Centre de la sécurité des télécommunications | Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

CONSEILS EN MATIÈRE DE CYBERSÉCURITÉ POUR LES INTERVENANTS POLITIQUES

INTRODUCTION

Le Centre canadien pour la cybersécurité a émis des avertissements selon lesquels des auteurs étrangers tenteront probablement de nuire au processus électoral canadien. Dès lors que vous êtes engagé dans des activités politiques – que ce soit à titre de candidat, de membre du personnel de campagne ou de bénévole – vous constituez une cible potentielle. Il est donc capital que vous preniez les mesures de protection qui s'imposent.

En l'occurrence, le Centre pour la cybersécurité est en mesure de vous conseiller judicieusement et de vous permettre d'éviter les menaces qui pèsent sur les médias sociaux. Bien qu'ils représentent une solution non exhaustive, les conseils prodigués dans la présente brochure vous permettront assurément d'accroître le degré de sécurisation de votre campagne. Pour obtenir de plus amples conseils, prière de consulter le site se trouvant à l'adresse suivante : cyber.gc.ca.

Les auteurs de cybermenace pourraient vous cibler :

- en recourant à des mesures courantes de piratage :
  - piratage de comptes de médias sociaux,
  - fuite de secrets, de stratégies de campagne ou de communications internes,
  - chantage ou atteinte à la réputation par la divulgation de secrets personnels;
- en dénigrant votre campagne ou votre plateforme :
  - usurpation d'identité et contrefaçon de comptes,
  - désinformation (fausses nouvelles),
  - trolls, ordinateurs zombies;
- en se servant de vos accès pour mettre la main :
  - sur des informations personnelles,
  - sur des renseignements financiers.

En somme, non seulement vous, mais aussi les ressources de votre campagne constituez des cibles. Assurez la protection de votre campagne contre les compromissions de cybersécurité, et évitez les embarras pouvant découler de telles compromissions.

Canada

ACCROÎTRE LE NIVEAU DE CYBERSÉCURITÉ : QUELQUES ÉTAPES À SUIVRE

Les mesures élémentaires ici présentées devraient être immédiatement appliquées sur tous vos dispositifs :

Utilisez une phrase de passe ou un mot de passe fort et distinct pour chacune des plateformes

Les phrases de passe devraient être uniques et les mots de passe complexes. Chacun des comptes, des sites Web ou des dispositifs devrait avoir une phrase de passe ou un mot de passe fort qui diffère des autres mots de passe. De plus, il importe de ne jamais partager les mots de passe. Par ailleurs, ne modifiez votre mot de passe que lorsque vous avez des raisons valables de le faire, par exemple, si vous soupçonnez qu'une ressource a été compromise.

Ayez recours à l'authentification à deux facteurs

Le recours à un deuxième facteur d'authentification (notamment la réception d'un texto contenant un code vous permettant d'ouvrir une session) constitue un second rempart contre les attaques qui pourraient cibler vos comptes.

Sécurisez votre dispositif mobile au moyen d'un mot de passe ou d'un autre facteur d'identification (reconnaissance faciale, empreintes digitales)

Si vous perdez votre dispositif mobile ou que celui-ci se fait voler, il n'y aura plus que le code de verrouillage ou une autre forme d'identification qui pourra protéger votre information. Au reste, la plupart des dispositifs chiffrent automatiquement l'information qu'ils contiennent dès que vous avez activé le numéro d'identification personnel (NIP) ou le mot de passe, ce qui renforce la protection de vos informations sensibles. d labels on equipment to ensure you are following proper safety procedures

Mettez régulièrement à jour (application des correctifs) votre ordinateur et vos dispositifs mobiles

Ces mises à jour contiennent notamment les correctifs de sécurité. Prière de ne jamais les ignorer.

Sécurisez vos comptes de médias sociaux et de courrier électronique.

Il arrive souvent que les comptes de divers intervenants soient accessibles au gestionnaire de campagne ou au personnel de soutien. Soyez au courant de vos options de délégation des pouvoirs (c.-à-d. la mesure à suivre lorsque plusieurs utilisateurs doivent accéder à un même compte). Utilisez le plus grand nombre de paramètres de sécurité possible pour chacune des plateformes de multimédias.

Soyez à l'affût des messages malveillants

Les messages d'hameçonnage visent généralement plusieurs personnes. En l'occurrence, ils revêtent un aspect légitime pour inciter les destinataires à baisser la garde. Quant aux messages de harponnage, ils sont plutôt personnalisés selon les activités professionnelles, les intérêts ou les caractéristiques personnelles des destinataires. En outre, il faut se méfier des messages dont la teneur ne correspond ni à vos intérêts ni à vos activités ou qui n'ont rien à voir avec les pratiques du destinateur allégué. Il ne faut ni cliquer sur des liens ni ouvrir des fichiers joints, à moins de savoir assurément qui a envoyé le message et pour quels motifs. Si vous ne connaissez pas l'envoyeur, ne cliquez pas.

Fermez adéquatement les sessions que vous avez ouvertes sur des ordinateurs communs

Lorsque vous accédez à l'un de vos comptes de médias sociaux depuis un ordinateur commun, assurez-vous de toujours fermer votre session avant de partir et veillez à ce que vos codes d'utilisateur et vos mots de passe ne soient jamais mémorisés par l'ordinateur en question. N'accédez jamais à vos comptes depuis des dispositifs non fiables, notamment ceux que l'on trouve dans les locaux de bureautique des hôtels, puisque ces dispositifs pourraient très bien être infectés par des logiciels malveillants.

Vérifiez régulièrement vos comptes et leurs paramètres de récupération

Vos comptes de médias sociaux et de courrier électronique disposent de fonctions de récupération et de réinitialisation du mot de passe. Vérifiez-les régulièrement et assurez-vous que les renseignements qu'ils contiennent (coordonnées, question de sécurité) sont exacts et à jour. Réglez vos paramètres de confidentialité au niveau le plus élevé.

Faites des copies de sauvegarde de vos informations

Il importe de faire des copies de sauvegarde des informations relatives à votre campagne, au cas où vous seriez victime d'une attaque par rançongiciel. Il importe également que vous sachiez comment récupérer votre information essentielle au cas où vos dispositifs seraient l'objet de dommages, de perte ou de vol.

Évitez de connecter vos dispositifs aux réseaux sans fil (Wi-Fi)

Les réseaux sans fil gratuits ou non sécurisés peuvent s'avérer pratiques, mais en revanche, ils facilitent la tâche de ceux qui auraient l'intention d'épier vos communications. N'accédez pas à vos comptes de courrier électronique ou de médias sociaux depuis un réseau sans fil gratuit ou non protégé. Si vous deviez absolument vous connecter à l'un de ces réseaux, veillez à n'entrer aucune information sensible tant que votre dispositif est connecté. Cette règle s'applique notamment aux justificatifs d'accès aux sites de votre campagne.

CONTACTEZ-NOUS

1-833-CYBER-88 ou 613-949-7048

contact@cyber.gc.ca

cyber.gc.ca