ateliers

# Bien protéger son ordinateur

Bibliothèque francophone multimédia

bfm.limoges.fr

LIMOGES ARTS DU FEU ET INNOVATION

Bfm

# Bien protéger son ordinateur

La protection de l'ordinateur et plus globalement de vos pratiques sur vos matériels et votre navigation internet ne peut pas être appliquée à l'aide d'exercices comme nous pourrions le faire sur une mise en page d'un document, la retouche de photos ou autres. Ce sont des usages, des précautions à acquérir, petit à petit et selon vos besoins.

Ci-dessous une liste non exhaustive des réflexes que vous devez adopter :

- Maintenir vos logiciels à jour. En particulier votre système d'exploitation (Windows, Linux, Mac OS X) ainsi que les logiciels que vous avez installés (navigateur internet par exemple)
- Activer votre pare-feu. Le pare-feu est la première barrière sur le réseau, le désactiver peut permettre un accès plus facile à votre ordinateur
- Installer un antivirus, les versions gratuites conviennent très bien pour une utilisation personnelle
- Utiliser un mot de passe sécurisé. Un mot de passe pour être considéré comme difficile à pirater doit contenir des minuscules, des majuscules, des chiffres, des caractères spéciaux et au moins 8 caractères (le seuil minimal accepté par la plupart des sites)
- Utiliser un bloqueur de publicité. Vous trouverez sur internet beaucoup de sites envahit par la publicité, certaines de ces publicités lorsque vous cliquez dessus peuvent vous diriger vers des sites frauduleux. Le bloqueur de publicité en plus de les masquer vous permettra de naviguer sans être embêter par toutes ces fenêtres.
- Entretenir votre ordinateur. Bien que cela n'augmente en rien le niveau de sécurité de votre matériel, il est conseillé de supprimer les applications et fichiers dont vous n'avez plus l'utilité. Cette opération peut être réalisée facilement grâce à quelques logiciels.
- Naviguer sans être pisté(e). En utilisant le navigateur Mozilla Firefox, il vous est possible de surfer sur la toile sans laisser de traces.

# Garder vos logiciels à jour

Même si les messages de vos logiciels concernant la disponibilité d'une nouvelle mise à jour sont parfois embêtants, ils n'en sont pas moins importants.

Les mises à jour ont deux buts majeurs :

- Corriger les failles de sécurité
- Modifier/Rajouter des fonctionnalités

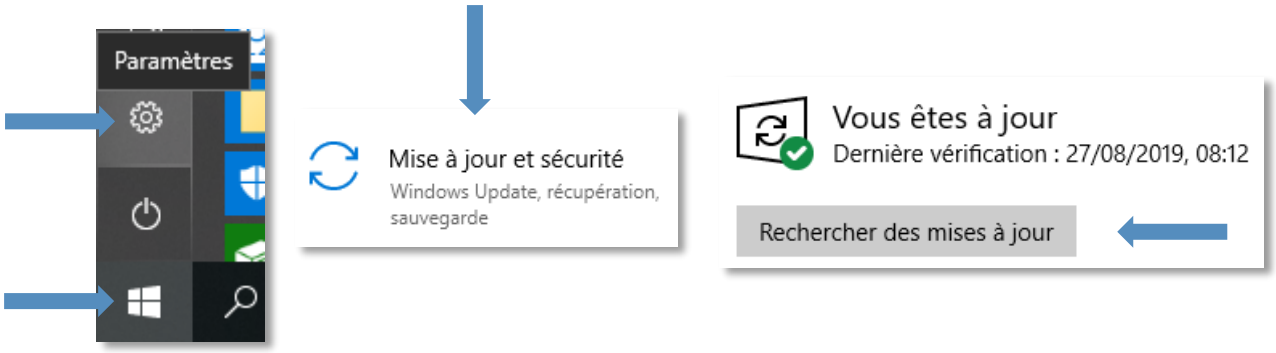
Vous n'êtes donc pas perdants en les exécutant.

Le logiciel que vous devez mettre à jour en priorité est votre système d'exploitation : Windows, OS X, Linux, etc. Les systèmes sont conçus pour vous indiquer quand des mises à jour sont disponibles, libre à vous par la suite de les lancer de suite ou d'attendre un peu.

Les autres logiciels que vous devez en suite maintenir à jour sont les programmes que vous utilisez sur votre ordinateur : antivirus, navigateur internet, lecteur de média, etc.

Pour mettre à jour le système Windows 10, ouvrez le *menu Démarrer*, cliquez sur *Paramètres*, accédez à la rubrique *Mise à jour et sécurité* et enfin lancez la recherche de mises à jour.

Vous n'avez plus qu'à patienter, Windows vous indiquera sûrement de redémarrer votre poste pour finaliser l'installation.




Les autres logiciels, eux, vous indiqueront la disponibilité d'une mise à jour au lancement de l'application à l'aide d'une petite fenêtre ou d'un message temporaire. Dans certains cas, vous serez redirigez vers le site porteur du logiciel afin de récupérer la nouvelle version pour d'autres un redémarrage de l'application peut suffire.

## Vérifier que votre pare-feu soit activé

Le pare-feu est normalement activé à chaque démarrage et vous n'avez donc pas besoin de vous en préoccuper. Si toutefois vous devez le réactiver, accédez aux **Paramètres** et à la catégorie **Mise à jour et sécurité** comme précédemment.

Sur la gauche, vous trouverez l'onglet **Sécurité de Windows**, cliquez dessus et dirigez-vous ensuite vers **Pare-feu et protection réseau** et enfin réactivez les pare-feu qui sont inactifs.


## Utiliser un antivirus

L'antivirus est une protection majeure pour votre ordinateur, il permet de scanner votre appareil et d'éliminer les infections repérées (il propose d'autres services mais celui-ci est le plus important). Il est très fortement conseillé d'en installer un, cependant, même si les offres semblent alléchantes, une version gratuite est suffisante. Libre à vous par la suite de voir si vous souhaitez tout de même acheter le logiciel ou prendre un abonnement.

Pour les ordinateurs sous Windows, vous pouvez vous rassurez, le système contient un antivirus, Windows Defender. Ce dernier est activé par défaut, et si toutefois vous souhaitez en prendre un autre, il se désactivera automatiquement ou fonctionnera en complément de son homologue.

Voici une liste d'antivirus que vous pouvez télécharger et installer :

- Avast
- AVG

- Avira
- Kaspersky
- Et il en existe encore plein d'autres !

Et une liste d'antivirus en ligne, ces derniers vous demanderont d'installer un programme très léger afin de pouvoir scanner votre appareil, ces programmes n'offrent cependant pas de protection en temps réel, ils sont principalement utilisés pour une analyse ponctuelle :

- Trend Micro – HouseCall
- ESET
- Panda Security
- F-Secure

**2 articles pour plus d'informations sur Windows Defender :**

- Protéger mon appareil avec Sécurité Windows
- Rester protégé avec Sécurité Windows

## Choisir un mot de passe sécurisé

Le mot de passe est capital pour empêcher les pirates d'accéder à vos espaces personnels, messageries et autres. Vous devez donc faire en sorte d'avoir un mot de passe différent sur chaque site et d'un niveau de sécurité assez élevé pour limiter les risques de piratage.

Pour cela vous pouvez essayer de trouver des moyens mnémotechniques : une partie du mot de passe est toujours la même et l'autre partie correspond au nom du site auquel vous êtes inscrit.

Pour corser un peu votre mot de passe, vous pouvez remplacer les caractères classiques par d'autres qu'y leur ressemblent beaucoup, inspirez-vous de ce que vous trouvez sur votre clavier :

- Le **i** par **!** (point d'exclamation)
- Le **A** par le **4**
- Le **E** par le **3**
- Le **o** par le **0**
- Etc.

**Vous pouvez aussi utiliser des générateurs de mots de passe :**

- Générateur de mots de passe de la CNIL
- Générateur de mots de passe de Dashlane
- Générateur de mots de passe de LastPass

# La sécurité sur internet

À partir du moment où vous connectez votre ordinateur (ou autre appareil) à internet, vous l'exposez à un risque d'infection.

Il y a tout de même quelques bonnes pratiques qui vous éviteront la plupart des tracas :

- Ne jamais ouvrir les pièces jointes d'un mail dont vous ne connaissez pas l'expéditeur, si le cas se présente un jour, ignorez-le et supprimez le message.
- Ne communiquez jamais vos informations personnelles par mail : comme vos identifiants et mots de passe. Une structure officielle ne vous demandera jamais ce type d'informations par messagerie.
- Faites attention aux sites sur lesquels vous naviguez, les pirates sont capables de générer des copies de site en tout point dans le but de récupérer vos données au moment où vous vous connecterez. Vérifiez donc qu'il n'y ait pas d'erreur, de lettres supplémentaires ou autres dans l'URL du site.
- Faites attention aux sites sur lesquels vous récupérez l'exécutable pour installer un logiciel. Un site qui paraît trop beau en offrant un logiciel normalement payant peut être très suspect, passez votre chemin.
- Prenez garde aussi aux coches déjà validées lors de l'installation de certains programmes, un programme vous propose parfois d'en installer un autre sans que vous y preniez garde, il peut s'agir de barres d'outils supplémentaires pour votre navigateur, ces outils paraissent inoffensifs mais ils peuvent être les prémices d'un virus plus embêtant.

**Vous pouvez aussi installer un bloqueur de publicité,** ce petit outil sur le principe n'ajoute rien à votre sécurité, il masquera simplement les publicités parfois envahissantes des sites que vous visitez. Ces publicités peuvent parfois vous redirigez, si vous cliquez dessus, vers des sites dangereux.

Il en existe plusieurs :

- UBlock Origin (lien pour Firefox)
- AdBlock Plus
- AdGuard
- Et encore d'autres, n'hésitez pas à faire quelques recherches selon le navigateur internet que vous utilisez

Sur Firefox, il vous est possible d'utiliser la navigation privée, cette option permet de ne pas garder l'historique de navigation, ceci pour éviter que les personnes qui utiliseront le poste après ne puissent pas avoir de vue sur les sites que vous avez consultés.

Firefox – Idées reçues sur la navigation privée

# Bien entretenir votre ordinateur

Il s'agit ici aussi de petites astuces pour garder une machine propre et la plus réactive possible.

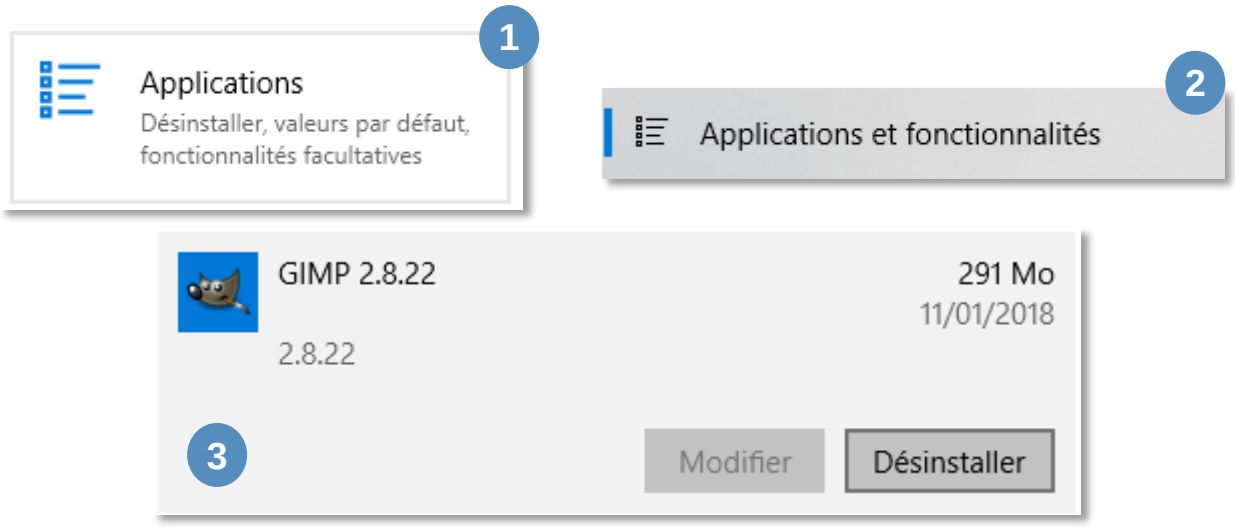
Il faut savoir qu'au fur et à mesure du temps, les documents et applications vont s'accumuler et faire ainsi gonfler le stockage interne de votre appareil. Plus l'espace mémoire sera occupé plus le temps d'ouverture des fichiers ou temps d'exécution des programmes sera long.

C'est inévitable, les mises à jour du système et des applications fournissant plus de services, changeant leur affichage seront plus longues à se lancer …

On peut néanmoins mettre un peu d'ordre et ne garder que ce qui nous intéresse et ce qu'on utilise !

- Faites le tri dans vos photos, vidéos et documents textes et ne garder que l'essentiel (pour les documents très importants, n'hésitez pas à en faire une copie sur un périphérique externe : Clé USB ou disque dur externe).
- Désinstallez les applications que vous n'utilisez plus. Très souvent, nous installons un logiciel pour les services qu'il va nous offrir mais quelques semaines ou mois plus tard, ce logiciel ne nous est plus utile. N'hésitez donc pas à le supprimer et ainsi limiter de la mémoire.

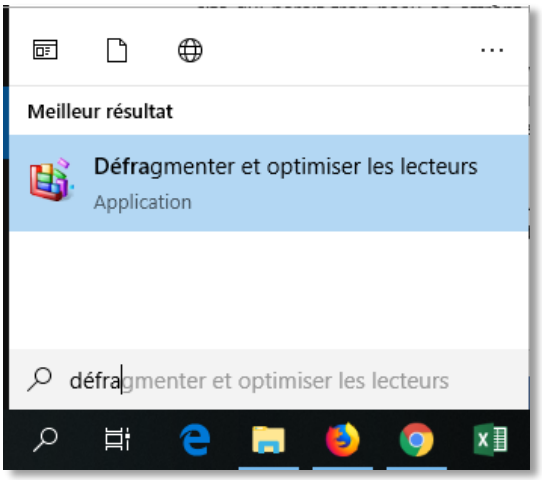
Pour désinstaller une application, accédez aux **Paramètres** depuis le **menu Démarrer** puis à la catégorie **Applications,** cliquez ensuite sur **Applications et fonctionnalités**, choisissez l'application à désinstaller et cliquez sur le bouton **Désinstaller**.



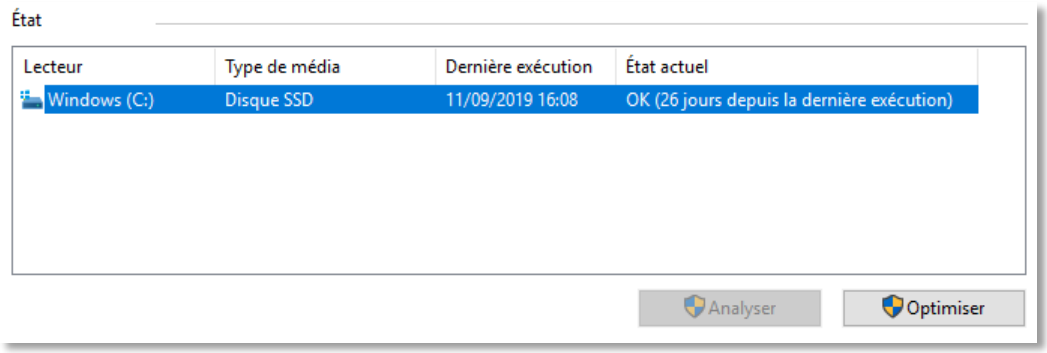

- Utilisez un logiciel de nettoyage comme Ccleaner. Les logiciels de nettoyage vous permettent de supprimer les fichiers temporaires accumulés à cause des navigateurs internet, supprimer le contenu de la corbeille, ainsi que d'autres fichiers plus difficiles à trouver pour des utilisateurs lambda mais que le logiciel repèrent aisément. Vous pouvez récupérer le logiciel gratuitement en cliquant sur ce lien : Télécharger Ccleaner.

**Enfin, pensez à défragmenter votre ordinateur de temps en temps**. La défragmentation permet de regrouper côte à côte sur le disque dur les fichiers qui composent un même programme/dossier accélérant ainsi son temps d'ouverture ou d'exécution.

- Pour défragmenter votre PC, saisissez **Défragmenter** dans la zone de recherche de la barre de tâches et cliquez sur l'application :




- Sélectionnez ensuite une à une les différentes partitions de votre disque (la seule s'il n'y en a qu'une) et cliquez sur le bouton **Optimiser**. Cette opération peut prendre plusieurs dizaines de minutes s'il y a beaucoup de déplacements à faire et si votre ordinateur est un peu lent.




Vous trouverez facilement d'autres informations à l'aide d'un moteur de recherche, faites cependant attention à la date de rédaction des articles. Les mesures de sécurité sont en constantes évolution et les manipulations d'hier ne seront plus valables aujourd'hui. Pensez également à vérifier les informations sur un autre site.

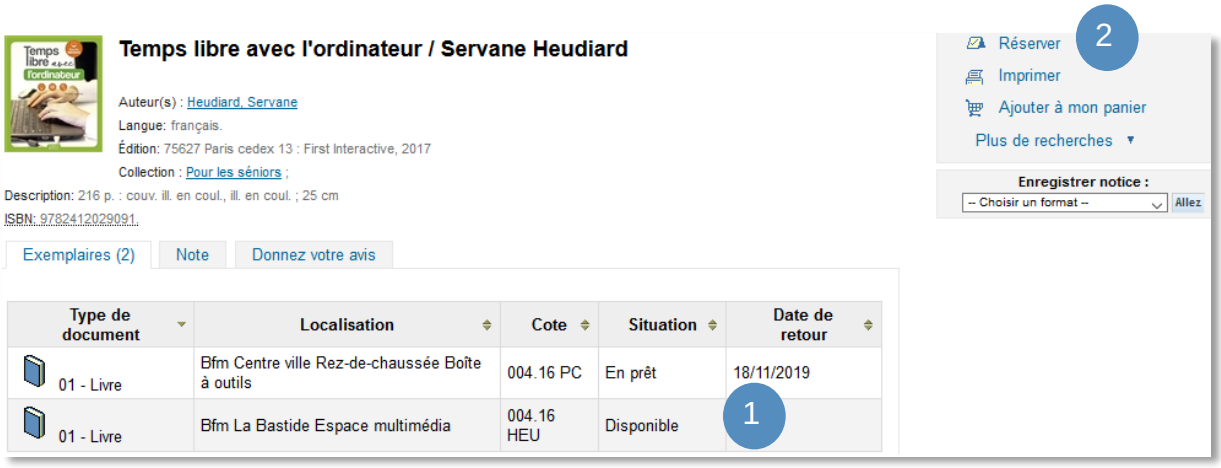
**Quelques ressources supplémentaires :**

- Hintigo - Comment protéger son PC des virus ?
- Comment ça marche – Sécurisation de son PC
- Wikipédia – Virus informatique

# Documents empruntables à la bibliothèque

Ci-dessous, quelques ouvrages disponibles sur le réseau de la Bfm. **Les titres et les couvertures des documents sont cliquables** : ils vous amèneront directement à la page du catalogue, où vous pourrez voir la disponibilité du document.

**S'il est disponible** vous pouvez le récupérer directement ou demander à ce qu'il soit transféré dans la bibliothèque du réseau que vous visitez le plus souvent. **Et si le document est emprunté**, connectez-vous à votre compte lecteur et réservez-le.




Maintenez la touche **Ctrl** enfoncée et cliquez sur le titre ou l'image pour ouvrir le catalogue


***Comment protéger votre vie numérique* / Michèle Germain**
005.8 GER

Vous trouverez dans cet ouvrage des informations sur les virus et les arnaques et plus précisément les différentes formes qu'ils peuvent prendre. Vous y trouverez également des astuces sur la manière de maintenir votre appareil (ordinateur, smartphone ou tablette) à jour et naviguer en tout sérénité, etc.


***Sécurité sur internet* d'Isabelle Ostermann**
005.8 OST

Ce document aborde de manière un peu moins détaillée mais dans des paragraphes plus aérés et sur pages couleurs les mêmes sujets que le précédent ouvrage. En supplément à la fin, vous pourrez tester vos connaissances à l'aide d'un quizz et approfondir votre vocabulaire avec un petit lexique sur les termes utilisés pour internet.