

# CONSEILS ESSENTIELS EN MATIÈRE DE CYBERSÉCURITÉ

DES SOLUTIONS PRATIQUES POUR VOUS PROTÉGER EN LIGNE  
[cyber.gov.au/learn](https://cyber.gov.au/learn)



MISES À JOUR AUTOMATIQUES

## Mettez à jour vos applis et appareils

La mise à jour de vos applis et appareils peut résoudre des problèmes et pallier de nouvelles préoccupations ou faiblesses en termes de sécurité que les pirates informatiques pourraient exploiter pour accéder à vos appareils ou comptes. Les mises à jour peuvent également ajouter de nouvelles fonctions.



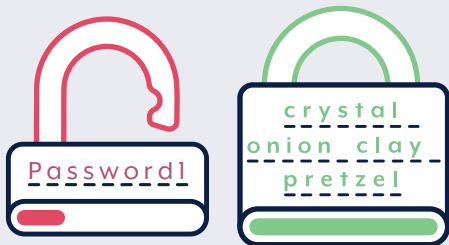
## Activez l'authentification multifactorielle (AMF)

L'AMF prévoit plusieurs processus de contrôle pour prouver votre identité relativement à un compte. Par exemple, vous pouvez avoir besoin d'un code provenant d'un SMS et de votre phrase de passe. L'accès de pirates informatiques à vos comptes est alors bien plus difficile.



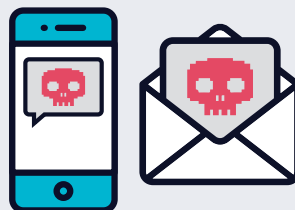
## Configurez et effectuez des sauvegardes régulières

Une sauvegarde est une copie numérique de vos informations les plus importantes sur un périphérique de stockage externe ou un serveur sur l'Internet, tel que le Cloud. En d'autres termes, elle vous permet de récupérer vos fichiers en cas de problème.



## Configurez des phrases de passe sécurisées

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



## Reconnaissez les arnaques et signalez-les

Les criminels utilisent souvent des courriels, des SMS, des appels téléphoniques et les réseaux sociaux pour arnaquer leurs victimes. En général, ils procèdent en vous contactant et en se faisant passer pour une personne ou une organisation que vous connaissez et à laquelle vous faites confiance. Soyez toujours sur vos gardes lorsque vous cliquez sur des pièces jointes ou des liens à l'intérieur des courriels ou des messages.



## Pour renforcer votre cybersécurité...

- Réfléchissez à ce que vous publiez en ligne.
- Abonnez-vous à notre service d'alerte gratuit pour recevoir des alertes au sujet de nouvelles menaces.
- Parlez de la cybersécurité avec votre famille et vos amis.
- Évitez d'utiliser une connexion WiFi publique quand vous effectuez des transactions bancaires ou des achats en ligne.
- Signalez les cyberattaques et les incidents en ligne pour contribuer à protéger l'Australie.

Accédez au site [cyber.gov.au/learn](https://cyber.gov.au/learn) pour des informations complémentaires

### Signalez les incidents liés à la cybersécurité :

[cyber.gov.au](https://cyber.gov.au) | 1300 CYBER1 (1300 292 371)

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