(1) Ne préjugez de rien. Prenez le temps de lire ce qui document qui concerne la sécurisation de votre système.

(2) Achetez et utilisez un logiciel de sécurité sérieux. Sélectionnez en un connu pour la fiabilité de ses résultats. Checkmark, AV-Test.org ou TuV sont parmi les plus respectés des évaluateurs indépendants de logiciels antivirus.

(3) Faites l'acquisition et utilisez une solution pare-feu de confiance. Là encore, misez sur les évacuateurs indépendants pour faire des choix appropriés. Certains systèmes d'exploitation sont livrés avec un pare-feu qui ne filtre que le trafic entrant. Utilisez un pare-feu qui filtre le trafic Internet entrant et sortant.

(4) N'ouvrez pas les fichiers joints à des messages dont l'objet est suspect ou très inattendu. Si vous voulez les ouvrir, enregistrez-les d'abord sur votre disque dur, puis analysez-les avec un programme antivirus récent.

(5) Supprimer toutes les chaînes e-mail et les messages non désirés. Ne les faites pas suivre et ne répondez pas à leurs expéditeurs. Ce type de courrier tombe dans la catégorie spam, car il est non désiré et non sollicité et qu'il surcharge le trafic Internet.

(6) Évitez d'installer sur le bureau des services et des applications dont vous n'avez pas besoin tous les jours : par exemple des serveurs de transfert et de partage de fichiers, serveurs à distance, et analogues. De tels programmes présentent des risques potentiels et ne devraient pas être installés s'ils ne sont pas absolument nécessaires.

(7) Mettez à jour aussi souvent que possible votre système et vos applications. Votre système d'exploitation est paramétré pour se mettre à jour automatiquement et certaines applications peuvent être paramétrés pour cela également. Si vous n'installez pas les correctifs disponibles suffisamment souvent, votre système peut souffrir de failles de sécurité pour lesquelles des remèdes existent déjà.

(8) Ne copiez aucun fichier dont vous ne connaissez pas la source, où dont la source ne vous inspire pas confiance. Vérifiez la source (provenance) des fichiers que vous téléchargez, et assurez-vous qu'un programme antivirus a déjà vérifié les fichiers à la source.

(9) Faites régulièrement des sauvegardes de vos fichiers personnels importants (correspondance, documents, images, etc.). Stockez ces copies sur des supports amovibles comme des clef USB, disque dur externe, ou mieux encore dans le cloud. C'est à dire en ligne ou il ne risque pas les pannes ou les chutes. Ou conservez vos archives sur un autre support que votre ordinateur.

(10) En cas de doute, YDConcept est là pour vous conseiller et vous aider, (service consulting). Prévenir coûte toujours moins que guérir.