Élections canadiennes de 2025

# Aider les utilisateurs à haut risque à demeurer en sécurité en ligne

Notre priorité absolue consiste à aider les gens à rester en sécurité en ligne,et nous reconnaissons que c'est particulièrement important lorsqu'il s'agit de nos institutions et de nos processus démocratiques. C'est pourquoi nous concevons nos produits avec des protections intégrées et investissons dans des équipes et des opérations mondiales pour prévenir les abus sur nos plateformes.

Au cours des dernières années, on a constaté une augmentation significative des menaces à la cybersécurité, surtout pour les individus et les groupes qui ont tendance à être plus exposés aux attaques en ligne, tels que les candidats, les journalistes, le personnel de campagne et les personnes travaillant dans la vie publique.

Pour aider toute personne à risque, nous rendons nos protections de sécurité les plus solides facilement accessibles et partageons plus d'informations sur les meilleurs outils et conseils ainsi que sur les meilleures ressources que les gens peuvent utiliser pour se protéger en ligne.

## 1. Google fournit plusieurs outils gratuits axés sur la sécurité des comptes.

La fonctionnalité **Vérification de la sécurité** fournit des recommandations de sécurité personnalisées pour votre compte Google, notamment des options de récupération, une vérification en deux étapes, des verrouillages d'écran, etc.

Le **Gestionnaire de mots de passe** simplifie l'utilisation d'un mot de passe fort et unique pour tous vos comptes en ligne. Lorsque vous l'utilisez, vous pouvez enregistrer des mots de passe dans votre compte Google ou sur votre appareil.

Pour en savoir plus et vous inscrire, veuillez visiter **support.google.com/accounts**.

## 2. Google se concentre également sur les menaces en ligne contre les utilisateurs à haut risque occupant des postes liés aux élections.

Le **programme de protection avancée** est la forme de sécurité de compte la plus renforcée de Google pour les personnes les plus exposées aux attaques ciblées, recommandé pour les gens travaillant aux élections. Il protège contre l'hameçonnage, en exigeant une clé d'accès ou des clés de sécurité lors de la connexion. Il vous protège également des téléchargements nuisibles en bloquant les fichiers qui pourraient être dangereux.

Il protège aussi vos renseignements personnels en autorisant uniquement les applis Google et les applis tierces vérifiées à accéder aux données de votre compte Google, et seulement avec votre permission. De nouvelles protections sont automatiquement ajoutées pour vous défendre contre la vaste gamme de menaces actuelles, et vous pouvez désormais vous inscrire avec l'authentification transparente et sécurisée des clés d'accès. Inscrivez-vous dès aujourd'hui sans frais en visitant **landing.google.com/intl/fr_ca/advancedprotection**.

**Project Shield** atténue le risque d'attaque par déni de service distribué (DDoS), une tactique courante utilisée par les acteurs malveillants pour perturber les services en ligne en les inondant d'un trafic massif, les rendant ainsi inaccessibles aux utilisateurs légitimes. Project Shield agit comme une couche de défense pour bloquer le trafic de ces attaquants et augmenter la stabilité d'un site Web. Project Shield est disponible sans frais pour les sites Web de nouvelles, de droits de la personne, liés aux élections (y compris les candidats politiques), les organismes à but non lucratif dans les domaines des arts et des sciences et pour les gouvernements confrontés à des circonstances exigeantes.

Pour en savoir plus sur la protection de votre site, consultez **projectshield.google**.

## 3. Les clés d'accès: un pas de plus vers un avenir sans mot de passe

Le nombre d'acteurs malveillants en ligne et de cyberattaques parrainées par des États a augmenté de façon spectaculaire. C'est pourquoi nous nous concentrons plus que jamais sur la protection des personnes, des entreprises et des gouvernements. Afin de contribuer à bâtir un monde plus sûr pour tous, nous partageons notre expertise, responsabilisons les membres de la société et travaillons continuellement pour faire progresser la cybersécurité de pointe .

### Défi

Depuis plus de 60 ans, on utilise des mots de passe sur les ordinateurs, mais aujourd'hui, ils ne suffisent plus à protéger les données des utilisateurs et des organisations. Les attaques d'hameçonnage continuent de prendre de l'expansion et deviennent de plus en plus sophistiquées en exploitant les faiblesses de sécurité des mots de passe.

### Solution

En partenariat avec la FIDO Alliance, nous avons activé la prise en charge des clés d'accès. Il s'agit d'une alternative plus simple et plus sécuritaire aux mots de passe, apportant une technologie résistante à l'hameçonnage à des milliards de personnes à travers le monde. Grâce aux clés d'accès, vous pouvez ignorer votre mot de passe pour une expérience de connexion plus simple et plus sécurisée, en utilisant votre empreinte digitale, votre reconnaissance faciale ou le verrouillage de l'écran pour vous connecter à votre compte Google. Pour en savoir plus, visitez **safety.google/authentication/passkey/**.

## 4. Une aide pour contrôler votre présence en ligne

Sur Recherche Google, nous proposons un ensemble de politiques et d'outils pour aider les utilisateurs à mieux contrôler la manière dont leurs informations sensibles et personnellement identifiables peuvent être trouvées.

Vous pouvez demander la suppression de certaines informations personnelles identifiables des résultats de Recherche Google. Ces renseignements comprennent l'adresse, le numéro de téléphone et/ou l'adresse courriel, entre autres. Pour en savoir plus, visitez **l'outil de suppression des informations personnelles identifiables** de Google.

Le **Google Civics Training Center** offre des outils et des ressources pour vous aider à établir une présence en ligne, notamment en configurant votre chaîne YouTube et en vous assurant que vos informations s'affichent avec précision dans Recherche.

## 5. Autres considérations de sécurité à garder en tête

### Protégez vos appareils

Si vous perdez votre téléphone ou qu'on vous le vole, vous pouvez accéder à votre compte Google et sélectionner « Localiser votre téléphone » pour protéger vos données en quelques étapes rapides. Que vous ayez un appareil Android ou iOS, vous pouvez localiser et verrouiller votre téléphone à distance afin que personne d'autre ne puisse utiliser votre téléphone ou accéder à vos informations personnelles.

### Naviguez sur le Web en toute sécurité

Soyez prudent lorsque vous utilisez les réseaux Wi-Fi publics ou gratuits, même s'ils nécessitent un mot de passe. Ces réseaux peuvent ne pas être cryptés, donc lorsque vous vous connectez à un réseau public, toute personne à proximité peut être en mesure de surveiller votre activité Internet, comme les sites Web que vous visitez et les informations que vous saisissez sur les sites. Si le Wi-Fi public ou gratuit est votre seule option, le navigateur Chrome vous indiquera dans la barre d'adresse si votre connexion à un site n'est PAS sécurisée.

### Évitez les escroqueries en ligne et les tentatives d'hameçonnage

L'hameçonnage est une tentative visant à vous inciter à révéler des renseignements personnels ou financiers critiques, comme un mot de passe ou des coordonnées bancaires. Cela peut prendre plusieurs formes, comme une fausse page de connexion. Pour éviter d'être victime d'hameçonnage, ne cliquez jamais sur des liens louches; vérifiez l'URL (en passant la souris sur le lien ou en appuyant longuement sur le texte sur un appareil mobile) pour vous assurer que le site Web ou l'appli est légitime; et assurez-vous que l'URL commence par « https ».

Si vous voulez en savoir plus ou avez des questions, veuillez contacter ca-elxn-esc@google.com

Google