NEWSLETTER DU CTRC DE FRANCHE-COMTÉ

Le 8 Septembre 2021

Vol de données personnelles : les 5 principales techniques d'arnaque

La récolte de données personnelles se fait de plus en plus de manière légale, à travers les cookies et autres. Mais elle se fait aussi de plus en plus de manière frauduleuse.

Présentation des 5 principales techniques utilisées pour accéder et récolter vos données par des personnes mal intentionnées.

Le Phishing : le mode opératoire de cette arnaque consiste à vous adresser par mail, SMS ou messagerie un remboursement d'argent ou le blocage de votre compte bancaire. Pour ce faire, on vous demande de remplir un formulaire.
L'objectif est d'obtenir vos données personnelles et vos coordonnées bancaires afin d'en usage et de vous voler de l'argent. Bien souvent, les personnes à l'origine de cette pratique usurpent l'identité d'administrations publiques et d'entreprises privées (telles que la CPAM ou les banques).

Comment s'en prémunir ? Ne surtout pas céder à l'appât du gain ou à la panique ! Jamais une administration ou une entreprise vous demandera vos données personnelles. Dans le doute, contactez directement l'entité soit-disant à l'origine du mail ou autre à partir de l'adresse mail ou du numéro de téléphone mentionnés son site internet officiel.

Le SIM Swapping : cette technique consiste à recueillir votre numéro de téléphone via les réseaux sociaux ou bien le piratage de votre boîte mail afin de récupérer les SMS de sécurité dans le but de valider des paiements en ligne frauduleux ou accéder à votre compte bancaire.

Comment s'en prémunir ? Si votre carte SIM semble ne plus fonctionner et que votre « opérateur » vous demande de lui communiquer un code reçu par SMS pour réactiver votre ligne, surtout ne le faites pas ! Il s'agit vraisemblablement d'une fraude.
Pour plus de sûreté et en cas de doute, prenez attache auprès de votre operateur.

Le Trojan bancaire (ou cheval de Troie) : cela consiste à voler vos identifiants d'accès à votre compte bancaire en vous adressant un message avec une pièce jointe, ou un lien, qui vous invite à mettre à jour votre navigateur internet ou encore à télécharger une application.

C.T.R.C Franche-Comté
Centre Technique Régional de la Consommation

Union d'associations de consommateurs

Bon à savoir

Le site internet du CTRC-FC a fait peau neuve ! Nous vous invitons à aller le consulter à l'adresse suivante :

http://ctrcfrz.cluster027.hosting.ovh.net/

CTRC-FC

8 rue des Vielles Perrières

25000 BESANÇON

Tel :03 81 83 46 85

Mail : ctrc.fc@wanadoo.fr

Comment s'en prémunir ? Ne téléchargez rien de ce qui paraît « louche ». Veillez à installer sur vos ordinateur et mobile une suite de sécurité capable de détecter ce type de programme pour être alerté en temps réel.

Le Ransomware : ce mode opératoire a pour but de chiffrer et rendre inaccessibles tous vos fichiers contenus dans votre ordinateur via un programme installé à votre insu à l'aide d'un lien frauduleux ou d'un site internet corrompu.
L'objectif est de vous demander de payer une certaine somme pour que vous puissiez à nouveau accéder à vos fichiers.

Comment s'en prémunir ? Si votre ordinateur est infecté, surtout ne payez pas la somme réclamée et déconnectez votre ordinateur d'internet. Déposez plainte et contactez les experts en sécurité informatique que le site Cybermalveillance.gouv.fr.

Le faux dépannage informatique : Un SMS ou un mail vous informe que vous risquez de perdre toutes vos données en raison d'un problème technique. Bien souvent, le SMS ou le mail contient le numéro d'un support technique à joindre pour vous dépanner. Le but est que vous contactiez ce numéro et qu'un faux dépannage vous soit facturé.

Comment s'en prémunir ? Ne composez jamais le numéro mentionné. Redémarrez et nettoyez votre ordinateur.

Quelques chiffres
En 2020, ce sont près de 105 000 personnes qui se sont rendues sur la plateforme Cybermalveillance.gouv.fr pour trouver une assistance technique et informatique suite à un acte frauduleux pratiqué sur leur ordinateur ou leur mobile. Avec 17% des recherches d'assistance, l'Hameçonnage arrive en tête suivi par le piratage de compte en ligne à hauteur de 12%. (Chiffres site Cybersécurité).

Copie carte d'identité
Enfin, lorsqu'une pièce d'identité vous est demandée pour telle ou telle transaction veillez à bien la barrer comme le modèle ci-dessous, afin que personne ne puisse usurper votre identité et effectuer des actions ou transactions à partir de votre identité volée. Veillez à notez sur la copie de votre CNI le nom de la personne ou de la société à qui vous remettez cette copie.

La vigilance est de mise à tous les niveaux, et comme dit le dicton « Mieux vaut prévenir que guérir ! »