SIGNALEZ LES CYBERCRIMES ET LES INCIDENTS EN LIGNE POUR CONTRIBUER À PROTÉGER L'AUSTRALIE.

ABONNEZ-VOUS

À notre service d'alerte gratuit
cyber.gov.au

SIGNALEZ

Les cybercrimes à REPORTCYBER:
cyber.gov.au/report

CONTACT

Appelez le 1300 CYBER1 ou rendez-vous sur le site cyber.gov.au

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

SUIVEZ-NOUS

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. FAITES ATTENTION AUX ARNAQUES

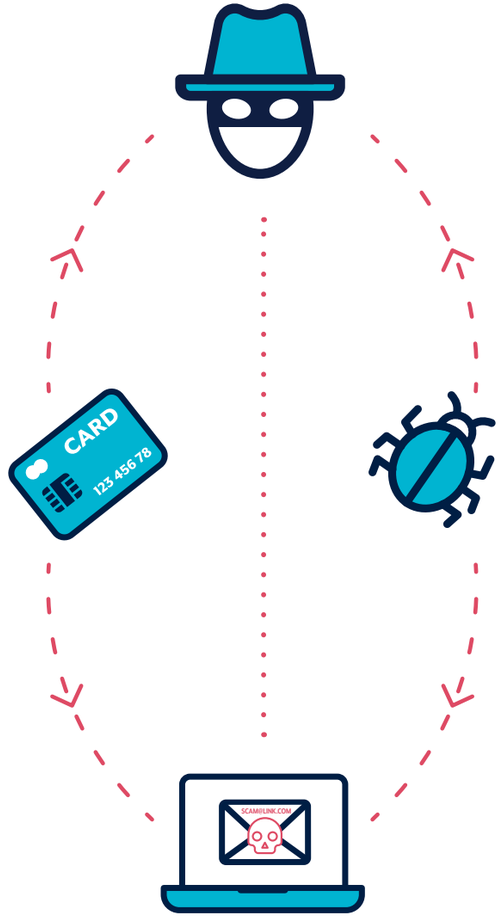
Les cybercriminels utilisent des courriels, des SMS, des appels téléphoniques et les réseaux sociaux pour vous inciter à ouvrir une pièce jointe, à vous rendre sur un site Web, à révéler des détails de connexion à un compte ou des informations sensibles, ou à transférer de l'argent ou des bons-cadeaux. Ces messages sont conçus pour sembler provenir de personnes ou d'organisations que vous pensez connaître ou en qui vous pensez pouvoir faire confiance.

Pour repérer les messages frauduleux, prenez le temps de réfléchir :

- **Légitimité :** Le message prétend-il provenir d'une personne officielle ?
- **Urgence :** Vous dit-on que vous devez répondre dans un délai limité ?
- **Émotions :** Le message vous fait-il paniquer ou vous inspire-t-il de la crainte, de l'espoir ou de la curiosité ?
- **Aubaine :** Le message offre-t-il quelque chose de difficile à se procurer ?
- **Événements de l'actualité :** Le message porte-t-il sur des sujets de l'actualité, de grands événements ou des périodes spécifiques au cours d'une année (par exemple, campagne de déclaration de revenus) ?

Pour vérifier si un message est légitime :

- Référez-vous à quelque chose en quoi vous pouvez faire confiance. Rendez-vous sur le site Web officiel, connectez-vous à votre compte ou appelez le numéro de téléphone indiqué. N'utilisez pas les liens ni les coordonnées figurant dans le message que vous avez reçu ou qui vous ont été fournis par téléphone.
- Vérifiez si la source officielle vous a déjà informé sur ce qu'elle ne vous demandera jamais. Par exemple, votre banque peut vous avoir déclaré qu'elle ne vous demandera jamais votre mot de passe.



Pour des informations complémentaires sur la manière de repérer des messages frauduleux, consultez la publication du Centre australien de la cybersécurité (Australian Cyber Security Centre – ACSC) consacrée à la reconnaissance des messages d'attaque d'ingénierie sociale et restez informé·e en vous abonnant au service d'alerte de l'ACSC sur le site **cyber.gov.au**

MESURES SIMPLES

POUR SÉCURISER VOS APPAREILS ET VOS COMPTES

RÉDUISEZ LE RISQUE DE DEVENIR LA CIBLE DE CYBERCRIMINELS EN APPLIQUANT CES MESURES

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. METTEZ VOS APPAREILS À JOUR

Les cybercriminels piratent des appareils en utilisant des faiblesses connues dans les systèmes ou les applis. Les mises à jour comportent des mises à niveau de sécurité qui visent à surmonter ces faiblesses. Activez les mises à jour automatiques afin qu'elles s'effectuent sans votre intervention.

Activez les mises à jour automatiques sur tous vos appareils :

- Téléphone portable
- Ordinateur portable
- Ordinateur de bureau

Contrôlez régulièrement l'existence de mises à jour pour vos :

- Applis
- Programmes
- Appareils intelligents

2. ACTIVEZ L'AUTHENTIFICATION MULTIFACTORIELLE (AMF)

L'AMF améliore votre sécurité, rendant plus difficile l'accès des cybercriminels à vos fichiers ou à vos comptes.

Activez l'AMF, en commençant par vos comptes les plus importants :

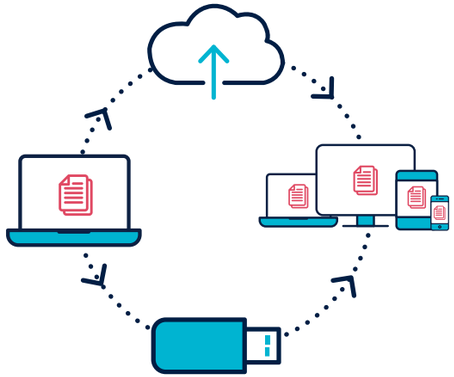
- Comptes de messagerie électronique
- Comptes bancaires en ligne et comptes avec des détails de paiement stockés
- Réseaux sociaux

3. SAUVEGARDEZ VOS APPAREILS

Une sauvegarde est une copie numérique des informations stockées sur votre appareil, telles que des photos, des documents, des vidéos et des données d'applications. Elles peuvent être enregistrées sur un périphérique de stockage externe ou sur le Cloud. Une sauvegarde vous permet de récupérer vos fichiers dans le cas où votre appareil serait perdu, volé ou endommagé.

Sauvegardez régulièrement vos appareils :

- Téléphone portable
- Ordinateur portable
- Ordinateur de bureau
- Tablette



4. CONFIGUREZ DES PHRASES DE PASSE SÉCURISÉES

Dans les cas où la fonction d'AMF n'est pas disponible, une phrase de passe sécurisée peut souvent être l'unique moyen de protéger vos informations et vos comptes contre les criminels.

Une phrase de passe comprend au moins quatre mots aléatoires comme mot de passe. Remplacez vos mots de passe par des phrases de passe en veillant à ce qu'elles soient :

- Longues : Plus votre phrase de passe est longue, mieux c'est. Créez-en une qui contient au moins 14 caractères
- Imprévisibles : Utilisez un mélange aléatoire de mots sans rapport entre eux
- Uniques : Ne réutilisez pas la même phrase de passe pour plusieurs comptes