

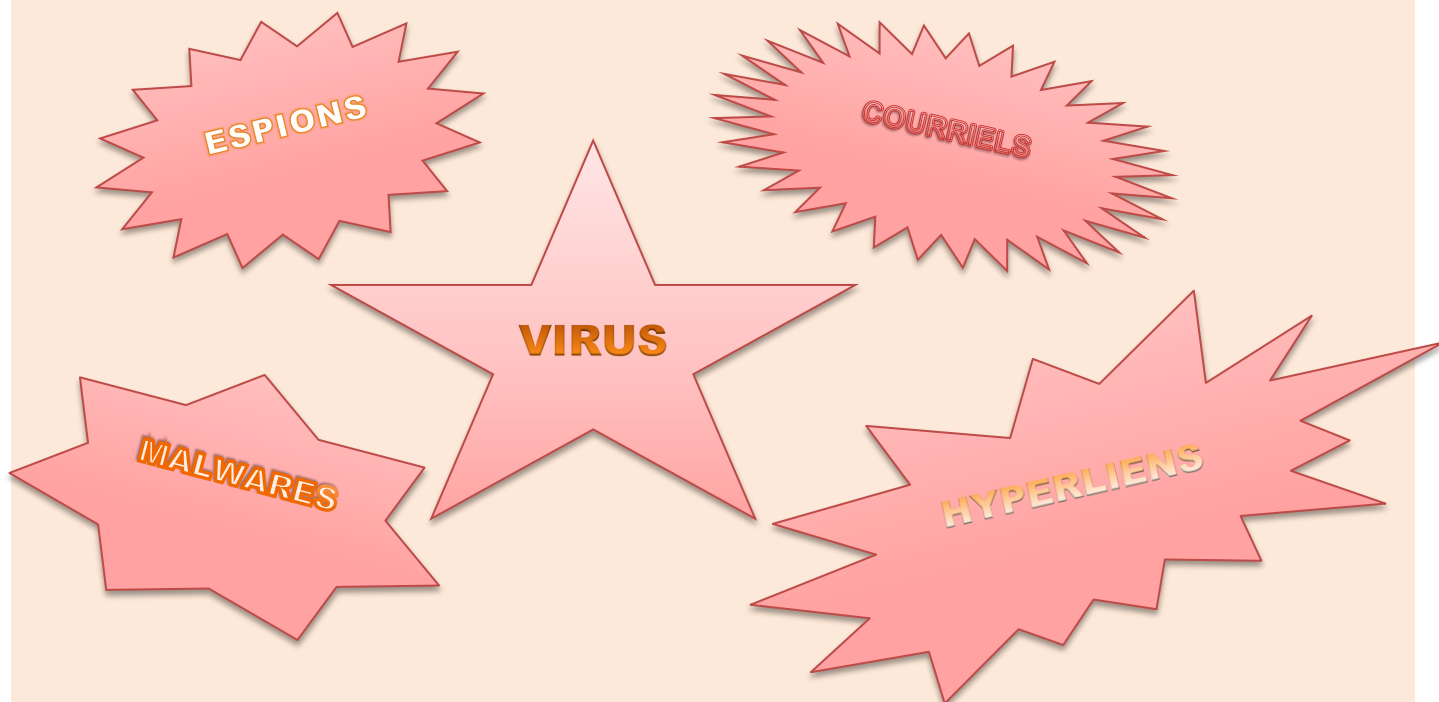


## L'ANTIVIRUS

Lors de la pandémie virale l'être humain doit se protéger sans cesse du danger de contamination, pour soi-même mais aussi pour autrui. Des mesures sont prises, adaptées au niveau de l'épidémie.

Il en est de même ici, dans notre ordinateur, que nous sommes obligés de protéger par un programme antivirus. C'est un élément essentiel et fondamental, car le plus grand danger qui le guette provient précisément des virus et autres méchantes petites bêtes, plus ou moins malveillants qui pullulent sur le net.

Nous avons souvent abordé ce problème tout au long du Cyberseniors, il fallait cerner ce danger dans un condensé pratique : l'essentiel vous est ici présenté.



Plusieurs sortes d'antivirus sont à disposition : ceux qui font obstacle aux virus mêmes et ceux qui protègent des virus, avant leur arrivée dans votre ordinateur ; on trouve aussi ceux qui nettoient la machine des « saletés » éventuelles ; enfin, certains programmes allient le tout et font le ménage à votre place.

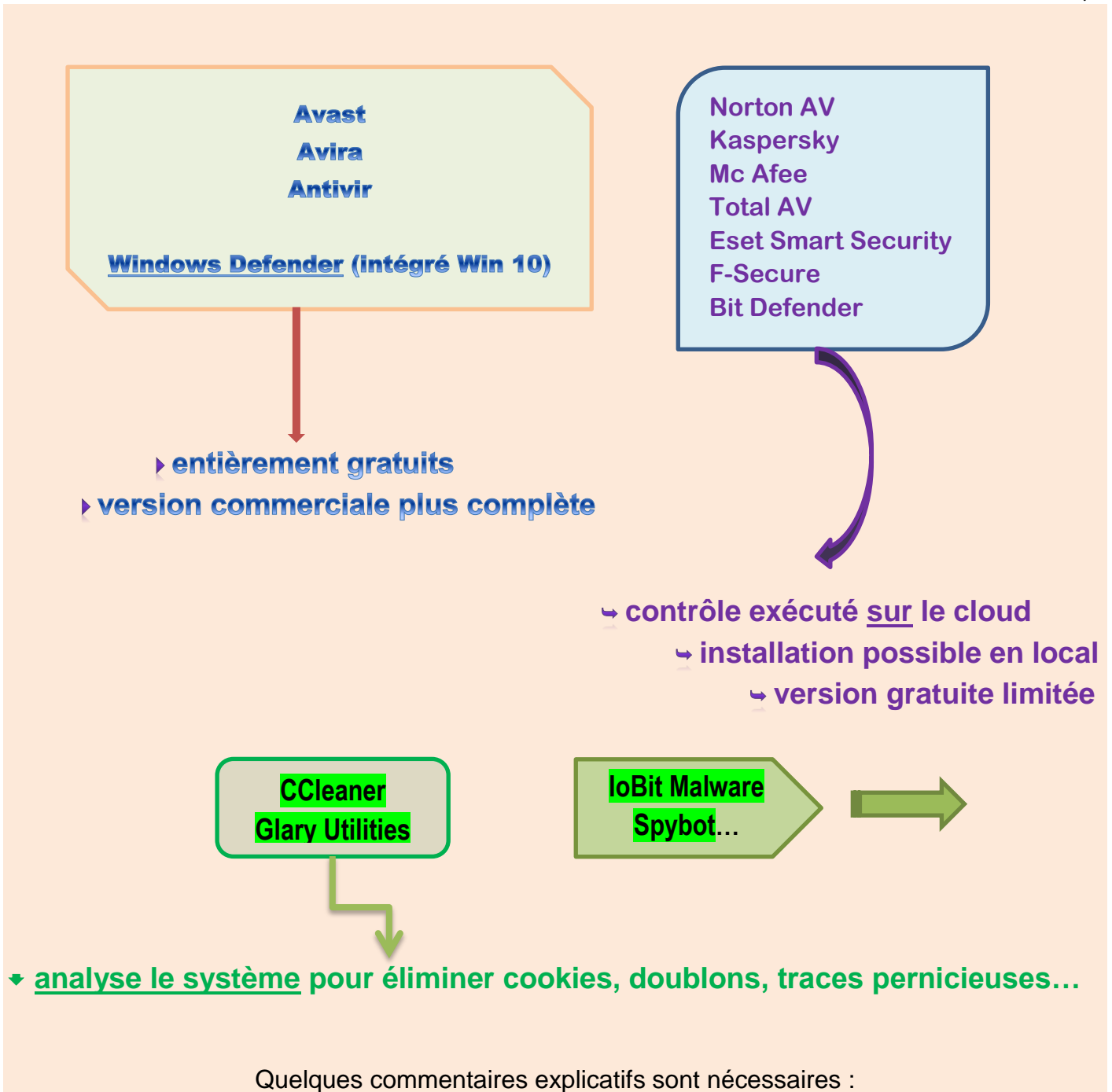
Des programmes se trouvent sur « le cloud », d'autres exigent une installation locale.

Des éléments sont gratuits, certains payants, plusieurs s'utilisent par abonnement annuel.

La palette offerte à l'internaute est donc fort variée, il convient alors de bien faire son choix en fonction de son travail. La plupart des plateformes permettent une prise en main ponctuelle, par une période d'essai offerte gracieusement.

Les cadres suivants vous montrent par la couleur de fond les divers types de logiciels :

- **jaune** ⇒ les gratuits      - **bleu** ⇒ ceux sur le cloud      - **vert** ⇒ les complets



- A) Windows Defender le logiciel antivirus intégré à Windows 10 est remarquable, à condition de le configurer entièrement ; ne pas hésiter à placer un contrôle serré, annulant la géolocalisation par exemple, évitant toute saisie de données personnelles.
- B) Avast semble être le meilleur choix dans la gratuité totale mais la version est un peu simpliste.
- C) Le contrôle dans le cloud est bien exécuté, mais rarement suivi d'effets dans la version gratuite, qui propose les mesures... sans les mettre en route, sauf dans la version payante.
- D) Il est de rigueur d'opérer deux fois dans l'analyse gratuite du système, de façon à vraiment éliminer les fichiers dangereux. Les programmes permettent également la suppression des logiciels devenus encombrants, et ce d'une manière officielle et très sûre. Ne pas se gêner !
- E) Dans cette rubrique, nous évoquons les logiciels gestionnaires, qui pour une mise à jour automatisées des programmes, qui pour une suppression systématique des fichiers et dossiers trop encombrants dans l'ordinateur. L'ennui vient de la lourdeur de leur présence dans la machine.

Vous devinez sans doute que nous n'avons pas évoqué d'autres endroits plus sensibles à l'arrivée des fichiers malfaisants que sont le courriel et l'hyperlien.

En général, l'internaute n'y prend pas trop garde, il manie sans trop y faire attention, messages et fichiers joints.

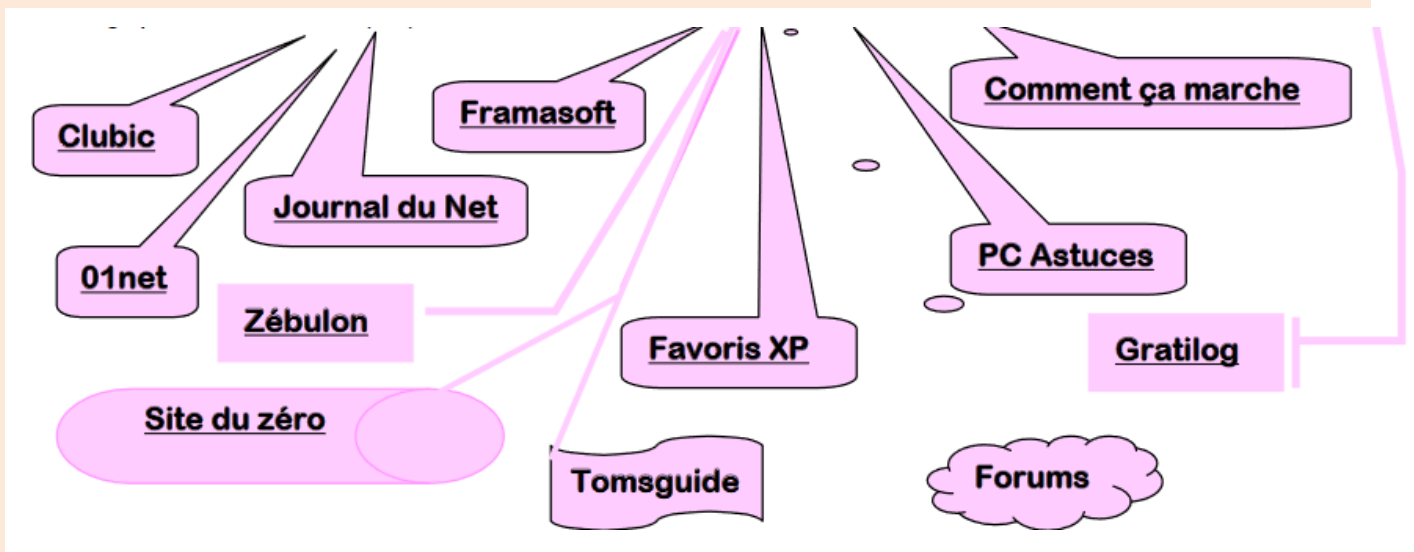
Or, là se loge aussi le danger : voir – mais souvent trop tard – l'arrivée soudaine de fichiers espions destinés à vous faire croire que l'expéditeur est connu de vous, l'architecture, la couleur, les images font illusion et... vous tombez dans le panneau !

En effet, un virus se cache fréquemment dans ces deux éléments ; bien vérifier alors : \* le DNS, l'hyperlien du correspondant avec le cadenas et l'orthographe dudit message ! Glisser la souris avant de cliquer, pour apercevoir les manques éventuels dans cette correspondance.

Nous conseillons de chercher un hyperlien, un nom de logiciel, une définition à connaître, bref... votre recherche doit s'effectuer avec des associations sérieuses d'internautes passionnés ; en voici quelques-unes qui ont pignon sur rue (voir fiches 24 et 29).

<https://www.meilleurantiviruscomparatif.com/meilleurs-antivirus-en-ligne> l'antivirus-en-ligne

[https://top5logicielantivirus.fr/?utm\\_medium=cpc&utm\\_source=bing&gclid=fb2a39753e6c1f9e40dc6791f95032c3](https://top5logicielantivirus.fr/?utm_medium=cpc&utm_source=bing&gclid=fb2a39753e6c1f9e40dc6791f95032c3) des antivirus



Voilà les gestionnaires importants pour bien connaître le web.

Nous conseillons vivement le programme **QWANT** comme moteur de recherches personnel ; *Google* est à bannir, sauf pour une recherche très fine et fort détaillée, car il engrange vos données personnelles à qui mieux mieux !

Le nom suffit pour recevoir immédiatement des liens pertinents ; bien surveiller – comme de coutume – le libellé du programme à télécharger !

Prendre garde à mettre de côté les *GAFAM* [Google, Amazon, Facebook, Apple, Microsoft] qui vous piratent toutes les données personnelles et autres secrets, suivant en cela l'*IA* [intelligence artificielle].

Nous récapitulons ici les différents types de logiciels rencontrés sur le Net. En effet, il vaut mieux se tenir au courant des arrivées de piratages et virus qui peuvent survenir lors de nos recherches, en particulier dans les nombreux programmes que nous téléchargeons à cette occasion. Bien sérier les problèmes. [cf. le Cybernet/surfeur.htm n°79]

<b>TYPES de logiciels à disposition du public (n°79)</b>	
freeware	entièrement gratuit
telware	libre durant 30 jours, après enregistrement sur Minitel acquisition possible gratuite (n'est plus utilisé)
postcardware	gratuit contre une carte postale illustrée de sa région
ad-aware	freeware avec la présence de publicité (en bannière animée la plupart du temps)
donationware	freeware avec la promesse de faire un don à une oeuvre caritative dédiée ou de son choix
shareware	gratuit pour une période d'essai de 30 à 50 jours, puis payant contre une modique somme
freeware # shareware	version complète et illimitée ou bien version complète et limitée à 30 jours = freeware ou shareware ?
libre (Linux)	gratuit ou payant, en boîte ou en téléchargement, avec accès au code source des applications de ce système d'exploitation
commercial	souvent gratuit en démonstration mais bridé et pas complet, puis payant après un certain délai
spyware	espionnage en français, récupère par internet les informations personnelles des internautes, logiciel espion
stalkerware	logiciel de harcèlement
ransomware (rançongiciel)	bloquer les données informatiques et les rendre contre de l'argent
firmware	actualisation d'un logiciel interne, mise à jour par "flashage" (notamment le graveur de CD/DVD)
"Peer to Peer"	échange de fichiers entre internautes (copie de fichiers, CD ou DVD, avec ou sans autorisation !)
version 'portable'	version <u>modifiée</u> d'un logiciel pour s'adapter sur une clé USB et permettre ainsi de créer un bureau ambulante autonome # ordinateur portable