ACSC Australian Cyber Security Centre

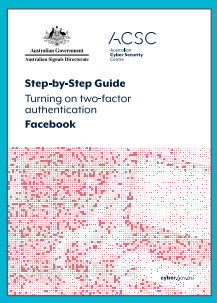
Australian Government
Australian Signals Directorate

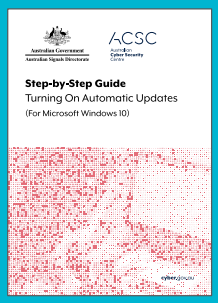
دليل الأمن السيبراني للشركات الصغيرة

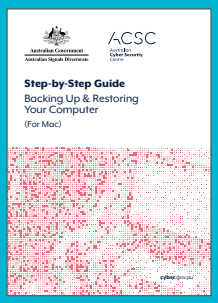
cyber.gov.au

أدلة إضافية

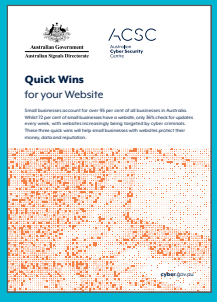
للمزيد من تدابير الأمن السيبراني للمساعدة في الحفاظ على عملك آمنًا، يُرجى الرجوع إلى باقة الأمن السيبراني للشركات الصغيرة في cyber.gov.au

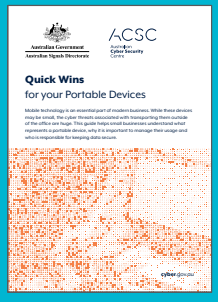


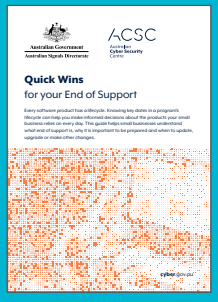




أدلة تفصيلية خطوة بخطوة.







أدلة "المكاسب السريعة"

جدول المحتويات

تمهيد

تم تطوير هذا الدليل لمساعدة الشركات الصغيرة على حماية نفسها من حوادث الأمن السيبراني الأكثر شيوعًا.

يمكن لحادث يتعلق بالأمن السيبراني أن يترك آثارًا مدمرة على الشركات الصغيرة.

لسوء الحظ، نحن في المركز الأسترالي للأمن السيبراني نرى تأثير حوادث الأمن السيبراني كل يوم على الأفراد والشركات الصغيرة والشركات الكبيرة.

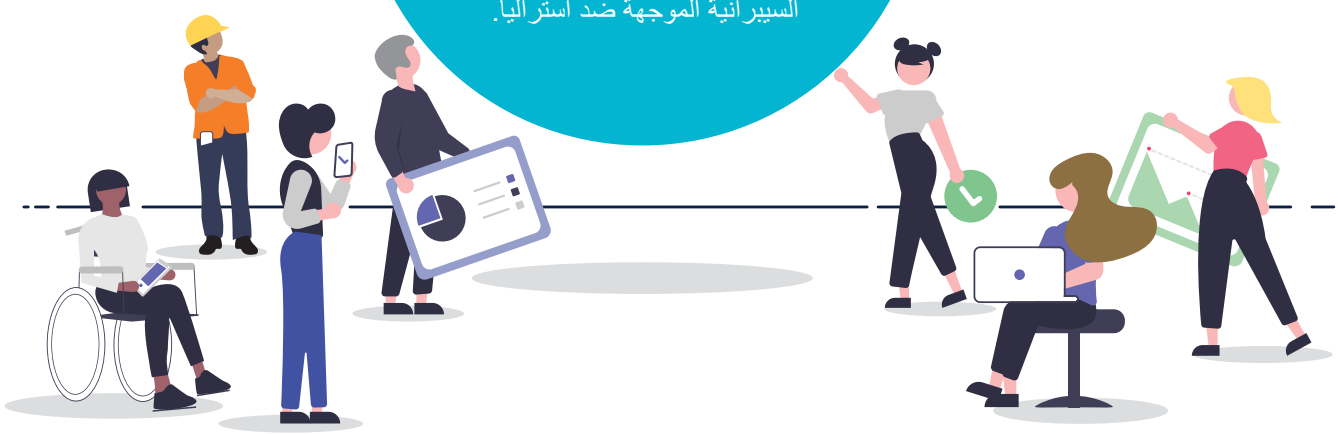
ندرك أن العديد من مالكي ومشغلي الشركات الصغيرة ليس لديهم الوقت أو الموارد لتكريسها للأمن السيبراني. ومع ذلك ، هناك تدابير بسيطة يمكن أن تقدمها الشركة الصغيرة للمساعدة في منع حوادث الأمن السيبراني الشائعة.

تم تصميم دليل الأمن السيبراني للأعمال الصغيرة الخاص بنا خصيصًا للشركات الصغيرة لفهم واتخاذ الإجراءات وزيادة مرونة الأمن السيبراني لديهم ضد تهديدات الأمن السيبراني دائمة التطور. اللغة واضحة، والإجراءات بسيطة، والإرشادات مصممة للشركات الصغيرة.

للحصول على نظرة عامة حول أساسيات الأمن السيبراني، يعد هذا الدليل مكانًا ممتازًا للبدء. إذا كنت ترغب في تحسين الأمن السيبراني لديك بشكل أكبر، يمكنك العثور على مزيد من المعلومات والنصائح على موقع المركز الأسترالي للأمن السيبراني **cyber.gov.au**

مهمة المركز الأسترالي للأمن السيبراني هي المساعدة في جعل أستراليا المكان الأكثر أمانًا للاتصال بالإنترنت.

يقدم المركز الأسترالي للأمن السيبراني، بصفته جزءًا من مديرية الإشارات الأسترالية، النصائح والمساعدة والاستجابات التشغيلية في مجال الأمن السيبراني لمنع وكشف ومعالجة التهديدات السيبرانية الموجهة ضد أستراليا.



التهديدات السيبرانية: المجالات الرئيسية

بالنسبة للشركات الصغيرة، يمكن أن يكون لأصغر حادث أمني سيبراني آثار مدمرة.

تم تصميم هذا الجزء لمساعدة الشركات الصغيرة على البقاء في حالة تأهب واستعداد. إنه يحدد ويشرح أكثر أنواع التهديدات السيبرانية شيوعًا وما يمكنك القيام به لحماية شركتك.

البرامج الضارة (البرمجيات الخبيثة)

ماذا تكون؟ برامج غير مصرح بها مصممة لإحداث ضرر

البرمجيات الخبيثة هي مصطلح شامل للبرامج الضارة بما في ذلك برامج الفدية والفيروسات وبرامج التجسس وأحصنة طروادة.

لماذا؟ التعطيل. التدمير. الخداع.

تمنح البرمجيات الخبيثة المجرمين طريقة للوصول إلى المعلومات المهمة مثل أرقام وكلمات مرور البطاقات المصرفية أو الائتمانية.

يمكنها أيضًا **التحكم في أو التجسس على** جهاز كمبيوتر المستخدم.
يتضمن ما يختار المجرمون فعله من خلال هذا الوصول والبيانات:

- **الاحتيال**
- **سرقة الهوية**
- **تعطيل** الأعمال
- **سرقة** البيانات الحساسة أو الملكية الفكرية
- **سرقة** موارد الكمبيوتر من أجل نشاط إجرامي أوسع

من؟ أي شخص، أي مكان

يمكن لمبتكري البرمجيات الخبيثة أن يكونوا في أي مكان في العالم.

كل ما يحتاجون إليه هو جهاز كمبيوتر ومهارات تقنية ونوايا خبيثة. يمكن للمجرمين الوصول بسهولة إلى أدوات رخيصة لاستخدام البرمجيات الخبيثة ضدك.

يلقي المجرمون شبكة واسعة ويلاحقون الأشخاص الأكثر ضعفًا. من خلال تنفيذ تدابير الأمن السيبراني والانتباه للتهديدات، يمكنك حماية شركتك من أن تكون هدفًا سهلًا.

الحماية من البرمجيات الخبيثة

- قم بالتحديث التلقائي لنظام التشغيل والبرامج والتطبيقات الخاصة بك
- قم بإجراء نسخ احتياطي بانتظام لبياناتك المهمة
- درّب موظفيك على التعرف على الروابط والمرفقات المشبوهة

رسائل الاحتيال (التصيد)

ماذا تكون؟ رسائل بريد إلكتروني أو رسائل أو مكالمات "مراوغة" مصممة لخداع المتلقين لسرقة أموالهم وبياناتهم

غالبًا ما سيستخدم المجرمون البريد الإلكتروني أو وسائل التواصل الاجتماعي أو المكالمات الهاتفية أو الرسائل النصية لمحاولة الاحتيال على الشركات الأسترالية.

قد يتظاهر هؤلاء المجرمون بأنهم فرد أو منظمة تعتقد أنك تعرفها، أو تعتقد أنك يجب أن تثق بها.

تحاول رسائلهم ومكالماتهم خداع الشركات للقيام بإجراءات محددة، مثل:

- **دفع فواتير مزورة** أو تغيير تفاصيل الدفع لفواتير شرعية
- **الكشف عن تفاصيل الحساب المصرفي** وكلمات المرور وأرقام بطاقات الائتمان (المعروفة أحيانًا باسم عمليات احتيال "التصيد"، حيث يمكن لمجرمي الإنترنت تقليد العلامات التجارية الرسمية والشعارات الصادرة عن البنوك والمواقع الإلكترونية لتبدو شرعية)
- **منح الوصول عن بعد** لجهاز الكمبيوتر أو الخادم الخاص بك
- **فتح مرفق** قد يحتوي على برمجيات خبيثة
- **شراء بطاقات هدايا** وإرسالها إلى المحتال

أين؟ رسائل البريد الإلكتروني، وسائل التواصل الاجتماعي، المكالمات الهاتفية، الرسائل النصية

لا تقتصر حيل التصيد على رسائل البريد الإلكتروني. إنها تتطور بشكل متزايد ويصعب اكتشافها.

كن حذرًا من الطلبات العاجلة للحصول على الأموال والتغييرات في الحسابات المصرفية والمرفقات غير المتوقعة وطلبات التحقق من تفاصيل تسجيل الدخول أو تأكيدها.

قم بزيارة **scamwatch.gov.au** للإبلاغ عن الاحتيال.

من؟ الشركات الأسترالية

يمكن إرسال الرسائل الاحتيالية إلى آلاف الأشخاص أو يمكن أن تستهدف شخصًا معينًا.

ومع ذلك، هناك تقنيات شائعة سيستخدمها المجرمون لمحاولة خداع موظفيك. قد تشمل رسائلهم:

- **السلطة**: هل تدعي الرسالة أنها من شخص مسؤول أو صاحب منصب كبير في الشركة؟
- **الأهمية**: هل يتم إخبارك بوجود مشكلة، أو أن لديك وقتًا محدودًا للرد أو الدفع؟
- **المشاعر**: هل تجعلك الرسالة تشعر بالذعر أو بالأمل أو بالفضول؟
- **الندرة**: هل تعرض الرسالة شيئًا غير متاح بكثرة، أو تعدك بصفقة جيدة؟
- **الأحداث الجارية**: هل الرسالة عن قصة إخبارية جارية أو حدث كبير جارٍ؟

إذا كنت تعتقد أن رسالة أو مكالمة ما قد تكون بالفعل من مؤسسة تثق بها (مثل البنك أو المورّد)، فابحث عن طريقة اتصال يمكنك الوثوق بها.

ابحث عن الموقع الرسمي أو اتصل برقم هاتفهم المعلن. لا تستخدم الروابط أو تفاصيل الاتصال الموجودة في الرسالة المرسلة إليك أو المعطاة عبر الهاتف حيث إنها قد تكون احتيالية.

برامج الفدية

ماذا تكون؟ نوع من البرمجيات الخبيثة التي تغلق جهاز الكمبيوتر الخاص بك أو ملفاتك حتى يتم دفع فدية

تعمل برامج الفدية عن طريق غلق ملفاتك أو تشفيرها بحيث لا يمكنك استخدامها أو الوصول إليها ثانيةً. في بعض الأحيان يمكنها حتى أن توقف أجهزتك عن العمل. يمكن لبرامج الفدية أن تصيب أجهزتك بنفس طريقة البرمجيات الخبيثة الأخرى. على سبيل المثال:

- زيارة مواقع غير آمنة أو مشبوهة
- فتح روابط أو رسائل بريد إلكتروني أو ملفات من مصادر غير معروفة
- ضعف الأمن على شبكتك أو أجهزتك (بما في ذلك الخوادم)

لماذا؟ المال

تقدم برامج الفدية لمجرمي الإنترنت دخلًا مجزيًا منخفض المخاطر. حيث إنه من السهل تطويرها وتوزيعها. عادةً ما يتم دفع الفدية باستخدام عملة رقمية عبر الإنترنت أو عملة مشفرة مثل البيتكوين، والتي يصعب تتبعها. كما أن معظم الشركات الصغيرة، وهذا لصالح مجرمي الإنترنت، غير مستعدة للتعامل مع هجمات برامج الفدية.

من؟ الشركات الصغيرة والمتوسطة والكبيرة

يمكن أن تكون الشركات الصغيرة معرضة للخطر بشكل خاص، حيث تقل احتمالية تنفيذها لتدابير الأمن السيبراني التي يمكن أن تساعد في الوقاية والتعافي من برامج الفدية.

لا تدفع فدية أبدًا

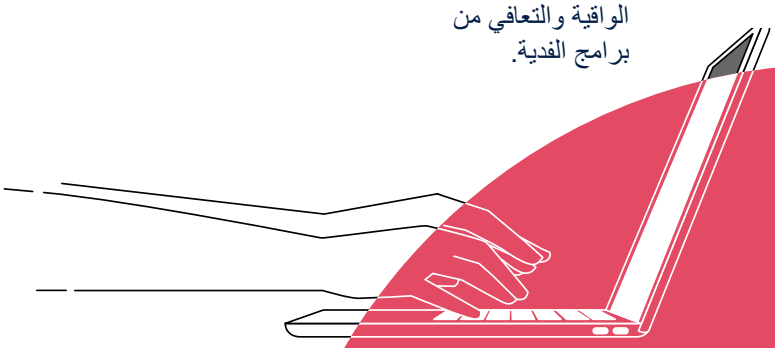
دفع الفدية لا يضمن استعادة ملفات الضحية، كما أنه لا يمنع نشر أي بيانات مسروقة أو بيعها لاستخدامها في جرائم أخرى. كما أنه يزيد من احتمالية استهداف الضحية مرة أخرى.

إذا واجهت حادثة برامج فدية وتحتاج إلى دعم، فاتصل بالخط الساخن المركز الأسترالي للأمن السيبراني على مدار الساعة طوال أيام الأسبوع على 1300 CYBER1 (1300 292 371).

بصرف النظر عن قرار دفع الفدية، نشجع الضحايا على الإبلاغ عن حوادث برامج الفدية إلى المركز الأسترالي للأمن السيبراني على موقع cyber.gov.au. تساعد مشاركة المعلومات حول الحوادث في حماية الشركات الأسترالية الأخرى.

الوقاية والتعافي من برامج الفدية

- قم بإجراء نسخ احتياطي لبياناتك المهمة بانتظام
- قم بالتحديث التلقائي لأنظمة التشغيل والبرامج والتطبيقات الخاصة بك
- حيثما أمكن، اطلب مصادقة متعددة العوامل للوصول إلى الخدمات (الصفحة 12)
- قم بتدقيق وتأمين أجهزتك (بما في ذلك الخوادم إذا كان لديك خوادم) وأي خدمات مكشوفة على لإنترنت على شبكتك (سطح المكتب البعيد، مشاركة الملفات، بريد الويب). ناقش هذا الأمر مع متخصص في تكنولوجيا المعلومات إذا لم تكن متأكدًا.



اعتبارات البرامج: المجالات الرئيسية

يمكن أن تؤدي إدارة البرامج والبيانات والحسابات عبر الإنترنت إلى زيادة حماية عملك بشكل كبير من أكثر أنواع التهديدات السيبرانية شيوعًا.

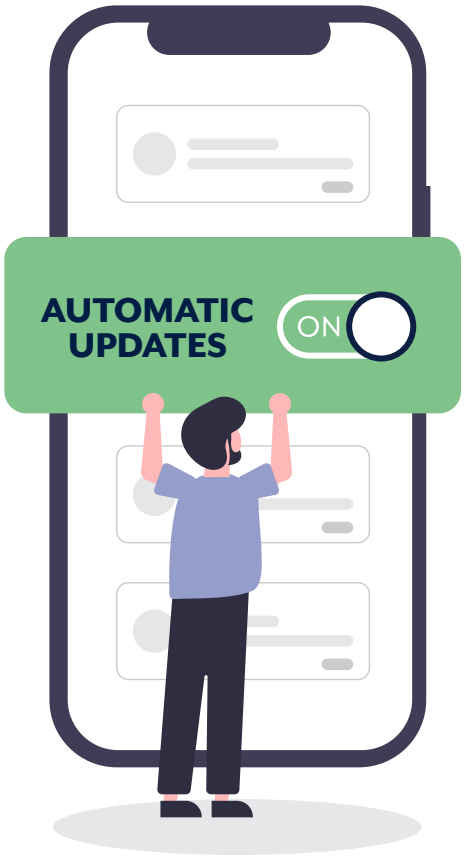
على سبيل المثال، يعد نظام التشغيل الخاص بك أهم جزء من البرامج على جهاز الكمبيوتر الخاص بك. فهو يدير أجهزة الكمبيوتر وجميع برامجه، وبالتالي يحتاج إلى التحديث بانتظام للتأكد من أنك تستخدم دائمًا الإصدار الأكثر أمانًا.

قم بتحسين المرونة وقم بالتحديث الدائم والحفاظ على الأمان مع اعتبارات البرامج هذه للشركات الصغيرة.

التحديثات التلقائية

ماذا تكون؟ تحديثات البرامج

التحديث هو نسخة محسنة من البرامج (البرامج والتطبيقات وأنظمة التشغيل) التي قمت بتثبيتها على الخوادم وأجهزة الكمبيوتر والأجهزة المحمولة الخاصة بك. **التحديث التلقائي** هو نظام افتراضي أو **نظام "يُضبط ويُنسى"** يقوم بتحديث برامجك بمجرد توفر تحديث لها.



لماذا؟ الأمن

- يعد تحديث نظام التشغيل والتطبيقات لديك **من أفضل الطرق لحماية نفسك من** حوادث الأمن السيبراني
- سيؤدي تحديث برنامجك بانتظام إلى **تقليل فرصة استخدام مجرمي الإنترنت لنقطة ضعف** معروفة لتشغيل برمجيات خبيثة أو اختراق جهازك
- **بتوفيرها لوقتك ومنعها لقلقك**، تعد التحديثات التلقائية جزءًا مهمًا من الحفاظ على أمان أجهزتك وبياناتك

متى؟ اليوم وكل يوم

- **قم بتشغيل التحديثات التلقائية**، خاصة لأنظمة التشغيل
- **تحقق بانتظام من وجود تحديثات** في حالة عدم توفر التحديثات التلقائية
- إذا تلقيت إشعارًا بتحديث نظام التشغيل الخاص بك أو برنامج آخر، فيجب عليك **تثبيت التحديث في أسرع وقت ممكن**
- **حدد وقتًا مناسبًا للتحديثات التلقائية** لتجنب حدوث اضطرابات في العمل كالمعتاد
- إذا كنت تستخدم **برنامجًا لمكافحة الفيروسات، فتأكد من تشغيل التحديثات التلقائية**

ملحوظة:

إذا كان جهازك أو برنامجك قديمًا جدًا، فقد يتعذر تحديثه وقد يصبح عملك نتيجةً لذلك عرضة للمشاكل الأمنية.

يوصي المركز الأسترالي للأمن السيبراني بترقية جهازك أو برامجك في أسرع وقت ممكن.

اعتبارًا من عام 2020، وصل كل من Windows 7 و Windows Server 2008 وMicrosoft Office 2010 إلى نهاية الدعم ولم يعد أي منها آمنًا.

لمزيد من المعلومات، اقرأ دليل المركز الأسترالي للأمن السيبراني، المكاسب السريعة لنهاية الدعم والمتاح على cyber.gov.au

النسخ الاحتياطية التلقائية

ماذا تكون؟ النسخ الاحتياطية للبيانات

إن **النسخة الاحتياطية** هي نسخة رقمية لأهم معلوماتك، مثل بيانات العملاء والسجلات المالية. ويمكن حفظها على جهاز تخزين خارجي أو على السحابة.

النسخ الاحتياطي التلقائي هو نظام افتراضي أو نظام "يُضبط ويُنسى" يقوم بنسخ برامجك بدون تدخل بشري.

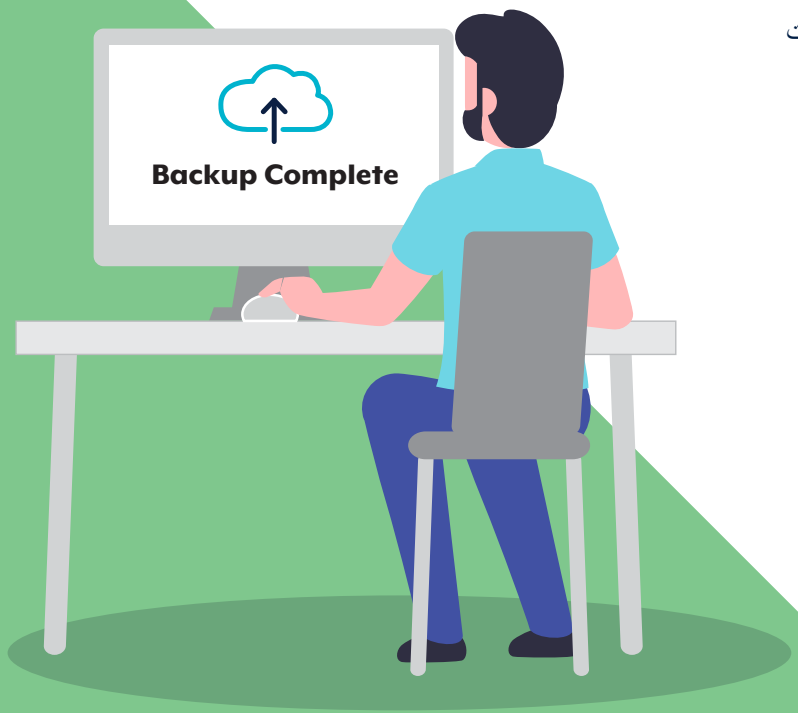
سيضمن فصل جهاز التخزين الاحتياطي وإزالته بأمان بعد كل نسخة احتياطية أن يظل آمنًا أثناء وقوع حادث إلكتروني.

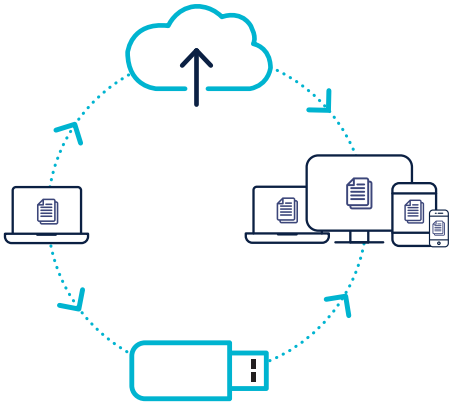
لماذا؟ استعادة بسيطة

- **النسخ الاحتياطي هو إجراء احترازي**، بحيث يمكن الوصول إلى بياناتك في حالة فقدها أو سرقتها أو تلفها
- **يسمح لشركتك بالتعافي** من حادثة إلكترونية (مثل برامج الفدية) وتقليل وقت التوقف عن العمل
- **يحمي مصداقية عملك** ويساعد على الوفاء بالالتزامات القانونية^

متى؟ اليوم وكل يوم

- **اختر نظام نسخ احتياطي يناسب عملك.** فكر فيما يمكنك تحمل خسارته في أسوأ السيناريوهات للمساعدة في توجيه المتطلبات مثل عدد مرات الاحتفاظ بنسخة احتياطية من بياناتك
- **اختبر النُسخ الاحتياطية بانتظام** بمحاولة استعادة البيانات
- **احتفظ دائمًا بنسخة احتياطية واحدة على الأقل مفصولة عن جهازك**، ويفضل أن تكون في مكان خارج موقع عملك في حالة حدوث كوارث طبيعية أو سرقة
- **لا تقم بتوصيل النسخة الاحتياطية الخاصة بك بالأجهزة المصابة** ببرامج الفدية أو الفيروسات





^ تلتزم بعض الصناعات بالاحتفاظ بالسجلات لفترات زمنية محددة. تأكد من أنك على دراية بمتطلبات الاحتفاظ بالبيانات الخاصة بك.

المصادقة متعددة العوامل

ماذا تكون؟ إجراء أمني يتطلب إثباتين أو أكثر للهوية لمنحك حق الوصول

تتطلب المصادقة متعددة العوامل عادةً مجموعة من:

- **شيء تعرفه** (كلمة المرور/عبارة المرور، رقم التعريف الشخصي، السؤال السري)
- **شيء تمتلكه** (البطاقة الذكية، الرمز المادي، تطبيق المصادقة)
- **شيء يعبر عن هويتك** (بصمة الأصبع أو غيرها من القياسات الحيوية).

لماذا؟ أمن أقوى بشكل ملحوظ

تعد المصادقة متعددة العوامل واحدة من أكثر الطرق فعالية للحماية من الوصول غير المصرح به إلى معلوماتك وحساباتك القيمة.

تجعل الطبقات المتعددة مهاجمة أعمالك أصعب بكثير على مجرمي الإنترنت. قد يتمكن المجرمون من سرقة إثبات هوية واحد مثل كلمة المرور الخاصة بك، لكنهم ما زالوا بحاجة إلى الحصول على إثباتات الهوية الأخرى واستخدامها للوصول إلى حسابك.

أين؟ الوصول إلى الحسابات المهمة

يجب على الشركات الصغيرة تطبيق المصادقة متعددة الطبقات على الحسابات المهمة حيثما أمكن ذلك، مع إعطاء الأولوية للحسابات المالية وحسابات البريد الإلكتروني. تتضمن بعض خيارات المصادقة متعددة العوامل، على سبيل المثال لا الحصر:

- الرمز المادي
- رقم التعريف الشخصي العشوائي
- القياسات الحيوية/ بصمة الأصبع
- تطبيق المصادقة
- البريد الإلكتروني
- رسالة نصية

الأشخاص والإجراءات: المجالات الرئيسية

تحتاج الشركات، مهما كانت صغيرة، إلى أن تكون على دراية بتدابير الأمن السيبراني وتطبقها بوعي على كل المستويات.

عملياتك الداخلية والقوى العاملة لديك هي آخر وضمن أهم خطوط الدفاع في حماية عملك من تهديدات الأمن السيبراني.

نظرًا لأن الشركات الصغيرة غالبًا ما تفتقر إلى الموارد التي تمكنها من الاستعانة بموظفي تكنولوجيا معلومات مخصصين لها، يتناول هذا القسم كيفية إدارة الوصول إلى المعلومات في شركتك وتأمين حسابات شركتك وتدريب موظفيك على كيفية منع حوادث الأمن السيبراني والتعرف عليها والإبلاغ عنها.

التحكم في الوصول

ماذا؟ التحكم فيمن يمكنه الوصول إلى ما هو موجود في شبكة الحواسيب الخاصة بشركتك

التحكم في الوصول هو وسيلة لتقييد الوصول إلى شبكة الحواسيب. وهو يساعد في حماية شركتك عن طريق تقييد الوصول إلى:

- الملفات والمجلدات
- التطبيقات
- قواعد البيانات
- صناديق البريد
- الحسابات على الإنترنت
- الشبكات

لماذا؟ لتقليل مخاطر الوصول بدون تصريح إلى المعلومات الهامة

عادةً، لا يحتاج الموظفون إلى الوصول الكامل إلى كل البيانات والحسابات والأنظمة في شركة ما لأداء دورهم.

يجب تقييد هذا الوصول حيثما كان ذلك ممكنًا، بحيث لا يعرض الموظفون ومقدمو الخدمات الخارجيون عملك للخطر سواء بشكل غير مقصود أو مقصود.

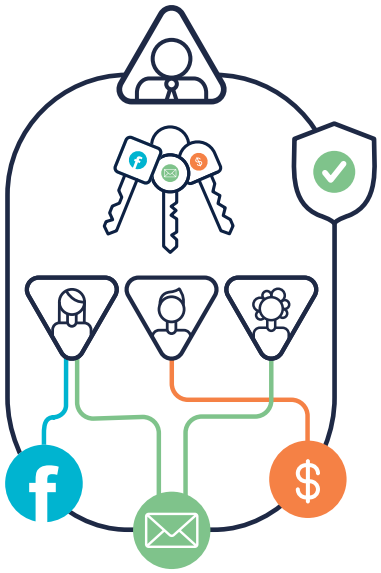
تسمح أنظمة وإجراءات التحكم في الوصول لصاحب العمل أو المشغل بما يلي:

- **تحديد من يجب عليه الوصول إلى** بعض الملفات وقواعد البيانات وصناديق البريد
- **التحكم في أي وصول مسموح به لمقدمي الخدمات الخارجيين،** على سبيل المثال، المحاسبين ومقدمي خدمات استضافة المواقع
- **تقييد من لديه حق الوصول إلى الحسابات** مثل مواقع الموردين ووسائل التواصل الاجتماعي
- **تقليل الضرر المحتمل** في حالة اختراق أي حسابات أو أجهزة أو أنظمة
- **إلغاء الوصول إلى الأنظمة والبيانات** عندما يغير أحد الموظفين أدواره أو يترك العمل

من؟ مبدأ الامتياز الأقل

اعتمادًا على طبيعة عملك، فإن مبدأ الامتياز الأقل هو النهج الأكثر أمانًا لمعظم الشركات الصغيرة.

فهو يمنح المستخدمين الحد الأدنى من الأذونات التي يحتاجون إليها لأداء عملهم. كما يقلل هذا أيضًا من مخاطر قيام "شخص من الداخل" بتعريض عملك للخطر سواء بغير قصد أو بقصد.



مبادئ التحكم في الوصول

- **انقل موظفيك من حسابات "المدير" إلى الحسابات القياسية على أجهزة الشركة**
- **راجع أذونات الوصول على الملفات والمجلدات الرقمية**
- **لا تشارك الحسابات أو عبارات المرور/ كلمات المرور بين الموظفين**
- **تذكر أن تقوم بإلغاء الوصول و/أو حذف الحسابات و/أو تغيير عبارات المرور/ كلمات المرور عند مغادرة أحد الموظفين للشركة، أو إذا قمت بتغيير مقدمي الخدمة**

عبارات المرور

ماذا؟ نسخة أقوى وأكثر أمانًا من كلمة المرور

تعد المصادقة متعددة العوامل (راجع الصفحة 12) واحدة من أكثر الطرق فعالية للحماية من الوصول غير المصرح به إلى معلوماتك وحساباتك القيمة. ومع ذلك، إذا لم تكن المصادقة متعددة العوامل متاحة، فيجب عليك استخدام عبارة مرور لحماية حسابك.

تستخدم عبارة الدخول أربع كلمات عشوائية أو أكثر ككلمة السر الخاصة بك. على سبيل المثال، "برتزل الفخار بالبصل الكريستالي".

لماذا؟ آمنة ويسهل تذكرها

يصعب على مجرمي الإنترنت اختراق عبارات المرور، لكن يسهل عليك تذكرها.

أنشئ عبارات مرور تكون:

- **طويلة:** فكلما كانت عبارة الدخول أطول كلما كان ذلك أفضل. اجعل طولها 14 حرفًا على الأقل.
- **لا يمكن التكهن بها:** استخدم مزيجًا عشوائيًا من كلمات لا صلة لها ببعضها البعض. لا تستخدم عبارات أو اقتباسات أو كلمات أغاني مشهورة.
- **فريدة:** لا تُعد استخدام عبارات المرور على حسابات متعددة.

إذا طلب أحد المواقع الإلكترونية أو إحدى الخدمات كلمة مرور معقدة تتضمن رموزًا أو أحرفًا كبيرة أو أرقامًا، فيمكنك تضمينها في عبارة المرور الخاصة بك. يجب أن تظل عبارة مرورك طويلة وغير متوقعة وفريدة من نوعها للحصول على أفضل أمان.

أين؟ حساباتك وأجهزتك

إذا كنت لا تستطيع استخدام المصادقة متعددة العوامل على حساب أو جهاز ما، فمن المهم استخدام عبارة مرور للبقاء آمنًا. في هذه الحالات، قد تكون عبارة المرور الآمنة هي الحاجز الوحيد بين الخصوم ومعلوماتك القيمة.

تذكر أن تجعل عبارات المرور الخاصة بك فريدة، حيث إن إعادة استخدام كلمة مرور يسهّل على مجرمي الإنترنت اختراق حسابات متعددة.

لمزيد من النصائح حول إنشاء عبارات المرور، راجع دليل المركز الأسترالي للأمن السيبرانيإنشاء عبارات مرور قوية المتوفر على **cyber.gov.au**

فكر في استخدام برنامج لإدارة كلمات المرور

تتيح برامج إدارة كلمات المرور (التي يمكن استخدامها أيضًا لتخزين عبارات المرور) عادات جيدة للأمن السيبراني. قد يبدو وجود عبارة مرور فريدة لكل حساب مهم أمرًا مربكًا؛ ولكن استخدام برنامج لإدارة كلمات المرور لحفظ عبارات المرور الخاصة بك سوف يريحك من عبء تذكر الأماكن التي تستخدم فيها عبارات المرور. تأكد من أن أي برنامج تستخدمه لإدارة كلمات المرور يأتي من مصدر موثوق به وذي سمعة طيبة ومحمي بعبارة مرور خاصة به قوية وسهلة التذكر.

تدريب الموظفين

ماذا؟ شيء تثقيفي لحماية موظفيك وأعمالك من التهديدات السيبرانية

علّم نفسك وعلّم موظفيك كيفية منع الجرائم السيبرانية والتعرف عليها والإبلاغ عنها.

قم بتدريب موظفيك على أساسيات الأمن السيبراني، بما في ذلك تحديث أجهزتهم وتأمين حساباتهم وتحديد رسائل الاحتيال.

يجب عليك أيضًا التفكير في تنفيذ **خطة الاستجابة لحوادث الأمن السيبراني** لتوجيه شركتك وموظفيك في حالة وقوع حادث سيبراني.

سيساعدك هذا على فهم أجهزتك وعملياتك المهمة، بالإضافة إلى جهات الاتصال الرئيسية التي يمكنك استخدامها للاستجابة والتعافي.

"علّم نفسك وعلّم موظفيك كيفية منع الجرائم السيبرانية والتعرف عليها والإبلاغ عنها."

لماذا؟ يمكن أن يكون الموظفون خط الدفاع الأول والأخير ضد تهديدات الأمن السيبراني

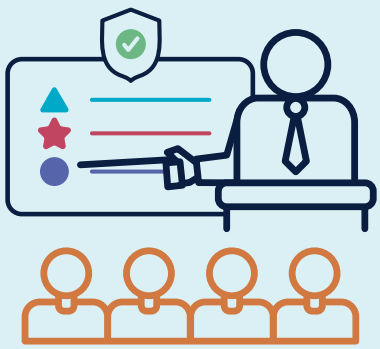
من شأن التدريب أن يغير عادات وسلوك الموظفين ويخلق مسؤولية مشتركة في الحفاظ على عملك آمنًا.

الأمن السيبراني هو مسؤولية الجميع.

متى؟ الوعي والتدريب المنتظم في مجال الأمن السيبراني

يتطور الأمن السيبراني باستمرار.

قد يكون إبقاء الجميع على اطلاع دائم بتهديدات الأمن السيبراني هو الفرق بين ما إذا كان المجرم سيتمكن من الوصول إلى أموالك أو حساباتك أو بياناتك أم لا.



نصائح للتوعية بالأمن السيبراني

- قم بتدريب موظفيك على التعرف على الروابط والمرفقات المشبوهة
- وفّر تدريبًا محدثًا في مجال الأمن السيبراني بانتظام
- ضع خطة استجابة لحوادث الأمن السيبراني
- شجع على التمتع بثقافة أمن سيبراني قوية
- شارك أمثلة على رسائل الاحتيال لمساعدة الموظفين على تحديد تهديدات الأمن السيبراني

قائمة مرجعية موجزة

اعتبارات البرامج

قم بالتحديث التلقائي لأنظمة التشغيل والبرامج والتطبيقات الخاصة بك

- إذا تلقيت إشعارًا بتحديث نظام التشغيل الخاص بك أو برنامج آخر، فيجب عليك تثبيت التحديث في أسرع وقت ممكن
- حدد وقتًا مناسبًا للتحديثات التلقائية لتجنب حدوث اضطرابات في العمل كالمعتاد

قم بإجراء نسخ احتياطي لبياناتك المهمة بانتظام

- اختبر النُسخ الاحتياطية بانتظام بمحاولة استعادة البيانات
- احتفظ دائمًا بنسخة احتياطية واحدة على الأقل مفصولة عن جهازك

قم بتمكين المصادقة متعددة الطبقات على الحسابات المهمة حيثما أمكن ذلك

- تعد المصادقة متعددة العوامل واحدة من أكثر الطرق فعالية لحماية معلوماتك وحساباتك القيمة
- أعط الأولوية للحسابات المالية وحسابات البريد الإلكتروني لتحقيق أقصى تأثير.

الأشخاص والإجراءات

تحكم فيمن يمكنه الوصول إلى ما هو موجود داخل شركتك

- استخدم مبدأ الامتياز الأقل لأذونات الوصول
- تذكر أن تقوم بحذف الحسابات و/أو تغيير عبارات المرور/ كلمات المرور عند مغادرة أحد الموظفين للشركة

عندما لا تكون المصادقة متعددة العوامل ممكنة، استخدم عبارات المرور لحماية الحسابات والأجهزة

- تستخدم عبارات المرور أربع كلمات عشوائية أو أكثر لتصبح كلمة المرور الخاصة بك.
- تكون عبارات المرور أكثر فاعلية عندما تكون طويلة ومعقدة ويصعب التكهن بها وفريدة.

قم بتدريب موظفيك على أساسيات الأمن السيبراني

- قد يتضمن هذا تحديث أجهزتهم وتأمين حساباتهم وتحديد رسائل الاحتيال.
- وفّر تدريبًا محدثًا في مجال الأمن السيبراني بانتظام

مسرد

برنامج مكافحة الفيروسات
برنامج مصمم لحماية الكمبيوتر أو الشبكة من فيروسات الكمبيوتر.

التطبيق
يُعرف كذلك باسم تطبيق الهاتف المحمول، وهو مصطلح يشير إلى البرنامج الذي يستخدم بشكل شائع للهاتف الذكي أو الجهاز اللوحي.

المرفق
ملف يتم إرساله مع رسالة بريد إلكتروني.

تطبيق المصادقة
تطبيق يستخدم لتأكيد هوية مستخدم الكمبيوتر للسماح بالوصول من خلال المصادقة متعددة العوامل.

القياسات الحيوية
تحديد هوية الشخص من خلال قياس سماته البيولوجية، على سبيل المثال بصمة الأصبع أو الصوت.

البيتكوين
عملة رقمية (عملة مشفرة)، تستخدم على الإنترنت لخدمات متنوعة.

هجوم قوة غاشمة
نوع من الهجوم يولد الملايين من مجموعات الرموز في الثانية. وهي فعالة ضد كلمات المرور القصيرة أو التي تتكون من كلمة واحدة.

السحابة
شبكة من الخوادم البعيدة التي توفر سعة تخزينية ضخمة وموزعة وقوة معالجة.

مجرم الإنترنت
أي شخص يقوم باختراق نظام كمبيوتر بشكل غير قانوني لإتلاف المعلومات أو سرقتها.

البيانات
البيانات هي معلومات تشمل الملفات أو النصوص أو الأرقام أو الصور أو مقاطع الصوت أو الفيديو.

الإعدادات الافتراضية
شيء حدده جهاز الكمبيوتر أو نظام التشغيل أو البرنامج مسبقًا للمستخدم.

هجمات المعجم
نوع من الهجمات يولد الملايين من المحاولات المحتملة بناءً على القواعد وقواعد البيانات. وهي فعالة ضد عبارات المرور الأقل تعقيدًا والمستخدمة بشكل شائع.

التشفير
عملية جعل البيانات غير قابلة للقراءة من قبل الآخرين بغرض منع الآخرين من الوصول إلى محتوياتها.

الشبكة
مجموعة من أجهزة الكمبيوتر أو الخوادم أو أجهزة الكمبيوتر المركزية أو أجهزة الشبكات أو الأجهزة الطرفية أو الأجهزة الأخرى المتصلة ببعضها البعض للسماح بمشاركة البيانات.

نظام التشغيل
برامج مثبتة على محرك الأقراص الثابتة بجهاز الكمبيوتر وهي تمكن أجهزة الكمبيوتر من الاتصال ببرامج الكمبيوتر وتشغيلها. أمثلة: Microsoft Windows وApple macOS وiOS وAndroid.

البرمجيات
تُعرف باسم البرامج، وهي مجموعة التعليمات التي تمكن المستخدم من التفاعل مع الكمبيوتر أو أجهزته أو أداء المهام.

برنامج التجسس
برنامج مصمم لجمع المعلومات حول نشاط المستخدم على جهازه بشكل سري.

الرمز المميز
رمز آمن يتم إنشاؤه بواسطة جهاز مادي أو تطبيق مصادقة للاستخدام أثناء المصادقة متعددة العوامل. قد يشير الرمز المميز أيضًا إلى الجهاز المادي الذي ينشئ الرمز الآمن الصغير بما يكفي ليوضع في سلسلة مفاتيح أو يكون على شكل بطاقة ائتمان.

حصان طروادة
نوع من البرمجيات الخبيثة يقوم بالتخفي غالبًا كبرنامج شرعي، ولكنه يحتوي على رمز ضار يستخدمه مجرمو الإنترنت للوصول إلى أنظمة المستخدمين.

الفيروس
برنامج مصمم لإحداث ضرر أو سرقة معلومات شخصية أو تعديل البيانات أو إرسال رسائل بريد إلكتروني أو عرض رسائل أو القيام بمزيج من هذه الإجراءات.

إخلاء المسئولية.
يشتمل هذا الدليل على معلومات عامة ولا ينبغي اعتبارها نصحًا قانونيًا أو الاعتماد عليها للمساعدة في أي ظرف أو حالة طارئة معينة. في حالة أي مسألة هامة، يجب أن تسعى للحصول على مشورة مهنية مستقلة مناسبة لظروفك الخاصة.

لا يتحمل الكومنولث أي مسؤولية أو التزام عن أي ضرر أو خسارة أو مصاريف متكبدة 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)

ACSC Australian Cyber Security Centre

Australian Government
Australian Signals Directorate