ASSURER LA SÉCURITÉ DES ÉVÉNEMENTS EN LIGNE

Alors que nous continuons d'intensifier nos efforts d'organisation numérique visant à mobiliser encore plus de Canadiennes et de Canadiens, les événements et les réunions en ligne sont essentiels pour pouvoir rester en contact et élargir notre mouvement.

Voici quelques conseils importants pour assurer la sécurité de vos vidéoconférences et de vos téléconférences.

✔ PROTÉGEZ VOS COMPTES

Vous devez protéger vos coordonnées d'accès aux services de vidéoconférence et de téléconférence tout autant que celles de vos courriels, de vos pages de médias sociaux, de vos bases de données et de vos autres réseaux.

- Utilisez des mots de passe/phrases de passe robustes et uniques et ne les partagez avec personne.
- Activez l'authentification à deux facteurs pour protéger encore davantage votre compte si votre mot de passe venait à être compromis.

✔ PROTÉGEZ VOS RÉUNIONS

Vous avez sans doute entendu parler du « Zoom-bombing ». Ce type d'infiltration peut arriver lorsqu'une vidéoconférence ou une téléconférence n'est pas adéquatement sécurisée. Faites en sorte que cela ne vous arrive pas!

- Assurez-vous que tous vos événements et toutes vos réunions sont protégés par un code d'accès.
- Ne publiez pas les codes d'accès sur les médias sociaux ou ailleurs. Ne les partagez qu'avec les personnes concernées. Même les événements ouverts peuvent être perturbés par des trouble-fêtes de toutes sortes.
- Évitez d'utiliser des codes de réunion personnels pour vos réunions publiques.
- Lorsque vous le pouvez, utilisez des « salles d'attente » ou des outils similaires pour que les autres participants ne puissent pas prendre la parole avant l'animateur ou que des utilisateurs non invités ne soient pas admis automatiquement.
- Vous pouvez aussi mettre les participants en mode silencieux au moment où ils se joignent à la séance, en particulier lorsqu'il s'agit de grands groupes.

✔ PROTÉGEZ VOTRE ORDINATEUR OU VOTRE APPAREIL MOBILE

Surveillez ce que vous téléchargez.

- Lorsque vous le pouvez, téléchargez la version Web des applications de vidéoconférence et de téléconférence.
- Comme toujours, faites attention aux liens sur lesquels vous cliquez. Des services comme GoToMeeting, Zoom, Google, Webex et bien d'autres ont tous été victimes de tentatives d'usurpation de nom de domaine ou d'imitation de leur application par des acteurs malveillants. Évitez donc les maliciels en vous assurant de télécharger uniquement la bonne application.
- Installez les dernières mises à jour pour que vos appareils et vos applications soient le plus possible protégés.

✔ PROTÉGEZ-VOUS

Suis-je sur écoute?

- Réglez toujours les paramètres de sorte que vous puissiez voir si votre caméra ou votre microphone est en marche et pour vous assurer que votre écran (ou les appels que vous organisez) ne sont pas enregistrés involontairement.
- N'organisez pas de vidéoconférences ou de téléconférences pour les discussions sensibles et ne tenez pas pour acquis que ces communications sont chiffrées du début à la fin.
- D'une certaine façon, les vidéoconférences sont comme si vous invitiez des gens chez vous. Veillez à vous présenter dans un décor neutre afin de protéger votre vie privée (pensez aux photos de famille ou aux espaces de vie que vous ne voulez pas partager avec vos interlocuteurs). Cela implique aussi de vous assurer qu'aucun mot de passe sans fil et aucun renseignement personnel ou professionnel ne sont à la vue des participants.
- Le bouton de mise en sourdine est votre meilleur ami – *le bruit d'une chasse d'eau peut être très malaisant…*

➡ POUR EN SAVOIR PLUS SUR LA FAÇON D'ASSURER VOTRE SÉCURITÉ EN LIGNE PENDANT LA COVID-19 ET EN TOUT TEMPS

Le Centre canadien pour la cybersécurité offre différentes ressources pour assurer votre sécurité en ligne et vous pouvez les consulter ici : cyber.gc.ca/fr/orientation/assurer-sa-securite-en-ligne-pendant-la-pandemie-de-la-covid-19.

Pour de plus amples renseignements, veuillez envoyer un courriel à **it-ti@liberal.ca**.