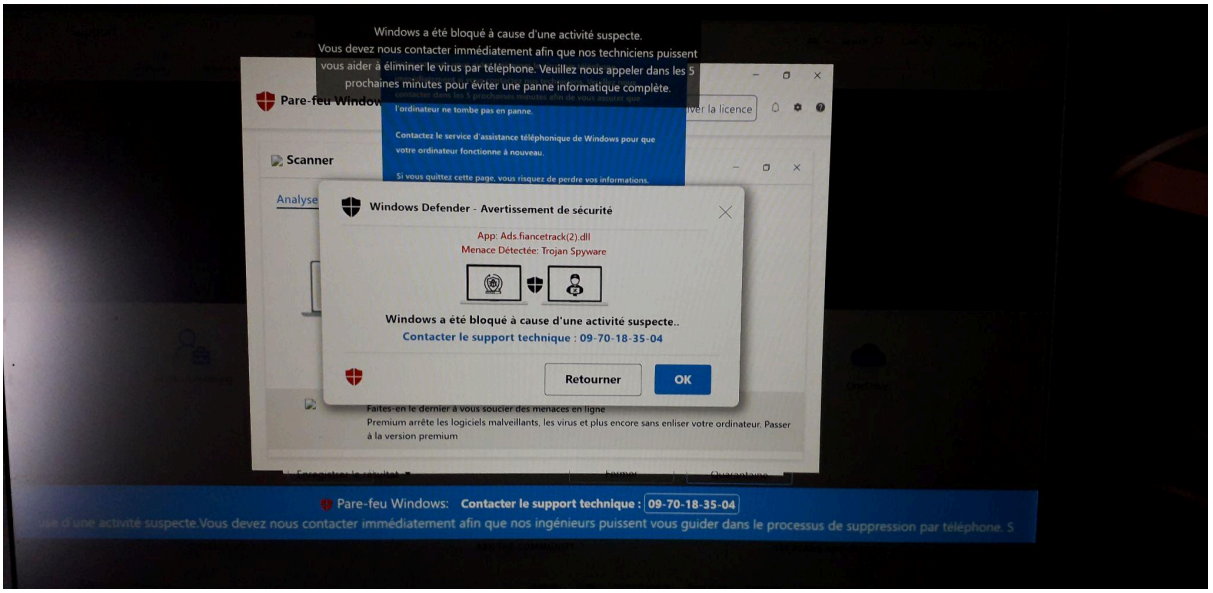
Lionel RAUCH
Conseiller Numérique
France Services

L'arnaque au faux support technique (Tech support scam en anglais) consiste à vous effrayer en vous indiquant un problème technique grave afin de vous pousser à payer un pseudo-dépannage informatique.



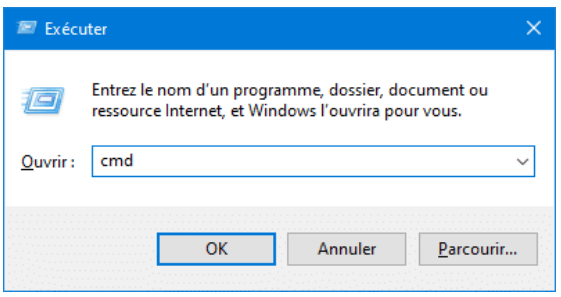
Visuel de l'arnaque (sur PC sous Windows 11) / octobre 2022

L'apparition du message semble bloquer l'ordinateur en indiquant qu'un problème technique grave a été détecté.

Ce n'est bien souvent qu'une fenêtre "pop-up" qui s'est ouverte mais comme elle prend toute la place de la fenêtre il n'est pas simple de s'en débarrasser … Une combinaison des touches Alt + F4 ou Ctrl + Alt + Suppr (pour ouvrir le gestionnaire de tâches et fermer le navigateur) permet de fermer cette fenêtre.

Le risque annoncé de la perte de ses données ou de l'usage de son équipement pousse à **contacter un prétendu support technique** officiel (Microsoft, Apple, Google…), pour ensuite convaincre de payer un pseudo-dépannage informatique et/ ou à acheter des logiciels inutiles, voire nuisibles.

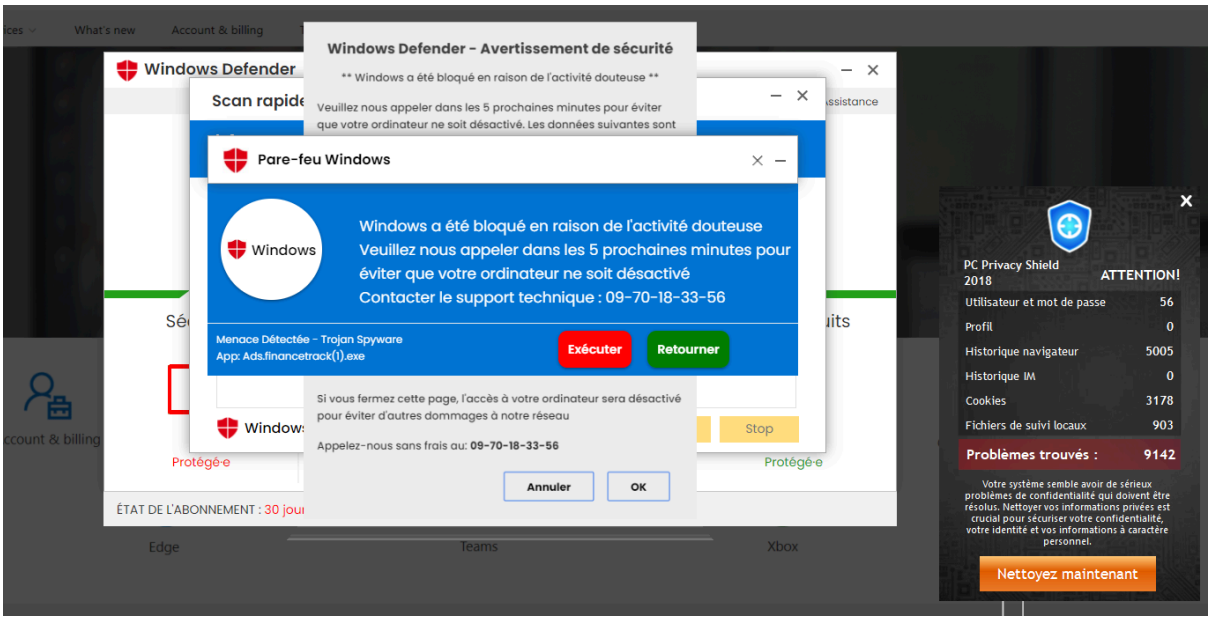
Au téléphone l'arnaqueur demande de faire quelques démarches afin de pouvoir prendre la main sur l'ordinateur soit disant infecté. Bien souvent il s'agit de commandes clavier comme **Windows + R** pour lancer la boîte de dialogue Exécuter.



Une nouvelle fois l'arnaqueur va demander de taper une adresse d'un site internet (dans le cas présent www.servicesordi.com) afin de pouvoir

accéder à l'outil de prise de contrôle à distance (ici le logiciel ConnectWise Control).

A partir de ce moment l'arnaqueur à la main sur l'ordinateur et il va installer un logiciel, PC Privacy Shield, qu'il va utiliser pour faire croire à une infection importante sur l'ordinateur.



PC Privacy Shield laisse à penser que l'ordinateur à beaucoup de problèmes (ce qui est faux)

C'est à ce moment-là qu'il annonce que la désinfection de l'ordinateur va coûter une certaine somme (entre 150 et 250€ selon l'arnaqueur), somme qui va être divisée par 2 comme par magie si vous payez tout de suite par carte bancaire.

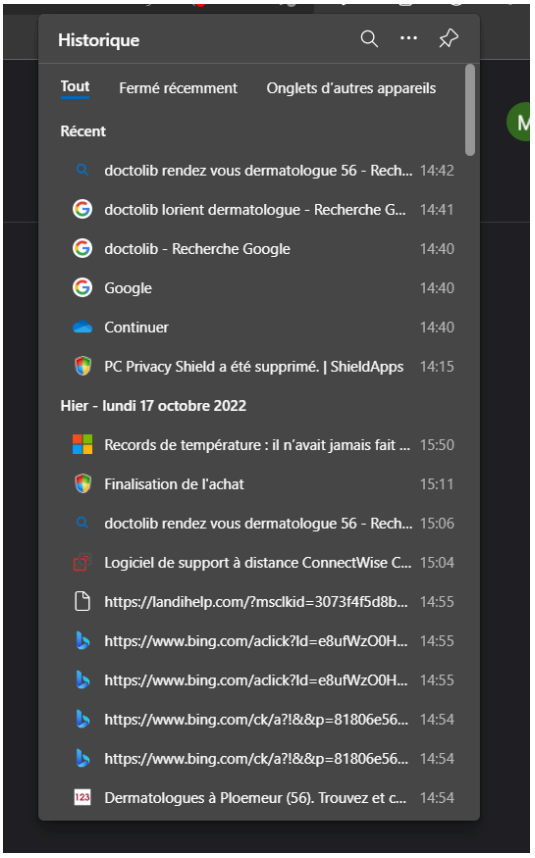
Bien entendu, il ne faut pas payer et couper court à la communication et éteindre son ordinateur et sa connexion Internet. Ce qui est plus facile à dire quand on est pas dans l'urgence et le stress de cette situation !

Désinfection de l'ordinateur

Le mal étant fait (arnaque poussée jusqu'au bout ou non) il convient donc de voir ce qu'il est possible de faire pour signaler l'arnaque mais aussi pour nettoyer l'ordinateur qui a été "pris en main" par l'arnaqueur.

1 - Conserver les preuves

Le site Cybermalveillance.gouv.fr indique sur son site : "*Conservez toutes les preuves pour le signalement ou le dépôt de plainte aux autorités.* ***Photographiez votre écran*** *au besoin.* ***Notez le numéro de téléphone*** *qui s'affiche sur votre écran ou qui est mentionné dans le message que vous avez reçu.*



Il arrive parfois que le faux support technique demande à ce que vous rappeliez un autre numéro de téléphone que celui qui s'affiche sur votre écran. Notez également ce numéro. Si vous le pouvez, ***conservez également l'adresse URL de la page malveillante****. Si le faux support vous a transmis des documents (facture, contrat, etc.), conservez-les également".*

Ces preuves permettront d'alimenter la plainte qui sera déposée concernant cette arnaque. On en reparle un peu plus tard ...

2 - Désinstallez toute nouvelle application qui vous semblerait suspecte

Comme l'arnaqueur à pris la main sur votre ordinateur il a donc pu installer différents logiciels ...

Vérifiez donc toutes les installations faites à la date de l'arnaque via le **panneau de configuration** puis **Programmes et fonctionnalités** et enfin **Désinstaller un logiciel** et en choisissant l'onglet **installé le** ... vous aurez ainsi la liste des logiciels installés ou modifiés à la date de l'arnaque.

Il pourra donc y avoir le logiciel PC Privacy Shield par exemple mais il peut aussi y avoir d'autres logiciels et/ou anti-virus qui auront été installés par l'arnaqueur. Il se peut que ce soient des logiciels tout à fait légaux (Pack Office par exemple) que l'arnaqueur va tenter de vendre via son lien d'affiliation qui lui permettra de gagner un peu d'argent.

Il convient aussi de faire une analyse approfondie de votre ordinateur. Pour cela, le logiciel gratuit **Adwcleaner de Malwarebytes** est parfait. Il analysera l'ordinateur, détectera les applications malveillantes et les mettra en quarantaine.

A la suite de cela il est aussi possible de lancer une analyse anti-virus (même si cela n'est pas indispensable, l'arnaqueur n'ayant pas utilisé le virus pour prendre la main sur votre ordinateur vu que c'est vous qui lui avez ouvert la porte !) cela permettra de vérifier qu'il n'y pas eu d'intrusion plus poussée sur votre ordinateur.

Changez vos mots de passe !

Si l'arnaqueur a eu accès à votre ordinateur il a pu éventuellement aller voir s' il y avait des mots de passe pré enregistrés sur votre navigateur (Paramètres puis Mots de passe). Listez dans ce cas tous les mots de passe en question et procédez à un changement complet avec un nouveau mot de passe sécurisé pour chacun des comptes présents sur votre navigateur. Le site **Cybermalveillance.gouv.fr** vous propose des astuces pour cela.

Portez plainte

Une fois votre ordinateur vérifié vous allez pouvoir aller déposer des plaintes via les plateformes mises en place sur Internet. La procédure **THESEE** (« traitement harmonisé des enquêtes et des signalements de e-escroqueries ») est accessible via le **site du Service**

Public. Il suffit de remplir les différents champs du questionnaire et de se laisser guider pour finaliser la plainte.

Le dépôt de plainte est possible via son compte FranceConnect, dont les données servent à identifier le déposant, qui pourra ensuite reprendre sa déclaration initiale, la compléter, ou la retirer. Cette plainte sera accessible dans le dossier personnel de « *FranceConnect* » pendant six ans (source).

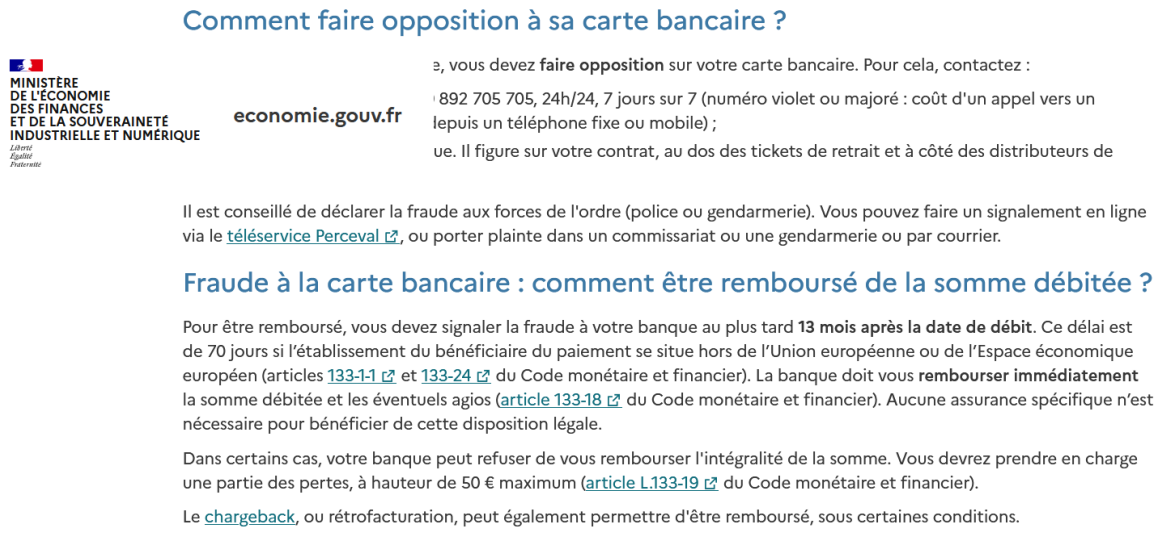
Il est aussi possible de signaler le contenu illicite (ici le site Internet par le biais duquel a été lancée l'escroquerie) via la plateforme **PHAROS**.

Se faire rembourser de l'arnaque

Si vous avez payé pour un service qui s'avère être une arnaque vous pouvez demander un remboursement auprès de votre banque. Vous pouvez ainsi faire un signalement via le **système PERCEVAL**, service accessible via FranceConnect. Vous aurez alors besoin de vos identifiants et votre numéro de carte bancaire.

Ce service permet de signaler une fraude à la carte bancaire si vous remplissez les conditions suivantes :

- Vous êtes toujours en possession de votre carte bancaire
- Vous n'êtes pas à l'origine des achats en ligne
- Vous avez fait opposition à la carte auprès de votre banque



Comment faire opposition à sa carte bancaire ?

MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE
Liberté
Égalité
Fraternité

economie.gouv.fr

…e, vous devez **faire opposition** sur votre carte bancaire. Pour cela, contactez :

… 892 705 705, 24h/24, 7 jours sur 7 (numéro violet ou majoré : coût d'un appel vers un …lepuis un téléphone fixe ou mobile) ;

…ue. Il figure sur votre contrat, au dos des tickets de retrait et à côté des distributeurs de …

Il est conseillé de déclarer la fraude aux forces de l'ordre (police ou gendarmerie). Vous pouvez faire un signalement en ligne via le téléservice Perceval, ou porter plainte dans un commissariat ou une gendarmerie ou par courrier.

Fraude à la carte bancaire : comment être remboursé de la somme débitée ?

Pour être remboursé, vous devez signaler la fraude à votre banque au plus tard **13 mois après la date de débit**. Ce délai est de 70 jours si l'établissement du bénéficiaire du paiement se situe hors de l'Union européenne ou de l'Espace économique européen (articles 133-1-1 et 133-24 du Code monétaire et financier). La banque doit vous **rembourser immédiatement** la somme débitée et les éventuels agios (article 133-18 du Code monétaire et financier). Aucune assurance spécifique n'est nécessaire pour bénéficier de cette disposition légale.

Dans certains cas, votre banque peut refuser de vous rembourser l'intégralité de la somme. Vous devrez prendre en charge une partie des pertes, à hauteur de 50 € maximum (article L.133-19 du Code monétaire et financier).

Le chargeback, ou rétrofacturation, peut également permettre d'être remboursé, sous certaines conditions.

Vous pouvez aussi demander le remboursement des sommes dépensées auprès de votre banque. Le site du **ministère de l'économie** indique en effet que : *Pour être remboursé, vous devez signaler la fraude à votre*

*banque au plus tard **13 mois après la date de débit**. Ce délai est de 70 jours si l'établissement du bénéficiaire du paiement se situe hors de l'Union européenne ou de l'Espace économique européen (articles 133-1-1 et 133-24 du Code monétaire et financier).*

*La banque doit vous **rembourser immédiatement** la somme débitée et les éventuels agios (article 133-18 du Code monétaire et financier). Aucune assurance spécifique n'est nécessaire pour bénéficier de cette disposition légale.*

Dans certains cas, votre banque peut refuser de vous rembourser l'intégralité de la somme. Vous devrez prendre en charge une partie des pertes, à hauteur de 50 € maximum (article L.133-19 du Code monétaire et financier).

Besoin d'aide ?

Il est possible de contacter un expert de la brigade numérique mise en place par la Gendarmerie Nationale via le site **Ma Gendarmerie**. Un service accessible via Internet 7 jours sur 7 et 24/24.

Si vous êtes un particulier, vous pouvez être accompagné gratuitement dans cette démarche par une association de France Victimes au 116 006 (appel et service gratuits), numéro d'aide aux victimes du ministère de la Justice. Service ouvert 7 jours sur 7 de 9h à 19h.