Parliamentarians: So You Think You've Been Hacked? What to do...

A compromise of your social media or email account has serious implications.

If you think your email or social media accounts have been breached, you should follow the steps below and contact your IT security officer. Depending on the nature of the suspected compromise, your IT security officer could be with the HoC. It could also be your DSO or your political party CIO. If you are not certain whom to call, you can reach out to the Canadian Centre for Cyber Security (Cyber Centre) and we can assist, as appropriate, and help guide you through the next steps.

If you believe your social media or email account has been compromised, you should:

Take Action to Regain Control of the Compromised Account

- Report the compromise to the social media or email provider. Follow on-screen instructions in the 'forgot my account' or 'account recovery' page.
- Change your password or passphrase. Use unique passphrases or complex passwords.
- Check your personal information in your account profile. If any information has been changed, re-enter the correct information, such as recovery email address and phone number, or security questions.
- Report the breach to the local police.

Assess and Contain the Breach

- For social media platforms, delete any posts that aren't yours.
- Assess what information may be at risk from the suspected compromise, e.g. personal, financial or official information.
- Consider advising your bank or others who may need to be aware of exposed information.
- If you used the same password for other accounts, change your password for each of the other accounts to a unique passphrase or complex password.

Make Yourself a Hard Target to Avoid Compromise

- Always use unique passphrases or complex passwords for each account or app. Password managers can help keep track of your passwords.
- Enable two-factor authentication to confirm your identity during login attempts. Consider using a hardware token as an extra security measure.
- Enable account notifications to receive an email when someone logs into your account from an unexpected device.
- Review your privacy settings.
- Create security questions for which the answers are not publicly available information (e.g. college roommate's hometown).
- Be suspicious of unsolicited or unusual emails, direct messages or texts/SMS.
- Do not click through embedded links in emails or other messages unless you are certain the sender is trusted. Consider using your web browser to visit the proposed site.
- Verify which apps and devices are connected to your account.
- Delete unused social media or email accounts.
- Update your apps regularly to ensure updated security patches are in place.
- Don't access your account from free or unprotected public wifi services or business stations.

cyber.gc.ca/parliamentarians

Parlementaires : vous croyez que vos comptes ont été piratés? Voici quoi faire…

La compromission d'un compte de média social ou de courriel entraîne des conséquences graves.

Si vous croyez que votre courriel ou vos comptes dans les médias sociaux ont été compromis, suivez les étapes décrites ci-dessous et communiquez sans tarder avec votre agent de la sécurité des TI. Selon la nature de la compromission, votre agent de la sécurité des TI pourrait se trouver à la Chambre des communes, il pourrait s'agir de votre ASM, ou autre (comme le DPI de votre parti politique). Si vous ne savez pas qui appeler, communiquez avec le Centre canadien pour la cybersécurité qui vous aidera en vous expliquant la démarche à suivre.

Si vous croyez que votre compte dans un média social ou votre compte courriel a été piraté, faites ce qui suit :

Prenez des mesures immédiates pour reprendre le contrôle du compte compromis

- Signalez la compromission au fournisseur de média social ou de courriel.
- Suivez les instructions sur la page de récupération de compte.
- Changez votre mot de passe ou phrase de passe. Optez pour des phrases de passe uniques et des mots de passe complexes.
- Vérifiez l'état de vos renseignements personnels dans le profil de votre compte. Si des informations ont été modifiées, corrigez-les (p. ex. votre adresse et numéro de téléphone de récupération du compte, ou vos questions de sécurité).
- Signalez l'incident à votre service local de police.

Évaluez et confinez la compromission

- En ce qui a trait aux médias sociaux, effacez toutes les publications qui ne sont pas les vôtres.
- Déterminez quelles informations pourraient être mises à risque en raison de la possible compromission (p. ex. informations personnelles, financières, officielles).
- Pensez à informer votre banque ou autres entités qui pourraient avoir besoin d'être mises au courant d'une possible divulgation d'informations.
- Si vous utilisez le même mot de passe pour différents comptes, changez le mot de passe de tous les autres comptes pour des phrases de passe uniques ou des mots de passe complexes.

Devenez une cible difficile à atteindre

- Optez toujours pour des phrases de passe uniques et des mots de passe complexes pour chacun de vos comptes ou applications. Un gestionnaire de mots de passe peut vous aider à faire le suivi de vos mots de passe.
- Activez la fonction d'authentification à deux facteurs pour confirmer votre identité lors de l'ouverture de session. Considérez l'utilisation de jetons matériels comme mesure de sécurité supplémentaire.
- Activez la fonction de notification d'accès de sorte à recevoir un courriel lorsque quelqu'un accède à votre compte à partir d'un ordinateur que vous n'utilisez pas habituellement.
- Ajustez vos paramètres de sécurité.
- Rédigez des questions de sécurité dont les réponses ne sont pas disponibles au public (p. ex. lieu de naissance de votre colocataire à l'université).
- Méfiez-vous des courriels, des messages privés et des textos non sollicités ou inhabituels.
- Ne cliquez jamais sur des hyperliens se trouvant dans un courriel ou tout autre message, à moins d'être sûr et certain que l'expéditeur est une personne de confiance. Pensez à utiliser votre navigateur pour visiter la page Web proposée.
- Vérifiez quels dispositifs et applications sont connectés à votre compte.
- Supprimez les comptes de média social ou de courriel que vous n'utilisez plus.
- Faites régulièrement des mises à jour de vos applications pour installer les correctifs de sécurité.
- N'accédez pas à vos comptes à partir de wifi public gratuit ou non protégé ou de postes de travail dans les hôtels.

cyber.gc.ca/parlementaires

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada