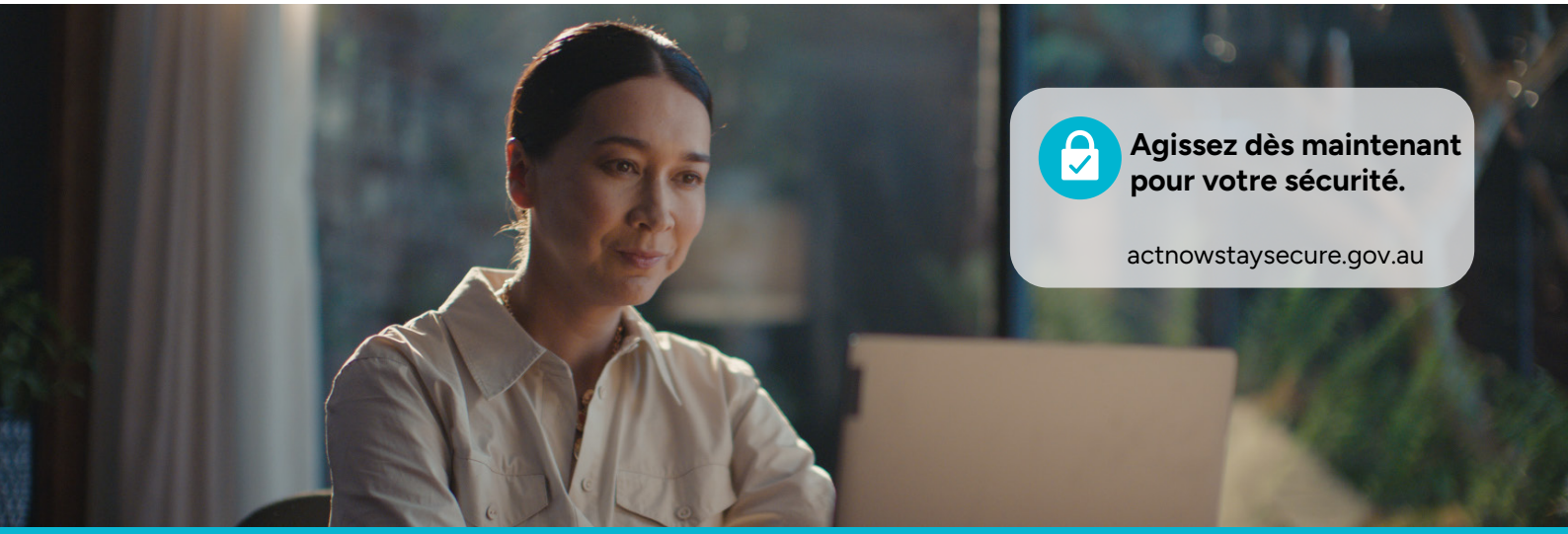
Australian Government

actnowstaysecure.gov.au



Savez-vous quels risques vous prenez en ligne ?

Les technologies progressent à vive allure et nous passons de plus en plus de temps en ligne. En Australie comme ailleurs, personne n'est à l'abri d'une cyberattaque.

La campagne « Agissez dès maintenant pour votre sécurité » a pour but d'informer les Australiens sur les bonnes pratiques à adopter pour se protéger contre la cybermalveillance.

Agissez dès maintenant pour votre sécurité.

Comment assurer sa sécurité numérique ?

Utilisez une seule et unique phrase de passe complexe pour chacun de vos comptes.

L'utilisation d'une phrase de passe unique et complexe pour chacun de vos comptes en ligne est l'un des moyens les plus efficaces de sécuriser votre vie numérique.

Les phrases de passe sont plus sûres que les mots de passe car elles associent des mots pris au hasard et sont plus faciles à mémoriser pour leurs utilisateurs et plus difficiles à deviner pour les cybercriminels.

Pour composer une phrase de passe unique et robuste :

- ✓ Choisissez quatre mots au hasard, voire plus.
- ✓ Utilisez plus de 15 caractères.
- ✓ Utilisez une phrase de passe par compte.
- ✓ N'incluez pas d'informations d'identification (noms de famille, dates de naissance, adresses, etc.).
- ✓ Utilisez des symboles, majuscules ou chiffres si le site Internet ou le service le demande.

N'hésitez pas à utiliser un gestionnaire de mots de passe pour créer et conserver toutes vos phrases de passe.

Installez toutes les mises à jour de logiciels pour protéger vos appareils.

Pensez à mettre à jour les logiciels de tous vos appareils connectés à Internet (téléphones, ordinateurs portables et montres connectées). Cela est essentiel pour sécuriser votre environnement numérique.

Les mises à jour de logiciels corrigent les failles ou les manquements de votre équipement en matière de sécurité. Une installation régulière des mises à jour permet de sécuriser vos appareils et complique la tâche des cybercriminels qui tentent d'y accéder.

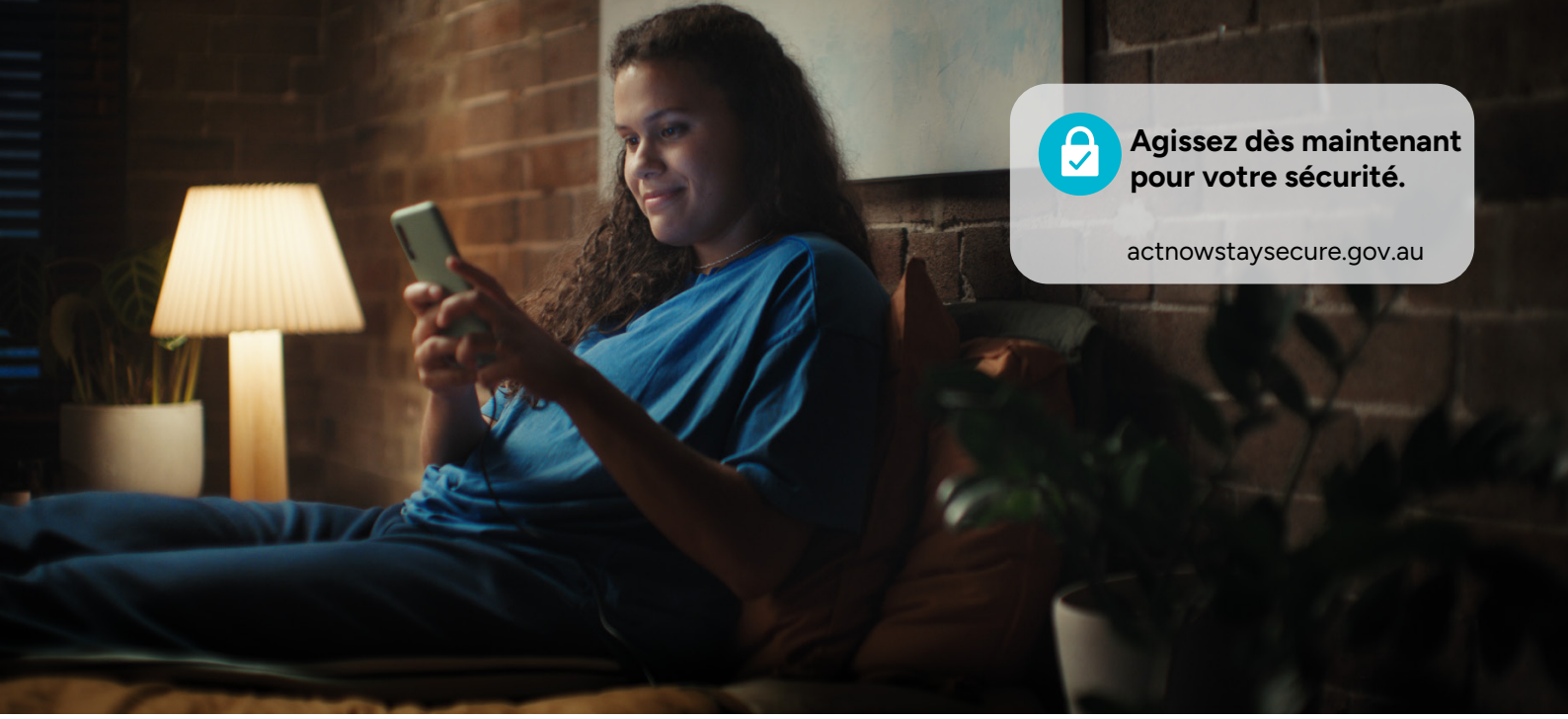
Activez l'option de mise à jour automatique et veillez à procéder aux installations lorsque vous y êtes invité.

Utilisez toujours l'authentification multifacteur.

Activez l'authentification multifacteur si le service le propose pour renforcer la sécurité de tous vos comptes en ligne.

L'authentification multifacteur exige deux, voire plusieurs modes de vérification pour se connecter à un compte. Par exemple, en plus d'un mot ou d'une phrase de passe, vous devez procéder à une seconde vérification, comme la saisie d'un code qui vous est envoyé sur une application d'authentification, par courriel ou par SMS.

L'authentification multifacteur protège vos comptes, même si un cybercriminel parvient à déjouer les autres modes d'authentification (phrase de passe par exemple).



Vous souhaitez renforcer votre sécurité en ligne ?

Vous souhaitez assurer votre sécurité numérique par d'autres moyens ? Voici quelques pratiques que vous pouvez adopter pour vous protéger.

Attention aux réseaux Wi-Fi publics

Lorsque vous êtes connecté à un réseau Wi-Fi public, ne consultez pas d'informations personnelles ou sensibles (réseaux sociaux, messagerie électronique et services de banque en ligne) car la connexion n'est pas sécurisée. Les cybercriminels peuvent accéder aux informations que vous transmettez en ligne.

Vérifiez et mettez à jour régulièrement vos paramètres de confidentialité et de localisation.

Il est important de régulièrement vérifier vos paramètres de confidentialité et de localisation pour être sûr de ne pas publiquement partager de manière accidentelle des informations personnelles ou permettant de vous identifier.

Les paramètres à vérifier sont, entre autres, les paramètres de confidentialité de vos comptes de réseaux sociaux et ceux de géolocalisation de vos applications et appareils.

La sécurité numérique : parlez-en avec votre famille et vos amis

L'information et la sensibilisation restent les meilleurs moyens de vous protéger en ligne et de protéger votre famille et vos amis, surtout si vous partagez des appareils connectés à Internet. Discuter de la cybersécurité avec les utilisateurs de vos réseaux est le meilleur moyen de veiller à la sécurité de tous et de les informer des dernières évolutions en matière de protection.

Attention aux arnaques en ligne

Les escrocs dupent les internautes en leur soutirant de l'argent ou en les incitant à transmettre leurs informations personnelles.

Ne donnez jamais d'argent ou d'informations personnelles à quelqu'un si vous doutez de l'identité de la personne avec qui vous avez affaire. Vérifiez son identité en contactant directement cette personne ou l'organisation à l'aide d'informations que vous aurez vous-même trouvées sur un site Web officiel ou une application.

Signalez toute cyberattaque et tout cyberincident

Il est essentiel de signaler les arnaques et les incidents en ligne pour que le gouvernement puisse connaître les nouveaux moyens qu'utilisent les cybercriminels, alerter la population et vous aider si vous avez été victime d'une cyberattaque.

Consultez le site actnowstaysecure.gov.au pour adopter dès maintenant les bonnes pratiques de protection en ligne.

Agissez dès maintenant pour votre sécurité.

actnowstaysecure.gov.au