Module : Naviguer en toute sécurité

1-Introduction à la sécurité internet

● **Article 1 = ANSSI - Dix règles d'or préventives**

Source : https://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regle-de-base/

● **Article 2** =MINISTERE DE L'ECONOMIE DES FINANCES ET DE LA SOUVERAINETE INDUSTRIELLE ET NUMERIQUE- Comment assurer votre sécurité numérique

Source : https://www.economie.gouv.fr/particuliers/comment -assurer-securite-numerique/

● **Article 3** = SiteW - Naviguez en toute sécurité sur Internet

Source : https://www.sitew.com/

2 - Créer des mots de passe forts

Utilisation de gestionnaire de mot de passe Lastpass.

Crée un compte en remplissant le formulaire.On doit choisir un mot de passe maitre . Le mot de passe choisit doit avoir de sécurité élévé . Cet mot de passe unique nous permet d'acceder à tous nos comptes. Pour le faire

- Télécharger l'extension sur ton navigateur
- Ajouter dans chrome
- Une fois installé, il te suffit d'accéder à cette extension et de t'y connecter
- (1) En haut à droite du navigateur, clic sur le logo "Extensions"
- (2) Épingle l'extension de LastPass avec l'icône
- Il ne te reste plus qu'à te connecter en effectuant un clic sur l'icône de
- l'extension et en saisissant ton identifiant et mot de passe

Désormais, lorsque tu te connectes à tes comptes, tu peux enregistrer le mot de passe grâce à LastPass.

Tu peux également ajouter des comptes manuellement en accédant au coffre-fort, espace de stockage de tous tes mots de passe. Pour y accéder, clic sur l'icône de l'extension puis sur "Ouvrir mon coffre-fort".

Tu arrives alors sur une page de gestion de ton compte LastPass. Pour ajouter un site et une connexion associée (identifiant + mot de passe), accède à la rubrique “Mot de passe” (2) et (3) puis clic sur “Ajouter un élément” (1).

Une fenêtre s’ouvre pour y insérer toutes les informations à retenir pour automatiser la prochaine connexion. LastPass demande l’URL du site en question ; on conseille de mettre l’URL de la page de connexion du site. Ensuite préciser l’id et le mot de passe. On peut personnaliser le nom, un commentaire associé ou encore un dossier si besoin.

Tu connais maintenant les grandes lignes de l’utilisation du gestionnaire de mot de passe LastPass.

Pour aller plus loin :

L’abonnement gratuit (freemium) te permet de faire les tâches principales. Si tu trouves cet outil incontournable, tu peux passer au compte premium. Il te permettra notamment de synchroniser ton compte LastPass sur tous les supports utilisés.

3 . **Fonctionnalité de sécurité de votre navigateur**

Identifier les éléments à observer pour naviguer sur le web en toute sécurité

1. Les sites web qui semblent être malveillants sont :

● www.morvel.com, un dérivé de www.marvel.com, le site web officiel de l’univers Marvel

● www.fessebook.com, un dérivé de www.facebook.com, le plus grand réseau social du monde

● www.instagam.com, un dérivé de www.instagram.com, un autre réseau social très utilisé

Les seuls sites qui semblaient être cohérents sont donc :

● www.dccomics.com, le site officiel de l’univers DC Comics

● www.ironman.com, le site officiel d'une compétition internationale de triathlon (et non

du super-héros issu de l'univers Marvel)

2. Tester si le navigateur qu'on utilise est à jour ?

On ouvre le menu, puis aller dans le parametre et cliquer sur le rubrique Apropos de chrome

On doit trouver chrome à jour sinon la version de chrome n'est pas à jour, pour moi j'utilise encore le windows 8 donc la mise à jours de chrome n'est pas automatique

Pour tester la mise à jour de firefox, on clique sur le menu de navigation, puis accéde au parametre et dans la rubrique "Général", on fait défiler jusqu'à voir la section "Mise à jour de

Firefox . Pour moi c'est bien le firefox est à jours

Comme on a pu le constater, les paramètres par défaut de ces deux navigateurs sont réglés

pour réaliser les mises à jour automatiquement. Comme d'habitude, Firefox affiche une

personnalisation des paramètres un peu plus poussée.

4. Eviter les spam et les phishing

Reconnaître plus facilement les messages frauduleux

Pour proteger contre les escroqueries par e-mail, les logiciels malveillants et le vol d'identité, on doit comprendre comment identifier et éviter le contenu potentiellement dangereux dans la boite de réception, y compris le spam et le tentatives de phishing .

on va exercer ta capacité à déceler les erreurs dans les messages cachant une action malveillante en arrière-plan.

Le Hameçonnage et légitime

Le Hameçonnage :il était difficile à repérer .Les documents PDF peuvent contenir des logiciels malveillants ou des virus. On doit vérifier toujours l'expéditeur est digne de confiance, et utilise un navigateur ou un service en ligne comme Google Drive pour les ouvrir en toute sécurité. Parfois les avertissements qu'il nous envoie est exacte mais les liens qu'il nous donne ne dirige pas vers le site exacte.

La communication légitime : L'expéditeur est « dropboxmail.com, qui est une entité inhabituelle mais légitime, et URL est un lien sécurisé (https) vers dropbox.com.

5. Comment éviter le logiciel malveillant

Objectif : sécuriser l'ordinateur et identifier les liens suspects

Lors de la navigation sur le web, il arrive d'avoir des doutes sur la sécurité de certains sites. Comme tu as pu le voir précédemment, le premier de niveau de vigilance à avoir se trouve dans la barre d'adresse des navigateurs web. La plupart affichent des indicateurs de sécurité pour donner une information sur la protection d'un site internet. Site n°1

- Indicateur de sécurité
  - HTTPS
- Analyse Google
  - Aucun contenu suspect

- Site n°2
  - Indicateur de sécurité
    - Not secure
  - Analyse Google
    - Aucun contenu suspect

- Site n°3
  - Indicateur de sécurité
    - Not secure
  - Analyse Google
    - Vérifier un URL en particulier (analyse trop générale)

Tu peux tester la sécurité d'autres sites à partir de ce lien. Ce site référence et explique les défauts de sécurité des sites dans le monde.

6. Achat en ligne sécurisés

Objectif : créer un registre des achats effectués sur internet

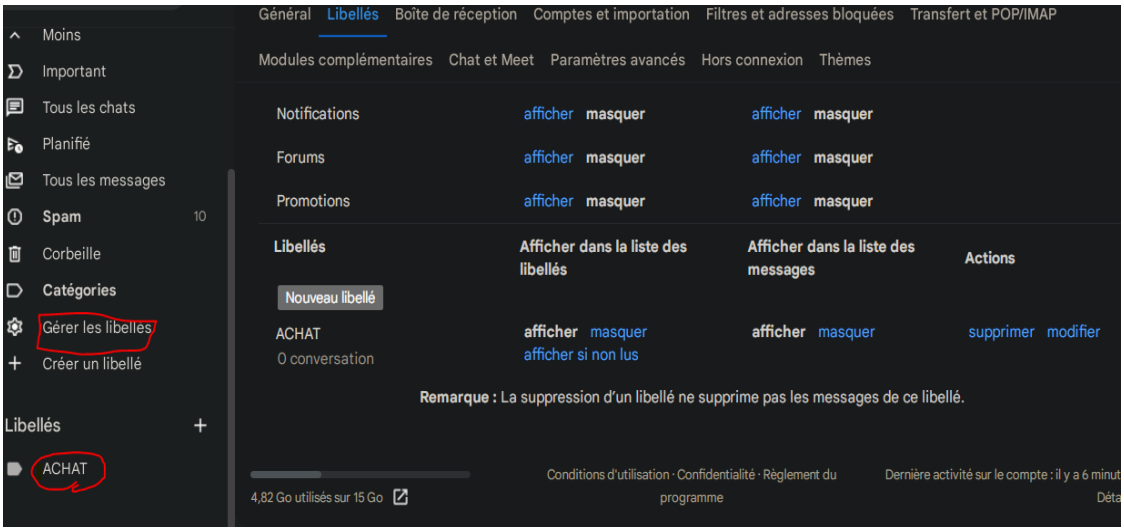
On va créer un registre des achats en ligne, le registre a pour but de conserver les informations de clients relative au achat en ligne . Très pratique lorsque on fait face à un litige, un problème sur la commande ou tout simplement pour faire le bilan de des dépenses du mois. Deux possibilités s'offrent à toi pour organiser ce registre :

1. Créer un dossier sur la messagerie électronique

2. Créer un dossier sur l'espace de stockage personnel (en local ou sur le cloud). Les étapes à suivre pour créer un registre des achats sur ta messagerie électronique.

Pour commencer, on doit accéder à la messagerie électronique. On peut yaccéder rapidement en ouvrant un nouvel onglet (dans la barre des favoris ou via le raccourci). Sur la page d'accueil de la messagerie, on trouvera sur la gauche les libellés initialement prévus (boite de réception, messages envoyés, etc.).

C'est dans cette partie que on va créer la rubrique des achats. Pour ce faire, on clic sur "Plus" et on va tout en bas des libellés. Pour créer un libellé rapidement il suffit d'effectuer un clic sur "Créer un libellé" et de le nommer "ACHATS" (pour notre exercice). On effectue un clic sur le bouton "Créer" pour valider l'opération .



Voici un exemple d'organisation de libellé pour gérer sa messagerie électronique :

● Achats : historique, facture, conversations liés aux achats

● Administratif : toutes les démarches administratives

● Banque : tous les documents et les conversations liés à la banque personnelle

● Création de compte : tous les messages liés à la création d'un compte (message de bienvenue, résumé du profil, etc.)

● Job : tous les messages liés à mon projet professionnel

● SAYNA : tous les messages liés mon activité avec SAYNA

7. **Comprendre le suivi de navigateur**

Objectif : exercice présent sur la gestion des cookies et l'utilisation de la navigation privée

Accéder au paramètre de navigation , puis aller dans paramètre et puis cliquer sur historique chrome et supprimer les données de navigation.

8 - Principes de base de la confidentialité des médias sociaux

Objectif : Régler les paramètres de confidentialité de Facebook

Paramètre de confidentialité sur Facebook

Comme tous le site Facebook aussi utilise de paramètre pour mettre en sécurité les données , on peut les personnalisés. On a déjà été amené à utiliser ce réseau social en partageant une publication. Pour faire la configuration il suffit de cliquer sur le menu puis parametre , paramètre et confidentiel

Ce sont les onglets “Confidentialité” et “Publications publiques” qui nous intéressent.

Accède à “Confidentialité” pour commencer et clic sur la première rubrique.

Cette rubrique résume les grandes lignes de la confidentialité sur Facebook

○ La première rubrique (orange) te permettra de régler la visibilité de tes informations personnelles

○ La deuxième rubrique (bleu) te permet de changer ton mot de passe

○ La troisième rubrique (violet) te permet de gérer la visibilité de ton profil pour la gestion des invitations

○ La quatrième rubrique (vert) permet de gérer la connexion simplifiée sur des applications ou des sites utilisés qui permettent cela

○ La dernière rubrique (rose) permet de gérer les informations récoltées par Facebook utiles pour les annonceurs

Lorsqu’on retourne dans les paramètres généraux en effectuant un clic sur la croix en haut à gauche. on peut continuer à explorer les rubriques pour personnaliser des paramètres. On choisit les informations qu’on souhaites partager et celles qu’on veut garder privées. Voici tout de même quelques conseils :

○ Si on utilises un compte Facebook uniquement pour communiquer avec les amis, règles les paramètres en conséquence en choisissant une visibilité “Amis” ou “Amis de leurs amis”.

○ Beaucoup de personnes utilisent Facebook en mêlant réseau professionnel et réseau personnel . Il existe **LinkedIn** pour utiliser un média social pour le réseau professionnel

○ Pour limiter les haters et les commentaires malveillants, tu peux restreindre les commentaires des publications. Ça se passe dans l'onglet "Publications publiques"

● Dans les paramètres de Facebook on a également un onglet "Cookies". On 'en a

parlé dans le cours précédent (Comprendre le suivi du navigateur). Maintenant qu'on sait comment sont utilisées les données, on es capable de choisir en plein conscience ce que'on souhaites partager.

Voici un exemple de paramétrage de compte Facebook pour une utilisation privilégiant les échanges avec les amis, mais autorisant le contact avec des inconnus (limite de leurs actions) :

● Confidentialité

On peut utiliser le paramètre de confidentialité aussi avec les autres réseaux sociaux comme Tweeter, Instagram,

9. Que faire si votre ordinateur est infecté par un virus

Les logiciels malveillants sont l'un des dangers les plus courants pour notre ordinateur lorsqu'on est en ligne, mais n'est facile de les éviter.. Même si on ne voit aucun signe de malware sur l'ordinateur, l'exécution de l'analyse régulière peut détecter tout malware qui a échappé à notre attention. La mise à jour de système d'exploitation, de notre navigateru et d'autres programmes de de sécurité est une étape importante dans la protection de notre ordinateur.

Il est parfois arrivé que le logiciel antivirus installé sur notre ordinateur soit incapable de détecter de nouveau virus, vers ou chevaux de Troie, même s'il est à jour. La tristesse vérité est qu'aucun logiciel antivirus ne peut nous garantir une sécurité fiable 100%.

Si un ordinateur est infecté par un virus, on doit déterminer l'origine de l'infection, identifier le fichier infecté et l'envoie au fournisseur dont le produit n'a pas détecté le logiciel malveillant et n'a pas réussi à protéger l'ordinateur.

La première chose à faire est d'assurer que les bases de données de notre antivirus sont à jour pour ensuite réaliser une analyse de notre ordinateur. Si cela n'aide pas, les solutions antivirus d'autres fournisseurs pourraient faire l'affaire. Si un antivirus ou un cheval de Troie est détecté,

assurez-vous d'envoyer une copier du fichier infecté à l'éditeur de la solution antivirus qui n'a pas réussi à le détecter avant. Si un autre antivirus ne détecte pas de malware, on vous recommande de déconnecter l'ordinateur d'internet ou du réseau local, de désactiver la connexion Wifi et le modem, avant de rechercher des fichiers infectées. Evitez d'utiliser des données personnelles ou confidentielles.

2.

Un **antivirus** est un logiciel installé sur votre ordinateur qui a pour objectif de vous **protéger** des principales **menaces d'Internet** tels que les **virus** et les programmes **malveillants** (cheval de Troie, logiciel espion,…).

Cet outil va **vérifier** tous les fichiers que vous téléchargez ou que vous exécutez sur votre ordinateur. Des opérations de **scan de fichiers** peuvent être **planifiées** ou lancées à la demande pour **analyser** un fichier, un dossier ou l'ensemble des documents enregistrés sur votre disque dur.

Dans le cas où un **virus** est détecté, celui-ci est **neutralisé** soit en étant placé en **quarantaine** avant d'être **éliminé** ou soit en étant directement **supprimé**.

Certains antivirus proposent également des **protections Internet** qui bloquent les sites ou les téléchargements qui peuvent présenter un **risque pour vos données**.

En ce qui concerne le tarif pour **bien protéger son PC**, il existe aujourd'hui de très bonnes solutions **gratuites** qui seront suffisantes pour la majorité des personnes. Les **solutions payantes** proposent souvent plus de fonctionnalité et offre un **support aux utilisateurs** pour quelques euros par an.

De nouvelles **menaces** apparaissent chaque jour, c'est pourquoi il est très important de garder constamment votre **logiciel antivirus à jour**. Toutefois, que vous choisissiez une solution gratuite ou payante, il n'existe pas et il n'existera jamais une solution antivirus **100% sécurisée**. Votre bon sens et votre prudence seront vos plus grands atouts pour éviter les **infections**.

Pour les personnes ayant un ordinateur sous **Windows 10**, je vous donnerai dans la suite de l'article les étapes pour activer l'antivirus intégré **Windows Defender**. Ce n'est certainement pas **le meilleur antivirus** mais il possède des avantages non négligeables, et notamment le fait d'être simple d'utilisation. De plus, cette solution est largement suffisante pour un usage

classique d'un ordinateur(vous ne **naviguez** pas sur des sites louches, vous ne **téléchargez pas** des logiciels n'importe où et vous n'ouvrez pas les **pièces jointes** des mails sans méfiance!).

Pour les autres personnes, je listerai à la fin de l'article, des solutions gratuites et payantes reconnues et **recommandées** pour leur **efficacité**

Quel est le rôle du pare-feu?

De nos jours, la majorité des ordinateurs et autres périphériques sont **connectés à Internet**. Cette hyper-connectivité implique de nombreux **échanges de données** entre votre ordinateur et Internet. L'exemple le plus simple est lorsque vous **surfez sur Internet** sur votre navigateur préféré (**Edge**, **Chrome**…). Ce dernier échange des **données** avec **Internet** pour les afficher sur votre écran d'ordinateur. Mais d'autres logiciels échangent des données en arrière-plan pour par exemple vérifier les **mises à jour disponibles**, télécharger la base de **virus** pour que votre **antivirus** soit à jour…

Le rôle du **pare-feu** ou **firewall** en anglais est de vous donner une vision de tous ces échanges et vous permettre d'autoriser ou non les différents échanges. Ainsi lorsque le **pare-feu** détectera un nouvel échange, il vous demandera la permission de continuer ou non. Ainsi si un **logiciel malveillant** s'installe malencontreusement sur votre machine, le **pare-feu** peut être un moyen de le détecter et de stopper sa propagation en coupant l'**accès Internet** de l'**application frauduleuse**.

Pour nos débuts sur **Internet**, je vous recommanderais le **pare-feu intégré à Windows**. Il n'est pas parfait, mais peut largement suffire à toutes personnes qui **naviguent** prudemment sur **Internet**. C'est l'outil a privilégier pour les débutants, les personnes plus à l'aise pourront installer un autre logiciel si le besoin s'en fait sentir.

Présentation de la solution de sécurité Windows

Windows 10 propose nativement un **antivirus** et un **pare-feu** respectivement nommés **Windows Defender** et **Pare-feu Windows**. Comme je l'évoquais dans les paragraphes précédents, ces deux solutions sont de bons produits et ils protégeront la majorité des utilisateurs.

Comme nous le verrons dans un article dédié aux bonnes pratiques de la **navigation sur Internet**, ces solutions s'intègrent dans une pack sécurité plus complet qui comprend notamment le **navigateur Edge** qui propose également une **protection** suffisante et efficace.

Voici les principaux avantages d'utiliser les solutions de sécurité proposées par **Windows** :

- **Simplicité d'utilisation** : les solutions de **sécurité Windows** sont directement intégrées dans le système d'exploitation. Contrairement à des **solutions logicielles** tierces souvent en anglais, l'installation est totalement transparente.De plus, les solutions antivirus commerciales ont la fâcheuse tendance à afficher périodiquement des promotions et offres. Avec la solution Windows vous n'aurez pas ce désagrément.
- **Efficacité** : l'environnement **Windows,** s'il est configuré et utilisé correctement, offre une sécurité et un confort d'utilisation incontestable. Pour cela il est recommandé d'accepter les **mises à jour Windows**, utiliser le navigateur **Edge** et télécharger le plus possible vos applications sur le **Windows Store.**
- **Confortable** : l'**antivirus** et le **pare-feu Windows** ne dégradent pas les performances de votre ordinateur. Les solutions logicielles de sécurité sont souvent gourmandes et peuvent alors ralentir votre pc.

Comment activer la solution de sécurité Windows

Le pas à pas suivant est destiné aux personnes qui possèdent Windows 10, mais celui-ci peut s'appliquer avec peu d'adaptation aux versions précédentes de Windows (Windows 8).

Supprimez les éventuelles solutions de sécurité existante

Il est fortement recommandé de n'activer qu'une seule **solution de sécurité** sur un même ordinateur. Lors de l'achat d'un nouvel ordinateur, un **antivirus** commercial peut être installé par défaut. Vous en serez rapidement informé car ces logiciels sont souvent des versions de

démonstration. Du coup, au bout d'un certain temps l'application vous demandera d'acheter la **solution** pour rester **protégé**.

Je vous conseille donc dans un premier temps de désinstaller ce type de logiciel. Pour vous aider, voici une liste des principaux **antivirus** du marché :

- **Avast** Free AntiVirus
- **AVG** Internet Security
- **Avira** Antivirus Pro
- **Bitdefender** Internet Security
- **Comodo** Internet Security Premium
- **Kaspersky** LabKaspersky Lab Internet Security
- **McAfee** Internet Security
- **Norton** Norton Security
- **Trend** MicroTrend Micro Internet Security

Nous verrons dans un prochain article comment installer et désinstaller un programme. Si vous ne savez pas comment procéder voici les principales étapes :

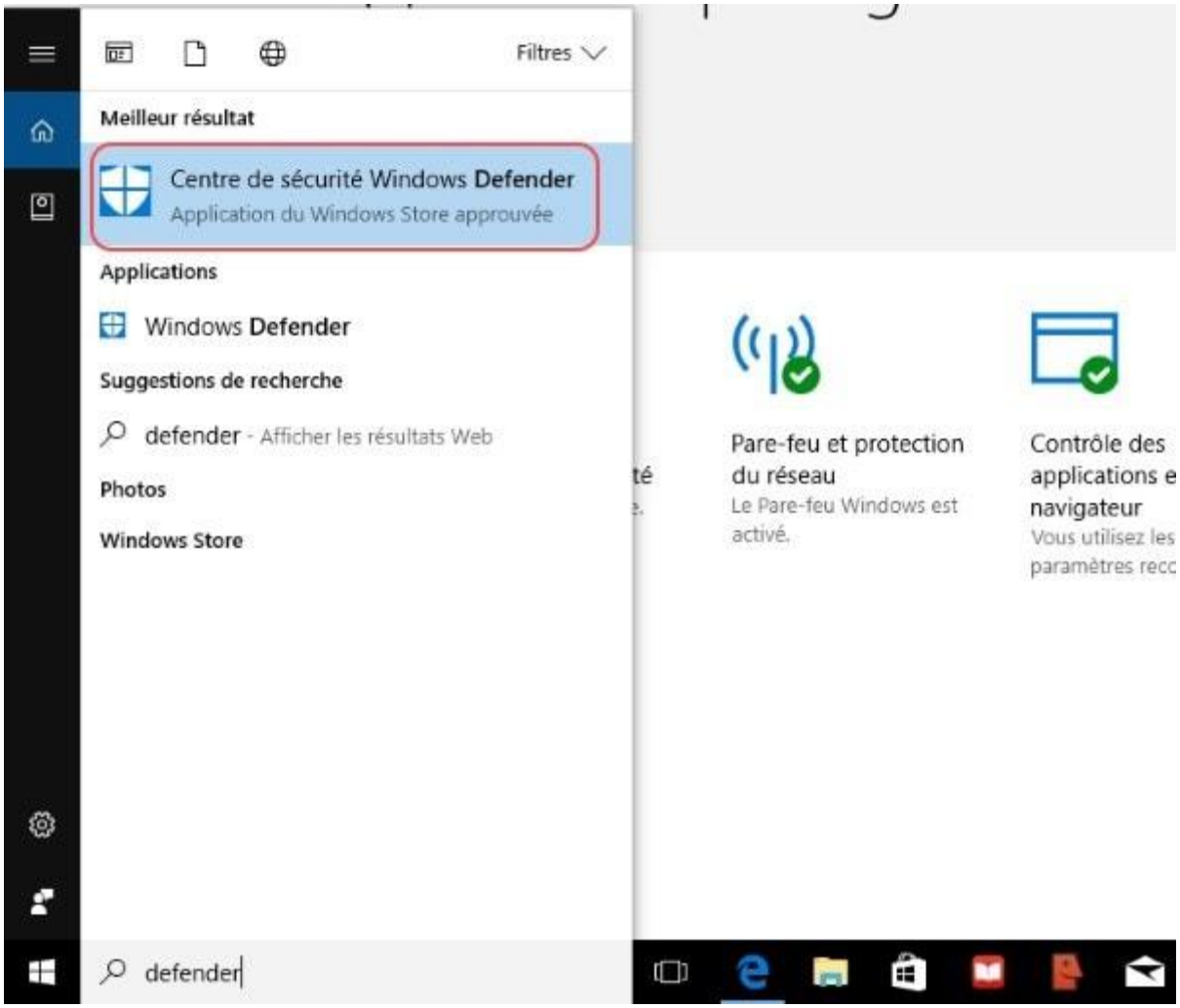
1. Saisissez et cliquez sur **Ajouter ou supprimer des programmes**(écrire les premiers caractères) dans le champ **Cortana**
2. Rechercher dans la liste un antivirus
3. Cliquez sur désinstaller puis suivez les instructions

Dans le cas où vous rencontrez des problèmes, demandez de l'aide sur le Forum Le Coin Retraite

Activer l'antivirus Windows Defender

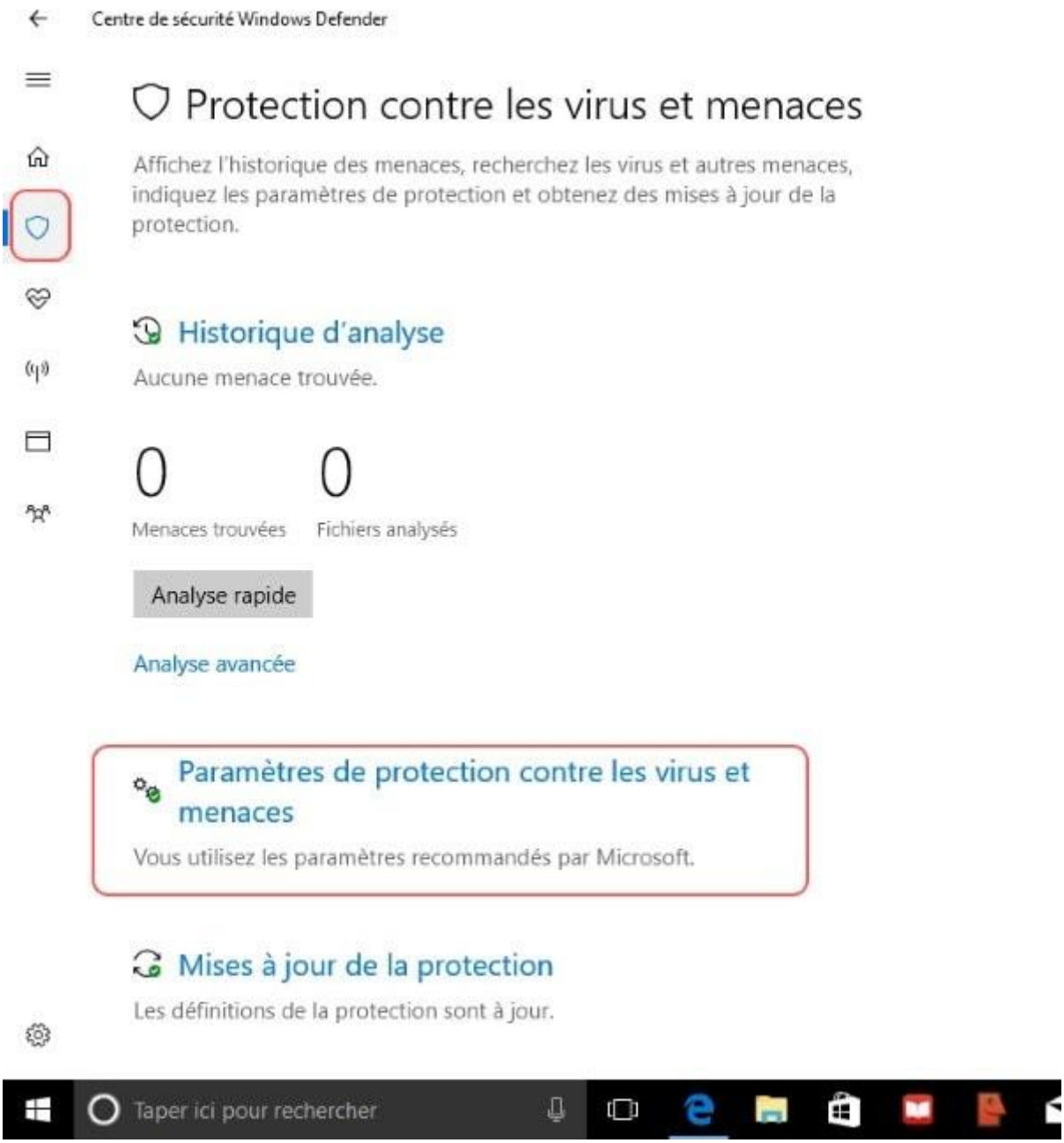
Pour savoir si **Windows Defender** est activé sur votre ordinateur suivez les étapes suivantes:

1. Tapez et cliquez sur **Centre de Sécurité Windows Defender** dans **Cortana**

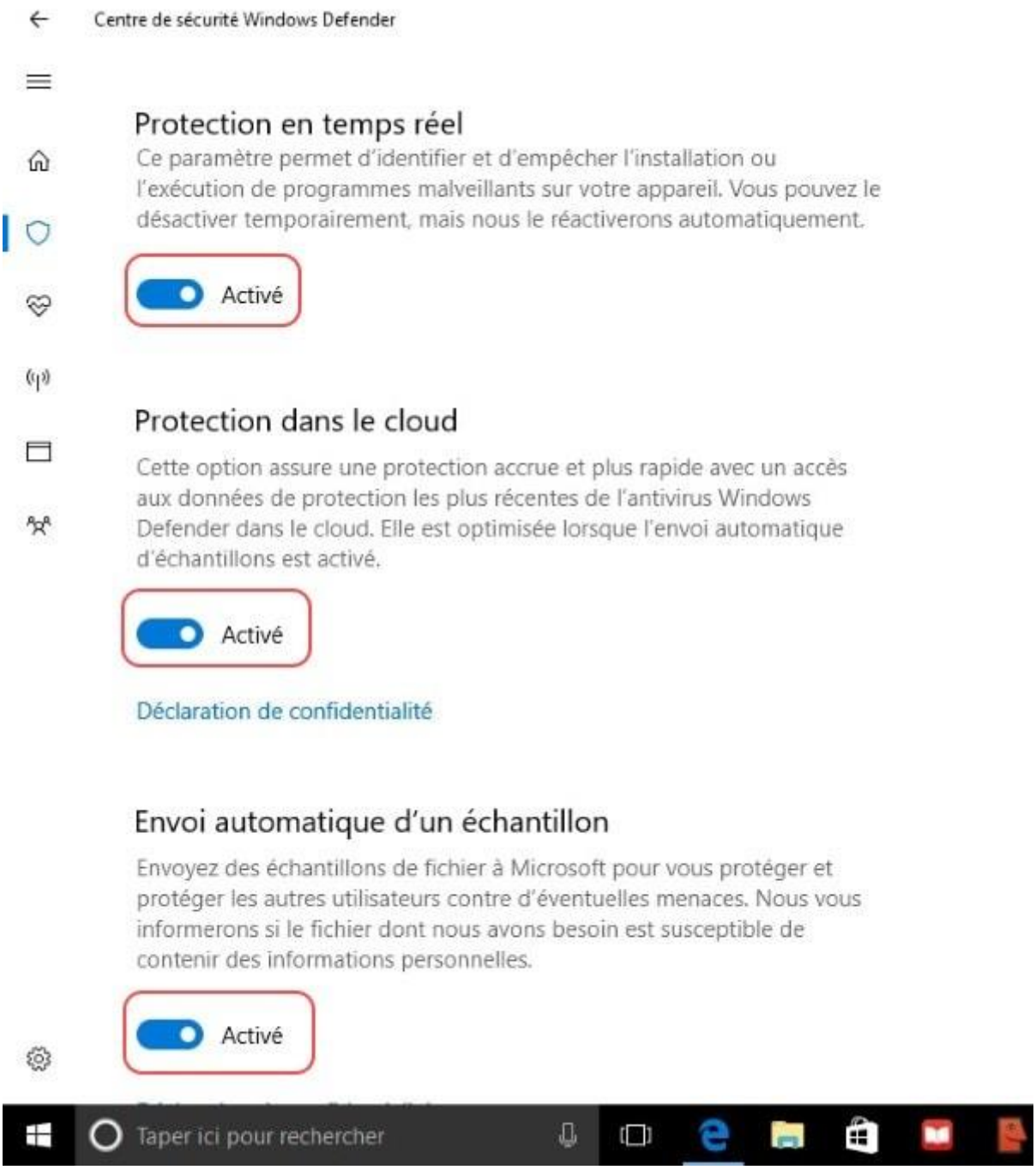


2. La fenêtre **Centre de Sécurité Windows Defender** s'ouvre. Dans celle-ci, cliquez sur le **petit bouclier** dans le menu de gauche, puis cliquez sur **Paramètres de protection contre**

les virus et menaces



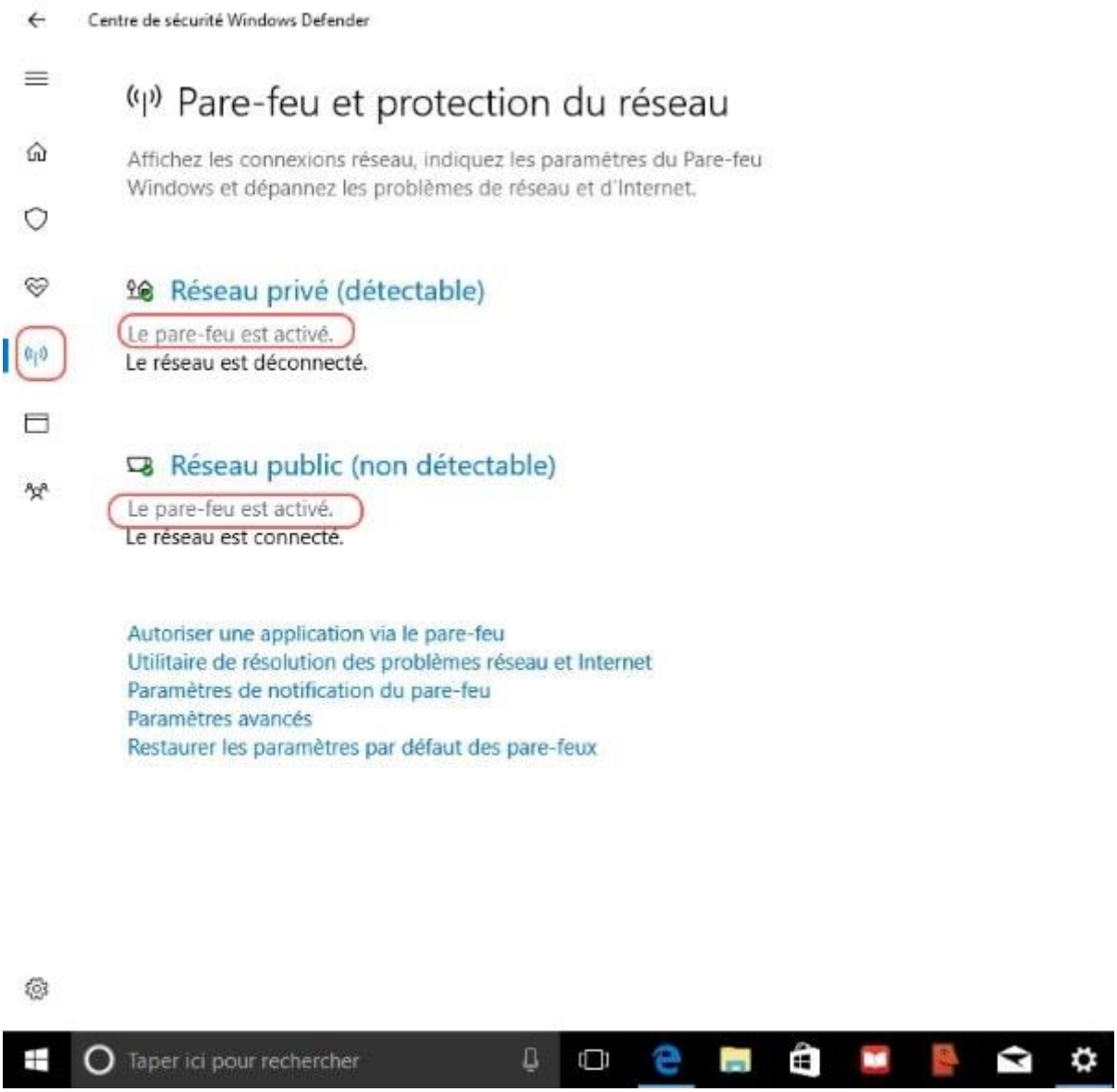
3. Dans la nouvelle fenêtre, vérifiez que tous les curseurs soient **Activés.**



4. Votre **antivirus Windows Defende**r est activé, votre ordinateur est **protégé**.

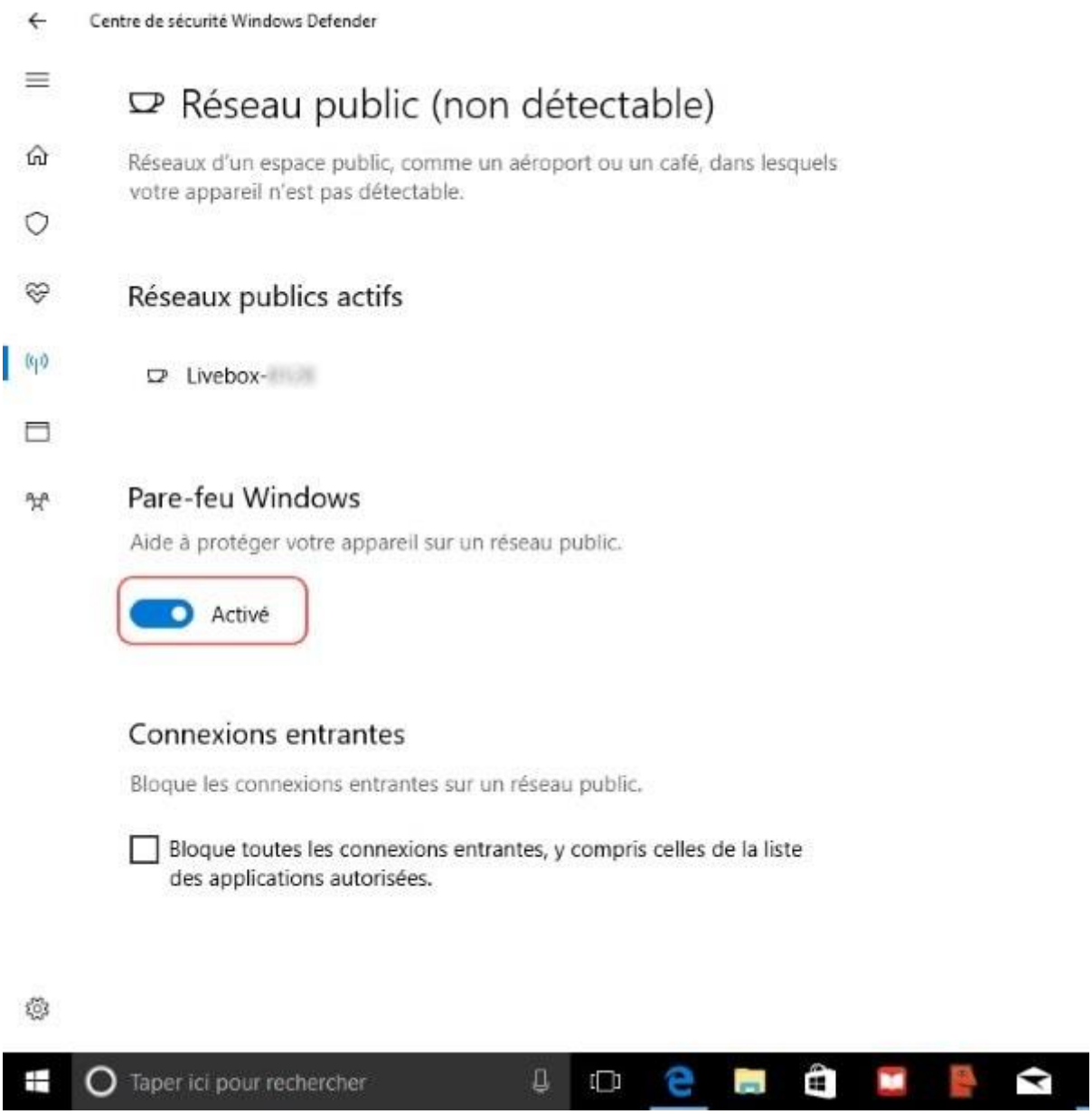
Activez le pare-feu Windows

Pour vérifier et/ou activer le **pare-feu Windows** cliquez sur la petite antenne à gauche de la fenêtre **Centre de sécurité Windows Defender**.



Dans cette dernière fenêtre vérifiez que la mention **Le pare-feu est activé** en dessous des deux menus principaux **Réseau privé** et **Réseau public**.

Dans le cas inverse, cliquez sur le menu sur lequel le **pare-feu** n'est pas activé, puis activez en cliquant sur le curseur adéquat.



Le **pare-feu Windows** est désormais en état de marche et vous protège.

Les autres solutions antivirus

Pour les personnes qui souhaitent installer une autre solution de sécurité sur leur ordinateur, voici mes recommandations.

Pour une solution gratuite efficace :

- **Comodo Internet Security**
- **Avast Free AntiVirus**
- **AVG Internet Security**

Les solutions payantes les plus efficaces sont :

- **Avira Antivirus Pro**
    - **Bitdefender Internet Security**
    - **Norton Security**

Pour votre sécurité et l »intégrité de votre système, télécharger impérativement ces logiciels sur les sites respectifs des éditeurs.