

Cyberattaque

- [Hameçonnage](#)
- [Se protéger sur Internet - Arnaques aux envois de RIB par e-mail](#)
- [Se protéger sur Internet - Fausse assistance Windows : comment réagir](#)

Hameçonnage



Définition

[Wikipédia](#) :

“ L’hameçonnage (l’anglicisme *phishing* étant couramment utilisé) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance, etc. En effet, 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 où elle pensait se connecter. 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. L’attaque peut aussi être réalisée par courrier électronique ou autres moyens électroniques. Lorsque cette technique utilise les SMS pour obtenir des renseignements personnels, elle s'appelle *SMiShing*.

Exemple

À : +33 6 22 18 58 64



Message
Aujourd'hui 08:48

Il y a une mise à jour sur votre colis. Article arrêté en raison de frais de douane impayés. Résolvez-le ici: <https://bit.do/fQsyT>

Le SMS contient un lien raccourci, on ne connaît pas la réelle adresse URL de destination.

La solution pour y voir plus clair consiste à utiliser un « vérificateur » d'URL comme [CheckShortURL](#). Certains raccourcisseurs d'URL permettent également de connaître l'adresse originale, mais ce n'est pas le cas ici pour [bit.do](#).

On entre l'adresse dans le champ prévu à cette effet :

CheckShortURL

Your shortened URL expander

CheckShortURL supports almost all URL shortening services:
t.co, goo.gl, bit.ly, amzn.to, tinyurl.com, ow.ly,youtu.be and many others!

Expand

Puis on clique sur le bouton Expand :

Screenshot of the distant page behind your short URL



Le site nous révèle un aperçu (« Screenshot ») de la page distante derrière l'URL raccourcie. On y voit un logo « IPS » ressemblant volontairement à celui de « UPS »...

Se protéger sur Internet - Arnaques aux envois de RIB par e-mail

Contexte

TL DR

“ Les boîtes des victimes sont discrètement piratées et les échanges de mails contenant un RIB [sont] détournés. Un phénomène qui prend de l'ampleur avec la crise économique et le télétravail.

[Le Parisien - Site Internet - Vous envoyez vos coordonnées bancaires par mail ?](#)

[Attention à la nouvelle arnaque aux faux RIB](#)

Les attaques aux faux ordres de virement et aux changements de RIB sont dans le *top 10* des cinquante principales arnaques touchant les professionnels.

Témoignages

“ Une administratrice d'une troupe de théâtre en région parisienne sollicite sa mairie afin d'obtenir une subvention de 4 000 €. Elle leur adresse donc un e-mail auquel elle joint son RIB. La mairie recevra bien le mail, mais le RIB aura été usurpé. Françoise ne recevra jamais sa subvention.

[Le Parisien - Site Internet - Vous envoyez vos coordonnées bancaires par mail ?](#)

[Attention à la nouvelle arnaque aux faux RIB](#)

Un arboriculteur dans la Sarthe pensait régler les 3 300 € pour la réparation d'une machine. Son virement ne créditera jamais son fournisseur. La facture était bonne, mais pas le RIB.

[Que Choisir - Site Internet - Le faux RIB fait irruption dans les boîtes mail](#)

Principe de l'arnaque

Le créancier transmet son relevé d'identité bancaire sur lequel figure son nom et ses coordonnées bancaires. Cependant, avant que le débiteur prenne connaissance du RIB, une tierce personne remplace les coordonnées bancaires par des coordonnées qui le rendent bénéficiaire du futur virement.

Les noms et adresse du bénéficiaire d'origine n'ont pas besoin d'être modifiés, seules les coordonnées bancaires sont nécessaires au virement, plus précisément le code IBAN (*International Bank Account Number : Numéro de compte en banque international*) et le code BIC (*Bank Identifier Code : Code d'identification de la banque*).

RIB : Relevé d'Identité Bancaire

Identifiant national de compte bancaire - RIB

| | | | | |
|--------|---------|-------------|-----|--------|
| Banque | Guichet | N° compte | Clé | Devise |
| 00000 | 00000 | 00000000000 | 00 | EUR |

| |
|---------------------------------|
| Domiciliation |
| NOM DE L'AGENCE DE RATTACHEMENT |

Identifiant international de compte bancaire

| | | | | | | |
|------------------------------------------|------|------|------|------|------|-----|
| IBAN (International Bank Account Number) | | | | | | |
| FR00 | 0000 | 0000 | 0000 | 0000 | 0000 | 000 |

| |
|----------------------------|
| BIC (Bank Identifier Code) |
| XXXXFRXX |

Domiciliation

NOM DE L'AGENCE DE RATTACHEMENT
ADRESSE DE LA BANQUE
CODE POSTALE ET VILLE
☎ 06 00 00 00 00

Titulaire du compte (Account Owner)

PRENOM NOM
ADRESSE DU TITULAIRE
CODE POSTALE ET VILLE

Mode opératoire

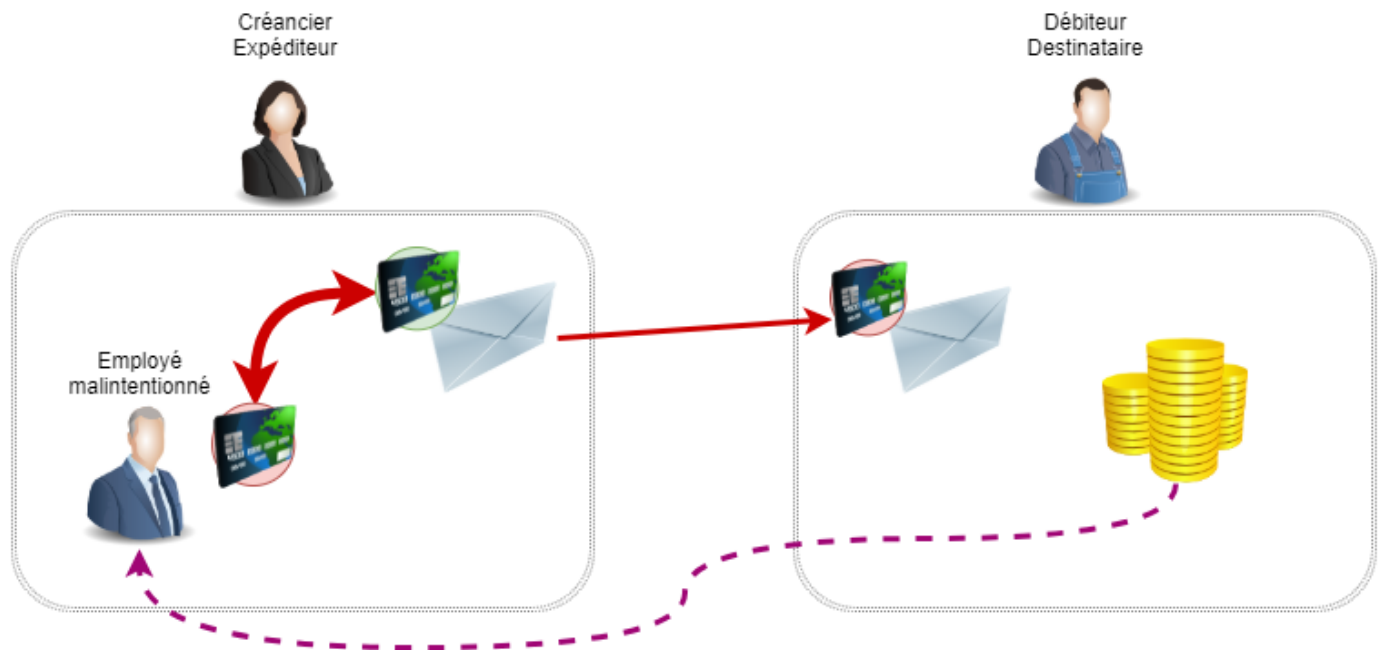
Malveillance interne

Une personne malintentionnée employée par le créancier pourrait se connecter à la messagerie de son entreprise afin de substituer le RIB original par un RIB dont il sera le bénéficiaire.

Cette procédure nécessite que l'employé ait accès à la messagerie de l'entreprise soit :

- sous un identifiant général,
- sous l'identifiant de la direction,
- ou un identifiant du service comptable.

L'identifiant désigne ici le couple « identifiant et mot de passe » du service de messagerie.



Hormis la substitution lors de l'envoi des e-mails, un employé ayant accès au serveur de stockage des données de l'entreprise pourrait substituer le RIB original par un autre dont il sera bénéficiaire.

Cybermalveillance

Côté expéditeur

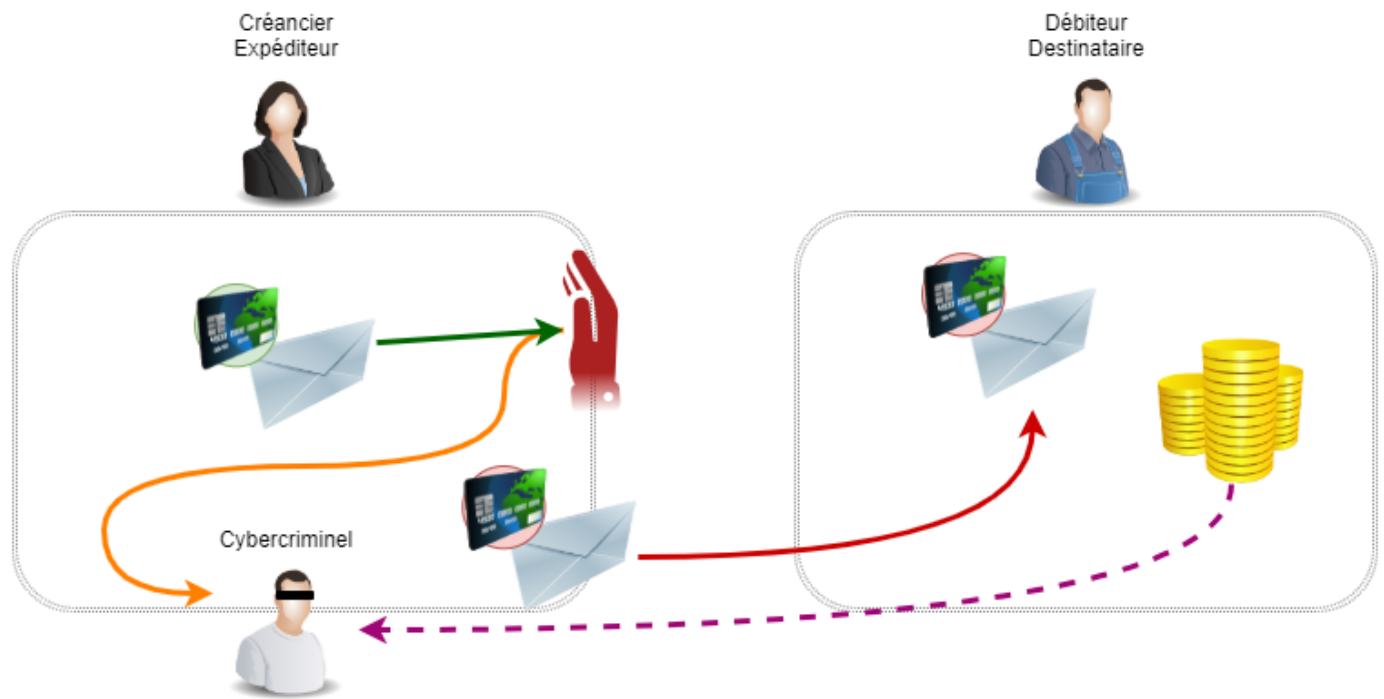
Un cybercriminel a infiltré le serveur de messagerie de l'expéditeur. Les messages contenant certains mots seront filtrés, comme :

- « RIB »,
- « Relevé d'identité bancaire »,
- « facture »...

Ce filtre aura deux fonctions :

- empêcher l'e-mail d'origine de partir ;
- informer le cybercriminel.

Ensuite, le cybercriminel substitue le RIB du créancier par le sien et transmet l'e-mail modifié au débiteur directement depuis la messagerie de l'expéditeur.



Cette approche est la plus technique à mettre en place, mais elle est aussi la plus difficile à déceler.

Côté destinataire

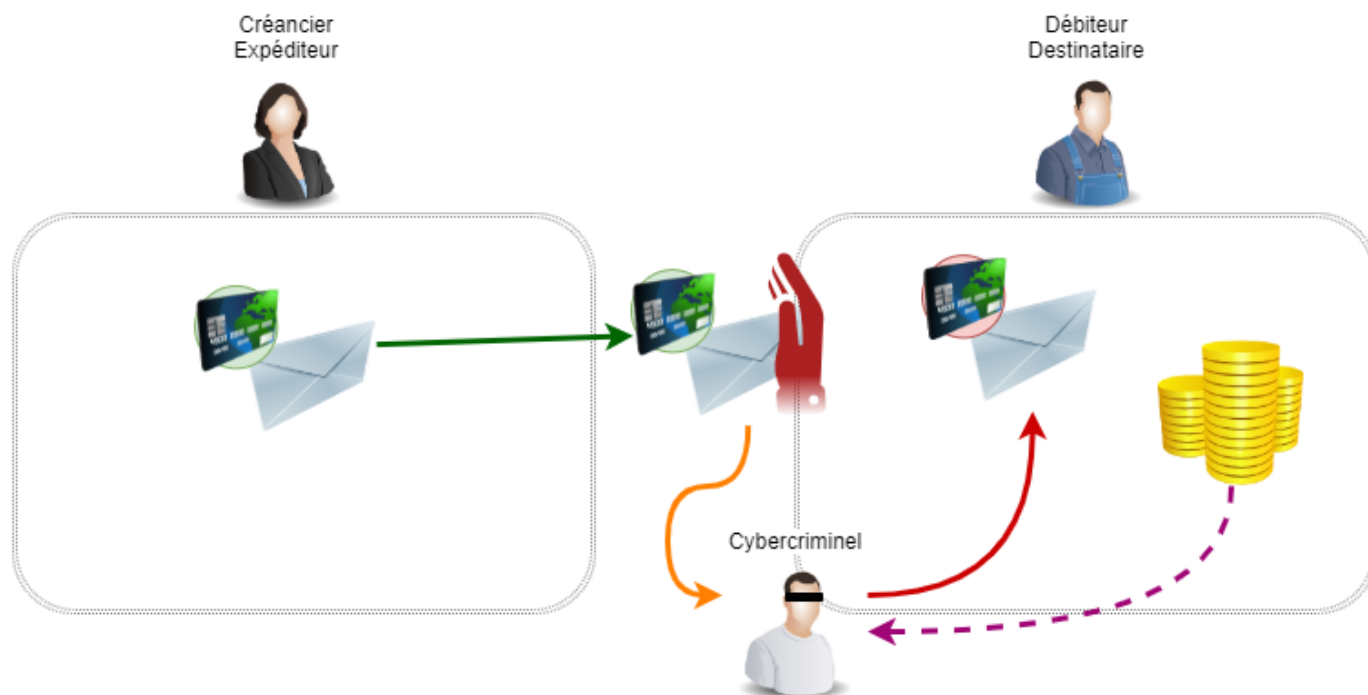
Un cybercriminel a infiltré la messagerie du destinataire. Les messages contenant certains mots seront filtrés, par exemple :

- « RIB »,
- « Relevé d'identité bancaire »,
- « facture »...

Ce filtre aura deux fonctions :

- empêcher d'être lu par le destinataire d'origine ;
- être transféré au cybercriminel.

Ensuite, le cybercriminel substitue le RIB du créancier par le sien, désactive le filtre et transmet l'e-mail modifié au débiteur.



Pour être plus crédible, le cybercriminel crée une adresse de messagerie proche de l'expéditeur d'origine. Par exemple :

- « ent.durand@gmail.com » **devient** « ent.durant@gmail.com »
- « jacques.durand@orange.fr » devient « jacques.durand@outlook.com »
- « contact@ent.durand.com » **devient** « contact.durand@orange.fr »

Cette approche est relativement simple à mettre en place. Le cybercriminel a besoin de disposer des identifiant et mot de passe de la messagerie internet du destinataire.

La finalité

Quel que soit le mode opératoire, la finalité reste la même : le compte bancaire de la personne malintentionnée est crédité et non celui du créancier. Le cybercriminel aura pris les dispositions afin de ne pas être identifiée (avec notamment un compte bancaire domicilié dans un pays étranger).

L'argent détourné est rapidement transféré, voire le compte bancaire frauduleux clôturé rendant impossible tout rappel de fond. Les chances de récupérer l'argent dérobé sont quasiment nulles.

“ Pour information

Les assurances ne couvrent pas ce désagrément, estimant qu'il s'agit d'un acte volontaire suite à une erreur de l'utilisateur, une négligence.

Précautions à prendre

Contexte de la requête

Tout comme dans l'arnaque au « faux président » ou « au prêt d'argent », il ne faut pas céder au chantage émotionnel et à l'urgence.

Le mail frauduleux peut faire mention de la nécessité de faire le virement au plus vite. Ce caractère d'urgence peut être accentué par un message expliquant que l'entreprise traverse des difficultés suite à un mauvais concours de circonstances. Sans ce règlement dans les meilleurs délais, l'entreprise devra, par exemple, se séparer de salariés.

Simple vérification du RIB

Une simple vérification du relevé d'identité bancaire peut mettre en déroute l'arnaque :

“ Votre plombier a rarement une banque basée aux îles Caïman.

[Jean-Jacques Latour – Responsable de l'expertise en cybersécurité à Cybermalveillance.gouv.fr](#)

Cette information se retrouve notamment dans le code BIC : xxxxFRxx.

Double vérification du RIB

Ce conseil peut sembler contraignant à l'air de la communication dite asynchrone (la discussion n'est pas directe mais lorsque les interlocuteurs sont disposés à répondre). Cependant, elle reste la première étape pour déceler avec certitude une tentative d'arnaque :

- Procéder à une double vérification des coordonnées bancaires par un autre moyen de communication, idéalement un échange téléphonique.

Double authentification de sa messagerie Internet

Le double authentification permet de s'assurer qu'une nouvelle connexion à son service de messagerie est bien volontaire.

Cette vérification peut se faire sous plusieurs formes :

- Envoi d'un code temporaire par SMS ;
- Authentification à deux facteurs (« **2FA** »).

Outre le fait d'en avoir connaissance, la configuration de cette sécurité nécessite une aisance relative avec les outils numériques. Comme beaucoup de mesures de sécurité, la double authentification n'a pas pour vocation à faciliter le quotidien de l'utilisateur, mais bel et bien de dissuader les personnes malintentionnées : la sécurité numérique passe souvent par une contrainte additionnelle.

“ Analogie

Nous fermons la porte de nos maisons à clef lorsque nous nous absentons. Cette contrainte est devenue un automatisme afin de sécuriser nos biens domestiques.

Gestion des mots de passe

Comme tout mot de passe, il est vivement conseillé d'utiliser un mot de passe dit « robuste ». Il s'agit d'un mot de passe :

- relativement long (au moins une dizaine de caractères),
- comportant des caractères variés (lettres minuscules, majuscules, nombres, caractères spéciaux),
- n'ayant pas de logique particulière (base commune suivi de caractères variants suivant le site),
- unique (ne pas réutiliser ses mots de passes).

“ Analogie

Les clefs de notre quotidien en plus d'être toutes différentes (maison, voiture, boîtes aux lettres, etc.) sont également complexes, voire non-reproductibles.

L'utilisation d'un gestionnaire de mots de passe est recommandé. Cependant, son usage nécessite une période d'apprentissage qui peut dissuader les utilisateurs.

Peines encourues

Pour information, le cybercriminel encoure de nombreuses peines :

- Poursuites pour escroquerie :

- cinq années de prison,
 - 375 000 € d'amende ;
 - Usurpation d'identité :
 - un an de prison,
 - 15 000 € d'amende ;
 - Accès frauduleux à un système de traitement de données :
 - deux ans de prison
 - 60 000 € d'amende.
-



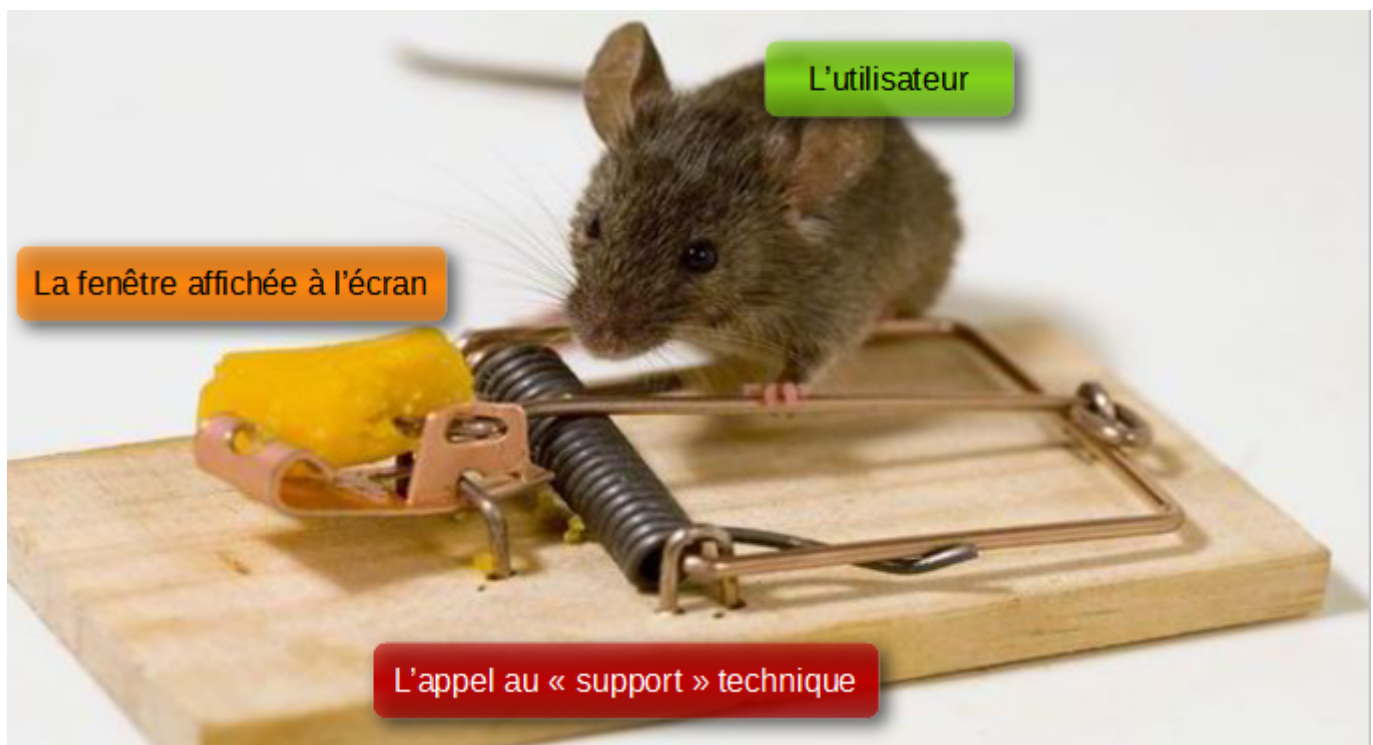
Se protéger sur Internet - Fausse assistance Windows : comment réagir

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 :**

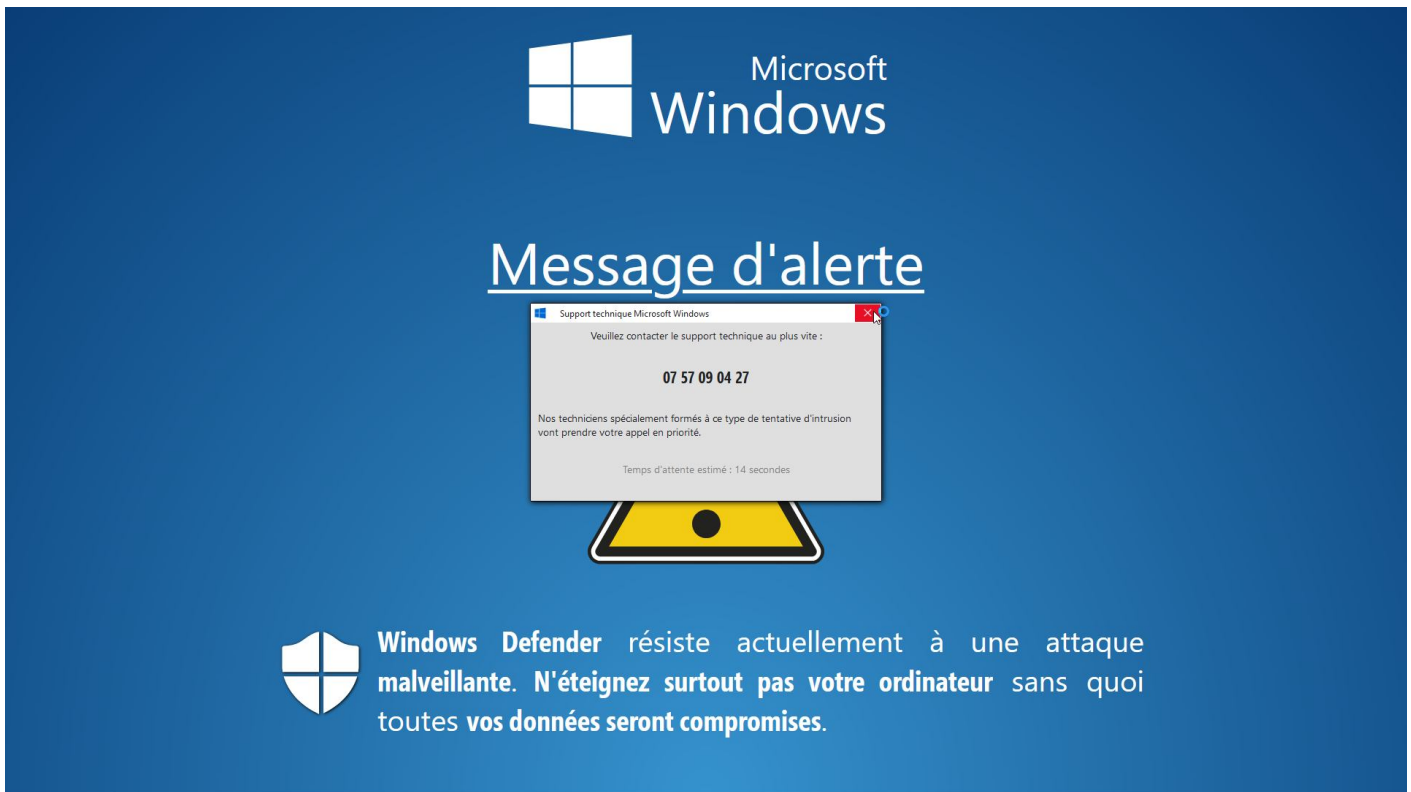
Soutirer de l'argent à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

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



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**.

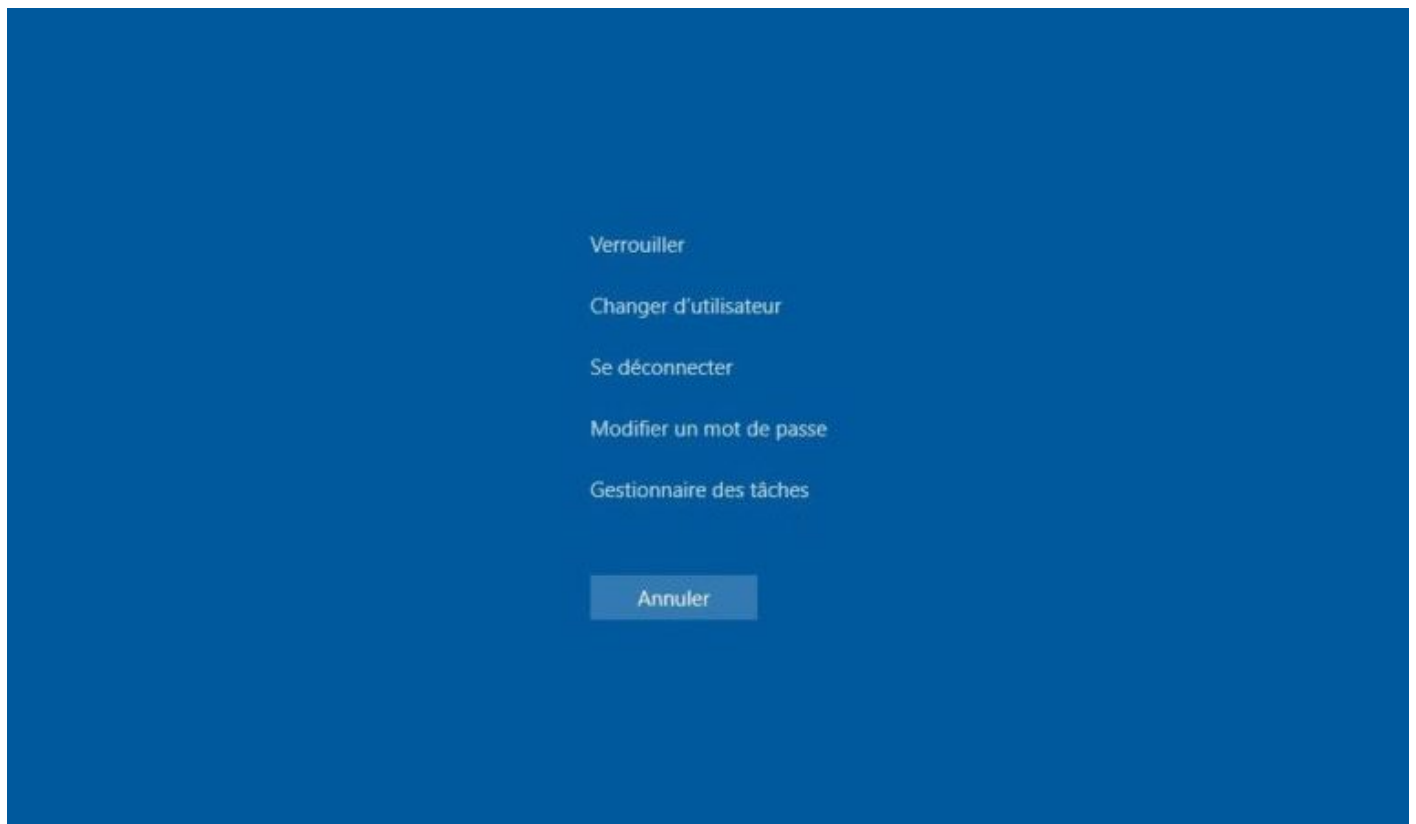
La page est instantanément fermée, dans le cas où il s'agit d'un unique onglet, le navigateur complet est fermé.

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

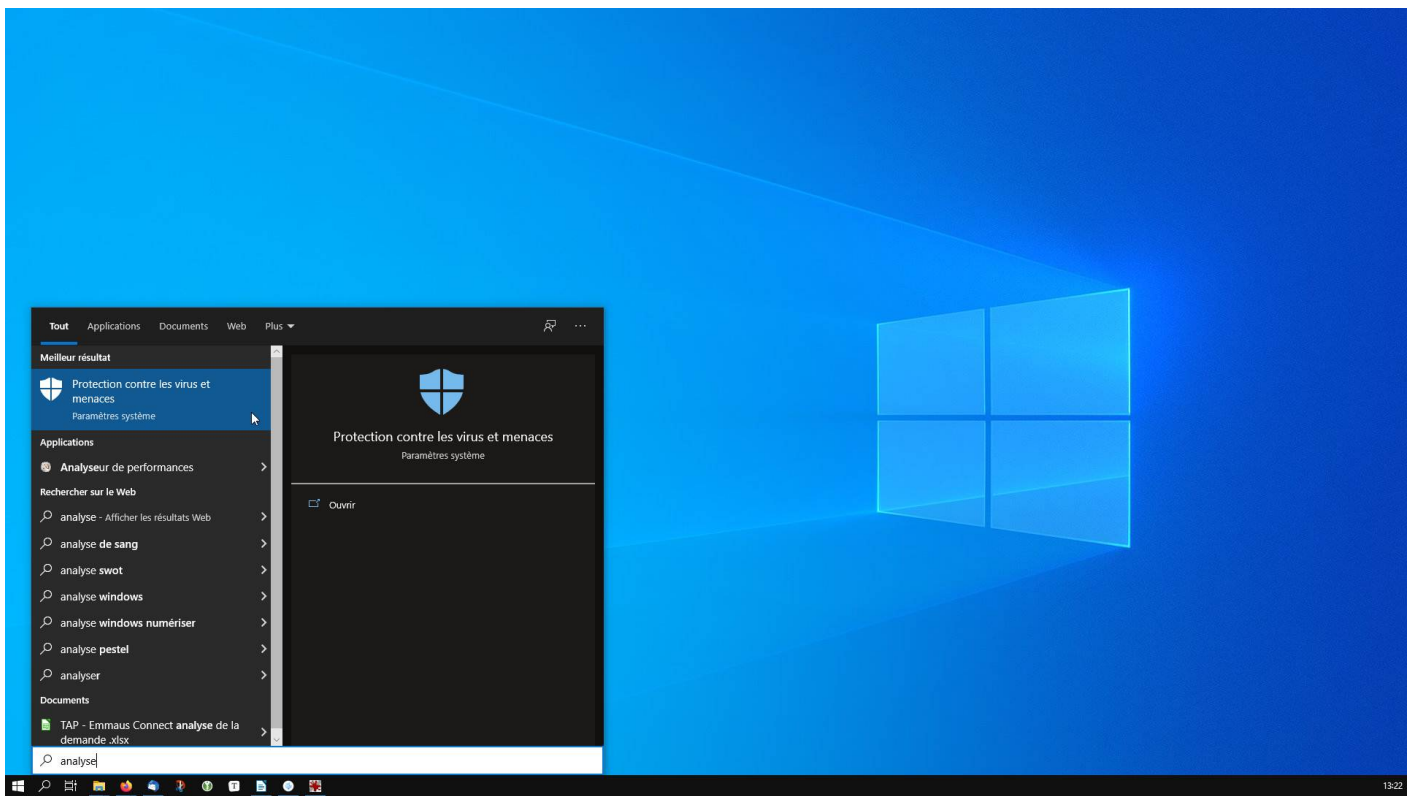
Pour forcer l'extinction d'un ordinateur, il faut maintenir le bouton permettant de l'allumer jusqu'à ce que l'écran s'éteigne. En général, il faut au moins appuyer 5 secondes.

Et après...

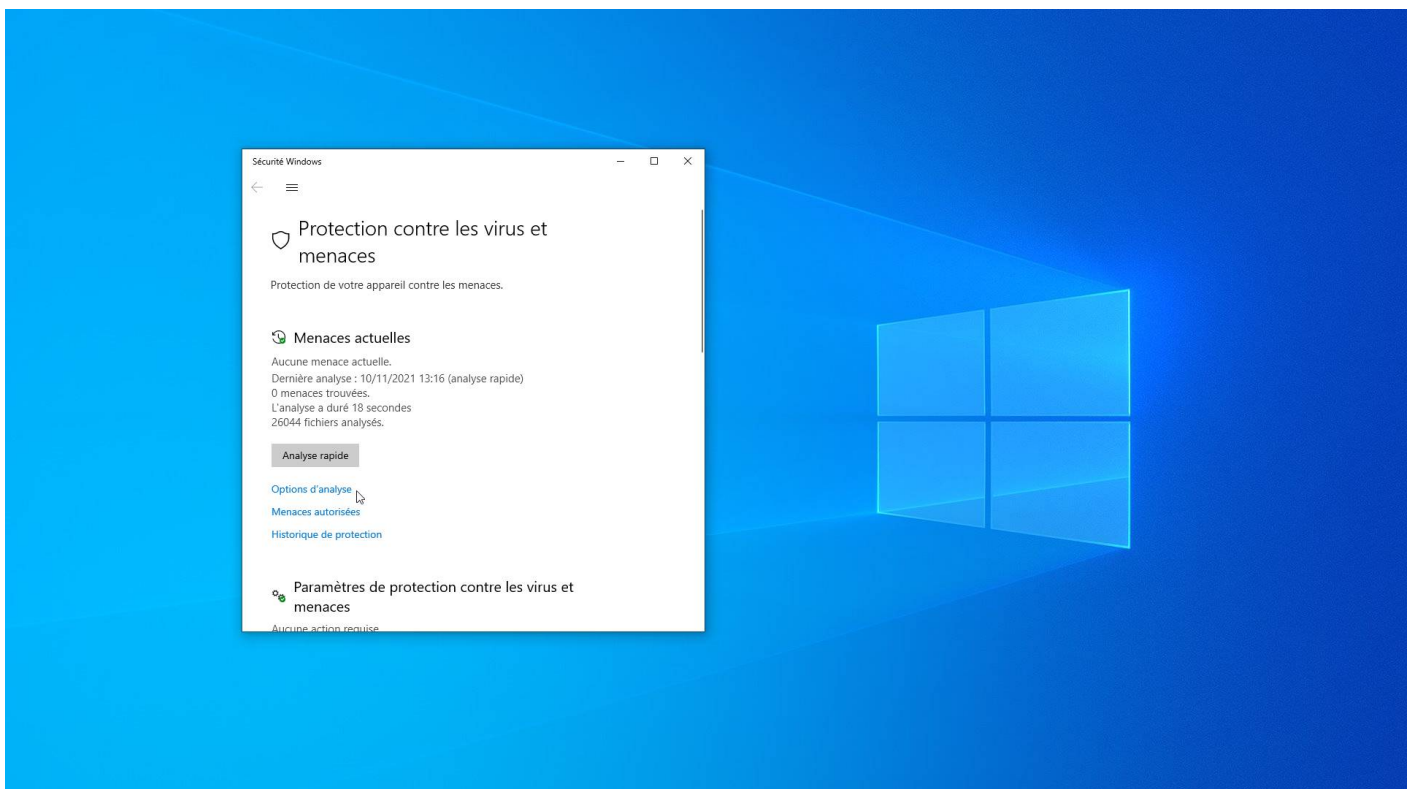
Dans tous les cas

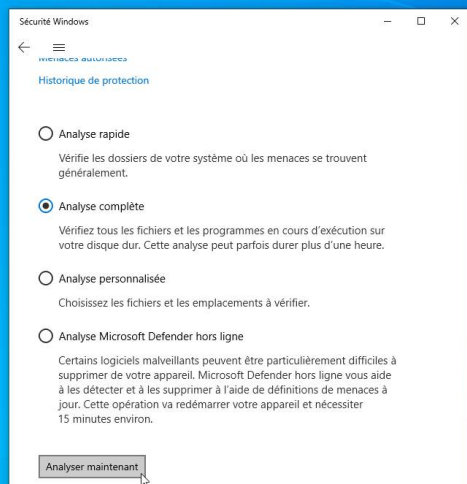
- **Nettoyer le navigateur Internet** : si le navigateur reste incontrôlable (affichage intempestif de fenêtres, navigation impossible, etc.), purger le cache, supprimer les cookies, réinitialiser les paramètres par défaut et, si cela ne suffit pas, supprimer et recréer un profil.
- **Désinstaller toute 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.

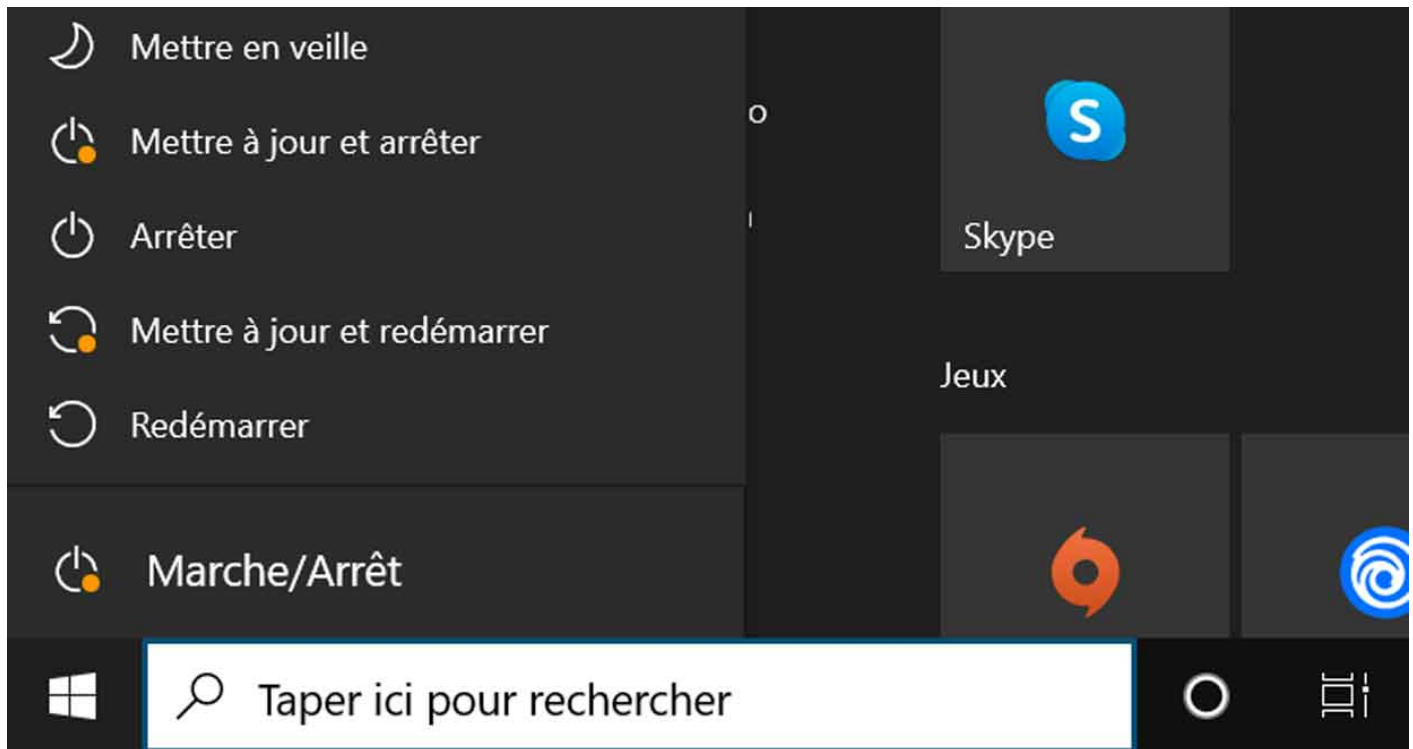
Pratique relativement simple à mettre en place, surtout dans un réseau public (du type gare, aéroport, restaurant, etc.). C'est pourquoi il faut être particulièrement vigilant dans l'utilisation d'un réseau ouvert.

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 :

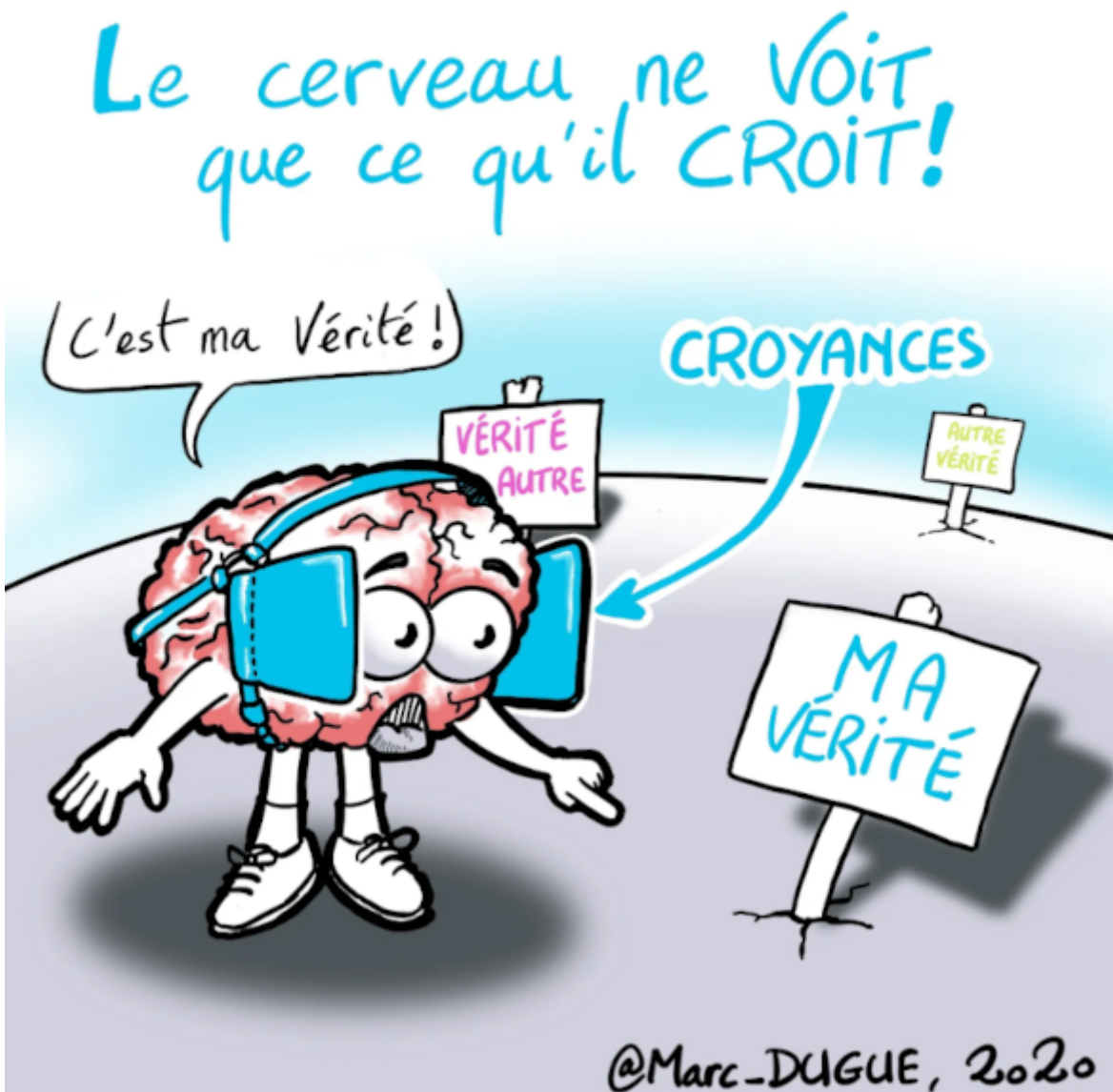
- *Mozilla Firefox*
- *Safari*
- *Microsoft Edge*
- *Google Chrome*

- 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).

