ccèsTI
AÎNÉS
2.0

SADC
Société
d'aide au développement
des collectivités
SHAWINIGAN

Thème 1
Identité numérique

Identité

L'identité est singulière et est propre à chaque individu. L'identité d'une personne est composée de plusieurs éléments :

- une **identité légale**, qui permet d'identifier et de reconnaitre la personne aux yeux de tous
- une **identité personnelle**, qui se construit au jour le jour par les choix qu'un individu peut faire

L'identité légale

Chaque individu est défini par :

- son nom
- son prénom
- sa nationalité
- son sexe
- son lieu
- sa date de naissance

Ces éléments sont **uniques** et **particuliers** à chaque individu. Ceci fait partie de l'**usurpation d'identité,** un grave délit sévèrement puni par la loi. Ces informations se retrouvent sur des papiers officiels : registre d'état civil, carte d'identité, passeport, etc.

L'identité personnelle

Alors que l'identité légale est encadrée par des normes et enregistrée sur des papiers officiels, l'identité personnelle est multiple et variée. Cependant, comme l'identité légale, elle reste unique et particulière à chaque individu.

Elle est composée des différents éléments qui forment l'**environnement** d'un individu comme :

- sa famille
- ses amis
- son milieu
- son école
- ses loisirs
- sa culture
- ses croyances religieuses
- son milieu professionnel
- ses goûts
- etc.

Ensemble, tous ces aspects forment l'identité personnelle, mais il faut rappeler qu'aucun d'eux ne suffit à définir un individu. Résumer une personne à son sexe, son âge ou ses convictions revient à faire preuve de **discrimination**.

Identité numérique

Aujourd'hui, ce nouveau type d'identité prend une place de plus en plus importante. Celle-ci contient des éléments propres à votre identité légale (nom, date et lieu de naissance, etc.) et à votre identité personnelle (goûts, opinions, croyances, etc.) et se construit en ligne.
Elle présente des risques, car elle peut être partagée et exposée sur Internet. Si l'on n'y prend pas garde, des éléments personnels voir confidentiels peuvent ainsi être récupérés puis diffusés à notre insu et à nos dépens.

L'identité numérique est constituée de toutes les traces que nous laissons ou que les autres laissent sur nous dans Internet ou dans un environnement numérique.

Présence numérique/empreinte

La présence numérique est constituée de toutes les activités qu'une personne peut faire en ligne et elle construit son identité numérique.
-

Quiconque utilise Internet laisse une empreinte. Exemple : les informations que l'individu saisit sur les réseaux sociaux ou ailleurs sur le Web. C'est son identité qu'il est en train de définir, et souvent, les gens n'en sont que trop peu conscients.

Les avantages et risques de l'identité numérique

L'identité numérique **peut être vérifiée à distance,** et ceci dans le but d'utiliser un service en ligne. C'est rapide et pratique. L'inconvénient majeur de l'identité numérique est de **perdre le contrôle de son compte** et de se faire usurper son identité. Pour cette raison, nous devons activer la double authentification qui, dans tous les cas, devient de plus en plus obligatoire sur diverses plateformes.

De plus, on ne peut pas négliger **l'erreur et l'oubli** venant de la personne elle-même. Exemple : oublier son mot de passe, etc. Un gestionnaire de mot de passe peut être une très bonne solution afin d'aider avec cet inconvénient.

Pourquoi la double authentification?

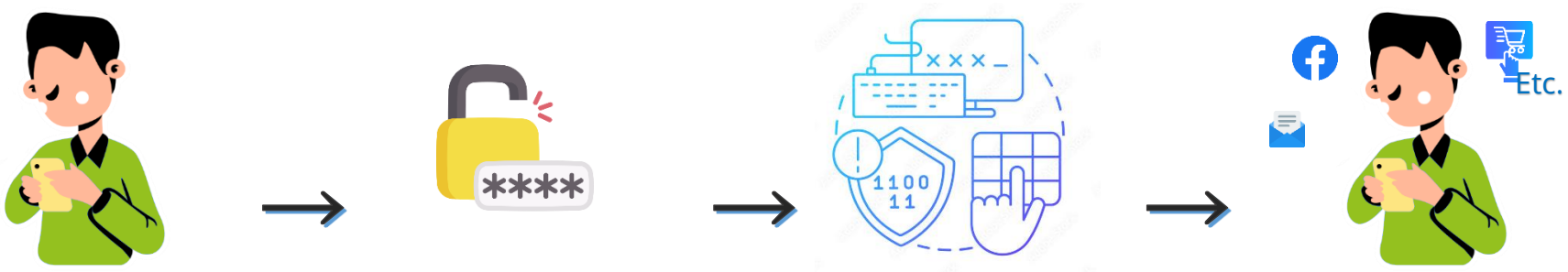
Il sera beaucoup plus difficile pour une personne mal intentionnée de voler ou pirater un compte si celui-ci doit s'authentifier deux fois. Il est donc fortement recommandé, par mesure de sécurité, d'activer ce facteur à deux temps (en deux étapes).

Comment fonctionne la double authentification?

Si le fournisseur de service que vous utilisez vous offre la double authentification, nous vous recommandons de l'activer. D'ailleurs, cette méthode de connexion est de plus en plus répandue et vous sera imposée ou suggérée presque partout.

Une authentification classique (simple) nécessite un nom d'utilisateur (ou une adresse de courriel) et un mot de passe afin de se connecter et utiliser un service. Ceux-ci sont choisis lors de la création du compte.

La double authentification (forte) demande de confirmer que c'est bien nous qui tentons de nous connecter au compte. La confirmation se fait via un code envoyé par message texte (texto) sur notre cellulaire ou par courriel. Certains fournisseurs de services ont même leur propre application d'authentification.



Comment s'authentifier

Par code

Courriel

C'est la méthode à utiliser **si vous ne possédez pas de cellulaire**.

1. Ouvrez la page de connexion du service à utiliser
2. Tapez votre nom utilisateur (adresse de courriel) et votre mot de passe
3. Votre code de confirmation vous sera envoyé à l'adresse de courriel qui est reliée au compte. Allez consulter vos nouveaux courriels, ouvrez le courriel contenant le code de confirmation et mémorisez ce code
4. Retournez à la page de connexion du service à utiliser et tapez ce code

Cellulaire

C'est la méthode **la plus utilisée**. Bien évidemment, il faut posséder un téléphone avec un service de messagerie texte.

1. Ouvrez la page de connexion du service à utiliser
2. Tapez votre nom utilisateur (adresse de courriel) et votre mot de passe
3. Votre code de confirmation vous sera envoyé par message texte au numéro de téléphone qui est relié au compte. Allez lire vos nouveaux messages texte, ouvrez le message et mémorisez ce code
4. Retournez à la page de connexion du service à utiliser et tapez ce code

Via une Application

Il y a des compagnies qui offrent de télécharger une application d'authentification. Exemple : Microsoft Authenticator. Cette façon de faire est **la plus rapide**, mais vous devez posséder une tablette ou un téléphone intelligent afin d'installer les applications.

1. Téléchargez et installez l'application
2. Ouvrez la page de connexion du service à utiliser
3. Tapez votre nom utilisateur (adresse de courriel) et votre mot de passe
4. Vous recevez une notification sur votre appareil (où est installée l'application) et vous n'avez qu'à confirmer que c'est bien vous qui tentez de vous connecter.

Gestionnaire de mots de passe

Un gestionnaire de mots de passe peut vous aider lors de la création d'un compte ainsi qu'à la connexion de celui-ci les fois suivantes.

Les sites Web, fournisseurs, etc. nous demandent toujours de créer un mot de passe de plus en plus fort. Exemple : 8 caractères minimum, au moins une minuscule, une majuscule, ainsi qu'un caractère spécial (!?/.#). **Il est vivement déconseillé d'utiliser le même mot de passe pour plus d'un compte**. Mais comment s'y retrouver avec tous ses mots de passe?

Le gestionnaire peut vous aider à choisir un mot de passe sécuritaire lors de la création d'un nouveau compte et l'enregistrer afin de vous connecter plus rapidement la fois suivante. D'ailleurs, il sert aussi à enregistrer ceux que vous utilisez déjà.

Avantage

- Possibilité de créer des mots de passe sécuritaires
- Accès rapide à vos mots de passe dans le coffre-fort
- Facilité à utiliser un mot de passe différent avec chacun de vos comptes en ligne

Inconvénient

Vous ne devez jamais oublier (perdre) le mot de passe Maître de l'application. Si vous perdez le mot de passe de votre application de gestion, vous perdez tous vos mots de passe.

Application

Si vous effectuez une recherche, vous verrez qu'il existe une panoplie d'applications afin de faire la gestion des mots de passe.
Voici une liste des plus populaires :

- 1Password
- EnPass
- LastPass
- Dashlane

-
- La plupart de ces applications sont payantes. Toutefois, LastPass permet gratuitement une utilisation limitée à une personne qui utilise l'application sur un seul appareil. Si vous possédez plus d'un appareil, cette version gratuite pourrait être contraignante pour vous.

Services gouvernementaux en ligne

Fédéral

Mon dossier ARC (Canada)

Mon dossier est un portail sécurisé qui vous permet de consulter vos renseignements personnels au sujet de l'impôt sur le revenu et des prestations et de gérer vos affaires fiscales en direct.

La double authentification est maintenant obligatoire. Elle se fera par **Code,** envoyé soit sur une ligne fixe ou sur un cellulaire.

Site officiel : https://www.canada.ca/fr/agence-revenu/services/services-electroniques/services-ouverture-session-arc.html

Mon dossier Services Canada (MDSC)

Mon dossier Service Canada (MDSC) est un portail en ligne sécurisé. Il vous permet de consulter ou mettre à jour vos renseignements de prestations d'assurance-emploi, du Régime de pensions du Canada (RPC), de prestations d'invalidité du Régime de pensions du Canada ou de la Sécurité de la vieillesse (SV).

La double authentification est maintenant obligatoire. Elle se fera par **Code**, envoyé soit sur une ligne fixe ou sur un cellulaire.

Site officiel : https://www.canada.ca/fr/emploi-developpement-social/services/mon-dossier.html

Provincial

ClicSéqur (Québec)

Mon dossier est un espace personnalisé conçu pour vous permettre de remplir vos obligations fiscales par Internet de manière **confidentielle** et **sécuritaire** et de gérer votre dossier relativement à certains programmes sociaux fiscaux.

La double authentification est obligatoire. Donc, à chaque connexion, vous devrez répondre à la question et inscrire un code de vérification à sept chiffres pour compléter votre authentification. Il vous sera transmis à l'adresse courriel ou numéro de téléphone associé à votre compte.

Site officiel : https://www.revenuquebec.ca/fr/citoyens/mon-dossier-pour-les-citoyens/

Carnet de santé en ligne (Québec)

Accédez à vos informations de **santé en ligne**. Vous devez vous connecter avec votre compte **ClicSéqur**.
Site officiel : https://carnetsante.gouv.qc.ca/portail

SAAQclic (Société de l'Assurance Automobile du Québec)

Services de la SAAQ en ligne.
La double authentification est obligatoire. Donc, à chaque connexion, un code vous sera envoyé par courriel.
Site officiel : https://saaqclic.saaq.gouv.qc.ca/

Services bancaires en ligne

Services pratiques afin de faire des transactions en ligne sécuritairement. Vous pouvez d'ailleurs les utiliser au moment qui vous convient. La procédure étant la même pour toutes les institutions.

1. Se créer un compte à l'aide de notre carte de débit. **Il faut choisir un mot de passe fort et sécuritaire**
2. On se connecte ensuite au compte à toutes les fois que nous avons besoin du service

Avant de vous connecter, assurez-vous d'être sur le site officiel de l'institution afin de ne pas divulguer vos informations de connexion à de potentiels fraudeurs.

Liens utiles

Ci-dessous quelques liens qui peuvent vous être utiles :

Institutions, sites officiels

BNC	https://www.bnc.ca
BMO	https://www.bmo.com
CIBC	https://www.cibc.com/fr/
Desjardins	https://www.desjardins.com

Sécurité

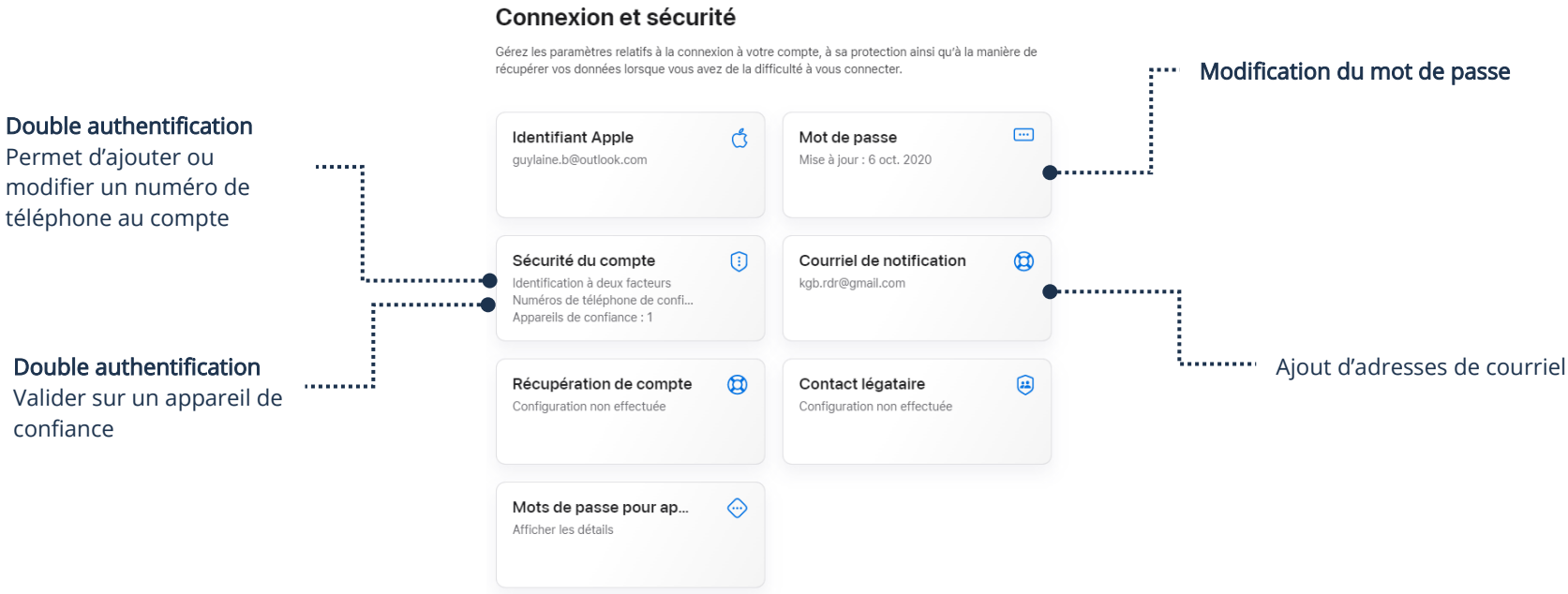
BNC	https://www.bnc.ca/particuliers/conseils/securite.html
BMO	https://www.bmo.com/principal/particuliers/vos-operations-bancaires/centre-de-securite/centre-de-formation
CIBC	https://www.cibc.com/content/cibcpublic/fr/privacy-security/banking-fraud/scam-quiz.html
Desjardins	https://www.desjardins.com/securite/index.jsp

Sécurité des comptes personnels en ligne

Apple

Gérer le compte Apple

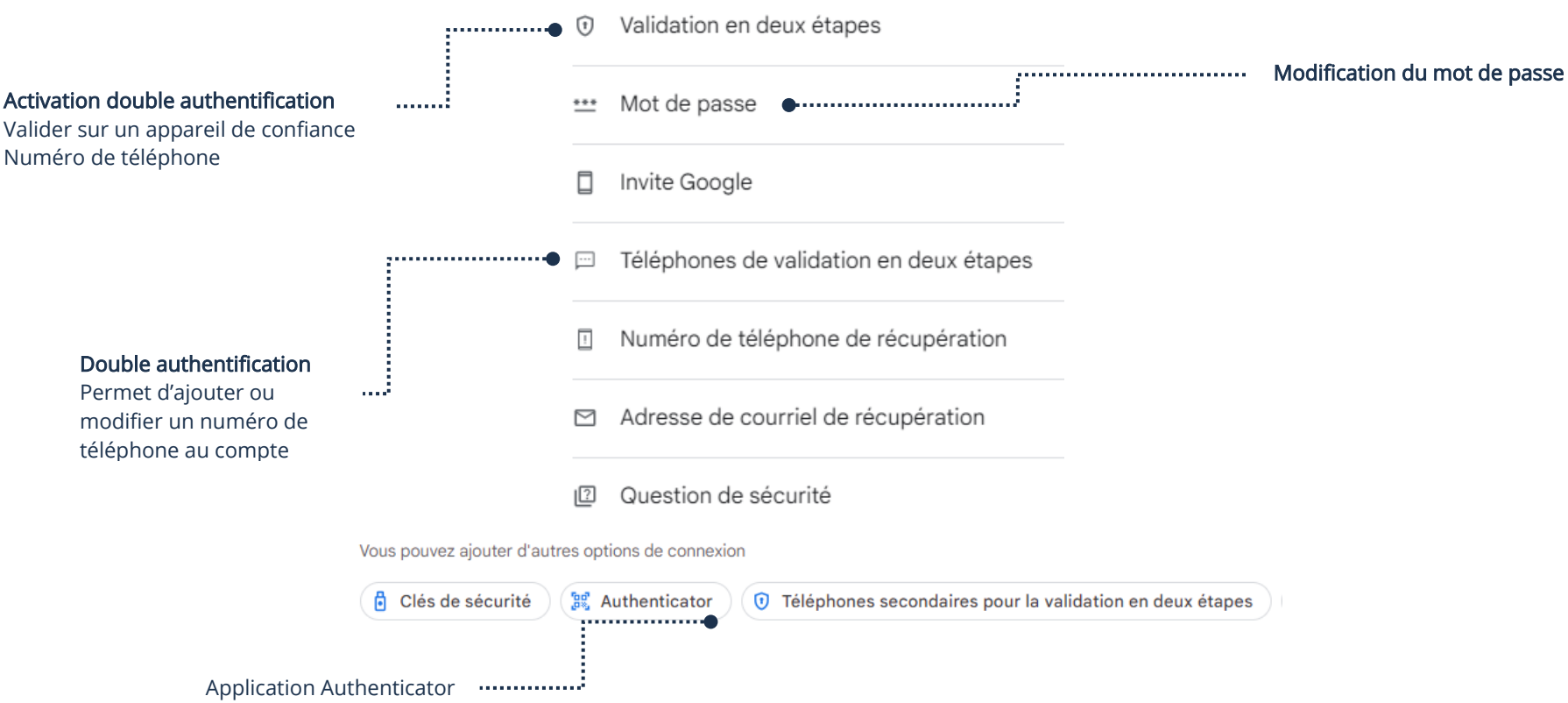
1. À partir du lien ci-dessous connectez-vous à votre compte :
https://appleid.apple.com/



Google

Gérer le compte Google

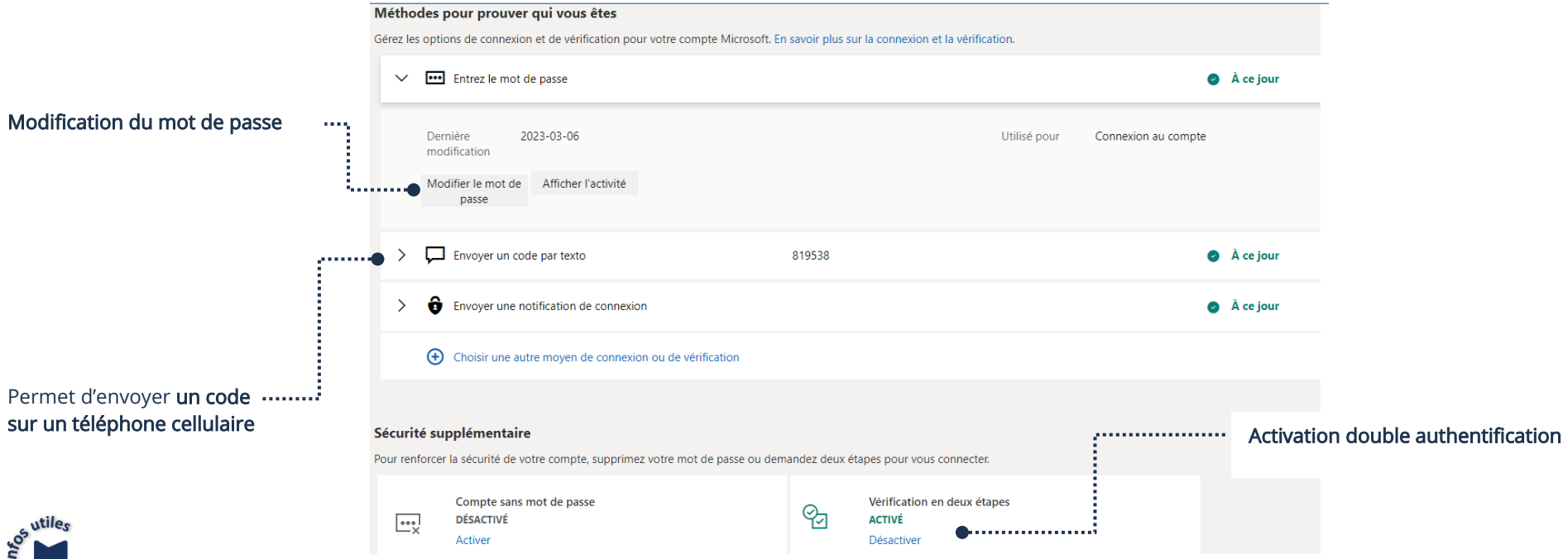
1. À partir du lien ci-dessous connectez-vous à votre compte :
https://myaccount.google.com/intro/security



Microsoft

Gérer le compte Microsoft

1. À partir du lien ci-dessous connectez-vous à votre compte :
https://login.live.com/
2. **Sécurité** → **Autres options de sécurité**



Infos utiles

Vous pouvez télécharger Microsoft Authenticator dans l'App Store ou le Play Store dépendamment de votre type d'appareil.

Facebook

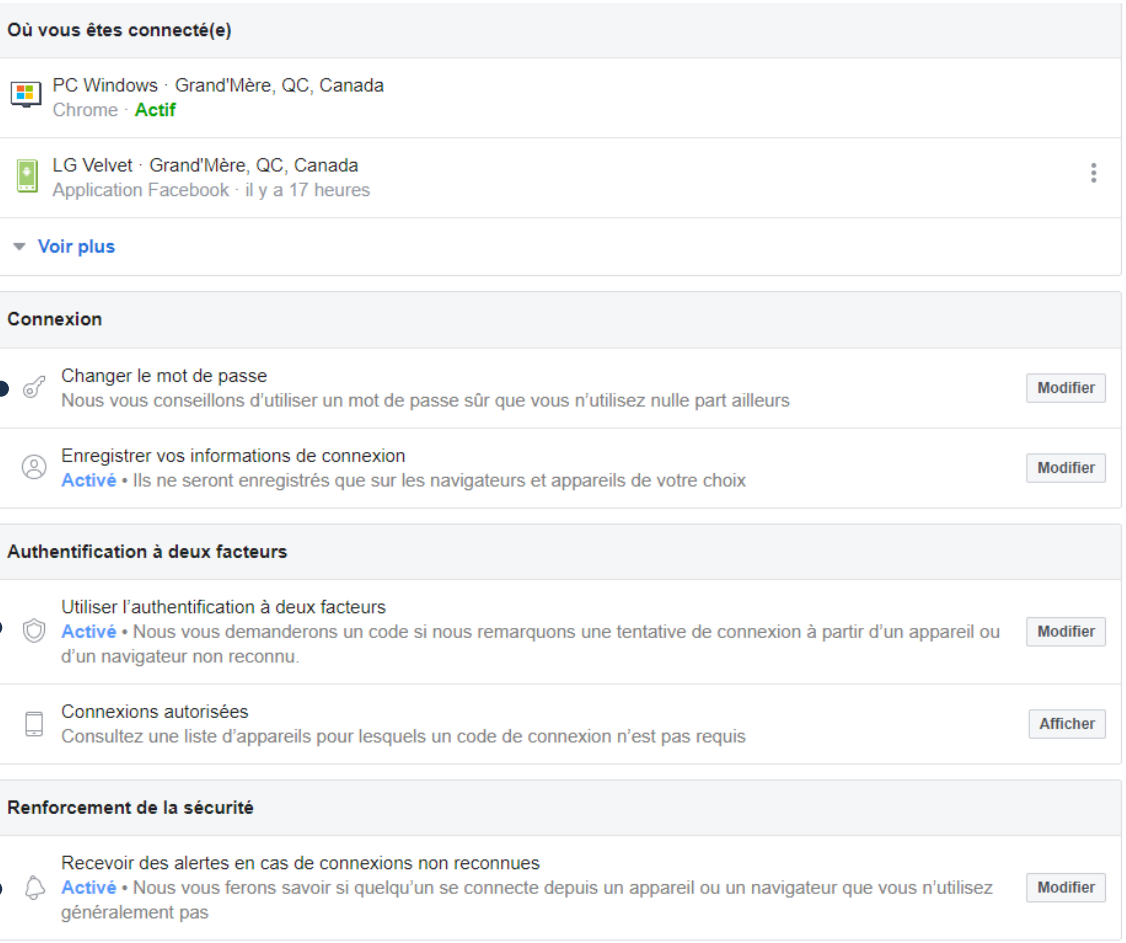
Gérer le compte Facebook

1. Connectez-vous à votre compte Facebook
2. **Menu** (votre photo en haut à droite ou les trois barres) → **Paramètres et Confidentialité** → **Paramètres** → **Sécurité et connexion**

Modification Mot de passe

Activation double authentification
Permet d'ajouter ou modifier un numéro de téléphone au compte

Sécurité renforcée



Conseils

1. Mettre à jour l'appareil et les applications
2. Si vous utilisez une application Navigateur Internet (Chrome, Safari, Edge, etc.), supprimez les témoins de navigation (cookies) et les fichiers cache
3. Choisissez un mot de passe fort et modifiez-le si vous doutez d'une violation
4. Ne divulguez jamais votre nom d'utilisateur et votre mot de passe
5. Si vous êtes sur un Wi-Fi public, n'entrez jamais de données personnelles
6. Si vous n'êtes pas sur votre appareil, utilisez toujours la fonction Déconnexion dans la page lorsque vous quittez un service en ligne

Pour la suppression des Témoins et des fichiers en cache via un Navigateur Internet, vous pouvez vous référer au **thème 10, J'utilise sécuritairement et efficacement Internet — Fiche 10.1**

Données personnelles

Si vous possédez une tablette, un cellulaire, un ordinateur, des comptes, si vous naviguez sur le Web, utilisez une montre intelligente, etc. vous communiquez un très grand nombre d'informations. Ce n'est donc plus un secret pour personne, vos activités génèrent des données.

Nous avons dépassé le « Je n'ai rien à cacher ». Toutes informations transmises ne sont pas forcément mauvaises, mais vous devez malgré tout rester vigilant.

Information sur Google

La recherche Google est souvent le premier outil que les gens utilisent pour trouver des informations publiées à votre sujet.

Tapez votre nom sur www.google.ca afin d'afficher les informations publiques vous concernant.

Si vous voulez voir les photos, vous devez filtrer les résultats par **Images**.

Si vous découvrez du contenu que vous ne souhaitez pas voir s'afficher en ligne, comme votre numéro de téléphone ou une photo inappropriée, déterminez tout d'abord qui contrôle ce contenu : vous ou une autre personne.

- **Si c'est vous** : Regardez où vous avez transmis l'information et vous pouvez gérer à partir de cet endroit toutes vos informations
- **Si c'est une autre personne** : Regardez où l'information a été transmise et demandez à la personne de la retirer

Violation de données

Il existe un site Web qui permet de savoir si notre adresse de courriel ou notre numéro de téléphone a été compromis. D'utilisation très simple, il peut vous permettre de savoir dans quel incident il y a eu une violation de vos données personnelles.

Ai-je été pwned?

https://haveibeenpwned.com/

Si des violations s'affichent, vous devez vous assurer que vos mots de passe sont forts et différents de celui lors de l'incident de sorte qu'une violation d'un service ne mette pas en danger tous vos autres services.

Comment savoir si vous êtes victime d'un vol d'identité financier?

- Vous ne recevez plus vos relevés bancaires et/ou de cartes de crédit
- Des achats ont été faits sur votre carte de crédit et ce n'est pas vous qui les avez faits
- Une agence de recouvrement vous signale que vous êtes en défaut de paiements
- Vous vous retrouvez avec un casier judiciaire sans que vous ayez commis aucun acte criminel
- Un créancier vous informe qu'il a approuvé votre nouvelle carte de crédit sans que vous en ayez fait la demande
- Recevoir une amende par la poste dont vous n'êtes pas l'auteur peut être aussi un indice

Que faire si vous croyez avoir été victime d'un vol d'identité financier?

- Communiquez avec la police de votre région
- Informez les institutions financières
- Si vous croyez que votre numéro d'assurance sociale a été volé, communiquez avec Service Canada

Vol de compte en ligne

Un vol de compte en ligne devient diminué si votre mot de passe est bien sécurisé et que la double authentification est activée.

Que faire si vous croyez avoir été victime d'un vol d'identité en ligne?

Modifiez votre mot de passe et vos questions de sécurité.
S'il est possible pour vous de contacter le service à la clientèle au téléphone, appelez-les sans tarder.

Faux profil Facebook

Certains s'amusent à voler la photo de profil et l'image de couverture de profils Facebook. Ensuite, ils créent de faux comptes Facebook avec ceux-ci. Évidemment, le profil sera créé avec le même nom que la personne à qui ils auront volé les photos. Le but étant ensuite de pouvoir faire des demandes d'amis à vos contacts. Si votre liste d'amis est accessible à tout le monde, ils seront d'autant plus tentés de vous choisir afin de piéger vos amis Facebook.

Comment reconnaitre un faux profil Facebook

La première chose à faire est d'afficher la page du profil.

- La date de création du compte

- Pas ou peu d'amis
- Le peu de contenu
- Dans l'éventualité d'un double compte d'ami, il vous suffit d'appeler la personne et lui demander si elle vient de créer un nouveau compte

Cacher sa liste d'amis Facebook

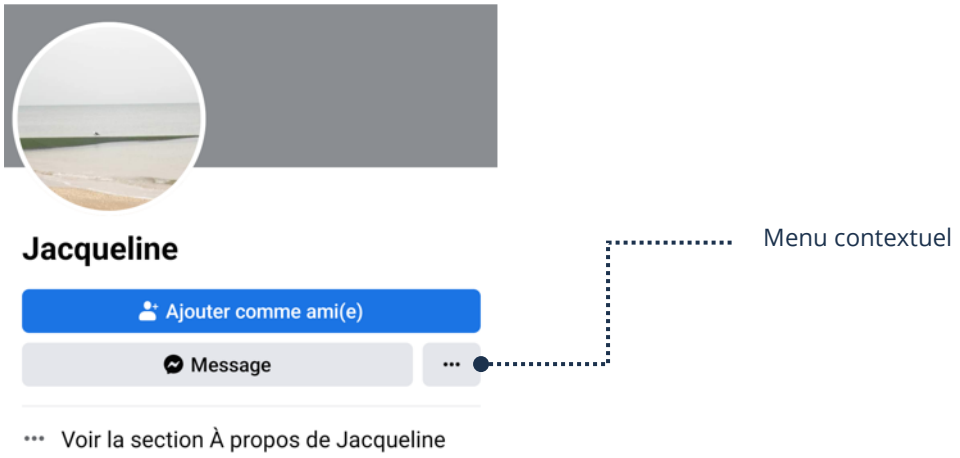
Si vos amis Facebook ne sont pas affichés à la terre entière, ceci pourra rebuter quelques voleurs d'identité.

1. **Ouvrez Facebook → Menu → Paramètres et confidentialité → Paramètres → Comment les autres peuvent vous trouver et vous contacte → Qui peut voir votre liste d'amis → Choisissez Amis**

Signalement d'un faux profil Facebook

Si, malgré tout, quelqu'un a créé un faux profil de vous, vous ou un de vos amis peut signaler ce faux profil.

1. **Faites afficher la page du faux profil → Menu contextuel → Signaler le profil → Usurpation d'identité et suivez ce qui est inscrit à l'écran**



Conseils

- Ne donnez vos renseignements personnels que lorsque la loi l'exige et seulement si vous avez confiance en la personne qui vous les demande
- Ne perdez pas de vu vos cartes de débit et crédits
- Déchiquetez vos documents avec des informations personnelles avant de les jeter
- Des mots de passe sécuritaires pour tous vos comptes en ligne

- Surveillez les irrégularités
- Si une personne vous envoie un courriel disant être en difficulté, renseignez-vous avant de répondre au courriel
- Si vous êtes vous-même victime d'envoi de courriel à votre nom, modifiez votre mot de passe de votre compte et assurez-vous que vous n'avez pas un filtre ajouté pour rediriger vos courriels vers quelqu'un d'autre
- Si vous êtes confus et ne savez pas quoi faire, demandez de l'aide