Info Délits Plus

Avril 2016

Division prévention criminalité

Escroqueries sur Internet

Au vu du nombre de tentatives et de cas avérés d'escroqueries sur Internet, nous nous devons de répéter nos conseils de prudence. Armés d'une inventivité sans limite, les escrocs profitent de toute opportunité pour commettre des tentatives d'escroquerie. Soyez critiques et n'agissez pas dans la précipitation, même si vous recevez des menaces de fermeture de comptes ou des messages urgents. Partagez vos doutes et n'hésitez pas à nous contacter.

Exemples et conseils pratiques

En général, la démarche commence par l'envoi d'un mail au caractère urgent comme le montre ces deux exemples. Nous avons remplacé le nom usurpé d'un établissement financier par un X :

1. « Verified By x » <securite@x.com> a écrit :
Bonjour chèr(e) client(e), Votre Carte Bancaire a été suspendue, car notre système de sécurité a détecté plusieurs échecs de tentatives de changement de votre code de sécurité.
Pour lever cette suspension, CLIQUEZ-ICI : http://www.guimaec.com/upload_histoire//vbv1/realvolition.com/verified%20by%20x/FR-fr/security/vbv-byx/onlineshop/x/france/information/cc/index.html et suivez la procédure indiquée pour mettre à jour vos informations personnelles et nous permettre de vérifier et de valider votre carte à nouveau.

Note: Si ce n'est pas fait dans les 48 heures, nous serons contraints de suspendre votre carte indéfiniment, car elle peut être utilisée à des fins frauduleuses

Nous vous remercions de votre coopération.
Clients Service.
Copyright 1999-2011 Verifedbyx . Tous droits réservés

****

2. Tartempion Pimpin <Tartempionpimpin@onet.eu> a écrit : Bonjour, j'attends urgemment de tes nouvelles pour t'exposer un problème délicat. Contactes-moi par mail, car je suis injoignable sur mon portable.
Cordialement.
M. Tartempion

Que ce soit pour accéder à votre compte en banque ou compte e-mail pour pouvoir envoyer en votre nom des demandes d'aide financière à vos contacts ou simplement avoir des données confidentielles, les buts sont multiples. En revanche, les méthodes sont souvent similaires. En instaurant la confiance, ces escrocs essaient de récupérer vos données et codes d'accès. Via un faux mail de votre banque, de la poste ou de votre fournisseur Internet, les pirates essaient de vous attirer sur des pages qui ressemblent aux originales et vous invitent à vous identifier avec votre login et votre mot de passe. Dans certains cas, ces liens téléchargent un mouchard sur votre ordinateur.

Aucun service officiel, établissement bancaire, postal ou autre prestataire de messagerie, ne vous demandera jamais vos codes sauf sur les sites sécurisés de paiement.

- Conseils !
  - Ne donnez jamais suite à ce genre de message, ne répondez pas, même si c'est pour poser une question !
  - D'une façon générale, à part les systèmes de paiement sécurisé, ne donnez jamais des renseignements personnels et bancaires par Internet !
  - Ne cliquez pas sur un lien qui vous est proposé dans un email de provenance inconnue ou douteuse !
  - Pour vous rendre sur le site de votre banque ou poste, passez par un moteur de recherches comme Google par exemple !
  - Si vous êtes sollicités par une œuvre de bienfaisance par messagerie et que vous voulez donner de l'argent, faites une recherche pour savoir si cette œuvre de bienfaisance existe réellement et a un site officiel. Ne faites pas votre versement depuis le message que vous avez reçu initialement !

Ransomware

Il s'agit d'un virus qui crypte vos disques durs. Le pirate vous demande ensuite de payer une rançon pour débloquer les systèmes. Ce virus s'installe en ouvrant un fichier attaché, que ce soit un **.exe**, un fichier **.doc, une photo** ou **un lien dans un fichier pdf.**

- Conseils !
  - N'ouvrez jamais un fichier attaché à un mail dont vous ne connaissez pas la provenance ou qui semble douteux !
  - Sauvez vos données importantes sur des disques durs **qui ne sont pas branchés en permanence sur votre ordinateur !** Les fichiers sauvés en synchronisation permanente sur un disque dur ou sur le cloud peuvent être attaqués.

Arnaques au logement

En cette période de l'année où les offres pour des appartements foisonnent sur les sites spécialisés, certaines sont aussi alléchantes que malhonnêtes.

L'escroquerie au logement consiste généralement en la diffusion d'une annonce, trop belle pour être vraie, sur différents sites Internet spécialisés. Lors du premier contact avec le prétendu propriétaire ou représentant officiel, ce dernier explique que le logement est inoccupé et disponible de suite, mais qu'il ne peut pas être présent pour une visite en raison d'un déplacement professionnel. Il demande tout de même par retour de courrier électronique, une copie des pièces d'identité, des attestations de

revenus ainsi que d'autres informations personnelles. En outre, il est possible qu'ils mentionnent une tierce personne, un agent d'affaires ou une société de location qui s'occuperait de gérer toutes les formalités en son absence. Puis, il demande un versement via une société de transfert de fonds en assurant qu'à réception de celui-ci, il enverra les clefs du logement en question.

- Conseils !
  - Renoncez à toute location lorsqu'il est demandé au potentiel « locataire » de verser des arrhes à l'étranger via une société de transfert de fonds !
  - Ne transmettez pas de copie de pièce d'identité ou numéro de compte bancaire via Internet. Ces coordonnées peuvent servir aux escrocs pour commettre d'autres méfaits !
  - Soyez critiques si l'offre vous paraît trop alléchante (rapport qualité/prix) !
  - Lors des échanges avec votre interlocuteur, demandez-lui ses coordonnées (adresse professionnelle voire privée, celle de son représentant, No de tél, …) et vérifiez-les sur Internet !
  - Ne payez rien avant d'avoir visité l'appartement que vous allez louer !
  - Ne versez pas d'argent par le biais d'une société de transfert de fonds !
  - Soyez attentifs à la terminologie utilisée ainsi qu'aux fautes d'orthographe et de syntaxe dans l'annonce ou lors d'échanges écrits !

Sources : PCV, Prévention suisse de la criminalité

Adresses web utiles

http://votrepolice.ch/fr/criminalite/item/arnaques-sur-internet-comment-se-proteger

http://votrepolice.ch/fr/criminalite/item/arnaques-a-la-location-d-appartements

https://www.melani.admin.ch/melani/fr/home.html

Pour obtenir plus d'information ou des conseils, contactez les gérants de sécurité :

Arrdt Est vaudois : Adj Borloz Christian, 021 557 88 05
Arrdt La Côte : Sgtm Christian Lambiel, 021 557 44 66
Arrdt Nord vaudois Ouest : Adj Mermod Willy, 024 557 70 24
Arrdt Nord vaudois Est : Adj Perruchoud Gilles, 024 557 70 07
Arrdt Lausanne : Ipa Bourquenoud Christian, 021 644 82 77