Repérer les tentatives d'arnaque

Nous recevons tous quotidiennement des e-mails dont il est difficile de dire s'ils sont légitimes ou si ce sont des tentatives d'arnaque. Voici un petit guide pour vous aider à identifier les messages frauduleux.

Hameçonnage ou Phishing

L'hameçonnage ou phishing est une technique utilisée par des fraudeurs pour obtenir des renseignements. Elle consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des informations.

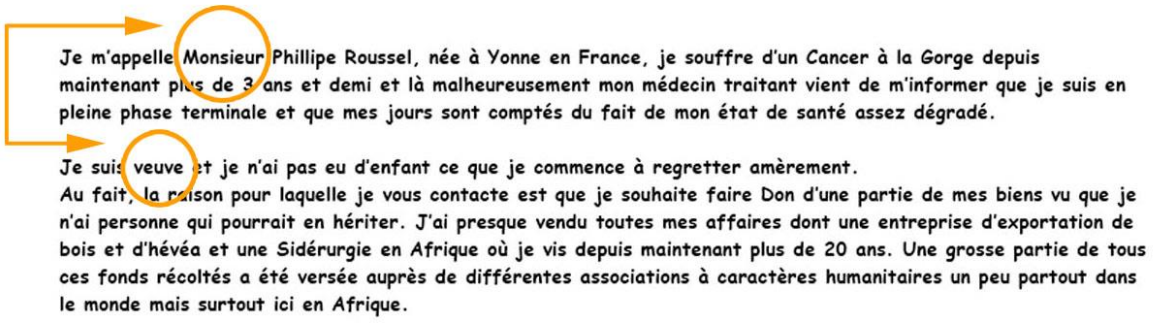
Le plus souvent, une copie exacte d'un site internet est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel. La victime va ainsi saisir ses codes personnels qui seront récupérés par celui qui a créé le faux site, il aura ainsi accès aux données personnelles de la victime et pourra dérober tout ce que la victime possède sur ce site.

Lorsque cette technique utilise les SMS pour obtenir des renseignements personnels, elle s'appelle SMiShing.

1/ Regardez l'orthographe, la syntaxe ou les incohérences

Les messages frauduleux contiennent fréquemment des fautes d'orthographe, de syntaxe ou des incohérences manifestes. Ces messages étant censés émaner que grosses sociétés ou d'administrations, la présence de ces erreurs est un premier indice. Attention toutefois, car les arnaqueurs font de plus en plus attention à la rédaction du contenu de leur message.

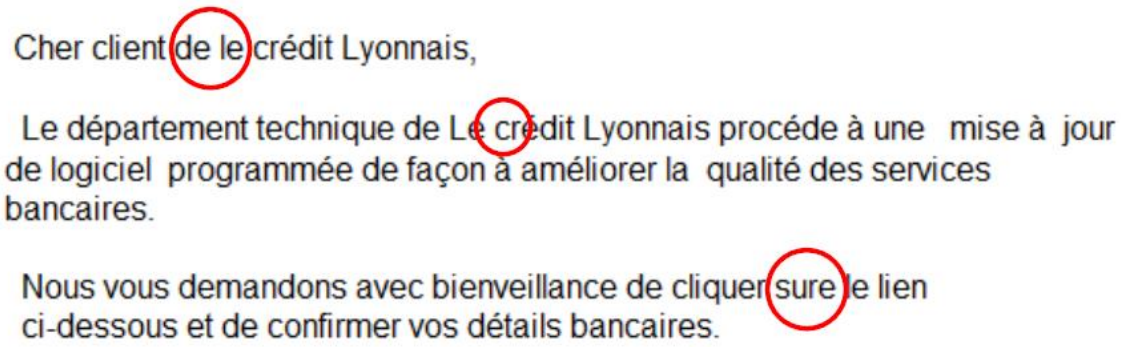
Ici, des majuscules sont manquantes, il manque des espaces après les points, il y a des doubles espaces et des fautes d'orthographe. Une banque ne rédigerait jamais un courrier avec autant de fautes. Elles restent néanmoins subtiles et nécessitent une lecture attentive.



Je m'appelle Monsieur Phillipe Roussel, née à Yonne en France, je souffre d'un Cancer à la Gorge depuis maintenant plus de 3 ans et demi et là malheureusement mon médecin traitant vient de m'informer que je suis en pleine phase terminale et que mes jours sont comptés du fait de mon état de santé assez dégradé.

Je suis veuve et je n'ai pas eu d'enfant ce que je commence à regretter amèrement.
Au fait, la raison pour laquelle je vous contacte est que je souhaite faire Don d'une partie de mes biens vu que je n'ai personne qui pourrait en hériter. J'ai presque vendu toutes mes affaires dont une entreprise d'exportation de bois et d'hévéa et une Sidérurgie en Afrique où je vis depuis maintenant plus de 20 ans. Une grosse partie de tous ces fonds récoltés a été versée auprès de différentes associations à caractères humanitaires un peu partout dans le monde mais surtout ici en Afrique.

Incohérence dans le texte



Cher client de le crédit Lyonnais,

Le département technique de Le crédit Lyonnais procéde à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

Nous vous demandons avec bienveillance de cliquer sure le lien ci-dessous et de confirmer vos détails bancaires.

Multiples fautes d'orthographe (« de le » au lieu de « du », « credit » sans majuscule, « sure » au lieu de « sur ».

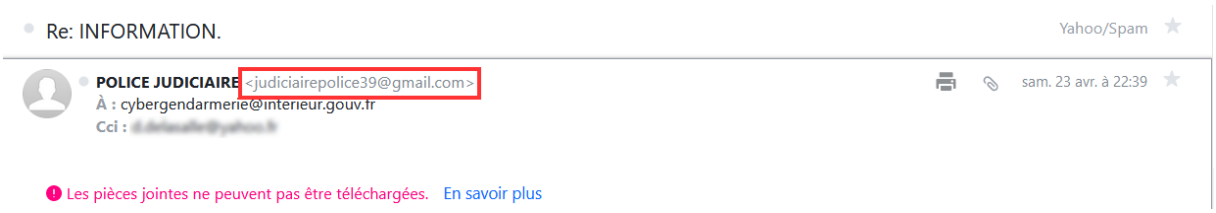
2/ L'adresse mail de l'expéditeur

Plus que le contenu du message, l'adresse mail de l'expéditeur est un indice vraiment significatif.

Pour rappel, une adresse mail est toujours composée de la façon suivante :

nom@nom_de_domaine.extension

Pour détecter une éventuelle arnaque, on analyse la partie **nom de domaine** et **extension** de l'adresse. Ce nom de domaine doit être cohérent par rapport au nom de l'expéditeur. Si je reçois un mail de Free, l'adresse de l'expéditeur doit en toute logique se terminer par « @free.fr ». Si ce n'est pas le cas, le message est suspect.



Re: INFORMATION. Yahoo/Spam

POLICE JUDICIAIRE <judiciairepolice39@gmail.com> sam. 23 avr. à 22:39

À : cybergendarmerie@interieur.gouv.fr

Cci :

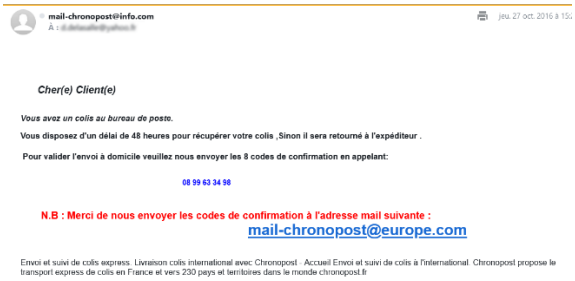
Les pièces jointes ne peuvent pas être téléchargées. En savoir plus

La police judiciaire utilise une adresse Gmail ? Etrange !

Pourquoi le Credit Agricole envoie-t-il un message avec un nom de domaine en elkom_vmv.bg (BG étant l'extension de la Bulgarie) et non en credit-agricole.fr ?

Il haut être vigilant car parfois, les arnaqueurs vont utiliser des adresses très proches de l'adresse officielle pour vous induire en erreur (ex : credit-agricol.com au lieu de credit-agricole.fr).

Si vous avez un doute sur le nom de domaine officiel d'une société, cherchez le site de la société dans un moteur de recherche et regardez quelle est l'adresse de la page officielle.

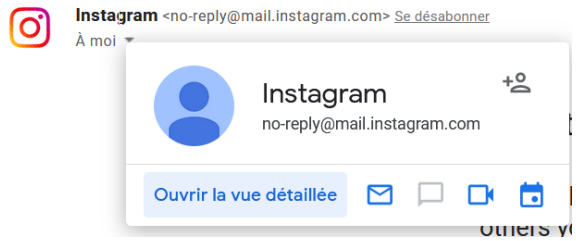


Ici, le message émane d'une adresse qui pourrait sembler légitime : mail-chronopost.com.

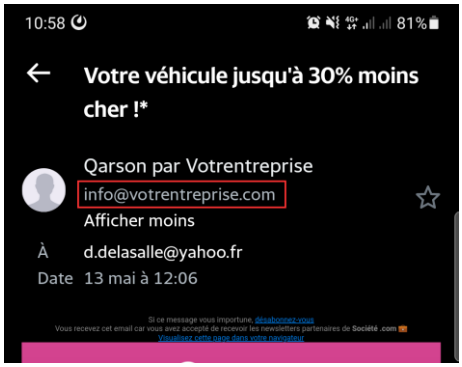
Après vérification sur un moteur de recherche, on voit que le nom de domaine associé à Chronopost se termine en .fr.

Afficher l'adresse mail complète de l'expéditeur

Selon le service de messagerie employé, il se peut que l'adresse mail complète ne soit pas affichés d'office ; à la place, figure un nom.
Si c'est le cas, laissez votre souris quelques instants sur le nom pour faire apparaître l'adresse détaillée de l'expéditeur.



C'est particulièrement vrai si vous consultez vos mails sur votre téléphone, dans ce cas, cliquez sur votre nom (Moi) dans l'en-tête du message pour afficher les détails de l'adresse.

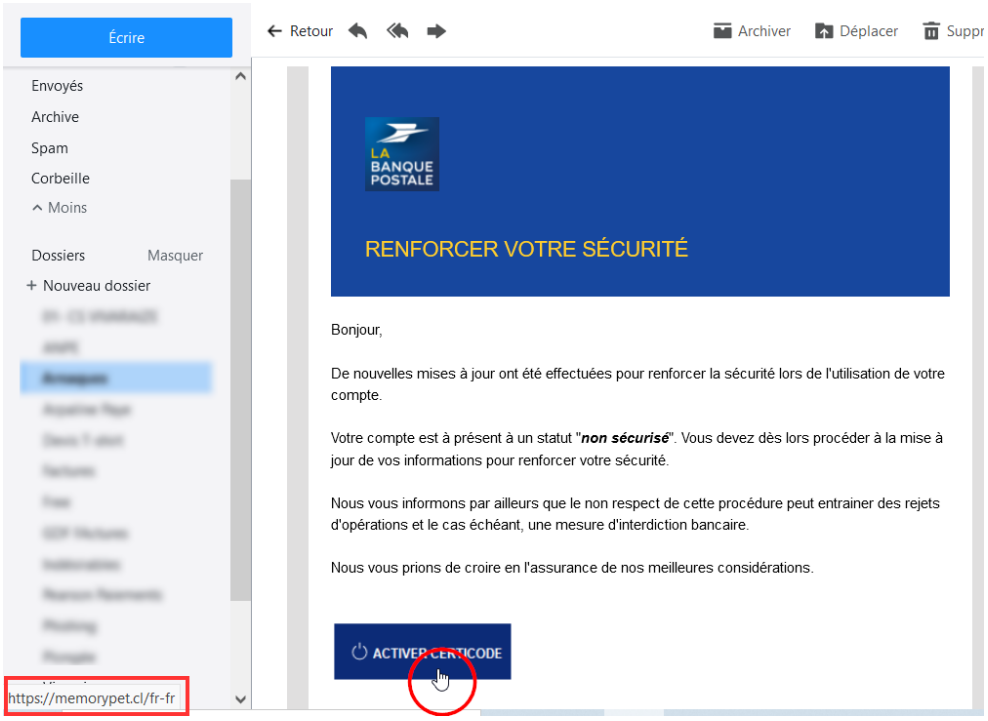


3/ La destination des liens du message

Les messages d'arnaque contiennent fréquemment des liens, puisque ces messages sont là pour vous inciter à remplir des formulaires sur des pages où les pirates pourront ainsi récupérer vos informations personnelles.

Si le contenu du message et l'adresse de l'expéditeur ne suffisent pas à déterminer si le message est légitime ou non, on peut analyser la destination des liens qu'il contient.

Pour connaître la destination d'un lien sans cliquer dessus, survolez-le avec le curseur de votre souris et observez ce qui s'affiche en bas à gauche dans la barre d'état du navigateur.



Ce message est censé provenir de la Banque Postale. En survolant le bouton, on voit que le lien pointe vers l'adresse memorypet.cl/fr-fr, une adresse située au Chili, qui n'a rien à voir avec celle de la banque postale (labanquepostale.fr).

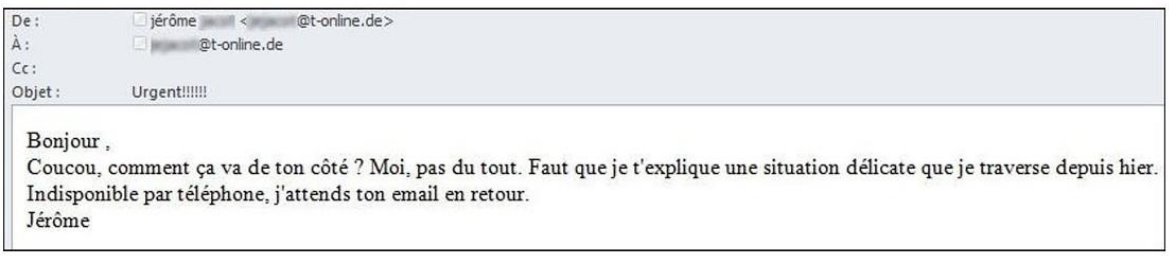
Cette technique peut aussi être utilisée lorsque vous consultez des pages Web.

4/ Les « appels au secours » de proches ou les « héritages surprise »

On peut aussi recevoir des messages de gens plus ou moins proches avec leur vraie adresse.
Dans ce cas, leur adresse a été piratée ; elle a été récupérée suite à des attaques sur les bases de données de sites sur lesquels elles ont créé des comptes (voir le support de cours « Vérifier si mon adresse mail a été compromise »).

A chaque fois, votre correspondant vous demandera de communiquer exclusivement par mail. Si vous l'appeliez, la supercherie serait immédiatement dévoilée. Les prétextes à vous demander de l'argent peuvent être une maladie soudaine, le vol de moyens de paiement, la perte d'un billet d'avion…

Si vous donnez suite au message, le correspondant finira par vous demander d'aller acheter des tickets prépayés au bureau de tabac et de lui communiquer les numéros pour procéder à un transfert d'argent. Cette méthode ne laisse aucune possibilité de remonter à l'arnaqueur.



Dans le cas des « héritages ou leg surprise », une personne très malade vous aura choisi comme légataire de sa fortune. Pour procéder au virement, elle vous demandera vos coordonnées bancaires et videra votre compte au lieu d'y virer le leg inattendu.

Bonjour,

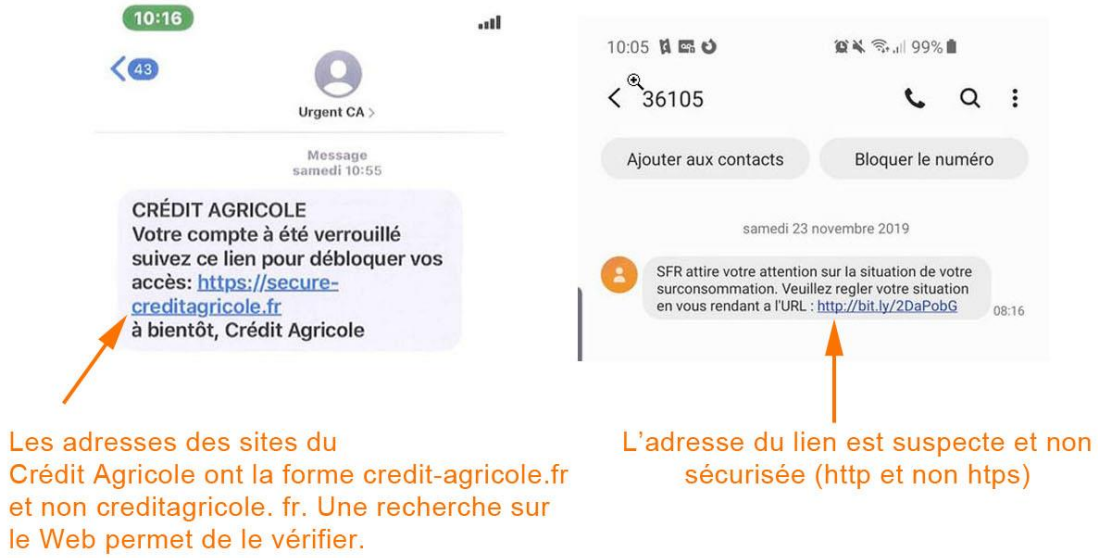
Acceptez et tolérez cette intrusion peu décente dans votre messagerie. Je sais que mon message sera d'une grande surprise quand t-il vous parviendra. Je suis Michel Labrosse, chrétienne et j'ai 67 ans. J'ai le cœur serin vu que je suis touchée par une maladie. Selon mon docteur, une boule de sang s'est installée dans mon cerveau et est à un niveau très avancé. Bien sûre que je ne vous connais pas, mais après une longue réflexion et à travers mes prières, j'ai pris cette décision de vous contacter. Je veux mettre à votre dis position une somme de 12 020 000 € (Douze million vingt mille d'euros) que je vous offre pour réaliser un projet qui consiste à aider les enfants de la rue, les orphelins et les gens qui sont dans le grand besoin. Car ce sont nos œuvres qui resteront quand tombera sur nous, le rideau de la mort. En mourant nous n'emportons aucun bien matériel avec nous. Les prières et la foi valent beaucoup plus que l'or. Le destin m'oriente vers vous, ce n'est pas un simple hasard. Votre destin n'est il pas ainsi tracé par le seigneur?

Toutefois, je comprendrais votre étonnement quant à ma façon de procéder. Je vous prie donc d'accepter cette offre que je veux mettre gracieusement à votre disposition contre votre prière pour moi et fait profiter les autres autour de vous. J'aimerais surtout que vous me répondiez car c'est la boite que je consulte le plus souvent et qui me donne l'espoir de continuer à vivre et à retrouver le sourire qui s'est détalé de moi. Alors, si vous êtes d'accord j'attends donc votre réponse.

Mme Michel Labrosse

Les arnaques par SMS

Longtemps cantonnées aux mails, les arnaques par SMS se multiplient.



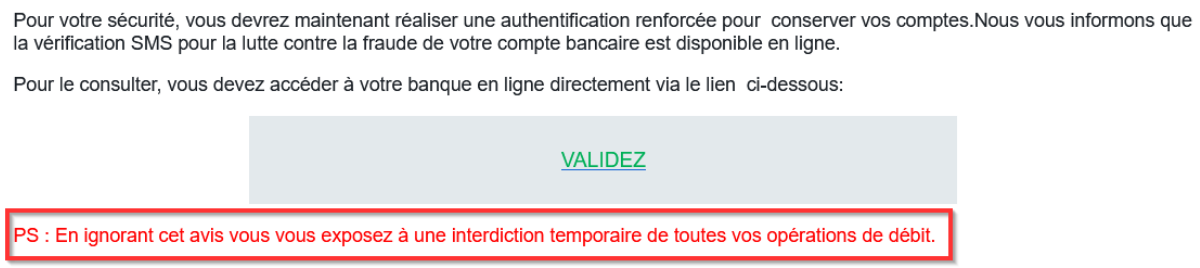
Appliquez les mêmes conseils que pour les mails pour détecter les tentatives d'arnaque par SMS.

Autres éléments qui peuvent attirer votre attention

Les premiers critères que nous avons vus suffisent généralement à déjouer les arnaques, mais soyez aussi vigilant aux :

- messages alarmistes, à caractère **urgent et problématique** (compte bloqué, facture impayée, etc.)

- messages insistant sur un **gain potentiel** (remboursement d'une facture, trop perçu des impôts, gain d'un concours)
- messages non attendus (pour la livraison de colis, par exemple)
- demandes d'informations personnelles (numéro de CB, pièce d'identité, RIB…)


Pour votre sécurité, vous devrez maintenant réaliser une authentification renforcée pour conserver vos comptes.Nous vous informons que la vérification SMS pour la lutte contre la fraude de votre compte bancaire est disponible en ligne.

Pour le consulter, vous devez accéder à votre banque en ligne directement via le lien ci-dessous:

VALIDEZ

PS : En ignorant cet avis vous vous exposez à une interdiction temporaire de toutes vos opérations de débit.

Les arnaqueurs jouent sur la notion d'urgence pour vous mettre la pression et éviter que vous ne preniez le temps de la réflexion.

- adresses qui figurent dans les mails. Vérifiez la localisation géographique des adresses qui figurent dans les mails
-

Que faire ?

- Souvenez-vous qu'aucune banque, institution ou administration ne vous demandera d'informations confidentielles pas mail.
- Ne cliquez jamais sur les liens présents dans le mail
- Ne répondez pas au message
- N'ouvrez surtout pas les fichiers envoyés en pièces jointes
- Vérifiez les adresses mail et les numéros de téléphone contenus dans les messages en les tapant dans un moteur de recherche.
- Si vous recevez un mail d'une personne connue avec une pièce jointe, mais que vous n'attendiez aucun message de cette personne et si le message vous semble suspect, n'hésitez pas à contacter l'expéditeur pour vous assurer qu'il est bien l'auteur du message.
- Signalez le message comme « courrier indésirable » (si cette fonctionnalité est accessible dans votre messagerie)
- Le supprimer

Réagir

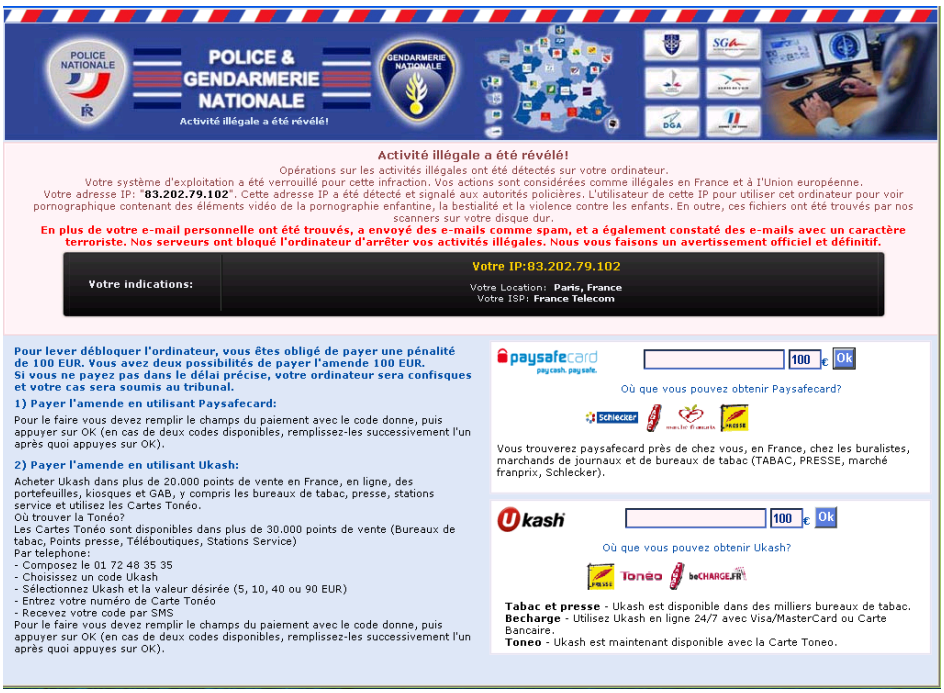
Malgré votre vigilance, vous avez été victime d'une arnaque. Quelle est la conduite à suivre ?

- Prévenez votre banque et contactez l'assurance de votre carte bancaire
- Prévenez l'administration ou l'entreprise concernée (banque, agence de location de vacances, Caisse d'allocations familiales, etc.) et transférez le mail à leur service client
- Changez le mot de passe de votre compte bancaire en ligne et celui du service qui a servi à vous tromper (CAF, Ameli, Impôts…)

- Faire un signalement sur www.internet-signalement.gouv.fr, uniquement pour mes arnaques par mail et sites Internet.
- Sur un téléphone portable, en cas d'arnaque par SMS, transférer le SMS au 33700

Et sur Internet…

Si vous tombez un jour sur un de ces écrans, surtout, ne payez rien, ne donnez aucune information personnelle. Pressez longuement sur le bouton d'alimentation de votre ordinateur pour forcer son arrêt, puis redémarrez-le.



S

Ouvrez l'œil ! Restez vigilant !