ccèsTI
AÎNÉS
2.0

SADC
Société
d'aide au développement
des collectivités
SHAWINIGAN

Thème 9 - Intermédiaire
J'utilise sécuritairement et efficacement mon périphérique

Localiser mon périphérique

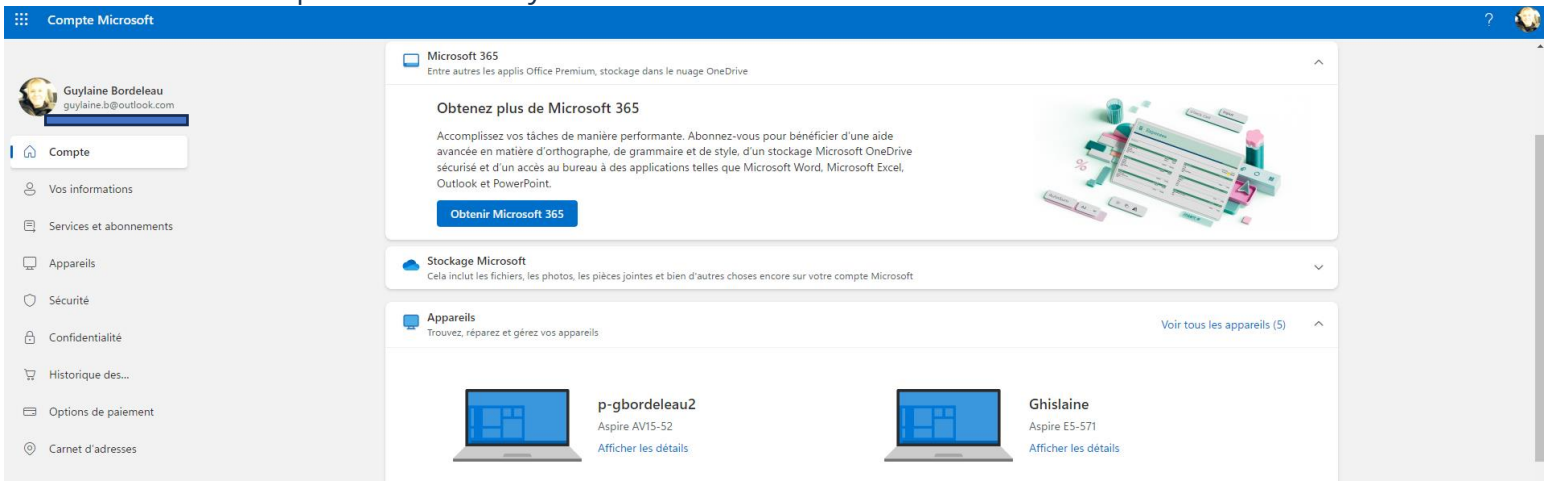
Si vous perdez votre ordinateur, ou s'il a été volé, vous pouvez localiser votre appareil et même supprimer les données de l'appareil tant que celui-ci est connecté à votre compte Windows et à Internet. Si votre appareil n'est pas connecté à Internet, vous pouvez tout de même localiser la dernière position connue, c'est-à-dire, la dernière fois qu'elle fût connectée à Internet.

Pour que la localisation fonctionne, vous devez vous assurer que l'option est activée. Il est donc important que cette option soit activée à l'avance. Lors de la perte d'un appareil, il sera trop tard si vous ne l'avez pas déjà activée :

1. **Paramètres → Confidentialité et sécurité → Localiser mon appareil**
2. Assurez-vous que l'option **Localiser mon périphérique** soit activé

Lorsque vous souhaitez trouver votre appareil, rendez-vous sur le site Internet : https://account.microsoft.com

1. Connectez-vous à votre compte Microsoft en y entrant vos informations de connexion



Il est **important de connaître le mot de passe** de votre compte Microsoft. Sans celui-ci, vous ne pourrez pas vous connecter sur votre appareil lorsque vous le retrouverez.

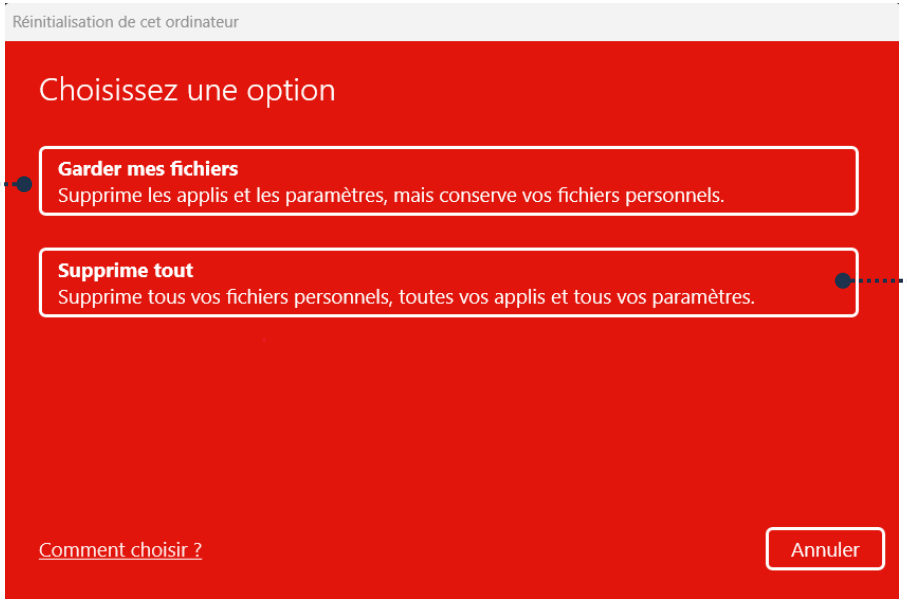
Réinitialiser mon appareil

Vous pouvez réinitialiser votre appareil afin d'en effacer complètement le contenu. Attention, cette action est irréversible. Conséquemment, il est important de bien sauvegarder ce que vous désirez conserver, soit par le nuage, ou un disque dur externe.

1. **Paramètre s→ Système → Récupération → Réinitialiser cet ordinateur personnel**

Supprime les applications et les paramètres et réinstalle Windows, mais conservera vos fichiers personnels

Attention : Conserveront vos fichiers personnels à condition qu'ils soient enregistrés convenablement dans vos documents



Supprime absolument tout et réinstalle Windows

Perte de données

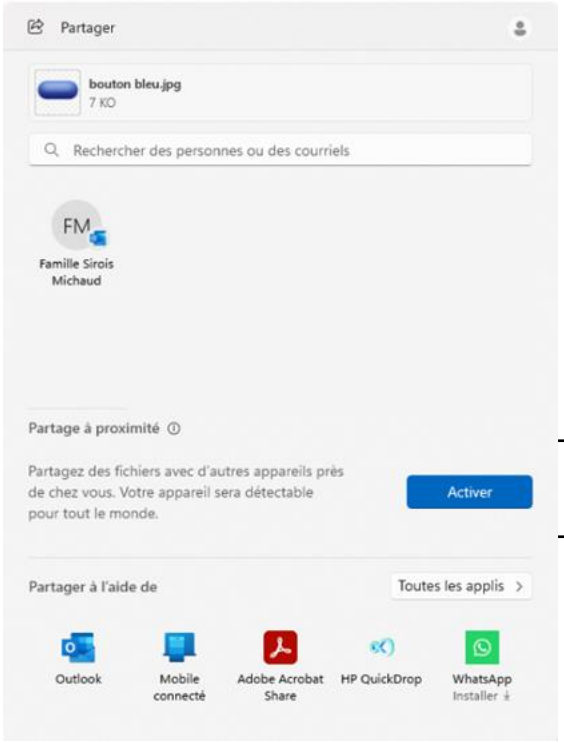
Lorsque vous réinitialisez et que vous supprimez tout, vous perdrez vos données. Il est donc important de comprendre le principe de sauvegarde et l'utilité des services nuagiques afin de pouvoir récupérer vos données efficacement.

Si vous avez des questions ou des doutes vis-à-vis la sauvegarde, vous pouvez vous référer au **thème 15 intermédiaire, Environnement Windows**

Partage à proximité

Il est possible de partager vos données vers un autre appareil Windows par principe de proximité. Cependant, l'autre appareil doit être à proximité du vôtre.

1. Assurez-vous que le **Bluetooth est activé** et que les deux appareils soient connectés sur le même réseau Wi-fi
2. Ouvrez le document ou la photo que vous souhaitez partager
3. Faites un clic **droit** et cliquez sur **Partager**



Les appareils à proximité détectés selon vos paramètres (**voir section suivante des fiches**) s'afficheront

4. Choisissez l'appareil correspondant au nom de l'appareil du destinataire à qui vous souhaitez partager pour envoyer

Le partage à proximité peut être une faille de sécurité. Il est important de savoir se protéger (voir section suivante : Les paramètres du Partage à proximité) afin d'utiliser cette fonction en toute sécurité.

Les paramètres du Partage à proximité

Pour que le partage à proximité fonctionne, il y a des paramètres à choisir.

1. **Paramètres → Système → Partage à proximité**

Si vous choisissez :

Désactivé : Il ne sera pas possible d'envoyer ou de recevoir par le Partage à proximité

Mes périphériques seulement : Vous pourrez envoyer ou recevoir seulement qu'à partir d'appareils connectés à votre compte Microsoft

Tout le monde en proximité : Tous les utilisateurs à proximité peuvent vous envoyer ou recevoir des documents

Pour plus de sécurité, activez le **Partage à proximité** seulement lorsque **vous en avez besoin**. Vous pouvez l'activer et le désactiver dans les paramètres. De cette façon, vous contournerez les failles de sécurité et vous serez certains de **ne pas recevoir de documents non voulus**.

Applications et logiciels malveillants

Il arrive que des applications ou des logiciels malveillants, fait par des gens mal intentionnés, se glissent sur des plateformes telles que Microsoft Store. Afin d'éviter d'avoir des soucis, vous pouvez diminuer les risques de tomber sur de telles applications en étant vigilant et en

utilisant les outils disponibles à même votre ordinateur. Tout d'abord, il est préférable de ne pas installer d'application sur votre ordinateur à partir de votre navigateur Internet. Seule exception, si vous êtes certain à 100 % que c'est sur un site officiel et connu. Ex. : Microsoft.

Voici quelques règles qui peuvent vous simplifier la vie :

- Ne téléchargez que **des applications prouvées par des compagnies fiables et connues**. Sinon, une petite recherche Google ou Bing sur l'application vous indiquera rapidement s'il y a un problème avec celle-ci;
- **Désinstallez les applications qui vous semblent suspectes** ou non voulues;
- **Vérifier, sur Internet**, s'il y a des applications connues pour des problèmes de sécurité. Des listes et articles existent et sont constamment mis à jour.

Windows Defender et Microsoft

Microsoft et son service inclus et gratuit sous Windows, Windows Defender, vous offrent un moyen de vous protéger. De plus, Microsoft se tient à jour, en incluant le Microsoft Store. Si une application malveillante est découverte par Microsoft, elle sera retirée du Store. C'est un bel outil qui vous aidera afin de rester sécuritaire. La chose importante, tenez Windows à jour grâce aux mises à jour logicielles.

Attention à votre environnement

Lorsque vous utilisez votre appareil en public, particulièrement lorsque vous y entrez des informations sensibles, il est important de rester au fait de son environnement. Entre autres, le reflet de l'écran lumineux apparaît très bien sur une fenêtre si vous êtes dos à celle-ci. Encore, assurez-vous que personne n'est derrière vous si vous accédez votre compte bancaire par exemple. Le but n'est pas d'avoir peur, mais seulement d'être vigilant.

L'utilisation d'une carte de crédit

Afin de profiter des services payants de Microsoft, ainsi que certains aspects d'Internet, dont le magasinage sur le Microsoft Store ou les magasins en ligne, vous devez payer avec une carte

Lorsque vous effectuez des achats sur Internet, il est important d'être prudent, certes, mais cette prudence doit découler de votre vigilance, et non de votre peur. Le plus gros risque de fraude est surtout lié au fait que les gens tombent dans une pièce qui provoque une diffusion des données de la carte ou de vos informations personnelles.
Nous vous **recommandons vivement d'effectuer des recherches** sur la prévention des fraudes et sur les tactiques des fraudeurs afin d'être au fait et de pouvoir être vigilant, en ayant les connaissances requises, **avant de vous lancer dans l'utilisation de votre carte de crédit sur Internet.**

Entre-temps, vous pouvez utiliser des cartes prépayées et des cartes cadeaux. Celles-ci ne seront pas liées à votre compte bancaire personnel et vous permettront d'effectuer des achats.

Également, nous vous recommandons de consulter nos fiches :

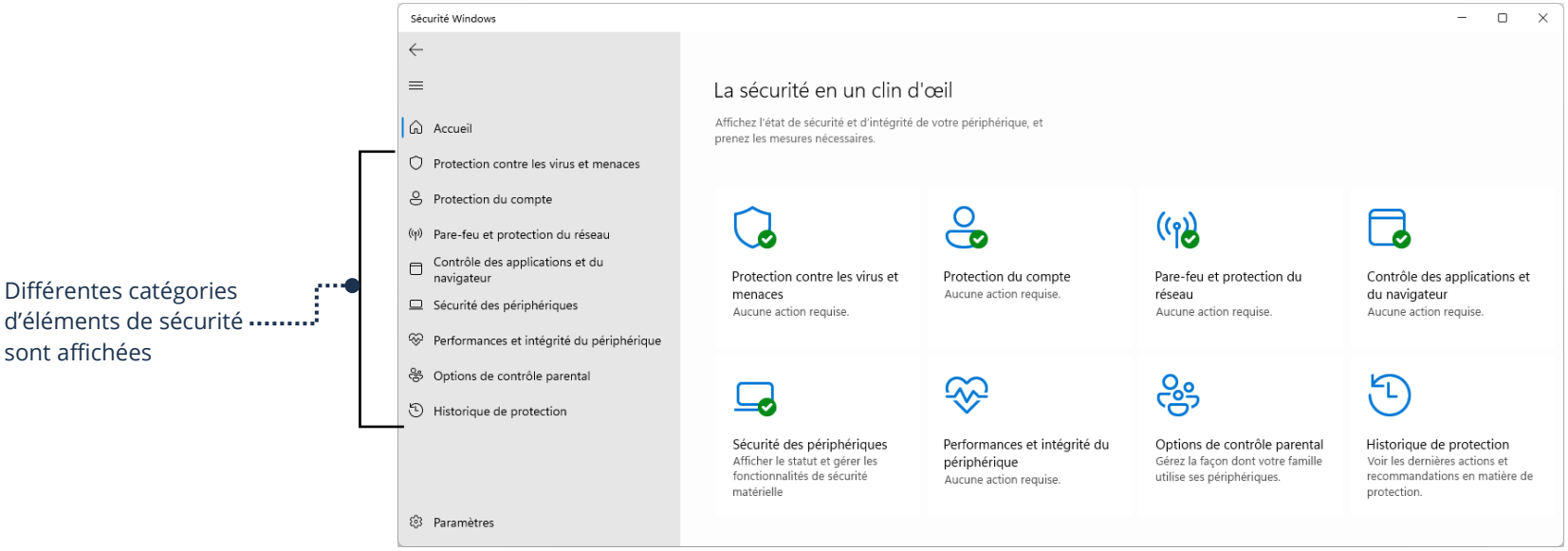
1. **Thème 9 de base et intermédiaire**
2. **Thème 10 de base et intermédiaire**
3. **Thème 15 de base et intermédiaire**

Ces fiches vous donneront une multitude de conseils et de connaissances afin de vous aider à bien vous outiller, notamment, sur la protection de vos comptes liés à votre carte.

Sécurité Windows

Votre système d'exploitation Windows inclut quelques options pour la sécurité, à même vos paramètres. Afin d'y accéder :

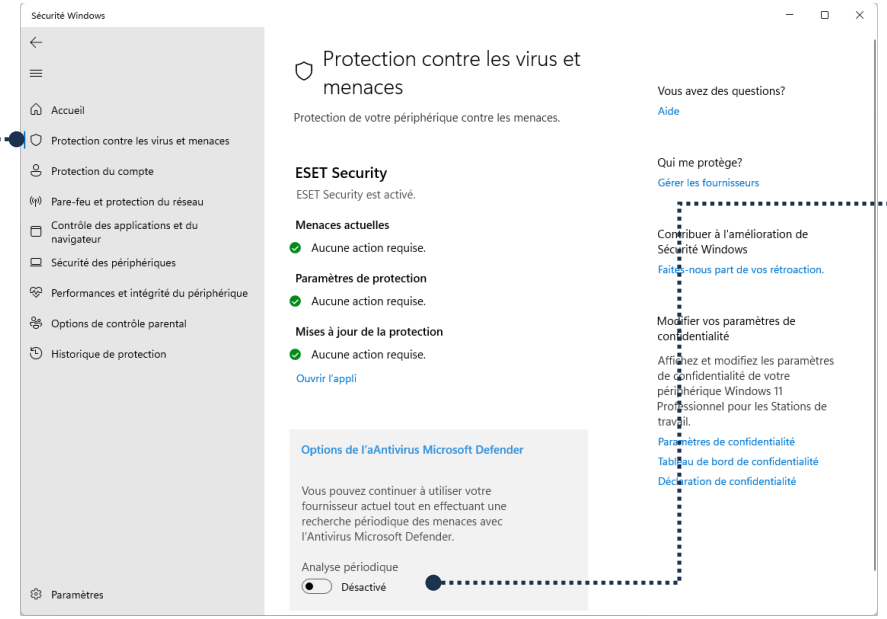
1. **Paramètres → Confidentialité et sécurité → Sécurité Windows**
2. Cliquez sur **Ouvrir Sécurité Windows**



Protection contre les virus et menaces

Toujours dans la fenêtre Sécurité Windows, cliquez sur **Protection contre les virus et menaces**

Cliquez sur l'onglet **Protection contre les virus et menaces** afin de visualiser vos protections installées sur votre périphérique



Il est **recommandé** d'activer l'Analyse périodique si vous n'avez pas d'antivirus installé.

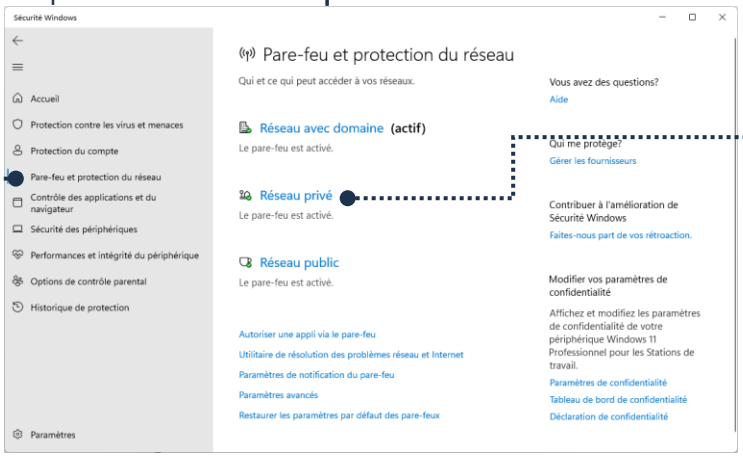
Si vous en avez un, vous pourriez avoir à le laisser désactiver, **selon votre antivirus**, afin de ne pas causer de conflit entre l'antivirus et Windows Defender. **Une recherche Google sur votre antivirus** à ce sujet vous donnera la réponse très rapidement.

Vous pourrez y voir **si vous avez** un antivirus installé. Dans l'exemple de la fenêtre ci-haut, nous avons ESET Security. Juste en dessous, vous avez **l'option d'activer Microsoft Defender** pour afin qu'il effectue **des analyses périodiques de votre appareil** afin de le protéger.

Pare-feu et protection du réseau

Toujours dans la fenêtre Sécurité Windows, cliquez sur **Pare-feu et protection du réseau**.

Cliquez sur l'onglet **Pare-feu et protection du réseau** afin de vérifier si vos Pare-feu sont actifs.



Si vous constatez qu'un des Pare-feu **n'est pas actif**, cliquez sur le lien correspondant au Pare-feu qui n'est pas actif. Vous serez devant une nouvelle fenêtre vous donnant la **possibilité de l'activer**

Les Pare-feu agissent comme un bouclier à même votre périphérique. Ils contribueront à bloquer certaines menaces à l'intégrité de votre appareil et de vos données.

Il peut arriver qu'un Pare-feu bloque une application que vous souhaitez utiliser. Si tel est le cas, vous n'avez qu'à cliquer sur **Autoriser une appli sur le Pare-feu** et **choisir l'application** qui cause un problème. **ATTENTION :** assurez-vous qu'il s'agit bel et bien **d'une application officielle et non d'un virus** ou de quelque chose du genre.

Confidentialité

Il est possible de changer certaines permissions quant à votre confidentialité lors de votre utilisation de votre périphérique.

1. **Paramètres → Confidentialité et sécurité → Général**

Autoriser les applications à me montrer des publicités personnalisées en utilisant mon identifiant publicitaire	En **désactivant cette option**, les publicités seront **un peu moins ciblées** en lien avec vos recherches précédentes
Permettre aux sites Web de me montrer du contenu local pertinent en accédant à ma liste de langue	En **activant cette option**, les sites Internet qui apparaîtront lors de vos recherches **seront orientés vers la langue choisie** dans votre système d'exploitation en priorité
Laissez Windows améliorer les résultats de démarrage et de recherche en suivant les lancements d'applications	En **activant cette option**, le Menu démarrer comptera les applications lancées et **affichera les applications lancées régulièrement** en priorité
Montrez-moi le contenu suggéré dans l'appli Paramètres	En **activant cette option**, du **contenu sera suggéré** dans l'appli Paramètres

Windows Update

En plus des mises à jour de base, il est recommandé de procéder à la mise à jour des pilotes de votre appareil. Les pilotes sont des programmes souvent liés aux pièces de votre ordinateur. Ces mises à jour règlent souvent des problèmes, tels que des bogues trouvés par les fournisseurs de pièces, ou encore, par Windows directement.

1. **Paramètres → Windows Update → Options avancées → Mises à jour facultatives**

2. Cliquez sur **Mises à jour des pilotes**
3. Cliquez **dans le case du pilote** que vous souhaitez installer
4. Cliquez sur **Télécharger et installer** afin de lancer l'installation