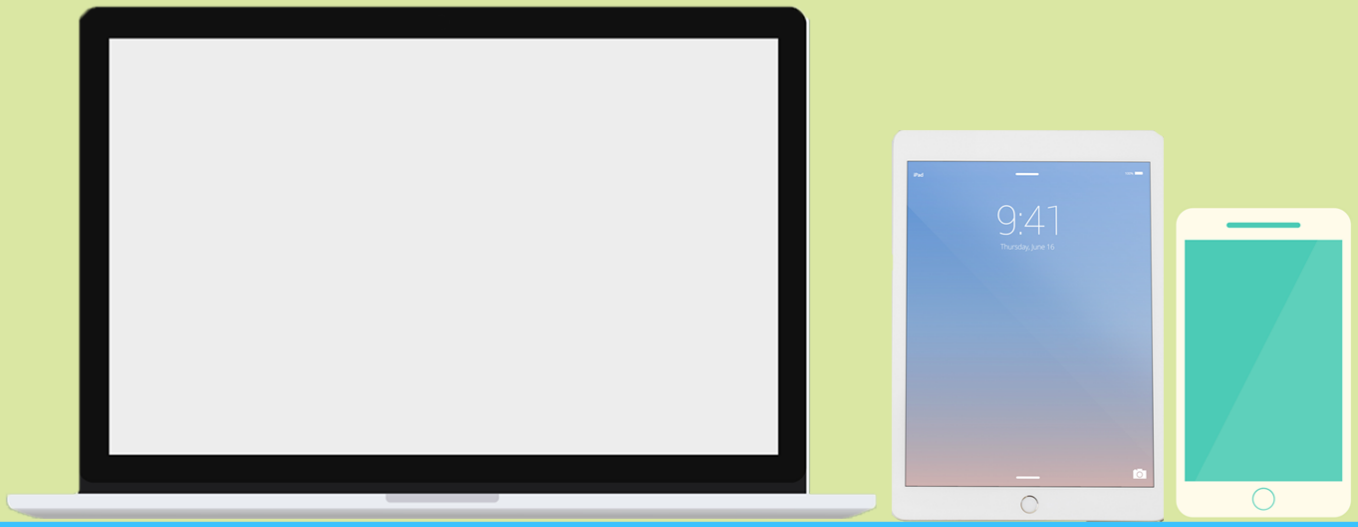
14 conseils (et outils) indispensables pour bien PROTEGER ses données personnelles



lebonantivirus.com

Ce document est offert par :

Savez-vous qu'il n'existe aucune solution de sécurité qui vous protège à 100% ?

Ni l'antivirus, ni le pare-feu, ni le VPN…

Il existe toujours des failles de sécurité exploitables par les cybercriminels.

En plus de ces failles, il y a l'utilisateur !

Un utilisateur qui manque de connaissances peut-être piraté facilement.

C'est pourquoi j'ai préparé cette **liste de contrôle de sécurité**, pour aider les utilisateurs de Windows à bien protéger leur ordinateur et par conséquent, leurs données et leur vie privée.

1 Configurer la mise à jour automatique de votre système d'exploitation

Que ce soit le système d'exploitation que vous utilisez, Windows ou Mac OS, vous devez configurer les mises à jour automatiques. Cela garantie que votre système reçoit tous les correctifs de sécurité diffusés par son développeur.

La même chose aussi pour les smartphones et tablettes, assurez-vous toujours que le système de votre smartphone ou tablette est bien à jour.

Comment faire

Pour vérifier les mises à jour dans Windows 10, cliquez sur le bouton Démarrer , puis accédez à **Paramètres** > **Mise à jour et Sécurité** > **Windows Update**. Si Windows Update indique que votre appareil est à jour, cela signifie que vous disposez de toutes les mises à jour actuellement disponibles. Pour garder votre système à jour, il est recommandé d'activer les mises à jour automatiques (Windows XP, 7, Vista et Windows 10).

Pour installer les mises à jour sur un smartphone sous android ou iOS, suivez l'un de ces tutoriels :

1. http://www.phonandroid.com/comment-mettre-a-jour-android-installer-derniere-version.html
2. https://support.apple.com/fr-fr/ht204204

2 Mettre à jour tous les logiciels

Un logiciel obsolète ou non mis à jour installé sur votre ordinateur présente une réelle faille de sécurité, il peut être exploité par les pirates pour s'infiltrer facilement dans votre ordinateur.

Assurez-vous donc de mettre à jour régulièrement tous les logiciels installés sur votre ordinateur, en particulier le navigateur Web, Java et l'antivirus.

Comment faire

Utilisez Secunia PSI, un logiciel de sécurité gratuit et facile à utiliser, pour vérifier et mettre à jour les logiciels vulnérables sur votre ordinateur.

3 Installer un bon logiciel de protection

Il faut avoir un logiciel de protection à jour en cours d'exécution sur votre ordinateur. Il est vrai que l'antivirus ne protège pas votre ordinateur à 100% mais l'existence d'un antivirus diminue le risque d'infection par les virus et logiciels malveillants.

Téléchargez et installez un bon logiciel antivirus.

4 Assurez-vous que le pare-feu est bien activé et opérationnel

Que ce soit un pare-feu intégré à votre logiciel antivirus ou celui de Windows, assurez-vous toujours qu'il est en état de marche.

Comment faire

Quand il s'agit d'un pare-feu intégré au logiciel antivirus, généralement vous avez une icône ou un onglet qui vous permet d'accéder aux paramètres de pare-feu. Quant à Windows, vous pouvez suivre ce tutoriel : http://www.windows8facile.fr/w10-configurer-pare-feu-firewall/

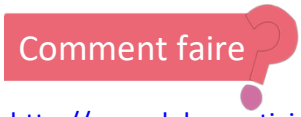
5 Créer des mots de passe sécurisés

Les mots de passe restent aujourd'hui encore la forme la plus courante et la plus utilisée pour protéger l'accès à nos comptes bancaires en ligne, messagerie, données sensibles et privées. C'est pourquoi il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à deviner par les pirates.

- Un bon mot de passe doit contenir au moins 12 caractères
- Utilisez une combinaison de majuscules, minuscules,symboles, nombres et espaces dans vos mots de passe, exemple : P@$$W000rD!!2019
- Evitez d'utiliser un mot de passe trop court
- Evitez d'utiliser le même mot de passe sur plusieurs comptes

6 Protégez vos données importantes

La meilleure façon de protéger ses données est de les sauvegarder, sur un disque dur externe ou sur une plateforme de sauvegarde en ligne.



http://www.lebonantivirus.com/procedure-de-sauvegarde-windows-tutoriel/

7 N'installez des logiciels que s'ils proviennent d'une source fiable

Une grande partie des virus et logiciels malveillants sont diffusés via les sites de téléchargement, en particulier les sites de téléchargement de logiciels.

Dans la mesure du possible, n'installez que les logiciels téléchargés par vous-même depuis des sites de téléchargement fiables.

8 Limiter les installations

Chaque fois que vous installez un logiciel, extension, barre d'outils. Rappelez-vous que vous créez plus de sources d'intrusions potentielles et vous laissez des trous ouverts dans votre système qui peuvent être exploités par les pirates informatiques.

1. Supprimer les logiciels préinstallés sur votre ordinateur
2. Faire un nettoyage de tous les logiciels que vous n'utilisez pas

9 Ne jamais faire enregistrer vos informations d'identification sur le navigateur web

Les navigateurs web vous suggèrent souvent d'enregistrer vos informations d'identification, et vos coordonnées bancaires que vous saisissez lorsque vous accédez à des sites web.

Cette fonctionnalité est très utile car il vous permet de gagner de temps, mais il est très dangereux pour votre sécurité. En cas de perte de votre ordinateur ou si un pirate arrive à accéder à votre PC, il peut facilement récupérer tous ces informations.

10 Utilisez un VPN quand vous êtes connecté à un wifi public

Au restaurant, à l'hôtel, lorsque vous vous connectez à Internet en utilisant un wifi public, les données échangées par votre ordinateur ou smartphone peuvent être surveillées et capturées par des personnes malhonnêtes. La solution pour se connecter en toute sécurité sur des réseaux wifi publics, est d'installer un VPN.

C'est quoi un VPN : http://www.lebonantivirus.com/qu-est-ce-qu-un-vpn-a-quoi-sert-un-vpn/

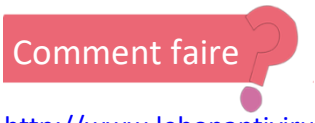
Les meilleurs VPN : http://www.lebonantivirus.com/meilleur-vpn-pas-cher/

11 Sécurisez votre réseau domestique

La protection du réseau domestique concerne le routeur, l'interface entre l'utilisateur et internet. La plupart de ces appareils sont préconfigurés pour une utilisation immédiate.

Après l'installation des routeurs, souvent, les utilisateurs se connectent directement à internet sans effectuer une configuration supplémentaire. Malheureusement, la configuration par défaut de la plupart des routeurs offre peu de sécurité et laisse les réseaux domestiques vulnérables aux attaques.

Il est donc nécessaire de prendre de votre temps et configurer les paramètres de sécurité de votre routeur.



http://www.lebonantivirus.com/les-10-etapes-cles-pour-securiser-son-reseau-wifi/

12 Installer un contrôle parental

Si vous avez des enfants, il est conseillé d'installer un logiciel de contrôle parental pour contrôler l'accès à certaines fonctionnalités sur votre ordinateur.

Remarque : Une suite de sécurité contient un logiciel de contrôle parental

13 Évitez d'ouvrir les courriels inconnus, pièces jointes et les liens hypertexte cliquables

- N'ouvrez jamais d'emails ou de pièces jointes provenant d'une source inconnue ou suspecte.
- Soyez prudent lorsque vous cliquez sur les liens, que ce soit dans un email ou sur les réseaux sociaux.
- Ne cliquez jamais sur un lien avant de le scanner avec votre antivirus ou en utilisant cet outil de scan en ligne.

14 Protégez-vous de « phishing »

Les arnaques de phishing sont une menace constante. En utilisant diverses méthodes de ciblage, les cybercriminels tenteront de vous inciter à divulguer des informations personnelles comme votre identifiant de connexion et votre mot de passe ou les informations de votre carte de crédit, etc.

Méfiez-vous d'un message électronique ou d'un appel téléphonique qui demande des informations personnelles ou financières.

Consultez notre article sur le phishing pour plus de détails, et surtout savoir comment s'en protéger ?