Ma sécurité et les médias sociaux

Action ontarienne contre la violence faite aux femmes
Janvier 2015

Action ontarienne contre la violence faite aux femmes

288, rue Dalhousie, pièce E
Ottawa (Ontario) K1N 7E6
Tél. : 613 241-8433
Téléc. : 613 241-8435

aocvf@francofemmes.org
www.aocvf.ca

INSTITUT DE FORMATION
EN MATIÈRE DE VIOLENCE FAITE AUX FEMMES
www.formationviolence.ca

Ce guide est accessible en ligne. Il est également accompagné de deux diaporamas sur les médias sociaux. Le tout est disponible dans la section réservée de la formation en ligne du site Internet de l'Institut de formation en matière de violence faite aux femmes (AOcVF) : www.formationviolence.ca

Étant donné que ce guide s'adresse au réseau de l'Action ontarienne contre la violence faite aux femmes, le texte a été féminisé.

Les opinions exprimées dans ce document représentent celles de l'auteure et ne représentent pas nécessairement le point de vue du gouvernement de l'Ontario.

Nous remercions le gouvernement de l'Ontario pour son soutien financier qui a permis la réalisation de cet outil.

Ontario

Rédaction : Virginie Tiberghien
Ce guide est disponible en grands caractères, sur demande.
Imprimé en janvier 2015

Table des matières

Introduction

À l'heure actuelle, les médias sociaux sont très présents dans la société. Facebook et Twitter en sont sûrement les plus populaires. Grâce à eux, partager des photos, des anecdotes de sa vie ou encore commenter des faits d'actualité… tout en s'adressant à un large public se font facilement.

Ces moyens de communiquer qui sont relativement récents et qui restent à la portée de toutes et tous mélangent et brouillent les frontières entre la sphère publique et le domaine privé. D'un seul clic, les pensées les plus intimes se retrouvent, en quelques secondes, lues par des dizaines, des centaines, voire parfois, des milliers d'autres personnes proches ou complètement étrangères.

Les médias sociaux présentent des avantages et des défis. Ils peuvent, d'un côté, se présenter comme un très bel outil de communication avec lequel il est facile et rapide d'atteindre un public cible. D'un autre côté, leur portée peut être plus large que celle à laquelle on pense. De plus, l'oubli numérique, qui consiste à faire effacer son passé sur la Toile, reste très difficile à obtenir.

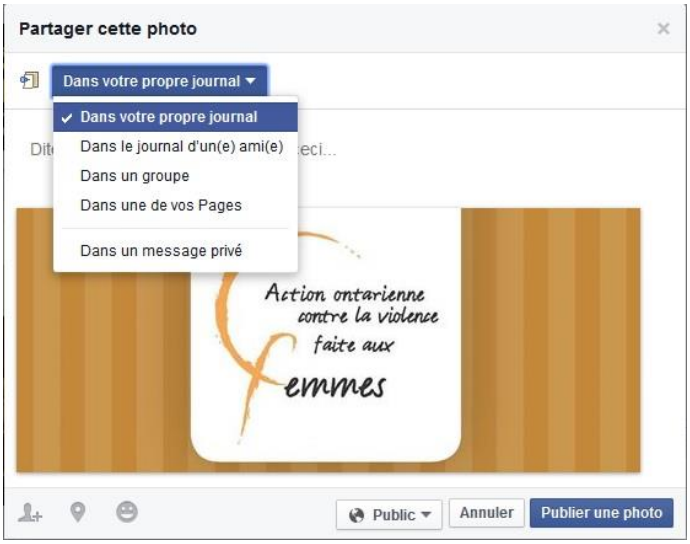
C'est pourquoi il est important lors de l'utilisation des médias sociaux, d'être conscientes des risques qu'ils peuvent représenter. Des moyens existent pour naviguer à travers eux et pour les utiliser de manière plus sécuritaire.

Ce guide présente les médias sociaux les plus populaires et explore les manières de se protéger pour favoriser une utilisation sécuritaire des ceux-ci. Les captures d'écran illustrent les explications des différentes options que l'on peut appliquer. Le monde des médias sociaux étant en constante évolution, certaines méthodes illustrées dans ce guide peuvent être soumises à des changements.

1. Ampleur des médias sociaux

Comme son nom l'indique, un média social est une plateforme Internet qui propose des fonctions « sociales » aux internautes : création participative de contenus, partage de photos, de liens, clavardage (ndlr : *chat* en anglais)…

Une des caractéristiques des médias sociaux est le partage. Très facilement, on peut partager des informations personnelles mais aussi des informations trouvées sur d'autres sites ou partagées par d'autres. De ce fait, les données envoyées sur les réseaux sociaux sont difficiles à effacer complètement car elles peuvent dépasser les limites du site sur lequel on publie l'information initialement.



Exemples ci-dessus : Sur Facebook, une photo partagée sur un profil peut être repartagée par les « amis » de ce profil sur leur propre profil, sur le journal d'un de leurs « amis »…

Au Canada, près de 24 millions de personnes, soit 69 % de la population, ont visité au moins un site de réseautage social en 2013. Facebook et Twitter sont en tête en termes de popularité auprès des Canadiennes et Canadiens.
19 millions de personnes d'un océan à l'autre se sont connectées sur Facebook au moins une fois par mois[1].

[1] Statistiques issues de l'Autorité canadienne pour les enregistrements Internet. 2014. Dossier Documentaire de l'ACEI. En ligne : http://www.cira.ca/factbook/2014/fr/the-canadian-internet.html

2. Sécurité dans l'usage des médias sociaux

a. Facebook

Le réseau social le plus populaire au Canada est Facebook. C'est pourquoi ce guide s'attarde sur les différentes procédures possibles à suivre pour être un peu plus maître de son profil. Facebook fait régulièrement des mises à jour dans les paramètres de sécurité et de confidentialité. Il est donc important de les vérifier régulièrement.

Inscription sur Facebook

À l'inscription sur ce réseau social, le site demandera obligatoirement d'y inscrire son prénom, son nom, son courriel ou son numéro de téléphone, sa date de naissance et de choisir un mot de passe.
À ce stade, le site demande d'inscrire son véritable nom et prénom qu'il est possible de modifier par la suite.

Suggestions pour la sécurité :

- Créer une adresse courriel qui ne sert qu'aux inscriptions sur les médias sociaux et qui ne contient pas le nom et le prénom réels.
- Toujours préférer mentionner son adresse courriel qu'un numéro de téléphone.

Une fois inscrite sur Facebook, ce réseau social suggérera d'y inscrire plus d'informations concernant le lieu de travail actuel et passé, la scolarité, le lieu de résidence actuel et passé, l'état civil (marié, célibataire, divorcé, dans une relation compliquée…), les membres de la famille, les croyances religieuses, les opinions politiques…

Suggestion pour la sécurité :

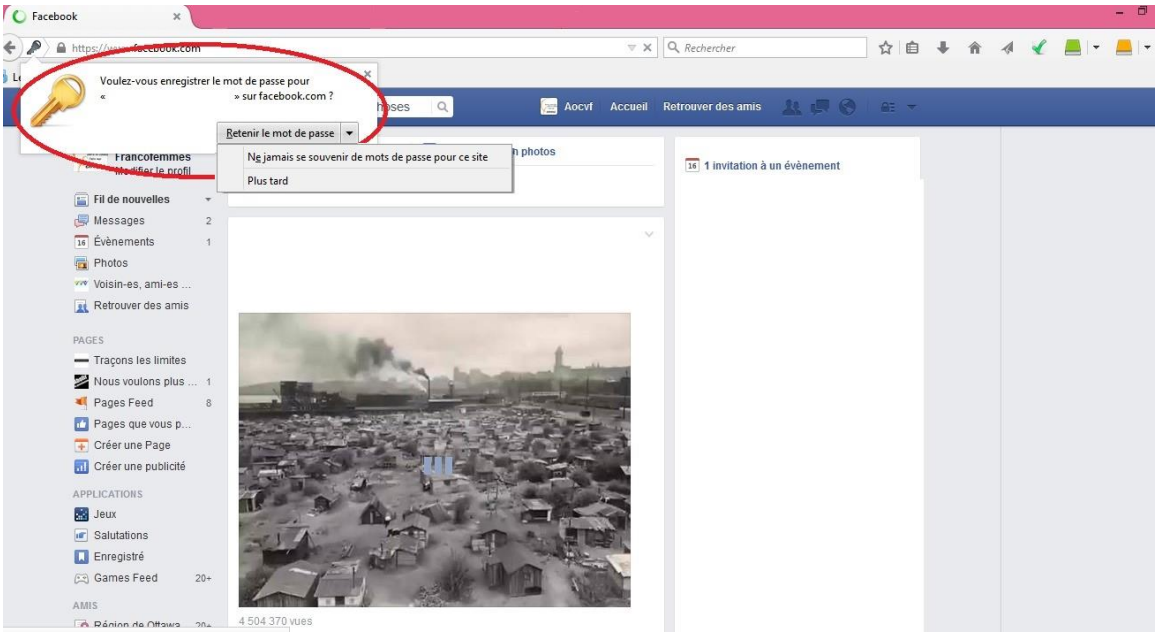
- Ne pas remplir ces champs d'informations. Plus d'informations personnelles se retrouvent sur Facebook, plus il sera facile de retrouver une personne ou d'entrer dans sa vie privée.

Connexion-Déconnexion à son profil

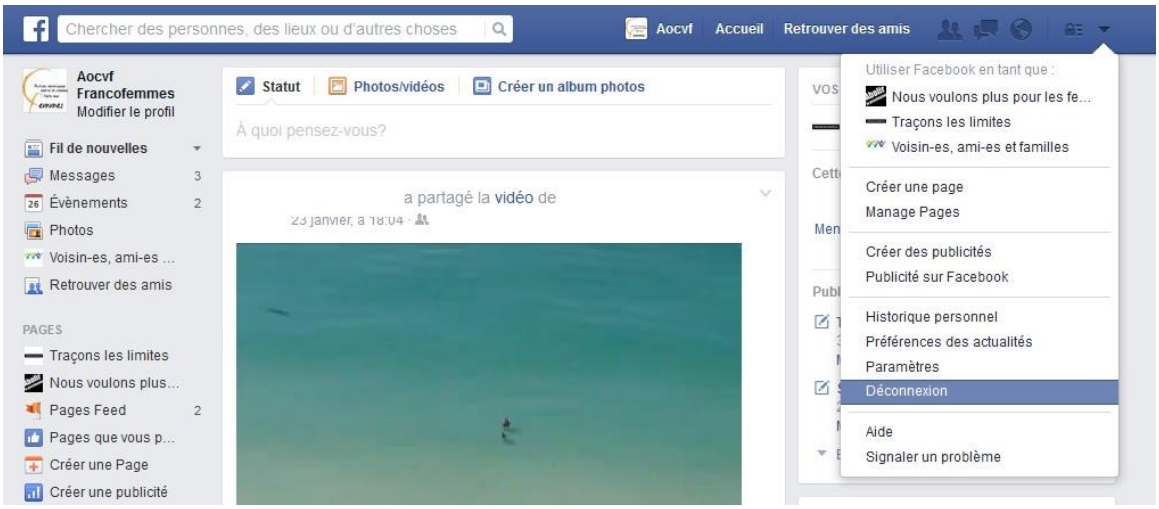
Pour se connecter à son profil, il faut introduire son adresse courriel et son mot de passe. Si plusieurs personnes utilisent le même ordinateur, il faut veiller à ce que la demande d'introduction de l'adresse courriel et du mot de passe se fasse à chaque fois.

Suggestions pour la sécurité :

- Ne pas cocher la case « Garder ma session active » sur la page d'accueil du site. Sinon, on entrera dans la session directement lorsqu'on navigue sur Facebook sans avoir à redonner l'adresse courriel ni le mot de passe.
- Ne pas accepter d'enregistrer le mot de passe associé à l'adresse courriel sur le site de Facebook, comme le propose le navigateur Internet. Ou cliquer sur « Ne jamais se souvenir de mots de passe pour ce site ».



Pour se déconnecter de son profil, il faut cliquer sur le bouton « Déconnexion » sous la flèche dans le coin supérieur droit de son profil. Fermer uniquement la fenêtre de navigation ne fermera pas le profil. À la prochaine visite sur Facebook, le site se connectera automatiquement au dernier profil visité s'il n'a pas été complètement déconnecté.



Suggestion pour la sécurité :

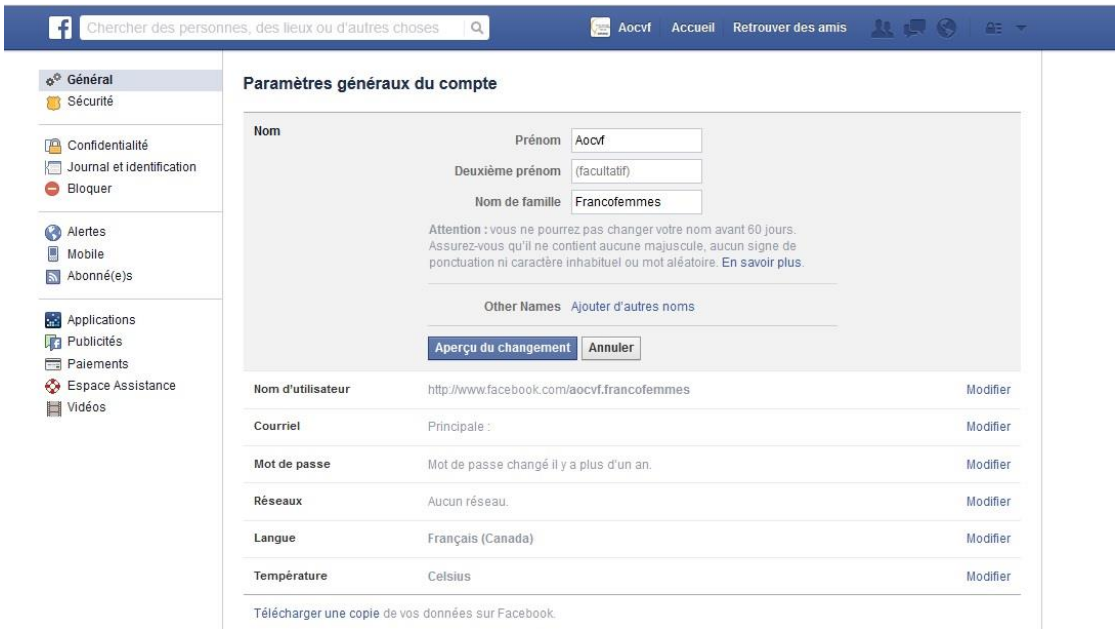
- Toujours se déconnecter complètement de son profil pour empêcher toute visite inattendue.

Paramètres de sécurité sur Facebook[2]

Pour accéder aux paramètres de sécurité et de confidentialité du profil créé sur Facebook, il faut cliquer sur la flèche qui pointe vers le bas dans le coin supérieur droit de l'interface de Facebook et ensuite, cliquer sur « Paramètres ».

Une page permettant de modifier son nom, son nom d'utilisateur, son courriel, son mot de passe s'affiche.

[2] Inspiré des notes de Bernard Charlebois sur les médias sociaux, réalisées pour Action ontarienne contre la violence faite aux femmes en 2014.



Suggestions pour la sécurité :

- Modifier son nom et son prénom pour être retrouvée moins facilement. Par exemple, en retirant les voyelles de son nom de famille.
- Utiliser une adresse courriel spécifique pour les inscriptions sur les médias sociaux. En effet, pour retrouver des personnes sur Facebook, on peut effectuer la recherche en utilisant l'adresse courriel. Si l'adresse courriel utilisée n'est pas celle que l'on communique généralement à ses contacts, personne ne pourra retrouver le profil au moyen de l'adresse courriel.
- Utiliser un mot de passe original combinant des caractères majuscules, minuscules, numériques et des sigles de ponctuation.
- Changer de mot de passe régulièrement.

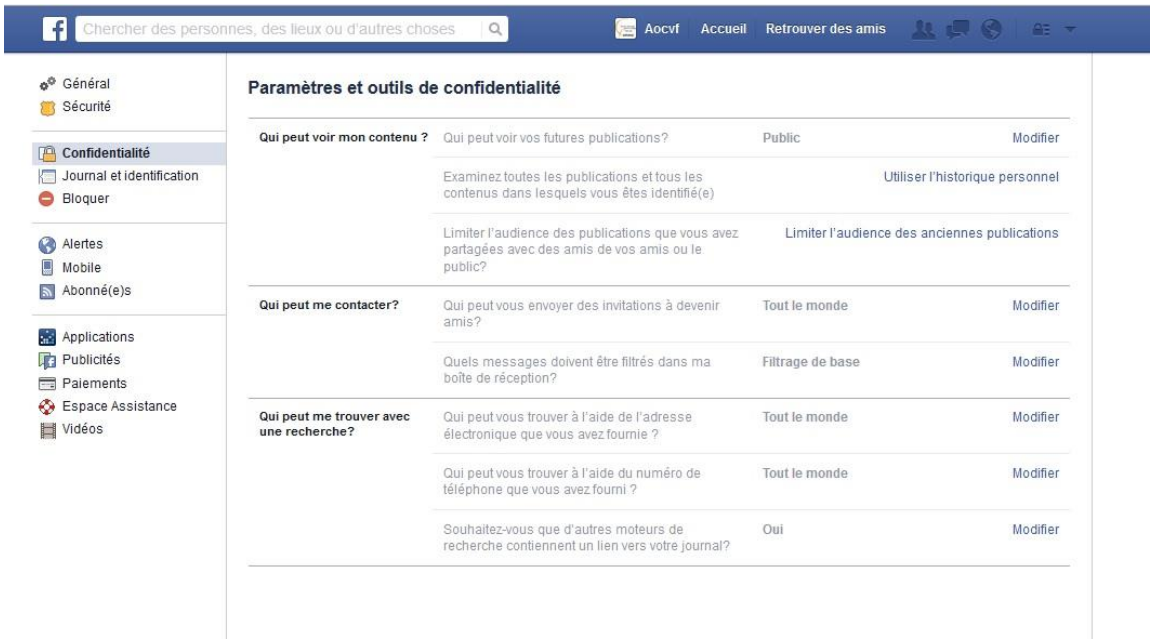
Dans l'onglet « Sécurité » dans la colonne de gauche sur la même page, on accède à des options proposées par Facebook pour augmenter sa sécurité.

- Alertes de connexion : avertir lorsque le compte est utilisé à partir d'un ordinateur ou d'un appareil mobile jamais encore utilisé. Avertissement par courriel ou message texte.
- Approbation de connexion : un code de sécurité est demandé lors d'accès au compte à partir de navigateurs non reconnus. Cette option limite davantage la possibilité que quelqu'un accède au compte.
- Générateur de code : application pour réinitialiser le mot de passe ou le code d'approbation de connexion à partir d'un mobile.
- Contacts de confiance : les contacts de confiance sont des amies ou amis qui peuvent aider en toute sécurité en cas de problèmes d'accès à son compte. Par exemple, en cas d'oubli du mot de passe.
- Navigateurs de confiance : possibilité d'enregistrer les navigateurs souvent utilisés pour ne pas devoir confirmer son identité et ne pas recevoir d'avertissement de connexion lorsqu'on tente de s'y connecter.
- Où vous êtes connectée : voir d'où la session est active présentement et avec quel navigateur Internet (Firefox, Google Chrome, Internet Explorer, applications téléphoniques). Le lieu peut être approximatif mais parfois, aussi très précis avec les GPS présents dans les téléphones intelligents et les tablettes.
- Désactiver votre compte : possibilité de désactiver le compte. Les informations partagées sur ce réseau social ne s'effaceront pas complètement du Net. Elles y resteront stockées. Mais ne seront plus accessibles par vous et les autres internautes. Le compte pourra être réactivé plus tard. Toutes les informations partagées avant la désactivation réapparaîtront.

Suggestion pour la sécurité :

- Lors d'un conflit de couple, par exemple, où le conjoint ou la conjointe devient menaçant, il est parfois mieux de désactiver complètement son compte temporairement ou définitivement, afin que des informations qui pourraient compromettre la sécurité des enfants ou de soi-même ne lui soient transmises.

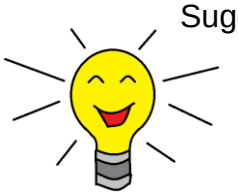
Paramètres et outils de confidentialité sur Facebook



Qui peut voir votre contenu ?

- Qui peut voir vos futures publications ? : préciser qui pourra lire les publications (public, amis, seulement moi ou personnalisé). L'option choisie sera mémorisée pour être appliquée par défaut lors des prochaines publications. Ce choix peut se faire également lors de la publication.
- Examiner le contenu dans lequel vous êtes identifiée : examiner toutes les publications et tout le contenu dans lesquels nous sommes identifiée. Pour ce faire, cliquer sur « Utiliser l'historique personnel » et examiner tout l'historique. Chaque action sur Facebook peut être masquée du profil ou supprimée via cet historique.

- Limiter l'audience des publications partagées avec des amis de vos amis ou le public : pour les publications passées qui auraient été publiées sous les paramètres « public » ou « amis de vos amis », il y a moyen d'y restreindre l'accès à la catégorie « amis » seulement. Attention, les personnes qui auraient été identifiées dans ces publications et qui ne font pas partie de la catégorie « amis » continuent à y avoir accès, malgré le changement de paramètres.



Suggestion pour la sécurité :

- Se méfier des options « Public », « Amis de vos amis » et « Amis des personnes identifiées » qui permettent à des personnes auxquelles on ne pense pas forcément de voir, copier, enregistrer nos publications. Si on veut restreindre l'accès à son profil, privilégier des listes d'amis que l'on connaît (voir « Gérer ses amis Facebook »).

Qui peut me contacter ?

- Qui peut vous envoyer des invitations pour devenir votre ami ? : préciser qui peut envoyer des invitations à devenir ami (tout le monde ou seulement, les amis des amis).
- Quels messages doivent être filtrés dans votre boîte de réception ? : choisir un filtrage pour trier les messages qui arrivent dans la boîte de réception de Facebook :
  - ✓ Le filtrage de base : recevoir les messages des amis et des gens possiblement de l'entourage
  - ✓ Le filtrage strict : recevoir exclusivement les messages des amis

Qui peut me trouver ?

- Qui peut vous trouver à l'aide de l'adresse courriel fournie ? : à la création d'un profil, Facebook permet d'importer directement ses contacts de son carnet d'adresse courriel. Si l'on choisit de ne pas être retrouvée par son adresse courriel, cela ne s'appliquera qu'aux personnes qui ne possèdent pas déjà cette adresse courriel dans leur carnet d'adresse et qui voudrait faire la recherche via la barre de recherche dans Facebook.
- Qui peut vous trouver à l'aide du numéro de téléphone fourni ? : à la création d'un profil, Facebook permet d'importer directement ses contacts de répertoire téléphonique. Si l'on choisit de ne pas être retrouvée par son numéro de téléphone, cela ne s'appliquera qu'aux personnes qui ne possèdent pas déjà ce numéro dans leur répertoire et qui voudrait faire la recherche via la barre de recherche dans Facebook.

- Souhaitez-vous que d'autres moteurs de recherche contiennent un lien vers votre journal ? : Lorsque ce paramètre est activé, des moteurs de recherche peuvent présenter un lien vers ce profil dans leurs résultats. En cas de désactivation de ce paramètre, un certain temps pourra être nécessaire avant que les moteurs de recherche arrêtent de présenter le lien dans leurs résultats.

Suggestions pour la sécurité (rappel) :

- Utiliser une adresse courriel spécifique pour les inscriptions sur les médias sociaux. En effet, pour retrouver des personnes sur Facebook, on peut effectuer la recherche en utilisant l'adresse courriel. Si l'adresse courriel utilisée n'est pas celle que l'on communique généralement à ses contacts, personne ne pourra retrouver son profil au moyen de l'adresse courriel.
- Il est préférable de ne pas inscrire son numéro de téléphone sur les réseaux sociaux.
- Se méfier des options « Tout le monde » et « Amis et leurs amis » qui permettent à des personnes auxquelles on ne pense pas ou qu'on préfère qu'elles ne nous trouvent pas, de nous rechercher.

Gérer ses amis Facebook

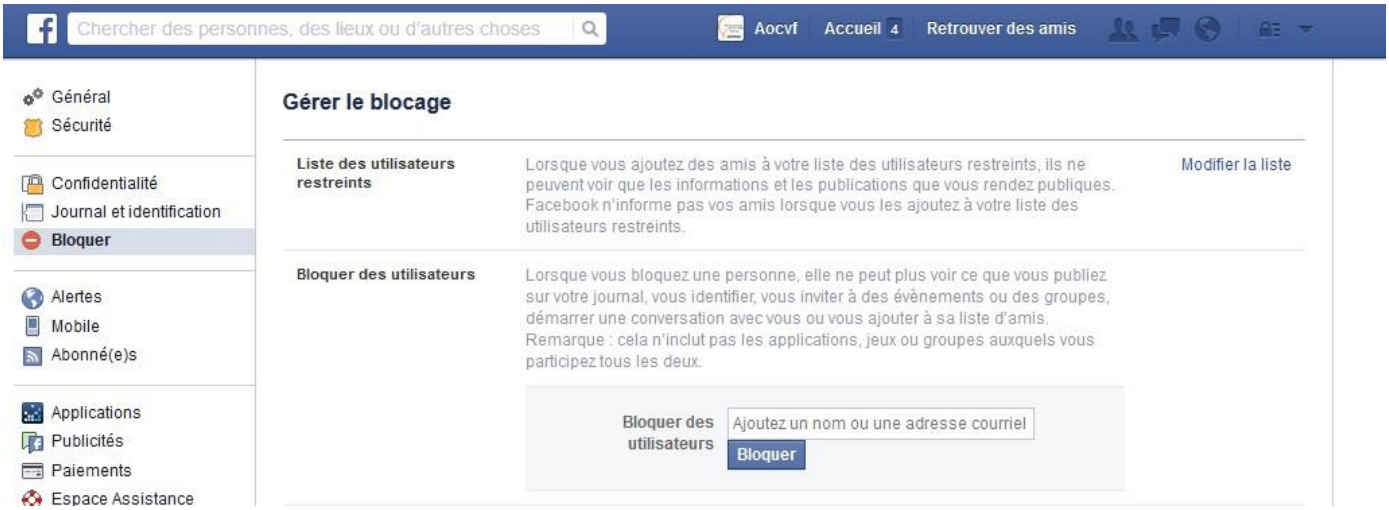
La facilité avec laquelle on peut entrer en contact avec des personnes pousse à accepter énormément de personnes, parfois pas vraiment proches, dans nos listes de contacts Facebook.

Il est possible de créer des groupes d'amis différents au sein de la liste générale d'amis. En allant dans sa liste d'amis et en cliquant sur le bouton 

à droite des noms, il est possible de les ajouter individuellement à une autre liste et de créer de nouvelles listes.

Dans la liste d'amis, il est possible également d'en « retirer de la liste d'amis » afin de les empêcher d'avoir accès définitivement à son profil.

Dans certains cas, le blocage d'une personne sera plus sécuritaire. Il est possible de le faire via l'onglet « Paramètres » auquel on accède dans le coin supérieur droit , puis « Bloquer ». Un champ de formulaire permet d'y inscrire une adresse courriel ou le nom d'une personne, si elle possède un profil sur Facebook. Ainsi, cette personne ne pourra pas retrouver ce profil ni le contacter pour l'ajouter dans sa propre liste d'amis.

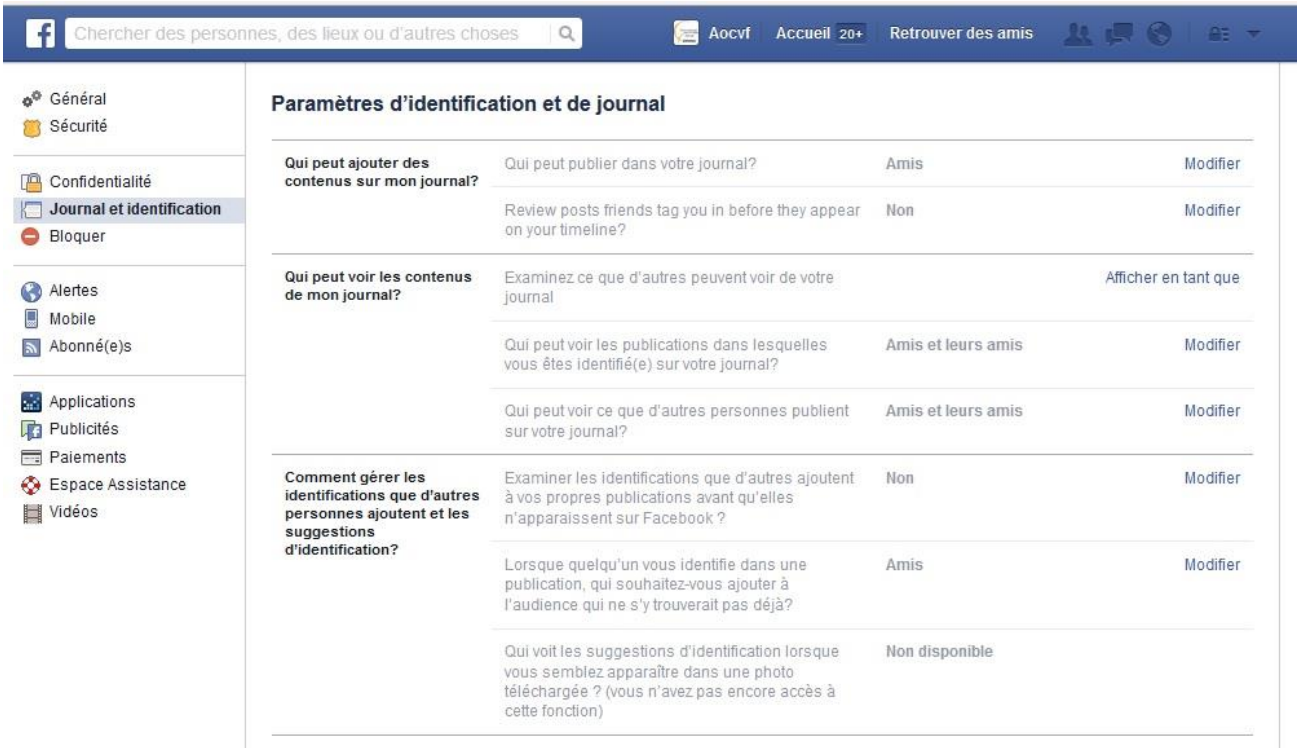


Suggestions pour la sécurité :

- Faire un tri régulièrement dans sa liste de contacts Facebook, ne pas hésiter à en supprimer. Aucune notification ne leur sera envoyée pour leur signaler qu'ils ne font plus partie de cette liste d'amis.
- Réfléchir avant d'accepter quelqu'un dans sa liste d'« amis », pour être certaine que c'est ce que l'on veut.
- Faire des groupes d'amis avec des accès différents aux informations partagées sur le réseau social.

Interagir sur Facebook

Facebook est un outil fabuleux pour interagir avec d'autres personnes qu'elles soient géographiquement proches ou éloignées. Il est aisé avec cet outil de partager des photos, partager des liens vers un article, des vidéos, d'écrire quelques lignes à une seule personne ou à toute une communauté, de retrouver des amis perdus de vue depuis longtemps, de « *chatter* » (ndlr : « clavarder » en français) en direct avec d'autres…
Toutes les publications que l'on fait sur Facebook peuvent être contrôlées via l'onglet « Journal et identification ».



Qui peut ajouter des contenus sur mon journal ?

- Qui peut publier dans votre journal ? : définir le groupe de personnes qui pourront publier du contenu sur le journal du profil. Choix disponibles : amis, seulement moi.
- *Review posts friends tag you in before they appear on your timeline* ? (en français, examiner les messages dans lesquels vos amis vous identifient avant que ceux-ci n'apparaissent dans votre journal) : permet d'approuver manuellement toutes les publications faites par d'autres faisant mention de la personne à qui appartient le profil. Cela évite que des informations soient dévoilées par d'autres et communiquées à un large public.

Suggestions pour la sécurité :

- Rester maître de ce qui est publié sur son profil est très important car on ne sait jamais ce que nos « amis » sur Facebook sont susceptibles de publier nous concernant. Restreindre donc leur possibilité de publier sur le journal.
- Vérifier régulièrement son profil afin de modérer les commentaires ou les publications que d'autres pourraient faire.

Qui peut voir les contenus de mon journal ?

- Examinez ce que d'autres peuvent voir de votre journal : outil intéressant pour voir exactement comment notre profil apparaît pour une personne en particulier.
  Cliquer sur « Afficher en tant que ». Dans la barre noire qui s'affiche, taper le nom d'une amie. Le profil s'affiche tel que cette personne le voit.

L'option est également disponible lorsqu'on se trouve sur son journal sous un bouton dans le coin inférieur droit de la photo de couverture, représenté par trois points.

- Qui peut voir les publications dans lesquelles vous êtes identifiée sur votre journal ? : spécifier qui peut voir les publications dans lesquelles la personne à qui appartient le profil est identifiée.
- Qui peut voir ce que d'autres personnes publient sur votre journal ? : spécifier qui peut voir les publications faites par d'autres personnes sur son journal.

Comment gérer les identifications que d'autres personnes ajoutent et les suggestions d'identification ?

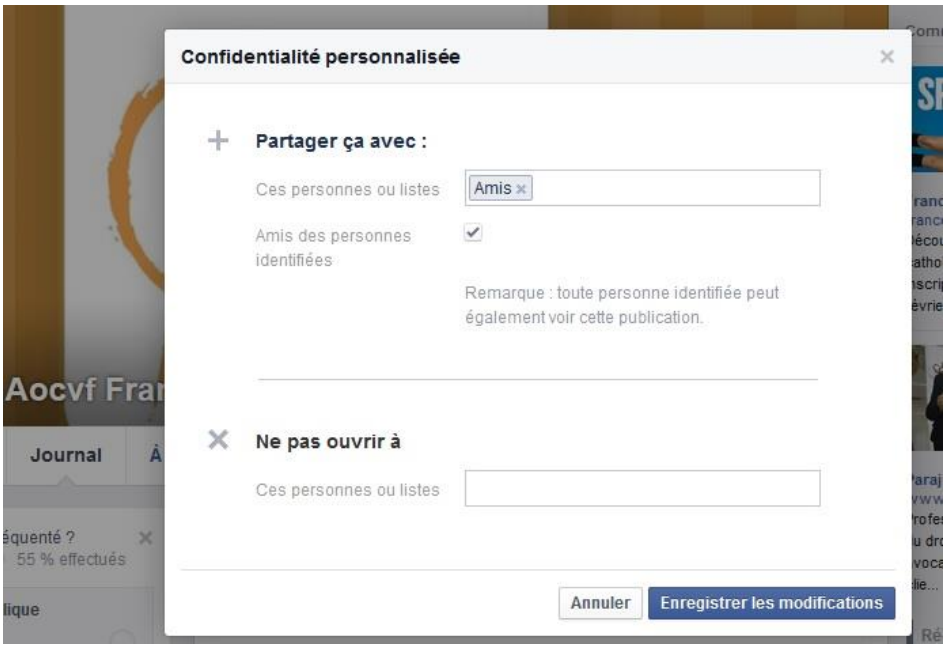
- Examinez les identifications que d'autres ajoutent à vos propres publications avant qu'elles n'apparaissent sur Facebook : permet d'approuver, préalablement à la publication sur Facebook, les identifications que les autres internautes pourraient faire sur nos propres publications
- Lorsque quelqu'un vous identifie dans une publication, qui souhaitez-vous ajouter à l'audience qui ne s'y trouverait pas déjà ? : possibilité d'ajouter des groupes d'amis à l'audience qui a accès aux éléments qui nous citent mais publiés par d'autres internautes.

En publiant un élément sur son profil, on a accès également aux paramètres de confidentialité. À chaque publication, on peut choisir l'auditoire auquel on veut s'adresser.

Suggestions pour la sécurité :

- À chaque publication, se poser la question : « Est-ce que j'aimerais que ce que je suis sur le point de publier sur Facebook se retrouve à la Une d'un journal distribué à grande échelle ? ». Car, avec ce réseau social, on ne peut jamais être sûre du lieu où cette information va se retrouver et par qui elle va être lue.
- Limiter au maximum l'audience qui a accès aux publications.
- Au besoin, pour limiter l'audience, créer des groupes d'amis (voir paragraphe « Gérer ses amis Facebook »).
- Éviter d'utiliser la géolocalisation, symbolisée comme suit : . Il est très facile de se géolocaliser de façon précise avec les téléphones intelligents et les tablettes. Mais en termes de sécurité, cela pourrait donner trop d'informations à une personne malveillante qui pourrait s'en servir afin de trouver quelqu'un.
- Éviter de publier des photos d'endroits que l'on pourrait reconnaître.
- Vérifier qu'on a les autorisations des personnes qui apparaissent sur la photo avant de la publier.

Quand on partage quelque chose sur Facebook, il existe une option d'audience, appelée « Personnalisé ». On peut ainsi autoriser le partage avec un groupe d'amis ou avec quelques personnes que l'on inscrit un à un dans le champ : « Partager ça avec : ces personnes ou listes ».
Cette fenêtre permet aussi de bloquer l'accès aux publications à certaines personnes. On peut partager avec ou exclure des personnes sélectionnées une à une, ou des groupes d'amis.

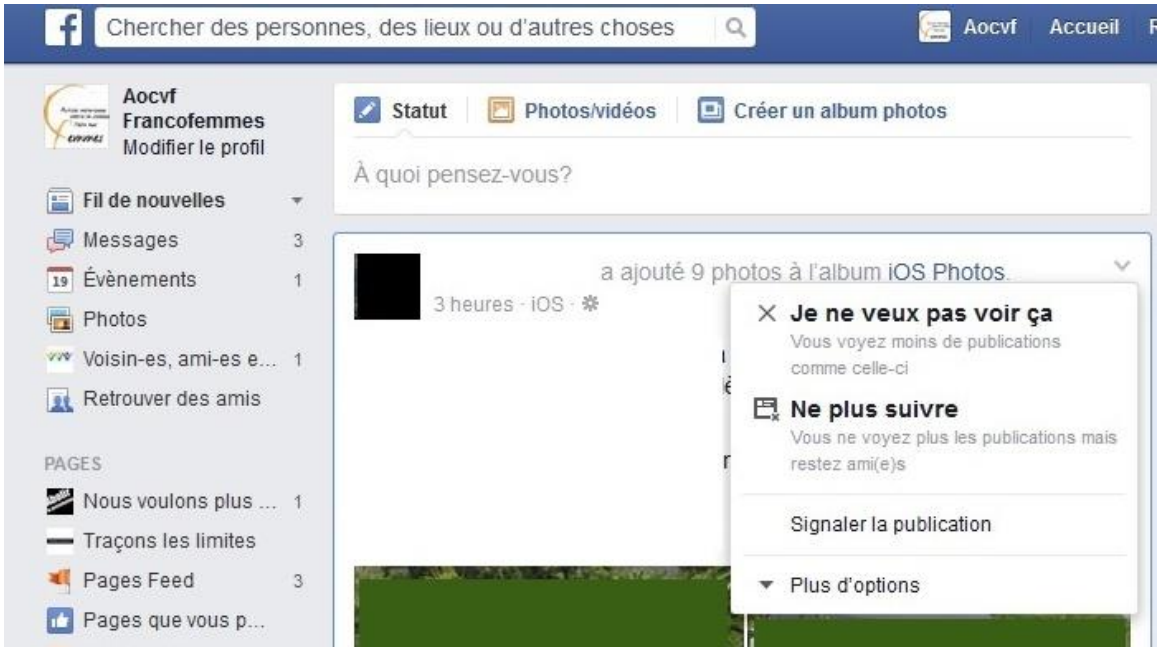


Suggestion pour la sécurité :

- Décocher la case « Amis des personnes identifiées » car elle vise l'ensemble des « amis » des amis qui seront identifiés dans nos publications.

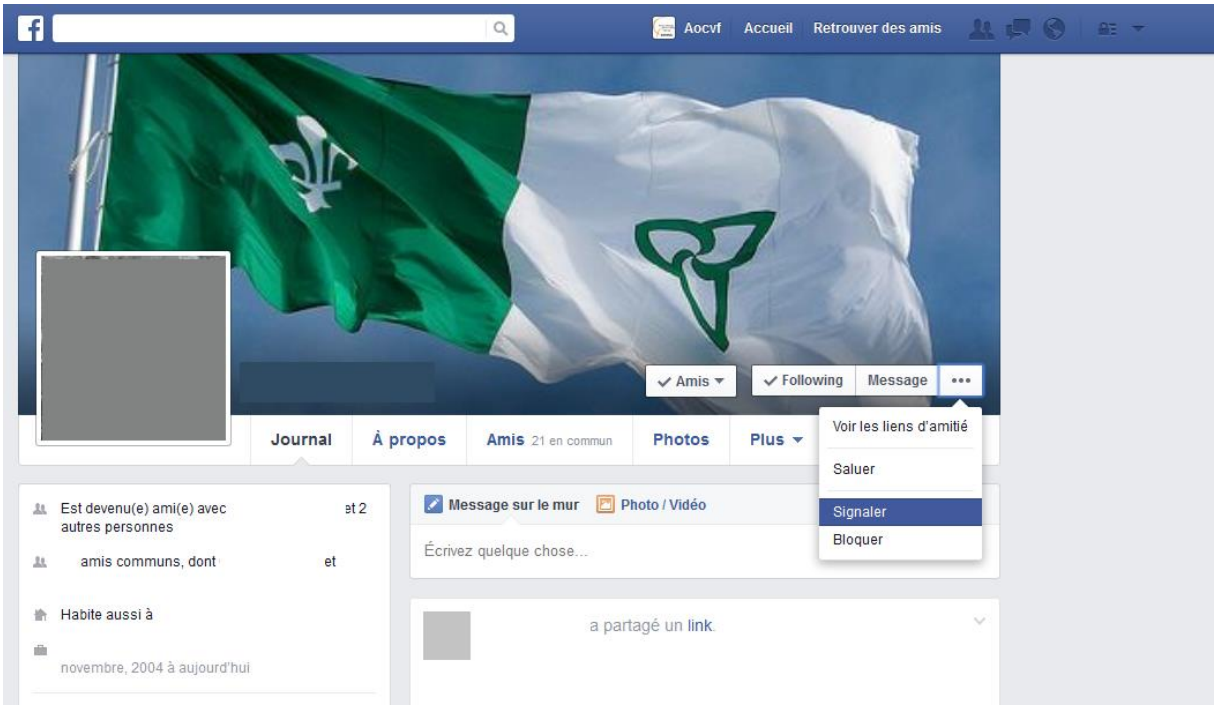
Signaler quelque chose ou quelqu'un sur Facebook

En cas de problème sur Facebook, il y a moyen de signaler les publications ou une personne aux administrateurs de Facebook.
Si une publication est dérangeante (nudité, harcèlement, incitation à la haine…), on peut faire le signalement à partir de la publication qui apparaît sur le fil de l'actualité (page d'accueil dans Facebook) en cliquant sur la flèche dans le coin supérieur droit du cadre de la publication : « Signaler la publication ».



Si la publication qu'on veut signaler se trouve sur son propre profil, on peut le faire via les options reprises sous la flèche dans le coin supérieur droit du cadre de la publication : « Je n'aime pas cette publication ».

Pour signaler une personne, aller sur le profil de celle-ci et cliquer sur le bouton qui contient trois points dans le coin inférieur droit de la photo de couverture. Cliquer sur « Signaler ».



Suggestion pour la sécurité :

- Tout en la signalant, ne pas hésiter également à bloquer la personne dès que des publications de sa part deviennent dérangeantes.

b. Twitter

Twitter est une plateforme Internet de microblogage qui permet aux internautes d'envoyer des messages courts (140 caractères), appelés gazouillis (ndlr : *tweet* en anglais). L'utilisation de mot-clic (ndlr : *hashtag*, en anglais) ou mot-dièse, symbolisé par #, permet de référencer le gazouillis pour faciliter les recherches sur le thème lié à ce mot-clic.
Le principe sur Twitter est que, normalement, tout ce qu'on publie est public. N'importe qui, même les personnes qui ne sont pas abonnées à ce média social, a accès aux publications des autres.
Les paramètres de sécurité et de confidentialité sont moins nombreux que sur Facebook.

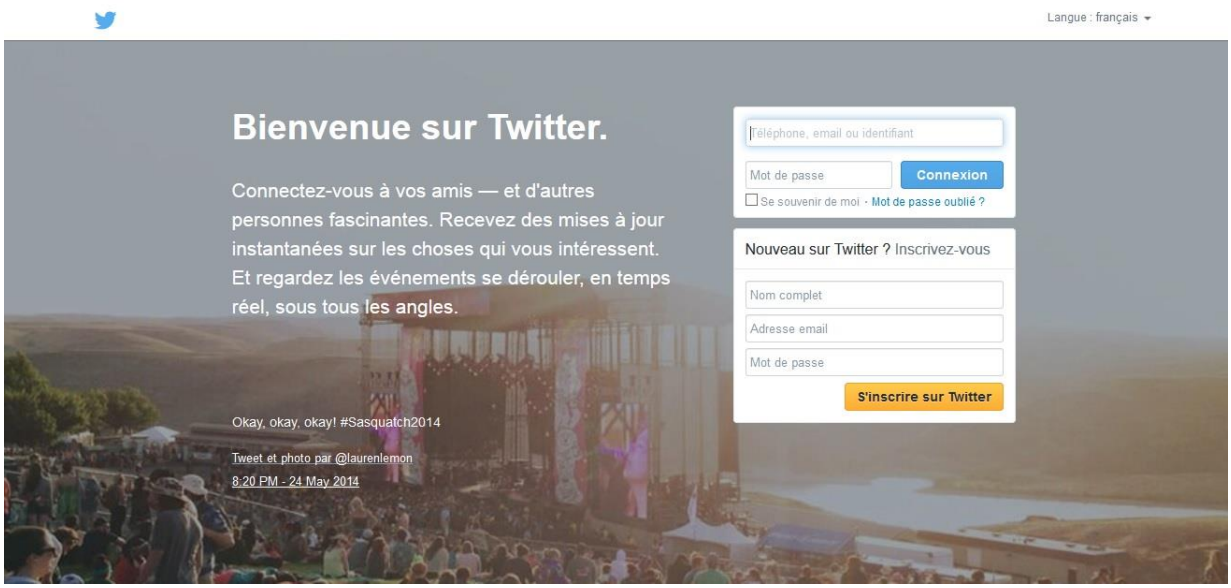
Suggestions pour la sécurité :

- Bien réfléchir à ce qu'on publie car
  - ✓ Tout est public.
  - ✓ Les moteurs de recherche référencent bien les gazouillis.
  - ✓ Un gazouillis retweeté par quelqu'un d'autre devient impossible à effacer complètement. Il n'appartient plus à son auteur original.

Inscription sur Twitter

Pour s'inscrire sur Twitter, il suffit d'indiquer son nom complet, une adresse courriel et un mot de passe. Une fois ce premier formulaire rempli, Twitter demandera de choisir un nom d'utilisateur qui sera le nom qui identifiera le compte sur ce réseau social.

> Par exemple, Action ontarienne contre la violence faite aux femmes a choisi comme nom d'utilisateur : AOcVFOntario.
> Quand on veut lui envoyer un message via Twitter, on utilise @AOcVFOntario.



Suggestions pour la sécurité :

- Ne pas prendre un nom d'utilisateur qui reprend le nom et le prénom réels. Un pseudonyme est plus prudent à utiliser.
- Créer une adresse courriel qui ne sert qu'aux inscriptions sur les médias sociaux peut être utile.
- Utiliser un mot de passe original combinant des caractères majuscules, minuscules, numériques et des sigles de ponctuation.
- Changer de mot de passe régulièrement.

Paramètres de sécurité et de confidentialité

Le site permet de régler quelques paramètres pour accroître la sécurité et la confidentialité de son profil.

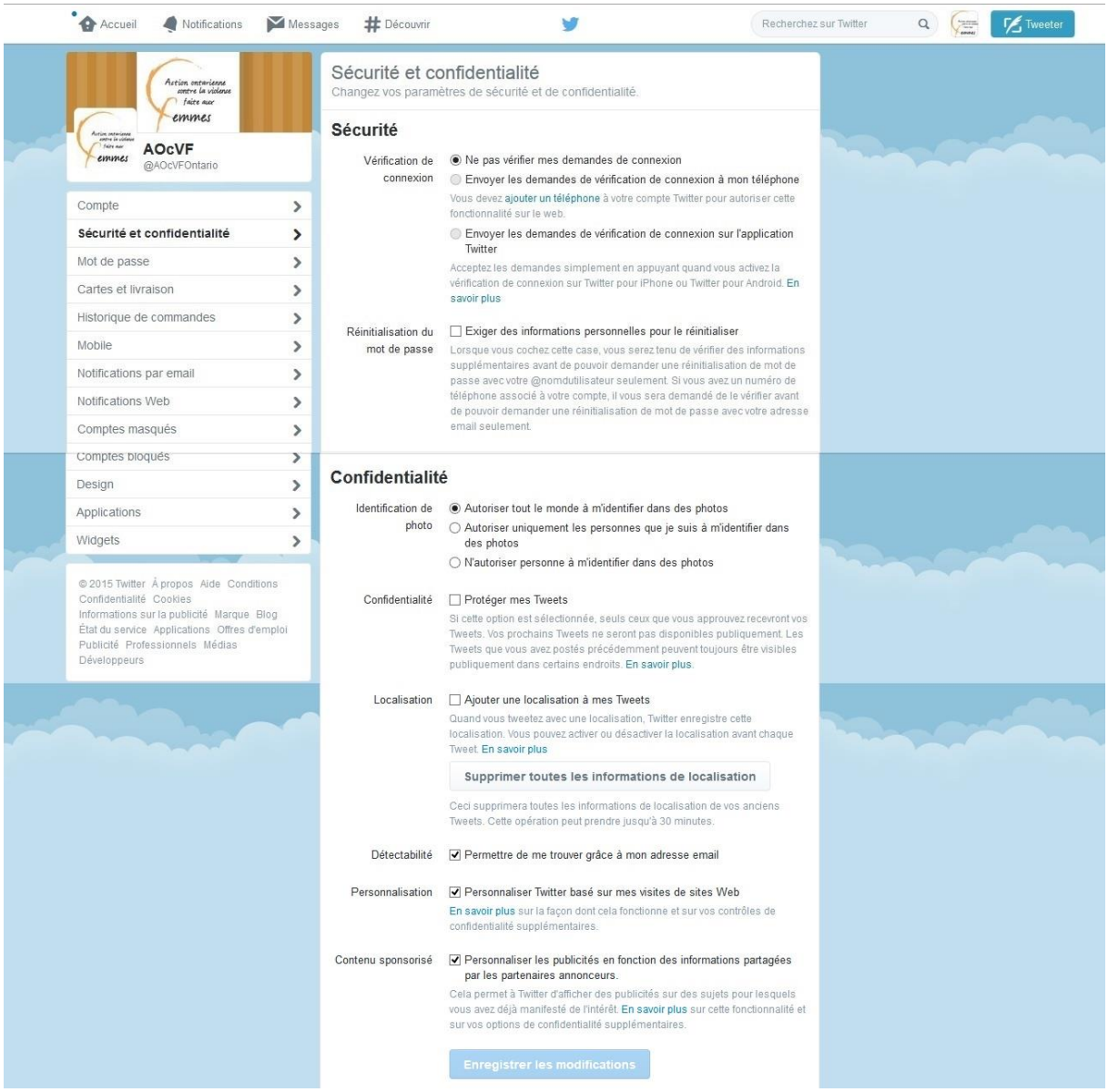
Pour y accéder, cliquer dans le coin supérieur droit de la page d'accueil du profil sur Twitter et ensuite, dans la colonne de gauche sur « Sécurité et confidentialité » (voir illustration page suivante).

Sécurité :

- Vérification de connexion : cette option permet d'envoyer un message texte ou un message électronique pour aviser que quelqu'un se connecte au compte Twitter. Pour activer cette option, il faut soit fournir un numéro de téléphone portable, ou avoir une tablette ou un téléphone intelligent pour pouvoir valider le message électronique via l'application Twitter.
- Réinitialisation du mot de passe : cette option permet de demander des informations personnelles supplémentaires pour réinitialiser le mot de passe.

Confidentialité :

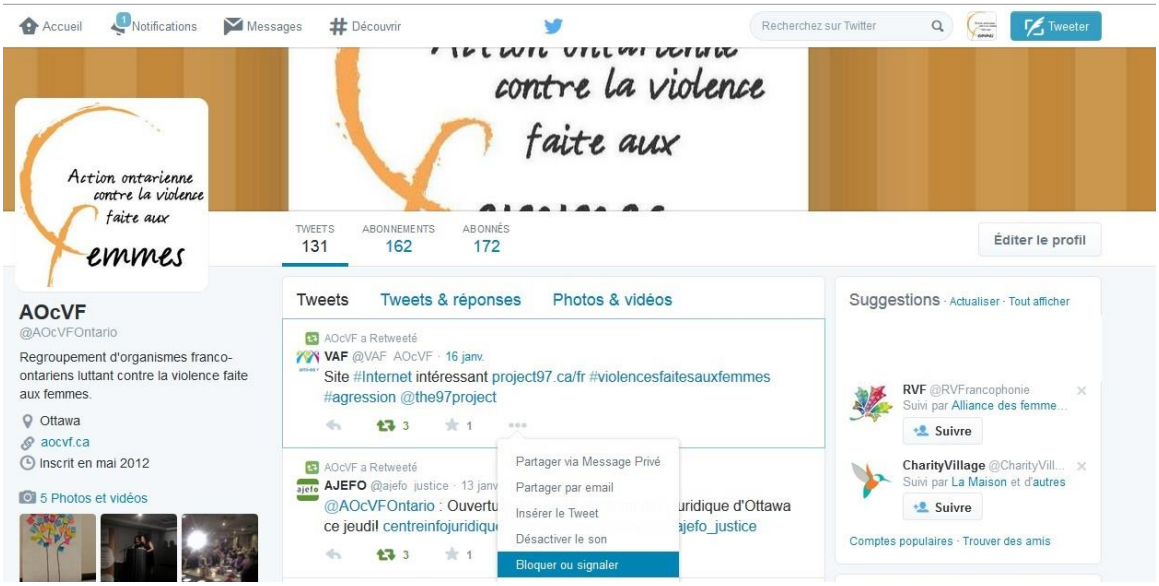
- Identification de photo : permet d'autoriser ou d'interdire d'être identifiée sur des photos publiées sur Twitter.
- Confidentialité : si l'option est cochée, les gazouillis ne seront plus publics. Seules les personnes approuvées pourront les voir.
- Localisation : option de géolocalisation qui permet qu'à chaque gazouillis, le lieu d'où il est publié soit affiché. Avec les téléphones intelligents et les tablettes, le lieu est assez précis (latitude et longitude). Avec le navigateur Internet d'ordinateur, le lieu est plus approximatif.
- Détectabilité : permet de retrouver un profil à partir d'une adresse courriel.



Suggestions pour la sécurité :

- Bien réfléchir avant de tweeter car les gazouillis sont généralement publics. Éviter de parler de sa vie privée, de ses opinions religieuses ou politiques…
- Les gazouillis retweetés par d'autres personnes sont impossibles à effacer, même si le gazouillis d'origine ou le compte d'où il a été tweeté est supprimé.
- Vu le caractère public des gazouillis, ne pas autoriser l'identification sur photo par d'autres personnes.
- Désactiver la géolocalisation pour éviter de donner un lieu précis d'où l'on tweete, comme l'adresse exacte de son domicile.

Signaler quelqu'un ou quelque chose sur Twitter



En cas de problème sur Twitter, il y a moyen de signaler ou de bloquer les publications ou une personne aux administrateurs de Twitter.
Si une publication est dérangeante (nudité, harcèlement, incitation à la haine…), on peut faire le signalement à partir de la publication en cliquant sur les trois points figurant en bas du gazouillis : « Bloquer ou signaler ».

c. Instagram[3]

Instagram sert à partager des photos et des vidéos. Par défaut, les photos que l'on publie sur Instagram sont publiques.

Sur le site Web d'Instagram, rien dans les options du profil ne permet de modifier ce réglage de confidentialité. La modification ne peut se faire que depuis l'application mobile.

[3] Inspiré des notes de Bernard Charlebois sur les médias sociaux, réalisées pour Action ontarienne contre la violence faite aux femmes en 2014.

Pour limiter la diffusion des photos au cercle d'amis, aller sur la page de profil. Cliquer sur les trois petits points verticaux dans le coin supérieur droit et ensuite, cliquer sur « Confidentialité de la photo ». Enfin, cocher la case « Les photos sont en accès privé ».

Suggestions pour la sécurité :

- Limiter le partage des photos avec ses amis.
- Vérifier qu'on a les autorisations des personnes qui apparaissent sur la photo avant de la publier.

d. Pinterest

Pinterest permet de partager des centres d'intérêt, des passions… en épinglant des photos ou des sites sur son profil. Ce qui y est partagé est public aux utilisateurs du site.
Pour s'y inscrire, il ne faut pas fournir beaucoup d'informations : une adresse courriel et un mot de passe. Dans l'onglet « Paramètres », il est possible également de désactiver le référencement du profil sur les moteurs de recherche.

Suggestion pour la sécurité :

- Quand un site Internet demande peu d'informations pour s'inscrire, donner le strict minimum nécessaire à l'inscription.

e. Autres médias sociaux

Beaucoup d'autres médias sociaux existent. Il est important de les explorer afin de maîtriser les différents paramètres de sécurité et de confidentialité. Chacun a ses spécificités.

- LinkedIn est un réseau social sur lequel il est possible de créer un profil sous forme de curriculum vitae afin d'établir un réseau professionnel. Il n'est donc pas adéquat d'y publier des éléments relatifs à la vie privée.
- Snapchat permet de partager des vidéos et des photos. Sa particularité est que celles-ci ne sont visibles que par le destinataire et que pour une durée limitée (d'une à dix secondes), après elles se suppriment du serveur. Mais des captures d'écran sont possibles, il faut donc y faire attention.
- Dropbox est une plateforme de partage de fichiers. Le propriétaire du dossier peut partager avec d'autres personnes les fichiers en autorisant l'accès à sa Dropbox. Il est important de se souvenir à qui on a donné accès aux fichiers et de ne pas y mettre des documents trop confidentiels.

3. Internet dans le quotidien

Internet permet de contrôler beaucoup de choses à distance. Notamment, l'alarme de sa maison, le chauffage, l'éclairage, le verrouillage des portes, etc. Cela a ses bons côtés mais en termes de sécurité, il y a des mesures à prendre.

Le contrôle à distance se fait via une application sur une tablette ou un téléphone intelligent, ou via un site Internet qui demandera une identification au moyen d'un mot de passe.

Les appareils contrôlés à distance passent par le réseau Internet sans fil de la maison. Il est important de le sécuriser.

Suggestions pour la sécurité :

- Utiliser un mot de passe original combinant des caractères majuscules, minuscules, numériques et des sigles de ponctuation pour le réseau Internet sans fil de la maison et l'application ou le site Internet qui permet la gestion à distance.
- Changer de mot de passe régulièrement pour le réseau sans fil de la maison et l'application ou le site Internet qui permet la gestion à distance.
- En cas de violence conjugale, changer de mot de passe le plus vite possible pour éviter que l'agresseur utilise le contrôle à distance.

4. La violence via les médias sociaux et le cyberharcèlement

Internet et les médias sociaux peuvent être utilisés pour commettre de la violence. En effet, actuellement, on observe des cas de cyberharcèlement, ce qui consiste à harceler une personne via des nouvelles technologies.
Plus on s'expose sur la Toile, plus il devient facile pour les potentiels harceleurs d'opérer.
L'actualité montre malheureusement régulièrement des cas de harcèlement via les réseaux sociaux.

Un groupe privé sur Facebook renferme des propos dégradants pour les femmes, des commentaires sexistes et misogynes. Les membres du groupe étudient en médecine dentaire à l'Université de Dalhousie, en Nouvelle-Écosse.

On y trouve des questions, telles qu'« avec qui voudriez-vous avoir des relations sexuelles brutales et haineuses (hate fuck)? ».[5]

Le cyberharcèlement est très grave. Ses conséquences peuvent être irréversibles. Il est important de le dénoncer. Via les médias sociaux eux-mêmes, les internautes peuvent signaler les publications qui tomberaient dans le harcèlement (voir pp.17-19 et 24).

[4] http://www.terrafemina.com/societe/international/articles/24687-rehtaeh-parsons-violee-et-harcelee-sur-facebook-elle-se-suicide.html
[5] http://ici.radio-canada.ca/regions/atlantique/2014/12/15/011-propos-sexiste-facebook-universite-dalhousie-nouvelle-ecosse.shtml

Il existe également des ressources sur le Net qui permettent de se renseigner et d'agir contre le cyberharcèlement.

- aidezmoisvp.ca : ce site est axé sur l'exploitation juvénile et le sexting sur Internet. Mais il explore les moyens disponibles pour se protéger sur Internet : comment faire retirer une photo de soi sur la Toile, comment signaler des cas d'intimidation…
- cyberaide.ca : ce site permet de dénoncer des cas d'exploitation sexuelle d'enfants et d'adolescents sur Internet.

En cas de cyberharcèlement, une plainte peut être faite à la police. Et de plus en plus de cas se retrouvent devant les tribuanux.

Suggestions pour la sécurité :

- Compiler les preuves de harcèlement via Internet en faisant des captures d'écran, en conservant les messages…
- Signaler et bloquer la personne harcelante.
- Ne pas transmettre à d'autres personnes des messages, des photos ou publications qui pourraient nuire à l'intégrité de quelqu'un.

5. Autres ressources et liens sur le sujet

www.undroitdefamille.ca : le webinaire « Les médias sociaux, le droit de la famille et la violence faite aux femmes est disponible sur http://www.undroitdefamille.ca/documents/webinaire_ms.pdf

Une courte vidéo sur la cyberintimidation a été réalisée dans le cadre des activités de l'Institut de formation en matière de violence faite aux femmes. Elle est disponible sur le site de l'Institut www.formationviolence.ca sous l'onglet « Multimédia ».

La campagne Traçons-les-limites.ca : la vidéo « Suivre son intuition » accompagnée du guide d'animation aborde le thème de la cyberintimidation. Elle se trouve sur le site www.tracons-les-limites.ca sous l'onglet « Outils ».
Des cartes postales de la campagne abordent aussi les dérives des médias sociaux.

Liens externes :

- L'intimidation, essayons d'y mettre un terme (2013). En ligne : http://www.edu.gov.on.ca/eng/multi/french/BullyingFR.pdf
- Loi modifiant la Loi sur l'éducation en ce qui a trait à l'intimidation et à d'autres questions (2012). En ligne : http://ontla.on.ca/web/bills/bills_detail.do?locale=fr&BillID=2549

6. Suivez-nous…

Sur Facebook :

AOcVF Francofemmes
Traçons les limites
Voisin-es, ami-es et familles

Sur Twitter :

@AOcVFOntario
@TraconsLimites
@VAF_AOcVF
@CampagneFODF

Annexe - Plan de sécurité virtuelle contre des dangers des médias sociaux dans des situations de violence

Ce plan de sécurité a pour objectif de sécuriser et protéger vos informations personnelles mises sur le Web.

En appliquant les points mentionnés ci-dessous, vous augmentez le niveau de sécurité de tous éléments affichés, publiés et partagés sur Internet.

Il ne faut pas oublier que toute information que vous mettez sur un média social peut être, si elle est jugée pertinente, utilisée comme preuve contre vous à la cour de la famille.

Si ce n'est pas encore fait, il est important de :

☐ Modifier tous vos mots de passe, incluant le mot de passe de votre réseau Internet

☐ S'acheter un journal pour rédiger tous commentaires ou pensées que vous voulez exprimer. Ainsi, vous éviterez d'afficher ces messages sur un réseau public

Facebook

☐ Vérifier régulièrement les onglets : Paramètres/sécurité/confidentialité, car Facebook les modifie fréquemment sans avertissement

☐ Si vous ne fermez pas temporairement votre compte Facebook, s'assurer que vous avez restreint l'accès à votre profil. Celui-ci ne doit être disponible qu'aux personnes de confiance

☐ Bloquer votre ex-partenaire et toutes autres personnes qui pourraient être en contact avec lui en allant dans la section « Paramètre » et « Blocage »

☐ Informer votre entourage de ne pas écrire, publier ou partager de l'information vous concernant pour une période déterminée

☐ Interdire à d'autres personnes la possibilité de vous mentionner dans une publication ou d'écrire sur votre mur

☐ Faire le tri de toutes les photos qui pourraient être interprétées (incluant des photos avec des substances illicites, commentaires inappropriés ou révélateurs, etc.)

☐ Ne pas mettre des photos pouvant donner des indices de l'endroit où vous êtes (par exemple, des photos prises dans la cuisine de l'amie qui vous héberge)

☐ Vérifier régulièrement les commentaires et messages qui pourraient être publiés sur votre page Facebook. Si vous craignez que certains commentaires puissent être interprétés négativement, effacer ces messages

☐ Limiter les informations personnelles sur votre profil (ne pas mentionner l'âge, l'emploi, les intérêts personnels, etc.)

☐ Enlever le système de géolocalisation pouvant indiquer approximativement votre lieu (par exemple, si vous allez au cinéma avec une personne, s’assurer que l'on ne vous inclut pas dans la géolocalisation)

Lexique

En français	En anglais	Définition
blogue	blog	Site Internet animé par un ou plusieurs auteurs qui s'expriment régulièrement sous la forme de billets, d'articles, de chroniques, pouvant faire l'objet de commentaires des visiteurs du site[6]
clavardage	chat	activité permettant à l'internaute d'avoir une conversation écrite, interactive et en temps réel avec d'autres internautes, par clavier interposé[7]
suivre	follow	terme utilisé sur plusieurs réseaux sociaux pour désigner le fait de suivre les activités publiées par une autre personne sur ce réseau
abonnée ou abonné	follower	terme utilisé sur plusieurs réseaux sociaux pour désigner la personne qui suit les activités d'une autre personne sur ce réseau
géopositionnement	GPS	système de localisation qui permet, à un moment précis, de déterminer la position d'un engin ou d'un objet qui se déplace, en se servant de signaux émis par des satellites[8]
mot-clic ou mot-dièse	hashtag	utilisé avec le sigle dièse #, ces mots-clés marquent du contenu sur Internet pour faciliter des recherches autour d'un même sujet
égoportrait ou autophoto	selfie	photo de soi réalisée avec un appareil numérique ou un téléphone intelligent

[6] Marie-Éva De Villers. 2012. Multi dictionnaire de la langue française. 5ème édition. Montréal : Québec Amérique
[7] Marie-Éva De Villers. 2012. Multi dictionnaire de la langue française. 5ème édition. Montréal : Québec Amérique
[8] Marie-Éva De Villers. 2012. Multi dictionnaire de la langue française. 5ème édition. Montréal : Québec Amérique

compteur intelligent	smart meter	compteur énergétique capable de suivre la consommation électrique d'un bâtiment et qui transmet les informations recueillies par Internet[9]
instantané	snap	
gazouillis	tweet	court message rédigé et publié sur le réseau social Twitter, il comporte un maximum de 140 caractères

[9] http://www.futura-sciences.com/magazines/environnement/infos/dico/d/developpement-durable-compteur-intelligent-6952