité et du hameçonnage.

Cependant, il existe des tests non seulement pour vérifier les connaissances des utilisateurs, mais aussi pour passer leur infrastructure au crible. On trouve notamment plusieurs contrôles de sécurité gratuits sur iBarry.ch :

- **le filtrage e-mail** montre si sa propre adresse électronique a fait l'objet de fuites de données ;
- **le filtrage réseau** vérifie si, au cours des derniers jours, son ordinateur a essayé de se connecter à un serveur dont on sait qu'il est infecté ;
- **le scanner de maliciels** analyse l'ordinateur à la recherche de virus, de chevaux de Troie et de vers ;
- **le Software-Check** est le logiciel qui permet de vérifier si son ordinateur présente des failles de sécurité.

Dans le domaine des contrôles de sécurité également, il est prévu d'ajouter des méthodes de test fonctionnelles. En outre, la SISA s'apprête à publier un dépliant qui pourra être distribué lors de manifestations d'information. Il sera aussi possible de le commander et, pour ceux qui le souhaitent, d'y ajouter son logo.

L'objectif ambitieux de la Swiss Internet Security Alliance (SISA) – l'association qui gère iBarry.ch – est de faire de la Suisse le pays à l'Internet le plus sûr au monde, avec, pour guide, le saint-bernard au pelage orange et blanc. À cette fin, la plate-forme de sécurité sur Internet doit devenir le *site de prévention pour la sécurité sur Internet en Suisse*. Aujourd'hui déjà, de nombreuses autorités et entreprises font référence à iBarry.ch. La SISA accueille favorablement tout autre engagement qui soutient cet objectif.

Pour plus d'information : ibarry.ch

La cybercriminalité nous concerne tous

Il n'y a aujourd'hui guère de délit plus accaparant et complexe pour les autorités judiciaires que celui de la cybercriminalité. C'est pourquoi il est essentiel de conjuguer les mesures préventives et répressives et de travailler en réseau, car l'efficacité de cette lutte passe obligatoirement par la collaboration étroite des divers acteurs concernés.

Auteure

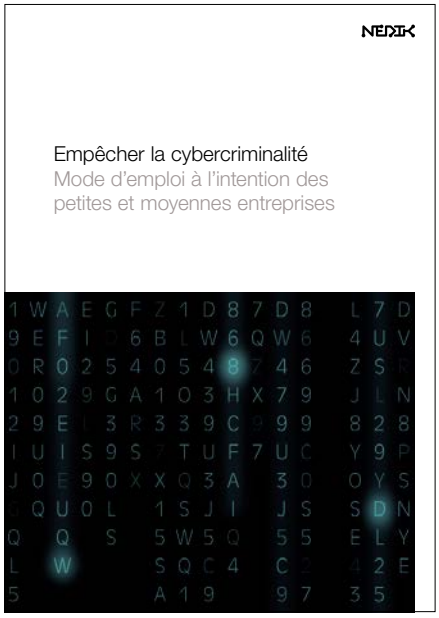
Fernanda Gurzeler est collaboratrice scientifique Prévention du centre de compétence Cyber de la police cantonale bernoise.

DR

Personne n'est à l'abri d'une cyberattaque de quelque nature qu'elle soit. En font l'objet, outre les particuliers, les entreprises grandes et petites, les institutions et les administrations. Vu la complexité croissante des méthodes d'agression et la professionnalisation des agresseurs, il devient de plus en plus difficile d'agir efficacement contre les cybercriminels, voire de les débusquer. Cela, ajouté au taux d'incidences en hausse, montre bien que la prévention dans le cyberespace est primordiale.

Le travail de sensibilisation de la police cantonale bernoise vise aussi les personnes qui jusqu'ici ne se sentaient pas concernées par cette forme de criminalité. Or difficile aujourd'hui d'échapper à Internet qui s'immisce pour ainsi dire partout et comprend une infinie diversité d'utilisateurs. De plus, une cybermenace peut en cacher d'autres : un prétendu courtier (« Fraude à l'investissement ») pourra en même temps attirer sa victime dans les filets d'une pseudo relation amoureuse (« Romance scam »), lui causant ainsi plusieurs dommages à la fois. Autre exemple : certaines entreprises sensibilisent leurs collaborateurs aux dangers d'Internet, mais négligent de se doter des mesures de protection techniques et organisationnelles nécessaires pour y faire face. Sans la conjonction de toutes les mesures préventives, ces entreprises risquent fort d'être la proie de cybercriminels bien organisés ou de pros du piratage informatique.

DR



DR

Les brochures «Guide à l'intention des communes» (www.cyber.police.be.ch → Informations aux communes) et «Mode d'emploi à l'intention des petites et moyennes entreprises» (www.cyber.police.be.ch → Informations aux PME) ont été conçues en collaboration avec différents partenaires.

Ce qui précède plaide clairement en faveur d'une coordination à tous les niveaux et d'une vision globale pour combattre la cybercriminalité tant du point de vue des thèmes abordés que du choix des mesures de prévention. Le but à terme est d'ancrer fermement dans les consciences non seulement les avantages, mais aussi les risques et les défis techniques inhérents aux médias numériques. Etant donné la diversité des utilisateurs – particuliers, autorités, entreprises, associations, hautes écoles, etc. – on voit aussi se profiler la nécessité d'une collaboration non seulement entre les autorités judiciaires, mais aussi avec d'autres partenaires.

Collaboration au niveau national

Les documents d'information élaborés pour les PME et les communes au sein du réseau policier NEDIK (voir encadré) sont un exemple de cette collaboration. La hausse du taux d'incidences et le montant élevé des dommages ont motivé divers corps de police suisses à sensibiliser les petites et moyennes entreprises à la prévention des cyberdélits. Quant aux administrations communales, elles ont fait part de leur souhait d'être davantage informées en la matière. Un des objectifs exprimés par la police est d'encourager les personnes lésées à collaborer, le cas échéant, avec les autorités judiciaires. En effet, les enquêtes ont montré que beaucoup de victimes ne contactaient pas la police ou qu'elles ne le faisaient que très tardivement.

En étroite collaboration avec le Centre national pour la cybersécurité (NCSC), la police cantonale zurichoise, le Réseau national de sécurité (RNS), l'Office fédéral pour l'approvisionnement économique du pays (OFAE), l'Office d'informatique et d'organisation du canton de Berne (OIO) et avec des représentants des divers groupes cibles, la police cantonale bernoise a coordonné la collecte d'informations sur les besoins et l'analyse de la situation sur le terrain en situation réelle. Ce travail a permis de rassembler des renseignements très utiles à l'élaboration des documents d'information. Car tout le monde le sait, les documents et les conseils sont légion, mais ce qui compte, c'est qu'ils soient lus et mis en pratique. C'est pourquoi il était clair dès le départ qu'en plus des documents, il faudrait élaborer d'autres instruments. La discussion entre les divers corps de police a rapidement fait germer l'idée de la mise sur pied de conférences sur le sujet, suivies de la formation correspondante pour les policiers et les policières. En outre, mandatée par le NEDIK dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022, la police cantonale bernoise participe au projet de formation en ligne eCyAd. Le but de ce projet est de sensibiliser les quelque 400 000 collaborateurs des administrations publiques de Suisse aux enjeux de la cybersécurité.

NEDIK

Mandatés par la Conférence des commandants des polices cantonales (CCPCS), les corps de police de Suisse ont mis sur pied le **réseau de soutien aux enquêtes dans la lutte contre la criminalité informatique** (NEDIK). Son objectif est de favoriser la collaboration entre eux dans la lutte contre la cybercriminalité. Ce réseau permet de mettre en commun les ressources et les compétences des polices cantonales et de coordonner les actions et les enquêtes pour mieux combattre les cyberdélits dans tout le pays. Il permet aussi de faire concorder les différentes mesures de répression, d'échanger des informations spécialisées et d'adapter les offres de formation et de formation continue. Le NEDIK permet aussi d'encourager et de coordonner la collaboration dans le domaine de la pédocriminalité, non seulement via la surveillance «peer-to-peer», mais aussi par les enquêtes secrètes en l'absence de soupçons que mènent les cantons dans le domaine numérique.

Ces mesures sont appliquées en accord avec celles de la Prévention Suisse de la Criminalité (PSC) et les complètent. En effet, outre l'élaboration de documents d'information, la PSC assure également la coordination d'autres mesures sur tout le territoire suisse. En 2019 par exemple, en collaboration avec les corps de police romands, elle a lancé la campagne « Et vous ? Vous auriez dit oui ? » qui porte sur divers aspects de la cybercriminalité. Cette année, elle cible le sexting, la fraude à l'investissement, la fraude à la commission sur un bien immobilier et le hameçonnage. De plus, du 3 au 7 mai, la semaine d'action pour la cybersécurité sensibilisera la population sur les importantes mesures à prendre pour assurer sa sécurité numérique.

Coup de projecteur sur le travail de prévention cantonal

Outre son travail de coordination nationale, la police cantonale bernoise, comme les autres corps de police, est toujours plus sollicitée par le défi monumental que représente la cybercriminalité. Dans le canton de Berne, les cyberdélits les plus fréquents relèvent de la criminalité économique : escroquerie aux petites annonces, hameçonnage, logiciels malveillants, fraudes à l'investissement, etc. Pour augmenter sa réactivité dans ce domaine, il est crucial que la police intensifie les mesures de prévention, notamment par des informations sur son site Internet, des jeux en ligne, des webinaires et des petites vidéos didactiques qui démontent les astuces et ficelles utilisées par les escrocs. Ici encore, la collaboration avec les divers acteurs de l'économie privée, de l'administration et de la formation s'avère indispensable, sans parler du contact direct avec la population qu'il s'agira de cultiver à nouveau, dès que possible, au moyen de manifestations destinées à un large public, bien sûr, mais aussi de conférences et d'ateliers pour différents groupes cibles, comme les représentants de PME ou de communes.

Comme l'intérêt des entreprises et des communes pour des conférences sur la cybersécurité est très fort, il est important d'y inclure des exemples réels tirés du quotidien policier et de donner des conseils concrets pour se protéger contre ces agissements criminels. Les discussions qui suivent ces conférences sont aussi un aspect non négligeable du travail de prévention, car les participants peuvent partager leurs connaissances respectives.

La prévention en matière de cybersécurité s'adresse aussi spécifiquement aux enfants, adolescents et jeunes adultes. Certes, les compétences médiatiques font déjà largement partie des programmes de formation, et certaines organisations et entreprises proposent des modules complémentaires en la matière. Mais ce sont le cadre juridique et l'actualisation des risques qui présentent des lacunes. On a pu par exemple le constater lorsqu'un cours à distance a été perturbé par l'intrusion d'hôtes indésirables dans la salle de classe virtuelle. Une action de sensibilisation rapide lancée sur divers canaux a permis de diffuser efficacement les informations nécessaires sur la question.

Par ailleurs, dès la rentrée 2021/2022, le canton de Berne va proposer une formation généralisée sur les « médias numériques » dès la sixième année. Outre les visites dans les écoles, ce projet comprend du matériel de formation accessible en ligne. Ainsi, un quiz pour les jeunes sur le thème du sexting et le cyberharcèlement a été publié en été 2020 sur le site Internet de la police cantonale bernoise. Là encore, c'est un projet qui a été mis sur pied en collaboration avec le ministère public des mineurs, les enseignants et les directions des écoles. Du reste, ce type d'offres est en plein essor et l'échange avec d'autres organisations permet de les faire concorder.

Expérience faite, on constate que la coopération interne et externe est extrêmement utile pour améliorer la prévention, notamment en matière de cybercriminalité, car toutes les parties prenantes à l'élaboration de solutions enrichissent le débat avec une diversité de points de vue et de réflexions. En fin de compte, toutes ces mesures visent non seulement à sensibiliser un maximum de citoyens, d'apprenants, d'entreprises et de communes et à les prémunir contre les cyberdélits, mais aussi à diffuser de façon cohérente et professionnelle les diverses mesures de protection élaborées en commun.

123RF/Elnur Amikishiyev

Le montant des dommages causés par les cyberdélits peut être considérable.

« Capter l'attention et éveiller l'intérêt, c'est ce qui importe »

Une interview avec Denise Nick, directrice, et Manuel Specker, conseiller senior, de l'agence Partner&Partner (Winterthour), sur la stratégie, les écueils et les enjeux de la campagne de prévention « Sécurité numérique ».

DR

Denise Nick

DR

Manuel Specker

Vous réalisez en ce moment une campagne pour aider les citoyennes et citoyens à assurer leur sécurité numérique, un mandat qui vous a été confié par la police, la Confédération et les milieux économiques. Avec un sujet aussi aride, il s'agit à la fois de faire passer un message et de tenir compte des différentes attentes. Qu'est-ce qui prédomine : l'emballement ou l'effarement ?

Denise Nick (DN) : L'emballement, sans hésiter. Il n'est pas rare dans un tel projet que plusieurs organisations soient parties prenantes. Mais il est toujours captivant de voir comment elles interagissent, quel est le partage des rôles ou les processus décisionnels. Nous ne trouvons pas que la sécurité numérique soit un sujet aride. Abstrait, oui, parce que les compétences manquent peut-être. Tous nous utilisons ces appareils, et en cette période de télétravail encore davantage. Mais la plupart d'entre nous sommes de simples utilisateurs peu au fait de la sécurité numérique.

Manuel Specker (MS) : Il est aussi très intéressant de voir combien une bonne coordination fait la différence lorsque tant d'organisations sont impliquées ; avec relativement peu de moyens, on peut être présent sur plusieurs canaux. Le potentiel est énorme pour toucher un grand nombre de personnes. Pour avoir une telle quantité de destinataires, il faut d'habitude engager des moyens considérables.

Y a-t-il des restrictions liées au fait que la police est le mandant ?

DN : Non, car la sécurité numérique n'est pas un sujet relevant spécifiquement de la police. Certes, il faut préserver un certain sérieux de style et de ton, mais ce n'est rien d'exceptionnel.

Comment abordez-vous la phase de mise en place d'une campagne ?

DN : Cela commence par la lecture, beaucoup de lecture…

MS : Il est important, au début, de se faire une idée des objectifs et de l'effet qu'on escompte. Ensuite on fait une comparaison avec la situation actuelle pour déterminer quels éléments sont déjà connus. A partir de là, se dégagent peu à peu les grandes lignes de la campagne. Il s'agit alors de déterminer quels canaux sont les plus adaptés, pour qui, et quelles sont leurs interactions : nous nous demandons où se trouve le point de convergence entre un thème et son destinataire, comment livrer des informations supplémentaires et quel est le point d'appui pour lancer l'action. La réflexion porte aussi sur les contenus à diffuser, en mettant fortement l'accent sur la langue et le ton qui sera donné. Un point essentiel, surtout pour une campagne de prévention. Il faut trouver le savant mélange qui permettra d'atteindre l'objectif recherché. Puis vient la phase de décantation avec le client pour formuler les messages et trouver comment les mettre en images.

DN : Les recherches faites au début autour d'un thème ont énormément d'importance. Il y a une masse d'éléments déjà pensés, écrits et publiés par les institutions les plus diverses. Réinventer les contenus n'aurait eu aucun sens, mais il nous a fallu déblayer le terrain pour partir sur une bonne base et savoir ce qui est essentiel.

Aurait-il été plus facile de formuler vous-mêmes les contenus ?

DN : Non, cette situation est confortable. Les contenus étant déjà connus, nous pouvons nous concentrer pleinement sur le message.

Et à quoi faut-il être attentif à ce stade ?

DN : Les contenus doivent être aisément compréhensibles et éveiller l'intérêt. Il s'agit d'approfondir la thématique et de s'informer sans en arriver au point d'avoir le sentiment que la matière est compliquée et qu'on ne peut que se fourvoyer.

Comment faites-vous pour ne pas en arriver là ?

MS : Sachant que le sujet est important, on peut partir de l'idée que les connaissances préalables en la matière sont déjà bien répandues dans la population et qu'il ne faudra pas engager trop de travail didactique. Le défi consiste plutôt à formuler les consignes de façon que chaque étape puisse être mémorisée aisément. Nous confortons ainsi tout un chacun dans la certitude que le but peut être atteint rapidement et sans obstacles insurmontables, ce qui le dispose favorablement à mettre ensuite ses connaissances en pratique. Il ne faut pas avoir l'impression de recevoir des leçons ni s'ennuyer, mais apprendre comment s'aider soi-même.

DN : C'est le propre des sujets de prévention : nous voulons susciter un changement de comportement chez un individu. C'est fort louable, mais il faut d'abord créer le terreau qui rendra ce changement possible. Pour cette campagne, nous avons donc prévu une page de renvois qui détaille pas à pas, simplement, ce qu'il faut faire. Les personnes intéressées y trouvent rapidement les informations souhaitées.

Comment parvenez-vous à persuader le public cible de l'utilité de changer de comportement ?

DN : Nous procédons par analogie avec la vie quotidienne, donc nous comparons des choses connues avec l'espace virtuel. C'est l'élément central de la campagne et des sujets à diffuser. Nous présentons des situations dans lesquelles habituellement on se protège et les extrapolons, sans lever de doigt moralisateur, en optant pour l'humour ou l'effet de surprise.

Justement, quel rôle joue l'humour dans ce type de campagne ?

MS : Il faut trouver le juste milieu. Prendre le sujet à la rigolade pourrait faire oublier la gravité du sujet. A éviter donc. Cette campagne traite de la sécurité. Un certain sérieux est de mise.

Que faut-il éviter à tout prix dans une campagne de prévention ?

DN : Il y a des règles fondamentales. On sait entre-temps que faire peser des menaces est peu productif. Pour mettre les gens en situation d'agir, il faut éviter d'actionner le levier de la peur, cela ne fonctionne pas.

Vous arrive-t-il de faire machine arrière, lorsque vous constatez que l'approche choisie ne fonctionne pas ?

DN : Cela arrive probablement dans chaque processus, dès que l'on se met à réfléchir au « comment ». A chaque fois, nous traçons plusieurs pistes, plusieurs approches de réalisation. Il est fréquent que nous butions ou que nous nous apercevions qu'une piste n'est pas praticable. Parfois, la piste choisie est celle dont nous n'escomptions pas qu'elle ait du potentiel. Il faut simplement se mettre en route. Au départ, tous les éléments de la mosaïque sont étalés devant nous : définition de l'objectif, termes du mandat, graphisme et texte ; et peu à peu le tableau émerge.

Vous nous avez récemment présenté le visuel de la campagne. Il y a eu naturellement des discussions, même si nous avions déjà opté pour une piste. Le chemin est manifestement sinueux avant que la mosaïque ne devienne un tableau…

DN : Nous avons toujours hâte de voir ce qui arrive quand nous faisons une première proposition. Les uns jettent un regard, et font très vite un commentaire : « Oui, je comprends la démarche, ça nous convient. » Et d'autres ont une approche plutôt scientifique ; il faut bannir toute équivoque. C'est souvent enrichissant pour nous, comme c'est le cas avec vous, car on voit les différences dans la manière d'appréhender une image. Au bout d'un moment, il faut trancher, arrêter de tenir compte de tous les avis et de faire des compromis. Sinon le message en pâtit. A force de vouloir être correct, l'image n'est plus bien comprise par le groupe cible. Capter l'attention et éveiller l'intérêt, c'est ce qui importe. Le travail d'approfondissement permet de tracer minutieusement les contours de ce qui est correct, mais lors du premier contact, on peut se permettre de ne pas être trop pointilleux et renoncer à échafauder des concepts tarabiscotés.

La campagne se focalise sur les médias sociaux. Cela cadre-t-il avec la police ?

DN : Les médias sociaux sont le vecteur idéal pour établir le contact avec la population et se rapprocher des gens. Nous le voyons à Winterthour. La police municipale utilise les médias sociaux avec une grande aisance et a une belle présence sur Tiktok. Elle est en phase avec la nouvelle génération. Les natifs de l'ère numérique ne lisent pas vraiment les dépliants. Ils passeraient à côté de beaucoup de sujets s'il n'y avait pas d'autres moyens. Les canaux numériques permettent une diffusion rapide et séquentielle. L'occasion pour la police de donner une tout autre image d'elle. Sans être concerné par un problème, on a peu de contact avec la police, et l'on ne sait pas qu'elle est beaucoup plus abordable et ouverte qu'on ne le pensait.

Qu'avez-vous hâte de découvrir lors de la semaine d'action en mai ?

DN : Une chose qui m'intéresse beaucoup : on a là un immense réseau avec un grand nombre de multiplicateurs, et c'est formidable de pouvoir actionner autant de leviers. Il faut néanmoins les orchestrer. Et c'est tout l'enjeu de la campagne. Chacun doit prêter main-forte et faire ce qu'il faut quand il le faut. Cela suppose une bonne organisation et une information sans fausse note, afin que tous sachent exactement quel matériel est disponible, à quel moment et pour quel usage. Un défi pas simple à relever, mais nous aimons ça.

Madame Nick, Monsieur Specker, un grand merci pour cet entretien riche en enseignements !

(Propos recueillis par Beatrice Kübli)

Nouveaux membres de commission

Les commissions de la PSC ont pris congé de quatre personnes, pour lesquelles des successeurs ont été trouvés.

Commission spéciale

Membre engagé pendant toutes les années passées à la Commission spéciale de la PSC, Bruno Lüthi est un expert qui fait autorité en matière de sécurité intégrale, de sécurité dans l'administration et de protection anti-effraction (la liste n'est pas complète !). Il a quitté la commission spéciale pour prendre une retraite bien méritée. Nous adressons nos vifs remerciements à Bruno pour les connaissances et l'allant dont nous avons pu bénéficier pendant si longtemps. Nous lui souhaitons à lui et au FC Thun nos meilleurs vœux pour le long avenir radieux qui s'ouvre à eux !

Bruno Lüthi sera remplacé par **Markus Friedli,** dont nous saluons l'arrivée dans la commission !

Markus Friedli, chef de secteur Conseil et projets de la PolCant bernoise n'est pas un novice en matière de prévention. Il est engagé depuis des années dans le domaine de la protection anti-effraction et dans beaucoup d'autres champs de la prévention. Nous sommes heureux que Markus Friedli partage ses connaissances spécialisées avec les membres de la commission spéciale !

Commission de projet

Nous avons dû malheureusement prendre congé de Kasi Bischoff, appelé à assumer d'autres fonctions au sein de la police municipale de Winterthour. Kasi a représenté les corps municipaux pendant plus de quatre ans, l'occasion pour la commission de fréquenter le représentant d'une police aussi moderne et innovante que celle de Winterthour. Nous remercions chaleureusement Kasi Bischoff pour ses suggestions toujours bienvenues, sa participation constructive, sans oublier sa bonne humeur indéfectible, et nous lui adressons nos meilleurs vœux à son nouveau poste.

Nous accueillons tout aussi chaleureusement son successeur **Thomas Egloff,** chargé lui aussi de représenter les corps de police municipaux. Nous sommes certains qu'il ne manquera pas de nous communiquer des idées et des suggestions utiles en nombre. Il nous vient aussi de la police municipale de Winterthour. Soyez le bienvenu, Monsieur Egloff !

Nous avons aussi dû prendre congé de Roland Hübner de la PolCant Appenzell Rhodes-Intérieures qui représentait le concordat Ostpol pour la police de sûreté. Roland nous a accompagnés pendant de nombreuses années en représentant de son petit canton toute la Suisse orientale avec ferveur et un grand esprit d'initiative. Nous adressons à Roland nos meilleurs vœux pour la suite de son parcours professionnel et le remercions de sa collaboration toujours bienvenue !

Ostpol sera désormais représenté par **Stephan Kühne,** chef de la sûreté de la PolCant saint-galloise. Nous lui souhaitons aussi la bienvenue et sommes heureux de pouvoir compter sur ce soutien vigoureux venu de l'Est !

Enfin, l'ancien chef de la sûreté de la PolCant Schwyz, Stefan Grieder, a quitté ses fonctions de représentant du concordat Suisse centrale, parce qu'il prend les commandes de la PolCant de Nidwald en février 2021. Nous le félicitons de tout cœur pour sa promotion et ce nouveau défi, et le remercions de son investissement de plusieurs années pour la CP et de sa collaboration constructive.

Nous avons le plaisir de souhaiter la bienvenue au nouveau représentant des polices de sûreté de la Suisse centrale, **Jürg Wobmann,** chef de la sûreté à la PolCant lucernoise. Nous nous réjouissons de poursuivre l'excellente collaboration qui a toujours prévalu avec les PolCant du cœur de la Suisse.


DR

Markus Friedli, chef de secteur Conseil et projets de la PolCant bernoise


DR

Cdt Thomas Egloff, MLaw, Chef de service principal


DR

Stephan Kühne, chef de la sûreté de la PolCant saint-galloise


DR

Jürg Wobmann, chef de la sûreté à la PolCant lucernoise

Le paradoxe de la prévention…

… pourrait se résumer ainsi : mieux elle fonctionne, moins elle nous semble nécessaire. Car les maux qu'elle doit empêcher ne se produisent pas, et la menace n'est souvent ni visible ni palpable. En revanche, les habitants du village craignent ce qui *pourrait* se passer si on n'avait *pas* construit de paravalanches. Ils le craignent même si le dispositif tient le coup : soit parce qu'ils étaient là lors du passage de la dernière avalanche, soit parce qu'ils connaissent les récits de catastrophe et qu'ils ont tous les jours devant leurs yeux la montagne enneigée – donc la menace. De même, le promeneur qui, un soir d'été au bord du lac, est accompagné d'une nuée de moustiques sans qu'aucun d'eux ne le pique, ne mettra jamais en doute l'effet préventif de son spray antimoustiques – d'autant moins qu'il a été piqué à *chaque* fois qu'il est sorti *sans* prendre de précaution. Les maux subis nous ouvrent les yeux ; reconnaître la menace, c'est aussi reconnaître le bien-fondé de la prévention.

Néanmoins, au-dehors, les nouvelles menaces sont légion, des menaces diffuses face auxquelles l'individu ne peut pas s'appuyer sur son vécu ou sur celui de sa famille, par exemple la pandémie. Pour prévenir efficacement, il faut se fier à des informations puisées hors de son propre horizon empirique. Apparaît alors un autre paradoxe de la prévention : plus je suis vulnérable parce que je fais partie d'un groupe à risque et donc d'une minorité, plus je profite de la prévention que pratique la collectivité, tandis que la majorité moins vulnérable n'en profite que très indirectement, et peut-être à long terme ; en outre, elle subit surtout des restrictions dans son mode de vie habituel, ce qui lui en coûte. Ce sont de bien mauvaises nouvelles pour la plupart des gens, raison pour laquelle beaucoup sont enclins à minimiser la menace, voire même à la nier. Le messager passera dès lors pour un oiseau de mauvais augure. Or, si le virus venait quand même à me toucher sérieusement, à quel saint me vouerais-je : à « vérité24.ch » ou à un véritable hôpital ?

Pour la cybercriminalité, au cœur de notre édition de PSC Info, c'est encore une autre histoire. La plupart des gens ne connaissent pas vraiment les différentes menaces dont il est question ici, mais dès que les connaissances auront été diffusées rapidement et à large échelle et des modules de cours mis en place, la prévention présentera des avantages pour tout un chacun et ce, sans paradoxe. Les particuliers en bénéficieront puisqu'ils sauront quels pièges leur tend la Toile et ce qu'il adviendrait de leurs avoirs. L'ensemble de l'économie en bénéficiera aussi, dès lors qu'elle s'est prémunie contre les cyberattaques directes et qu'elle peut continuer de tabler sur la stabilité financière de clients et de partenaires eux aussi prémunis. Dans ce cas, protéger les individus, c'est aussi protéger la collectivité, et vice-versa.

Pour finir, un dernier exemple de paradoxe de la prévention, illustré par le changement climatique. A l'inverse des avalanches, des pandémies et des moustiques, il ne sera probablement pas possible d'attendre que surviennent des dégâts pour obtenir des valeurs empiriques solides sur lesquelles fonder des actions préventives efficaces pour le futur. Il s'agirait plutôt d'éviter que n'advienne quelque chose qui est de l'ordre du jamais vu. Il existe nombre d'évidences qu'une catastrophe se prépare, mais pas de preuves ; pour la première fois, les êtres humains ne devraient pas entendre raison une fois les *maux* subis mais en se servant précisément de leur *raison*. Que la fête continue à battre son plein sur le pont supérieur du paquebot, alors que l'iceberg (le dernier ?) a déjà éventré la coque, est une hypothèse. Il faudra attendre pour la vérifier. Rappelons-nous la fameuse phrase du chef amérindien : « Quand le dernier arbre aura été abattu […] quand le dernier poisson aura été pêché, alors on saura que l'argent ne se mange pas. ». D'ici là : porter son masque, se protéger contre le virus, et si le téléphone sonne… ne pas décrocher !

Volker Wienecke
Contact : redaktion@skppsc.ch

TOUTE L'ACTUALITÉ PSC

«Sexe en ligne : ne vous laissez pas rançonner !»
Ce qu'il faut savoir sur la sextorsion

Il fait très mal … ce moment où une personne réalise que quelqu'un la fait chanter avec des photos ou des vidéos intimes. Les cas de sextorsion sont multiples. Ils peuvent survenir après un tchat érotique ou se présenter sous forme de message électronique frauduleux. Les deux modes opératoires profitent du fait que les victimes veulent éviter la publication de matériel photo compromettant (supposé existant) ou son envoi à des amis et des connaissances. Les victimes paient donc la rançon. Dans un cas comme dans l'autre, le message de prévention est le suivant : *Keep calm and don't pay !*

«Rendements de rêve ? Gare au réveil !»
Ce que vous devez savoir sur la fraude à l'investissement sur Internet

Les escrocs prolifèrent sur Internet pour vous proposer des placements prometteurs sur leurs prétendues plateformes de négoce. Y donner suite, c'est perdre à coup sûr ! Le nouveau dépliant PSC explique de manière aisément compréhensible comment se passe classiquement la fraude à l'investissement sur Internet, comment vous informer avant de placer votre argent dans des cryptomonnaies et que faire si vous avez perdu de l'argent. Vous trouverez aussi des astuces pour détecter – à temps – si une offre est sérieuse ou frauduleuse.
Le dépliant a été mis au point avec l'aimable collaboration d'EBAS («eBanking – en toute sécurité !»).

«Ta vie en ligne ?»

Le mini-dépliant au format carte de crédit est un condensé d'informations sur le comportement des jeunes dans Internet et sur la réaction qu'ils devraient avoir en présence d'un comportement incorrect et irrespectueux. Cette publication complète les brochures Safebook, plus détaillées, destinées aux jeunes et aux responsables éducatifs. C'est par son graphisme jeune et délibérément différent qu'elle entend toucher son public-cible.

Les trois dépliants sont disponibles à l'adresse : www.skppsc.ch → Téléchargements → Brochures + dépliants

ÇA RIME AVEC CRIME

Afin d'amener un peu de légèreté dans le contexte souvent éprouvant et peu réjouissant de la lutte contre la criminalité, nous envisageons d'ouvrir les colonnes de PSC INFO à un trait d'humour (de nos lectrices et lecteurs !). Poème, anecdote tirée du quotidien de la police, blague bien tournée ou caricature : laissez libre cours à votre imagination ! Si cela vous tente, envoyez vos propositions à info@skppsc.ch !

«Cybercrime», de Mario Capitanio, Berne

SKPPSC
Prévention Suisse de la Criminalité
Maison des cantons
Speichergasse 6
Case postale
CH-3001 Berne

www.skppsc.ch