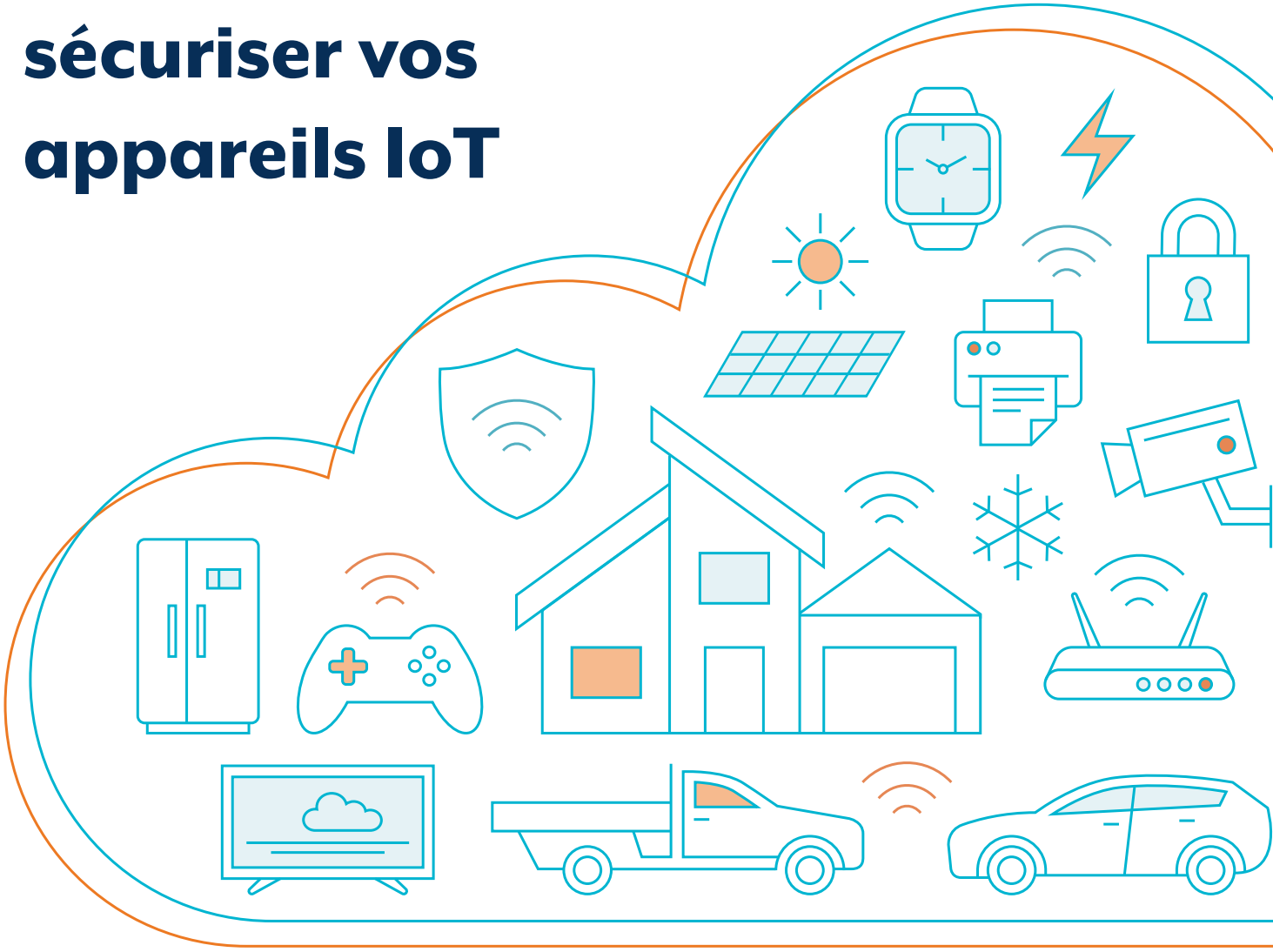
# Conseils pour sécuriser vos appareils IoT



Le Centre australien de cybersécurité a élaboré ces informations pour aider la communauté à acheter et utiliser des appareils Internet des objets (Internet of Things, IoT) en toute sécurité. Un appareil IoT est un objet du quotidien auquel est ajoutée une connexion Internet. Parmi les exemples d'appareils IoT, on peut citer les écoute-bébés, les drones, les caméras de sécurité, les téléviseurs intelligents et les onduleurs solaires. Les appareils IoT utilisés à la maison et au travail utilisent généralement le Wi-Fi ou les réseaux cellulaires, tels que la 4G ou la 5G, pour se connecter à Internet.

De nombreux appareils IoT, couramment utilisés dans les foyers et les entreprises australiennes, n'ont pas été conçus dans un souci de sécurité. De ce fait, ils sont vulnérables aux compromissions via Internet. De tels incidents peuvent permettre aux cybercriminels d'accéder à votre appareil et à vos données personnelles à des fins malveillantes.

# Avant d'acheter un appareil IoT

Il est important de se renseigner sur les appareils avant d'acheter, car les fabricants offrent différents niveaux de sécurité. Avant d'acheter un appareil, comparez les appareils similaires vendus par différents fabricants. Voici quelques points à prendre en compte:

1. **L'appareil est-il fabriqué par une entreprise réputée et vendu par un magasin réputé?** Les entreprises réputées sont plus susceptibles de produire des appareils en mettant l'accent sur la sécurité. Les magasins réputés sont plus susceptibles de vendre uniquement des appareils d'entreprises réputées et ont une chaîne d'approvisionnement plus stricte, garantissant que l'appareil vous parvienne comme prévu par le fabricant.

2. **Est-il possible de modifier le mot de passe?** Il est toujours judicieux de modifier son mot de passe. Cependant, si l'appareil est livré avec un mot de passe par défaut faible, cela devient plus important. Un appareil bien sécurisé doit avoir des mots de passe uniques, imprévisibles, complexes et impossibles à deviner, car les mots de passe par défaut faibles constituent le moyen le plus simple d'attaquer un appareil.

3. **Le fabricant fournit-il des mises à jour?** Il est important que les entreprises proposent des mises à jour pour corriger les vulnérabilités des appareils dès qu'elles sont découvertes. Par exemple, si le logiciel de l'appareil présente des vulnérabilités connues ou si des pirates informatiques développent de nouvelles méthodes pour compromettre votre appareil, des mises à jour sont nécessaires pour y remédier.

4. **Quelles données l'appareil collectera-t-il et avec qui seront-elles partagées?** Les informations concernant les données collectées et leur utilisation doivent être facilement accessibles sur le site Web du fabricant ou dans sa politique de confidentialité. Il est important de toujours tenir compte des informations collectées par l'application en ligne ou mobile.

5. **L'appareil fait-il uniquement ce que vous souhaitez?** Acheter un appareil qui dépasse vos besoins, notamment la connexion à Internet, peut réduire votre sécurité. Les fonctionnalités de l'appareil que vous n'utiliserez pas peuvent accroître sa vulnérabilité aux attaques sans vous apporter aucun avantage.

# Appareil IoT

Gardez à l'esprit quelques questions simples lors de la configuration de votre appareil afin de mieux sécuriser votre réseau et vos données.

1. **L'appareil doit-il être connecté à Internet?** Ce n'est pas parce qu'il peut être connecté qu'il doit l'être. Les appareils non connectés à Internet sont beaucoup moins susceptibles d'être compromis. Si vous n'utilisez pas les fonctionnalités nécessitant une connexion Internet, vous devez vous demander si une connexion est nécessaire.

2. **L'appareil est-il dans un endroit sûr?** Si l'appareil n'a pas besoin d'être installé dans une zone non sécurisée, son installation dans un endroit sûr peut réduire le risque de compromission physique.

3. **Dois-je modifier le nom d'utilisateur et le mot de passe par défaut?** Il est important d'utiliser un mot de passe ou une phrase secrète robuste. Si votre appareil n'est pas livré avec un mot de passe unique, imprévisible, complexe et impossible à deviner, ce mot de passe doit être modifié. Les noms d'utilisateur et les mots de passe par défaut sont collectés et publiés en ligne, ce qui rend votre appareil vulnérable.

4. **Mon réseau Wi-Fi est-il configuré de manière sécurisée et possède-t-il un mot de passe sécurisé?** Sécurisez votre réseau Wi-Fi et votre routeur pour compliquer l'accès à votre appareil et à votre réseau par des pirates.

### Allez plus loin

Configurez un réseau Wi-Fi supplémentaire sur votre routeur pour les appareils IoT uniquement. Ce réseau peut être appelé réseau « invité » sur votre routeur Wi-Fi. Si vos appareils IoT ne nécessitent pas de communication entre eux, activez la fonction « isolation client ». En isolant vos appareils IoT de vos données sensibles, vous évitez qu'une compromission de l'un d'entre eux n'autorise l'accès à vos autres appareils ou données.

5. **Les fonctionnalités inutiles de l'appareil sont-elles désactivées?** Si votre appareil possède des fonctionnalités indésirables ou superflues (comme des caméras ou des microphones), désactivez-les autant que possible.

### Allez plus loin

Recherchez un paramètre de configuration mentionnant l'activation de l'accès à distance à l'interface d'administration Web de l'appareil depuis le réseau local ou le WAN/Internet. Assurez-vous qu'il est configuré sur le réseau local, sauf si vous avez besoin d'un accès à distance.

# Entretien d'un appareil IoT

Voici quelques points importants à retenir une fois votre appareil IoT configuré et utilisé. Cela inclut:

1. **Redémarrez régulièrement vos appareils.** Des virus peuvent être présents si l'appareil IoT commence à ralentir ou à devenir inutilisable. La plupart des logiciels malveillants sont stockés en mémoire et peuvent être facilement supprimés par un redémarrage de l'appareil, c'est-à-dire en l'éteignant puis en le rallumant. Si l'appareil continue d'être lent ou inutilisable après un redémarrage, essayez une réinitialisation d'usine. Sachez toutefois que cela pourrait effacer toutes vos données utilisateur et vos paramètres personnalisés.

2. **Appliquez des mises à jour régulières.** Certains appareils appliquent les mises à jour automatiquement. Pour ceux qui ne le font pas, consultez régulièrement le fabricant et installez les mises à jour dès qu'elles sont disponibles. Lorsqu'il n'y a plus de mises à jour disponibles pour votre appareil, envisagez de passer à un appareil plus récent disposant de mises à jour. Les appareils qui n'ont pas accès aux mises à jour de sécurité ne seront pas protégés si de nouvelles vulnérabilités sont découvertes, et ils peuvent constituer un risque pour votre réseau, votre confidentialité et vos données.

3. **Éteignez votre appareil lorsqu'il n'est pas utilisé.** Laisser des appareils inutilisés et non surveillés allumés et connectés à votre réseau Wi-Fi pendant de longues périodes peut augmenter le risque d'attaque. Une solution pour activer cette fonction automatiquement consiste à utiliser une minuterie de prise de courant pour alimenter l'appareil uniquement pendant les heures spécifiées.

4. **Surveillez toute augmentation significative de votre consommation ou de votre facture Internet mensuelle.** Une augmentation significative de votre consommation ou de vos frais Internet peut indiquer que votre appareil a été compromis. Sauf si le service informatique de votre entreprise doit enquêter sur ce problème, une réinitialisation d'usine doit être effectuée (attention, cela pourrait effacer toutes vos données utilisateur et vos paramètres personnalisés), suivie de la modification de votre mot de passe.

# Mise au rebut d'un appareil IoT

La mise au rebut d'un appareil (en le jetant ou en le vendant) peut permettre à d'autres personnes d'accéder facilement à vos informations personnelles. Pour éviter cela, plusieurs solutions sont possibles :

1. **Effacer toutes les données et informations personnelles.** Le fabricant doit fournir une méthode pour effacer vos données et informations personnelles de l'appareil et des applications associées. Effacer vos informations personnelles garantit que personne n'y aura accès après la mise au rebut de l'appareil. Supprimez votre compte en ligne s'il n'est plus nécessaire sans l'appareil IoT.

2. **Réinitialiser l'appareil aux paramètres d'usine.** Une réinitialisation d'usine permet d'effacer les données stockées dans le stockage local et de réinitialiser les mots de passe, les noms d'utilisateur et les paramètres par défaut. Consultez le manuel d'utilisation de l'appareil ou le site Web du fabricant pour savoir comment effectuer une réinitialisation d'usine.

3. **Dissocier l'appareil des téléphones portables et autres appareils.** La mise au rebut d'un appareil ayant encore accès à vos autres appareils, à votre réseau ou à vos comptes en ligne peut permettre à d'autres d'y accéder. Assurez-vous de vérifier vos autres appareils et de supprimer toute association avec l'appareil que vous mettez au rebut. Supprimez toutes les autorisations accordées à l'application mobile qui ne sont plus nécessaires.

4. **Retirer tout support amovible (par exemple, clé USB, carte mémoire, etc.) connecté à l'appareil.** Les supports amovibles peuvent contenir des données personnelles non supprimées lors d'une réinitialisation d'usine et doivent être retirés, détruits et éliminés séparément de l'appareil.

# Aide

Contactez le Centre australien de cybersécurité de la Direction australienne des signaux par courriel à asd.assist@defence.gov.au ou appelez le numéro d'urgence 24h/24 et 7j/7 pour une assistance urgente au **1300 CYBER1** (**1300 292 371**).

Signalez les cybercrimes à ReportCyber à l'adresse www.cyber.gov.au/report

Contactez IDCARE via son site Web www.idcare.org si vous avez été victime d'une usurpation d'identité.

Consultez www.cyber.gov.au pour obtenir des conseils pour vous et votre famille. Inscrivez-vous gratuitement au service d'alerte de l'ACSC sur les menaces en ligne récentes.

Faisons de l'Australie l'endroit le plus sûr pour se connecter en ligne.

Pour des conseils en matière de cybersécurité, consultez www.cyber.gov.au

**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.

**Droits d'auteur**

© Commonwealth d'Australie 2025

À l'exception du blason et sauf indication contraire, toute la documentation présentée dans cette publication est fournie sous une licence Creative Commons Attribution 4.0 International | creativecommons.org.

Pour éviter toute ambiguïté, cela signifie que cette licence ne s'applique qu'aux éléments tels qu'ils figurent dans ce document.

Les détails des conditions de licence pertinentes sont disponibles sur le site Web de Creative Commons, tout comme le Code juridique de la licence CC BY 4.0 | creativecommons.org.

**Utilisation du blason**

Les conditions dans lesquelles le blason peut être utilisé sont détaillées sur le site Web du Département du Premier Ministre et du Cabinet Informations et directives sur le blason du Commonwealth | pmc.gov.au.

**Pour en savoir plus 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.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre