



Guide d'hygiène informatique

**Politiciens
et partis politiques**

facebook

Initiative canadienne pour l'intégrité électorale

Conception de ccm.design

Image de couverture de Songquan Deng

facebook

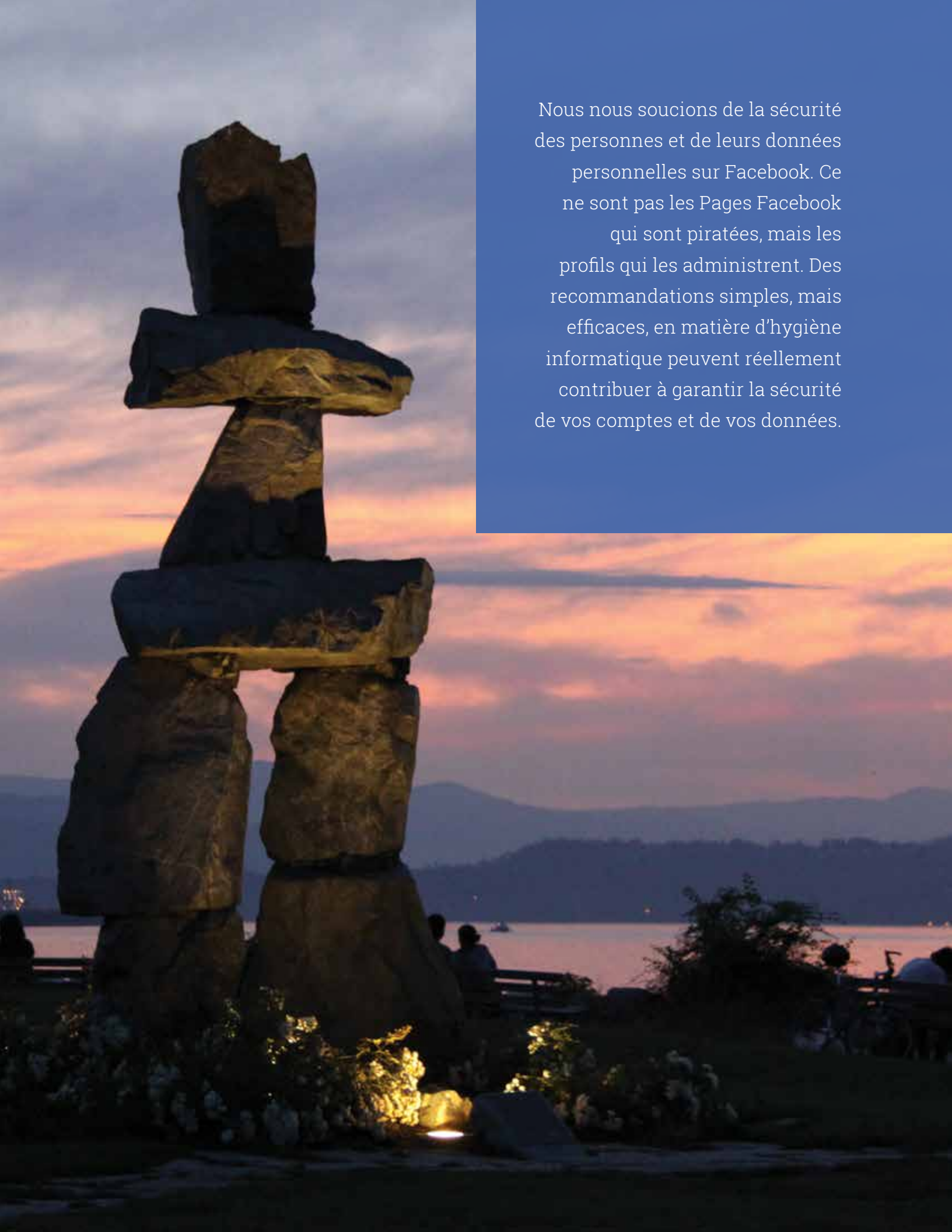


Aider à préserver l'intégrité du processus électoral au Canada

En réponse à une demande émanant de la Ministre des Institutions démocratiques, le Centre de la sécurité des télécommunications (CST) a publié en juin 2017 son rapport intitulé *Cybermenaces contre le processus démocratique du Canada*, fournissant une évaluation rigoureuse des cybermenaces pour différents aspects du processus démocratique. Facebook prend les cybermenaces très au sérieux, et s'engage à faire ce qu'il faut pour protéger et préserver l'intégrité du processus électoral au Canada.

Ce **Guide d'hygiène informatique** fournit des pratiques d'excellence pour les politiciens et les partis politiques afin de garantir la sécurité de leurs Pages et de leurs comptes Facebook. Nous mettons également à la disposition des politiciens et des partis politiques du Canada une **adresse courriel spéciale en cas de crise liée à des cybermenaces** pour les Pages et les comptes Facebook piratés. Ces efforts font partie de l'initiative canadienne globale de Facebook pour garantir l'intégrité électorale.

Photo de Matt Thomason sur Unsplash



Nous nous soucions de la sécurité des personnes et de leurs données personnelles sur Facebook. Ce ne sont pas les Pages Facebook qui sont piratées, mais les profils qui les administrent. Des recommandations simples, mais efficaces, en matière d'hygiène informatique peuvent réellement contribuer à garantir la sécurité de vos comptes et de vos données.

Le rôle préventif majeur des administrateurs de Page

Le guide suivant fournit des conseils utiles pour protéger les Pages et les comptes Facebook des partis politiques, des politiciens, des personnalités officielles et des équipes chargées de gérer leurs comptes.

Les politiciens et les partis politiques peuvent interagir avec des citoyens et des électeurs sur Facebook en créant une Page Facebook. Toute personne ayant un compte Facebook peut créer une Page ou participer à sa gestion, tant qu'elle possède un rôle sur la Page. Les personnes qui aiment une Page peuvent suivre l'actualité de cette Page, en recevant par exemple des publications, des photos ou des vidéos dans leur fil de nouvelles.

Les Pages qui appartiennent à des personnalités et des institutions politiques sont souvent administrées par plusieurs personnes, et donc, par plusieurs comptes Facebook. C'est la raison pour laquelle toutes les personnes concernées doivent être conscientes de l'importance de préserver la sécurité de leurs comptes personnels. Toutes les options de sécurité et de confidentialité doivent être activées pour chaque administrateur d'un compte politique.

Par Christina Chan

Protéger les comptes des administrateurs de Page

Protégez votre mot de passe et votre compte



N'utilisez pas votre mot de passe Facebook ailleurs en ligne et ne le partagez jamais avec quiconque. Vous devez être la seule personne à le connaître. Évitez d'utiliser des renseignements permettant de vous identifier qui peuvent être facilement découverts, tels que votre nom, numéro de téléphone, date de naissance, adresse courriel, etc. **Votre mot de passe doit être difficile à deviner.**

Utilisez des alertes de connexion pour être informé si quelqu'un se connecte à votre compte depuis un nouvel ou un autre appareil.

Utilisez des approbations de connexion comme fonctionnalité de sécurité supplémentaire dans le cadre de l'authentification à deux facteurs.

Déconnexion de votre compte

La section Vos Connexions de vos paramètres de sécurité et de connexion affiche une liste d'ordinateurs, de téléphones et de tablettes qui ont récemment été utilisés pour vous connecter à votre compte.

Pour vous déconnecter de Facebook sur un autre ordinateur, téléphone ou tablette, accédez à vos Paramètres, puis cliquez sur Sécurité et paramètres de connexion. Dans la section vos connexions, recherchez la session que vous voulez fermer et cliquez sur Déconnexion.

Vous trouverez les alertes de connexion dans la section Sécurité, sous Paramètres.

Lorsque vous activez les alertes de connexion, nous vous avisons par courriel ou au moyen d'une alerte chaque fois qu'une personne se connecte à votre compte depuis un nouvel endroit.

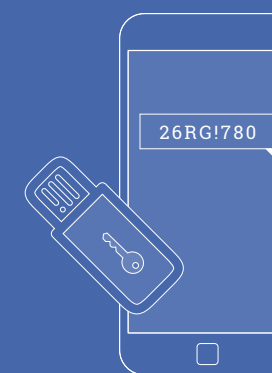
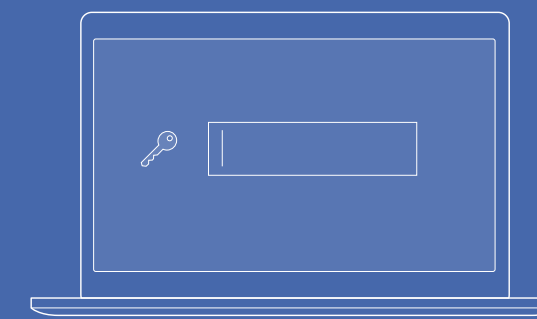
Authentification à deux facteurs

DE QUOI S'AGIT-IL?

L'authentification à deux facteurs est une fonctionnalité de sécurité qui permet de protéger votre compte Facebook en plus de votre mot de passe. Si vous configurez une authentification à deux facteurs, il vous sera demandé de saisir un code de sécurité spécial ou de confirmer votre tentative de connexion chaque fois qu'une personne essaie d'accéder à Facebook depuis un ordinateur ou un appareil mobile non reconnu. Vous pouvez également recevoir des alertes lorsque quelqu'un essaie de se connecter depuis un ordinateur que nous ne reconnaissons pas.

Pour activer ou gérer l'authentification à deux facteurs:

- 1 Accédez à vos paramètres de sécurité et de connexion en cliquant en haut à droite de Facebook sur **Paramètres > Sécurité et paramètres de connexion.**
- 2 Faites défiler l'écran vers le bas jusqu'à **Utiliser l'authentification à deux facteurs** et cliquez sur **Modifier.**
- 3 Choisissez la méthode d'authentification que vous souhaitez ajouter et suivez les instructions à l'écran.
- 4 Cliquez sur **Activer** une fois que vous avez sélectionné et activé une méthode d'authentification.



FONCTIONNEMENT

Il existe différents **moyens d'accéder à votre code de sécurité spécial** :

- 1 Chaque fois que vous en avez besoin, nous vous envoyons un code de connexion par texto.
- 2 Vous pouvez demander jusqu'à dix codes que vous pourrez imprimer, noter ou enregistrer afin de pouvoir en disposer lorsque nécessaire.
- 3 Vous pouvez utiliser le Générateur de code si l'application Facebook est installée sur votre téléphone intelligent ou votre tablette.
- 4 Vous pouvez utiliser une **clé de sécurité Universal 2nd Factor.**

CYBERMENACE

TECHNIQUES À SURVEILLER

Vous devez vous familiariser avec les approches standard généralement utilisées par ceux qui ciblent des représentants élus, des candidats et les personnes associées. Vous pouvez protéger votre compte Facebook en vous assurant que votre compte de messagerie et votre site web sont sécurisés. Voici des stratégies fréquemment utilisées et des renseignements pour minimiser le risque de piratage de comptes.

Si votre compte est piraté, veuillez communiquer par l'intermédiaire de notre adresse courriel dédiée aux crises liées à des cybermenaces au Canada.



Harponnage

Dans la technique du harponnage, les mauvais acteurs envoient des courriels très personnalisés à des individus pris pour cible. Ces courriels sont faits pour ressembler à une correspondance légitime, mais contiennent souvent des liens ou des documents malveillants. Les exemples de harponnage incluent notamment les courriels ou les messages indiquant que le mot de passe de votre compte de messagerie doit être réinitialisé. Le courriel contient un lien raccourci qui dirige vers une fausse page de connexion par courriel. Si vous saisissez vos renseignements sur cette page, le pirate peut les récupérer et accéder à votre compte.

Il est important de comprendre que vos comptes de messagerie personnelle, de médias sociaux et autres sont tout aussi attrayants que les comptes que vous utilisez à des fins professionnelles, gouvernementales et officielles. Protégez vos comptes personnels avec la même vigilance dont vous faites preuve pour les comptes que vous utilisez pour des fonctions officielles.

Recommandation : si vous recevez un courriel ou un message inattendu vous demandant de réinitialiser un mot de passe, ne cliquez pas sur les liens contenus dans le message. En revanche, consultez le site web officiel de l'expéditeur pour vérifier la légitimité de la demande.

Par Yeshi Kangrang sur Unsplash

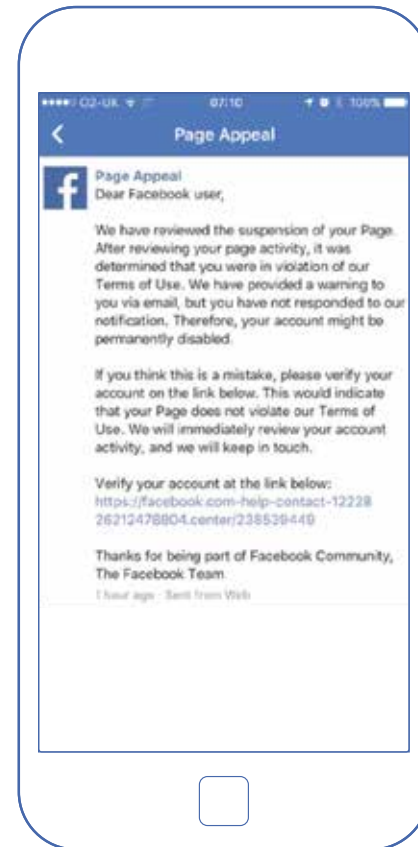
Hameçonnage imitant une Page au nom de Facebook

Il arrive parfois que des campagnes de hameçonnage tentent de convaincre des utilisateurs cibles que leur Page ou leur compte Facebook a été suspendu, et le message semble avoir été envoyé directement par Facebook. Ces campagnes sont conçues pour recueillir vos renseignements confidentiels grâce à un lien vers un domaine qui collecte les identifiants. En ayant accès à vos identifiants de connexion, les pirates pourront se connecter à votre compte et apporter des modifications à vos paramètres qui, à terme, vous empêcheront totalement d'utiliser le compte.

Les attaques de hameçonnage qui imitent une Page au nom de Facebook utilisent illégalement la marque Facebook pour envoyer des messages, généralement par Messenger, ce qui accroît l'impression que l'alerte est réelle et personnalisée.

Un clic sur le lien contenu dans le message compromet le compte et bloque les utilisateurs en dehors de leurs comptes. Une remontée de l'incident à l'équipe de Sécurité Facebook est nécessaire pour résoudre le problème. Les pirates qui utilisent cette méthode de hameçonnage ont développé des moyens d'empêcher la détection de leur activité tout en conservant l'accès à la Page ou au compte Facebook ciblé. Ces campagnes sont motivées par l'appât du gain et ont tendance à cibler des Pages Facebook influentes avec un nombre important d'abonnés, ce qui fait des décideurs politiques une cible attractive.

Recommandation : si vous pensez avoir été la cible d'une campagne de hameçonnage imitant la marque Facebook, veuillez écrire à l'adresse courriel dédiée aux crises liées à des cybermenaces ou communiquez avec le siège de votre parti, et l'équipe Sécurité Facebook vous aidera à résoudre le problème.



Ciblage des équipes professionnelles

Les menaces de sécurité en ligne ne s'étendent pas seulement à vous, mais également à vos collègues et à votre personnel. Une technique courante consiste à utiliser la même approche avec tout le personnel de la victime choisie afin de rassembler le maximum de données pertinentes.

Recommandation : partagez les pratiques d'excellence en matière de sécurité avec votre personnel et vos collègues. Une formation interne sur la sensibilisation à la sécurité dans votre organisation devrait accentuer la valeur de vos données et la probabilité que des acteurs malveillants dédiés essaient d'y accéder.



Piratage de site web

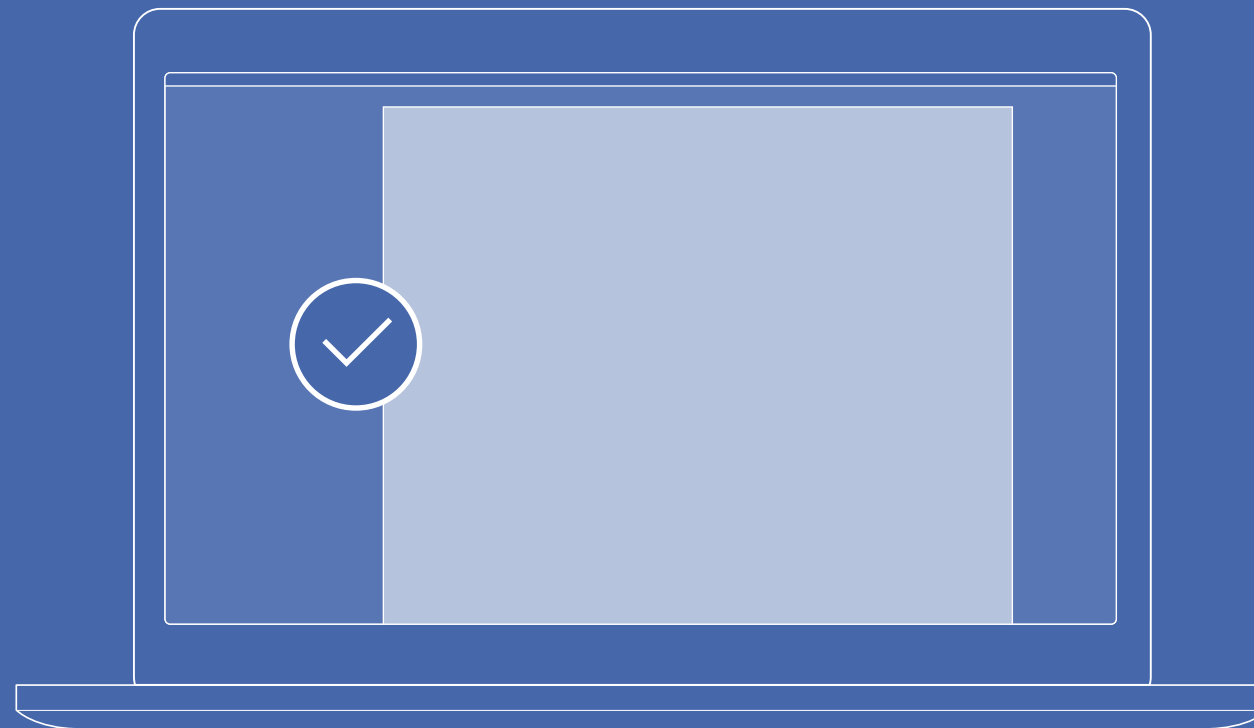
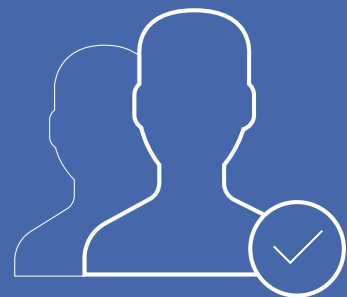
Une autre approche utilisée par les mauvais acteurs est le « piratage web stratégique », par lequel ils infectent certains sites web que leurs cibles sont susceptibles de consulter. L'accès à l'un de ces sites conduit au téléchargement automatique d'un code malveillant, souvent dans le navigateur de la cible. Ce code malveillant est ensuite utilisé pour mener d'autres attaques, comme la copie et le partage de données que la victime a consultées ou parcourues. Récemment, ce type d'activité s'est concentré sur les sites web du Ministère des Affaires étrangères et de l'ambassade, qui sont susceptibles d'être consultés par des diplomates, des politiciens et leurs équipes professionnelles.

Recommandation : utilisez uniquement des navigateurs web s'ils ont des dispositifs de sécurité intégrés, comme Google Chrome, et corrigez et mettez à jour régulièrement les navigateurs web et les autres logiciels que vous utilisez.



Véritable identité des administrateurs de Page

Facebook repose sur le principe de véritable identité. Lorsque les utilisateurs donnent leur opinion et agissent en indiquant leur véritable identité et en mettant en jeu leur réputation, notre communauté est plus responsable. Par conséquent, si nous découvrons que certaines personnes n'utilisent pas leur véritable identité, nous désactivons leur compte. Lorsque des administrateurs de Page n'utilisent pas leur véritable identité, ils prennent le risque de voir leur compte désactivé et de perdre l'accès à leur Page.



Pages vérifiées

Les Pages et les profils peuvent être vérifiés par Facebook pour informer les gens qu'ils sont authentiques. Un badge bleu sur une Page ou un profil indique que Facebook a confirmé l'authenticité d'une Page ou d'un profil pour une personnalité publique ou un parti politique.

Pour demander un badge de vérification bleu, votre Page ou votre profil doit respecter les conditions de service de Facebook et disposer des éléments suivants :

- ① Une photo de couverture
- ② Une photo de profil
- ③ Un nom qui respecte les règles de Facebook
- ④ Du contenu publié sur le compte
- ⑤ L'option « S'abonner » activée (pour les profils uniquement)

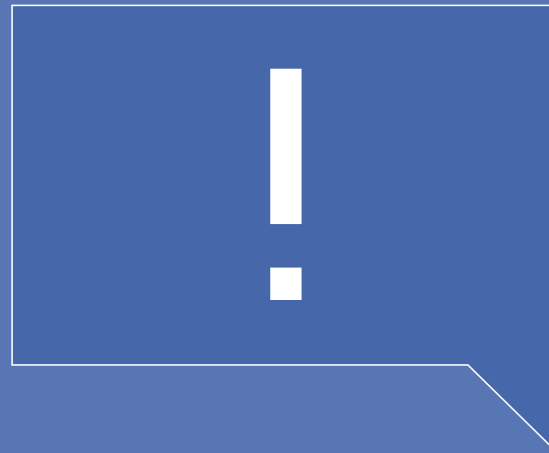
L'admissibilité au badge de vérification bleu repose sur différents facteurs, tels que l'exhaustivité du compte, le respect de la politique et l'intérêt public.

Vous pouvez envoyer une demande en remplissant le **formulaire de demande de badge de vérification bleu**. Pour valider votre demande, nous aurons besoin d'une copie de votre pièce d'identité officielle avec photo (par ex., votre passeport, permis de conduire ou carte d'identité nationale). Nous vous encourageons à fournir des renseignements supplémentaires pour nous aider à examiner votre demande plus efficacement. Veuillez expliquer en quelques phrases pourquoi le compte devrait recevoir le badge de vérification bleu et inclure des URL pertinentes qui illustrent l'intérêt public du compte.

Le **formulaire de demande de badge de vérification bleu** est disponible dans les pages d'aide Facebook :

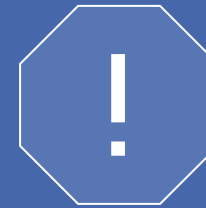
www.facebook.com/help

Réagir aux contenus offensants



Les standards de la communauté Facebook visent à trouver le juste équilibre entre offrir aux personnes un espace pour s'exprimer et promouvoir un environnement accueillant et sûr pour tout le monde.

www.facebook.com/communitystandards



SIGNALER DU CONTENU OFFENSANT

Le meilleur moyen de signaler du contenu offensant ou indésirable sur Facebook est d'avoir recours au lien Signaler à côté de la publication. Nous analysons les signalements et prenons les mesures nécessaires.

Voici quelques exemples montrant la façon de signaler du contenu :

Signaler un commentaire sur Facebook

Cliquez sur X en haut à droite.

Sélectionnez Signaler.

Signaler un message

Ouvrez le message que vous souhaitez signaler. Cliquez sur l'engrenage en haut à droite. Cliquez sur Signaler du contenu indésirable ou un abus... et suivez les instructions.

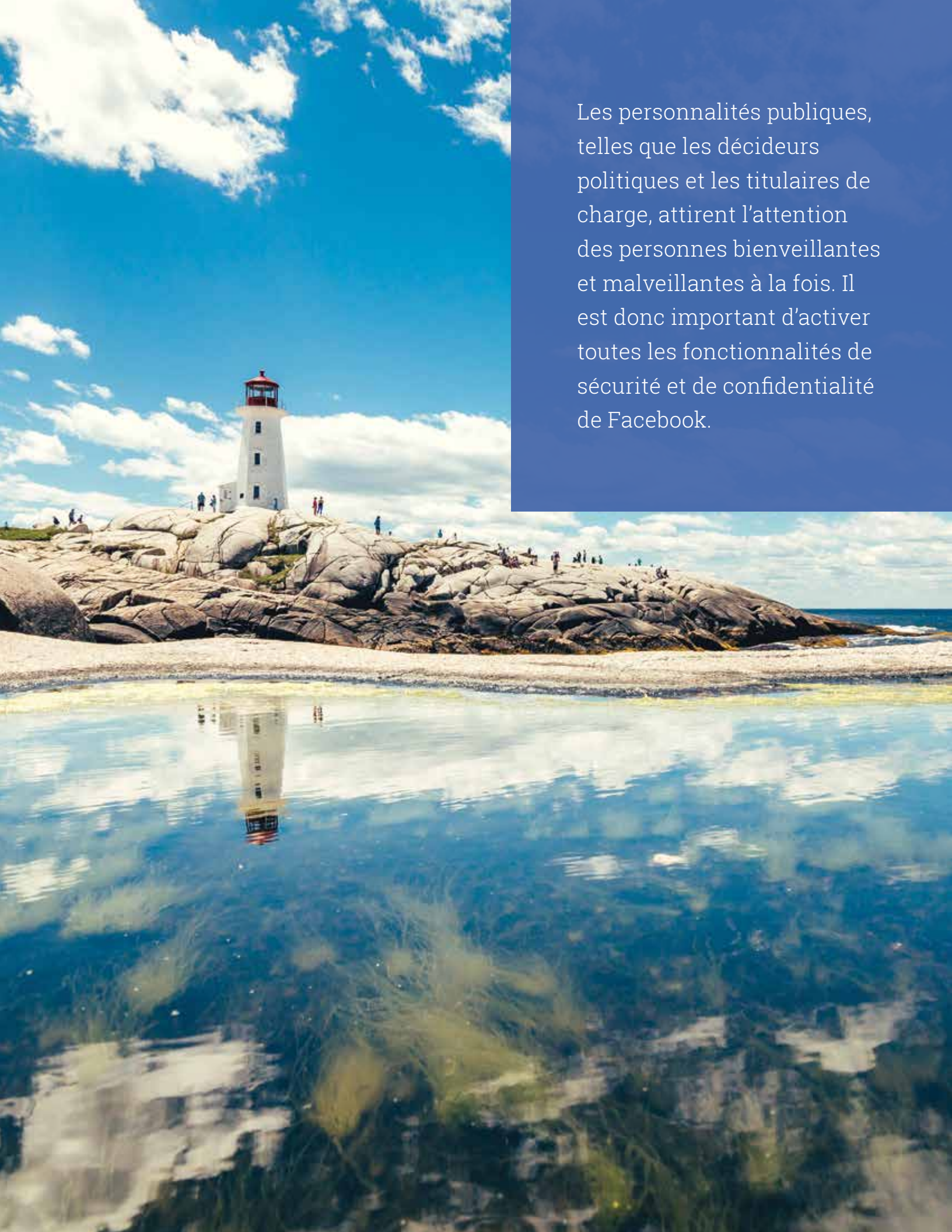
Vous pouvez trouver des instructions pour signaler tous les types de contenu en accédant à www.facebook.com/report.



ENREGISTRER LES CONTENUS OFFENSANTS

Si vous souhaitez signaler du contenu illégal auprès des forces de l'ordre, nous vous recommandons d'effectuer des captures d'écran des activités malveillantes.

Si vous pensez que vous ou une personne que vous connaissez êtes en danger, communiquez avec les services de police locaux.



Les personnalités publiques, telles que les décideurs politiques et les titulaires de charge, attirent l'attention des personnes bienveillantes et malveillantes à la fois. Il est donc important d'activer toutes les fonctionnalités de sécurité et de confidentialité de Facebook.

Principaux conseils de sécurité

Voici quelques conseils de sécurité pour protéger votre compte :

- 1 Protégez votre mot de passe.
- 2 Utilisez nos **fonctionnalités de sécurité supplémentaires**, telles que l'authentification à deux facteurs, les alertes de connexion, les mots de passe à usage unique, les mots de passe d'application et les contacts de confiance.
- 3 Assurez-vous que vos comptes de messagerie sont sécurisés.
- 4 Déconnectez-vous de Facebook lorsque vous utilisez un ordinateur partagé avec d'autres personnes. Si vous oubliez de le faire, vous pouvez vous déconnecter à distance.
- 5 Exécutez un logiciel antivirus sur votre ordinateur.
- 6 Faites attention avant de cliquer sur un élément ou de télécharger quoi que ce soit.

Évitez d'utiliser votre mot de passe Facebook sur d'autres sites.

Ne partagez jamais votre mot de passe. Vous devez être la seule personne à le connaître.

Évitez d'utiliser votre nom ou des noms communs. Votre mot de passe doit être difficile à deviner.

D'autres conseils de sécurité sont disponibles dans les pages d'aide Facebook : www.facebook.com/help

Vérification de la sécurité

Vous pouvez utiliser la vérification de la sécurité Facebook pour examiner et améliorer le niveau de sécurité de votre compte. Avec la vérification de la sécurité:

- 1 Déconnectez-vous de Facebook sur les applications et les navigateurs inactifs.
- 2 Recevez des alertes lorsque quelqu'un tente de se connecter à votre compte depuis un ordinateur ou un appareil mobile non reconnu.
- 3 Apprenez à protéger votre mot de passe.

La vérification de la sécurité est disponible dans les pages d'aide Facebook: www.facebook.com/help



Aider à préserver l'intégrité du processus électoral au Canada

Chez Facebook, nous prenons très au sérieux la sécurité de notre plateforme et des utilisateurs. Nous nous engageons à faire ce qu'il faut pour protéger et préserver l'intégrité du processus électoral au Canada.

Adresse courriel dédiée aux crises liées à des cybermenaces

Nous mettons à la disposition des politiciens et des partis politiques du Canada une **adresse courriel spéciale en cas de crise liée à des cybermenaces** pour les Pages et les comptes piratés. Cela leur permet de récupérer des comptes piratés et de résoudre les cybermenaces le plus vite possible.

Pour plus de renseignements et de liens

www.facebook.com/safety

www.facebook.com/help

www.facebook.com/about/basics

Par Bernard Gagnon

Initiative canadienne pour l'intégrité électorale

facebook

Initiative canadienne pour l'intégrité électorale