

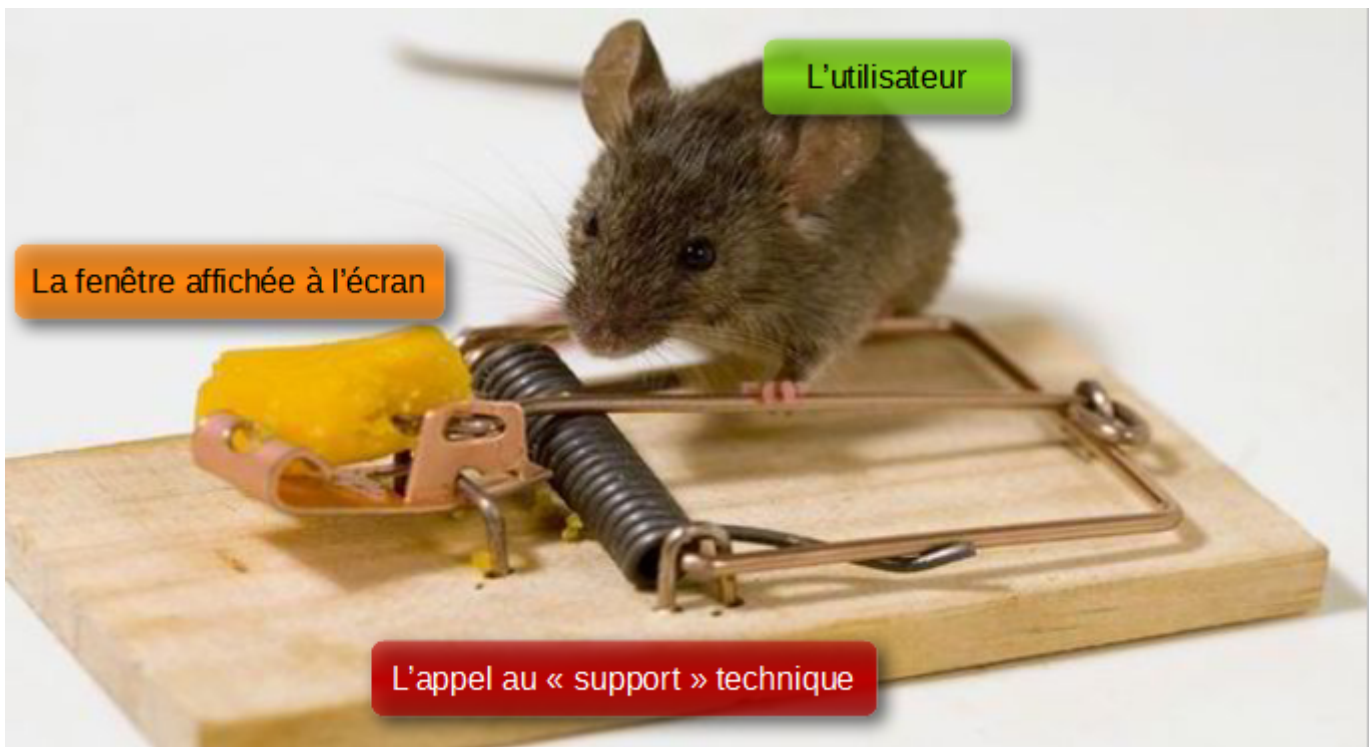
Se protéger sur Internet - Fausse assistance Windows : comment réagir

Processus

Contexte

Lors de la navigation sur le web, une fenêtre surgit informant que notre ordinateur est infecté. L'ordinateur se met à parler d'une voix robotisé en lisant l'avertissement de sécurité. Les touches du clavier ne répondent pas forcément, il semble impossible de fermer cette fenêtre : la situation est oppressante...

« Heureusement », la fenêtre présente un numéro de téléphone afin de contacter le « support » technique. C'est en appelant ce numéro que le piège se referme.



Que se passe-t-il lors de l'appel ?

Le protocole est généralement le même, à savoir :

- Après une courte attente, un opérateur répond.
- Il comprend très bien l'attaque qui est en train de se dérouler.
- Il explique les manœuvres à effectuer pour couper le son.
- Il demande si l'ordinateur dispose d'un antivirus, si tel est le cas, il guide l'utilisateur pour désactiver l'antivirus en expliquant qu'il n'est pas adapté à ce genre de tentatives d'intrusion.
- Il donne des démarches pour installer un logiciel lui permettant de prendre la main sur l'ordinateur.
- Il fait un « bilan » de l'ordinateur expliquant qu'il est très infecté, c'est très grave, il est urgent d'intervenir.
- Il propose de résoudre tous les problèmes grâce à un logiciel certifié par Microsoft.
- Ce logiciel a un coût que l'opérateur se charge de valoriser en vantant une protection face aux futures attaques.

“ Attention

Comme souvent dans les arnaques, le malfaiteur joue sur le caractère d'urgence et sur les sentiments : « vous risquez de perdre vos photos dans quelques minutes si vous ne me laissez pas intervenir rapidement ».

But recherché :

Soutirer de l'argent à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

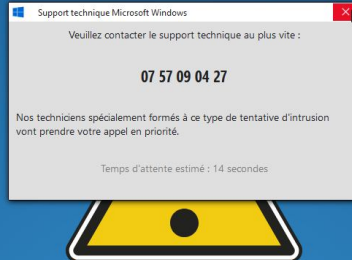
Témoignage

“ « J'étais sur Internet quand tout à coup une sirène s'est mise à hurler et une fenêtre a surgi sur mon écran me disant que j'avais un virus et que je devais rappeler un numéro pour le supprimer sous peine de perdre tous mes fichiers. Mon ordinateur était complètement bloqué et c'était très angoissant. J'ai donc appelé le numéro et un technicien m'a demandé de pouvoir accéder à distance à mon ordinateur pour le réparer. Il m'a ensuite demandé de payer 350 € pour le dépannage et un contrat d'assistance d'un an. Il avait l'air sûr de lui et professionnel, moi je n'y connais pas grand-chose, alors je lui ai fait confiance. Il est « entré dans mon ordinateur à distance », comme il me l'a dit. Quand j'ai raconté cette histoire à mon fils, il m'a dit que je m'étais fait arnaquer. J'ai appelé ma banque pour faire opposition à ma carte et j'ai déposé plainte, mais je ne pense pas revoir un jour mon argent. »

Exemple de page de fausse attaque



Message d'alerte



Windows Defender résiste actuellement à une attaque malveillante. N'éteignez surtout pas votre ordinateur sans quoi toutes vos données seront compromises.

Solutions

“ Pour bien comprendre

En réalité, il ne s'agit pas du tout d'une attaque ou d'un message système mais simplement d'une page internet. Elle reproduit simplement les codes graphiques de *Microsoft Windows*.

Par conséquent, la solution réside dans le fait de fermer l'onglet responsable de cet affichage, voire le navigateur internet au complet.

Fermer directement l'onglet : **Ctrl** + **w**

Étant donné que l'écran présente un onglet du navigateur Internet affiché en plein écran, le but est de fermer cet onglet. La combinaison de touches s'applique quel que soit le navigateur : **Ctrl** + **w**.

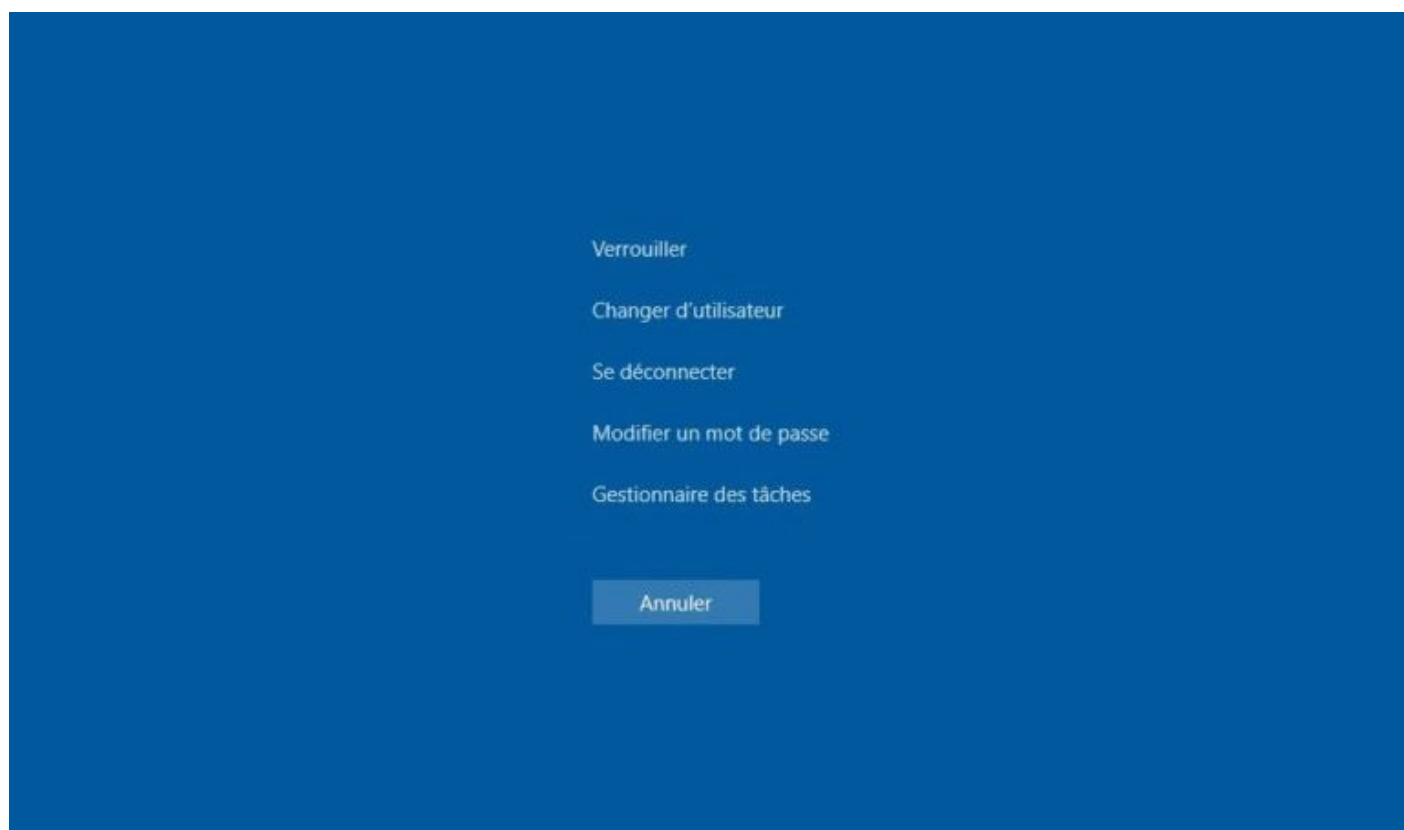
La page est instantanément fermée, dans le cas où il s'agit d'un unique onglet, le navigateur complet est fermé.

Touche **Esc** pour reprendre le contrôle sur l'onglet

Les navigateurs (modernes et à jour) interdisent de désactiver l'action de la touche **Esc** (ou **Échap**, il s'agit de la touche en haut à gauche du clavier). Étant donné qu'il s'agit d'une simple page internet en plein écran, la touche **Esc** permet de quitter le plein écran. Il devient alors possible de fermer l'onglet (en cliquant sur la petite croix).

Gestionnaire des tâches pour fermer le navigateur

Une combinaison de touche permet dans tous les cas de reprendre la main sur son ordinateur : **Ctrl** + **Alt** + **Suppr**. Ainsi il devient possible d'accéder au gestionnaire des tâches.



“ Note

La fenêtre du gestionnaire des tâches peut être affichée directement avec le raccourci clavier suivant : **Ctrl** + **Maj** + **Esc**.

- Sans détails :
 - Le gestionnaire de tâches montre uniquement les fenêtres actives.
- Avec détails :
 - Le gestionnaire de tâches montre les fenêtres actives ;
 - Les tâches actives dites « tâches de fond » (même sans action de notre part, l'ordinateur exécute des opérations : vérification des mises à jour, gestion de l'heure, affichage de l'écran, etc.).

Processus						
Performance						
Historique des applications						
Démarrage						
Utilisateurs						
Détails						
Services						
Nom	Statut	4% Processeur	47% Mémoire	0% Disque	0% Réseau	P
Applications (8)						
> Explorateur Windows (3)		0%	71,3 Mo	0 Mo/s	0 Mbits/s	
> Firefox (15)		2,6%	2 891,6 Mo	0,1 Mo/s	0,1 Mbits/s	
> Gestionnaire des tâches		0%	25,1 Mo	0 Mo/s	0 Mbits/s	
> IrfanView 64-bit		0%	1,3 Mo	0,1 Mo/s	0 Mbits/s	
> KeePassXC		0%	4,2 Mo	0 Mo/s	0 Mbits/s	
> LibreOffice		0%	179,1 Mo	0 Mo/s	0 Mbits/s	
> Thunderbird (2)		0%	342,3 Mo	0 Mo/s	0 Mbits/s	
> VSCodium (2)		0,1%	16,7 Mo	0 Mo/s	0 Mbits/s	
Processus en arrière-plan (75)						
> Adobe Acrobat Update Service (...)		0%	0,1 Mo	0 Mo/s	0 Mbits/s	
? Aide et support Microsoft		0%	0,5 Mo	0 Mo/s	0 Mbits/s	
AMD External Events Client Mo...		0%	0,8 Mo	0 Mo/s	0 Mbits/s	

Moins de détails

Fin de tâche

Il faut sélectionner le navigateur internet et cliquer sur « Fin de tâche ». Le navigateur va ensuite être arrêté de force.

Note

Ensuite, il est fort probable qu'à la réouverture du navigateur, il propose de rouvrir les précédents onglets : il faut refuser. Sans quoi la page de fausse demande d'assistance va se relancer.

Éteindre l'ordinateur

Comme dans tous les cas de figures envisageables, il est possible de forcer l'extinction de l'ordinateur. Tout comme dans la méthode précédente, la réouverture du navigateur proposera peut-être de reprendre les onglets de la navigation précédente : il faut refuser pour ne pas retourner sur la même page.

💡 Astuce

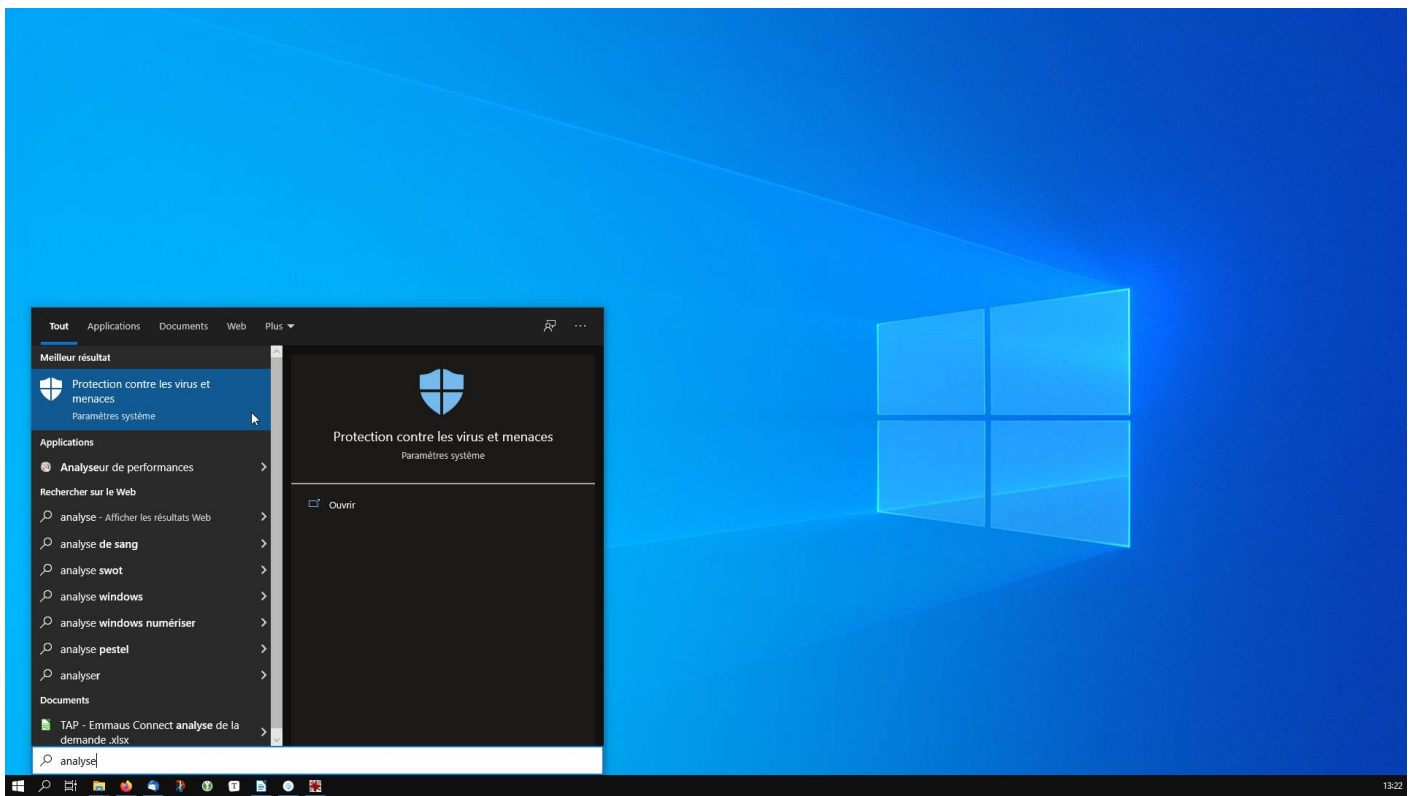
Pour forcer l'extinction d'un ordinateur, il faut maintenir le bouton permettant de l'allumer jusqu'à ce que l'écran s'éteigne. En général, il faut au moins appuyer 5 secondes.

Et après...

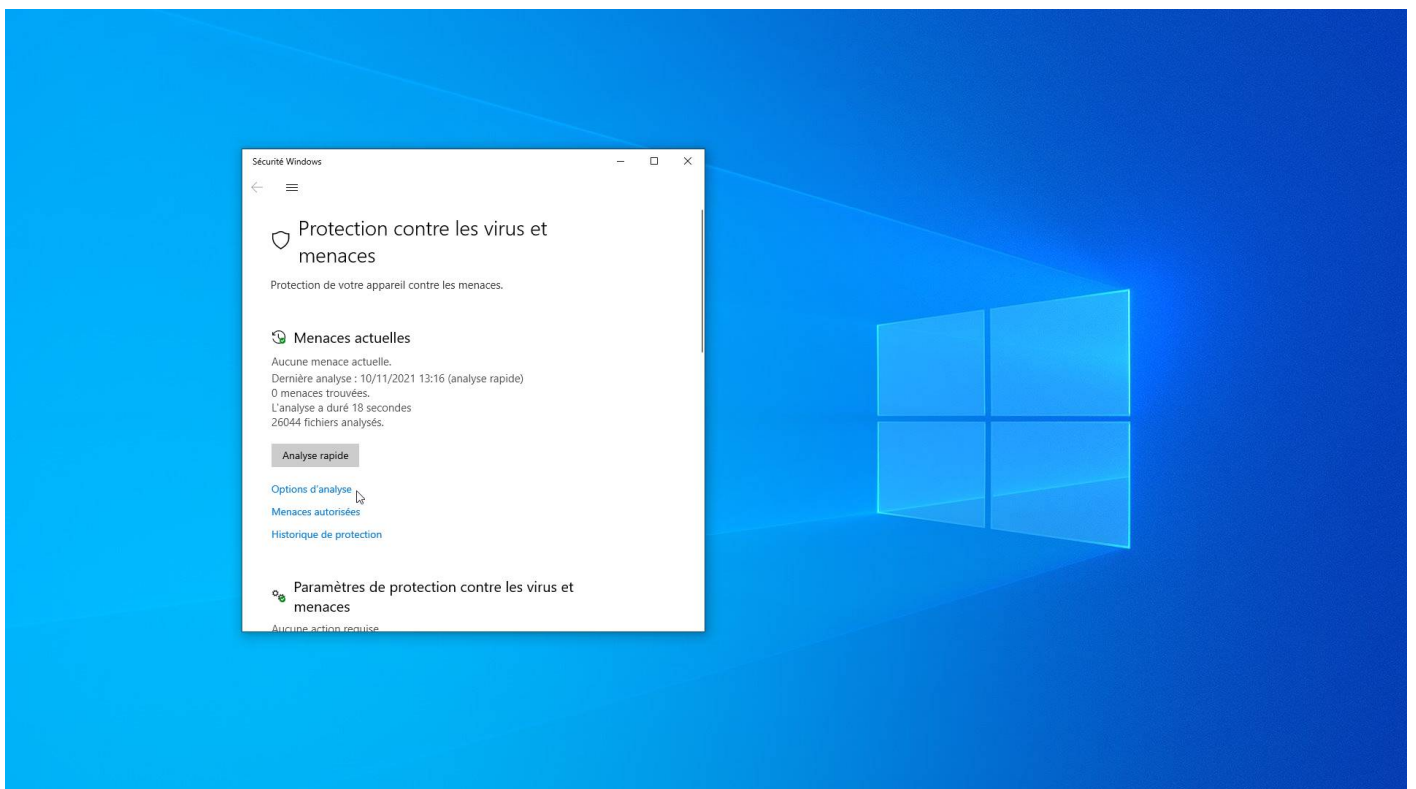
Dans tous les cas

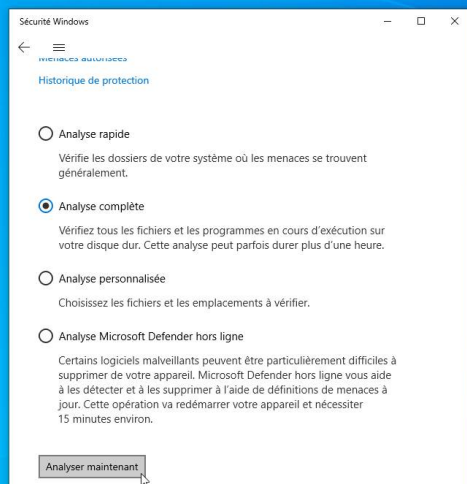
- **Nettoyer le navigateur Internet** : si le navigateur reste incontrôlable (affichage intempestif de fenêtres, navigation impossible, etc.), purger le cache, supprimer les cookies, réinitialiser les paramètres par défaut et, si cela ne suffit pas, supprimer et recréer un profil.
- **Désinstaller toute nouvelle application qui semblerait suspecte** : vérifier qu'aucune nouvelle application suspecte n'est présente sur l'appareil et, si c'est le cas, la désinstaller.
- **Faire une analyse antivirus complète de l'appareil** : réaliser une analyse approfondie (scan) de l'appareil avec un antivirus. Au préalable, ne pas oublier de le mettre à jour.

L'outil d'analyse complète intégré dans *Windows 10* se trouve, par exemple, en cherchant « analyse » dans la recherche de la barre des tâches.



Ensuite, il faut cliquer sur « Options d'analyse » afin de révéler l'analyse complète. L'analyse dure longtemps, il est préférable de laisser l'ordinateur libre pendant ce temps.





“ Note

Si vous rencontrez des difficultés pour réaliser ces opérations, renseignez-vous auprès de professionnels, de sites Internet spécialisés ou du site Internet de l'éditeur de votre navigateur.

En cas d'appel

- **Désinstaller le programme de gestion à distance et changer les mots de passe.**
Si un faux technicien a pris le contrôle de la machine, désinstaller le programme de gestion à distance, et changer tous les mots de passe.
- **Faire opposition et demander le remboursement :** si des coordonnées bancaires ou numéro de carte de crédit ont été transmis, faire opposition sans délai auprès de l'organisme bancaire ou financier. Si un paiement est débité sur le compte, exiger le remboursement auprès du faux support en précisant qu'un dépôt de plainte s'ensuivra le cas échéant.
- **Signaler les faits sur la plateforme PHAROS du ministère de l'Intérieur :**
www.internet-signalement.gouv.fr.
- **Déposer plainte** au commissariat de police ou à la brigade de gendarmerie en fournissant toutes les preuves disponibles.

Mode opératoire

Adresse internet ressemblante

Les malfaiteurs comptent sur une erreur de typographie. Cette pratique n'est pas la plus courante, cependant elle a des avantages comme la possibilité d'avoir un certificat en règle (le petit cadenas ⓘ), mais aussi d'hameçonner facilement à travers un e-mail.

- gooogle.fr..... *au-lieu de*..... google.fr
- impots-gouv.fr..... *au-lieu de*..... impots.gouv.fr

(Ces exemples ne sont qu'à titre informatif.)

Insertion dans le site consulté

Le site en cours de consultation a été infiltré par un malfaiteur. Il a détourné un lien du site d'origine pour afficher sa page de fausse attaque.

Il y a aussi la possibilité que le site consulté soit de connivence avec le malfaiteur. Ainsi il redirigerait occasionnellement des visiteurs vers la page de son complice.

DNS menteur

“ Comment fonctionnent les adresses internet :

Les ordinateurs communiquent entre eux grâce aux adresses IP.

Il s'agit d'une suite de chiffre (exemple : l'adresse IP de google.com est 142.250.81.228).

À l'image des annuaires téléphonique, le DNS permet de transformer les adresses internet, comme nous les connaissons, en suite de chiffres que les ordinateurs en réseau comprennent.

La modification de la requête DNS, intercepte la demande pour fournir une autre réponse. On dit qu'il s'agit d'un DNS menteur.

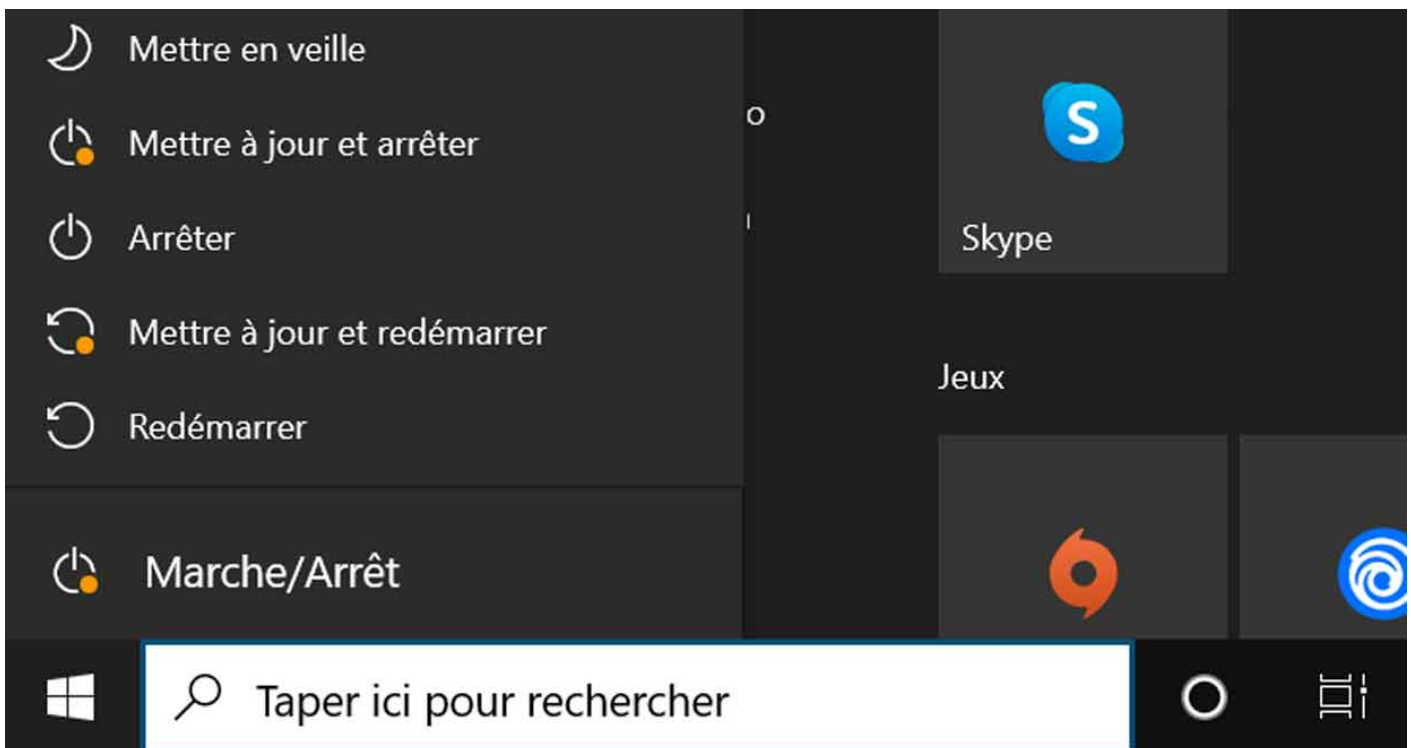
Pratique relativement simple à mettre en place, surtout dans un réseau public (du type gare, aéroport, restaurant, etc.). C'est pourquoi il faut être particulièrement vigilant dans l'utilisation d'un réseau ouvert.

Précaution à prendre

Faire les mises à jour

Microsoft Windows

Microsoft Windows gère le téléchargement des mises à jour automatiquement, cependant il faut les appliquer lorsque l'on éteint l'ordinateur.



De plus, il est nécessaire d'utiliser une version de *Microsoft Windows* dont le support des mises à jour est actif :

- *Windows 7* ne reçoit plus de mises à jour de sécurité depuis le 14 janvier 2020.
- *Windows 10* sera supporté jusqu'au 14 octobre 2025.

Le navigateur Internet

Les navigateurs internet modernes téléchargent généralement eux-mêmes leurs mises à jour. Ils les appliquent ensuite automatiquement lors de leur redémarrage.

Depuis 2019, **Microsoft** lui-même conseille de ne plus utiliser *Microsoft Internet Explorer* (dernière version : 11), en plus de ne pas être performant et de souffrir de vulnérabilités de sécurité, il ne sera plus suivi par *Microsoft* à partir du 15 juin 2022.

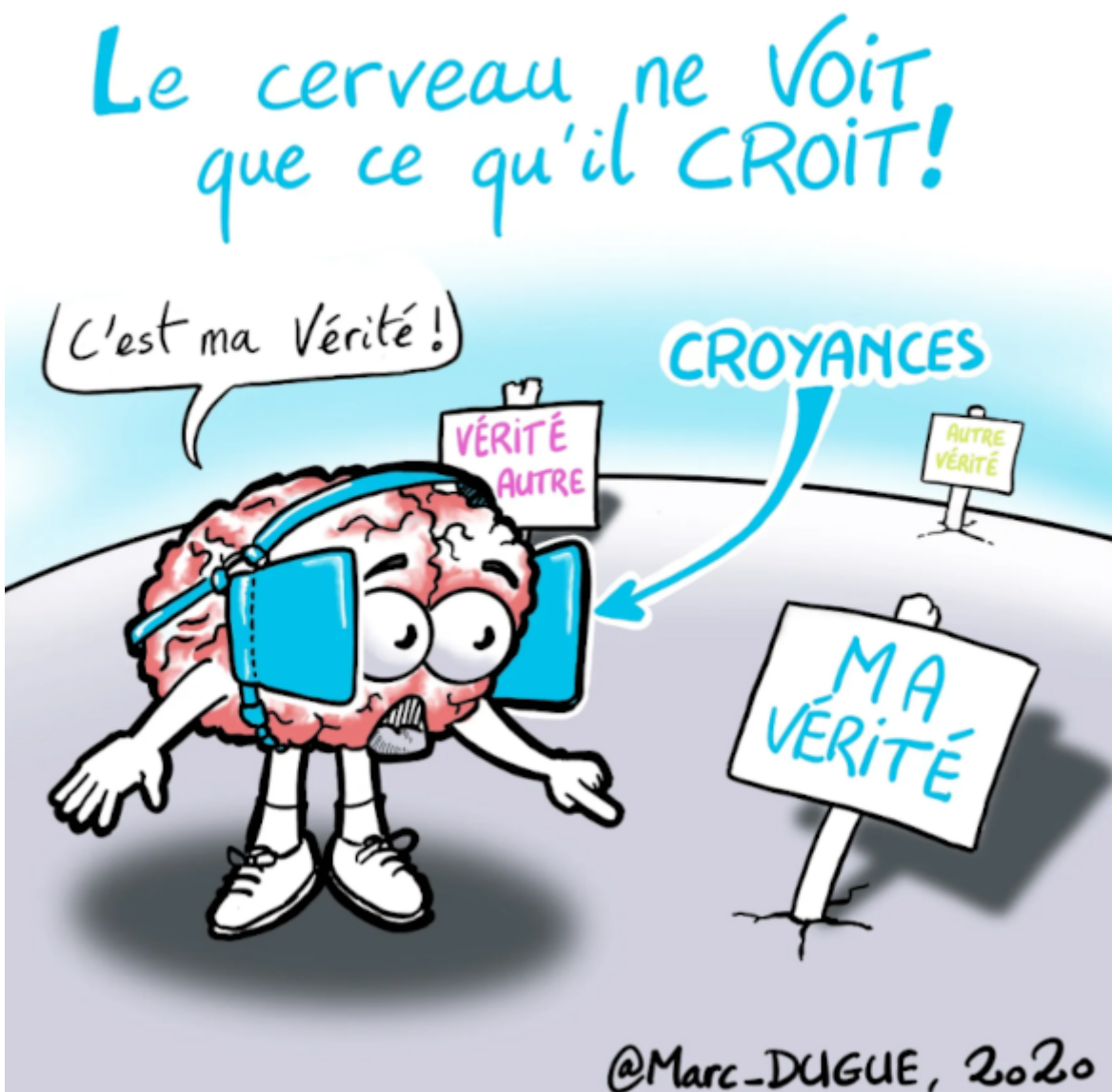
Les navigateurs modernes les plus courants sont, entre autres :

- Mozilla Firefox
- Safari
- Microsoft Edge
- Google Chrome
- Chromium
- Opera

Douter de ce que l'on voit

Ce n'est pas parce qu'ils disposent d'information, comme la localisation (plus ou moins précise), le fournisseur d'accès internet, le dernier site consulté, ou autres informations, qu'ils sont légitimes.

« *Le cerveau ne voit que ce qu'il croit !* », en l'occurrence si l'on pense être face à une attaque informatique, l'on va être convaincu que c'est bel et bien le cas.



Sur Internet...

... il ne faut pas croire ce que l'on voit !

Faire attention aux pages que l'on consulte

Lien dans les e-mails

Provenance suspecte

Ne pas cliquer sur les liens contenus dans un e-mail dont la provenance est suspecte.

Personne connue

Cependant, il faut également se méfier d'un e-mail reçu de personnes connues, surtout si celui-ci diffère des échanges habituels. La personne peut très bien s'être faite subtiliser ses identifiants, dans ce cas, sa boîte de messagerie peut avoir été piratée.

Organisme officiel

Un e-mail peut très bien se faire passer pour un message officiel. Il peut reprendre les codes graphiques (c'est-à-dire le jeu des couleurs, le logo) et aussi être expédié depuis une adresse e-mail qui ressemble beaucoup à une adresse officielle.

De plus, les organismes officiels (administration par exemple) ne sont pas à l'abri d'un piratage. Les serveurs informatiques du FBI (aux États-Unis) ont été infiltrés par des cybercriminels. Ils étaient en mesure d'envoyer des e-mails depuis des adresses officielles. Seul le contenu et la méfiance peuvent alerter l'utilisateur.

Site de streaming

Les sites de streaming illégaux sont souvent vecteurs de fausse page d'assistance. Le site peut avoir été piraté ou être de connivence avec les malfaiteurs.

Tout autre site

La liste des sources potentielles ne peut pas être exhaustive... Tout site Web peut être porteur de faux site d'assistance. C'est pourquoi il est important d'être au fait de cette pratique pour ne pas se laisser déstabiliser.

Faire attention aux logiciels que l'on installe

Pour télécharger un logiciel, il est vivement conseillé de se rendre sur la page officielle du programme.

“ Astuce

En cas de doute sur l'adresse internet du site officiel, utiliser le site de *Wikipédia* en renseignant le nom du logiciel voulu.

Ensuite, depuis la « carte d'identité » de l'application (encadré sur la partie droite) cliquer sur le lien correspondant au site web.

Garder son sang-froid

Toute la démarche derrière la fausse page de support technique est de stresser l'utilisateur afin qu'il perde la raison.

De plus, aucun support technique officiel ne contacte des usagers pour réclamer de l'argent.

Consulter un site de référencement des arnaques

Signal Arnaques

Il ne faut surtout pas en faire une obsession, cependant, il peut être intéressant de se tenir informé des pratiques utilisées par les malfaiteurs. Pour cela, un site communautaire recense des arnaques rencontrées sur Internet : www.signal-arnaques.com.

Cybermalveillance.gouv.fr

“ Cybermalveillance.gouv.fr...

... a pour missions d'assister les particuliers, les entreprises, les associations, les collectivités et les administrations victimes de cybermalveillance, de les informer sur les menaces numériques et les moyens de s'en protéger.

Peines encourues

L'incrimination principale qui peut être retenue est l'escroquerie. L'escroquerie est passible de :

- 5 ans d'emprisonnement ;
- 375 000 € d'amende.

Si la victime est menacée de suppression de ses fichiers ou en est victime, de tels procédés relèvent de l'extorsion de fonds. L'extorsion est passible de :

- 7 ans d'emprisonnement ;
- 100 000 € d'amende.

L'infraction d'atteinte à un système de traitement automatisé de données (STAD) pourra également être retenue. Cette infraction est passible de :

- 2 ans à 7 ans d'emprisonnement ;
- 60 000 à 300 000 € d'amende.

Pour aller plus loin

- Exemple de [faux support Microsoft Windows](#) (Lien directe avec identification incluse [ici](#)).
Attention !!! C'est une fausse page Google, ne pas ouvrir le lien en cas de doute, sinon :
 - Entrer quelques caractères dans la barre de recherche ou cliquer sur le bouton « Recherche Google » ;
 - La fausse page se lance en plein écran avec une sonnerie stressante ;
 - Presser la touche *Échappe* pour sortir du plein écran et fermer l'onglet.
- Article sur le site [Malekal.com](#) intitulé « [Arnaque support et hotline téléphonique](#) » présentant notamment différentes astuces utilisées par les malfaiteurs pour rendre la page crédible aux yeux de l'utilisateur.
- Exemples de fausses pages d'assistance Microsoft en recherchant « [scam microsoft](#) » dans un moteur de recherche.
- Exemple d'arnaque par SMS en recherchant « ["arnaque" sms](#) » dans un moteur de recherche.
- Vidéos *YouTube* de [Micode](#) « [J'ai infiltré un réseau d'arnaqueurs](#) » (83 minutes).



Révision #8

Créé 17 novembre 2021 14:07:00 par Mickaël G.

Mis à jour 9 décembre 2021 21:58:35 par Mickaël G.