Gendarmerie Nationale

Éviter les arnaques sur Internet

Les « pirates » ne manquent pas d'imagination pour piéger les internautes. Quelques notions simples sont donc prescrites pour surfer sereinement.

Protéger son ordinateur

Installer un pare-feu ou un antivirus et les mettre à jours.

Installer des logiciels de nettoyage PC et les lancer régulièrement :

Exemples de logiciels gratuits : (liste non exhaustive)

- Ccleaner : nettoyer les traces de navigation sur Internet et les fichiers-système inutiles. ...
- AdwCleaner : se débarrasser des logiciels indésirables et des programmes publicitaires. ...
- Malwarebytes Anti-Malware : éradiquer les programmes malveillants. ...

Ne jamais conserver sur des fichiers de son ordinateur ou boites de courrier électronique des codes d'accès, mots de passe.

Essayer d'utiliser des mots de passe compliqués. Il est préférable de mélanger chiffres et lettres (Majuscules et minuscules) + des signes « / + * ... » .

Escroquerie sous Windows – L'ordinateur est-il vraiment bloqué ?

Cet affichage peut apparaître après l'allumage de l'ordinateur

NE JAMAIS APPELER LE NUMÉRO AFFICHÉ ---- ETEINDRE LE PC ….. LE RALLUMER

NE JAMAIS CONTACTER LE NUMÉRO… COMME INDIQUÉ

L'escroquerie au coupon « P.C.S, Transcash, Toneo, Neosurf… »

Le succès de cette arnaque repose sur sa simplicité : aucun compte à ouvrir, aucun site sur lequel s'inscrire, la victime n'a qu'à se rendre en bureau de tabac pour acheter une recharge PCS Mastercard, Transcash, Toneo ou Neosurf.

Il s'agit d'une sorte de ticket de caisse sur lequel figure un code, qui permet à celui qui le possède de récupérer l'argent crédité. **Il est d'ailleurs précisé que le code ne doit en aucun cas être communiqué à un tiers**… *Même et surtout sur des sites de vérification, pour la simple et bonne raison que 100% des sites de vérification sont des arnaques ! Pas 99% ou 99,5%... Mais bien 100% ! Certains de ces sites se payent même le luxe de faire des annonces sur Google !*

En plus d'un prix trop alléchant, vous remarquerez que le vendeur ne veut traiter QUE par email. Il pourra prétexter des problèmes de téléphone, et fera en sorte que la transaction se fasse très vite, vous parlant par exemple de nombreux acheteurs intéressés. Inutile de préciser que c'est faux.

Qu'est-ce que la carte P.C.S ?

La carte prépayée PCS (*Prepaid Cash Services* **) TRANSCASH, TONEO, NEOSURF etc.…** est une carte de paiement et de retrait sans compte bancaire et sans engagement **(achetée et détenue par l'escro).** Elle est utilisée pour payer et retirer de l'argent sur l'ensemble du réseau.

Elle peut être ré-alimentée par coupons recharges dans plus de 32 000 points de vente en France

« Une des clés du succès des cartes prépayées est incontestablement la possibilité de les créditer à l'aide de tickets recharges achetés en espèces dans les commerces de proximité. Le principe est simple Vous versez 50€, 100€ ou 250€ en espèces à un revendeur afin que celui-ci vous imprime un ticket "recharge" (aussi appelé coupon) de valeur équivalente. Ce ticket contient un code secret confidentiel qui vous permet, une fois saisi dans l'espace dédié à la gestion de votre carte prépayée, de créditer cette dernière du montant correspondant. S'agissant de monnaie électronique, ces coupons sont comme des espèces et il est donc possible de se les faire dérober si on est négligeant. Si bien que certains malfaiteurs ont mis en place des techniques sophistiquées et bien rôdées pour vous convaincre de leur communiquer les codes secrets de vos tickets. Petit point sur les choses indispensables à savoir pour éviter les pièges tendus par ces cyber-brigands. »

L' opération est anonyme et irréversible. Il est impossible pour les victimes de se faire rembourser ou de retrouver les escrocs (installés très souvent à l'étranger)

Dans tous les cas, ne payez jamais un inconnu avec une recharge. …. JAMAIS.
Votre banque ne vous remboursera pas, le paiement étant volontaire.

Les escrocs vous manipuleront, vous faisant croire qu'il est plus sécurisé de payer par ce biais que via **des plateformes pourtant reconnues, comme Paypal ou Paylib, pour ne citer qu'elles.**

Différents cas de figure se présentent alors :

- Le vendeur joue « la confiance », et vous demande le code avant envoi du colis. Que vous ne verrez jamais.

- Le vendeur vous demande de vérifier la « validité » du coupon, en entrant le code sur un site internet dont il vous aura donné l'adresse. En entrant le code, vous ne ferez que créditer le compte de l'escroc. Il n'existe aucun code de vérification, et ces sites sont créés par les escrocs eux même.

- Variante : le vendeur vous demande d'entrer les codes sur un site, qui d'après lui conservera l'argent jusqu'à ce que vous confirmiez la réception du colis… que vous ne verrez jamais.

- Variante : une de vos connaissances **vous contacte par mail de France** ou de l'étranger **(**Elle a été victime d'un piratage de sa boîte e-mail. L'usurpateur a envoyé un message à tous les contacts en se faisant passer pour la personne en question**)**
***** Elle a été victime **d'une agression ou d'un vol** et elle aurait **perdu tous ces papiers & moyens de paiements.**
***** Elle n'a désormais **plus que vous pour l'aider à rejoindre son domicile.**
***** Elle vous demande de **vous rendre dans un bureau de tabac ; d'acheter des coupons « PCS » (** ou mandat cash western union **) pour une certaine valeur et de lui envoyer les codes par mails.**

L'escroquerie ; Fraude à la « nigériane »

La fraude nigériane est une sollicitation par courriel, à l'origine en provenance du Nigéria, un pays d'Afrique, promettant une importante somme d'argent en échange d'une aide financière. Cette arnaque a pour but d'user de la crédulité et de l'inexpérience des utilisateurs de messageries électroniques (courriels) pour leur soutirer de l'argent.

Vous recevez un courriel d'une personne que vous ne connaissez pas, se disant d'origine nigériane et vous demandant de l'aider. La fraude est bien orchestrée, il vous explique qu'il possède de l'argent et vous fait part de son besoin de le transférer rapidement sur votre compte en échange de quoi il vous offre un pourcentage de cette somme.

L'objectif de cette escroquerie est d'**amener la victime à accepter de verser une participation financière pour régler des soit-disant frais de dossiers**, payer des intermédiaires...etc, avant que le transfert soit effectif. Bien entendu, cette dernière opération ne sera jamais réalisée.

L'escroquerie via le « phishing » (hameçonnage ou filoutage)

Le principe du phishing consiste à récupérer des données personnelles sur internet. Le moyen utilisé est l'usurpation d'identité, adaptée au support numérique.

L'escroquerie repose le plus fréquemment sur la contrefaçon d'un site internet (celui d'une banque, d'un marchand en ligne ou d'une administration). L'adresse URL du lien comprise dans le mail est également « masquée ou maquillée » afin de paraître authentique.

Des mails à connotation alarmiste (« Votre compte va expirer », « Vous venez d'effectuer un achat », etc.) ou d'autres alléguant d'un prétendu remboursement en faveur de l'internaute sont ensuite massivement adressés.

Ils semblent provenir d'une source de confiance (banque, CAF, opérateurs de téléphonie, impôts, sites de VAD, etc.) et invitent à se rendre sur une page de formulaire à celle de l'organisme évoqué sur laquelle seront demandées et récupérées des données personnelles, souvent à caractère financier (coordonnées bancaires).

► Les mails constituant des tentatives de phishing sont très généralement anonymes (« Cher client », « Madame, Monsieur », etc.).

► **Les centres des impôts n'envoient jamais ce genre de courriel ni les banques et organismes sociaux (CAF, mutuelles, etc.)**. Ils ne passent jamais par un courrier électronique pour demander à leurs clients de saisir leurs informations personnelles.

► **Ne pas cliquer sur les liens contenus dans les courriers électroniques** : les liens affichés dans les courriers électroniques peuvent en réalité diriger les internautes vers des sites frauduleux.

► Préférer se rendre directement sur le site de l'organisme en question en tapant soi-même l'adresse de celui-ci dans le navigateur.

► Être vigilant lorsqu'un courriel demande des actions urgentes.

► **Ne jamais répondre ou transférer ces courriels.**

► Supprimer le message de votre boite aux lettres électronique.

► En cas de doute ou de problème, prendre contact rapidement avec son agence bancaire ou l'organisme qui aurait envoyé ce courriel.

► D'une manière générale, être vigilant et faire preuve de bon sens : ne pas croire que ce qui vient d'internet est forcément vrai.

Les appels téléphoniques par de faux agents des services fraudes de banques

Vous êtes invité(e) encore et toujours, à la plus grande prudence en cas d'appel téléphonique de personnes se faisant passer pour un service de la banque

D'autres tentatives de fraudes peuvent également être réalisées par e-mail ou par SMS.

Des fraudeurs se font passer pour des collaborateurs de banque et tentent, par exemple, de vous alarmer en vous signalant un paiement en attente sur votre compte ou prétextant la détection d'opérations de fraudes en cours.

Toutes ces pratiques sont destinées à vous amener à communiquer vos codes d'accès à votre espace sécurisé sur Internet, à récupérer vos données de carte bancaire (numéros de carte, date de fin de validité, cryptogramme) **ou le code d'authentification permettant de valider un achat sur internet ou de faire des virements.**

Soyez vraiment vigilant(e) si vous êtes confronté(e) à ce type de demande, n'y répondez en aucun cas et contactez immédiatement votre conseiller.

Vous avez déjà communiqué ce type d'informations ?

Il vous est recommandé de faire opposition sans attendre sur votre carte bancaire et de modifier vos mots de passe.

N'hésitez pas à contacter votre agence, votre conseiller se tient à votre disposition pour tout renseignement complémentaire.

SE PREMUNIR CONTRE LA FRAUDE : LES 5 CHOSES QUE VOTRE BANQUE **NE VOUS DEMANDERA JAMAIS**

1 - De communiquer ou modifier vos données personnelles
2 - De communiquer votre identifiant et votre mot de passe pour accéder à votre espace personnel de banque en ligne
3 - De communiquer des éléments liés à votre carte bancaire *(numéro, date d'expiration…)*
4 - De communiquer des éléments relatifs à vos moyens d'authentification *(Secur'Pass, code généré par SMS)*
5 - D'annuler un paiement par carte bancaire présenté comme étant frauduleux ou de valider un paiement

L'utilisation & la fraude via les organismes de transferts d'argents

Souvent utilisée par les fraudeurs du Web, il convient d'inciter les éventuels utilisateurs de ces organismes à la prudence. Il s'agit du circuit financier le plus utilisé par les « pirates » sur internet ; surtout dans les pays d'Afrique d'où partent la plupart des arnaques.

Cette société américaine n'est pas une banque mais un organisme financier spécialisé dans les transferts d'argent en espèces **de particulier à particulier**.

Les fraudeurs profitent des avantages de ce système qui repose essentiellement sur la rapidité des transactions puisque les fonds sont envoyés puis retirés en quelques minutes.

Comment lutter contre la fraude ?

- Connaître personnellement la personne à qui vous envoyez l'argent (et non un inconnu ou une personne rencontrée sur Internet)
- Ne jamais effectuer un transfert d'argent pour un achat.

- Ne jamais utiliser cette transaction pour :

- percevoir un supposé gain que vous auriez gagné
- une opportunité professionnelle
- louer une propriété, un appartement

Exemples d'organismes les plus utilisés par les fraudeurs :

**** WESTERN UNION***
**** RIA MONEY TRANSFERT*** *(envoyer facilement de l'argent à des proches vivant à l'étranger ou de manière urgente)*
**** MONEYGRAM***
**** VP Europe*****,**
**** REMITLY***
**** MONISNAP*** *(envoyer de l'argent dans les pays d'Afrique Maroc, Tunisie, Sénégal, Cameroun)*

L'escroquerie à la « petite annonce »

Sites de petites annonces

- Éviter d'acheter sur un site de petites annonces sans aller voir le produit ou le chercher en personne. Recentrer vos recherches dans la région. Au-delà, vous accentuez le risque de ne jamais recevoir le paiement ou de ne pas pouvoir l'encaisser faute de provisions. Il peut arriver que le produit n'arrive jamais ; qu'il soit différent ou inutilisable.

- Méfiez-vous des offres trop alléchantes. Prenez votre temps, n'agissez jamais dans l'urgence.

- N'envoyez jamais vos coordonnées de carte bancaire ou vos coupons de cartes prépayées par email.

- N'expédiez jamais un colis avant que l'argent soit bien viré sur votre compte bancaire ou votre compte PAYPAL.

- Recherchez l'émail de votre interlocuteur sur un moteur de recherche pour vérifier son identité ou s'il n'est pas connu défavorablement.

- Lorsque vous publiez une petite annonce, masquez les informations qui pourraient être utilisées pour usurper votre identité ;

Escroquerie avec demande de virement

Si vous répondez à une annonce sur un site de ventes entre particuliers, attention aux demandes de versements du montant de la transaction à partir de RIB fourni par le vendeur.
RIB frauduleux commençant par : **FR76 2183 3000 0100 xxxxxxxx**

Ces références proviennent de l'établissement de paiements et monnaies électroniques « ***PREPAID FINANCIAL SERVICES LTD*** » qui a certes, une agence à PARIS mais les fonds déposés sont immédiatement transférés à l'étranger.

L'escroquerie du « chantage à la WEBCAM »

Les utilisateurs victimes d'arnaques au chantage à la webcam prétendue piratée reçoivent un message d'un inconnu qui se présente comme un pirate informatique (« hacker »). Ce prétendu « pirate » prétend avoir pris le contrôle de l'ordinateur de sa victime suite à la consultation d'un site pornographique. Le cybercriminel annonce alors avoir des vidéos compromettantes de la victime faites avec sa webcam. Il menace de les publier à ses contacts personnels, ou même professionnels, si la victime ne lui paie pas une rançon. Cette rançon, qui va de quelques

centaines à plusieurs milliers d'euros, est réclamée dans une monnaie virtuelle (généralement en Bitcoin).

Pour effrayer encore plus la victime, les cybercriminels vont parfois jusqu'à écrire à la victime avec sa propre adresse mail, afin de lui faire croire qu'ils en ont réellement pris le contrôle de son compte.

Dans certaines campagnes, les cybercriminels vont jusqu'à dévoiler à la victime un de ses mots de passe pour lui faire croire qu'ils ont bien pris le contrôle de son ordinateur.

Ces messages de chantage sont parfois écrits en anglais, mais ciblent également de plus en plus souvent les victimes dans leur langue natale. On constate une augmentation de messages écrits dans un français plus ou moins correct.

Ces arnaques au chantage à la webcam prétendue piratée s'inspirent des chantages à la webcam ciblés, également appelés « sextorsion » pour effrayer les victimes. Mais il s'agit ici de messages envoyés en masse par les cybercriminels. Dans les cas réels de sextorsion ciblée, la victime « connaît » son maître chanteur auquel elle a fourni des images ou vidéos compromettantes de son plein gré après avoir été abusée.

Faut-il avoir peur ?

La réponse est simple : **non !** Car il s'agit d'une simple arnaque qui vise à escroquer des victimes crédules en leur faisant peur.

En premier lieu et si vous y réfléchissez bien, vous n'avez sans doute rien à vous reprocher de compromettant. Ensuite, si le « piratage » annoncé par les cybercriminels n'est en théorie pas impossible à réaliser, en pratique, il reste assez complexe techniquement et surtout long à mettre en œuvre. Comme les escrocs ciblent leurs victimes par milliers, on peut donc en déduire qu'ils n'auraient matériellement pas le temps de réaliser ce qu'ils affirment avoir fait.

On peut également noter que de nombreux internautes qui ont reçu ce type de message n'avaient tout simplement pas de webcam, ou que leur adresse de messagerie usurpée ou le mot de passe dévoilé n'étaient plus utilisés depuis plusieurs années.

Enfin, si de très nombreux cas de réception de ces messages de chantage sont rapportés, aucun cas n'a jamais été signalé jusqu'à présent de victimes qui auraient vu les cybercriminels mettre leurs menaces à exécution.

Tous ces éléments tendent à démontrer que ces messages ne sont que des tentatives d'arnaques au chantage à la webcam prétendue piratée . **Autrement dit, si vous recevez un tel message de chantage et que vous ne payez pas, il ne se passera certainement rien de plus.**

Ces messages constituent une simple intimidation et ne présentent aucun risque de sécurité. Ils ne contiennent pas de pièce jointe ou de lien cliquable. Il convient de simplement de les détruire.

Faux sites administratifs, attention aux arnaques !

Ces sites n'hésitent pas à tromper le consommateur **en prenant l'apparence de sites officiels** : reproduction à l'identique de la charte graphique du site, usage des couleurs bleu-blanc-rouge, référence à des ministères, référencement en tête des moteurs de recherche.

Bon à savoir

Pour éviter toute confusion, vérifier l'adresse Internet (URL) du site :
les URL de l'administration française se terminent invariablement par "gouv.fr " ou ".fr" et jamais par ".gouv.org" ou ".gouv.com " ou "-gouv "

Rappels sur les paiements en ligne !

Aucune entreprise, établissement bancaire ou institution ne vous demandera de régler une somme par le biais d'un mail**. Ne cliquer jamais sur un lien** qui vous transférera sur un site frauduleux

Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur.

À savoir :
Pour la sécurité de vos transactions, gardez secret le cryptogramme visuel (CVV) de votre carte bancaire. Cet identifiant est nécessaire pour réaliser des achats sur internet. Il ne vous sera jamais demandé par les forces de l'ordre ; ni par les établissements bancaires.

N'achetez pas n'importe où

- Achetez sur des sites connus – si ce n'est pas le cas :
* tapez le nom du site sur un **moteur de recherche** (afin de voir s'il n'existe pas de traces d'arnaques). * vérifiez la fiabilité du site web à partir de **« franceverif.fr »**

- Ne jamais acheter en répondant à un mail ; y compris pour une marque connue car les cybercriminels imitent parfaitement les pages de sites institutionnels. Mieux vaut aller directement sur le site concerné, mais ne payez jamais après avoir cliqué sur un lien.

- Ne répondez jamais à un courriel vous demandant des informations personnelles ou vos numéros de carte bancaire ; même s'il semble émis par un de vos fournisseurs (banque, téléphone, internet, administration, etc)

Vous ne gagnez jamais

- Personne ne vous annoncera que vous avez gagné à une loterie ou à un jeu-concours par mail. Si vous recevez un tel mail, inutile de cliquer c'est une arnaque. Vous risquez en outre, de faire entrer un virus dans votre système.

- Aucune entreprise ou institution ne vous demandera de régler une somme par le biais d'un mail. Ne cliquer jamais sur un lien qui vous transférera sur un site frauduleux.

► PERCEV@L : Simplifiez vos démarches en cas de fraude à la carte bancaire sur internet

En utilisant le téléservice percev@l, vous êtes guidés au travers d'une démarche simple de signalement aux forces de l'ordre sur internet, sans avoir à vous déplacer.

Vous découvrez un usage frauduleux de votre carte bancaire (transaction dont vous n'êtes pas à l'origine) ; **alors que vous êtes toujours en possession de la carte,** prévenez votre banque pour provoquer l'opposition – 0 892 705 705 (n° interbancaire 7/7 et 24/24).

Effectuez un signalement sur internet grâce à la plateforme PERCEV@L via le site officiel de l'administration **« www.service-public.fr »** puis saisir **« percev@l »** ou **« fraude carte bancaire ».** Vous gardez le droit de déposer plainte ultérieurement. Remplissez ensuite le formulaire. Une fois renseigné des éléments utiles, Percev@l transmet un récépissé.

Demandez le remboursement des opérations auprès de votre banque en joignant le récépissé transmis par la plateforme Percev@l.

Les informations saisies sont rassemblées et analysées par des officiers de police judiciaire, en vue d'identifier les auteurs d'appropriations frauduleuses/recels de numéros de cartes bancaires. Vous êtes susceptible d'être contacté si les faits entrent dans le cadre d'une enquête.

THESEE : La plainte en ligne pour les victimes d'e-escroqueries

En utilisant le téléservice « THESEE » vous serez guidés au travers d'une démarche simple de dépôt de plainte en ligne. Les informations que vous communiquerez seront analysées et recoupées par des enquêteurs de la police judiciaire qui mèneront l'enquête. Elles contribueront à une recherche plus efficace des auteurs.

Le téléservice Thésée a été officialisé par un arrêté du 26 juin 2020 publié au Journal officiel du 30 juin 2020. **Sa date d'entrée en vigueur n'est toutefois pas encore connue.**

- Votre adresse courriel ou votre profil de réseau social a été piraté et de l'argent a été demandé à vos contacts en votre nom

- Vous avez été escroqué(e) par un faux acheteur suite à la vente d'un produit en ligne sur un site de petites annonces

- Vous avez été escroqué(e) par un faux vendeur suite à l'achat d'un produit en ligne sur un site de petites annonces

- Vous avez été escroqué(e) à l'occasion d'une démarche pour louer un bien immobilier en ligne

- Vous avez été escroqué(e) lors d'un achat sur un site de vente en ligne frauduleux

Les fichiers de votre ordinateur, tablette ou téléphone mobile ont été cryptés et une rançon vous est demandée. (RANSOMWARE)

- Vous faites l'objet de menaces en ligne de diffusion d'images portant atteinte à votre honneur

- Lors d'une relation en ligne, vous avez été incité(e) par des moyens frauduleux à verser de l'argent. (Escroquerie aux sentiments)

Comment déposer plainte ?

- Je vais sur internet : www.service-public.fr » rubrique « Arnaque sur internet »
- Je me laisse guider pour personnaliser ma démarche
- Je m'identifie grâce à « FranceConnect » et ses fournisseurs d'identité (Impôts, Ameli, La poste, etc)
- Je rempli mon formulaire
- Je reçois ma plainte dans mon espace personnel.