CYBERSECURITY AWARENESS MONTH

PROTÉGEZ VOTRE ORDINATEUR PERSONNEL

Recommandations du programme de sécurité de l'information de Mauser Packaging Solutions

VERROUILLEZ VOTRE OUVERTURE DE SESSION

Créez une phrase passe longue et unique. Une phrase passe sûre est une phrase qui se compose d'au moins 12 caractères.

SI VOUS DOUTEZ, JETEZ

Les liens dans les courriels, les tweets, les messages textes, les publications, les messages de médias sociaux et les publicités en ligne sont le meilleur moyen pour les cybercriminels d'obtenir vos renseignements sensibles. Méfiez-vous des liens ou des téléchargements qui proviennent d'étrangers ou que vous n'attendiez pas.

GARDEZ VOTRE MACHINE PROPRE

Gardez à jour tous les logiciels sur les appareils connectés sur Internet (notamment les ordinateurs personnels, les téléphones intelligents et les tablettes) pour réduire le risque d'infection par des logiciels de rançon ou des programmes malveillants. Configurez vos appareils de façon que les mises à jour se fassent automatiquement ou qu'ils vous avisent quand une mise à jour est disponible.

FAITES DES SAUVEGARDES

Faites des copies électroniques de votre musique, de vos photos et de vos autres renseignements personnels et stockez-les dans des endroits sûrs. Si vous avez une copie de vos données et que votre appareil fait l'objet d'une attaque par un logiciel de rançon ou d'une autre cybermenace, vous pourrez récupérer vos données de cette copie.

MAÎTRISEZ VOTRE PRÉSENCE EN LIGNE

Dès que vous ouvrez un nouveau compte, téléchargez une nouvelle application ou obtenez un nouvel appareil, configurez immédiatement les paramètres de confidentialité et de sécurité selon votre niveau de confort en matière de partage des renseignements. Vérifiez régulièrement ces paramètres (au moins une fois par année) pour vous assurer qu'ils sont toujours configurés selon vos besoins.

PARTAGEZ AVEC PRUDENCE

Réfléchissez avant de publier en ligne quelque chose sur vous ou sur d'autres personnes. Déterminez ce que la publication révèle, qui peut la consulter et quelle incidence elle peut avoir sur vous et les autres. Envisagez de créer une personne fictive pour vos profils en ligne afin de limiter la quantité de données personnelles que vous partagez.

SOYEZ BIEN AVISÉ(E) AU SUJET DES POINTS D'ACCÈS WIFI

Les réseaux sans fil publics et les points d'accès ne sont pas sécurisés, ce qui signifie que n'importe qui peut voir ce que vous faites sur votre ordinateur portable ou votre téléphone intelligent quand vous y êtes connecté. Limitez ce que vous faites quand vous êtes connecté(e) à un réseau Wi-Fi public, et évitez d'ouvrir des sessions dans vos principaux comptes comme le courriel et les services financiers.

Le programme de sécurité de l'information de Mauser Packaging Solutions gère plusieurs de ces fonctions pour les biens de votre entreprise. Faites votre part et protégez vos biens personnels. #BeCyberSmart