5 PRACTICAL WAYS TO PROTECT YOUR CAMPAIGN

As a kickstart to your cyber security planning, here are five practical measures you can take right now to make your campaign more secure.

Visit www.cyber.gc.ca for more on any of these steps.

PRACTICE GOOD PASSWORD ETIQUETTE

Use unique passphrases and complex passwords.

Don't share passwords. Don't use the same password for multiple accounts, websites or devices.

Use two-factor authentication (2FA) when available.

SECURE YOUR SOCIAL MEDIA AND EMAIL ACCOUNTS

Use as many security options (settings) as you can for each social media and email platform.

Know your options for delegating authority (what to do when you need multiple users to access one account).

STORE YOUR DATA SECURELY AND KNOW YOUR BACK-UP PROCEDURES

Use only new USB memory sticks purchased by the campaign team. Use them for campaign-related work only. Do not use them on untrusted computers.

Secure data stored in the cloud or online by turning on the available security features. Consider storage solutions with restricted access.

Back up your vital campaign information and know where you have it backed up.

Practice recovering your data at least once. This way you'll know what to do if you become a ransomware victim.

APPLY UPDATES TO YOUR MOBILE DEVICES, COMPUTERS, AND APPLICATIONS

Those updates are crucial to your security: they contain what we call security "patches." Don't ignore them.

Be sure to apply updates to your mobile applications in addition to your device operating systems and get them to automatically update.

Schedule a mandatory training session in which all campaign members update their devices and applications.

BE ON GUARD FOR PHISHING AND SPEAR-PHISHING MESSAGES

Know how to spot phishing and spear-phishing messages.

Be wary of suspicious links – don't click on them.

Use anti-virus or anti-malware software on computers.

5 MOYENS PRATIQUES POUR PROTÉGER VOTRE CAMPAGNE

Voici cinq moyens pratiques à mettre en œuvre dès maintenant pour vous aider à planifier vos mesures de cybersécurité et rendre votre campagne plus sécuritaire.

Vous trouverez de plus amples informations au www.cyber.gc.ca.

ASSUREZ LA SÉCURITÉ DE VOS MOTS DE PASSE

Optez pour des phrases de passe uniques et des mots de passe complexes.

Ne dévoilez jamais vos mots de passe. N'utilisez pas le même mot de passe pour différents comptes, sites Web ou appareils.

Utilisez l'authentification à deux facteurs lorsqu'elle est offerte.

SÉCURISEZ VOS COMPTES DE MÉDIAS SOCIAUX ET DE COURRIEL

Activez tous les paramètres de sécurité offerts dans chacun de vos comptes de médias sociaux et de courriel.

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).

STOCKEZ VOS DONNÉES DE FAÇON SÉCURITAIRE ET SACHEZ COMMENT RÉCUPÉRER LES COPIES DE SAUVEGARDE

Utilisez uniquement des clés USB neuves et fournies par l'équipe de la campagne. Utilisez ces clés uniquement pour le travail lié à la campagne. Ne les branchez jamais à un ordinateur non fiable.

Sécurisez les données stockées dans le nuage ou en ligne en activant toutes les mesures de sécurité disponibles. Faites appel à des solutions de stockage à accès restreint.

Faites des copies de sauvegarde de l'information importante et sachez où elles se trouvent.

Exercez-vous au moins une fois à récupérer vos copies de sauvegarde. Vous saurez ainsi quoi faire si jamais vous êtes victime d'une attaque par rançongiciel.

METTEZ À JOUR VOS APPAREILS MOBILES, VOS ORDINATEURS ET VOS APPLICATIONS

Les mises à jour sont essentielles à la sécurité, car elles contiennent les correctifs de sécurité. Ne les ignorez jamais.

Assurez-vous d'appliquer les mises à jour non seulement aux systèmes d'exploitation, mais aussi aux applications mobiles. Optez pour les mises à jour automatiques.

Conviez tous les membres de l'équipe de la campagne à une séance de formation obligatoire au cours de laquelle ils devront mettre à jour leurs appareils et les applications qu'ils contiennent.

SOYEZ À L'AFFÛT DES MESSAGES D'HAMEÇONNAGE ET DE HARPONNAGE

Sachez reconnaître les messages qui sont des tentatives d'hameçonnage ou de harponnage.

Méfiez-vous des liens suspects, ne cliquez jamais dessus.

Utilisez un logiciel antivirus ou antimaliciel sur vos ordinateurs.

Centre de la sécurité des télécommunications
Communications Security Establishment
Canada