LA SÉCURITÉ [028]

Vers la fin des pages du “Cyberseniors”, nous aimerions rappeler les actions de sécurité ; elles sont primordiales, d’abord pour sauvegarder vos données laborieusement engrangées, mais ensuite et surtout pour éviter erreurs et conflits au cours de votre navigation, afin de retrouver vos travaux sans dommages et en toute sérénité.

Pour ce faire, on recommande de passer en revue dans une liste, les 35 actions à entreprendre de manière systématique au fur et à mesure de votre avancée, et dans votre ordinateur et sur Internet :

1. posséder antivirus (*Windows Defender*, *Avira, Avast*), antispam tout au début dès l’acquisition d’un ordinateur. À défaut, les pages de *BitDefender* vous désinfectera tout de suite : <http://goo.gl/GxuMe>. Le programme *IObit Malware* vous débarrasse des petites méchantes bêtes qui infestent vos machines !

2. choisir un onduleur pour préserver vos divers périphériques (hardware) et éviter les micro-coupures si néfastes pour les machines !

3. lors d’une inscription, ne jamais indiquer votre nom véritable mais plutôt un pseudo, un avatar ; de même la date de naissance doit être 1935 au moins afin d’éviter l’inquisition des robots : à cet âge là on ne craint plus rien… !

4. à la fin d’un programme qui demande un code (*identifiant* et *mot de passe*), choisir toujours la rubrique « **Déconnexion**/Se déconnecter » et *non* ~~pas le clic sur la croix de Saint-André~~ ! Ne pas oublier cette sortie sécurisée !
Ne pas confondre entre sortir => fermer l’onglet de navigation et quitter => fermer le programme

5. vérifier toujours si la sécurité du dossier est bien établie : * le **s** ajouté à https://... ainsi que la présence simultanée du cadenas situé en haut/bas de l’écran près de la barre des tâches, lors de connexion bancaire ou commerciale notamment

6. les fichiers Word, Excel peuvent être sécurisés et protégés d’un simple clic (protéger le document) ; on peut crypter les autres ponctuellement (*AxCrypt*, *True Crypt, Glary Utilities*) pour une sécurité optimale. L’envoi via le cloud devrait être toujours crypté !

7. prêter attention à la **mise à jour** régulière et automatique des systèmes, à l’actualisation des programmes lancée de manière autonome, à l’acquisition des derniers pilotes (*drivers*) ! Laisser agir le système automatiquement pour la programmation ‘Java, Windows de Microsoft, Acrobat Reader’ et les logiciels de programmes connus logés dans votre ordinateur *CCleaner* et *Glary Utilities*, surtout les applications que vous utilisez constamment. Les outils de diagnostic sont ici fondamentaux : ***ma config*** <http://ma-config.com> et ***update checker*** <http://www.filehippo.com/fr/updatechecker>, voire *IObit Driver Booster* <http://www.iobit.com> [voir le dossier 024 réparation]

8. se préoccuper dès le début de la configuration d’un programme (software), le façonner à votre goût, pour vous rendre la tâche plus facile. Choisir ses logiciels en connaissance de cause ! Surtout les mettre en forme selon vos goûts : voir *Outils*, *Propriétés… .*

9. bien prendre les précautions d'usage indispensables dans votre navigation sur la toile et votre organisation dans votre ordinateur : codes, répertoire provisoire, téléchargements, sauvegarde régulière…sur un autre disque dur interne, un disque dur externe, une clé USB, une carte mémoire…
Ne jamais déroger à la règle suivante : **sauvegarder toutes les 5 minutes !**

10. chercher à se protéger des intrusions extérieures : **cookies**, habitudes de connexion, parades contre le piratage, surfer anonyme ('*in Private* IExplorer, *navigation privée* Firefox, *incognito* Chrome')… Voir aussi '*Collusion*' Firefox ou *DuckDuckGo* qui protègent vos données privées, ainsi que les moteurs de recherche *Qwant* et *StartPage*.

11. ne pas hésiter à acquérir les logiciels de contrôle de votre machine : *CCleaner*, *Glary Utilities*, *Malware Antimalware*, *Ad-Aware Antivirus, Driver Booster*, *ma config* ; les activer régulièrement vous fera gagner de la place et enlever les intrus et les doublons !
Pour connaître tout sur votre ordinateur, installer *Speccy* ou *Aïda64* est une sage précaution : il vous délivre tous les renseignements techniques en liste thématique !

12. vider de façon régulière la corbeille, l'historique des navigations, les répertoires et fichiers temporaires, en surplus mais inutiles ! Pour ce faire, activer **CCleaner** et **Glary Utilities**, voire **IOBit Antimalware** afin d'éliminer tous les programmes superflus ; même la base de registres sera concernée. Un contrôle hebdomadaire nous paraît indispensable, voire quotidien !

13. comptabiliser les périphériques installés : clé USB, lecteur/graveur de CDVD, disque dur externe, carte mémoire ; vérifier leur fonctionnement et leurs branchements, au besoin les tester par un antivirus (cf n°19)

Attention maintenant à la clé USB ! Il existe deux types de clés : normale mais à connexion usb typée 2, 3, 3.1 selon la rapidité. Une clé USB contient jusqu'à 512 Go ! L'autre modèle est à connexion type-C, plus petite et réservée au système Androïd. La nouveauté réside dans le choix à double connexion par un petit taquet à choisir selon sa connexion. Une telle clé devient fort réduite… mais peut se perdre ! En revanche, elle devient parfaite dans le monde d'aujourd'hui terriblement connecté !

14. éteindre la netbox et vos appareils chaque nuit, afin de reposer les condensateurs et surtout d'éviter l'intrusion dans vos machines hors de votre vision. Mesure indispensable !

15. éviter de se rendre sur **les réseaux sociaux** (Facebook, Twitter…) sans prendre les plus grandes précautions pour rester anonyme ! Ne jamais dévoiler son registre personnel ! Garder toujours un cercle privé ! Surtout à présent que les données privées (*big data*) sont susceptibles de se trouver piratées ! [voir n°34]

16. créer un **disque de réparation** (Windows XP/7/8/10) et un disque de *boot* (démarrage) (par le logiciel *CD BunerXP* par exemple) qui fonctionne aussi, bien sûr, avec les autres versions ultérieures), pour repartir éventuellement sur ce cédérom ou DVD au cas où le système ne voudrait point démarrer. C'est la solution ultime. Il faut paramétrer le **BIOS**, c'est-à-dire le départ de la machine dès que le courant électrique est envoyé, car le système doit dans ce cas là démarrer non pas sur le disque dur comme de coutume, mais bien plutôt sur le DVD de réparation, voire la clé USB que vous avez placé dans le lecteur idoine.
En général, la touche SUPPR permet de visualiser le BIOS de l'ordinateur dès le démarrage ; on vous indiquera toujours (souvent en anglais mais vous pouvez franciser) la manœuvre à accomplir pour ce genre de tactique, différente selon les marques (<F10/CTRL>…).
Voir http://poloastucien.free.fr/cd_de_boot_h.html

Un disque bootable de démarrage était naguère créé automatiquement grâce aux logiciels : Hirens' Boot CD – Ultimate Boot CD – Nlite (à télécharger sur internet).

Avec Windows10, la nouvelle mouture de Microsoft, l'internaute peut créer dès que possible son propre outil DVD/clé USB de sécurité-réparation : <..*Démarrer****Paramètres***Mise à jour**sécurité*\..> .

Dans le cas du multiboot (divers accès au démarrage selon vos systèmes OS comme Windows, Apple et Linux) le programme *EasyBCD* est recommandé.

17. un partitionnement de vos disques durs est aussi une solution à vos ennuis ; en effet, les informations sont diversement installées sur le disque dur et parfois à des endroits opposés, ce qui actionne sans cesse le disque mécanique, ralentit le rythme et provoque une certaine usure. Par conséquent, il est recommandé d'opérer de la sorte de temps à autre, sans oublier la sécurisation préalable du système

Attention ! Prendre les précautions d'usage, à savoir sauvegarder la base de registre et ses données sur un autre disque dur, une clé USB, un CDVD avant toute intervention de ce genre !

18. une situation embarrassante peut arriver et vous laisser perplexe devant le phénomène. Souvent en tapant, le doigt accroche les touches non désirées et l'internaute doit alors envisager les solutions qui viennent à l'esprit, sans trop considérer le problème gigantesque :

- **a)** le clavier arrive en anglais mais plus en français. Les touches ALT + MAJ le font revenir aussitôt dans la langue de Molière

- **b)** le pavé numérique s'égare follement : la touche Verr Num fut sans doute désactivée par inadvertance. Il suffit de réappuyer pour qu'elle reprenne du service. Un voyant led la contrôle. Certains nouveaux claviers ont éliminé cette touche, et donc le pavé numérique est unique !

- **c)** même processus avec la touche MAJ qui lors de frappe trop rapide prend de la vitesse et transforme tous les caractères en majuscules, ce qui s'avère alors fort gênant. Un nouvel appui annule la procédure. Nous conseillons de ne pas laisser la touche MAJ active de façon systématique ; mieux vaut la choisir au fur et à mesure du travail demandé. Ici aussi un voyant led facilite le repérage

- **d)** ne pas oublier que la connexion du clavier sur un poste fixe est obligatoire mais pas la souris. Ainsi, l'installation complète sans clavier ne fonctionnera pas du tout. Évidemment, ce périphérique est incorporé dans l'ordinateur portable sous la forme d'un pavé tactile ('*touchpad*' en anglais). Vérifier le contrôle en leds des *touches MAJ* et *pavé numérique* sur votre clavier. L'expérience en montre l'utilité extrême.

- **e)** les 2 couples de touches suivantes entraînent une action différente et fort fréquente car la frappe devient alors rapide et efficace ; toutefois attention au dérapage !

MAJ + ENTR(ÉE) => ligne suivante **CTRL + ENTR**(ÉE) => paragraphe suivant

- **f)** la touche ESPACE est souvent désignée quand on doit appuyer sur une touche quelconque lors d'installation de logiciel, car elle n'initie aucune action, si ce n'est uniquement un espace après le caractère précédent ; par conséquent, aucune contre-indication !

- **g)** attention à la frappe de la touche **Inser** qui annule l'action et efface le caractère précédant le curseur ; appuyer à nouveau la touche enlève ce procédé de Word

19. Pour vérifier une clé USB et une URL, utiliser le programme *Virustotal* https://www.virustotal.com/fr/ qui vous certifiera ensuite qu'aucun virus ne les infecte ! Votre antivirus habituel fera aussi le nécessaire.

20. La protection de vos données est indispensable de nos jours par de petits outils intégrés au navigateur : ***StartPage***, ***Qwant*** ne délivrent aucune donnée personnelle sur internet ! Les choisir en priorité ! Ce dernier est de plus un produit entièrement français !

21. <http://www.reforme.net/une/societe/pistes-aider-jeunes-utilisateurs-dinternet> cette adresse vous donne quelques conseils pour éviter de se voir plongé(e) dans les méandres de la toile mondiale… À méditer absolument !

*** Consulter les pages « cyber-attaques, comment s'en protéger » par Nicolas Gavet in VSD n°1950 08-14/01/2015 ; « limiter la publicité » in le Pèlerin n°6899 09/02/2015 ; « sécuriser ses données sur internet » in le Colporteur n°234 février 2017 ; les pages de l'Internaute : http://www.linternaute.com/hightech/internet/1361918-.../1362450-photos-de-vos-enfants?een=d774f3f3a3e3d668adc1da3c5787dbfd&seen=2&utm_source=greenarrow&utm_medium=mail&utm_campaign=ml284_photosanepaspos ➔ les photos à ne pas livrer sur les réseaux sociaux !

♥ ♥

22. Si par malheur, votre ordinateur semble rendre l'âme, **pas de panique !**
Plusieurs actions salutaires sont à effectuer :

- a) brancher l'ordinateur défaillant sur un autre ordinateur mais comme esclave (*slave*) et non plus comme maître (*master*). Un petit taquet (*slot*) est à ajuster à la bonne place [M ou S] sur le côté du disque dur incriminé.
- b) sortir le disque dur malade puis le brancher sur un autre PC qui marche, en s'assurant de la bonne position des deux connexions de base, la fiche informatique à plusieurs ergots avec son câble multibrins ainsi que la petite broche blanche pour l'équipement électrique.
- c) vérifier toutes les connections et les multiples branchements divers dans votre machine. Les retirer puis les rebrancher suffit souvent à remettre de l'ordre dans la machine.
- d) une solution également est de réinstaller l'ordinateur au départ d'usine, au moment où on vous l'a livré.
- e) opérer un contrôle sériel, c'est-à-dire périphérique par périphérique, débrancher chaque élément séparément et le rebrancher afin de vérifier ainsi le fonctionnement de chacun.
- f) parfois une erreur (*bug*) survient alors qu'on ne s'y attendait pas du tout ; le conflit entre unités peut survenir, par exemple entre clés USB ou disques de cédérom. Eh oui, certaines marques ne sont pas acceptées partout ! Et puis la situation dépend aussi de la vétusté de votre appareil : plus de 15 ans est vraiment une ancienneté redoutable ! Que dire du système utilisé [*OS*] ? Remontez-vous à Windows 95 ? Changez alors vite votre produit ! Préférer Windows 10 avec système 64 bits.
- g) pour terminer, la solution ultime demeure l'accès aux commandes du DOS, cet ancêtre du numérique. Il convient d'abord d'aller sur <*Démarrer\Exécuter\..*> puis de taper les bonnes lettres : voir *fiche 24a le DOS*.
- h) pour le portable, se méfier de la chaleur qui se dégage sous l'appareil ; rehausser donc le portable avec des cales sous chaque coin. Il bougera moins et sera plus en sécurité en étant moins brûlant !

23. L'hébergement de pages internet sur « **le cloud** » exige de grandes précautions, notamment le choix de la machine distante ; préférez une légère participation payante comme *OVH* ou *Gandi* qui vous assure discrétion et sécurité ainsi que le logiciel libre *owncloud*. Se méfier des solutions gratuites ! FREE assure la gratuité de pages web sur le net jusqu'à 50 Go.

Nous abordons ici le problème des **données personnelles** mises peut-être dans un "coffre-fort" virtuel, en réalité dans un serveur aux multiples ramifications qui stocke les données « *nuagiques* » !. Le grand danger est alors d'avoir accès à ces précieuses ressources, souvent fort personnelles, si cruciales pour le particulier. Force est de conseiller de placer à cet endroit tout, sauf les codes bancaires et autres renseignements privés ! Bien opérer la différence entre le transfert et la sauvegarde dans le cloud !

De nombreux sites proposent un tel transfert sécurisé : ***Transfert.free*** (réservé aux abonnés de la freebox), ***Sendbox, WeTransfer, SwissTransfer, Grosfichiers…*** ; Digiposte (à vie), MEGA, Informaniak ; Avira Secure Backup, Dropbox, Nextsend, Google Drive, Onedrive, hubic.com… par la gratuité (1, 2 Go d'espace) et durée limitée (*30 jours, 3 jours, 7 jours, 15 jours*) ; d'autres avec faible contribution (5 à 10 Go), d'autres encore en abonnement privatisé illimité sur plusieurs gigaoctets. (Voir fiche 029, page 10)
Vous optez aussi pour "*le cloud*" offert par votre FAI payant : Orange, Free, SFR, Bouygues…

Ceux *en* ***gras*** *italique* n'exigent aucune inscription préalable, si ce n'est un mél !

24. Il est temps de parler de la sécurisation des données lors de paiement sur Internet, c'est-à-dire dans le 'e-commerce', au cours de vos achats virtuels. Il est vivement conseillé de faire très attention au moment de **régler ses achats**. De plus en plus le système 3D Secure [*Certicode*] est mis en place : autrement dit, vous recevez par SMS un code de validation pour effectuer et finaliser votre acquisition, voire un code à 4 éléments.

Là, vous êtes vraiment protégé(e) !

N'oublions pas encore d'autres systèmes comme la reconnaissance vocale et faciale ainsi que le paiement sans contact, à prohiber. Votre carte de paiement doit se trouver logée entre deux feuilles d'aluminium ou dans un emballage adéquat : ainsi, aucun lecteur de smartphone ne peut avoir accès sans votre consentement à votre puce !

Enfin, la solution du paiement via le **e-SEPA** - le télépaiement numérique – comme à EDF/EAU/GAZ… par exemple, devient le plus pratique et le plus sûr car en direct entre les banques, sans intermédiaire !
Les références **IBAN** et **BIC** sont alors indispensables !

25. le dernier point important – et non des moindres – concerne la sécurité physique de l'internaute. Un sujet vraiment primordial, le **problème de santé** vis-à-vis de l'informatique : l'attitude, le comportement, la gestuelle face à la machine, afin d'éviter douleur, contraction, tendinite… bref, une mauvaise posture devant cet outil peut rendre la vie quotidienne impossible. Suivre surtout les **conseils** donnés dans le Netscolaire.

26. Consulter dans "*le Cyberseniors*" la fiche 024 sur le dépannage, les réparations, la protection.

27. Pour terminer, ne pas hésiter à indiquer sur le site gouvernemental officiel les dérives de l'internet : https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action . Voir le ***Bloctel*.**

28. Ne passons pas sous silence les effets nocifs des ondes électromagnétiques, principalement avec l'utilisation des Ipad, Iphone, mobiles, smartphone, le WiFi... Les URL suivantes apportent un réconfort :
* électroprévention ; * sécurité sanitaire ; * rayonnements électromagnétiques ; * sécurité électromagnétique ; * association santé-environnement .

Pensons aussi aux méfaits des appareils sur les enfants et les jeunes ! ATTENTION !

29. Au numéro 7. on propose la mise à jour régulière des grands logiciels utilisés quotidiennement. Il convient de prendre conscience que cette action peut – on répète, peut – avoir des conséquences funestes, si l'on ne prend pas la précaution de bien discerner les *programmes des éditeurs*.

Ainsi avec :
-- Windows, Acrobat Reader, CCleaner, Glary Utilities, IObitMalware, Malwarebytes Antimalware ;
-- le logiciel de messagerie (Winmail, Outlook, Thunderbird, Foxmail, Opera Mail) ;
-- le navigateur (Edge, Firefox, Safari, Chrome, Opera, Vivaldi) ;
-- l'antivirus (Windows Defender, Avast, Antivir, BitDefender, Kaspersky, Trend Micro, Panda Activescan) ;
-- l'utilitaire système gestionnaire (Totalcommander, Freecommander) ;
-- Office Pro* (Word, Excel, Power Point) et Libre Office (libres) ;

➔ laisser agir l'installation de la mise à jour, souvent automatisée.

30. En revanche, prêter attention aux **modes de transmission** des virus et piratages.
* la pièce jointe dans un courriel piégé,
* le fichier compressé *.*zip*
* le fichier Word en *.*doc* ou *.*docx*
* le fichier en *.*pdf* tant prisé sur le net,
* la fenêtre *popup* de publicité invasive,
* le document exigeant le langage *Java* à installer,
* les extensions de ~~*fichier en flash*~~ comme ~~*Adobe Flash Player*~~ ou ~~*Microsoft Silverlight*~~ !
* le pirate de navigateur prend la place de votre navigateur préféré et dirige les opérations !

Prendre garde à cette nouvelle technique !

* le stockage dématérialisé dans les nuages (cloud), toujours instable : à savoir dans « le cloud » comme *Google Drive* ou *Microsoft OnDrive* !

Vous devez absolument être sûr(e) et certain(e) de la provenance des éléments téléchargés.

Vous en connaissez l'origine et vérifiez **sur la barre d'adresses** qu'ils proviennent bien des sites officiels ! Les logiciels *IObit Malware* et *Driver Booster* optimisent les mises à jour réelles dans votre machine. Vérifier au passage le http***s*** et le ***cadenas*** dans l'adresse.

Dans le cas contraire, supprimer systématiquement, même s'ils sont intéressants pour vous, quitte à reprendre l'activité plus tard, sur un autre opérateur.

Le documentaire de Victor Castanet « *vous avez été hacké(e)* » sorti chaîne 13ème Rue 2017 montre bien les techniques de piratage des données personnelles. Bon courage !

31. Nous avons relevé dans le quotidien “le Progrès” du samedi 23/12/2017 l’article de Jean-Michel Lahire sous le titre « *nous sommes tous accrocs à nos smartphones* », les lignes suivantes qui offrent un bon résumé sécuritaire :
« ***plus vous restez, plus vous cliquez, plus vous participez, plus la publicité paie, et plus vous rapportez !*** ». On pourrait ajouter d’ailleurs «… ***plus vous êtes pistés !*** ».

32. En plus du n° 22, n’oubliez pas de démarrer un programme récalcitrant sous la forme de l’administrateur : cliquer droit sur le fichier .exe par exemple et cliquez gauche sur les éléments suivants : -..\ *Propriétés\Raccourci\Avancé**exécuter en tant qu’administrateur**\OK* .
Normalement votre programme doit démarrer. Agissez de même pour tous vos programmes exécuteurs.

33. Cerner les grosses entreprises multimedia dans vos recherches pointues :
◊ Geoportail => cartes et photos anciennes,
◊ Google Earth => vues aériennes à manier avec grande précaution !
◊ Google Street => routes et alentours,
◊ ‘remonter le temps => retrouver le passé des régions de terroir.

34. Agir de même avec les réseaux sociaux, dont il faut absolument se méfier ! *Facebook* en particulier piste tous les internautes, même ceux qui n’ont pas ouvert de compte !
En conséquence, ne pas trop “*importer vos contacts”,* ni cliquer sur les boutons “*j’aime*” ou “*partager*”. Sans cliquer dessus, l’internaute transmet malgré tout sans le vouloir les données personnelles concernant *Facebook*. D’où le scandale récent sur ce réseau social. On n’est jamais trop prudent ! *Twitter* agit de même ! Éviter ces connections aux réseaux sociaux !

35. Ultime précaution : “**prévenir vaut mieux que guérir**”, n’est-ce pas ?

Ce sera notre conclusion. Si vous avez bien écouté et lu nos directives, vous allez de votre propre chef résumer en un tableau synoptique nos propositions. En effet, il convient avant tout de se protéger des maux actuels dans le numérique, à savoir le piratage des données et leur utilisation à de mauvaises fins. Je veux citer ici l’**IA** (intelligence artificielle) qui facilite sous prétexte de rassemblement de données personnelles la mise en valeur des problèmes d’autrui, car le grand nombre d’indications identiques incite à observer des actions similaires et partant des conclusions provisoires. D’où les ennuis pour le grand public qui observe de plus en plus la mise sous tutelle de ses propres activités humaines, dans tous les domaines. Il s’agit là d’une fuite presque légalisée de nos envies, nos désirs, nos manies, nos manières de vivre… phénomène vraiment nouveau et particulièrement nocif. Les ***GAFAM*** sont pointés ici du doigt ! Sans parler des impôts non perçus de leur part !
Voir « *Ne laissons pas les GAFAM verrouiller l’accès au numérique* » par Jean-Baptiste Rudelle – in le Monde jeudi 8 août 2019. À ce propos, il est conseillé de verrouiller justement vos précieuses données par le biais d’un programme d’encryptage qui forcera l’internaute à décrypter votre dossier/fichier (*Axcrypt* et *Glaries Utilities*) ; la transaction doit avoir un chiffrement important comme SSL2048bit.

Terminons par l’action à mener contre les extorsions financières illégales, surtout avec **la carte de paiement** devenue le moyen pratique de régler ses achats !
Utilisez donc les hyperliens officiels gouvernementaux qui nous protègent de ces excès :
- ***Bloctel*** pour éviter les appels téléphoniques incongrus
- ***Perceval*** afin de signaler l’utilisation illégale de sa carte bancaire
- pour signaler un abus => http://www.internet-signalement.gouv.fr
- Info-escroquerie => 0811 02 02 17 ; dépôt de plainte en personne (commissariat ou gendarmerie)
- Les fondamentaux de la culture web, la publication sur les réseaux sociaux :
http://cache.media.education.gouv.fr/file/Education_aux_medias/44/4/Gestion_de_crise_sur_les_reseaux_sociaux_Mars_2015_407444.pdf

Cybermallveillance l’autodéfense numérique :
https://www.cybermalveillance.gouv.fr/bonnes-pratiques

SE PROTÉGER EN SE LIBÉRANT DES CARCANS CONTRAIGNANTS !

1. ~~éviter~~ de se lier à *Google, Facebook, Twitter* et autres réseaux sociaux. Cela ne signifie pas les enlever de notre route, mais ne pas en devenir esclave avec les applications par exemple. Donc, éviter *Chrome et Edge* (Win 10) comme navigateur, *Gmail et Courrier* (Win 10) comme logiciel de messagerie personnelle, *Google et Bing* comme moteur de recherche.

2. préférer de loin les outils libres – en open source comme Mozilla – en constance amélioration par les utilisateurs eux-mêmes qui apportent leur propre expérience, un peu comme le célèbre Wikipédia.

3. . prendre le groupe Mozilla est une sage mesure : *Firefox* en navigateur, *Thunderbird* pour la messagerie ; pour la recherche ***QWANT*** est français pur jus !

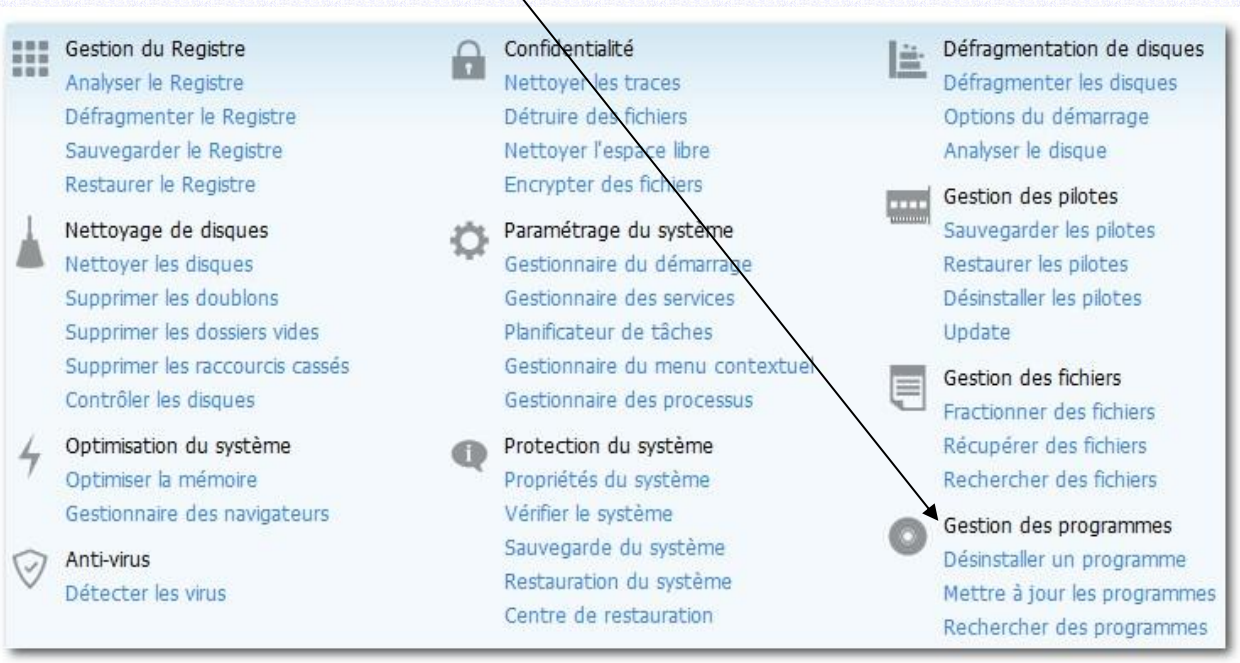
4. ne pas hésiter à s'entourer de programmes utilitaires de protection. Certes, un antivirus est obligatoire, *Avast* suffit amplement, mais *IObit Malware* élimine les mauvaises graines.
Voir aussi *CCleaner* et *Glary Utilities* spécialistes des suppressions de petits fichiers inutiles.

5. quant aux auxiliaires de vie numérique oserais-je ajouter, il s'agit là de logiciels utiles dans le graphisme, le documentaire, l'explicatif, le participatif… etc, bref, des programmes hors du système d'exploitation de l'ordinateur, en somme de logiciels optionnels. Ils sont devenus indispensables mais n'entravent en aucune façon la bonne marche des machines.
Nous en avons parlé longuement dans ces pages web, reportez-vous à la fiche adéquate, les programmes fondamentaux.

6. garder sans cesse la ligne directrice adaptée : oui, plutôt ne pas voir que regarder les ennuis présents devant vous ! Il vaut mieux se contraindre que d'avoir tout à foison et… pleurer devant les dégâts ! Savoir se limiter, voire se restreindre plutôt que se voir obligé de réparer !

7. Eh, n'oubliez pas les ***messages indésirables*** ! Oui, ceux qui polluent notre messagerie quotidienne, véritables verrues, incisives et néfastes dans notre courriel. Dans le logiciel de messagerie conseillé *Thunderbird,* vous pouvez très facilement écarter les intrus en configurant correctement la saisie et les déplacer dans le dossier des *indésirables* ou *en quarantaine*, puis de les éliminer.

8. Au risque de répétitions, n'oubliez pas que le logiciel *Glary Utilities* possède des trésors, en particulier les commandes de contrôles :



Vous apercevez le tableau des incidences concernant la sécurité des variétés de disques en votre possession. Ne pas hésiter à tester une clé USB, un petit disque dur, un lecteur de DVD… etc. Tout est possible et votre webmestre vous engage à manier un tel programme pour vérifier pleinement la parfaite sûreté de vos plateformes puis de les nettoyer vigoureusement.

9. enfin… **les instructions ultimes !**

Que dire ici ? Tout a été indiqué plus haut dans ces pages web. Prendre note que l'activité numérique bouge sans cesse, comme la séismique ! Des programmes disparaissent, d'autres voient le jour, plusieurs logiciels reçoivent une mise à jour approfondie, certains n'existent plus… bref, nous devons nous tenir sur nos gardes, rester vigilants et se mettre au goût du jour : la rançon de la technologie moderne se trouve là !

Suivre nos conseils : ouvrir l'œil, se mettre à la page numérique… et surtout prendre patience et se détendre souvent après le dur labeur…

Enfin, on ne peut ignorer la copie automatisée de dossiers et fichiers sur un autre disque dur, par exemple un disque dur externe ou bien encore mieux un NAS, afin de sauvegarder de façon autonome les dossiers et fichiers rectifiés, à partir de votre disque dur de départ. Le logiciel ***Cobian Backup*** est à recommander ; Les programmes *Fullsync* et *SynBackFree* font aussi parfaitement l'affaire, quoique un peu plus complexes.
Il est bon d'avoir en permanence une sauvegarde automatique de vos dossiers précieux !

À propos de la sauvegarde de vos dossiers importants, on doit connaître la différence entre la *sauvegarde complète* et la *sauvegarde incrémentielle* : *complète* signifie une sauvegarde entière de tous les répertoires et fichiers alors que *incrémentielle* ne sauve que les données les plus récentes, sans systématiquement tout reprendre et sauvegarder. La date prend là une grande importance.

10. **mise en forme et mise à jour** [*voir fiche 026*.]

Osons un récapitulatif sur la mise à jour des programmes. En effet, il s'agit surtout de mettre en forme les nouveautés technologiques apportées au fur et à mesure de l'avancée numérique.

Mettre à jour = optimiser = réinitialiser sont des termes pratiquement synonymes. Le programme subit une nouvelle adaptation au nouveau régime en cours, il suit en quelque sorte la mode du temps.

On doit alors considérer plusieurs facteurs de stabilité afin d'éviter désordres et confusions.

➥ vérifier la langue, souvent offerte en option si par hasard le produit ne se trouve pas déjà rédigé en français. Voir alors *language* dans la version anglaise de base.

➥ consulter la version nouvelle, libellée par *v.3.2.5* par exemple, à comparer avec la vôtre actuellement en cours.

➥ éviter les doublons qui surchargent inutilement la mémoire de l'ordinateur, signalés par une parenthèse située en fin de fichier, comme *qwant.exe(2)* par exemple.

➥ trouver la nouvelle mouture dans le répertoire idoine, nommé *Téléchargement* sous Windows 10 (ou bien *Downloads en anglais*) et situé dans *l'Accès rapide* du système.

➥ porter votre choix sur la rapidité annoncée de votre machine, et donc 32 ou bien 64 bits selon le cas. Vous trouverez toujours dorénavant cette annonce lors du téléchargement.
Ne pas négliger cette donnée pour la bonne marche de l'appareil ; préférer bien sûr 64 bits.

➥ utiliser peut-être les outils de gestion adéquats, dédiés à ce genre de pratique : *01net, PC astuces, comment ça marche, Zdnet, clubic, tomsguide*… etc. qui vous offrent d'amples renseignements et de commentaires sur les programmes.

➥ installer la mise à jour par un *clic gauche* sur le fichier souvent signalé par *une extension *.exe,* qui se déroulera de façon automatisée dans le grand répertoire *C:\Program Files..* .

➥ trouver enfin l'icône correspondante sur votre Bureau pour un démarrage rapide du programme. Au besoin *cliquer droit* + *Propriétés/changement d'icône* pour plus de clarté.

Windows 10 et sa réinstallation

Voilà trois jours passés à replacer le système Windows 10 famille dans mon ordinateur !
Eh oui, le bureau était conforme... mais aucune icône ne fonctionnait ! La catastrophe en vue... Je ne connais pas l'origine de mon problème qui est survenu d'un seul coup. J'imagine à vrai dire qu'une nouvelle mise à jour du système d'exploitation Windows 10 en est la cause.

Que faire ? Remettre le système en route avec un DVD ou clé USB d'installation. Ma version sur la machine était officielle, avec licence d'utilisation, mais il fallait tout réinstaller... En général, tous les 4-5 ans, il est de mise de tout reprendre à zéro, afin d'obtenir une machine neuve et saine, sans trop de scories accumulées.

Donc, j'avais bien des DVD de sauvegarde... qui se trouvaient un peu anciens (1 an !). En conséquence, je suis allé virtuellement chez Microsoft télécharger la version famille de Windows 10, directement, et j'ai constitué une sécurité en DVD et clé USB à la mode des normes actuelles. Il est vrai que les codes propriétaires se trouvaient déjà dans le système car je n'ai eu nul besoin de les inscrire à nouveau au cours de l'installation.

Les dossiers et répertoires furent maintenus pour la plupart. Seuls les logiciels installés par le webmestre avaient disparu, Microsoft l'avait indiqué d'ailleurs. J'ai pris sur la toile la nouvelle version de mes programmes préférés.

Vous comprenez mon silence... j'avoue que je n'ai pas chômé pour tout remettre en ordre. Il faut avouer que le réseau, par exemple, s'est replacé tout seul sans ennui (un vieil ordi fixe sous XP qui commence à fléchir, un portable Windows 7 vers 10 et mon fixe Win 10, plus l'imprimante, sans oublier le serveur NAS de 3 To. Vaste entreprise !

L'unique disparition dans la machine fut les codes du FTP, pour les divers sites web à placer sur le net. Bien entendu, j'avais sauvegardé en détails les diverses manœuvres.
Ce ne fut qu'une question de temps…

Conclusion : l'ordinateur marche bien mieux, est plus rapide, est moins encombré. À propos, les outils antivirus et autres utilitaires ont dû comme de coutume être installés encore une fois. Le temps est vraiment le mot clé en informatique.

N'oubliez jamais, surtout, de construire un DVD, une clé USB de secours… de préparer la sauvegarde complète et entière de votre ordinateur fixe de bureau ainsi que du portable.
<..\Démarrer\Paramètres\Mise à jour et sécurité\Paramètres de mise à jour\Sauvegarde
\Accéder à l'outil Sauvegarder et restaurer Windows 7\Créer une image système\..>
\Accéder à l'outil Sauvegarder et restaurer Windows 7\Créer un disque de réparation système\..>

Bien entendu, un Dvd ou une clé USB de 64 Go doit être prêt à l'emploi pour une mise en route immédiate des sauvegardes : <https://support.microsoft.com/fr-fr/help/17127/windows-back-up-restore>

Prêtez attention à **la lutte contre la pollution en numérique** !
https://ekwateur.fr/2020/06/30/diminuer-pollution-numerique/ cet hyperlien vous donne la meilleure information avec astuces à l'appui… et mises en garde numériques !

Sachez que *BitLocker* ne se trouve que dans la version *Pro* de Windows 10 ; ce programme crypte répertoire, fichier, périphérique à la demande. Fort pratique.

Les solutions de secours

Les liens ci-après montrent les pistes importantes pour l'élaboration de clé USB et DVD de secours :

https://gandalsmart.com/windows-10-comment-booter-votre-cle-usb-en-mode-uefi/

https://www.commentcamarche.net/informatique/windows/187-creer-une-cle-usb-bootable-de-windows-10/

https://www.pcastuces.com/pratique/windows/disque_cle_usb_installation_windows_10/page3.htm

https://www.ubackup.com/fr/windows-10/creer-disque-recuperation-windows-10.html

https://www.ubackup.com/fr/windows-10/creer-image-systeme-sur-cle-usb-windows-10.html

- https://lecrabeinfo.net/demarrer-pc-a-partir-cle-usb-cd-dvd.html
- https://www.commentcamarche.net/informatique/windows/187-creer-une-cle-usb-bootable-de-windows-10/
- https://www.pcastuces.com/pratique/windows/solution_secours/page1.htm
- https://lecrabeinfo.net/creer-un-lecteur-de-recuperation-usb-pour-windows-11-10-8
- https://www.ubackup.com/fr/windows-10/creer-image-systeme-sur-cle-usb-windows-10.html
- https://www.ubackup.com/fr/windows-10/creer-disque-recuperation-windows-10.html

La création d'une **clé bootable** de secours – c'est-à-dire une clé qui réinitialise l'ordinateur en cas de panne ou non activité du système de Windows 10 – est la base fondamentale pour un travail numérique sérieux. Les noms des liens ci-dessus sont parlants et offrent plusieurs options pour l'internaute.

Les *§ 13 et 16* de la présente fiche vous indiquent déjà quelques pistes ; de même *la fiche 035a* vous sera d'une grande aide.

Il faut cependant par ces lignes offrir un récapitulatif général.

1. créer une image système [HDD]

Clic droit sur *Démarrer* puis cliquer sur *Windows Power Shell (admin). ;*
* ensuite taper sur l'invite de commandes l'instruction suivante *: <sdclt.exe /BLBBACKUPWIZARD> ;.* *
sélectionner votre disque dur externe (2 à 4 To) dans le champ suivant ; choisir et confirmer la sauvegarde ;
* démarrer la sauvegarde de *l'image système*. Attention, cela peut durer un certain temps ! Ne pas précipiter les choses.

Il est souhaité de recommencer chaque mois, afin d'avoir une image disque pas trop ancienne.

2. créer une clé de réparation [clé USB]

* Cliquer sur *Rechercher\Récupération\Créer un lecteur de récupération\Sauvegarder les lecteurs système* ;
* Puis cliquer sur *Suivant* pour sélectionner votre lecteur usb de récupération. Choisissez le bien dans la liste.
* Ensuite cliquer sur *Suivant* pour créer ce lecteur, avant de choisir *Termine*r pour finaliser votre action.
La restauration pourra commencer en suivant alors les instructions recommandées dans **ce lien** .

L'important est de se constituer un domaine sécuritaire en cas de mauvaise manipulation ou bien de circonstances malheureuses vous obligeant à reconstruire votre système. C'est la solution extrême, quand votre écran ne veut plus du tout se procurer Windows !

Regarder les divers hyperliens proposés devient une pratique habituelle, car chaque machine réagit selon ce qu'elle possède dans son "cœur". Son centre névralgique diffère selon ses acquisitions.

3. créer un lecteur de récupération usb

En suivant les commandes suivantes :
* *Démarrer\Paramètres\Mise à jour et sécurité\Récupération\Démarrage avancé\Redémarrer maintenant* vous atteignez les options de démarrage avancé de Windows 10.
* Choisir l'option qui vous convient, sans doute *à partir d'une clé usb* ; elle doit contenir au moins 16 Go.

4. avec les cookies numériques

Désormais l'entrée dans un programme numérique suppose l'accord de l'internaute. En réalité, le système demande l'acception de recevoir l'information de cookies de façon automatique, et souvent mais pas toujours malheureusement, la phrase « *Continuer sans accepter* » se trouve en bonne place, écrite tout petit dans un coin de l'écran. Le clic suffit à poursuivre votre route.

Toutefois, en l'absence de cette offre, il ne reste que deux solutions antithétiques : OUI ou NON, autrement dit, vous acceptez la présence de cookies dans votre machine ! Si d'aventure vous refusez, alors point de salut : il vous sera absolument impossible de continuer la lecture du programme en question ! Quel dilemme !

5. brève bibliographie

A) la cybersécurité pour les nuls – Joseph Steinberg – Ed pour les nuls 2022

B) le guide – comment démarrer dans la cybersécurité – Valentin Chéneau – Ed Cyberinstitut 2022

Il est vrai que le grave danger actuel provient précisément de la cybersécurité !
Elle doit se trouver au premier plan de notre activité : même chez le particulier, car les données sont une proie devenue facile. Pensez à l'IA, cette intelligence artificielle interactive !

Méfiez-vous à chaque activité ! Prenez moult précautions ! Évitez la localisation ! Entre autres… !