Arnaques, phishing & Spam

Dans cette page, nous voulons lister quelques arnaques et autres courriels frauduleux parvenus à notre connaissance.

UN SEUL MOT D'ORDRE : MÉFIANCE, MÉFIANCE, MÉFIANCE ! Soyez toujours sur vos gardes et vérifiez tout.

Remarque préliminaire : ce n'est pas parce qu'un courriel vous parvient d'une adresse connue qu'il est parfaitement sûr. Certains virus reprennent votre boîte courriel et envoient à sa liste de favoris leur marchandise toxique !

1. Téléphone. Une première arnaque est de vous téléphoner en se faisant passer pour Microsoft (ou autre) et vous annonçant que votre PC a un virus (ou autre problème) ou que l'on pourrait améliorer ses performances. L'appelant demande à prendre le contrôle de l'ordinateur, ou que vous lui donniez votre (vos) mot(s) de passe. Il peut menacer de bloquer votre ordinateur. REFUSEZ et fermez le téléphone. Soyez très sec s'il insiste. Jamais Microsoft ni aucune autre société sérieuse ne procède comme cela. N'acceptez de contrôle à distance que d'une personne en qui vous avez entièrement confiance et que vous avez vous-même sollicitée pour cela.
Si vous avez déjà cédé à ce chantage, retirez immédiatement la prise Internet de votre PC, fermez le WiFi et modifiez tous vos mots de passe.

Autre arnaque au téléphone : une personne se fait passer pour Visa ou Mastercard et vous annonce qu'une utilisation de votre carte semble frauduleuse. Vous êtes priés de confirmer que c'est le cas. Puis il vous demande le No de sécurité à 3 chiffres au dos de la carte soit-disant pour vérifier qu'elle est bien en votre possession. NE LE DONNEZ PAS ! Dans les minutes qui suivent, il l'utilisera pour effectuer un achat par Internet, et vous aurez beaucoup de peine à vous faire rembourser. Il ne vous demande pas votre No de carte CAR IL L'A DÉJÀ !

2. Phishing (tentative de vous soutirer vos mots de passe ou autre renseignement confidentiel) : Voir des cas récents avec ce lien. Le phishing est une tentative de vous soutirer vos identités d'utilisateur et vos mots de passe avec un courriel du genre "Confirmez vos données / votre compte". NE DONNEZ JAMAIS UN MOT DE PASSE, ni au téléphone ni dans un courriel.
Indices : Expéditeur ne correspond pas (@gmail.com au lieu de @BCV.ch) / courriel dans une langue autre que la langue habituelle de communication de votre banque / Absence de logo / fautes d'orthographe / destinataire(s) non identifié(s) / menaces de fermeture du compte / adresses réelles différentes de celles qui apparaissent.
Précautions : Vérifiez les indices ci-dessus. Vérifiez toujours les adresses réelles qui apparaissent quand on place la souris sur le texte (NE PAS CLIQUER). Allez sur le site indiqué en entrant la référence directement dans votre navigateur, n'utilisez pas les hyperliens.

... et virus : Attention aussi aux virus qui peuvent être cachés dans les pièces attachées (voir ce lien)

ATTENTION AU PHISHING : Lisez notre rubrique "Arnaques, Phishing, Spam, Virus"
J'ai reçu récemment plusieurs courriers électroniques (y compris sur mon smartphone) suspects :

- un message de serviceverification3[at]hotmail.com intitulé CONFIRMATION DE VOTRE COMPTE, où *on me demande entre autres mes mots de passe et question secrète, un courriel de Swisscom <info[at]swisscom.ch> intitulé "Swisscom la mise à jour" qui me demande de cliquer un lien sur un site net78.net, un courrier de Service-client intitulé " Swisscom, la mise à jour" qui me demande de cliquer sur un lien, et deux autres avec zip ou pdf attaché sans aucun texte.*

De la même eau, un courriel de "Service-client <christian.carriere[at]alsatis.net> : *Pour évitez une suspension de votre compte cliquez ici http://serv-info-web-pro.com <http://serv-info-web-pro.com/> et enregistrez vous immédiatement.*

Encore un : de bluewin requirement <mailto:suegillespie[at]zoominternet.net> / to: info[at]mail.com / *Subject: urgent attention / TEXTE : requirment! bluewin account user clean up your account mailbox to avoid account disable. http://bluewinservicec.jimdo.com/*

Et un autre : de Swissonline[at]no-log.org / à : SAV[at]bluewin.ch / Titre : Swisscom La mise à jour / TEXTE : *Pour évitez une suspension de votre compte cliquez ici http://temporairesettings.fr/ et enregistrez vous immédiatement.*

NE REPONDEZ PAS, ne cliquez JAMAIS sur les liens ou les pièces attachées : ce sont typiquement des phishings ! Méfiez-vous en particulier des pièces attachées .zip !

Un de nous s'est fait pirater sa boîte de courrier électronique, qui a envoyé un fichier scan.zip à plusieurs d'entre nous, probablement ceux qui avaient la chance de figurer parmis ses contacts. Comme toujours, n'ouvrez pas cette pièce jointe, mais effacez ce courrier immédiatement.
ATTENTION AUX VIRUS : Le virus très destructeur Rombertik peut causer une perte totale de vos fichiers et programmes. Si vous êtes attrapé, il n'y a pas de réparation. Voyez donc impérativement les moyens de prévention !

ATTENTION AUX RANSOMWARE : L'un de nous a eu le "ransomware" Cryptowall. Celui-ci encrypte vos fichiers et vous demande 500 US$ de rançon pour vous fournir la clé de décryptage. Alors soit vous avez une copie de sécurité récente de vos fichiers, soit vous payez... Il y apparemment une faiblesse : il ne peut crypter que 256 répertoires mais ceux-ci doivent contenir au moins 1 fichier. Faites-vous donc 256 répertoires et sous-répertoires au début de l'alphabet et mettez-y au moins 1 fichier.

ATTENTION AUX FAUX VIRUS sur smartphone Android : Sur mon smartphone Android, en allant sur Internet j'ai reçu une *alerte au virus Tapsnake, mais qui ne venait pas de mon antivirus AVG. Ceci était une fausse alerte, destinée à me faire télécharger une application*. Voir http://androidadvices.com/beware-tapsnake-virus-warning-android-phones/.

En même temps, je reçois un avertissement que je dois mettre à jour le logiciel de l'appareil. Il me *demande mon No et affiche le texte suivant : "Le client, qui a enregistré sur ce site est inscris en temps que participant et souscrit. Le coût est de 5 CHF par SMS, max 3 messages par semaine. Les produits ne sont pas téléchargés conserver vos valables même après déconnexion. Vous pouvez vous désabonner à tout moment. Envoyer STOP OK pour 925. Support : 0848 324689. Accès, la participation et l'utilisation du service est entièrement personnes agées Clive et /ou des personnes qui sont des mineurs admis avec le consentement du représentant légal. Participer à et l'utilisation du service vous avez lu et accepté*

remplissant les conditions/coûts. Vous devez activer l'option dans le téléphone WAP. Les frais sur votre compte seront factures mobile déduits ou de votre solde feeder: Nearly Normal BV, Weegschallstraat 3, 5632 CW Eindhoven, Pays Bas. Pour plus de renseignements, appeler le 0848 123767 ou contactez-nous par email suisse@mob.support. S'il vous plaît lire attentivement les conditions générales qui s'appliquent".

Pas besoin de beaucoup d'explication pour deviner que c'est une arnaque : personne de sérieux n'écrirait un si mauvais français, même pas un logiciel de traduction :-). Seule solution pour s'en sortir (provisoirement) : faire afficher la liste des applications récemment ouvertes et les fermer toutes (ce qui ferme Internet), puis relancer Internet avec une adresse différente (il garde en mémoire la dernière adresse ouverte avec le lien que j'utilisais).

3. Spam On appelle Spam tout courrier électronique publicitaire ou autre reçu sans avoir été sollicité. Il peut s'agir de vous vendre de la poudre à lessive ou de vous inviter à une exposition, voir vous demander un don pour une bonne oeuvre. Ils vous remplissent votre boîte aux lettres électronique et vous prennent du temps pour les examiner et les éliminer. Vous avez gagné à la loterie / Je cherche à faire un transfert / j'ai un cancer / j'ai une affaire à vous proposer ... Voir cas récents avec ce lien.
Vous n'êtes pas assez naïfs pour croire que vous pouvez avoir gagné quelques centaines de milliers de dollars (ou Euros) sans rien avoir fait pour cela , ou que quelqu'un de parfaitement inconnu va vous léguer sa fortune, n'est-ce pas ? Effacez immédiatement ces courriels. Ils sont en général inoffensifs. Mais certains de ces courriels peuvent contenir des virus dans les pièces attachées ou dans des liens Internet.

Les entreprises honnêtes mettent en général en fin de message une possibilité de se désabonner à leurs envois.

Il y a de bons filtres anti-spam qui les dévient vers un dossier ad hoc avec une efficacité qui n'est cependant pas totale. Mais attention, ceux-ci peuvent aussi dévier des courriels acceptables et il vous faut quand même aller voir régulièrement dans ce dossier s'il n'y a pas de bons messages.

On peut normalement établir une liste noire d'expéditeurs dont les messages iront de toutes façons dans ce dossier "Spam" (ou courriers indésirables), et une liste blanche d'expéditeurs dont les messages n'iront de toutes façons pas dans ce dossier.

4. Internet

a. Vous avez sur votre écran Internet des publicités, qui sont en général présentes quel que soit le site visité. Cela est dû à un programme parasite (Sizlsearch, ClearThink, V2-HD ou analogue) qui ouvre automatiquement un site de publicités au démarrage de votre navigateur. Ceci n'est pas dangereux, mais très ennuyeux.

Actions possibles :
- Changez de navigateur : Mozilla Firefox est mieux protégé
- Installez un filtre anti-publicités
- Désinstallez le programme en question (via le Panneau de Configuration, Programmes, Désinstaller un programme).

b. Vous voyez sur une page Internet un message "Votre PC est lent" ou analogue. N'y croyez pas, il n'a rien vérifié et rien vu sur votre PC. Il cherche uniquement à vous vendre un programme correcteur, réel ou bidon.

c. Méfiez-vous des téléchargements de programmes gratuits : c'est le téléchargement qui est gratuit, mais l'utilisation du programme peut fort bien être payante ! Éventuellement, le logiciel en question fait gratuitement le scan de votre disque pour dérecter les imperfections (réelles) mais la license est indispensable pour effectuer la réparation des erreurs !

d. Bien des logiciels gratuits ont une version Pro qui est plus performante, mais payante. Lors de la mise à jour, vous êtes subtilement dirigés vers cette version payante. Cherchez soigneusement la version gratuite si vous ne voulez pas la version payante.

5. Logiciels Potentiellement Indésirables (Potentially Undesirable Programmes)

Quand vous installez ou téléchargez un programme, il arrive qu'un autre programme s'installe en même temps. Evitez ce genre de situation désagréable.

6. Mouchards

Internet regorge de programmes mouchards, qui tracent et enregistrent toutes vos activités. Pour éviter cela, **vous pouvez activer un module complémentaire (dans Outils) : choisissez Extensions et activez Ghostery.** Ensuite, dans les réglages de Ghostery sélectionner le blocage de touts les mouchards. Vous serez étonnée comme moi qu'un simple site comme rtsinfo.ch en comporte 7 et weather.com 12. Le présent site ARNInfo.ch n'en a pas !

Vous pouvez aussi **activer le plugin AdBlock qui vous évite bien des publicités inutiles**.

7. Courriels d'amis en détresse à l'étranger
Vous recevez un courriel d'une personne connue qui vous dit s'être fait voler toutes ses affaires et/ou être à l'hôpital à l'étranger et vous demande de lui avancer une somme d'argent pour payer son retour. Vérifiez 3 fois avant de verser quoi que ce soit. Il est fort probable qu'elle s'est fait pirater la liste de contacts de sa boîte aux lettres électronique.

8. Hoax

Certains plaisantins lancent des chaînes de courriels avec un message du genre "Avertissez tous vos contacts de tel ou tel fait". Ce peut être un enlèvement d'enfant, un virus destructeur ou autre évènement menaçant. Ces arnaques sont inoffensives en principe pour votre ordinateur. Mais d'une part elles génèrent des paniques inutiles et idiotes, et d'autre part elles encombrent Internetde millions de messages inutiles pendant DES ANNEES.

Les sites Internet http://hoaxkiller.com et http://hoaxbuster.com inventorient ces hoax et les analysent. A visiter impérativement si vous avez des doutes. Le hoax ci-dessous y est dûment répertorié !

Exemple

"A lire ci-dessous et transmettre absolument."

Subject: Fw: A transmettre largement..URGENT!

TRANSMETTRE A TOUS TES CONTACTS - URGENT
vérifié sur hoaxkiller...Alerte avérée
ALERTE VIA LA GENDARMERIE
Pour ton ordinateur et le mien, fais circuler cet avis à tes amis, famille, contacts
Dans les prochains jours sois attentif : n'ouvre aucun message avec une archive annexe appelée "Actualisation de Windows live", indépendamment de qui que ce soit qui te l'envoie.
C'est un virus qui brûle tout le disque dur. Ce virus viendra d'une personne connue que tu as dans ta liste d'adresses. C'est pour cela que tu dois envoyer ce message à tous tes contacts.
Si tu reçois le message appelé : "Actualisation de Windows live", même si c'est envoyé par un ami, ne l'ouvre pas et arrête immédiatement ton ordinateur.
C'est le pire virus annoncé par CNN. Il a été classé par Microsoft comme le virus le plus destructeur qui ait existé. Ce virus fut découvert hier après midi par Mc Afee. Il n'y a pas de possibilité de dépannage pour ce genre de virus.
Il détruit simplement le Secteur Zéro du Disque dur. Souviens-toi : si tu l'envoies à tes connaissances cela bénéficiera à nous tous.

Commentaire : semer la panique, se donner l'air officiel avec référence à la gendarmerie, à l'administration, à Microsoft ou à McAfee : voilà des caractéristiques fréquents des hoax.