Sécurité du système :

		A faire	A ne pas faire (peu préférable)
Niv. 1	Pour le système en général:	Faire ses mises à jour régulièrement. (*voir fiche méthode*)	Ne pas laisser son pare-feu ou son antivirus désactivé trop longtemps.
	Pour les mails:	Avoir un mot de passe suffisamment compliqué (majuscules, nombres...)	Ne pas laisser son adresse sur tous les sites. Cliquer sur un lien venant de mails d'inconnus! C'est le meilleur moyen de se faire *scamer*
	Face aux Virus:	Avoir un antivirus efficace type Avast (gratuit et téléchargeable sur internet).	Faites évidemment attention aux téléchargements et soyez attentifs lors des installations.
Niv. 2	Pour le système en général:	Nettoyer sa machine avec Ccleaner et AdwCleaner.	Ne pas avoir installé au moins un des deux logiciels cités.
	Pour les mails:	Créer une adresse *trash* (poubelle) pour les spams. *Yopmail* par exemple est un site de création de fausses adresses mails…	Ne pas s'inscrire sur différents sites avec votre adresse mail principale pour éviter les *spams*.
	Face aux Virus:	Effectuer des scans Ccleaner/ Adwcleaner et chercher de l'aide spécifique en ligne (par ex : copiez collez votre "diagnostique" sur internet).	Ne pas laisser son PC dans l'état où il à été infecté.
Niv. 3	Pour le système en général:	Vérifiez que vos drivers soient eux aussi bien à jour. (*voir fiche pratique*)	Ne pas refuser les mises à jour des drivers proposés par les différents constructeurs des composants de votre PC (par ex. Nvidia pour votre carte graphique).
	Pour les mails:	Hébergez vos mails sur votre ordinateur, vous aurez plus de place et vous pouvez même coder un petit programme pour trier vos mails intelligemment. Cryptez vos mails.	Si vous tenez a rester sur une boite mail, contentez vous de deux ou trois adresses: -une poubelle pour les pubs (yopmail.com) -une adresse pour les confirmations de sites, de comptes… -une adresse professionnelle et/ou privée
	Face aux Virus:	Si vous n'arrivez pas à vous débarrasser du virus, un formatage complet de l'ordinateur peut être nécessaire. D'où l'importance de sauvegarder ses données les plus importantes sur un disque dur externe par exemple.	Ne pas continuer d'utiliser son PC normalement même après une infection, car tout ce que vous faites peux être vu et suivit.

Fiche pratique :

- Mise à jour des drivers

Pour mettre à jour ses drivers, rien de plus simple. Un logiciel: “driver Booster” vérifie automatiquement si vos drivers sont à jour et si ce n’est pas le cas, il s’en occupe!
Plus difficile mais tout aussi efficace : un autre logiciel très complet nommé “Driver Pack Solution” fait la même chose et existe en 2 versions : lite et complète. La “lite” pioche des drivers en ligne par rapport aux besoins de votre PC ; tandis que la complète est très lourde (en place) et vous permet de mettre à jour vos drivers sans internet (après mise à jour de sa base de donné en ligne).

1. Crypter ses mails

L’application est plutôt compliquée, et n’est principalement utile que si vous hébergez vos mails. Vous pouvez chercher par vous même sur des forums car la démarche est longue à détailler.
Vous pouvez crypter vos fichiers avec un petit logiciel nommé “Axcrypt”, et ainsi ouvrir ce fichier sur n’importe quel ordinateur sans avoir le programme installé !

1. Les mises à jour

Normalement, Windows va faire les mises à jour système automatiquement. Si ce n’est pas le cas, vous pouvez rechercher sur votre ordinateur “Windows update”. Il y aura un onglet “rechercher mise à jours”.

1. Ccleaner/Adwcleaner

Quelles sont les différences entre ces deux logiciels? Ccleaner va “faire le ménage” sur vos disques dur. Il va supprimer les fichiers inutiles et éventuellement repérer et éliminer les virus. Adwcleaner va, quant à lui, “faire le ménage” sur votre navigateur internet. Il va supprimer cookies, adwares etc.
Vous pouvez télécharger Ccleaner et Adwcleaner (sur leurs sites officiels respectifs). Ensuite vous n’avez qu’à lancer un scan avec ces logiciels. Patientez et supprimez les menaces éventuelles. Vous aurez grâce à cela un ordinateur tout propre!

Remarque:
On trouve de tout sur internet… ne suivez pas aveuglément les conseils d’un inconnu seulement parce qu’il a l’air sympa. De plus, renseignez vous et apprenez de vos erreurs. C’est la clef de la sécurité.

Pro tip:
Pour télécharger un logiciel ne passez pas par une application tierce (ex: Softonic). Et privilégiez le DirectDownlad au Peer to Peer.

Glossaire de l’expert:

Le virus :
c’est le cousin direct du virus organique : il commence par pondre son ADN (lignes de code) en utilisant les failles de votre système d’exploitation ou de certains logiciels. Il perturbe plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme Internet, et notamment par l’intermédiaire des messages électroniques ou de leurs pièces attachées.

Le cheval de troie :

C’est un logiciel malveillant, qui une fois installé sur votre ordinateur, va permettre d'exécuter tout un tas d’actions telles qu’installer un virus,un logiciel espion…
A la différence du virus qui n’est qu’un morceau de programme, le cheval de troie est un logiciel entier se faisant passer pour un logiciel connu et légitime auprès des pare-feu et antivirus de votre ordinateur.

L’antivirus :
Cet outil souvent payant va analyser toutes les actions de vos logiciels ainsi que les éléments téléchargés. Son but est de référencer et bloquer les actions anormales (envoyer un message sans votre permission à tous vos contact par exemple) et les potentielles empreintes de virus. Car en effet les virus ont un point faible : ils sont facilement identifiables (souvent à la fin du programme, codé en assembleur…).

Le pare-feu :
Au même titre que l’antivirus, il est bienveillant mais souvent payant. Il est la plus part du temps dépendant ou intégré à votre système d’exploitation. Son but est de poser une barrière entre votre ordinateur et l’extérieur (comme une sorte de douane frontalière). Ainsi pour chaque élément rentrant ou sortant, il vérifie par différentes procédures s’il est en droit ou non de continuer sa route. Si l’élément est considéré comme potentiellement malveillant, le choix de l’administrateur tranchera (c’est la fameuse fenêtre qui vous dit “voulez-vous laisser ce programme apporter des modifications...”)

*Scam: vol d’un compte suite à un abus de confiance.

*Hack: piratage qui consiste à manipuler le système pour arriver à ses fins.

*Spam: des annonces ou pubs indésirables.

Fiche réalisée par Tom Dumoulin,
Thomas Carbonne, Jérémy Bachelot,
Nolwenne Duchêne, Karim Belhadj et Samuel Aychet-Claisse