



Australian Government



Agissez dès maintenant
pour votre sécurité.

Comment se protéger sur Internet

Version Lecture facile



Comment utiliser ce guide



Nous sommes le gouvernement australien.

Nous avons rédigé ce guide.



Nous avons écrit certains mots en **gras**.

Nous expliquons la signification de ces mots.

Vous trouverez également un glossaire de ces mots à la page 28.



Vous pouvez demander à une personne de confiance de vous aider à :

- lire ce guide
- trouver davantage d'informations.



Ceci est un résumé en version Lecture facile d'un autre guide

Il ne comprend que les idées les plus importantes.



Vous pouvez trouver l'autre guide sur notre site internet.

www.actnowstaysecure.gov.au

Que contient ce guide ?

À propos de ce guide	4
Sécurisez vos comptes	6
Vérifiez vos paramètres pour protéger vos informations	10
Protégez vos appareils	16
Les arnaques en ligne	20
Faites entendre votre voix	25
Glossaire	28
Nous contacter	30

À propos de ce guide



Nous devons tous réfléchir à la manière dont nous pouvons assurer notre sécurité numérique.

C'est ce qu'on appelle la **cybersécurité**.



« Cyber » fait référence à quelque chose en lien avec Internet.



Ce guide vous explique ce que vous pouvez faire pour vous protéger en ligne.

Par exemple, contre la **cybercriminalité**.



On parle de cybercriminalité lorsque des criminels utilisent Internet pour commettre des délits.

Par exemple, ils peuvent utiliser Internet pour :

- voler vos données personnelles
- prendre le contrôle de vos comptes ou profils en ligne.

La cybercriminalité peut toucher n'importe quel appareil.



Notamment :

- votre ordinateur
- votre téléphone portable
- votre montre connectée.



Vous pouvez prendre des mesures pour vous protéger contre la cybercriminalité.



Nous vous expliquons ce que vous pouvez faire dans les pages suivantes.

Sécurisez vos comptes



Réfléchissez à la manière de protéger vos comptes en ligne.

Utilisez des phrases de passe complexes et variées



Une **phrase de passe** est un type de mot de passe plus complexe.

La deviner est plus difficile pour les tiers.



L'utilisation de phrases de passe complexes et variées est l'un des moyens les plus efficaces de sécuriser vos comptes.



Utilisez une phrase de passe différente pour chacun de vos comptes en ligne.



Des phrases de passe robustes incluent :

- 4 mots au hasard, voire plus.
- 15 lettres et chiffres, voire plus.



Vous pouvez inclure des majuscules.



Vous pouvez aussi inclure des symboles tels que :

- un tiret
- le symbole du dollar
- le symbole de l'arobase @.



N'utilisez pas d'informations personnelles dans vos phrases de passe.



Par exemple :

- votre date d'anniversaire
- les noms des membres de votre famille ou de vos animaux de compagnie.

Ajoutez des étapes supplémentaires pour vous connecter à vos comptes



Vous pouvez protéger vos comptes en ligne grâce à **l'authentification multifacteur (MFA)**.

La MFA consiste à utiliser au moins deux méthodes différentes pour vous connecter à votre compte à chaque fois.



Par exemple, vous devrez peut-être saisir d'abord votre phrase de passe.

Puis entrer un code que vous recevrez sur votre téléphone.

Vous aurez peut-être le choix entre :



- télécharger une application sur votre téléphone pour obtenir le code



- recevoir le code par mail



- recevoir le code par SMS.



La MFA rend plus difficile l'accès à vos comptes en ligne par des tiers.

Même s'ils parviennent à découvrir votre phrase de passe.

Vérifiez vos paramètres pour protéger vos informations



Vous pouvez vérifier que vos paramètres protègent bien vos informations en ligne.



Cela comprend les paramètres de :

- vos comptes en ligne
- vos appareils
- vos applications.



Vous pouvez :

- modifier vos paramètres
- choisir quelles applications peuvent utiliser vos données.

Vous pouvez accéder aux paramètres de votre appareil :



- en recherchant l'icône en forme d'engrenage
- ou
- en saisissant « paramètres » dans la barre de recherche de votre appareil.



Vous pouvez accéder aux paramètres d'une application ou d'un compte en ligne en ouvrant le menu.

Le menu est souvent représenté par trois lignes droites.



Certains de ces paramètres peuvent divulguer des informations concernant :

- votre identité
- votre localisation
- votre lieu de résidence.



Le partage de ces informations en ligne peut vous exposer à des risques de cybercrimes.



Les cybercriminels peuvent utiliser vos données pour se faire passer pour vous.

Par exemple, ils peuvent utiliser des informations telles que :



- votre lieu de résidence



- les noms des membres de votre famille



- les noms de vos animaux de compagnie.



Vous pouvez configurer vos comptes de telle sorte que seules les personnes que vous connaissez puissent voir vos profils sur les réseaux sociaux.

Par exemple, votre profil Facebook.



Ces paramètres sont généralement appelés « paramètres de confidentialité ».



Vous pouvez également gérer vos **paramètres de localisation**.

Les paramètres de localisation indiquent où se trouve votre appareil.



Vous pouvez activer ou désactiver les paramètres de localisation.

Vous pouvez également choisir quelles applications peuvent accéder à vos paramètres de localisation.



Vous pouvez le faire pour :

- vos comptes en ligne
- vos appareils
- vos applications.

Certaines applications peuvent également vous demander si elles peuvent :



- utiliser votre appareil photo



- accéder à vos photos.



N'autorisez que les applications que vous connaissez bien à accéder à votre appareil photo et à vos photos.

Protégez vos appareils



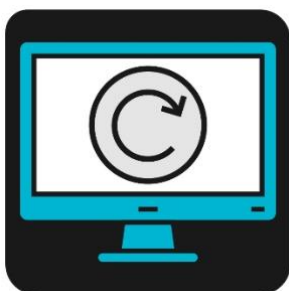
Réfléchissez à la manière de protéger vos appareils afin d'assurer votre sécurité numérique.

Par exemple, votre téléphone ou votre montre connectée.



C'est particulièrement important pour les appareils qui se connectent à Internet.

Mettez vos appareils à jour



Vous pouvez mettre vos appareils à jour pour assurer leur sécurité en ligne.

Par exemple, votre téléphone et votre ordinateur portable.



Sur votre appareil, cela s'appelle peut-être une mise à jour de logiciel.



Les mises à jour aident un appareil à se protéger contre la cybercriminalité.



Vous pouvez configurer un appareil de telle sorte qu'il puisse se mettre à jour automatiquement.



Vous trouverez de plus amples informations sur la mise à jour de vos appareils sur notre site Internet.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Les réseaux Wi-Fi publics



Soyez prudent lorsque vous utilisez un réseau **Wi-Fi public**.



Le Wi-Fi public est un accès Internet sans fil gratuit auquel vous pouvez vous connecter dans les lieux publics.



Par exemple dans :

- un café
- un aéroport
- un hôtel.



Faites attention aux informations que vous saisissez sur un site Internet lorsque vous utilisez un réseau Wi-Fi public.



Par exemple :

- vos coordonnées bancaires
- vos comptes de messagerie électronique
- vos profils sur les réseaux sociaux.



Certains cybercriminels peuvent utiliser les réseaux Wi-Fi publics pour :

- voir ce que vous faites en ligne
- voler vos données.

Car en effet :



- tout le monde peut l'utiliser



- il est plus difficile de protéger vos appareils.



Vous pouvez découvrir comment utiliser le Wi-Fi public en toute sécurité sur notre site Internet.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Les arnaques en ligne



On parle **d'arnaque en ligne** lorsqu'un tiers tente :

- de vous tromper
- de vous soutirer de l'argent.



Un **arnaqueur ou escroc en ligne** est quelqu'un qui commet des arnaques.

Les escrocs en ligne peuvent tenter de vous piéger par le biais :



- d'un SMS ou d'un appel téléphonique
- d'un mail
- des réseaux sociaux
- d'un site Internet.



Ils peuvent sembler sympathiques.

Mais ils peuvent vous duper afin de vous soutirer vos données.

Ils peuvent s'en servir pour :



- accéder à vos comptes en ligne



- se faire passer pour vous



- vous voler votre argent.

Les escrocs en ligne peuvent aussi :



- créer de faux comptes pour vous piéger



- partager des liens et des publicités pour vous inciter à cliquer dessus.

Comment repérer une arnaque

Il peut s'agir d'une arnaque si :



- on vous demande d'agir rapidement



- on vous propose beaucoup d'argent



- on vous demande de l'argent



- on vous demande de cliquer sur un lien.



Les escrocs peuvent également se faire passer pour une entreprise que vous connaissez et en laquelle vous avez confiance.

Par exemple, votre banque.



Les escrocs agissent ainsi pour vous inciter à leur communiquer vos informations personnelles.



Si vous pensez que cette personne est un escroc, cessez toute communication avec elle.



Vérifiez que cette personne est bien celle qu'elle prétend être.

Vous pouvez contacter cette personne ou cette entreprise en utilisant les coordonnées auxquelles vous faites confiance et que vous avez trouvées vous-même.



Réagissez rapidement pour vous protéger si quelque chose vous semble louche.

Comment signaler une arnaque



Scamwatch aide les Australiens à :

- comprendre les arnaques
- signaler les arnaques.



Scamwatch vient également en aide aux Australiens qui ont été victimes d'arnaques.



Vous pouvez signaler une arnaque sur le site Internet de Scamwatch.

www.scamwatch.gov.au/report-a-scam

Faites entendre votre voix



N'hésitez pas à faire entendre votre voix, notamment sur la manière dont les autres peuvent se protéger en ligne.

Cela comprend :



- le signalement des cybercrimes



- le partage de vos connaissances sur le sujet avec votre famille et vos amis.



Nous vous expliquons comment vous y prendre pour faire entendre votre voix dans les pages suivantes.

Signalez une arnaque en ligne

Signaler une arnaque en ligne aide les autorités à :



- comprendre comment les cybercriminels tentent d'attaquer les gens



- protéger davantage de personnes.



Vous pouvez signaler une arnaque en ligne sur le site Internet ReportCyber.

www.cyber.gov.au/report

Discutez avec votre famille et vos amis des mesures à prendre pour naviguer en ligne en toute sécurité



N'hésitez pas à partager vos astuces sur la sécurité en ligne avec votre famille et vos amis.

Ils peuvent aussi vous apprendre des choses.



Vous pouvez vous protéger et protéger votre entourage en partageant vos connaissances sur la sécurité en ligne.



C'est également important si vous partagez vos appareils avec d'autres personnes.

Glossaire

Cette liste explique la signification des mots en **gras** dans ce guide



Cyber

« Cyber » signifie que quelque chose a un rapport avec Internet.



Cybercrimes

On parle de cybercrimes lorsque des criminels utilisent Internet pour commettre des délits

Par exemple, ils peuvent utiliser Internet pour :

- voler vos données personnelles
- pirater vos comptes en ligne.



Paramètres de localisation

Les paramètres de localisation indiquent où se trouve votre appareil.



Authentification multifacteur (MFA)

La MFA consiste à utiliser au moins deux méthodes différentes pour vous connecter à votre compte à chaque fois.



Phrase de passe

Une phrase de passe est un type de mot de passe plus complexe.

La deviner est plus difficile pour les tiers.



Wi-Fi public

Le Wi-Fi public est un accès Internet sans fil gratuit auquel vous pouvez vous connecter dans les lieux publics.



Arnaques en ligne

On parle d'arnaque en ligne lorsqu'un tiers tente :

- de vous tromper
- de vous soutirer de l'argent.



Arnaqueurs/Escrocs

Un arnaqueur ou escroc en ligne est quelqu'un qui commet des arnaques.

Nous contacter



Vous pouvez appeler la ligne d'assistance australienne dédiée à la cybersécurité.

1300 292 371



Vous pouvez consulter notre site Internet.

www.actnowstaysecure.gov.au



Vous pouvez signaler un cybercrime sur le site Internet ReportCyber.

www.cyber.gov.au/report



Le groupe Information Access a créé ce document en version Lecture facile à l'aide de photos d'archives et d'images personnalisées. Ces images ne peuvent être réutilisées sans autorisation. Pour toute question concernant ces images, veuillez consulter le site www.informationaccessgroup.com. Veuillez indiquer le numéro de commande 6342.
