Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

COMMENT UTILISER L'INTERNET EN TOUTE SÉCURITÉ

GUIDE À L'INTENTION DES PERSONNES ÂGÉES

cyber.gov.au

Introduction

L'Internet vous permet de garder le contact avec vos amis et votre famille, de vous renseigner sur différents sujets et même de jouer à des jeux.

Tout comme vous avez l'habitude d'attacher votre ceinture de sécurité avant de prendre le volant, vous devriez prendre certaines mesures avant d'utiliser l'Internet pour renforcer votre sécurité.

Le Centre australien de la cybersécurité (Australian Cyber Security Centre – ACSC) veut s'assurer que toutes les personnes sont en sécurité lorsqu'elles surfent en ligne. Le présent document couvre certaines pratiques de cybersécurité de base que vous pouvez appliquer pour vous protéger quand vous accédez à l'Internet.

Le Centre australien de la cybersécurité (Australian Cyber Security Centre – ACSC), qui fait partie de la Direction australienne responsable du renseignement et de la sécurité électronique (Australian Signals Directorate – ASD), propose des conseils, un soutien et des réponses opérationnelles permettant de prévenir, de déceler et de pallier les cybermenaces qui ciblent l'Australie. L'ACSC a pour mission d'aider à faire de l'Australie le pays le plus sûr où se connecter à l'Internet.

Pour des informations, des guides et des conseils complémentaires sur la cybersécurité, veuillez vous rendre sur le site cyber.gov.au

Comment utiliser l'Internet en toute sécurité

La cybersécurité pour les personnes âgées

Conseil 1 : Mettez votre appareil à jour

Mettre à jour vos logiciels, c'est comme faire faire un entretien pour votre voiture. Cela améliore la performance de votre appareil et en renforce la sécurité.

Les cybercriminels trouvent toujours de nouvelles méthodes pour pirater les appareils. Configurer votre appareil de manière à ce qu'il installe automatiquement les mises à jour permet de surmonter toutes les faiblesses dans vos logiciels et de vous prémunir contre les pirates informatiques.

Pour des informations complémentaires, recherchez le terme « Updates » (mises à jour) sur le site cyber.gov.au

LE SAVIEZ-VOUS ?

Les mises à jour peuvent également ajouter de nouvelles fonctions dans votre appareil et le faire fonctionner plus rapidement.

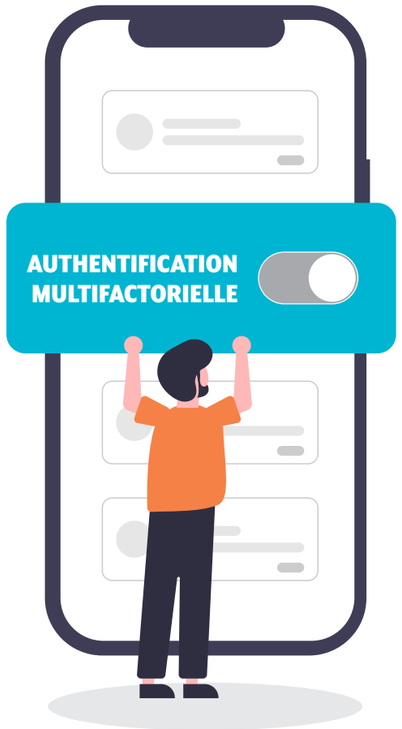
Conseil 2 : Activez l'authentification multifactorielle

Activer l'authentification multifactorielle sur votre compte, c'est comme parer votre maison d'un écran de sécurité. Ce dernier vous protège contre les criminels qui tentent d'entrer par effraction.

Lorsque l'authentification multifactorielle est activée, vous devez fournir plusieurs informations pour accéder à votre compte. Par exemple, vous pouvez devoir saisir votre mot de passe et un code envoyé par SMS pour vous connecter à votre profil sur les réseaux sociaux.

Grâce aux différentes couches de sécurité, il est plus difficile pour les cybercriminels de pirater votre système. Ils peuvent réussir à déjouer une partie du système de protection, comme votre mot de passe, mais ils doivent encore obtenir d'autres pièces du puzzle pour accéder à votre compte.

Pour des informations complémentaires, recherchez l'expression « Multi-factor authentication » (authentification multifactorielle) ou « MFA » (AMF) sur le site cyber.gov.au



SOUVENEZ-VOUS :

Si vous avez besoin d'une assistance pour activer l'authentification multifactorielle, demandez à un ami ou à un membre de votre famille de vous aider.

Conseil 3 : Sauvegardez votre appareil

La réalisation d'une « sauvegarde » consiste à effectuer une copie de vos fichiers importants et à la placer en lieu sûr. C'est comme si vous photocopiez des photos auxquelles vous tenez particulièrement pour les protéger en cas de perte des originaux.

Quand vous sauvegardez votre ordinateur, votre téléphone ou votre tablette, des copies de vos fichiers sont enregistrées en ligne ou sur un autre appareil. Avec une sauvegarde de vos fichiers importants et de vos photos fétiches, vous aurez l'esprit tranquille.

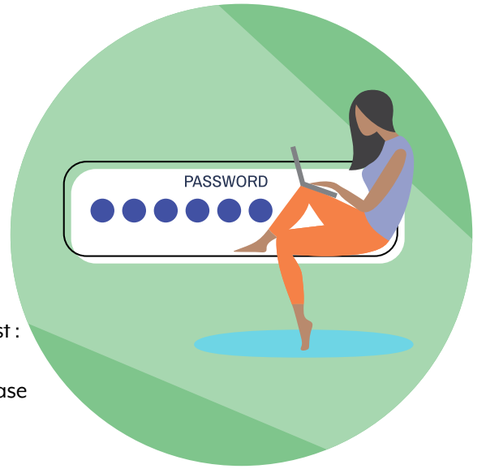
En cas de problème avec votre appareil ou si vous faites l'objet d'une attaque de cybercriminels, vous pouvez facilement récupérer vos fichiers depuis vos sauvegardes.

Pour des informations complémentaires, recherchez le terme « Backups » (sauvegardes) sur le site cyber.gov.au

LE SAVIEZ-VOUS ?

Grâce à des sauvegardes régulières de votre appareil, vous aurez toujours accès à vos fichiers les plus à jour.

Conseil 4 : Utilisez une phrase de passe

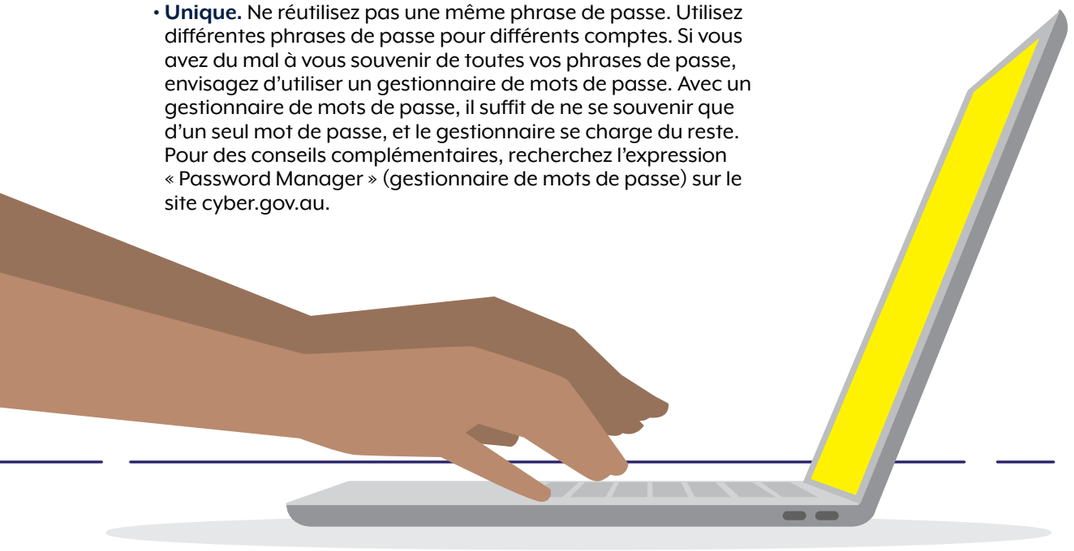


Un mot de passe sert de cadenas pour votre compte, mais une phrase de passe possède son propre système de sécurité !
Une phrase de passe offre une alternative plus robuste et plus sécurisée qu'un mot de passe.

Si vous ne pouvez pas activer la fonction d'AMF, utilisez une phrase de passe pour sécuriser votre compte. Une phrase de passe est similaire à un mot de passe, mais elle comprend au moins quatre mots aléatoires. De ce fait, elle est difficile à deviner pour les cybercriminels, mais vous pouvez vous en souvenir facilement.

Quand vous créez une phrase de passe, assurez-vous qu'elle est :

- **Longue.** Plus elle est longue, mieux c'est. Efforcez-vous d'en créer une qui contient au moins 14 caractères. Pour une phrase de passe efficace, utilisez au moins quatre mots aléatoires dont vous vous souviendrez.
  Par exemple, « violet canard patate bateau ».
- **Imprévisible.** Moins votre phrase de passe est prévisible, mieux c'est. Des phrases complètes peuvent faire d'excellentes phrases de passe, mais elles sont plus simples à deviner. Avec un mélange d'au moins quatre mots aléatoires, la phrase de passe sera plus robuste.
- **Unique.** Ne réutilisez pas une même phrase de passe. Utilisez différentes phrases de passe pour différents comptes. Si vous avez du mal à vous souvenir de toutes vos phrases de passe, envisagez d'utiliser un gestionnaire de mots de passe. Avec un gestionnaire de mots de passe, il suffit de ne se souvenir que d'un seul mot de passe, et le gestionnaire se charge du reste. Pour des conseils complémentaires, recherchez l'expression « Password Manager » (gestionnaire de mots de passe) sur le site cyber.gov.au.



Pour en savoir plus sur la création de phrases de passe sécurisées, recherchez l'expression « Passphrases » (phrases de passe) sur le site cyber.gov.au

Comment utiliser l'Internet en toute sécurité

Conseil 5 : Reconnaissez les arnaques et signalez-les

LE SAVIEZ-VOUS ?

Les cybercriminels sont astucieux et pourraient utiliser un nom et une adresse électronique qui vous sont familiers.
Méfiez-vous si :
- **on vous demande de payer une facture de toute urgence.**
- **on vous demande de changer vos détails de connexion ou votre mot de passe.**
- **on vous demande de cliquer sur un lien ou d'ouvrir une pièce jointe.**

Plus tôt vous signalez une arnaque, plus vite nous pourrons agir.

Si vous pensez que quelqu'un tente d'utiliser l'Internet pour vous arnaquer, il vaut mieux faire preuve de proactivité et de prudence que de risquer de se faire léser.

Si c'est trop beau pour être vrai, c'est certainement le cas. Bien qu'un message puisse vous annoncer que vous avez remporté un prix ou que votre ordinateur contient un virus, ce message n'est pas unique à vous.

Il pourrait provenir d'un arnaqueur qui souhaite profiter de vous.

Souvenez-vous que les arnaqueurs prétendent souvent être une personne ou une organisation à laquelle vous faites confiance. Méfiez-vous si vous recevez un message qui semble provenir d'une personne en qui vous avez confiance, mais qui utilise un nouveau numéro de téléphone, une nouvelle adresse électronique ou un nouveau profil sur les médias sociaux. Avant de répondre, vérifiez que la personne ou l'organisation qui vous envoie un message est réellement celle qu'elle dit être en la contactant par un canal fiable. Par exemple, si vous recevez un SMS semblant provenir de l'un de vos enfants, mais qu'il a été envoyé depuis un nouveau numéro, n'y répondez pas. Commencez par envoyer un message à votre enfant sur les réseaux sociaux pour vérifier s'il a réellement changé de numéro de téléphone.

Conclusion

Maintenant que vous possédez les connaissances requises pour utiliser l’Internet de manière plus sécurisée, vous pouvez surfer en toute confiance et continuer à profiter du temps que vous passez en ligne.

Toutefois, souvenez-vous que les cybercriminels trouvent toujours de nouvelles façons de cibler les gens.

Ça ne peut pas faire de mal de renforcer de temps en temps vos connaissances techniques en termes de cybersécurité et d’apprendre de nouvelles méthodes pour assurer votre protection.

Conseils complémentaires

Vous souhaitez connaître plus de moyens de préserver votre sécurité en ligne? Consultez les conseils suivants.

Réfléchissez à ce que vous publiez.

Réfléchissez attentivement aux informations que vous partagez en ligne et aux personnes qui les voient. N’acceptez des demandes de contact que de la part de personnes que vous connaissez personnellement.

Recevez nos alertes sur les nouvelles menaces.

Abonnez-vous à notre service d’alerte gratuit. Cela vous permettra d’être informé·e chaque fois que nous découvrons une nouvelle cybermenace.

Ce service vous donnera également des conseils sur ce qu’il faut faire en cas d’attaque.

Parlez de la cybersécurité avec votre famille et vos amis.

Maintenant que vous avez acquis des compétences en cybersécurité, partagez ce que vous avez appris avec votre famille et vos amis.

Vos connaissances pourraient un jour les aider à s’extirper d’une situation difficile !

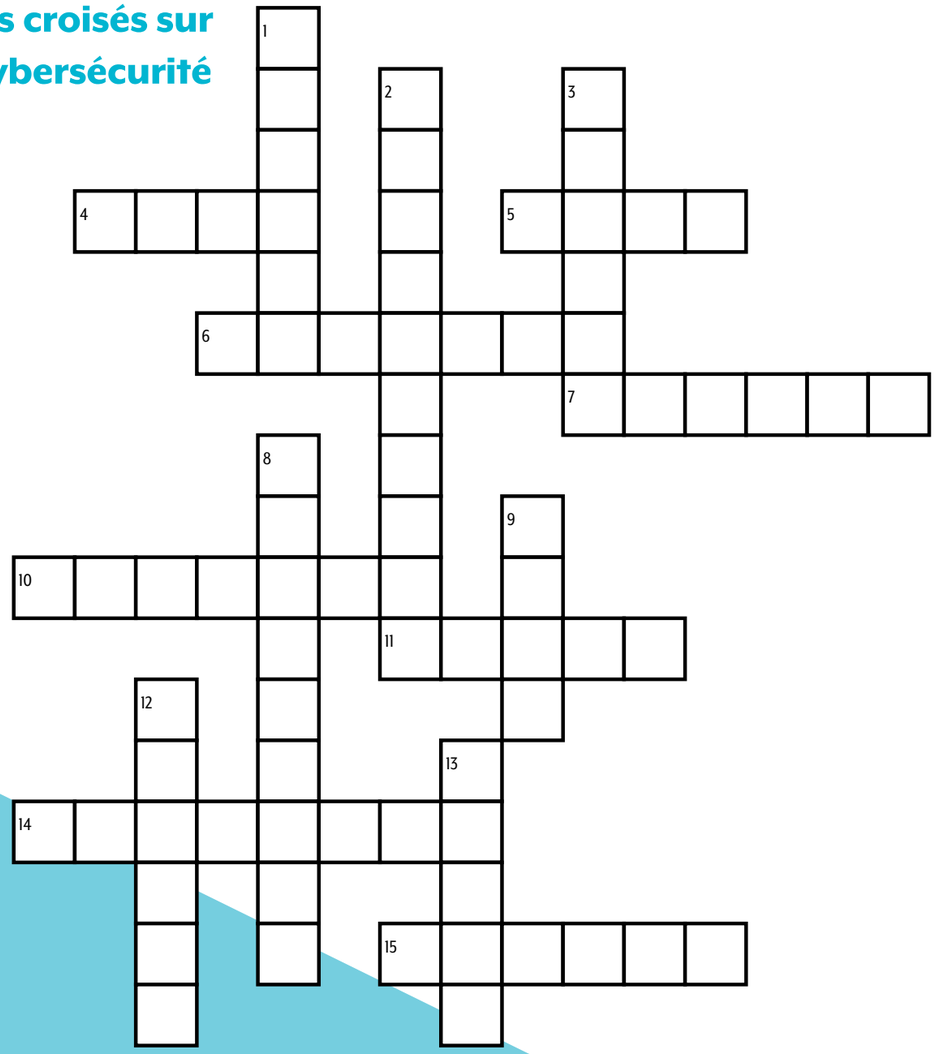
Évitez d’utiliser une connexion WiFi publique quand vous effectuez des transactions bancaires ou des achats en ligne.

Les connexions WiFi publiques sont très utiles pour regarder des vidéos ou consulter des sites Internet, mais n’utilisez que votre connexion Internet personnelle pour toutes vos activités en ligne impliquant de l’argent. Les connexions WiFi publiques peuvent poser des risques.

Signalez les cybercrimes et les incidents en ligne pour contribuer à protéger l’Australie.

Si vous pensez que vous avez été victime d’un cybercrime, agissez sans attendre. Des conseils complémentaires sont disponibles sur le site cyber.gov.au

Mots croisés sur la cybersécurité



VERTICALEMENT

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer’s files
13. Relating to, or involving computers

HORIZONTALEMENT

4. Wireless networking technology
5. Australia’s lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Guides supplémentaires

Pour de plus amples informations, veuillez consulter notre série sur la *cybersécurité personnelle* : trois guides conçus pour aider les Australiens ordinaires à comprendre les fondements de la cybersécurité et les mesures qu’ils peuvent prendre pour se protéger contre les cyberattaques courantes.

Les trois guides sont accessibles sur le site **cyber.gov.au**

Solution des mots croisés :

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Remarques

Avis de non-responsabilité
Les éléments figurant dans ce guide sont de caractère général et ne doivent pas être considérés comme des conseils juridiques ou une forme d'aide dans des circonstances particulières ou dans une situation d'urgence. Pour toute question importante, vous devriez obtenir les conseils d'un professionnel indépendant relativement à vos circonstances spécifiques.

Le Commonwealth n'endosse aucune responsabilité en cas de dommages, de perte ou de dépenses découlant de l'utilisation des informations contenues dans ce guide.

Pour des informations complémentaires ou pour signaler un incident de cybersécurité, contactez-nous :

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Vous ne pouvez appeler ce numéro que depuis l'Australie.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre