PensezCybersecurite.ca/Defi

RELEVEZ LE DÉFI PENSEZ CYBERSÉCURITÉ

La cybersécurité est plus simple quand on la divise en petits morceaux. Mettez-vous au défi de prendre chaque jour de petites mesures pour rendre vos comptes et vos appareils plus sûrs. Voici une liste de contrôle qui vous aidera à démarrer.

SEMAINE 1

PHRASE DE PASSE ROBUSTE

☐ **APPRENEZ À CRÉER UNE PHRASE DE PASSE ROBUSTE**

Visitez le site PensezCybersécurité.ca pour obtenir des conseils sur la création d'une phrase de passe robuste, en utilisant 4 mots ou plus et 15 caractères ou plus.

☐ **ASSUREZ-VOUS QUE TOUS VOS COMPTES SONT PROTÉGÉS PAR UNE PHRASE DE PASSE ROBUSTE ET UNIQUE.**

Passez en revue chacun de vos comptes (même ceux que vous n'utilisez pas souvent) et remplacez les mots de passe faibles ou répétés par des phrases de passe uniques et plus robustes.

Faire tout ça en une journée n'est peut-être pas possible pour tout le monde. Commencez par une seule phrase de passe et faîtes un grand pas pour **#DevenirCyberSécurisé**. Un défi relevé pour la journée ! Continuez à changer un mot de passe par jour ou par semaine, et vous aurez vite fait le tour !

☐ **UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE**

Conservez vos nouvelles phrases de passe dans un gestionnaire de mots de passe pour ne jamais les oublier. Assurez-vous de sécuriser le gestionnaire avec sa propre phrase de passe robuste !

****

SEMAINE 2

AUTHENTIFICATION MULTIFACTORIELLE

☐ **FAITES UNE LISTE DE VOS COMPTES LES PLUS IMPORTANTS**

Notez tous les comptes qui contiennent des informations personnelles vous concernant, comme votre nom complet, votre adresse ou toute information financière.

☐ **DÉTERMINER LES FACTEURS D'AUTHENTIFICATION QUI FONCTIONNENT POUR VOUS**

En fonction de ce que vous devez sécuriser, différentes options d'**authentification multifactorielle (ou AMF)** peuvent être disponibles, comme l'authentification par empreinte digitale ou par texte.

☐ **ACTIVEZ L'AUTHENTIFICATION MULTIFACTORIELLE**

Passez en revue vos comptes et appareils importants et activez l'authentification multifactorielle dans la mesure du possible. Vous devriez le trouver dans les paramètres de confidentialité.

SEMAINE 3

MISES À JOUR DES SYSTÈMES

☐ **METTEZ À JOUR TOUS VOS APPAREILS**

Oui, **tous**. Lancez une vérification des mises à jour sur tous vos appareils qui sont connectés à Internet, de votre téléphone à votre frigo intelligent.

Faire tout ça en une journée n'est peut-être pas possible pour tout le monde. Commencez par mettre à jour un appareil par jour ou par semaine, pour **#DevenirCyberSécurisé** très vite !

☐ **ACTIVEZ LES MISES À JOUR AUTOMATIQUES**

Vérifiez les paramètres de vos appareils et activez les mises à jour automatiques partout où vous le pouvez. Programmez-les à des moments où vous n'utilisez pas vos appareils, comme pendant la nuit.

☐ **DÉSINSTALLEZ LES APPLICATIONS ET LOGICIELS INUTILISÉS**

Les logiciels que vous n'utilisez pas peuvent être corrompus et vous mettre en danger. Désinstallez les applications et les logiciels que vous n'avez pas utilisés depuis un certain temps.

SEMAINE 4

SÉCURISEZ VOTRE WI-FI

☐ **CHANGEZ LE MOT DE PASSE PAR DÉFAUT DE VOTRE ROUTEUR**

Ne vous contentez pas du mot de passe fourni avec votre routeur. Créez un nouveau mot de passe unique ou une phrase de passe pour sécuriser votre connexion Wi-Fi.

☐ **CRÉEZ UN RÉSEAU D'INVITÉS**

Créez un réseau distinct avec un mot de passe unique que vous pouvez utiliser pour tous les visiteurs ou appareils intelligents qui veulent se connecter à votre Wi-Fi.

☐ **DÉPLACEZ VOTRE ROUTEUR DANS UN ENDROIT SÛR**

Gardez vos périphériques réseau aussi près que possible du centre de votre maison pour empêcher les personnes extérieures de s'y connecter.

☐ **BONUS : INSTALLEZ LE BOUCLIER CANADIEN**

Le **Bouclier canadien** est un coupe-feu de Système de noms de domaines (DNS) gratuit de l'Autorité canadienne pour les enregistrements Internet qui bloque les logiciels malveillants et garde privées vos données en ligne.

✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

VOUS AVEZ COCHÉ TOUTE LA LISTE ?

Obtenez d'autres conseils pour sécuriser vos comptes et vos appareils à

PENSEZCYBERSECURITE.CA

Centre de la sécurité des télécommunications
Communications Security Establishment
Canada

Numéro de catalogue : D96-39/2021F-PDF | ISBN : 978-0-660-39106-9