Si on regarde la définition de « antivirus » sur Wikipédia, on nous indique « Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique1 ne sont qu'une catégorie). Ces derniers peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de logiciels modifiant ou supprimant des fichiers, que ce soit des documents de l'utilisateur stockés sur l'ordinateur infecté, ou des fichiers nécessaires au bon fonctionnement de l'ordinateur »

Je ne rentrerais évidemment pas dans les détails du fonctionnement de ce logiciel indispensable, mais je me bornerais ici, à vous donner certaines solutions si vous n'êtes pas encore équipé d'un solution fiable et à vous rappelez que vous devez disposer d'une solution de ce genre sur votre ordinateur.

Les campagnes d'hameçonnage par mail[1], les rançongiciels[2] les sites internets sur lequel on trouvera des chevaux de Troie, ou encore les virus de type vers[3] sont de plus en plus courante. Ne négligez donc pas cette aspect. Une simple clé USB connecté sur un pc infecté peut propager rapidement par un réseau domestique ou professionnel un virus bien conçu si celle si n'est pas désinfecté par une solution de sécurité à jour.

Donc voici une petite sélection d'outils de sécurité à installer en plus d'un ordinateur dont les mise à jour sont faites régulièrement.

1 L'hameçonnage (phishing) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels souvent par mail dans le but de perpétrer une usurpation d'identité.

2 Le ransomware (ou rançongiciel) est un type de logiciel malveillant qui empêche l'utilisateur d'accéder au système ou à ses fichiers personnels en les chiffrant et qui exige le paiement d'une rançon en échange du rétablissement de l'accès.

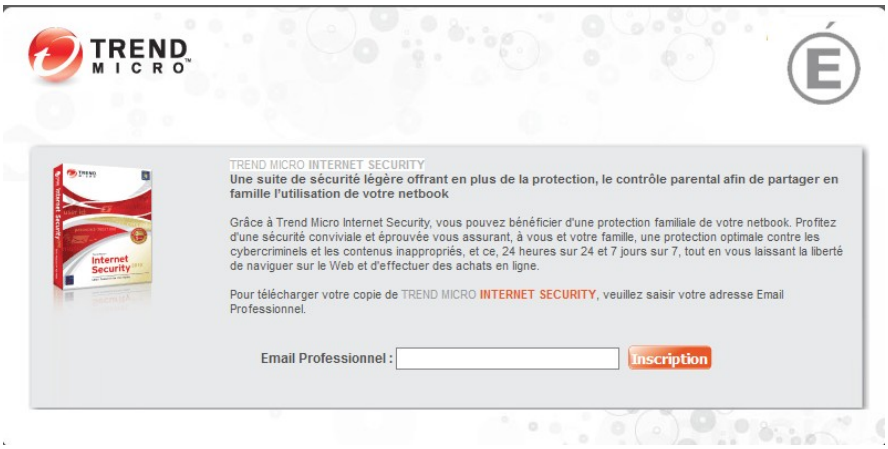
3 Les virus-vers, sont des virus classiques car ils utilisent un programme hôte. Cependant, ils s'apparentent aux vers « worm » car leur mode de propagation est lié au réseau, comme des vers, en général via l'exploitation de failles de sécurité et leur action se veut discrète, et non destructrice pour les utilisateurs de la machine infectée.

Pré-ambule

https://www.av-comparatives.org/consumer/
Un site intéressant pour vous informer sur les différentes solutions du marché, malheureusement en anglais uniquement, mais si vous souhaitez connaître l'efficacité de votre solution actuelle ou pressentie, c'est l'endroit adapté. On y teste une bonne partie des antivirus gratuits ou payants sous tous les aspects : Protection en temps réel (en continu), anti-phishing (antihameçonnage), d'un point de vue des performances...

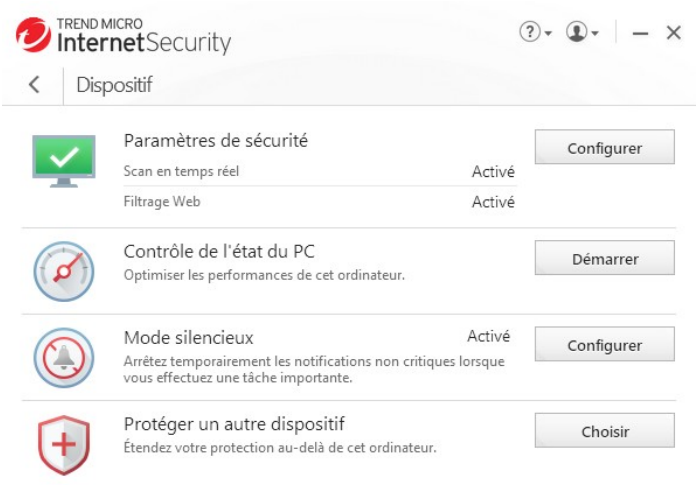
La lutte contre les virus

1 / TREND MICRO **INTERNET SECURITY** (Windows – macOS – ~~Linux~~) – Gratuit – Non libre
Ce n'est pas forcement le meilleur du marché mais c'est malgré tout une excellente solution que celle proposée par l'éducation nationale dans le cadre d'un marché avec la société Trend Micro. Vous avez ainsi accès gratuitement à la suite de sécurité TREND MICRO **INTERNET SECURITY** 16 en vous inscrivant à partir de ce lien et en saisissant votre adresse mail professionnelle. Vous recevrez ainsi, le numéro de licence, le lien vers l'installeur (Windows et macOS) et le lien du document utilisateur.



C'est la solution que j'utilise actuellement depuis deux ans.

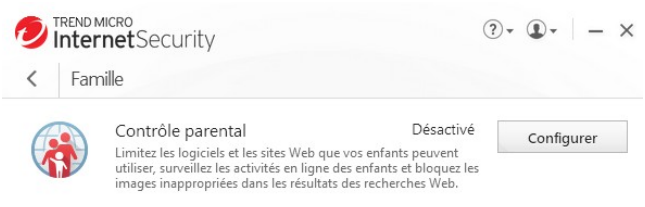
Il possède toutes les fonctionnalités pour vous protéger de la plupart des situations
_ scan en temps réel (s'effectue en tâche de fond pendant que vous utilisez votre ordinateur ;
_ protection Web au moyen d'une extension au sein de votre navigateur préféré (Chrome, Firefox, Edge)
_ protection jusqu'à 3 ordinateurs, utile pour protéger celui des autres membres de la famille



_ protection de vos paiements internet,
_ protection de vos données personnelles,

_ protection contre les rançongiciels,
_ effacement sécurisé de vos données personnelles

_ protection des enfants au moyen d'un contrôle parental.



Je n'ai pas d'action chez Trend Micro, mais c'est une excellente solution, le meilleur rapport qualité / prix !

2 / Microsoft Defender (Windows – ~~macOS~~ – ~~Linux~~) – Gratuit – Non libre
C'est la solution installer par défaut sur les ordinateurs équipés de Microsoft Windows 10. Il est généralement bien coté dans les comparatifs et propose également de multiples moyens de protection sans atteindre ceux de la solution précédente. Mais il peut tout à fait s'avérer suffisant pour celles et ceux qui ne veulent pas se prendre la tête. Les mises à jour sont régulièrement et le paramétrage par défaut est bien fait.

3 / Il existe bien évidemment de multiples autres solutions, je n'en retiendrais que quelques-unes pour les avoir testés. Sachez tout de même que les solutions gratuites sont très fiables, leur seul défaut, un peu de publicité pour vous poussez vers la solution payante, c'est un moindre mal mais qui peut être pénible à la longue.

_ Kaspersky qui propose une solution gratuite et une payante reste l'une des meilleures solutions du marché.
_ Avast qui propose une solution gratuite et une payante

La lutte contre les logiciels malveillants

Dans une catégorie un peu différente des virus, on trouve les logiciels malveillants tels que les Chevaux de Troie[4] ou les logiciels espions[5], ou encore les Adwares[6].
Les logiciels antivirus tel que ceux cités si dessus permettent une protection plus ou moins complètent, mais pas efficace à 100 %, c'est le minimum syndical !
Devant cette autre forme de menace, certains éditeurs ont développé des solutions à installer en complément d'un antivirus ou bien en cas de besoin avéré.

1 / Malwarebytes (Windows – macOS – ~~Linux~~) – Gratuit – Non libre
C'est le plus connu et l'un des plus efficaces, depuis la version 3 il peut même faire office d'antivirus et devenir donc une solution tout-en-un. Il existe une version gratuite et une version payante.
La version gratuite doit être démarrée manuellement, tandis que la version payante planifie automatiquement des scans. La version payante ajoute également une protection en temps réel, des blocages basés sur l'IP pour empêcher l'accès à des sites malveillants et le déclenchement de logiciels malveillants par Flash7.

C'est une solution que je préconise en cas de toutes quant à une infection, souvent visible au sein du navigateur (ouverture de pages non voulues) ou encore en cas de ralentissement important de votre ordinateur du jour au lendemain à cause d'une application.
Le logiciel est simple à prendre en main et en français, on installe, on scanne, et on nettoie en fonction des recommandations.

4 Un cheval de Troie (Trojan horse en anglais) est un type de logiciel malveillant, qui ne doit pas être confondu avec les virus ou autres parasites. Le cheval de Troie est un logiciel en apparence légitime, mais qui contient une fonctionnalité malveillante. Son but est de faire entrer cette fonctionnalité malveillante sur l'ordinateur et de l'installer à l'insu de l'utilisateur.
5 Un logiciel espion, un mouchard ou un espiogiciel (spyware) est un logiciel malveillant qui s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.
6 Un adware, logiciel publicitaire ou publiciel est un logiciel qui affiche de la publicité lors de son utilisation.
Un logiciel publicitaire contient habituellement deux parties, une partie utile (le plus souvent un jeu vidéo ou un utilitaire) qui incite un utilisateur à l'installer sur son ordinateur, une partie qui gère l'affichage de la publicité.

2/ d’autres solutions existent :
_ Malwarebytes AdwCleaners contre les adwares (Gratuit, non libre et uniquement pour Windows)
_ Spybot (Payant, non libre et uniquement pour Windows)

Conclusion

Pour conclure, je l’ai déjà dit mais une seule solution ne vous protège pas de toutes les menaces, cependant, une bonne hygiène informatique[7] et une bonne solution antivirus telle que celle que propose l’éducation nationale devrait vous permettre d’éviter les déconvenues.

L’antivirus fait donc partie d’un ensemble, une brique qu’il ne faut pas négliger mais qui seul ne vous protégera pas. Les bonnes pratiques de sécurité numériques, telles qu’un bon mot de passe changer régulièrement, permettent de vous prémunir de certaines menaces.

Je poursuivrais donc dans les semaines à venir dans ce domaine pour vous aider à vous protéger, quel que soit votre outil de communication.

7 La notion d'hygiène informatique désigne l'ensemble des bonnes pratiques que chaque personne ayant besoin d'utiliser de l'informatique devrait respecter