Communiqué de presse du 26 avril 2021

Semaine nationale d'action pour plus de sécurité dans le cyberespace

Les annonces de cyberincidents ont fortement augmenté ces dernières années en Suisse (fig. 1). Du 3 au 7 mai 2021, la semaine nationale d'action sur la «sécurité du cyberespace» vise à sensibiliser aux risques existants et à la manière de se protéger. Son comité d'organisation compte des partenaires renommés issus des autorités ainsi que des milieux scientifiques et économiques.

Le coronavirus a donné un coup d'accélérateur à la transformation numérique, en Suisse comme partout dans le monde. Beaucoup de gens travaillent depuis la maison, font davantage d'achats en ligne ou sont devenus friands d'offres numériques. Les cyberincidents tendent dès lors à se multiplier et frappent davantage les esprits. Les annonces faites à la police ou au guichet unique du Centre national pour la cybersécurité (NCSC) ont augmenté, avant de se stabiliser à un niveau élevé. Les cas de fraude et d'hameçonnage (*phishing*), surtout, sont en hausse (fig. 2). Pendant la crise du coronavirus, les escrocs ont profité de l'essor du commerce en ligne pour envoyer des messages de phishing signalant une livraison de colis à valider. De nouveaux scénarios de fraude sont également apparus, comme l'arnaque aux dons en faveur des victimes du COVID-19 ou les fausses commandes de masques faciaux.

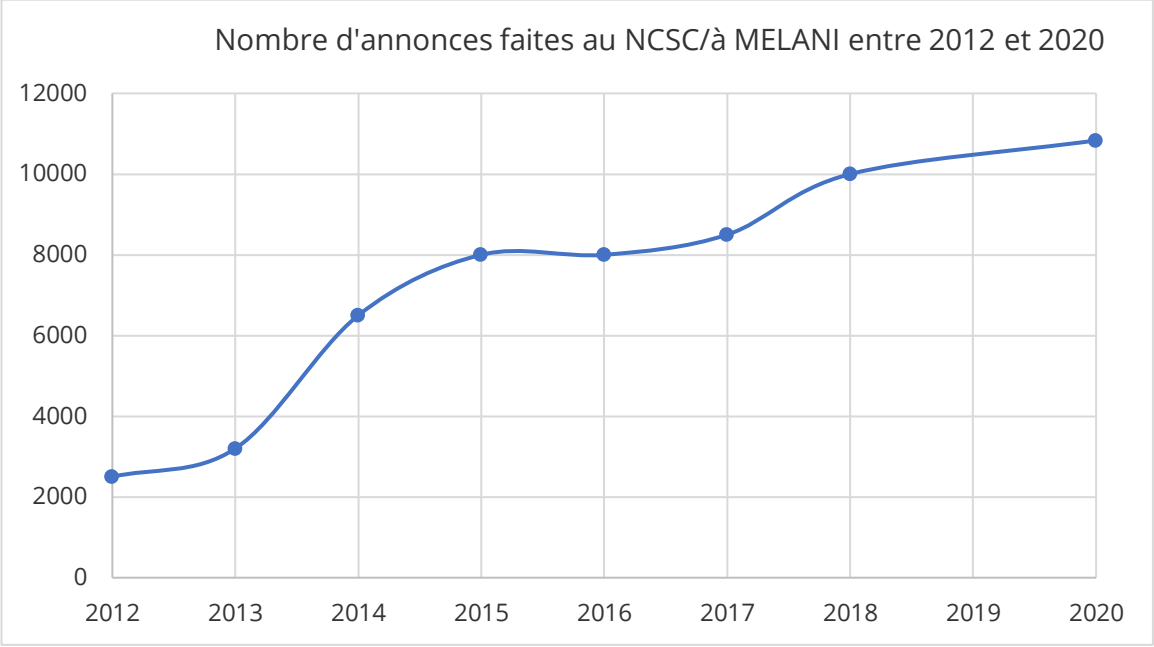

Fig. 1: Augmentation du nombre de cyberattaques signalées au NCSC, 2012-2020. Copyright: NCSC, 2021

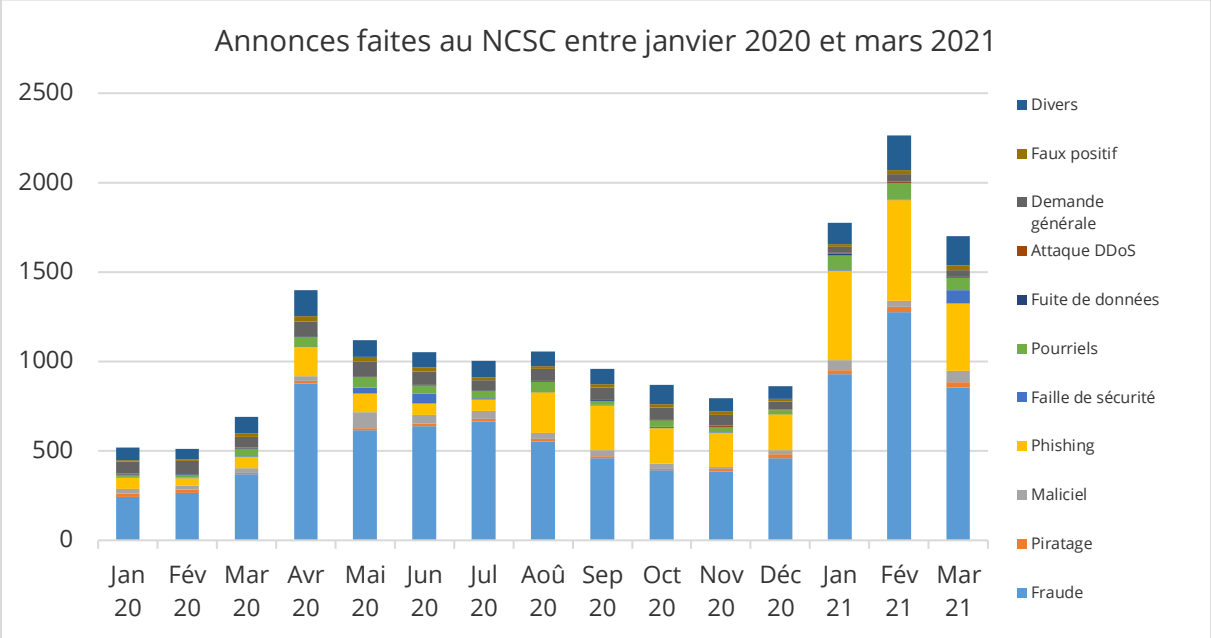

Fig. 2: Typologie des cyberattaques signalées au NCSC en 2020/2021. Copyright: NCSC, 2021

Semaine nationale d'action organisée avec des partenaires renommés

La semaine nationale d'action vise à attirer l'attention sur la cybersécurité. Il s'agit encore de montrer que chacun de nous peut sensiblement améliorer sa sécurité personnelle sur Internet, avec des moyens simples et sans grands efforts: en choisissant des mots de passe robustes, en effectuant des mises à jour régulières de ses logiciels ou en faisant preuve de vigilance dans le cyberespace.

La Prévention Suisse de la Criminalité (PSC) a lancé cette semaine d'action avec le concours du Centre national pour la cybersécurité (NCSC), de la plateforme «eBanking – en toute sécurité!» de la Haute école de Lucerne (HSLU), de la plateforme pour la sécurité sur Internet iBarry de la Swiss Internet Security Alliance (SISA), ainsi que des corps de police cantonaux et municipaux.

Des activités d'accompagnement sont prévues du 3 au 7 mai 2021, sur divers canaux en ligne ou hors ligne. Elles coïncideront, le jeudi 6 mai, avec la Journée mondiale du mot de passe. D'éminents représentants du monde économique et politique livreront leur témoignage durant la campagne.

Le site www.S-U-P-E-R.ch constitue la pièce maîtresse de la campagne. Outre des conseils et astuces (sauvegarde des données, mises à jour de sécurité, protection contre les virus, mots de passe, comportement adéquat sur Internet), les visiteurs y découvriront un aperçu des cyberrisques, avec les mesures de prévention à prévoir et des instructions pratiques. Des webinaires gratuits seront également proposés sur différents thèmes.

Cinq thèmes centraux sur la cybersécurité – et un truc mnémotechnique

Un thème différent sera traité chaque jour pendant la semaine d'action. Chaque thème est associé à une lettre de l'alphabet, dont la combinaison donne le terme S-U-P-E-R. Ce truc mnémotechnique aidera les internautes à acquérir des réflexes utiles à leur sécurité personnelle sur Internet:

- **S comme Sauvegarder** – lundi 3 mai 2021
  Sauvegardez régulièrement vos données sur au moins un autre support.

- **U comme Utiliser ses mises à jour** – mardi 4 mai 2021
  Mettez à jour votre système, vos programmes et vos applis en installant les versions les plus récentes.
- **P comme Protéger avec un antivirus** – mercredi 5 mai 2021
  Assurez-vous d'avoir installé un antivirus sur votre appareil.
- **E comme Équiper ses accès d'un mot de passe fort** – jeudi 6 mai 2021
  Connectez-vous exclusivement avec des mots de passe forts.
- **R comme Réduire** – vendredi 7 mai 2021
  Réduisez les risques d'escroquerie dans le cyberespace en faisant preuve d'une bonne dose de méfiance.

La prévention, moyen le plus efficace

«Les enquêtes cybercriminelles sont d'une grande complexité, pour un bilan souvent maigre. La campagne actuelle est utile pour prévenir de tels incidents», souligne Fabian Ilg, spécialiste en cybercriminalité et directeur suppléant de la PSC.

Même si la proportion de cyberincidents signalés tend à augmenter, ce n'est que la pointe de l'iceberg. «Il est important d'annoncer les attaques. Cela aide le NCSC à évaluer la situation encore plus rapidement, à identifier de bonne heure les nouveaux développements et à prendre les mesures utiles», souligne Florian Schütz, délégué à fédéral à la cybersécurité, directeur du NCSC. Daniel Nussbaumer, président de la SISA, renchérit: «cette semaine d'action vise à attirer l'attention de la population et des médias sur ce thème, car la prévention constitue le moyen d'agir le plus efficace.»

Les cyberattaques comportent de multiples facettes. Il arrive que des ordinateurs ou des smartphones soient utilisés à l'insu de leur propriétaire à des fins illégales et que les données personnelles des victimes, les informations sur leur carte de crédit, leurs données d'ouverture de session, voire leur identité complète soient dérobées et utilisées à mauvais escient. «Les cybercriminels débordent d'imagination, sont très au point et souvent organisés au niveau international», explique Fabian Ilg. «Il est donc important d'attirer aujourd'hui l'attention de la population sur les risques et de lui fournir aide et information. Car au fond, ce n'est pas sorcier de se protéger contre les cyberattaques.»

Pour en savoir plus

www.S-U-P-E-R.ch

Matériel graphique

Le matériel graphique* est disponible ici.

Partenaires organisationnels

Prévention Suisse de la Criminalité
«eBanking – en toute sécurité!» – plateforme indépendante de la Haute école de Lucerne
Centre national pour la cybersécurité NCSC
iBarry – Plateforme pour la sécurité sur Internet

Contact pour les questions générales des médias

Fabian Ilg, directeur suppléant, Prévention Suisse de la Criminalité PSC
Maison des Cantons, Speichergasse 6, 3001 Berne
fi@skppsc.ch
Tél.: +41 31 511 00 08

*Il ne peut pas être modifié et ne peut être utilisé que dans le cadre d'un compte rendu de la campagne.

Vos contacts (par ordre alphabétique)

Les personnes ci-après répondront volontiers à vos questions et vous accorderont des interviews sur les thèmes indiqués, dans le contexte de vos comptes rendus de la semaine d'action.

Marcus Beyer
Security Awareness Officer Swisscom (Suisse) SA

- Sécurité informatique
- Sensibilisation à la cybersécurité
- Cyberrésilience en entreprise

marcus.beyer@swisscom.com
Tél.: +41 58 221 12 18 / +41 79 307 81 33

Andreas Hölzli
Responsable du centre de compétences Cyberrisques, Mobilière Suisse Société d'assurances SA

- Assurance des cyberrisques pour les particuliers, les PME et les entreprises
- Cyberattaques contre les PME

Contact: Jürg Thalmann, porte-parole
media@mobiliar.ch
Absence du 30 avril au 7 mai 2021

Chantal Billaud
Directrice, Prévention Suisse de la Criminalité PSC

- Criminologie et psychologie
- Mécanisme des cyberfraudes

cb@skppsc.ch
Tél.: +41 31 511 00 09

Fabian Ilg
Directeur suppléant, Prévention Suisse de la Criminalité PSC

- Prévention en matière de cybersécurité
- Phénomènes de cybercriminalité

fi@skppsc.ch
Tél.: +41 31 511 00 08

Ivan Bütler
Fondateur et président du conseil d'administration de Compass Security

- Tests d'intrusion et exemples concrets réalisés en Suisse/concernant des sociétés suisses
- Progression des cyberrisques

ivan.buetler@compass-security.com
Tél.: +41 79 250 06 28

Centre national pour la cybersécurité NCSC

- Faits et chiffres du guichet unique du NCSC
- Attaques par des maliciels
- Procédure en cas (de suspicion) d'attaque
- Projections

ncsc-media@gs-efd.admin.ch

André Duvillard (en français et en allemand)
Délégué du Réseau national de sécurité RNS

- Politique suisse de sécurité
- Coopération des acteurs suisses de la sécurité
- Poursuites pénales et criminologie

andre.duvillard@gs-vbs.admin.ch
Tél.: +41 58 464 21 13

Daniel Nussbaumer
Directeur de la cybersécurité pour la Suisse chez T-Systems, président de la Swiss Internet Security Alliance SISA

- Cybercriminalité et prévention
- Risques et chances de la numérisation

daniel@swiss-internet-security-alliance.ch
Tél.: +41 79 672 32 05

Serdar Günal Rütsche
Chef de la division Cybercrime de la Police cantonale zurichoise, responsable du réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique NEDIK

- Criminalité numérique et cybercriminalité

gus@kapo.zh.ch
Tél.: +41 44 247 22 00, Absence du 19 au 23 avril 2021

Stephan Walder
Procureur en chef adjoint, Ministère public II du canton de Zurich, Centre de compétence Cybercrime

- Poursuites pénales et situation juridique

stephan.walder@ji.zh.ch
Tél.: +41 44 247 31 40

Oliver Hirschi
Professeur, expert en sécurité de l'information et responsable de la plateforme «eBanking – en toute sécurité!», Haute école de Lucerne HSLU

- Attaques par force brute (y c. démonstration en direct)
- Expertise en matière de mots de passe et d'e-banking
- Vol d'identité

oliver.hirschi@hslu.ch
Tél.: +41 41 757 68 58

Témoignage anonyme

- Victimes de l'arnaque aux petites annonces

medien@skppsc.ch
Tél.: +41 52 269 16 64 (Mme Honegger)
Absence: du 5 au 15 mai 2021

Interviews et déclarations mises à disposition

Ces interviews ne peuvent être citées que dans le cadre d'un compte rendu de la semaine d'action. Les personnes concernées doivent être préalablement contactées pour toute utilisation de leurs propos dans un contexte différent ou sous une forme modifiée.

Situation générale: «La cybersécurité est devenue un enjeu majeur»

Florian Schütz, délégué fédéral à la cybersécurité, directeur du NCSC

Pour quelles raisons les annonces d'incidents ont-elles augmenté pendant la pandémie de COVID-19?
Le NCSC a en effet enregistré beaucoup plus d'annonces d'incidents. Par contre, les cyberattaques ont été à peine plus fréquentes. Nous attribuons cet afflux d'annonces à une prise de conscience des entreprises et des particuliers. Les cybercriminels ont quant à eux utilisé la pandémie comme prétexte pour diffuser leurs logiciels malveillants.

Quelles sont en ce moment les menaces les plus répandues?
Nous examinons en détail quelles formes de menaces gagnent du terrain, en sachant que tout peut changer très vite. Il existe différents types de menaces, le phishing étant l'une des plus connues et un sujet de préoccupation constant. Les escrocs tentent d'amener la victime, avec des courriels ou des SMS falsifiés, à leur livrer des informations personnelles, comme des mots de passe ou des informations sur leur carte de crédit. De tels courriels ou SMS ont parfois une apparence très professionnelle et sont impossibles à repérer au premier coup d'œil.

Que dois-je faire si j'ai été victime d'une cyberattaque ou si j'ai de telles craintes?
Tout dépend du genre d'attaque. En principe, il est conseillé d'agir vite pour limiter les dégâts. Il vous faut par exemple faire bloquer vos cartes de crédit et prévenir les personnes susceptibles d'avoir la même mésaventure. En outre, il convient d'annoncer l'incident au Centre national pour la cybersécurité (NCSC). Si vous avez subi un préjudice financier, vous devriez porter plainte auprès de l'autorité de police compétente.

Quel rôle la cybersécurité joue-t-elle en Suisse?
À l'heure de la transformation numérique, la cybersécurité revêt une importance grandissante. Au niveau fédéral, il s'agit déjà d'une priorité de la politique extérieure et de sécurité. Mais la cybersécurité tend également à devenir un passage obligé pour la place économique et pour la population suisse.

Thème de la prévention: «Plus on en sait, moins les cybercriminels auront la tâche facile.»

Daniel Nussbaumer, président de la Swiss Internet Security Alliance (SISA), qui a lancé la plateforme iBarry.ch

Pourquoi les autorités et les milieux économiques insistent-ils tant sur la prévention dans le cyberespace?
La poursuite pénale gagne en efficacité dans le cyberespace. La justice parvient plus souvent et toujours mieux à faire rendre des comptes aux escrocs. Mais comme la criminalité numérique s'est mondialisée et sachant que les poursuites pénales internationales sont d'une grande complexité et ont tendance à échouer faute de base légale, il est important d'informer la population sur les risques encourus.

La prévention est-elle toujours à la traîne des escrocs?
Il existe toutes sortes d'escrocs. Si les uns sont peu inventifs, d'autres sont toujours à l'affût de nouvelles astuces et méthodes, et compliquent notre travail. La prévention fait donc appel à différentes techniques. D'abord, nous décrivons tous les types de fraude, des faux appels de support technique aux courriels de phishing, en passant par l'arnaque aux sentiments. Ensuite, nous montrons que même quand ils inventent de nouvelles histoires, les criminels utilisent toujours des techniques similaires pour nous piéger. Car ils connaissent nos points faibles.

Pourriez-vous préciser?
Ils commencent par éveiller l'intérêt de leur victime. Tous les moyens sont bons: demande d'amitié dans les réseaux sociaux, prétendue commande passée à une entreprise, courriel, message WhatApp, petite annonce ou appel téléphonique. Une fois le contact établi, ils tentent d'empêcher la victime potentielle de prendre du recul et d'analyser la situation, en la mettant sous pression. Les escrocs multiplient les courriels, les messages ou appels, laissent à la victime un délai de réflexion très court, voire lui fournissent eux-mêmes de prétendues preuves afin qu'elle ne fasse ses propres recherches.

La prévention affiche-t-elle des résultats?
Il est toujours difficile de démontrer les résultats de la prévention. Mais les milieux économiques et les autorités ont déjà beaucoup investi dans le travail d'information, et nous constatons que la population suisse en sait toujours plus sur les risques d'Internet. Les comportements en ligne laissent toutefois encore à désirer. C'est pourquoi nous avons lancé la campagne de sensibilisation S-U-P-E-R.ch.

Thème «Sauvegarder»: «Pensez à votre smartphone.»

Fabian Ilg, directeur suppléant de la PSC

Tout le monde sait aujourd'hui qu'il faut sauvegarder ses données sur un autre support, n'est-ce pas?
C'est possible, encore faut-il le faire. Nous estimons qu'un tiers de la population suisse ne sauvegarde pas ses données séparément.

Les pertes de données sont-elles fréquentes?
Pensez à votre smartphone – on a vite fait de l'égarer, il risque d'être volé ou de se casser. Les données sont alors perdues, si on ne les a pas enregistrées ailleurs. Beaucoup de gens ne s'en rendent compte qu'une fois qu'un malheur est arrivé. La perte de telles données est très douloureuse.

Que faire alors?
Il convient d'enregistrer régulièrement ses données sur un disque dur externe ou dans le nuage. La première solution prend un peu de temps, et peut donc paraître dissuasive. C'est pourquoi les systèmes d'exploitation usuels proposent des programmes de sauvegarde très simples à utiliser. Nous avons compilé sur www.S-U-P-E-R.ch toutes les informations utiles à connaître.

Thème «Utiliser ses mises à jour»: «Aucun logiciel n'est parfait.»

Ivan Bütler, fondateur de Compass Security

Pourquoi les mises à jour sont-elles si utiles?
Loin d'être parfait, un logiciel comporte toujours des vulnérabilités. Les mises à jour corrigent les failles de sécurité. Autrement dit, faute d'effectuer les mises à jour, on s'expose à ce que les vulnérabilités restantes soient exploitées par des pirates – qui sont aux aguets et pourront aisément s'introduire dans un tel système pour causer des dommages.

En quoi le piratage d'une ancienne version d'un logiciel est-il problématique pour les particuliers?
Le chantage est la principale menace à laquelle s'expose un particulier en pareil cas: les pirates accèdent de l'extérieur à ses données et les verrouillent, avec pour résultat qu'elles cessent d'être accessibles. Une rançon est exigée en échange du déchiffrement et de la restitution des données. Or bien souvent, il ne se passe rien après le versement de la rançon, et la victime a perdu à la fois son argent et ses données.

Thème «Protéger avec un antivirus»: «C'est comme à la maison: fermez la porte à clé.»

André Duvillard, délégué du Réseau national de sécurité RNS

Les programmes de protection sont entre-temps une évidence – n'est-ce pas?
Hélas non: nous avons plutôt l'impression que les internautes sont toujours moins nombreux à installer un antivirus, ou du moins qu'ils s'en désintéressent par la suite.

Comment les maliciels et les virus s'introduisent-ils dans un système?
L'humain reste le maillon faible: à moins d'avoir protégé son système, on s'expose à y introduire des maliciels et des virus en cliquant sur un lien infecté, ou lors d'un téléchargement imprudent. Le cas échéant, le système risque de fonctionner au ralenti ou de se bloquer. Des données peuvent être volées, ou les escrocs sont susceptibles de prendre le contrôle de votre ordinateur ou smartphone.

Que peut-on faire concrètement?
Faites comme à la maison: fermez la porte d'entrée à clé, afin que personne ne s'introduise chez vous. Dans le cas de l'ordinateur, ce rôle revient à un logiciel de protection, par exemple un antivirus. Il faudrait encore régulièrement s'assurer, lors d'analyses du système, que l'ordinateur n'a pas été infecté. Le site www.S-U-P-E-R.ch offre un bon aperçu des logiciels de protection conçus pour les différents systèmes d'exploitation. Il est également possible et souhaitable de protéger les smartphones.

Thème «Équiper ses accès d'un mot de passe fort»: «Pas besoin de toujours changer de mot de passe.»

Oliver Hirschi, professeur et responsable de la plateforme «eBanking – en toute sécurité!» à la Haute école de Lucerne

À quoi reconnaît-on un bon mot de passe?
Il s'agit d'empêcher autant que possible un pirate de deviner votre mot de passe ou de le trouver en tâtonnant. Par conséquent, plus le mot de passe est long et complexe, et moins il risque d'être découvert.

Comment faire?
Il convient tout d'abord de choisir un mot de passe fort. Nous avons résumé les principales règles à suivre sur le site www.S-U-P-E-R.ch. Ensuite, un mot de passe différent sera utilisé par identifiant (login). Moyennant cette précaution, il est inutile de changer à tout moment de mot de passe, comme on le prétend souvent. Il est encore possible de faire appel à un gestionnaire de mots de passe, dont quelques-uns sont décrits sur le site précité.

Quels sont les risques inhérents aux mots de passe faibles?
La situation peut devenir gênante si, par exemple, des pirates s'emparent du mot de passe de services comprenant des moyens de paiement – de telles informations risquent d'être interceptées et utilisées à mauvais escient. En cas d'intrusion dans vos appareils, des escrocs pourront dérober vos données ou installer des maliciels.

Thème «Réduire»: «Personne n'est à l'abri.»

Chantal Billaud, directrice de la PSC

N'importe qui peut-il être victime d'une cyberfraude?
Absolument, même si la plupart des gens croient encore qu'ils ne se feraient pas piéger. Les victimes de fraude qui s'annoncent chaque jour chez nous ne sont ni naïves ni stupides. Elles sont issues de toutes les classes sociales.

Comment de tels incidents se produisent-ils?
Chacun a des moments de faiblesse, où il est vulnérable et dans le besoin. Il peut s'agir d'un manque de reconnaissance, d'affection et d'intimité, ou de difficultés financières. Les escroqueries tirent toujours parti d'une de ces vulnérabilités. Quand les tentatives de fraude sont réalisées à grande échelle sur Internet, il y a de fortes chances qu'une personne au moins morde à l'hameçon. Moyennant une contrainte temporelle et l'impression que l'offre est limitée, le piège peut se refermer sur la plupart d'entre nous.

Comment y remédier?
Il suffit parfois d'être bien informé: si l'on sait que n'importe quelle information peut être falsifiée dans Internet et que les escroqueries sont monnaie courante sur la toile, on croira peut-être moins facilement tout ce qui vient de là. Par exemple qu'un militaire de carrière américain basé en Afghanistan meurt d'envie de vous épouser. On examinera un profil ou une offre d'un œil plus critique. Les «compétences médiatiques» et la diffusion d'informations aident par conséquent à protéger les gens face aux fraudes.