Arnaques et Précautions

Volume 1

Ou comment naviguer sur Internet avec prudence

Aux éditions du Club ICPF

Par Michel CHAIGNAUD

Introduction

Internet est une formidable source d'informations, d'échanges, d'activités diverses et variées, d'achats, de ventes. Internet est aussi une méthode pour faciliter les relations, résoudre des difficultés, ou plus simplement effectuer ses démarches administratives avec l'ensemble du service publique (administration fiscale, carte grise, caisse d'assurance maladie, etc.) ou des services privés (banques, les mutuelles de santé, assurances, fournisseurs d'énergie, etc.).

Mais, comme dans toute organisation, il y a le bon côté, mais aussi le mauvais côté. Ce mauvais côté, c'est celui des profiteurs, des arnaqueurs et autres malfrats.

L'inconvénient, avec Internet, c'est que ces personnes malfaisantes se cachent derrière leurs écrans. Elles n'agissent pas au vu et au su de tout le monde, mais depuis des sites qui peuvent être dans d'autres lieux, d'autres pays, d'autres continents que le nôtre.

Il est par conséquent difficile, pour les services en ayant la charge, de traquer ces personnes et d'en démanteler les réseaux.

Nous allons donc, dans ce livret, de voir comment s'en prémunir au mieux et quels sont les moyens mis à disposition par l'Etat pour signaler ces agissements.

Il faut savoir que la fraude et l'arnaque, sur Internet, peuvent mettre à mal les finances de tout un chacun si l'on n'y prend garde.

Il ne faut pas, non plus, que cela empêche les honnêtes citoyens et utilisateurs de ce formidable outil, de ne plus s'en servir, ce serait bien dommage au regard de ce que cela peut apporter.

Dans un premier temps, nous allons voir quelles sont les types d'arnaques et fraudes, puis comment faire pour éviter de se faire piéger.

Mais avant de décrire les différents types de fraudes, il faut d'abord définir ce que sont les données sensibles.

Données sensibles

Mais d'abord, qu'est-ce que des données sensibles ?

Les données sensibles sont des informations qui peuvent être utilisées par des personnes malveillantes dans le but de s'en servir pour, dans la pluparts des cas, de soutirer de l'argent de manière illégale.

Les premières données sensibles sont :

- Nom
- Prénom
- Date de naissance prénom
- Adresse
- Numéro de téléphone.

Ces données sont forcément laissées sur vos espaces personnels. Toutefois, leur utilisation frauduleuse reste limitée.

Les données beaucoup plus sensibles sont :

- Vos coordonnées bancaires
- Votre numéro de sécurité sociale
- Les informations de votre permis de conduire
- La carte grise de votre véhicule
- Carte d'identité
- Mots de passe

Ces données peuvent être utilisées pour faire des achats sur Internet, dans le cas d'usurpation d'identité, d'usurpation de l'immatriculation, etc.

Il apparait donc évident qu'il va falloir protéger au mieux ces données.

Types d'arnaques et fraudes

Il existe, bien sûr, plusieurs types d'arnaques et de fraudes. Nous allons en décrire un certain nombre, sachant que nous en découvrons de nouvelles régulièrement, et que les malfrats ont toujours un coup d'avance sur ceux qui les traquent.

Il existe trois endroits particulièrement vulnérables pour les tentatives de fraude.

Le premier est votre navigateur Internet, quel qu'il soit. Le deuxième, les supports de stockage de vos données (disque dur, clé usb, etc.) et le dernier la boite mail.

1 – Disque dur :

Le disque dur est l'endroit le plus aisé pour stocker vos données, et ce quelques soient ces données (photos, documents, relevés de compte, avis d'imposition, etc.).

Si certains documents ne présentent pas de danger particulier en cas de piratage, d'autres, tels que des copies du permis de conduire, carte d'identité, carte vitale, etc. Ces copies sont souvent réalisées pour permettre de les refaire plus facilement en cas de perte ou de vol.

Il en est de même concernant les mots de passe d'accès à vos espaces personnels. Il est très tentant de créer un fichier contenant ces mots de passe. Mais en cas de piratage de votre ordinateur, votre pirate aura alors accès à tous vos espaces sécurisés, un vrai bonheur pour lui.

2 – Navigateur :

Il existe deux types de fraudes assez répandues via le navigateur :

A – Fraude par les données sensibles

Les tentatives de fraudes et arnaques via le navigateur se font principalement sur les sites pour lesquels vous avez des données sensibles tels que Les fraudeurs vont donc essayer de pénétrer vos espaces personnels (bancaires, les impôts, vos fournisseurs d'énergie, les sites marchands, etc.) pour récupérer vos données, les données bancaires étant particulièrement visées.

Il est donc évident qu'il ne faut pas faciliter l'accès à vos espaces personnels et :

Qu'il ne faut donc jamais enregistrer vos identifiants et mots de passe dans votre navigateur.

B – Fraude par le biais de sites d'aide

Ce type de fraude se fait au travers de sites non officiels qui ressemblent, parfois de très près, a des sites officiels publics ou privés.

Prenons un exemple :

Vous souhaitez renouveler votre carte d'identité. Vous allez donc voir sur Internet quels documents sont à fournir pour cette opération.

Il est fort probable que, dans votre recherche, vous tombiez sur un site qui vous propose de faire les démarches à votre place. Vous vous dites « Chouette ! Cela va me faciliter la vie ». Si vous continuez sur ce site d'assistance, vous allez payer un euro symbolique, ce n'est pas cher pour faire le travail. Mais en fait, ce site ne fera rien du tout. Et comme vous ne lirez pas les conditions générales de ventes, vous n'aurez pas vu que la case qui vous abonne automatiquement à ce site pour vos démarches, est restée cochée, vous serez donc prélevé mensuellement de quelques euros sur votre compte bancaire en guise d'abonnement qui ne vous servira jamais à rien.

Vous pourrez toutefois vous désabonner, mais vous aurez perdu quelqu'argent.

2 – Boite mail :

La boite mail est un endroit privilégié des fraudeurs. Nous allons y trouver particulièrement 2 types de tentatives d'arnaques.

La première est le piratage du carnet d'adresses. Cela parait anodin à première vue. L'arnaque va consister en la récupération du carnet d'adresse mail. Le pirate va alors se servir de l'ensemble des adresses pour demander à chacun, par l'envoi d'un mail, un peu d'argent. Le mail ressemblera à une demande miséreuse, précisant que le demandeur est malade, sans le sou, ou bien bloquer dans un endroit où plus rien n'existes, qu'il a besoin de secours d'urgence, etc. etc.

La deuxième arnaque consiste en l'envoi de mail du centre des impôts, ou de la caisse d'assurance maladie. Ces mails, dont le contenu ressemble comme deux gouttes d'eau au site officiel, vont stipuler que les impôts, ou la sécurité sociale vous sont redevables d'une certaine somme. Ils vous demandent de cliquer sur un bouton « ***Cliquez ici*** » pour que vous puissiez alors être remboursé.

Ne cliquez jamais sur l'endroit indiqué.

Jamais les impôts ou la sécurité sociale ne feront ce genre d'information. Si ils vous doivent de l'argent, ils effectueront un virement directement sur votre compte bancaire, car ils ont vos coordonnées bancaires. Et s'ils ont besoin de vous en informer, ils le feront par courrier postale.

Il existe bien évidemment d'autres arnaques, les voyous sont sans limite dans la recherche d'escroquerie. C'est pour cela qu'il faut toujours être vigilant et supprimer un mail dans lequel nous n'avons pas confiance, plutôt que de voir son ordinateur piraté.

……

Solutions pour éviter de se faire avoir

Nous venons de voir les différents types de fraudes et d'arnaques auxquelles il est possible de se retrouver confronté. Il est malheureusement évident que cela ne représente qu'une partie de ce qui peut exister.

nc clair qu'il **faut être extrêmement vigilant pour éviter de tomber dans les pièges des personnes malfa**

Nous allons donc essayer de voir comment se prémunir de ces attaques et comment les signaler, car il existe des sites et des outils pour signaler ces agissements.

1 – Disque dur :

Le disque dur est, par essence, l'endroit rêvé sur l'ordinateur pour y stocker des données. On ne peut s'y introduire que si l'ordinateur est connecté à un réseau par quelque manière que ce soit.

Stocker ses fichiers sur le disque dur permet d'y avoir accès en permanence et donc de les travailler comme bon nous semble.

Apparemment, on pourrait croire que le disque dur est un élément sécurisé dès lors qu'l'on n'est pas connecté. Et qu'en se connectant à minima, le risque de piratage n'existe pas. Mais les personnes malveillantes auront tout loisir à installer « ***un cheval de Troie*** » sur votre machine dès qu'elle le pourra. Vous ne pourrez pas détecter ce « ***un cheval de Troie*** » et celui-ci aura tous loisirs loisir à pirater votre ordinateur à chaque connexion que vous effectuerez.

Vous comprenez donc que le disque dur est un endroit où aucune donnée ne devrait être stockée.

Il ne faut donc y laisser aucun fichier sensible et surtout ne pas y laisser un fichier contenant vos identifiants et mots de passe pour chaque site vous concernant. Car oui, il est tentant de créer un fichier avec identifiants et mots de passe, car votre mémoire peut être défaillante.

Les données que vous souhaitez garder seront beaucoup mieux sur un support externe à votre ordinateur. Ces supports peuvent être un disque dur externe, une clé USB, un CD-DVD ou encore le Cloud.

2 – Navigateur :

Pour naviguer en toute sérénité sur Internet, n'hésitez pas à suivre ces conseils :

A – Fraude par les données sensibles

Pour ce type de fraude, une personne malveillante va chercher à récupérer les identifiants et mots de passe de vos sites préférés. En effet, les navigateurs vous proposent d'enregistrer ces identifiants et mots de passe dans votre système pour que vous n'ayez plus à les saisir.

Mais si cela peut vous faciliter la vie, n'oubliez pas que cela va aussi la faciliter à quelqu'un qui aura su s'introduire dans votre ordinateur, ou qui vous l'aura « emprunté ».

Et comme par miracle, vous pourriez voir votre compte bancaire se vider irrémédiablement.

Pour vous éviter ces désagréments, je vous invite à vous reporter aux parutions du club ICPF sue ce sujet. Vous y trouverez les informations nécessaires pour n'enregistrer ni les identifiants, ni les mots de passe.

Vous pouvez y accéder en suivant le lien ci-dessous :

PARUTIONS DU CLUB

Sécurité Mot de Passe navigateur Internet

B – Fraude par le biais de sites d'aide

Lorsque vous souhaitez faire des démarches administratives par Internet, de nombreux sites, ressemblant à s'y méprendre aux sites officielles du gouvernement, vous proposent leur aide pour réaliser ces démarches.

Attention ! ces sites son t payants et peuvent finir par couter cher.

La meilleure solution pour éviter de se faire piéger est de se référencer au site du gouvernement « **https://www.service-public.fr** ».

Vous y trouverez les accès qui vous intéressent. Et sachez que de nombreuses démarches sont gratuites et/ou vous obligent à vous déplacer.

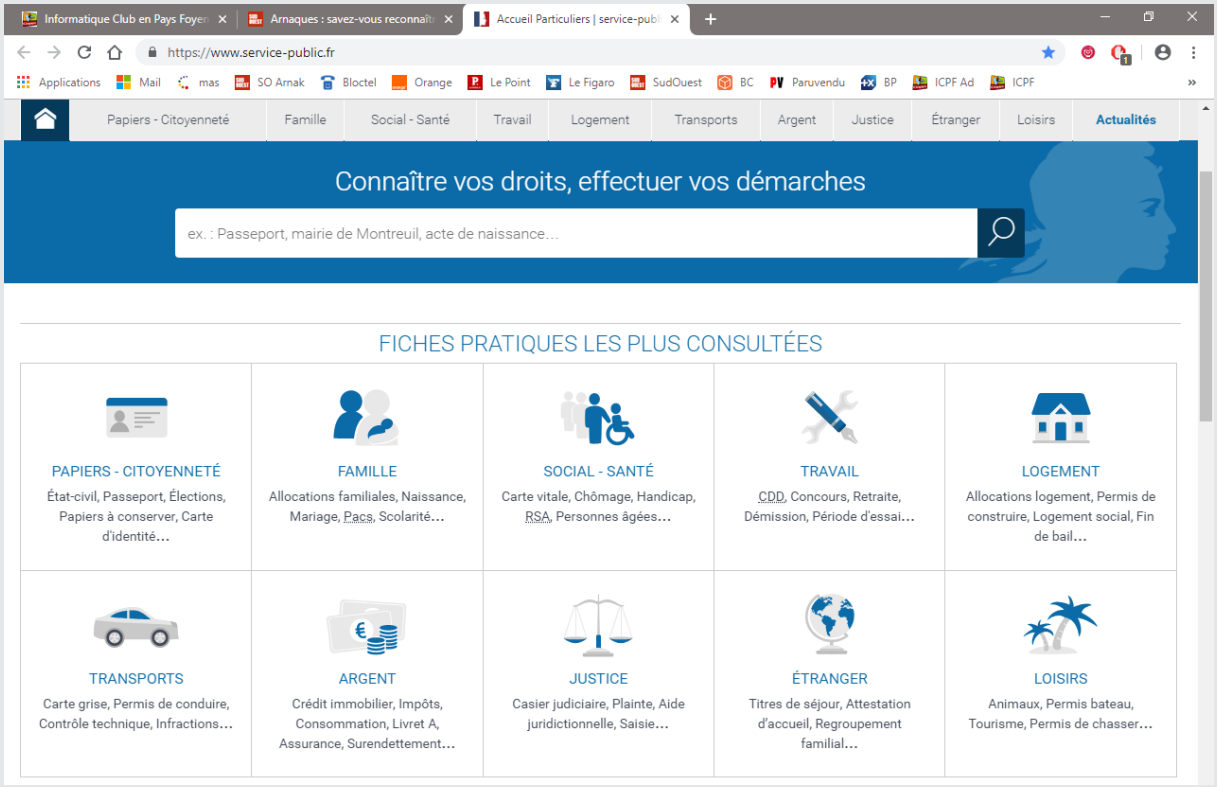

Figure 1

noter : les sites administratifs officiels ne se terminent absolument **jamais** par **« .gou.org » ou « .gouv.co**

Quant aux sites marchands, la DGCCRF vous conseille vivement de vous rendre sur le site « **https://www.europe-consommateurs.eu**» qui permet de vérifier si un vendeur est vraiment sérieux. Mais dans tous les cas, la vigilance reste de mise.

2 – Boite mail :

La boite mail est un outil par lequel nous faisons circuler bon nombre d'informations, autant d'ordre privé que d'ordre administratif, au sens général du terme. Et bien évidemment, plus il y a d'informations, plus la sécurité est fragilisée.

A – Carnet d'adresses :

Pour se protéger d'éventuelles arnaques, peu de solutions semblent exister.

Une astuce voudrait qu'en créant des adresses mails en début de carnet et fin de carnet protège celui-ci. Ceci n'est pas vraiment vérifié, mais cette combine a l'avantage d'être gratuite, facile à mettre en œuvre et donc pourquoi ne pas le faire.

Il suffit de créer une adresse « **aaaaa@aaa.aaa** » et « **zzzzz@zzz.zzz** ». Ces deux adresses prendront place en début et en fin du carnet et pourront éviter les piratages du carnet.

Vous trouverez ci-dessous l'explication (**forum de PCAstuces**).

J'ai reçus de cette astuce cet émail la est ce que cela est vrais ou cela ne fonctionne pas. Merci de vos réponses.

COMMENT PROTÉGER VOTRE CARNET D'ADRESSES (facile)
Un technicien en informatique a déclaré qu'un carnet d'adresse, c'est comme de l'or! (Et c'est une très bonne chose!)

J'ai appris un truc d'informatique aujourd'hui qui est tout simplement ingénieux dans sa simplicité. Comme vous le savez, lorsque/si un virus (ver) entre dans votre ordinateur, il se dirige directement vers votre carnet d'adresse de courriels, et envoie lui-même un message infecté à toutes les personnes inscrites dans votre carnet d'adresses, infectant du même coup tous vos amis et associés.

Ce truc n'empêchera pas le virus de se rendre à votre ordinateur, mais l'arrêtera d'utiliser votre carnet d'adresses pour se répandre davantage, et vous avisera du fait qu'il y a un tel virus qui vient d'entrer dans votre système.

Voici tout simplement ce que vous devez faire :

1. Ouvrez votre carnet d'adresses et cliquez sur «Nouveau contact ». (Comme si vous vouliez rajouter un nouvel ami à votre liste de courriels).

2. Dans la fenêtre où vous entreriez le prénom de votre contact, entrez « a ». Pour l'adresse courriel, entrez «aaaaa@aaa.aaa».

Maintenant, voici ce que cela fait dans votre ordi :

Le nom « a » sera placé en premier dans votre liste de contacts comme entrée numéro 1.

C'est l'endroit où le virus-ver commencera pour envoyer son premier email à toute votre liste de contacts, dans un élan pour envoyer plusieurs courriels à tous vos contacts.

Mais, lorsqu'il essaye d'envoyer le courriel à aaaaa@aaa.aaa, le message sera impossible à acheminer, parce que l'adresse courriel que vous avez entrée est complètement fausse. Et lorsque le premier essai échoue (comme dans ce cas-ci), le ver ne pourra se propager plus loin et aucun de vos contacts n'en sera infecté.

Voici le second avantage de cette méthode :

Lorsqu'un courriel ne peut être livré à son destinataire, vous êtes avisés de ceci dans votre boîte de courrier presque immédiatement.

Par conséquent, si vous recevez un courriel disant que vous avez envoyé un message à « aaaaa@aaa.aaa » qui n'a pu se rendre à son destinataire, vous saurez immédiatement que vous avez un virus-ver dans votre système. Vous pourrez alors prendre les mesures pour vous en débarrasser!

Facile, n'est-ce pas? Si tous ceux que vous connaissez étaient protégés de cette façon, alors vous ne seriez pas inquiets d'ouvrir du courrier de vos amis.

Passez donc le mot

B – Spam ou pourriel :

Les spam ou pourriels sont des mails délictueux envoyés pour infester votre ordinateur. Cela peut aussi être des mails publicitaires.

La plupart des fournisseurs de boite mail ont inclus des filtres anti-spam, il ne faut surtout pas désactiver ces filtres. Ces filtres ont pour effet de diriger dans la boite « **courrier indésirable** » les mails qui seront considérer comme délictueux. A vous de les vérifier et de les transférer dans la « **boite de réception** » si vous les considérez comme sûrs.

Si vous recevez ce genre de mails, la première action est de ne pas jouer les curieux en ouvrant ces mails. Vous pourriez, par cette action, libérer un virus dans votre ordinateur.

La deuxième action serait de signaler ces pourriels. En effet, le service des fraudes a mis en place un site qui permet de les signaler, les services de l'Etat engage alors les actions nécessaires pour lutter conte ces personnes malveillantes.

Pour les signaler, aller sur le site « **https//www.signal-spam.fr** ». Il faut alors s'inscrire sur le site (pas toujours aisé de le faire), puis de télécharger le module de signalement correspondant à votre navigateur et de l'activer.

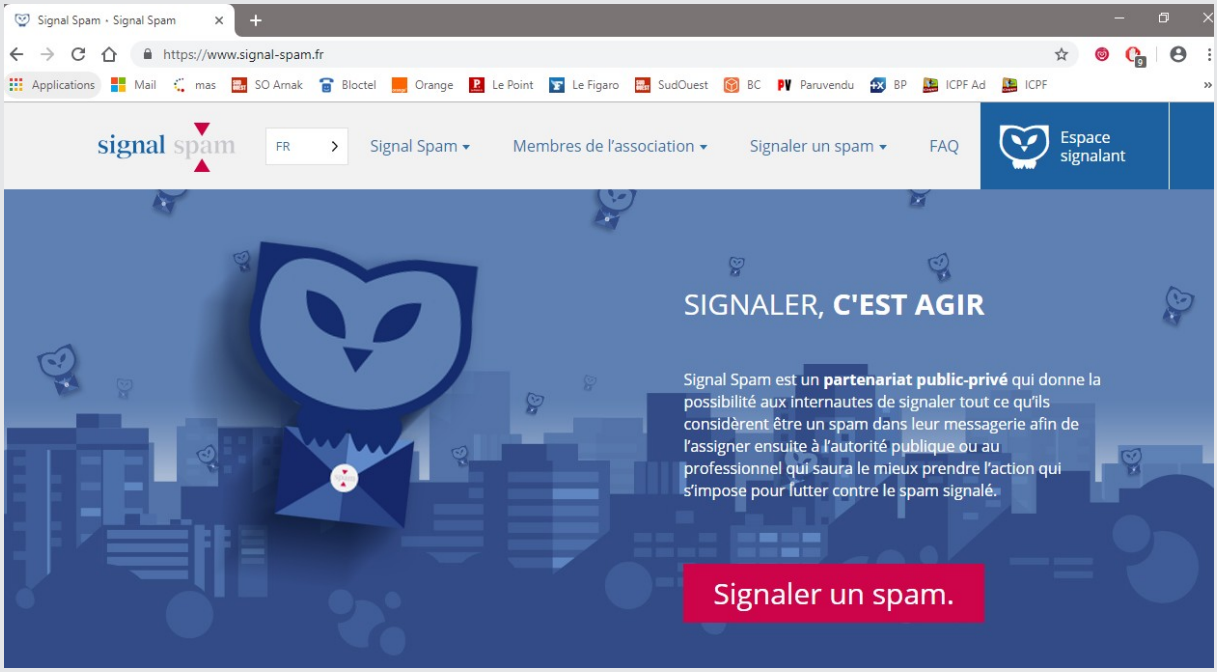

Figure 2

Le signalement se fait alors de manière très facile. Lorsque votre module de signalement est actif, une icône apparait alors en haut et à droite de votre écran (voir figure N° 3).

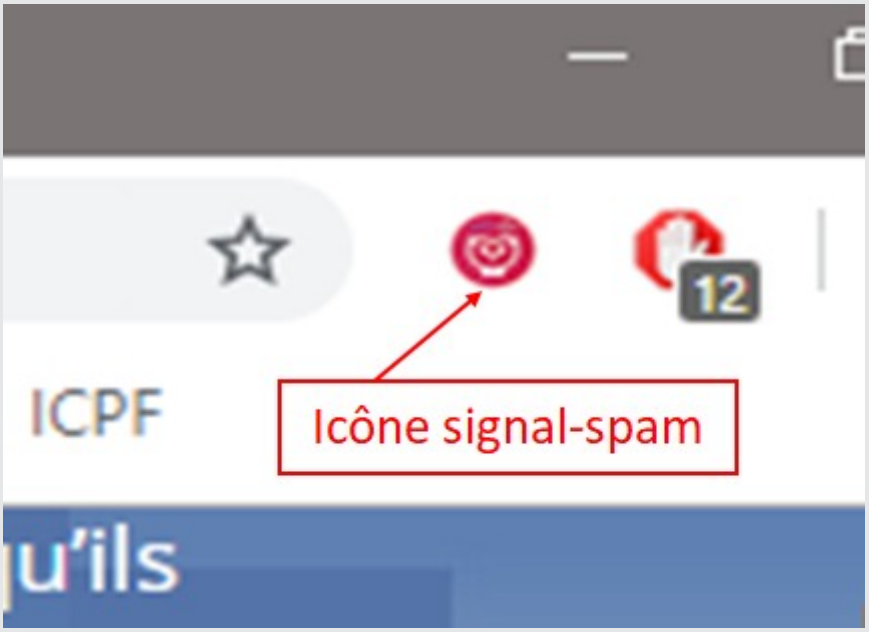

Figure 3

Pour effectuer un signalement, il suffit de sélectionner le mail délictueux, puis de cliquer sur l'icône « **signal-spam** », cela suffit.

B – Escroquerie :

Si vous pensez être victime d'une escroquerie (notamment suite à une dépose d'annonce que vous auriez pu faire sur un site d'annonces gratuites comme « **Leboncoin** » ou « **Paru-vendu** »), sachez que vous pouvez aussi signaler ces abus sur le site « **https://www.internet-signalement.gouv.fr** ».

Vous aurez alors accès au site (figure N° 4, vous cliquez sur « **Signalez >>**» et laisser vous guider pour effecteur votre signalement.

Figure 4

Epilogue

Voilà ce que nous pouvions dire sur les arnaques et les fraudes. Mais ce n'est malheureusement qu'une partie des attaques que l'on peut rencontrer sur Internet. Il nous est impossible de tout lister, ne serais-ce déjà par ignorance. Comme tout le monde le sait, la malveillance a toujours un coup d'avance par rapport à l'honnêteté.

En résumé :

Restez vigilant.
Ne laissez pas vos identifiants et mots de passe trainer n'importe où.
Ne stockez pas de données sensibles sur votre ordinateur
N'hésitez pas à signaler sur les sites officiels de l'Etat tout mail suspect.
Ne laisser pas en évidence vos numéros de carte bancaire et leur code.
N'ouvrez pas de mails qui vous paraissent délictueux.
Ne désactivez pas vos anti-virus.

-

En espérant que cet ouvrage puisse vous aider, bonne navigation sur Internet.

FIN

Achevé d'imprimé Octobre 2018