ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Government
Australian Signals Directorate

المصالح التجارية الصغيرة
دليل الأمن السيبراني

تعقيد المحتوى
بسيط ○○●

cyber.gov.au

المقدّمة

بالنسبة لمصلحة تجارية صغيرة، قد تكون حتى لحادث أمن سيبراني بسيط آثار مدمّرة. يتضمن هذا الدليل تدابير أمنية أساسية للمساعدة في حماية مصلحتك التجارية من التهديدات الشائعة للأمن السيبراني . كنقطة انطلاق، نوصي باتخاذ التدابير الثلاثة التالية:

- **شغّل المصادقة متعددة العوامل**
- **حدّث برنامج الكومبيوتر لديك**
- **احتفظ بنسخة احتياطية لمعلوماتك**

قد يتضمن هذا الدليل تدابير لا صلة لها بمصلحتك التجارية أو قد تكون لمصلحتك التجارية احتياجات أكثر تعقيداً. بعد الانتهاء من هذا الدليل، نوصي المصالح التجارية الصغيرة بتطبيق Maturity Level One من Essential Eight. إذا كانت لديك أسئلة حول هذه النصيحة أو الأمن السيبراني بشكل أوسع، فإننا نوصيك بالتحدث إلى متخصّص في تكنولوجيا المعلومات أو مستشار موثوق به.

قم بزيارة cyber.gov.au لقراءة دليلنا بالكامل، بما في ذلك النصيحة عن كيفية تطبيق كل تدبير

جدول المحتويات

التهديدات للمصالح التجارية الصغيرة 4
رسائل احتيال 4
هجمات البريد الإلكتروني 5
البرمجيات الخبيثة 6
أمّن حساباتك 7
شغّل المصادقة متعددة العوامل 7
استخدم كلمات مرور أو عبارات مرور قوية 7
أدِر الحسابات المشتركة 7
طبّق ضوابط الدخول 7
احمِ أجهزتك ومعلوماتك 8
حدّث برنامج الكومبيوتر لديك 8
احتفظ بنسخة احتياطية لمعلوماتك 8
استخدم برنامج الأمان 8
أمّن شبكتك وخدماتك الخارجية 9
عزّز حماية موقعك الإلكتروني 9
أعد ضبط أجهزتك قبل بيعها أو التخلص منها 9
احتفظ بأجهزتك مقفلة وموضوعة في مكان آمن 10
احمِ بيانات مصلحتك التجارية 10
جهّز موظفيك 11
ثقّف الموظفين 11
ضع خطة طوارئ 11
ابق على اطلاع 11

التهديدات للمصالح التجارية الصغيرة

رسائل احتيال

عمليات الاحتيال طريقة شائعة يستهدف بها مجرمو الإنترنت المصالح التجارية الصغيرة. هدفهم هو خداعك أنت أو موظفيك لـ:

- إرسال نقود أو بطاقات هدايا
- الضغط على روابط أو مرفقات خبيثة
- إعطاء معلومات حساسة، مثل كلمات السر.

قد يحاول مجرمو الإنترنت الاحتيال على مصلحتك التجارية من خلال البريد الإلكتروني والرسائل النصية والمكالمات الهاتفية ووسائل التواصل الاجتماعي. غالباً ما يتظاهر المحتالون بأنهم شخص أو منظمة تثق بها.

هجمات التصيّد الاحتيالي

ما يثير قلق المصالح التجارية الصغيرة بشكل خاص **هجمات التصيّد الاحتيالي** غالبًا ما تحتوي عمليات الاحتيال هذه على رابط لموقع إلكتروني مزيّف حيث يتم تشجيعك على تسجيل الدخول إلى حساب أو إدخال تفاصيل سرية.

تؤدي هجمات التصيّد الاحتيالي عادةً إلى اختراق كلمات مرور حسابك. غالبًا ما يستخدم مجرمو الإنترنت هذه الطريقة «للاستحواذ» على حسابات وسائل التواصل الاجتماعي للمصالح التجارية الصغيرة وإخضاعها للفدية.

طرق التخفيف

إذا كانت الرسالة من جهة معروفة وبدت مشبوهة، كن حذراً. اتصل بالشخص أو المصلحة التجارية بشكل منفصل للتحقّق مما إذا كانت الرسالة صحيحة. استخدم تفاصيل الاتصال التي تجدها من خلال مصدر شرعي، على سبيل المثال من خلال زيارة الموقع الرسمي للمصلحة التجارية، وليس ذلك الوارد في الرسالة المشبوهة.

اعرف المزيد عن تحديد عمليات الاحتيال وهجمات التصيّد الاحتيالي بالموارد التالية:

- تعرّف على عمليات الاحتيال وبلّغ عنها
- تعلّم كيفية اكتشاف عمليات التصيّد الاحتيالي
- الكشف عن الرسائل المهندسة اجتماعيًا

دراسة حالة:

تلقّت موظفة في شركة للبريد السريع رسالة عبر البريد إلكتروني من أحد مدرائها التنفيذيين، يطلب منها شراء 6 × 500 دولار من بطاقات ائتمان المدفوعة Mastercard مسبقًا. طلب منها المدير التنفيذي أن تُبقي الأمر سرّاً لأن البطاقات ستكون قسائم هدايا للموظفين. ما أن تمّ شراؤها، حتى طُلب من الموظفة تصوير جانبيْ البطاقات وإرسالها إلى المدير التنفيذي كدليل على الشراء.

وفقًا للتعليمات، ذهبت الموظفة إلى مكتب بريد واستخدمت بطاقتها الائتمانية الشخصية لشراء بطاقات الهدايا. ردّت على البريد الإلكتروني للمدير التنفيذي وأرسلت صور بطاقات الهدايا كدليل.

بعد عودتها من مكتب البريد، أعطت الموظفة البطاقات الفعلية للمدير التنفيذي - الذي لم يكن على علم بها. لدى المراجعة **جاءت جميع رسائل البريد الإلكتروني بشأن بطاقات الهدايا من عنوان بريد إلكتروني عشوائي ولم تكن من حساب البريد الإلكتروني الشرعي للمدير التنفيذي. لقد كانت عملية احتيال.**

هجمات البريد الإلكتروني

بالإضافة إلى عمليات الاحتيال مثل التصيّد الاحتيالي، فإن هجومًا شائعاً بالبريد الإلكتروني ضد المصالح التجارية الصغيرة هو **اختراق البريد الإلكتروني للمصالح**(BEC). يمكن للمجرمين انتحال شخصية ممثلي المصلحة التجارية باستخدام حسابات البريد الإلكتروني المخترقة، أو من خلال وسائل أخرى - مثل استخدام اسم نطاق يشبه المصلحة الحقيقية. بالإضافة إلى سرقة المعلومات، الهدف من هذه الهجمات عادة هو خداع الضحايا لإرسال الأموال إلى حساب مصرفي يديره المحتال.

طرق التخفيف

أفضل دفاع ضد هجمات البريد الإلكتروني هو تدريب موظفيك وتوعيتهم . تأكّد من أن موظفيك يعرفون توخي الحذر دائمًا من رسائل البريد الإلكتروني التي تتضمّن ما يلي:

- طلبات دفع، خاصة إذا كانت عاجلة أو متأخرة
- تغيير تفاصيل الحساب المصرفي
- عنوان بريد إلكتروني لا يبدو صحيحًا تمامًا، مثل اسم النطاق الذي لا يطابق بالضبط اسم شركة المورّد.

في حين أن هذه الهجمات يمكن أن تكون مدمّرة، فإن تدابير التخفيف منها سهلة ولا تكلّف شيئًا تقريبًا. **عندما يتلقّى الموظفون رسائل بريد إلكتروني مثل هذه، فإن أكثر الطرق فعالية للتخفيف منها هو الاتصال بالمرسل للتأكد من شرعيتها.** لا تستخدم تفاصيل الاتصال التي تم إرسالها إليك لأنها قد تكون احتيالية. استحدث عملية رسمية يتّبعها الموظفون لدى استلام طلبات الدفع أو تغيير التفاصيل المصرفية.

تعلّم حماية مصلحتك التجارية من عمليات احتيال BEC واختراق البريد الإلكتروني بالموارد التالية:

- اختراق البريد الإلكتروني للمصالح
- احم مصلحتك التجارية من عمليات الاحتيال والاختراق عبر البريد الإلكتروني
- ماذا تفعل إذا استُهدفت مصلحتك التجارية بعمليات احتيال أو اختراق عبر البريد الإلكتروني

دراسة حالة:

تلقّت مصلحة صغيرة للبناء رسالة بريد إلكتروني من مورّدها تفيد بأنه غيّر تفاصيله المصرفية. قدّم المورّد تفاصيل حسابات جديدة لدفع الفواتير. بما أنّ البريد الإلكتروني بدا شرعيًا، **لم تتصل مصلحة البناء بالمورّد لتأكيد التغيير في تفاصيل الحساب المصرفي.**

دفعت المصلحة فاتورة من المورّد بأكثر من 70 ألف دولار. في اليوم التالي، دفع موظف آخر عن طريق الخطأ نفس الفاتورة مرة أخرى مقابل مبلغ إضافي يزيد عن 70 ألف دولار. في المجموع، تم دفع أكثر من 150 ألف دولار للحساب المصرفي الجديد.

عندما اتصلت المصلحة التجارية بمورّدها لتسأل عما إذا كان بإمكانهم ردّ الدفعة المزدوجة، أبلغهم المورّد أن تلك التفاصيل المصرفية كانت غير صحيحة. تمّ فتح تحقيق على الفور، واكتشف المورّد أنه تمّ اختراق أحد حسابات بريده الإلكتروني وكان يُرسل تفاصيل حسابات مصرفية احتيالية. **لم يتمّ استرداد أي أموال**

البرمجيات الخبيثة

البرامج الضارة هي مصطلح شامل للبرامج الخبيثة المصممة لإحداث ضرر، مثل برامج الفدية والفيروسات وبرامج التجسس وأحصنة طروادة. يمكن للبرامج الضارّة :

- سرقة أو إقفال الملفات في جهازك
- سرقة أرقام حسابك المصرفي أو بطاقات الائتمان الخاصة بك
- سرقة أسماء المستخدم وكلمات المرور الخاصة بك
- السيطرة أو التجسس على جهاز الكومبيوتر الخاص بك.

يمكن للبرامج الضارة منع جهازك من العمل بشكل صحيح، أو حذف ملفاتك ،أو إفسادها ، أو السماح للآخرين بالوصول إلى معلوماتك الشخصية أو التجارية. إذا كان جهازك مصابًا ببرامج ضارة، فقد تكون عرضة لهجمات أخرى. يمكن أن يمتدّ البرنامج الضار أيضًا إلى أجهزة أخرى على شبكتك.

يمكن أن يصاب جهازك ببرامج ضارة بعدة طرق، بما في ذلك:

- زيارة مواقع إلكترونية أصيبت ببرامج ضارة
- تحميل ملفات أو برامج مصابة من الإنترنت
- فتح مرفقات البريد الإلكتروني المصابة.

برامج الفدية

برامج الفدية نوع شائع وخطير من البرامج الضارة. إنها تعمل عن طريق إقفال أو تشفير ملفاتك حتى لا يعود بإمكانك الوصول إليها. يُطلب فدية، عادة في شكل عملة مشفرة، لاستعادة الوصول إلى الملفات. قد يهدد مجرمو الإنترنت أيضًا بنشر أو بيع البيانات عبر الإنترنت، ما لم يتمّ دفع فدية.

طرق التخفيف

في حين أن برامج مكافحة الفيروسات أو برامج الأمان يمكن أن تساعد في حمايتك من البرامج الضارّة، لا يوجد برنامج فعّال بنسبة 100٪. يجب على الموظفين أن يكونوا متيقظين بشأن رسائل البريد الإلكتروني والمواقع الإلكترونية وتحميل الملفات، وعليهم أن يُحدّثوا أجهزتهم بانتظام للبقاء في أمان.

راجع الموارد التالية لمزيد من المعلومات حول حماية مصلحتك التجارية من برامج الفدية:

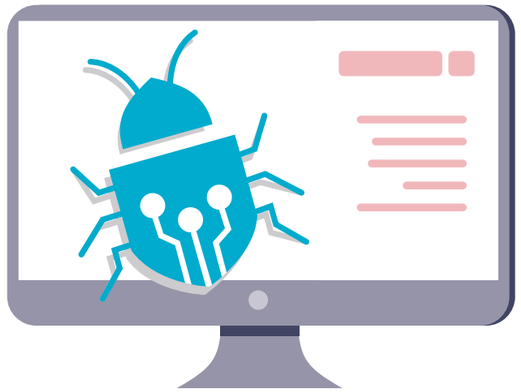
- برامج الفدية
- احم نفسك من هجمات برامج الفدية
- ما يجب فعله إذا كنت رهينة لفدية.

دراسة حالة:

جاء موظفو متجر قطع غيار سيارات إلى العمل ذات صباح ولم يتمكنوا من بدء تشغيل خادم جهاز الكومبيوتر الخاص بهم. عندما تمكّن مزوّد تكنولوجيا المعلومات الخاص بهم من الوصول إلى الخادم، وجدوا نافذة مفتوحة تقول إنه تمّ تشفير جميع بيانات الكومبيوتر. طالبت المذكرة بدفع فدية بعملة البيتكوين لفتح الملفات.

كان هناك محرّك أقراص احتياطي موصول بالكومبيوتر، وقد تم تشفيره أيضًا. حاولوا توصيل المزيد من محرّكات الأقراص الاحتياطية، غير أنّ الملفات تمّ تشفيرها تلقائيًا في غضون ثوانٍ. **لقد فشلوا في إزالة برامج الفدية قبل محاولة استعادة بياناتهم وفقدوا كلّ ملف احتياطي لديهم.**

كان الخيار الوحيد المتبقي هو إعادة ضبط الخادم على إعدادات المصنع الأصلية والبدء من جديد بنظام جديد. فقدت مصلحتهم التجارية بيانات عن عدة سنوات واضطروا إلى البدء من جديد.



أمّن حساباتك

شغّل المصادقة متعددة العوامل

تصعّب المصادقة متعددة العوامل (MFA) على مجرمي الإنترنت الوصول إلى حساباتك.

تضيف MFA طبقة أخرى من الأمان إلى حسابك. إنها واحدة من أكثر الطرق فعالية لحماية حساباتك من وصول شخص ما إليها، لذلك يجب أن تستخدمها حيثما أمكن ذلك. سيحتاج أي شخص يقوم بتسجيل الدخول إلى حسابك إلى تقديم شيء آخر بالإضافة إلى اسم المستخدم وكلمة المرور الخاصيْن بك. يمكن أن يكون هذا رمزًا فريدًا من رسالة نصية أو تطبيق مصادقة. لمزيد من المعلومات، إقرأ نصيحتنا حول MFA، المتاحة على **cyber.gov.au/mfa** .

✓ شغّل MFA حيثما أمكن ذلك، بدءًا من أهم حساباتك.

طبّق ضوابط الدخول

يمكن أن يحدّ حظر وصول المستخدم من الضرر الناجم عن حادث أمن سيبراني.

التحكّم في الوصول هو وسيلة للحدّ من الوصول إلى بعض الملفات والأنظمة. إجمالاً، لا يحتاج الموظفون إلى الوصول الكامل إلى جميع البيانات والحسابات والنظم في المصلحة التجارية. يجب السماح لهم فقط بالوصول إلى ما يحتاجون إليه لأداء واجباتهم.

يساعد حظر الوصول في الحد من الضرر الناجم عن حادث أمن سيبراني. على سبيل المثال، إذا أصيب جهاز الكومبيوتر الخاص بموظف ما ببرنامج الفدية، مع تشغيل ضوابط الوصول المناسبة، فقد يؤثر فقط على عدد صغير من الملفات بدلاً من المصلحة التجارية بأكملها.

✓ تأكد من أنّ بإمكان كل مستخدم الوصول فقط إلى ما يحتاجه للدور الذي يؤديه.

استخدم كلمات مرور أو عبارات مرور قوية

احمِ حساباتك من مجرمي الإنترنت بكلمة مرور أو عبارة مرور آمنة.

تواجه العديد من المصالح التجارية الصغيرة هجمات إلكترونية نتيجة سلوكيات استعمال كلمة مرور ضعيفة. على سبيل المثال، إعادة استخدام نفس كلمة المرور في حسابات متعددة. يمكنك استخدام كل من مدراء كلمات المرور وعبارات المرور لإنشاء كلمات مرور قوية.

يعمل **مدير كلمة المرور** مثل خزنة افتراضية لكلمات المرور لديك. يمكنك استخدامه لإنشاء وتخزين كلمات مرور قوية، **وفريدة** لكل حساب من حساباتك. إذا كان لديك الكثير من الحسابات، فهذا يزيل عبء تذكّر كلمات المرور الفريدة. لا يتعيّن عليك تذكّر كلمات المرور أو الحسابات التي تعود إليها، حيث يتمّ تسجيل كل ذلك في مدير كلمة المرور الخاص بك.

بالنسبة للحسابات التي تسجّل الدخول إليها بانتظام، أو خلافاً لذلك، تلك التي لا ترغب في تخزينها في مدير كلمات المرور، فكّر في استخدام عبارة مرور ككلمة مرور. عبارات المرور هي مزيج من كلمات عشوائية، على سبيل المثال «كريستال بصل طين بريتزل». إنها مفيدة عندما تريد كلمة مرور آمنة يسهل تذكّرها. استخدم مزيجًا عشوائيًا من أربع كلمات أو أكثر واجعله فريدًا - **لا تُعد استخدام عبارة مرور** عبر حسابات متعددة. لمزيد من المعلومات، إقرأ نصيحتنا حول عبارات المرور ومدراء كلمة المرور، المتاحة على **cyber.gov.au/passphrases**.

✓ يمكنك استخدام مدير كلمة المرور لإنشاء وتخزين كلمات مرور فريدة لكل حساب من حساباتك.

أدِر الحسابات المشتركة

يمكن لمشاركة الحسابات أن تعرّض الأمان للخطر وتجعل من الصعب تتبّع النشاط الضار.

في مصلحة تجارية صغيرة، قد تكون هناك أسباب مشروعة لحاجة الموظفين إلى تقاسم الحسابات، ولكن يجب تجنبّها قدر الإمكان. عندما يستخدم العديد من الموظفين نفس الحساب، قد يكون من الصعب تتبّع نشاط موظف معيّن وحتى من الأصعب تتبّع مجرمي الإنترنت الذين يخترقون الحساب. ما لم تقم بتغيير كلمة المرور، يمكن للموظفين أيضًا الاستمرار في الوصول إلى الحسابات حتى بعد تركهم العمل.

✓ ضع حدّاً لاستخدام الحسابات المشتركة وأمّن أي حسابات يتم استخدامها في مصلحتك التجارية.

احمِ أجهزتك ومعلوماتك

حدّث برنامج الكومبيوتر لديك

يُعدّ تحديث برنامج الكومبيوتر أحد أفضل الطرق لحماية مصلحتك التجارية من هجوم سيبراني.

يمكن أن تُصلح التحديثات العيوب الأمنية في نظام التشغيل الخاص بك والبرامج الأخرى، بحيث يصعب على مجرم الإنترنت اختراقها. يتم اكتشاف عيوب جديدة طوال الوقت، لذلك لا تتجاهل مطالبات التحديث سيؤدي التحديث المنتظم لبرنامجك إلى تقليل فرصة المجرم الإلكتروني من استخدام نقطة ضعف معروفة لتشغيل البرامج الضارة أو اختراق جهازك. إذا كنت بحاجة إلى المساعدة، فقد نشرت ACSC إرشادات حول التحديثات.

إذا كان جهازك أو برنامجك قديمًا جدًا، فقد لا تكون التحديثات متاحة. إذا توقفت الشركة المصنّعة عن دعم المنتج بالتحديثات، فيجب عليك التفكير في التحسين إلى منتج أحدث للبقاء آمنًا. الأمثلة على الأنظمة التي لم تعد تتلقى تحديثات رئيسية هي **iPhone 7** و **Microsoft Windows 7** .

لمزيد من المعلومات، اقرأ نصيحتنا حول الإرشادات بشأن التحديثات، المتاحة على **cyber.gov.au/updates**.

✓ شغّل التحديثات التلقائية لأجهزتك وبرامجك.

استخدم برنامج الأمان

يمكن أن تساعد برامج الأمان مثل المضادة للفيروسات والحماية ضدّ برامج الفدية في حماية أجهزتك.

استخدم برامج الأمان لاكتشاف البرامج الضارة وإزالتها من أجهزتك. يمكن إعداد برنامج مضاد للفيروسات لفحص الملفات والبرامج المشبوهة بانتظام. عند العثور على تهديد، ستتلقى تنبيهًا وسيتمّ عزل الملفّ المشبوه أو إزالته.

يمكن للعديد من المصالح التجارية الصغيرة **استخدام Windows Security** لحماية نفسها من الفيروسات والبرامج الضارة. إن Windows Security مدمج في أجهزة **Windows 10** و **Windows 11** ويتضمّن حماية مجانية من الفيروسات والتهديدات. يمكنك أيضًا استخدامه لتشغيل ميزات الحماية من برامج الفدية على جهازك.

للحصول على منتجات وخيارات بديلة، اقرأ نصائحنا حول البرنامج المضاد للفيروسات من خلال البحث عن مضادات الفيروسات على cyber.gov.au.

✓ ضع برنامج أمان لإكمال عمليات المسح المنتظمة على أجهزتك.

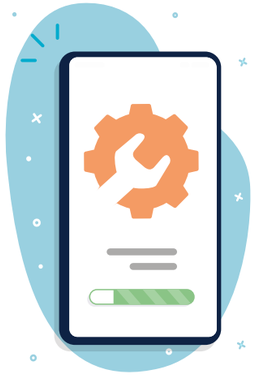
احتفظ بنسخة احتياطية لمعلوماتك

يمكن أن يساعدك النسخ الاحتياطي المنتظم في استعادة معلوماتك إذا فقدت أو تعرّضت للاختراق.

يجب أن يكون النسخ الاحتياطي للمعلومات المهمة ممارسة منتظمة أو تلقائية في مصلحتك التجارية. بدون إجراء نسخ احتياطي منتظم، قد يكون من المستحيل عليك استعادة معلوماتك بعد هجوم سيبراني.

هناك العديد من الطرق والمنتجات التي يمكنك استخدامها لإجراء نسخ احتياطي لمعلوماتك. للحصول على نصائح مفصلة حول النسخ الاحتياطي لبيانات مصلحتك التجارية، اقرأ نصائحنا للحصول على نسخ احتياطية ، متاحة على **cyber.gov.au/backups**. سيختلف الخيار الأفضل لكل مصلحة تجارية، لذا تحدّث مع أخصائي تكنولوجيا المعلومات إذا كنت غير متأكد.

✓ ضع خطة لإجراء نسخ احتياطي لمعلوماتك بانتظام ونفّذها.



أمّن شبكتك وخدماتك الخارجية

احمِ مصلحتك التجارية من هجوم سيبراني من خلال معالجة نقاط الضعف المحتملة في شبكتك.

يمكن أن تكون الأجهزة والخدمات في شبكتك هدفًا رئيسيًا لمجرمي الإنترنت. يمكن أن يكون العديد من هذه الأنظمة معقدة لتأمينها، لذا ناقش التوصيات التالية مع أخصائي تكنولوجيا المعلومات.

- **أمّن الخوادم الخاصة بك :** إذا كنت تستخدم **NAS** أو خادمًا آخر في منزلك أو مصلحتك التجارية، فاحرص على تأمينه. تشكّل هذه الأجهزة أهدافاً شائعة لمجرمي الإنترنت لأنها غالبًا ما تخزّن ملفات مهمة أو تؤدي وظائف مهمة. هناك العديد من استراتيجيات التخفيف المطلوبة لحماية هذه الأجهزة. على سبيل المثال، من المهم التأكد من تحديث أي خادم أو أجهزة **NAS** بانتظام. يجب تأمين الحسابات الإدارية بعبارة مرور قوية أو مصادقة متعددة العوامل.
- **قلّل إلى أدنى حدّ البصمة من الخارج** دقّق في أي خدمات إنترنت مكشوفة على شبكتك وأمّنها. قد يشمل ذلك الكومبيوتر المكتبي عن بُعد، ومشاركة الملفات، والبريد الإلكتروني، وخدمات الإدارة عن بُعد.
- **انتقل إلى الخدمات السحابية:** فكّر في استخدام الخدمات عبر الإنترنت أو السحابية التي توفر أمانًا مدمجًا، بدلاً من إدارة خدماتك الخاصة. على سبيل المثال، استخدم الخدمات عبر الإنترنت لأشياء مثل البريد الإلكتروني أو استضافة المواقع الإلكترونية بدلاً من تشغيل وتأمين هذه الخدمات بنفسك.
- **حسّن أمان جهاز التوجيه الخاص بك:** اتبع إرشاداتنا حول طرق تأمين جهاز التوجيه الخاص بك، بما في ذلك تحديث كلمات المرور الافتراضية، وتشغيل شبكة **Wi-Fi** «الضيف» للزبائن أو الزوار، واستخدام أقوى بروتوكولات التشفير. إبحث عن جهاز التوجيه على **cyber.gov.au** لمزيد من المعلومات.
- **افهم سلسلة التوريد السيبراني الخاصة بك:** غالبًا ما تستعين المصالح التجارية الحديثة بمصادر خارجية لخدمات متعددة. على سبيل المثال، استخدام مزوّد الخدمة المُدارة للحفاظ على تكنولوجيا المعلومات الخاصة بهم. يمكن أن يكون للمسائل الأمنية مع هذه الخدمات أو مقدمي الخدمات تأثير كبير على عملك. للحصول على مشورة مفصّلة حول إدارة مخاطر سلسلة التوريد السيبرانية، اقرأ إرشادات سلسلة التوريد السيبرانية الخاصة بنا على **cyber.gov.au**.

✓ تحدّث مع أخصائي تكنولوجيا المعلومات حول طرق تأمين شبكتك.

عزّز حماية موقعك الإلكتروني

تُعد المواقع الإلكترونية هدفًا رئيسيًا للهجمات السيبرانية.

احمِ موقعك الإلكتروني من القرصنة باتّباع بعض الإجراءات الأمنية الأساسية:

- أمّن تسجيل الدخول إلى موقعك الإلكتروني بمصادقة متعددة العوامل أو كلمة مرور قوية
- حدّث بانتظام أنظمة وملحقات إدارة محتوى موقعك على الإنترنت
- قم بالنسخ الاحتياطي المنتظم لموقعك الإلكتروني حتى تتمكن من استعادته بعد هجوم سيبراني.

لدى **ACSC** موارد إضافية متاحة لمالكي المواقع الإلكترونية. إبحث عن هذه الموارد على **cyber.gov.au**:

- مكاسب سريعة لموقعك الإلكتروني
- شهادات التنفيذ ، و ، و الانتهازية
- أمّن نظام اسم النطاق لأصحاب النطاق
- الاستعداد لهجمات حجب الخدمة والرد عليها

✓ اقرأ موارد ACSC حول أمن الموقع الإلكتروني.

أعد ضبط أجهزتك قبل بيعها أو التخلص منها

يمكن للغرباء الوصول إلى البيانات الموجودة على أجهزتك القديمة.

إذا لم تتخلّص من أجهزتك بشكل آمن، فيمكن لمجرمي الإنترنت الوصول إلى المعلومات الموجودة عليها. يمكن أن يشمل ذلك رسائل البريد الإلكتروني وملفات وبيانات أخرى للمصلحة التجارية. احذف جميع المعلومات من أجهزة مصلحتك التجارية قبل بيعها أو تداولها أو التخلص منها. على سبيل المثال، من خلال إعادة الضبط على إعدادات المصنع الأصلية. سيساعد ذلك في مسح أي معلومات وإعادة الجهاز إلى إعداداته الأصلية.

للحصول على المشورة بشأن إعادة ضبط أجهزتك، اقرأ إرشاداتنا حول كيفية التخلص من جهازك بأمان ابحث عن تخلص على **cyber.gov.au**.

✓ أعد ضبط أجهزة مصلحتك التجارية إلى إعدادات المصنع الأصلية قبل بيعها أو التخلص منها.

احتفظ بأجهزتك مقفلة وموضوعة في مكان آمن

سيؤدي تقييد الوصول إلى أجهزة مصلحتك التجارية إلى تقليل فرص النشاط الضار.

يُعد الحدّ من الوصول الفعلي إلى أجهزة مصلحتك التجارية طريقة بسيطة لمنع سرقة البيانات أو أي نشاط ضار آخر. لا ينبغي الاحتفاظ بأجهزة المصلحة التجارية حيث يمكن للموظفين غير المصرح لهم أو عامة الناس الوصول إليها.

استخدم ضوابط الأمان لحماية أجهزة مصلحتك التجارية بشكل أكبر. كحد أدنى، يجب أن تكون مقفلة بعبارة مرور أو رقم التعريف الشخصي أو القياسات الحيوية. تأكد من ضبط هذه الأجهزة لتقفل تلقائياً بعد فترة قصيرة من عدم النشاط.

✓ **صمّم الأجهزة لتُقفل تلقائيًا بعد وقت قصير من عدم النشاط.**

احمِ بيانات مصلحتك التجارية

البيانات التي تحتفظ بها مصلحتك التجارية هدف جذاب لمجرمي الإنترنت.

خروقات البيانات في ارتفاع - فلا تدَع مصلحتك التجارية تقع ضحية. من المهم أن تعلم ما هي البيانات التي تحتفظ بها مصلحتك التجارية، وفي أي مواقع. بمجرد معرفتك، استخدم التوصيات الواردة في هذا الدليل للمساعدة في حماية بياناتك من وصول مجرمي الإنترنت إليها. قد تكون لبعض المصالح التجارية الصغيرة أيضًا التزامات إضافية بموجب التشريع.

- **ادمج بيانات مصلحتك التجارية**
قد تكون لديك بيانات مخزّنة عبر العديد من الأجهزة أو الخدمات. عندما تكون البيانات موزّعة، فإنها تزيد من عدد الأنظمة التي يتعيّن عليك الحفاظ عليها آمنة ومنسوخة احتياطياً. يمكن للعديد من الأنظمة أيضًا خلق المزيد من الفرص لهجمات مجرم الإنترنت . حيثما أمكن، خزّن بيانات مصلحتك التجارية في موقع مركزي آمن ويُنسخ احتياطياً بانتظام. يمكن أن تؤدي مركزية بياناتك إلى انتهاك أكبر إذا تم اختراق أنظمتك، لذا تأكد من حماية هذا الموقع المركزي بشكل كافٍ من خلال إعدادات آمنة ووصول مقيَّد. تحدث إلى أخصائي تكنولوجيا المعلومات أو الأمن السيبراني للحصول على المشورة.
- **تعرّف على التزاماتك لحماية البيانات.**
قد تكون لبعض المصالح التجارية الصغيرة التزامات قانونية للتعامل مع المعلومات الشخصية التي تجمعها. اقرأ دليل مكتب مفوض المعلومات الأسترالي للمصالح التجارية الصغيرة لمعرفة المزيد، والمتاح على oaic.gov.au. استشر أخصائيًا قانونيًا إذا كنت غير متأكد.

✓ **افهم البيانات التي تحتفظ بها مصلحتك التجارية ومسؤولياتك عن حمايتها.**

جهّز موظفيك

ثقّف الموظفين

الموظفون الذين لديهم ممارسات أمنية سيبرانية جيدة هم خط دفاعك الأول ضد الهجمات السيبرانية.

يجب أن يكون لدى موظفيك وعي بالأمن السيبراني، بما في ذلك الموضوعات التالية:

- تهديدات الأمن السيبراني الشائعة مثل اختراق البريد الإلكتروني للمصالح التجارية وبرامج الفدية
- تدابير الحماية بما في ذلك كلمات المرور أو عبارات المرور القوية، وتحديثات MFA والبرمجيات
- كيفية اكتشاف عمليات الاحتيال وهجمات التصيّد الاحتيالي
- السياسات الخاصة بالمصلحة التجارية (على سبيل المثال، عمليات الإبلاغ عن رسائل البريد الإلكتروني المشبوهة أو التثبّت من صحة الفواتير قبل الدفع)
- ما يجب القيام به في حالة الطوارئ.

يحتوي موقع ACSC على موارد لمعظم هذه الموضوعات على cyber.gov.au/learn. قد تفكّر في طرق أخرى لتثقيف موظفيك، على سبيل المثال من خلال دورة رسمية أو تدريب داخلي. كيفما قرّرت، تذكّر أن التدريب على الأمن السيبراني ليس مطلوباً لمرة واحدة ويجب تحديثه بشكل دوري.

✓ **حدّد كيف سيتمّ تعليم الوعي بالأمن السيبراني في مصلحتك التجارية.**

ضع خطة طوارئ

يمكن لخطة الطوارئ أن تقلّل من تأثير الهجوم السيبراني على مصلحتك التجارية.

عند الاستجابة لحادث أمن إلكتروني، كل دقيقة لها أهميتها. إن وجود خطة طوارئ يعني أن موظفيك يمكنهم قضاء وقت أقل في معرفة ما يجب القيام به والمزيد من الوقت في اتخاذ الإجراءات.

ضع في اعتبارك الأسئلة التالية عند إنشاء خطة الطوارئ الخاصة بك:

- ما هي العملية التي يتّبعها موظفوك للإبلاغ عن الحوادث المحتملة للأمن السيبراني ؟
- بمَن تتصل للحصول على المساعدة ؟ على سبيل المثال، متخصصو تكنولوجيا المعلومات ومصرفك.
- كيف سيتم إبلاغ الحادث لموظفيك أو حَمَلة الأسهم أو الزبائن ؟
- كيف ستدير المصلحة التجارية كالمعتاد، إذا كانت أيّ من الأنظمة المهمة غير متصلة بالإنترنت ؟

تأكد من أن موظفيك على دراية بخطة الطوارئ، بما في ذلك أي أدوار أو مسؤوليات قد تكون مناطة بهم. احتفظ بنسخة ورقية من الخطة في حال كانت أنظمتك غير متصلة بالإنترنت عند الحاجة إليها.

✓ **أعدّ خطة طوارئ لحوادث الأمن السيبراني.**

إبقَ على اطلاع

كن شريكًا في ACSC لتتلقى أحدث المعلومات من ACSC.

ابقَ على اطلاع على أحدث التهديدات ونقاط الضعف السيبرانية بأن تصبح شريكًا في ACSC. ستُرسل لك هذه الخدمة رسائل إخبارية وتنبيهات شهرية عند اكتشاف تهديد سيبراني جديد.

الأمن السيبراني هو مجال سريع التطوّر. ينشطّ مجرمو الإنترنت على استغلال نقاط الضعف في غضون دقائق من اكتشافها. سيساعد البقاء على اطلاع بمجال الأمن السيبراني مصلحتك التجارية على فهم التهديدات التي من المحتمل أن تواجهها وكيفية الحماية منها.

✓ **سجّل مصلحتك التجارية مع برنامج شراكة ACSC.**

إخلاء المسؤولية

المادة الواردة في هذا الدليل هي ذات طابع عام ولا ينبغي اعتبارها مشورة قانونية أو الاعتماد عليها للمساعدة في أي ظرف معيّن أو حالة طارئة. في أي مسألة مهمة، يجب أن تطلب مشورة مهنية مستقلة مناسبة ذات علاقة بظروفك الخاصة.

لا يقبل الكومنولث أي مسؤولية أو مساءلة قانونية عن أي ضرر أو خسارة أو نفقات تكبّدتها نتيجة الاعتماد على المعلومات الواردة في هذا الدليل.

لمزيد من المعلومات، أو للإبلاغ عن حادث أمن سيبراني، اتصل بنا:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

هذا الرقم متاح للاستخدام داخل أستراليا فقط.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Australian Government

Australian Signals Directorate