Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Guide sur la cybersécurité pour les petites entreprises

Complexité du contenu
SIMPLE ● ○ ○

Introduction

Pour une petite entreprise, même un incident de cybersécurité mineur peut avoir des conséquences dévastatrices.
Le présent guide propose des mesures de sécurité de base conçues pour aider à protéger votre entreprise contre les menaces courantes à la cybersécurité.
Pour démarrer, nous recommandons les trois mesures suivantes :

- Activez l'authentification multifactorielle
- Mettez vos logiciels à jour
- Sauvegardez vos informations

Il se peut que ce guide inclue des mesures qui ne sont pas adaptées à votre entreprise, ou que votre entreprise ait des besoins plus complexes. Après avoir consulté l'intégralité de ce guide, nous recommandons aux petites entreprises de mettre en œuvre le premier niveau de maturité des **huit stratégies d'atténuation essentielles**.
Pour toute question au sujet de ces conseils ou de la cybersécurité en général, nous vous encourageons à parler à un professionnel de l'informatique ou à un conseiller de confiance.

Rendez-vous sur le site cyber.gov.au pour consulter notre guide complet, notamment des conseils pratiques associés à chaque mesure.

Table des matières

Les menaces à l'égard des petites entreprises 4
Les messages d'arnaque 4
Les attaques par courriel 5
Les logiciels malveillants 6
Sécurisez vos comptes 7
Activez l'authentification multifactorielle 7
Utilisez des mots de passe ou des phrases de passe renforcé(e)s 7
Gestion de comptes partagés 7
Mettez en œuvre des contrôles d'accès 7
Protégez vos appareils et vos informations 8
Mettez à jour vos logiciels 8
Sauvegardez vos informations 8
Utilisez des logiciels de sécurité 8
Sécurisez votre réseau et vos services externes 9
Renforcez votre site Internet 9
Réinitialisez vos appareils avant de les vendre ou de les mettre au rebut 9
Gardez vos appareils verrouillés et physiquement sûrs 10
Protégez les données de votre entreprise 10
Préparez votre personnel 11
Éduquez vos employés 11
Élaborez un plan d'urgence 11
Tenez-vous informé·e 11

Les menaces à l'égard des petites entreprises

Les messages d'arnaque

Les arnaques sont un moyen courant par lequel les cybercriminels ciblent les petites entreprises. Leur objectif est de vous leurrer, vous et votre personnel, afin que vous :

- envoyiez de l'argent ou des bons-cadeaux
- cliquiez sur des liens ou des pièces jointes malveillant(e)s
- révéliez des informations sensibles comme des mots de passe.

Les cybercriminels peuvent tenter d'arnaquer votre entreprise par le biais de courriels, de SMS et d'appels téléphoniques, ainsi que sur les réseaux sociaux. Souvent, ils se font passer pour une personne ou une organisation à laquelle vous faites confiance.

Les attaques d'hameçonnage

Parmi les plus grandes menaces à l'égard des petites entreprises figurent les **attaques d'hameçonnage**. Ces types d'arnaques contiennent souvent un lien vers un site Internet fictif où vous êtes encouragé·e à vous connecter à un compte ou à saisir des détails confidentiels.

Les attaques d'hameçonnage compromettent généralement les mots de passe de vos comptes. Les cybercriminels recourent fréquemment à cette méthodes pour « prendre le contrôle » des comptes de réseaux sociaux des petites entreprises et demander une rançon.

Moyens permettant d'atténuer ces risques

Si un message provient d'une entité connue, mais qu'il semble suspect, soyez prudent·e. Contactez la personne ou l'entreprise séparément pour vérifier si le message est légitime. Utilisez les coordonnées figurant sur une source légitime – par exemple, en accédant au site Internet officiel de l'entreprise – et non pas celles qui sont indiquées dans le message suspect.

Les ressources suivantes fournissent des informations complémentaires sur l'identification des arnaques et des attaques d'hameçonnage :

- Reconnaissez les arnaques et signalez-les
- Apprenez à repérer les arnaques d'hameçonnage
- Reconnaissance des messages d'ingénierie sociale.

Étude de cas :

Une employée d'une société de coursiers a reçu un courriel de l'un de ses supérieurs lui demandant d'acheter 6 cartes de crédit MasterCard prépayées de 500 $. Le supérieur lui a dit de n'en parler à personne car les cartes seront des bons-cadeaux pour les membres du personnel. Une fois cet achat effectué, l'employée a été priée de photographier les deux côtés des cartes et d'envoyer les photos à son supérieur à titre de preuve d'achat.

Conformément aux instructions, l'employée est allée à la poste et a utilisé sa carte de crédit personnelle pour acheter les bons-cadeaux. Elle a ensuite répondu au courriel de son supérieur en lui envoyant des photos des bons-cadeaux à titre de preuve.

Une fois de retour de la poste, l'employée a remis les cartes physiques à son supérieur, qui n'en avait pas connaissance. Après un examen, **tous les courriels concernant les bons-cadeaux provenaient d'une adresse électronique aléatoire et non pas du compte de messagerie légitime du supérieur de l'employée. Il s'agissait d'une arnaque.**

Les attaques par courriel

Outre les arnaques telles que l'hameçonnage, l'une des attaques par courriel ciblant fréquemment les petites entreprises est **l'arnaque du faux dirigeant d'entreprise**. Les criminels peuvent se faire passer pour des responsables d'entreprise en utilisant des comptes de messagerie électronique compromis ou d'autres moyens – par exemple, un nom de domaine similaire à celui d'une entreprise existante. Outre le vol d'informations, l'objectif de ces attaques est généralement d'inciter leurs victimes à envoyer des fonds sur un compte bancaire contrôlé par l'arnaqueur.

Moyens permettant d'atténuer ces risques

La meilleure parade contre les attaques par courriel consiste à former et à sensibiliser vos employés. Veillez à ce que votre personnel sache qu'il doit toujours faire attention aux courriels présentant les caractéristiques suivantes :

- ils contiennent des demandes de paiements, surtout s'il est indiqué qu'elles sont urgentes ou en souffrance
- ils annoncent un changement de coordonnées bancaires
- ils proviennent d'une adresse électronique qui ne semble pas tout à faire correcte – par exemple, le nom de domaine ne correspond pas exactement au nom de l'entreprise du fournisseur.

Bien que de telles attaques puissent être dévastatrices, les mesures permettant de les atténuer sont simples et ne coûtent presque rien. **Quand un employé reçoit un courriel comme celui-ci, le moyen le plus efficace pour réduire les risques consiste à appeler l'expéditeur pour confirmer la légitimité du courriel.** N'utilisez pas les coordonnées figurant dans le message que vous avez reçu car elles pourraient être frauduleuses. Mettez en place un processus officiel permettant au personnel d'effectuer un suivi des dates de réception des demandes de paiements ou de changement des coordonnées bancaires.

Apprenez à protéger votre entreprise contre les arnaques de faux dirigeant d'entreprise en vous appuyant sur les ressources suivantes :

- L'arnaque du faux dirigeant d'entreprise
- Protégez votre entreprise contre les fraudes et les arnaques par courriel
- Mesures à prendre si une fraude ou une arnaque par courriel a ciblé votre entreprise.

Étude de cas :

Une petite entreprise de construction a reçu un courriel de son fournisseur l'informant qu'il a changé de banque. Le fournisseur a fourni les coordonnées du nouveau compte pour les paiements de factures. Du fait que le courriel semblait légitime, **l'entreprise de construction n'a pas appelé le fournisseur pour confirmer le changement de ses coordonnées bancaires.**

L'entreprise a payé une facture du fournisseur de plus de 70 000 $. Le lendemain, un autre employé a payé une nouvelle fois la même facture par erreur, versant un montant supplémentaire de plus de 70 000$. Au total, plus de 150 000 $ ont ainsi été payés sur le nouveau compte bancaire.

Quand l'entreprise a appelé son fournisseur pour lui demander s'il pouvait rembourser le paiement dupliqué, le fournisseur l'a informée que les coordonnées bancaires n'étaient pas les bonnes. Une enquête a immédiatement été lancée et le fournisseur a découvert que l'un de ses comptes de messagerie électronique avait été piraté et qu'il avait été utilisé pour envoyer des coordonnées de compte bancaire frauduleux. **Aucun fonds n'a été recouvré.**

Les logiciels malveillants

Logiciel malveillant est une expression générale qui désigne un logiciel nuisible conçu pour faire du tort, comme les logiciels rançonneurs, les virus, les logiciels espions et les chevaux de Troie. Un logiciel malveillant peut :

- voler ou verrouiller les fichiers sur votre appareil
- voler vos numéros de cartes bancaires ou de crédit
- voler vos noms d'utilisateur et mots de passe
- espionner sur votre ordinateur ou en prendre le contrôle

Un logiciel malveillant peut empêcher votre appareil de fonctionner correctement, supprimer ou corrompre vos fichiers ou permettre à d'autres personnes d'accéder à vos informations à caractère personnel ou aux informations de votre entreprise. Si votre appareil est infecté par un logiciel malveillant, vous pourriez être exposé·e à d'autres attaques. Le logiciel malveillant pourrait se propager sur d'autres appareils raccordés à votre réseau.

Un certain nombre d'actions permettent à un logiciel malveillant d'infecter votre appareil, notamment :

- si vous accédez à des sites Internet qui ont été infectés par ce logiciel malveillant
- si vous téléchargez des fichiers ou des logiciels infectés sur Internet
- si vous ouvrez des fichiers infectés joints à un courriel

Les logiciels rançonneurs

Un logiciel rançonneur est un type de logiciel malveillant courant et dangereux. Il est conçu pour verrouiller ou crypter vos fichiers afin que vous ne puissiez plus y accéder. Une rançon vous est alors demandée, généralement sous forme de cryptomonnaie, pour rétablir votre accès aux fichiers. Les cybercriminels peuvent également menacer de publier ou de vendre des données en ligne à moins que vous ne payiez une rançon.

Moyens permettant d'atténuer ces risques

Bien que les antivirus ou logiciels de sécurité puissent contribuer à vous protéger contre les logiciels malveillants, aucun logiciel n'est efficace à 100 %. Le personnel doit être vigilant avec les courriels, les sites Internet et les téléchargements de fichiers et mettre à jour régulièrement ses appareils pour rester protégé.

Consultez les ressources suivantes pour des informations complémentaires sur la protection de votre entreprise contre les logiciels rançonneurs :

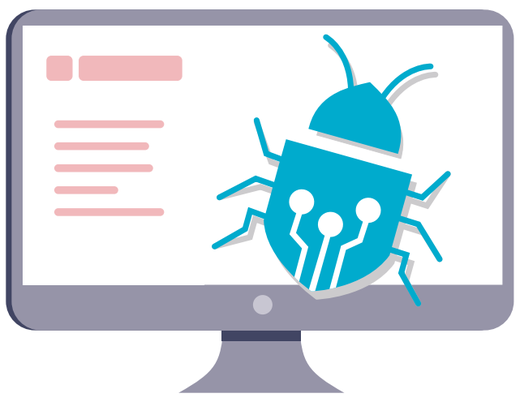
- Les logiciels rançonneurs
- Protégez-vous contre les attaques de logiciels rançonneurs
- Mesures à prendre si l'on vous demande une rançon.

Étude de cas :

Un matin, les employés d'un magasin de pièces automobiles sont arrivés au travail et n'ont pas pu démarrer leur serveur informatique. Quand leur prestataire de services informatiques a accédé au serveur, il a trouvé une fenêtre ouverte indiquant que toutes les données de l'ordinateur avaient été cryptées. La note demandait le paiement d'une rançon en bitcoins pour déverrouiller les fichiers.

Un disque de sauvegarde était raccordé à l'ordinateur, dont le contenu a également été crypté. Le prestataire a tenté de raccorder plus de disques de sauvegarde, mais en quelques secondes, les fichiers ont été automatiquement cryptés. **Le logiciel rançonneur n'avait pas été supprimé avant la tentative de recrouvement des données, et tous les fichiers de sauvegarde existants ont été perdus.**

La dernière option possible consistait à réinitialiser le serveur aux paramètres usine et à redémarrer à zéro avec un nouveau système. Leur entreprise a perdu de nombreuses années de données et elle a dû tout recommencer.



Sécurisation de vos comptes

Activez l'authentification multifactorielle

Avec l'authentification multifactorielle (AMF), l'accès de pirates informatiques à vos comptes est bien plus difficile.

L'AMF protège votre compte par une nouvelle couche de sécurité. Comme c'est l'une des méthodes les plus efficaces pour empêcher quelqu'un d'accéder à vos comptes, il est recommandé de l'utiliser aussi souvent que possible. Toute personne se connectant à votre compte doit non seulement fournir votre nom d'utilisateur et votre mot de passe, mais une autre information également. Il peut s'agir d'un code unique envoyé par SMS ou d'une appli. d'authentification. Pour de plus amples informations, veuillez consulter nos conseils sur l'AMF en accédant au site **cyber.gov.au/mfa**.

✓ **Activez l'AMF chaque fois que c'est possible, en commençant par vos comptes les plus importants.**

Mise en œuvre de contrôles d'accès

Des mesures de limitation de l'accès des utilisateurs permettent de réduire les dommages découlant d'un incident de cybersécurité.

Le contrôle des accès vise à restreindre l'accès à certains fichiers et systèmes. En général, le personnel n'a pas besoin d'un accès complet à toutes les données et à tous les comptes et systèmes au sein d'une entreprise. Il ne doit pouvoir accéder qu'aux informations dont il a besoin pour assumer ses obligations.

Des mesures de limitation de l'accès contribuent à réduire les dommages découlant d'un incident de cybersécurité. Par exemple, si l'ordinateur d'un employé est infecté par un logiciel rançonneur mais que des contrôles appropriés des accès sont en place, le logiciel peut n'affecter qu'un nombre limité de fichier plutôt que l'ensemble de l'entreprise.

✓ **Veillez à ce que chaque utilisateur ne puisse accéder qu'aux informations dont il a besoin relativement à son rôle.**

Utilisez des mots de passe ou des phrases de passe renforcé(e)s

Protégez vos comptes contre les cybercriminels avec un mot de passe ou une phrase de passe renforcé(e).

Un grand nombre de petites entreprises sont confrontées à des cyberattaques suite à une utilisation inappropriée des mots de passe. Par exemple, un même mot de passe a été utilisé sur plusieurs comptes. Vous pouvez utiliser à la fois des gestionnaires de mots de passe et des phrases de passe pour créer des mots de passe renforcés.

Un **gestionnaire de mots de passe** est comme un coffre-fort virtuel pour vos mots de passe. Vous pouvez l'utiliser en vue de créer et de stocker des mots de passe renforcés et **uniques** pour chacun de vos comptes. Si vous avez beaucoup de comptes, cela vous évite d'avoir à vous souvenir de chacun des mots de passe. Vous n'avez pas besoin de vous rappeler des mots de passe ou des comptes qui y sont associés car tout est enregistré dans votre gestionnaire de mots de passe.

S'agissant des comptes auxquels vous vous connectez régulièrement ou pour lesquels vous ne souhaitez pas enregistrer de mot de passe dans un gestionnaire de mots de passe, envisagez d'utiliser une phrase de passe plutôt qu'un mot de passe. Les phrases de passe sont une combinaison de mots aléatoires – par exemple, « cristal oignon argile bretzel ». Elles sont utiles quand vous souhaitez avoir un mot de passe renforcé dont vous pouvez vous souvenir facilement. Utilisez un mélange aléatoire unique d'au moins quatre mots – **ne réutilisez pas une même phrase de passe** pour plusieurs comptes. Pour des informations complémentaires, consultez nos conseils sur les phrases de passe et les gestionnaires de mots de passe en accédant au site **cyber.gov.au/passphrases**.

✓ **Utilisez un gestionnaire de mots de passe afin de créer et de stocker des mots de passe uniques pour chacun de vos comptes importants.**

Gestion de comptes partagés

Le partage de comptes peut compromettre la sécurité et compliquer le processus d'identification d'activités malveillantes.

Dans une petite entreprise, il peut y avoir des raisons légitimes pour lesquelles des employés doivent partager des comptes, mais il est préférable de l'éviter autant que possible. Quand plusieurs employés utilisent un même compte, il peut être difficile d'attribuer la conduite d'activités à un employé spécifique, et encore plus ardu de repérer les activités de piratage de cybercriminels. À moins que vous ne changiez le mot de passe, les employés pourraient également continuer à accéder aux comptes, même après avoir quitté l'entreprise.

✓ **Limitez l'utilisation de comptes partagés et sécurisez tous ceux qui sont utilisés dans votre entreprise.**

Protégez vos appareils et vos informations

Mettez vos logiciels à jour

Le maintien de vos logiciels à jour est l'un des meilleurs moyens de protéger votre entreprise contre une cyberattaque.

Du fait que les mises à jour peuvent colmater des brèches de sécurité dans votre système d'exploitation et d'autres logiciels, il est plus difficile pour les cybercriminels de les pirater. Étant donné que de nouvelles failles sont constamment découvertes, n'ignorez pas les rappels de mise à jour. Une mise à jour régulière de vos logiciels permet de réduire le risque qu'un cybercriminel exploite une faiblesse connue pour exécuter un logiciel malveillant ou pirater votre appareil. Si vous avez besoin d'aide, le Centre australien de la cybersécurité (Australian Cyber Security Centre – ACSC) a publié des orientations sur les mises à jour.

Si votre appareil ou votre logiciel est trop ancien, les mises à jour ne sont pas nécessairement disponibles. Si le fabricant a cessé de prendre en charge le produit avec des mises à jour, vous devriez envisager de passer à un produit plus récent pour préserver votre sécurité. Parmi les systèmes qui ne font plus l'objet de mises à jour majeures figurent **iPhone 7** et **Microsoft Windows 7**.

Pour des informations complémentaires, consultez nos orientations sur les mises à jour en accédant au site **cyber.gov.au/updates**.

✓ **Activez les mises à jour automatiques sur vos appareils et logiciels.**

Utilisez des logiciels de sécurité

Les logiciels de sécurité tels que les antivirus et une protection contre les logiciels rançonneurs peuvent contribuer à protéger vos appareils.

Utilisez un logiciel de sécurité pour repérer et supprimer les logiciels malveillants de vos appareils. Il est possible de configurer les logiciels antivirus de manière à contrôler régulièrement la présence de fichiers et de programmes douteux. Si une menace est trouvée, vous recevez une alerte et le fichier suspect est mis en quarantaine ou supprimé.

Un grand nombre de petites entreprises peuvent **utiliser Windows Security** pour se protéger contre les virus et les logiciels malveillants. Intégré dans les appareils sous Windows 10 et Windows 11, Windows Security comprend une protection gratuite contre les virus et les menaces. Vous pouvez également l'utiliser pour activer des fonctions de protection contre les logiciels rançonneurs sur votre appareil.

Pour d'autres produits et solutions, consultez nos conseils sur les logiciels antivirus en cherchant *antivirus* sur le site cyber.gov.au.

✓ **Configurez votre logiciel de sécurité de façon à ce qu'il analyse régulièrement vos appareils.**

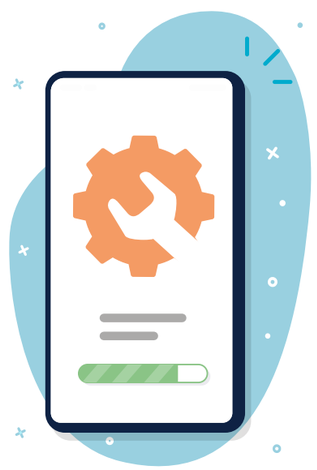
Sauvegardez vos informations

Des sauvegardes régulières peuvent vous aider à recouvrer vos informations si elles sont perdues ou compromises.

La sauvegarde des informations importantes doit être une procédure régulière ou automatique au sein de votre entreprise. Sans sauvegardes régulières, vous pourriez ne pas pouvoir recouvrer vos informations après une cyberattaque.

Les méthodes et les produits que vous pouvez utiliser pour sauvegarder vos informations sont nombreuses. Pour des conseils détaillés sur la sauvegarde des informations de votre entreprise, consultez nos conseils sur les sauvegardes en accédant au site **cyber.gov.au/backups**. Comme la meilleure option varie selon l'entreprise, parlez à un professionnel de l'informatique si vous avez des doutes.

✓ **Créez et mettez en œuvre un plan de sauvegarde régulière de vos informations**



Sécurisez votre réseau et vos services externes

Protégez votre entreprise contre les cyberattaques en remédiant aux vulnérabilités potentielles sur votre réseau.

Les appareils et les services raccordés à votre réseau peuvent être une cible de choix pour les cybercriminels. Étant donné qu'un grand nombre de ces systèmes peuvent être complexes à protéger, discutez des recommandations suivantes avec un professionnel de l'informatique.

- **Sécurisez vos serveurs** : Si vous utilisez un serveur en réseau ou un autre serveur chez vous ou dans votre entreprise, ne lésinez pas sur les précautions à prendre pour les sécuriser. Ces appareils sont souvent la cible des cybercriminels car ils stockent souvent des fichiers importants ou assument des fonctions clés. Un grand nombre de stratégies d'atténuation sont requises pour protéger ces appareils. Par exemple, il est important de veiller à ce que tous les serveurs ou les serveurs en réseau soient régulièrement mis à jour. Les comptes administratifs doivent être protégés par une phrase de passe renforcée ou par la fonction d'authentification multifactorielle.
- **Minimisez l'empreinte extérieure** : Contrôlez et sécurisez tous les services sur votre réseau qui sont exposés à l'Internet. Il peut notamment s'agir de Remote Desktop, de File Shares, de Webmail et de services d'administraiton à distance.
- **Migrez vers des services sur le Cloud :** Envisagez d'utiliser des services en ligne ou sur le Cloud qui offrent une sécurité intégrée, plutôt que de gérer cela vous-même. Par exemple, utilisez des services en ligne pour vos courriels ou l'hébergement d'un site Web au lieu d'exécuter et de sécuriser ces services vous-même.
- **Améliorez la sécurité de votre routeur :** Suivez nos orientations sur les moyens de sécuriser votre routeur, notamment en actualisant vos mots de passe par défaut, en activant une connexion WiFi « d'invité » pour vos clients ou visiteurs et en utilisant les protocoles de cryptage les plus efficaces. Pour des informations complémentaires, cherchez *router* (routeur) sur le site **cyber.gov.au**.
- **Comprenez votre chaîne d'approvisionnement en ligne :** Les entreprises modernes externalisent souvent une multitude de services. Par exemple, elles utilisent un prestataire de services gérés pour maintenir leur équipement informatique. Les problèmes de sécurité que rencontrent ces services ou prestataires pourraient avoir un impact considérable sur vos activités. Pour des conseils détaillés sur la gestion des risques dans la chaîne d'approvisionnement en ligne, consultez nos Orientations sur la chaîne d'approvisionnement en ligne en accédant au site **cyber.gov.au**.

✓ **Parlez à un professionnel de l'informatique des moyens permettant de sécuriser votre réseau.**

Renforcez votre site Internet

Les sites Internet sont une cible de choix pour les cyberattaques.

Protégez votre site Internet contre le piratage en appliquant certaines mesures de sécurité élémentaires :

- sécurisez les détails de connexion à votre site Internet avec la fonction d'authentification multifactorielle ou avec un mot de passe renforcé
- mettez régulièrement à jour les systèmes de gestion du contenu et les extensions de votre site Internet
- sauvegardez régulièrement votre site Internet afin de pouvoir le rétablir après une cyberattaque.

L'ACSC dispose de ressources supplémentaires à l'intention des propriétaires de sites Internet. Recherchez ces ressources sur le site **cyber.gov.au** :

- Des solutions rapides pour votre site Internet
- Mise en œuvre de certificats et de protocoles TLS, HTTPS et TLS opportuniste
- Sécurité des systèmes de noms de domaine pour les propriétaires de domaines
- Préparation et réponse à des attaques de déni de service

✓ **Consultez les ressources de l'ACSC sur la sécurité des sites Internet.**

Réinitialisez vos appareils avant de les vendre ou de les mettre au rebut

Des inconnus pourraient accéder aux données contenues dans vos anciens appareils.

Si vous n'assurez pas une mise au rebut sécurisée de vos appareils, des cybercriminels pourraient accéder aux informations qu'ils contiennent. Il peut s'agir de courriels, de fichiers et d'autres données de votre entreprise. Supprimez toutes les informations des appareils de votre entreprise avant de les vendre, de les échanger ou de les jeter. Par exemple, effectuez une réinitialisation aux paramètres usine. Cela contribuera à effacer toutes les informations et à rétablir les paramètres de l'appareil à ses réglages d'origine.

Pour des conseils en matière de réinitialisation de vos appareils, veuillez lire nos orientations sur la mise au rebut sécurisée de vos appareils. Recherchez *dispose* (mise au rebut) sur le site **cyber.gov.au**.

✓ **Effectuez une réinitialisation aux paramètres usine avant de vendre ou de mettre au rebut les appareils de votre entreprise.**

Gardez vos appareils verrouillés et physiquement sécurisés

Des mesures de limitation de l'accès aux appareils de votre entreprise permettent de réduire les risques d'activités malveillantes.

La restriction de l'accès physique aux appareils de votre entreprise offre une solution simple pour empêcher le vol de vos données ou autres activités malveillantes. Les appareils de votre entreprise ne doivent pas être conservés si du personnel non autorisé ou des personnes extérieures ont pu y accéder.

Utilisez des contrôles de sécurité pour mieux protéger les appareils de votre entreprise. Au minimum, ils doivent être verrouillés par une phrase de passe, un code PIN ou une fonction d'authentification biométrique. Assurez-vous que ces appareils sont réglés de manière à se verrouiller automatiquement après une courte période d'inactivité.

✓ **Configurez les appareils afin qu'ils se verrouillent automatiquement après une courte période d'inactivité.**

Protégez les données de votre entreprise

Les données détenues par votre entreprise représentent une cible attrayante pour les cybercriminels.

Les violations de données sont en hausse – assurez-vous que votre entreprise n'en devient pas une victime. Il est important de comprendre les données que détient votre entreprise et où elles sont stockées. Une fois que vous détenez ces informations, suivez les recommandations figurant dans ce guide pour vous aider à protéger vos données contre l'accès de cybercriminels. Certaines petites entreprises peuvent également être assujetties à des obligations supplémentaires en vertu de la loi.

- **Consolidez les données de votre entreprise.** Il se peut que vos données soient stockées sur un grand nombre d'appareils ou de services. Quand des données sont décentralisées, cela augmente le nombre de systèmes dont vous devez assurer la protection et la sauvegarde. Une multiplicité de systèmes peut également offrir plus d'opportunités d'attaques aux cybercriminels. Dans la mesure du possible, stockez les données de votre entreprise dans un lieu central qui est régulièrement sécurisé et sauvegardé. Étant donné que la centralisation de vos données peut déboucher sur une violation plus importante si vos systèmes sont compromis, veillez à ce que ce lieu central bénéficie d'une protection adéquate avec des configurations sûres et un accès restreint. Parlez à un professionnel de l'informatique ou de la cybersécurité pour lui demander conseil.
- **Connaissez vos obligations en termes de protection des données.** Certaines petites entreprises peuvent être soumises à des obligations légales en matière de traitement des informations qu'elles recueillent. Pour des informations complémentaires, veuillez lire le guide à l'intention des petites entreprises du Commissariat australien à l'information, disponible sur le site **oaic.gov.au**. Consultez un conseiller juridique en cas de doute.

✓ **Comprenez les données que détient votre entreprise et vos responsabilités relativement à leur protection.**

Préparez votre personnel

Éduquez vos employés

L'application de pratiques de cybersécurité efficaces par vos employés constitue votre première ligne de défense contre les cyberattaques.

Vos employés doivent posséder des connaissances sur la cybersécurité, notamment sur les sujets suivants :

- les menaces courantes à la cybersécurité telles que l'arnaque du faux dirigeant d'entreprise et les logiciels rançonneurs
- les diverses mesures de protection existantes, notamment les mots de passe ou les phrases de passe renforcé(e)s, la fonction d'AMF et les mises à jour logicielles
- la manière de repérer des arnaques et des attaques d'hameçonnage
- les politiques spécifiques de l'entreprise (par exemple, les processus de signalement de courriels suspects ou de validation de la légitimité des factures avant leur paiement)
- ce qu'il faut faire en cas d'urgence.

Le site Internet de l'ACSC propose des ressources sur la plupart de ces sujets, à l'adresse cyber.gov.au/learn. Vous pourriez envisager d'autres moyens d'éduquer vos employés, par exemple, dans le cadre d'un cours formel ou d'une formation interne. Quelle que soit votre décision, souvenez-vous que les formations à la cybersécurité ne sont pas une exigence ponctuelle, mais qu'elles nécessitent des remises à niveau régulières.

✓ **Déterminez la manière dont la cybersécurité sera enseignée au sein de votre entreprise.**

Élaborez un plan d'urgence

Un plan d'urgence pourrait réduire l'impact d'une cyberattaque sur votre entreprise.

Face à un incident de cybersécurité, chaque minute compte. Grâce à un plan d'urgence, votre personnel peut consacrer moins de temps à chercher une solution et plus de temps à agir.

Lors de la création de votre plan d'urgence, examinez les questions suivantes :

- Par quel processus votre personnel signale-t-il les incidents de cybersécurité potentiels ?
- Qui contactez-vous pour obtenir de l'aide ? Par exemple,des professionnels de l'informatique et votre banque.
- Comment l'incident sera-t-il communiqué à votre personnel, vos parties prenantes ou vos clients ?
- Comment maintiendrez-vous le cours normal des opérations si des systèmes critiques sont hors ligne ?

Veillez à ce que votre personnel soit familiarisé avec le plan d'urgence, notamment toutes les fonctions ou les responsabilités qu'il peut devoir assumer. Conservez une copie imprimée du plan pour le cas où vous en auriez besoin mais que vos systèmes seraient hors ligne.

✓ **Créez un plan d'urgence pour les incidents de cybersécurité.**

Tenez-vous informé·e

Devenez une entreprise partenaire de l'ACSC pour recevoir les dernières informations de l'ACSC.

Restez informé·e des dernières cybermenaces et vulnérabilités en devenant une entreprise partenaire de l'ACSC. Ce service vous enverra des bulletins d'information mensuels et des alertes chaque fois qu'une nouvelle cybermenace est identifiée.

La cybersécurité est un domaine qui évolue rapidement. Dès que les cybercriminels découvrent des vulnérabilités, il ne leur faut que quelques minutes pour les exploiter activement. En vous tenant au courant de l'évolution de la cybersécurité, vous serez en mesure de comprendre les menaces auxquelles votre entreprise est susceptible de faire face et la manière de l'en protéger.

✓ **Inscrivez votre entreprise au programme de partenariat de l'ACSC.**

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 2023

Hormis le blason et sauf déclaration contraire, tous les éléments figurant dans cette publication sont fournis en vertu de la licence internationale Creative Commons Attribution 4.0 (www.creativecommons.org/licenses).

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 la licence pertinente sont disponibles sur le site Internet de Creative Commons, de même que le code légal complet au titre de la licence CC BY 4.0 (www.creativecommons.org/licenses).

Utilisation du blason

Les conditions dans lesquelles il est possible d'utiliser le blason sont présentées sur le site Internet du ministère du Premier ministre et du Cabinet (www.pmc.gov.au/government/commonwealth-coat-arms).

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