Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

CYBERSÉCURITÉ PERSONNELLE

PREMIÈRES MESURES

cyber.gov.au

Série sur la cybersécurité personnelle

Série sur la cybersécurité personnelle

Le guide intitulé ***La cybersécurité personnelle : premières mesures*** est le premier d'une série de trois guides qui sont conçus pour aider les Australiens ordinaires à comprendre les fondements de la cybersécurité. Découvrez les mesures que vous pouvez prendre pour vous protéger contre les cybermenaces courantes.

Premières Mesures

Mesures Suivantes

Mesures Avancées

Table des matières

Introduction

Qu’est-ce que la cybersécurité personnelle ?

Dans un monde qui s’appuie de plus en plus sur les technologies, nous utilisons dans notre quotidien des appareils et des comptes qui sont vulnérables aux cybermenaces :

- Vos appareils peuvent comprendre des ordinateurs, des téléphones portables, des tablettes et d’autres dispositifs connectés à l’Internet.
- Il se peut également que vous utilisiez des comptes en ligne pour vos courriers électroniques, vos opérations bancaires, vos achats, des plateformes de réseaux sociaux et des sites de jeux, entre autres.

Afin d’assurer votre cybersécurité personnelle, il faut appliquer continuellement certaines mesures pour protéger vos comptes et vos appareils contre les cybermenaces.

Que sont les cybermenaces ?

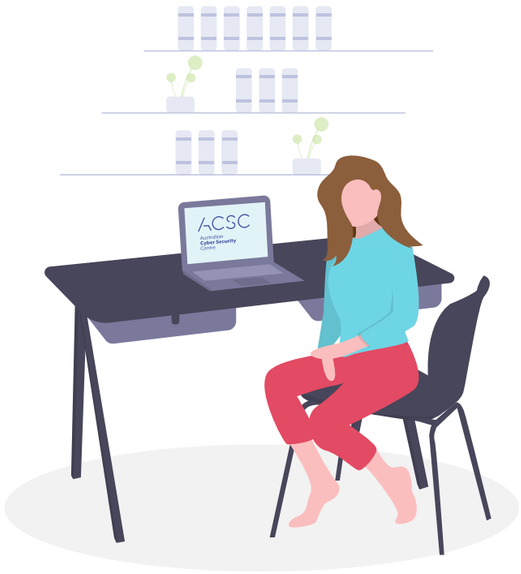
Les principales cybermenaces qui touchent les Australiens ordinaires peuvent se présenter sous forme **d’arnaques et de logiciels malveillants**.

- « **Logiciel malveillant** » **est une expression générale qui désigne un logiciel nuisible** conçu pour faire du tort. Il peut s’agir de virus, de vers, de logiciels espions, de chevaux de Troie et de logiciels rançonneurs.
  Les cybercriminels utilisent des logiciels malveillants pour voler vos informations et votre argent et pour contrôler vos appareils et comptes.
- **Les arnaques se présentent sous forme de messages que des cybercriminels** vous envoient dans le but de vous inciter à leur fournir des informations sensibles ou d’activer des logiciels malveillants sur votre appareil.

Ces attaques peuvent avoir d'importantes répercussions personnelles et financières sur leurs victimes. En outre, elles sont de plus en plus sophistiquées et fréquentes.

Comment ce guide peut-il contribuer à assurer ma protection contre les cybermenaces ?

Que ce soit la première fois que vous entendez parler de la cybersécurité ou que vous cherchiez tout simplement à vous tenir au courant sur le sujet, ce guide est un excellent point de départ. Le guide La cybersécurité personnelle : premières mesures est le premier d’une série de trois guides qui sont destinés à vous aider à comprendre les fondements de la cybersécurité.



Activez les mises à jour automatiques

Que sont des mises à jour ?

Une mise à jour est une version améliorée d'un logiciel (programme, appli. et système d’exploitation) que vous avez installé sur votre ordinateur et vos appareils mobiles.

- **Les mises à jour logicielles contribuent à protéger vos appareils** en résolvant les « bogues » (les erreurs de codage ou les vulnérabilités) dans les logiciels. Les cybercriminels et les logiciels malveillants peuvent exploiter ces « bogues » pour accéder à vos appareils et voler vos données à caractère personnel, les informations sur vos comptes et vos finances, ainsi que votre identité.
- **Les cybercriminels trouvent et exploitent constamment** de nouveaux « bogues » dans les logiciels. La mise à jour des logiciels sur vos appareils aide à vous protéger contre les cybermenaces.

Comment configurer des mises à jour automatiques ?

Les mises à jour automatiques sont un réglage par défaut ou que l’on n’effectue qu’une seule fois pour installer de nouvelles mises à jour dès qu’elles sont disponibles.

- **Activez et confirmez les mises à jour automatiques** sur tous vos logiciels et appareils.
- **La procédure d’activation des mises à jour automatiques peut varier** selon les logiciels et les appareils.
- **Si possible, définissez une heure pratique pour les mises à jour** – par exemple, quand vous dormez ou à des heures auxquelles vous n'utilisez généralement pas votre appareil.

Votre appareil doit être mis sous tension, branché à une alimentation électrique et disposer d’un espace de stockage libre.

Conseil : Si vous recevez une invitation à mettre à jour les logiciels sur votre appareil, vous devriez le faire dès que possible.

Vous trouverez des informations plus détaillées sur la manière d’activer les mises à jour automatiques en cherchant « Updates » (mises à jour) sur le site cyber.gov.au

Que faire si le réglage des mises à jour automatiques n'est pas disponible ?

Si le réglage des mises à jour automatiques n'est pas disponible, vous devriez contrôler régulièrement l'existence de nouvelles mises à jour et les installer par le biais du menu des réglages de vos logiciels ou appareils.

Que faire si mes appareils et logiciels anciens ne reçoivent pas de mises à jour ?

Si votre appareil, votre système d'exploitation ou votre logiciel est trop ancien, il se peut que le fabricant ou le développeur ne le prenne plus en charge.

Quand des produits atteignent leur étape de « fin de prise en charge », ils ne reçoivent plus de mises à jour. Cela peut vous exposer à des cyberattaques. Parmi les produits en fin de prise en charge figurent le système d'exploitation Windows 7 et l'iPhone 7.

Si votre appareil, votre système d'exploitation ou votre logiciel est en fin deprise en charge, le Centre australien de la cybersécurité (Australian Cyber Security Centre – ACSC) recommande d'effectuer une mise à niveau sans délai pour assurer votre protection.

Pour des informations complémentaires, recherchez « End of support » (fin de prise en charge) sur le site cyber.gov.au

Cybersécurité personnelle : Premières mesures

Activez l'authentification multifactorielle (AMF)

Qu'est-ce que l'AMF ?

Vous pouvez utiliser l'authentification multifactorielle (AMF) pour améliorer la sécurité de vos comptes les plus importants. L'AMF exige que vous fournissiez une combinaison d'au moins deux types d'authentification avant de vous permettre d'accéder à un compte.

- **Quelque chose que vous connaissez** (par exemple, un code PIN, un mot de passe ou une phrase de passe)
- **Quelque chose que vous avez** (par exemple, une carte intelligente, un jeton physique,une appli. d'authentification, un SMS ou un courriel)
- **Quelque chose d'unique à vous** (par exemple, une empreinte digitale, la reconnaissance faciale ou le balayage de l'iris)

Grâce à l'AMF, les pirates informatiques rencontrent plus de difficultés lorsqu'ils tentent d'accéder à vos comptes. Comme elle augmente le nombre de couches d'authentification, il faut plus de temps, d'efforts et de ressources pour pirater vos comptes.

Comment puis-je activer l'AMF pour protéger mes comptes les plus importants ?

Les mesures d'activation de l'AMF varient selon le compte, l'appareil ou l'application logicielle. Vous devriez activer l'AMF dès maintenant,en commençant par vos comptes les plus importants :

- Tous vos comptes bancaires et financiers en ligne (par exemple, votre banque, PayPal)
- Tous vos comptes de messagerie électronique (par exemple, Gmail, Outlook, Hotmail, Yahoo!)

Si vous possédez un grand nombre de comptes de messagerie électronique, privilégiez ceux qui sont associés à votre compte bancaire en ligne ou à d'autres services importants.

Consultez des informations complémentaires sur la manière d'activer l'authentification multifactorielle en recherchant « Multi-factor authentication » (authentification multifactorielle) ou « MFA » (AMF) sur le site cyber.gov.au

Sauvegardez régulièrement vos appareils

Qu'est-ce qu'une sauvegarde ?

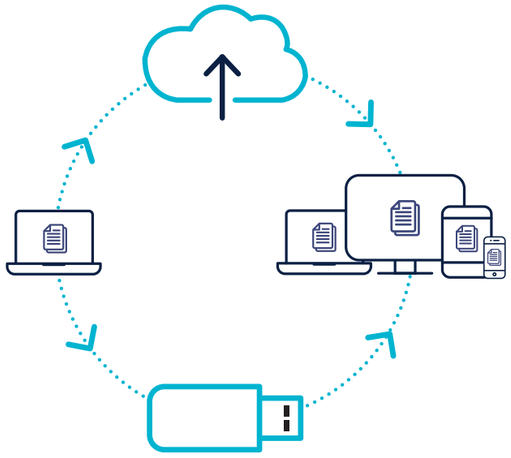
Une sauvegarde est une copie numérique de vos informations. Elle peut comprendre divers éléments tels que des photos, des informations financières ou des dossiers que vous avez enregistré(e)s sur un périphérique de stockage externe ou sur le Cloud.

La sauvegarde de vos informations est une mesure de précaution qui permet de les recouvrer en cas de perte, de vol ou de dommages.

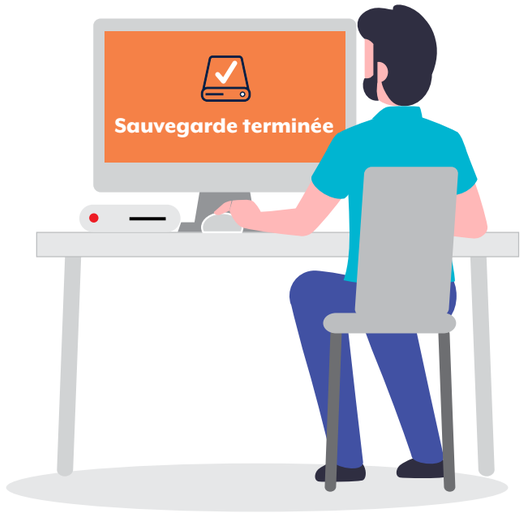
Comment puis-je sauvegarder mes appareils et mes fichiers ?

Vous devriez régulièrement sauvegarder vos fichiers et vos appareils. C'est à vous d'en décider de la fréquence, que ce soit au quotidien, chaque semaine ou chaque mois. La fréquence de vos sauvegardes pourrait dépendre du nombre de :

- nouveaux fichiers que vous chargez sur votre appareil,
- changements que vous apportez à vos fichiers.



Conseil : Contrôlez régulièrement vos sauvegardes afin de vous familiariser avec le processus de récupération. Veillez toujours à ce que vos sauvegardes fonctionnent correctement.



Vous trouverez des informations plus détaillées sur la manière de sauvegarder vos informations en cherchant « Backups » (sauvegardes) sur le site cyber.gov.au

Cybersécurité personnelle : Premières mesures

Utilisez des phrases de passe pour sécuriser vos comptes importants

L'authentification multifactorielle (AMF) est l'une des méthodes les plus efficaces pour protéger vos comptes contre les cybercriminels. **Si la fonction d'AMF n'est pas disponible**, une phrase de passe unique renforcée peut mieux protéger votre compte qu'un simple mot de passe.

Qu'est-ce qu'une phrase de passe ?

Une phrase de passe est similaire à un mot de passe, mais elle comprend au moins quatre mots aléatoires.

Par exemple, « cristal oignon argile bretzel ».

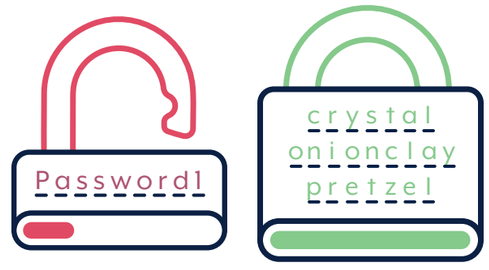
- **Les phrases de passe sont plus sécurisées** que de simples mots de passe.
- Les phrases de passe sont **difficiles à deviner pour les** cybercriminels, mais il **est facile de vous** en souvenir.

Comment puis-je créer une phrase de passe ?

Créez des phrases de passe qui sont :

- **Longues :** comprenant au moins quatre mots aléatoires d'un total de 14 caractères minimum. Plus votre phrase de passe est longue, plus elle est sûre.
- **Imprévisibles :** employez un mélange d'au moins quatre mots sans rapport entre eux. N'utilisez pas des phrases, des citations ou des paroles de chansons célèbres.
- **Uniques :** ne réutilisez pas la même phrase de passe pour plusieurs comptes.

Si un site Internet ou un service exige un mot de passe complexe comprenant des symboles, des lettres majuscules ou des nombres, vous pouvez inclure ces types de caractères dans votre phrase de passe. Pour maximiser votre sécurité, votre phrase de passe doit toujours être longue, imprévisible et unique.



Quels comptes devrais-je protéger par une phrase de passe ?

Si vos comptes les plus importants ne sont pas protégés par la fonction d'AMF, remplacez vos mots de passe par des phrases de passe uniques renforcées, en commençant par vos :

- Comptes bancaires et financiers en ligne
- Comptes de messagerie électronique

Si vous possédez un grand nombre de comptes de messagerie électronique, privilégiez ceux qui sont associés à votre compte bancaire en ligne ou à d'autres services importants.

En général, vous pouvez remplacer votre mot de passe par une phrase de passe unique renforcée en utilisant le menu des réglages de votre compte.

Conseil : 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.

Vous trouverez des informations plus détaillées sur la manière de créer des phrases de passe en cherchant « Passphrases » (phrases de passe) sur le site cyber.gov.au

Sécurisez votre appareil mobile

De nos jours, les téléphones intelligents et les tablettes sont utilisés au quotidien. Nous les utilisons pour nous connecter, faire des achats, travailler, effectuer des opérations bancaires, surveiller notre forme physique et réaliser des centaines de tâches à tout moment, n'importe où.

Que faire si mon appareil mobile a été compromis, perdu ou volé ?

- Il se peut qu'il soit utilisé par des cybercriminels pour voler votre argent ou votre identité. Pour ce faire, les cybercriminels utilisent des informations stockées sur votre appareil, notamment sur vos comptes de réseaux sociaux et de messagerie électronique.
- Vous pouvez perdre des données irremplaçables telles que des photos, des notes ou des messages (si ces données ne sont pas sauvegardées).
- Un cybercriminel peut utiliser votre numéro de téléphone pour arnaquer d'autres personnes.

Comment puis-je protéger mon appareil mobile ?

Sécurité des appareils :

- **Verrouillez** votre appareil avec une phrase de passe, un mot de passe, un code PIN ou un code de passe. Faites en sorte que ce soit difficile à deviner – votre date de naissance et les schémas de verrouillage sont simples à déduire pour les cybercriminels. Utilisez une phrase de passe pour optimiser votre sécurité (voir page 6). Vous pourriez également envisager d'utiliser la reconnaissance faciale ou une empreinte digitale pour déverrouiller votre appareil.
- **Assurez-vous** que votre appareil est réglé de manière à se verrouiller automatiquement après une courte période d'inactivité.
- **Ne chargez pas** votre appareil sur une station de chargement publique et évitez les chargeurs de tiers.
- **Traitez** votre téléphone comme s'il s'agissait de votre portefeuille. Gardez-le constamment en sécurité et sur vous.

Sécurité des logiciels et des applis :

- **Utilisez** la fonction de mise à jour automatique de votre appareil pour installer les nouvelles mises à jour des applications et du système d'exploitation dès qu'elles sont disponibles.
- **Réglez** votre appareil afin qu'il exige une phrase de passe/un mot de passe avant d'installer des applications. Il est également possible d'utiliser les contrôles parentaux à cette fin.
- **Contrôlez** attentivement les autorisations liées à la confidentialité lors de l'installation de nouvelles applis sur votre appareil, en particulier des applis gratuites. N'installez que les applis de fournisseurs réputés.

Sécurité des données :

- **Activez** les fonctions de verrouillage et d'effacement à distance si votre appareil les prend en charge.
- **Veillez** à supprimer de votre appareil l'intégralité des données à caractère personnel vous concernant avant de le vendre ou de le mettre au rebut.

Sécurité de la connectivité :

- **Désactivez** les connexions Bluetooth et WiFi quand vous ne les utilisez pas.
- **Assurez-vous** que votre appareil ne se connecte pas automatiquement à de nouveaux réseaux WiFi.

Vous trouverez des informations plus détaillées sur la manière de vous assurer de pouvoir trouver votre appareil mobile en cherchant « Secure your mobile phone » (sécurisez votre téléphone portable) sur le site cyber.gov.au

Développez votre capacité de discernement en ligne

La cybersécurité personnelle ne se limite pas à changer des réglages, elle consiste également à modifier votre façon de penser et vos comportements.

Faites attention aux arnaques en ligne

Les cybercriminels sont connus pour utiliser des courriels, des messages, les plateformes de réseaux sociaux ou des appels téléphoniques pour tenter d'arnaquer les Australiens. Ils se font passer pour une personne ou une organisation que vous pensez connaître ou à laquelle vous pensez que vous devriez faire confiance.

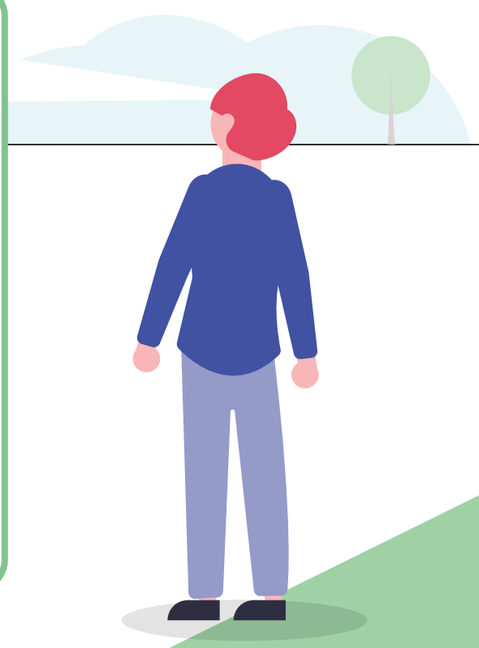
Leurs messages et appels tentent de vous inciter à effectuer des actions spécifiques, par exemple :

- révéler les détails de vos comptes bancaires, vos mots de passe et vos numéros de carte de crédit
- leur permettre d'accéder à votre ordinateur à distance
- ouvrir une pièce jointe qui peut contenir un logiciel malveillant
- envoyer de l'argent ou des bons-cadeaux

Comment puis-je reconnaître des messages d'arnaque ?

Les messages d'arnaque peuvent être difficiles à reconnaître. Les cybercriminels emploient souvent des méthodes spécifiques pour vous tromper. Leurs messages peuvent s'appuyer sur :

- **La légitimité** : le message prétend-il provenir d'une personne officielle, par exemple, de votre banque ?
- **L'urgence** : vous dit-on qu'il y a un problème ou que vous avez un délai limité pour répondre ou payer ?
- **Les émotions** : le message vous fait-il paniquer ou vous inspire-t-il de l'espoir ou de la curiosité ?
- **Un effet d'aubaine** : le message offre-t-il quelque chose de difficile à se procurer ou promet-il une bonne affaire ?
- **Les événements de l'actualité** : le message porte-t-il sur un sujet courant de l'actualité ou un grand événement ?



Apprenez à repérer les messages d'hameçonnage ou d'arnaque en accédant à la section « Learn the basics » (apprenez les fondamentaux) sur le site cyber.gov.au

Que dois-je faire si je reçois un messaged'arnaque ?

Si vous recevez un message ou un appel téléphonique d'arnaque, vous devez l'ignorer, le supprimer et le signaler au service Scamwatch de la Commission australienne de la concurrence et de la consommation (Australian Competition and Consumer Commission – ACCC), à l'adresse scamwatch.gov.au

Vous pouvez également contacter le service d'assistance téléphonique de l'ACSC sur la cybersécurité au **1300 CYBER1** (1300 292 371) si vous avez des inquiétudes à propos de votre cybersécurité.

Si vous avez répondu à une arnaque et que vous pensez que vos comptes bancaires ou vos cartes de crédit ou de débit sont compromis(es), contactez votre institution financière immédiatement. Elle peut être en mesure de fermer votre compte ou de stopper une transaction.

Que faire si je ne suis pas certain·e qu'un message est une arnaque ?

Si vous pensez qu'un message ou un appel pourrait véritablement provenir d'une organisation dans laquelle vous avez confiance (par exemple, votre banque), trouvez une méthode de contact fiable. Recherchez le site Internet officiel de l'organisation, appelez le numéro de téléphone indiqué ou rendez-vous dans un magasin ou une succursale physique. N'utilisez pas les liens ni les coordonnées figurant dans le message que vous avez reçu ou qui vous ont été fournis par téléphone, car ils pourraient être frauduleux.

Conseil :
Réfléchissez avant de cliquer

Si vous pensez être la victime d'un cybercrime, signalez-le au service ReportCyber de l'ACSC sur le site cyber.gov.au/report ou appelez notre service d'assistance téléphonique de cybersécurité au 1300 CYBER1 (1300 292 371).

Vous pouvez également rester informé·e des dernières menaces en vous abonnant au service d'alerte gratuit de l'ACSC. Recherchez « Subscribe to the ACSC alert service » (abonnez-vous au service d'alerte de l'ACSC) sur le site cyber.gov.au
Nous vous enverrons une alerte chaque fois que nous identifions une nouvelle cybermenace.

Cybersécurité personnelle : Premières mesures

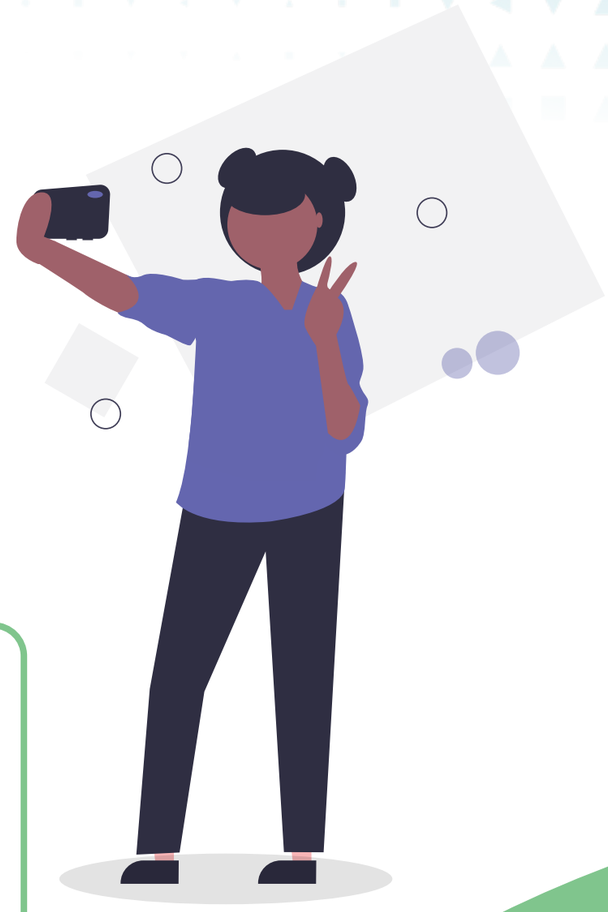
Prenez un moment pour réfléchir avant de partager quoi que ce soit sur les réseaux sociaux

Dans leurs arnaques et cyberattaques, les cybercriminels peuvent utiliser les informations que vous avez publiées publiquement sur votre ou vos compte(s) de réseaux sociaux.

Souvenez-vous qu'une fois que des informations sont publiées sur l'Internet, elles le sont de façon permanente et vous ne pourrez jamais les supprimer complètement.

Quelles questions me poser avant de publier en ligne ?

- **Réfléchissez :** Comment un cybercriminel pourrait-il utiliser ces informations pour me cibler moi ou mes comptes ?
- **Réfléchissez :** Serais-je à l'aise de montrer ces informations ou cette image hors ligne à une personne que je ne connais pas du tout ?



Quelles informations devrais-je éviter de partager ?

Évitez de partager des informations (y compris des photos) en ligne que les cybercriminels peuvent utiliser en vue de vous identifier, de vous manipuler au travers d'une arnaque ou de deviner les réponses aux questions permettant de recouvrer votre compte. Il peut s'agir de :

- Votre lieu de naissance et votre date de naissance.
- Votre adresse et votre numéro de téléphone.
- Votre employeur et votre expérience professionnelle.
- Les écoles que vous avez fréquentées.
- Toute autre information à caractère personnel qu'il est possible d'exploiter pour vous cibler.

Liste de contrôle récapitulative

Avez-vous parcouru l'intégralité de ce guide?

Utilisez cette liste de contrôle pratique pour assurer un suivi de vos progrès :

- **J'ai activé les mises à jour automatiques sur tous mes appareils :**
  - Ordinateur (de bureau ou portable)
  - Téléphone portable
  - Tablette
- **J'ai activé l'authentification multifactorielle sur mes comptes les plus importants :**
  - Tous vos comptes bancaires et financiers en ligne (par exemple, votre banque, PayPal)
  - Tous mes comptes de messagerie électronique (par exemple, Gmail, Outlook,Hotmail, Yahoo!)
- **Je sauvegarde mes appareils et mes fichiers régulièrement :**
  - Ordinateur (de bureau ou portable)
  - Téléphone portable
  - Tablette
- **J'utilise des phrases de passe renforcées sur mes comptes les plus importants qui ne sont pas protégés par l'AMF :**
  - Comptes bancaires et financiers en ligne
  - Comptes de messagerie électronique
- **J'ai protégé mes appareils mobiles :**
  - Ordinateur portable
  - Téléphone portable
  - Tablette
- **Chaque jour, je fais appel à mes capacités de discernement en ligne :**
  - Je peux reconnaître les messages d'arnarque
  - Je sais ce qu'il faut faire si je reçois un message d'arnaque
  - Je sais comment vérifier si un message est une arnaque en cas de doutes
  - Je réfléchis avant de cliquer sur des liens et des pièces jointes
  - Je réfléchis avant de partager quoi que ce soit sur les réseaux sociaux
- **Je sais où obtenir de l'aide si je suis la victime d'un cybercrime ou d'une arnaque**

Glossaire

Recouvrement de compte
Un processus utilisant un ensemble de questions ou d'autres méthodes de vérification pour recouvrer un compte ou pouvoir à nouveau y accéder, ou pour modifier la phrase de passe ou le mot de passe d'un compte.

Appli.
Également appelée « application mobile », une appli. désigne un logiciel qui est communément utilisé sur des téléphones intelligents ou des tablettes.

Pièce jointe
Un fichier envoyé dans un message électronique.

Appli. d'authentification
Une appli. qui permet de confirmer l'identité de l'utilisateur d'un ordinateur afin que celui-ci puisse y accéder à l'aide de l'authentification multifactorielle (AMF).

Le Cloud
Un réseau de serveurs distants qui offrent un espace de stockage distribué et une puissance de traitement énormes.

Cybercriminel
Une personne qui accède illégalement à un système informatique ou un compte pour endommager ou voler des informations.

Appareil
Un dispositif informatique ou de communications. Par exemple, un ordinateur de bureau ou portable, un téléphone portable ou une tablette.

Fin de prise en charge
Situation dans laquelle une société cesse de prendre un produit ou un service en charge. Cela s'applique généralement à des produits matériels ou logiciels dont une société lance une nouvelle version et cesse de prendre les anciennes versions en charge.

Logiciel malveillant
Un logiciel malveillant est utilisé pour accéder sans autorisation à l'ordinateur d'un utilisateur et le contrôler, voler des informations et perturber ou désactiver des réseaux.

Système d'exploitation
Un logiciel installé sur le disque dur d'un ordinateur qui permet au matériel informatique de communiquer avec les programmes de l'ordinateur et de les exécuter. Exemples : Microsoft Windows, Apple macOS, iOS, Android.

Jeton physique
Un dispositif physique que l'on peut généralement accrocher sur un porte-clés et qui génère un code de sécurité pour confirmer l'identité de l'utilisateur d'un ordinateur à l'aide d'une AMF.

Accès à distance
L'accès à des appareils et réseaux et leur contrôle depuis un site externe.

Logiciel
Souvent appelé « programme », un logiciel est un recueil d'instructions qui permettent à une personne d'interagir avec un ordinateur et ses composants ou d'effectuer des tâches.

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