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

Thème 9 Android, Apple et Windows le style du titre n'est pas ok

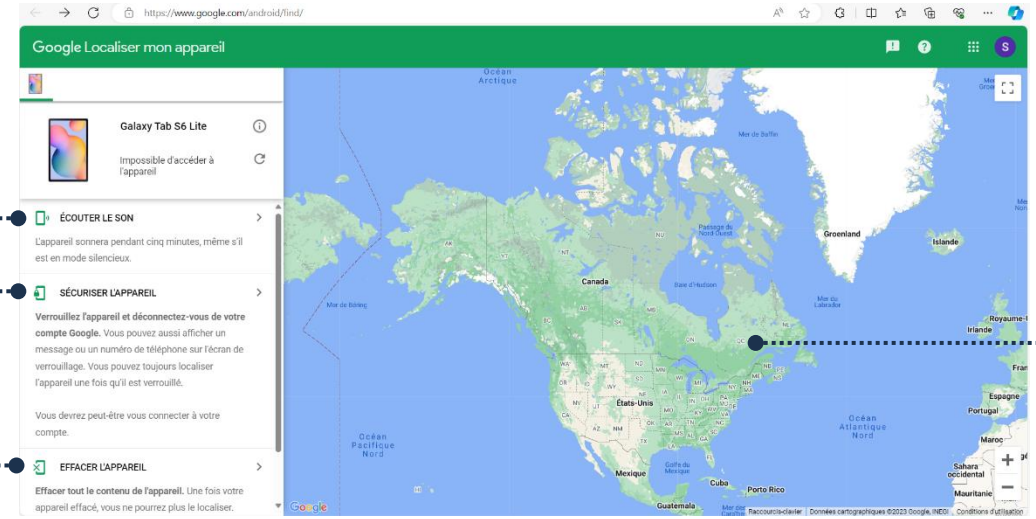
Si vous perdez votre appareil, ou qu'il a été volé, vous **pouvez localiser votre appareil et même supprimer les données de l'appareil** tant que celui-ci **est connecté à votre compte Google et à Internet**. C'est donc très utile dans le cas d'un téléphone avec des données cellulaires, parce qu'il sera techniquement toujours connecté à Internet. Si votre tablette, quant à elle, ne possède pas de données cellulaires, 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 → Google → Localiser mon appareil**
2. Assurez-vous que l'option **Utiliser Localiser mon appareil** soit activée

Lorsque vous souhaitez **trouver votre appareil**, rendez-vous sur le **site Internet** : https://www.google.ca/Android/Find

1. Connectez-vous à votre compte Google en y entrant vos informations de connexion
2. Vous vous retrouverez devant cette fenêtre :



Provoque une alarme sonore afin de localiser l'appareil s'il est à proximité

Déconnecte votre compte Google de l'appareil et vous permet de le verrouiller

Efface tout le contenu de votre appareil

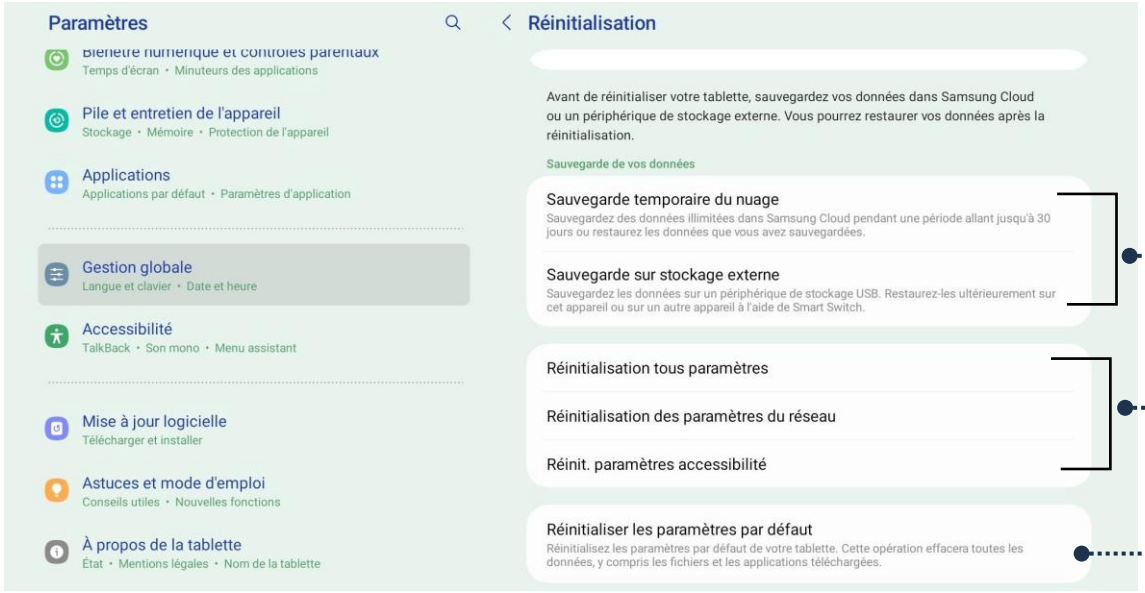
Votre appareil **apparaîtra sur la carte**, vous donnant ainsi sa localisation en temps réel

Il est **important de connaître le mot de passe** de votre compte Google. 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. Pour réinitialiser :

1. **Paramètres → Gestion Globale → Réinitialiser**



Permet d'effectuer une sauvegarde. Attention, ce ne sera pas sur votre Google, mais le nuage Samsung si vous choisissez cette option. Sinon, vous pouvez sauvegarder sur un disque dur externe

Permet de réinitialiser certains paramètres

Permet de réinitialiser l'appareil en entier

Perte de données

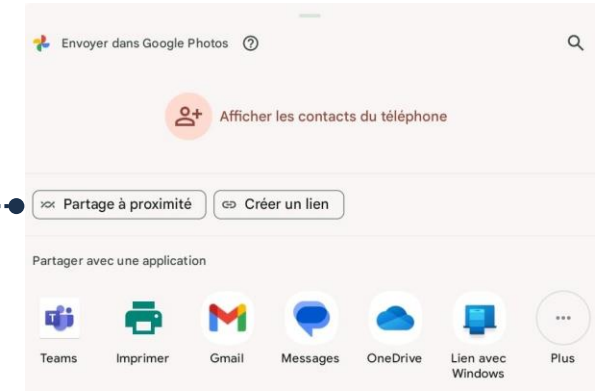
Lorsque vous réinitialisez, **vous perdrez vos données**. Il est donc important de comprendre le principe de la sauvegarde et de l'utilité des services nuagiques afin de pouvoir récupérer vos données efficacement.

Si vous avez des questions ou des doutes vis-à-vis la sauvegarde, vous pouvez vous référer au **thème 14 intermédiaire, Environnement Android et Google**

Partage à proximité

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

1. Assurez-vous que le **Bluetooth est activé**
2. Assurez-vous que la **localisation est activée**
3. Ouvrez le document ou la photo que vous souhaitez partager
4. Touchez l'icône **Partager** 



Partage à proximité vous permettra de procédez au partage

5. Touchez **Partage à proximité**

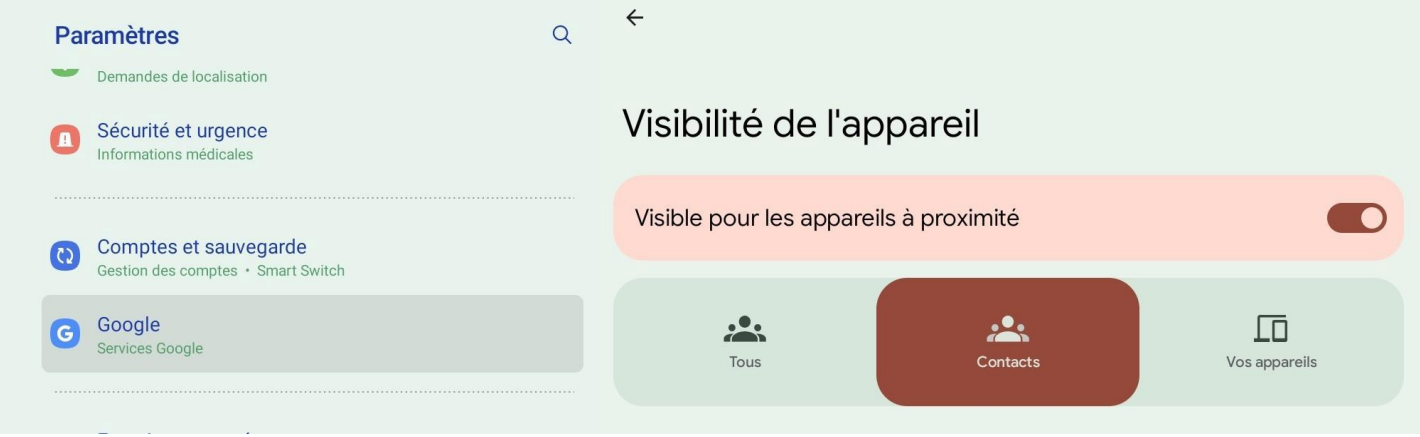
Les appareils à proximité détectés selon vos paramètres (voir section suivante des fiches) s'afficheront

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

Les paramètres du Partage à proximité

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

1. **Paramètres → Google → Appareils et partage → Partage à proximité → Visibilité de l'appareil**



Si vous choisissez :

Tous : Tout le monde peut vous acheminer ce qu'ils veulent. Cette option n'est pas recommandée.

Contacts : Seulement les gens inscrits dans votre liste de contacts peuvent vous acheminer des documents par le partage à proximité.

Vos appareils : Il n'y a que les appareils connectés à votre compte Google qui peuvent vous envoyer des documents.

Nous vous recommandons de choisir **Contacts.** Si vous souhaitez utiliser le **Partage à proximité**, vous n'avez qu'à ajouter la personne dans vos contacts. C'est plus sécuritaire.

Pour plus de sécurité, activez le **Partage à proximité** seulement lorsque **vous en avez besoin**. Vous pouvez l'activer et le désactiver par le menu rapide en glissant vers le bas à partir du coin supérieur gauche de votre appareil. De cette façon, vous contournerez les failles de sécurité et vous serez certains de **ne pas recevoir de documents non voulus**.

Applications malveillantes

Il arrive que des **applications malveillantes**, fait par des gens mal intentionnés, **se glissent sur des plateformes telles que Play 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 l'appareil. Tout d'abord, il est préférable **de ne pas installer d'application sur votre appareil 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.

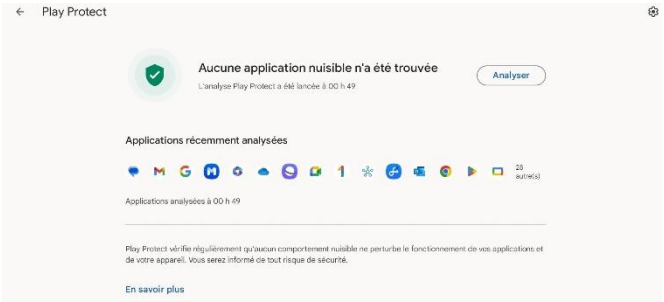
Voici quelques règles qui peuvent vous simplifier la vie.

1. Ne téléchargez que **des applications prouvées par des compagnies fiables et connues**. Sinon, une petite recherche Google sur l'application vous indiquera rapidement s'il y a un problème avec celle-ci
2. **Désinstallez les applications qui vous semblent suspectes** ou non voulues.
3. **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

Play Protect

Le Play Store vous offre, gratuitement, **un moyen de vous protéger**. Google se tient à jour, conséquemment, s'il est découvert qu'une application est malveillante, **Play Protect** la découvrira et vous pourrez la supprimer. Ce n'est pas fiable à 100% dans le sens où il est possible qu'une application malveillante ne soit pas encore ajoutée à la liste de Google, mais c'est un bel outil si une application que vous possédez fait partie des applications malveillantes selon la liste officielle de Google :

1. Ouvrez **Play Store**
2. Touche**z l'icône** en haut à droite représentant **votre compte**
3. Touchez **Play Protect**



4. Touchez **Analyser**. Si une application malveillante est trouvée, vous pourrez la supprimer

Attention à votre environnement

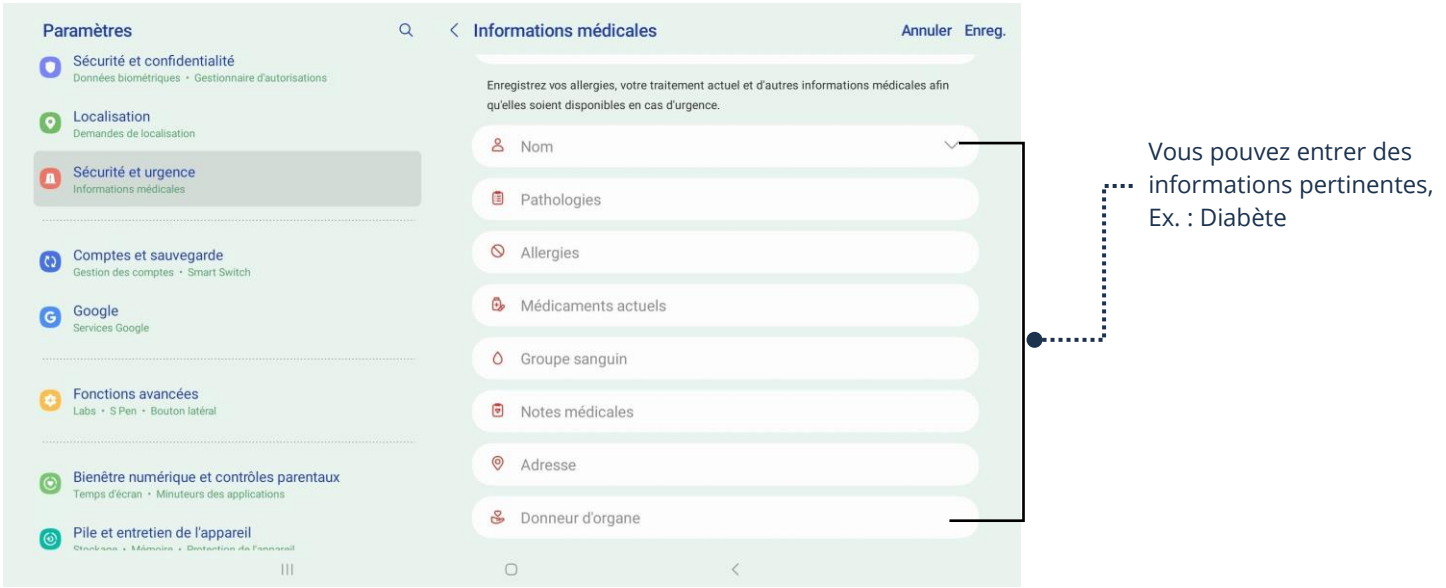
Lorsque vous utilisez votre appareil **en public**, particulièrement lorsque vous **y entrez des informations sensibles**, il est important de rester au **fait de son environnement**. Entre autres, le reflet de votre appareil lumineux apparaît très bien sur une fenêtre si vous êtes dos à celle-ci. Encore, 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**.

Les services d'urgences

Votre appareil Android, particulièrement les téléphones intelligents, peut **vous aider à communiquer avec les services d'urgences,** et ce, de façon subtile si besoin est.

Sur un téléphone cellulaire, vous pouvez **appuyer à répétition sur le bouton marche/arrêt** afin de communiquer avec les services d'urgences**.** Il est également possible de configurer votre appareil afin d'y afficher **des informations pertinentes quant à votre état de santé**, particulièrement si vous avez une condition déjà diagnostiquée afin de donner un maximum d'informations rapidement si, par exemple, vous étiez retrouvé inconscient.

1. **Paramètres → Sécurité et urgence → Information médicale**



2. Après avoir entré vos informations, n'oubliez pas de toucher **Enreg**. afin d'enregistrer ce que vous avez inscrit

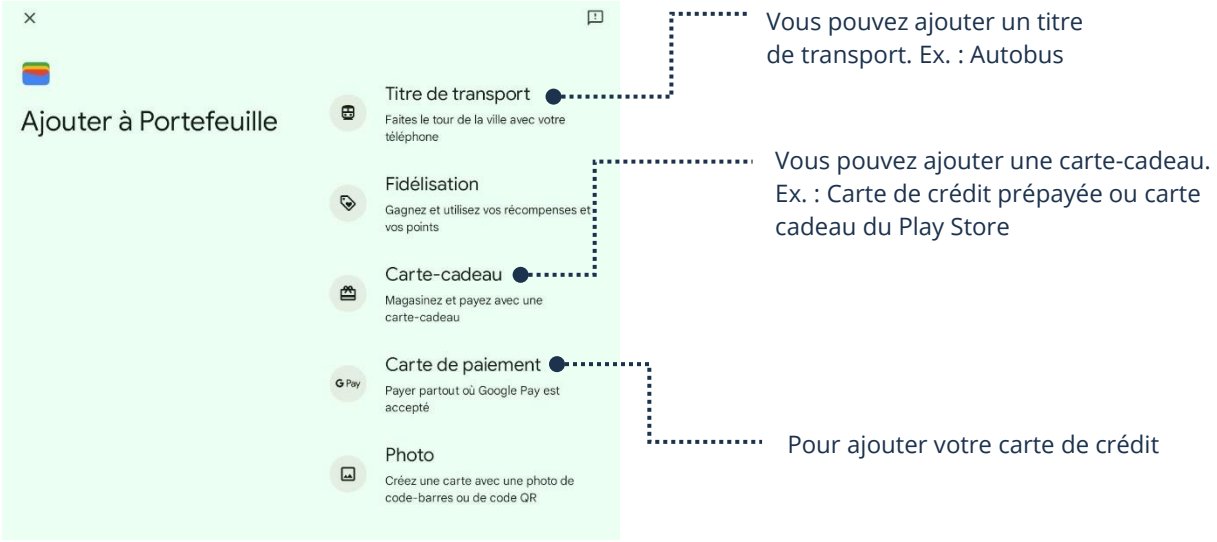
L'utilisation d'une carte de crédit

Afin de profiter des services payants de Google, ainsi que certains aspects d'Internet, dont le magasinage sur le Play Store et les applications des magasins, vous pouvez enregistrer votre carte de crédit sur votre compte Google et/ou entrer les informations de votre carte lors de l'achat.

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 un piège qui provoque une diffusion des données de la carte. Le deuxième risque est l'usurpation de votre compte auquel la carte est liée, c'est pourquoi ils doivent être bien protégés. Tant que vous pratiquez certaines règles de sécurité sur Internet, que vos comptes sont bien protégés et que vous êtes vigilants face aux fraudes et aux pièges, magasiner sur Internet devient beaucoup plus sécuritaire tant et aussi longtemps que vous **faites affaire avec des entreprises connues**, par les voies officielles des entreprises, diminuant significativement les risques.

Google Portefeuille (Wallet)

1. Téléchargez l'application **Google Portefeuille**
2. **Connectez-vous** à votre compte Google dans l'application
3. Touchez **+ Ajouter à Portefeuille**



4. **Sélectionnez l'option désirée** et **suivez les étapes**. Si vous ajoutez votre carte de crédit, il est possible que vous soyez également dirigé vers votre application bancaire afin d'accepter les conditions afin de pouvoir ajouter votre carte.

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 :

- **Thème 9** de base et intermédiaire
- **Thème 10** de base et intermédiaire
- **Thème 14** 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.

Google Pay

Une fois votre carte enregistrée, il est possible d'acheter et de payer rapidement grâce à Google Pay à même votre appareil. De plus, il s'agit d'une façon de payer très sécuritaire, à condition que votre compte Google et votre appareil soient bien protégés. En effet, lors des transactions, Google va crypter les données bancaires, ce qui fait en sorte que les commerçants ou les machines TPV n'auront pas vos informations. Nous vous recommandons de faire vos recherches et de demander conseil à votre institution bancaire si vous souhaitez utiliser cette fonction.

Sécurité physique de votre appareil

La sécurité physique de votre appareil n'est pas chose à négliger afin de protéger votre investissement. Nous vous recommandons de vérifier votre magasin de choix afin de vérifier les étuis offerts, et compatibles avec votre appareil. Certains possèdent même un portefeuille intégré afin d'alléger ce que vous devez transporter. Lors de l'achat, vérifiez également si le produit possède la technologie RFID. Cette technologie protège vos cartes, et votre appareil, des tentatives de lecture et de clonage à même le portefeuille.

D'autres ont même des vitres de protection ultra résistante, tout dépend de vos besoins. Dans tous les cas, un étui de protection adéquat prolongera la durée de vie de votre appareil vis-à-vis les accidents.