ACSC Australian Cyber Security Centre

Australian Government
Australian Signals Directorate

الأمن السيبراني الشخصي
الخطوات الأولى

cyber.gov.au

سلسلة الأمن السيبراني الشخصي

دليل ***الأمن السيبراني الشخصي: الخطوات الأولى*** هو الأول ضمن سلسلة من ثلاثة أدلة مصممة لمساعدة الأستراليين غير الخبراء على فهم أساسيات الأمن السيبراني وكيف يمكنك اتخاذ إجراءات لحماية نفسك من التهديدات السيبرانية الشائعة.

يمكنك الوصول إلى الدليلين الآخرين على موقع **cyber.gov.au**

الخطوات المتقدمة

الخطوات التالية

الخطوات الأولى

جدول المحتويات

المقدمة

ما هو الأمن السيبراني الشخصي؟

في عالم يعتمد على التكنولوجيا بشكل متزايد، نستخدم كل يوم أجهزة وحسابات معرضة للتهديدات السيبرانية:

- قد تتضمن أجهزتك أجهزة الكمبيوتر والهواتف المحمولة والأجهزة اللوحية وغيرها من الأجهزة المتصلة بالإنترنت.
- يمكنك أيضًا استخدام حسابات عبر الإنترنت للبريد الإلكتروني، والخدمات المصرفية، والتسوق، ووسائل التواصل الاجتماعي، والألعاب والمزيد.

الأمن السيبراني الشخصي هو الخطوات المستمرة التي يمكنك اتخاذها لحماية حساباتك وأجهزتك من التهديدات السيبرانية.

ما هي التهديدات السيبرانية؟

التهديدات السيبرانية الرئيسية التي تؤثر على الأستراليين غير الخبراء هي **عمليات الاحتيال والبرمجيات الخبيثة**.

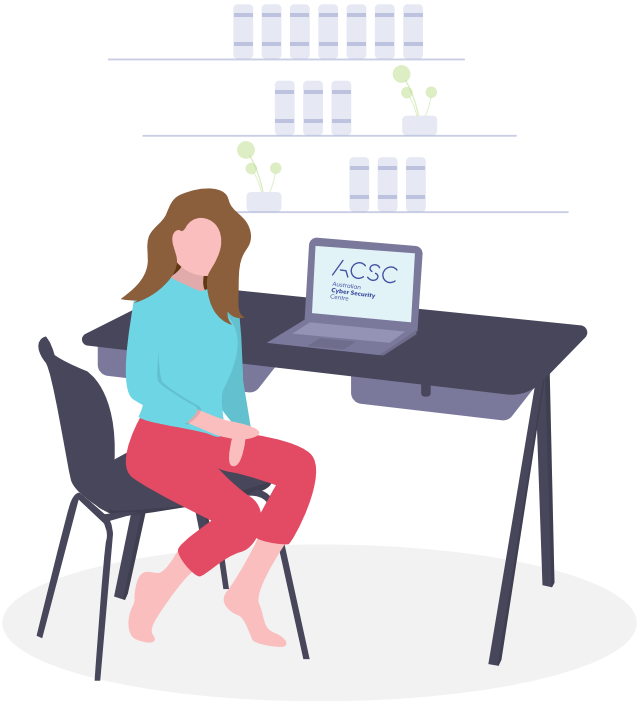
- **البرمجيات الخبيثة هي مصطلح شامل للبرامج الضارة** تم تصميمها لإيقاع الضرر بما في ذلك الفيروسات والديدان الحاسوبية وبرامج التجسس وأحصنة طروادة وبرامج الفدية. يستخدم مجرمو الإنترنت البرامج الضارة لسرقة معلوماتك وأموالك، والتحكم في أجهزتك وحساباتك.
- **الحيل هي رسائل يرسلها مجرمو الإنترنت** مصممة للتلاعب بك للإفصاح عن معلومات حساسة أو لتنشيط البرمجيات الخبيثة على جهازك.

يمكن أن يكون لهذه الهجمات تأثير شخصي ومالي كبيرين على الضحايا وهي تتزايد تعقيدًا وتكرارًا.

كيف يمكن لهذا الدليل أن يساعد في حمايتي من التهديدات السيبرانية؟

دليل الأمن السيبراني الشخصي: الخطوات الأولى هو الأول ضمن سلسلة من ثلاثة أدلة مصممة لمساعدة الأستراليين غير الخبراء على فهم أساسيات الأمن السيبراني وكيف يمكنك اتخاذ إجراءات لحماية نفسك من التهديدات السيبرانية الشائعة.

إذا كنت تتعلم عن الأمن السيبراني لأول مرة، أو كنت تبقي نفسك على اطلاع دائم، فإن هذا الدليل يعد بداية ممتازة.



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

لمزيد من المعلومات والأدلة والنصائح حول الأمن السيبراني، قم بزيارة موقع المركز الأسترالي للأمن السيبراني cyber.gov.au.

إذا كنت تعتقد أنك ضحية لجريمة سيبرانية، فأبلغ عنها من خلال ReportCyber التابع للمركز الأسترالي للأمن الأسترالي على الموقع cyber.gov.au أو اتصل بالخط الساخن للأمن السيبراني على (1300 292 371) 1300 CYBER1.

ابق على اطلاع بأحدث التهديدات السيبرانية: اشترك في خدمة التنبيهات المجانية الخاصة بالمركز الأسترالي للأمن السيبراني على الموقع cyber.gov.au.

ارفع مستوى الأمن السيبراني لديك

قم بتشغيل التحديثات التلقائية

ما هي التحديثات؟

التحديث هو نسخة محسنة من البرامج (البرامج والتطبيقات وأنظمة التشغيل) التي قمت بتثبيتها على حاسوبك وأجهزتك المحمولة.

تساعد تحديثات البرامج على حماية أجهزتك عن طريق إصلاح "عيوب" البرامج (أخطاء الترميز أو نقاط الضعف) التي يمكن لمجرمي الإنترنت والبرامج الضارة استخدامها للوصول إلى جهازك وسرقة بياناتك الشخصية وحساباتك ومعلوماتك المالية وهويتك.

يتم العثور باستمرار على "عيوب" البرامج الجديدة واستغلالها من قبل مجرمي الإنترنت، لذا فإن تحديث البرامج على أجهزتك يساعد في حمايتك من الهجمات السيبرانية.

كيف أقوم بإعداد التحديثات التلقائية؟

التحديثات التلقائية هي إعداد افتراضي أو إعداد "يُضبط ويُنسى" يقوم بتثبيت التحديثات الجديدة بمجرد توفرها.

- **قم بتشغيل التحديثات التلقائية وتأكيدها** على جميع أجهزتك.
- **قد تختلف طريقة تشغيل التحديثات التلقائية** بحسب البرامج والجهاز.
- **حدد وقتًا مناسبًا للتحديثات التلقائية**، إن أمكن، مثل الوقت الذي تكون نائمًا فيه أو لا تستخدم جهازك عادةً.
- **يجب أن يكون جهازك مدارًا** وموصلاً بالطاقة وبه مساحة تخزين غير مستخدمة.

إذا تلقيت إشعارًا بتحديث برامج جهازك فيجب عليك فعل ذلك في أسرع وقت ممكن.

ماذا لو كان إعداد التحديث التلقائي غير متاح؟

في حالة عدم توافر إعداد التحديث التلقائي، فيجب عليك البحث بانتظام عن التحديثات الجديدة وتثبيتها من خلال قائمة إعدادات البرنامج أو الجهاز.

ماذا لو لم تتلق أجهزتي وبرامجي القديمة أي تحديثات؟

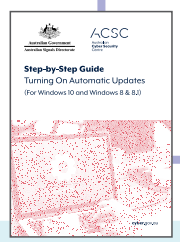
إذا كان جهازك أو نظام التشغيل أو البرنامج قديمًا جدًا، فقد لا يكون مدعومًا من قبل الشركة المصنعة أو المطورة.

عندما تصل المنتجات إلى مرحلة "نهاية الدعم" هذه، فإنها لن تتلقى تحديثات بعد الآن، مما يجعلك عرضة للهجمات السيبرانية بسبب "عيوب" البرامج المعروفة. تتضمن أمثلة المنتجات التي انتهى دعمها نظام التشغيل Windows 7 و iPhone 6.

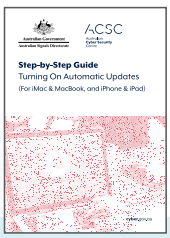
إن كان جهازك أو نظام التشغيل أو البرنامج وصل لمرحلة نهاية الدعم فإن المركز الأسترالي للأمن السيبراني يوصي بالترقية في أسرع وقت ممكن لتبقى آمنًا.

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

لمزيد من المعلومات المفصلة حول كيفية تشغيل التحديثات التلقائية، اقرأ أدلة المركز الأسترالي للأمن السيبراني *خطوة بخطوة* المتاحة على cyber.gov.au:



تشغيل التحديثات التلقائية (لنظام Microsoft Windows 10 و Windows 8 & 8.1)



تشغيل التحديثات التلقائية (لأجهزة iMac و MacBook و iPhone و iPad)

قم بتشغيل المصادقة متعددة العوامل

ما هي المصادقة متعددة العوامل؟

يمكنك استخدام المصادقة متعددة العوامل لتحسين أمان حساباتك الأكثر أهمية. تتطلب منك المصادقة متعددة العوامل إنتاج مزيج من نوعين أو أكثر من أنواع المصادقة التالية قبل منحك الوصول إلى أحد حساباتك:

- **شيء تعرفه** (مثل رقم التعريف الشخصي أو كلمة المرور أو عبارة المرور)؛
- **شيء تمتلكه** (مثل البطاقة الذكية أو الرمز المادي أو تطبيق المصادقة أو رسالة نصية أو رسالة بريد إلكتروني)؛ و
- **شيء يعبر عن هويتك** (مثل بصمة الإصبع أو التعرف على الوجه أو مسح قزحية العين).

تصعّب المصادقة متعددة العوامل على مجرمي الإنترنت الوصول المبدئي إلى جهازك وحسابك ومعلوماتك من خلال إضافة المزيد من طبقات المصادقة مما يتطلب المزيد من الوقت والجهد والموارد لاختراقها.

المصادقة الثنائية (2FA) هي النوع الأكثر شيوعًا للمصادقات متعددة العوامل، حيث تتطلب نوعين مختلفين من المصادقة.

كيف يمكنني تفعيل المصادقة الثنائية لحماية حساباتي الأكثر أهمية؟

يجب عليك تفعيل المصادقة الثنائية الآن، بدءًا من حساباتك المهمة:

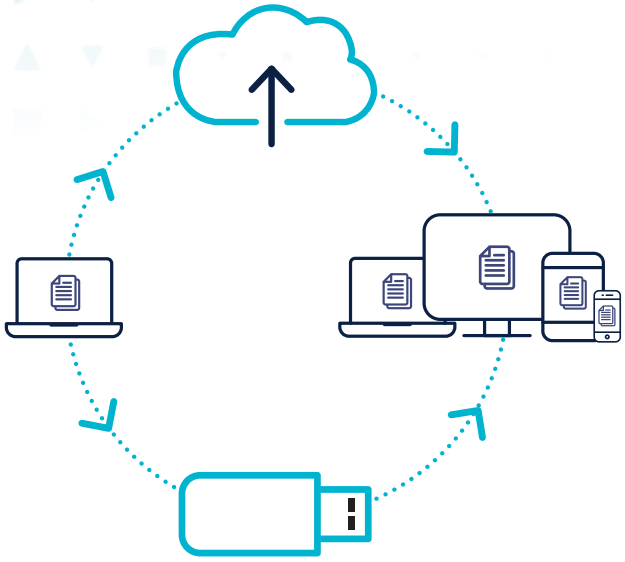
- **جميع الحسابات المصرفية والمالية الإلكترونية (على سبيل المثال، البنك الذي تتعامل معه، PayPal)**
- **جميع حسابات البريد الإلكتروني (مثل Gmail و Outlook و Hotmail و Yahoo!)**

إذا كان لديك الكثير من حسابات البريد الإلكتروني، فامنح الأولوية لتلك المرتبطة بالخدمات المصرفية عبر الإنترنت أو الخدمات الهامة الأخرى.

تختلف خطوات تنشيط المصادقة الثنائية باختلاف الحساب أو الجهاز أو تطبيق البرنامج.

لمزيد من المعلومات حول كيفية تشغيل المصادقة الثنائية على حساباتك الأكثر أهمية، اقرأ أدلة المركز الأسترالي للأمن السيبراني *خطوة بخطوة* المتاحة على cyber.gov.au أو زر الموقع الإلكتروني لمقدم الخدمة الخاصة بحسابك.

قم بإجراء نسخ احتياطي لمحتويات أجهزتك بانتظام



ما هو النسخ الاحتياطي؟

النسخ الاحتياطي هو وضع نسخة رقمية لأهم معلوماتك (مثل الصور والمعلومات أو السجلات المالية) المحفوظة على جهاز تخزين خارجي أو على السحابة.

النسخ الاحتياطي هو إجراء احترازي، يمكنك من استعادة معلوماتك في حالة فقدها أو سرقتها أو تلفها.

كيف يمكنني إجراء نسخ احتياطي لأجهزتي وملفاتي؟

يجب أن تقوم بإجراء نسخ احتياطي بانتظام لملفاتك وأجهزتك.

ويعود القرار إليك في النهاية إن شئت القيام بذلك يوميًا أو أسبوعيًا أو شهريًا. قد يتوقف عدد مرات النسخ الاحتياطي على عدد:

- **الملفات الجديدة** التي تقوم بتحميلها على جهازك،
- **التغييرات** التي تجريها على الملفات، و
- الملفات التي تكون **على استعداد لخسارتها**.

يشجعك المركز الأسترالي للأمن السيبراني على التحقق من نسخك الاحتياطية حتى تكون على دراية بعملية الاسترداد ولضمان أن النسخ الاحتياطية الخاصة بك تعمل جيدًا.

لمزيد من المعلومات المفصلة حول كيفية النسخ الاحتياطي على كل من أجهزة التخزين الخارجية والسحابة، اطلع على أدلة المركز الأسترالي للأمن السيبراني *خطوة بخطوة* المتاحة على cyber.gov.au:

لأجهزة الكمبيوتر:

- *النسخ الاحتياطي واستعادة ملفاتك*
  - *لجهاز الكمبيوتر (على السحابة)*
- *النسخ الاحتياطي واستعادة ملفاتك*
  - *لجهاز الكمبيوتر (باستخدام جهاز تخزين خارجي)*

لأجهزة MAC:

- *النسخ الاحتياطي واستعادة ملفاتك*
  - *لجهاز Mac (على السحابة)*
- *النسخ الاحتياطي واستعادة ملفاتك*
  - *لجهاز Mac (باستخدام جهاز تخزين خارجي)*

لنظام IOS:

- *النسخ الاحتياطي واستعادة ملفاتك*
  - *لجهاز iPhone (على السحابة)*

استخدم عبارات المرور لتأمين حساباتك المهمة

تعد المصادقة متعددة العوامل (راجع الصفحة 4) واحدة من أكثر الطرق فعالية للحماية من الوصول غير المصرح به إلى معلوماتك وحساباتك القيمة. **في حالة عدم توفر المصادقة متعددة العوامل**، يمكن لعبارة مرور قوية وفريدة من نوعها حماية حسابك بشكل أفضل مقارنة بكلمة المرور البسيطة.

ما هي عبارة المرور؟

تستخدم عبارة الدخول أربع كلمات عشوائية أو أكثر ككلمة السر الخاصة بك.

على سبيل المثال، "برتزل الفخار بالبصل الكريستالي".

- **عبارات المرور أكثر أمانًا** من كلمات المرور البسيطة.
- يصعب **على مجرمي الإنترنت** اختراق عبارات المرور، لكن **يسهل عليك** تذكرها.

كيف يمكنني إنشاء عبارة مرور؟

أنشئ عبارات مرور تكون:

- **طويلة:** طولها 14 حرفًا على الأقل، باستخدام أربع كلمات عشوائية أو أكثر. فكلما كانت عبارة الدخول أطول كانت أكثر أمانًا.
- **لا يمكن التكهن بها:** استخدم مزيجًا عشوائيًا من أربع كلمات أو أكثر لا صلة لها ببعضها البعض. لا تستخدم عبارات أو اقتباسات أو كلمات أغاني مشهورة.
- **فريدة:** لا يُعاد استخدامها عبر 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.

ما هي الحسابات التي يجب عليّ تأمينها باستخدام عبارة مرور؟

إذا كانت حساباتك الأكثر أهمية غير محمية بالمصادقة متعددة العوامل (راجع الصفحة 4)، فقم بتغيير كلمات المرور الخاصة بك إلى عبارات مرور قوية وفريدة، ولتبدأ بالتالي:

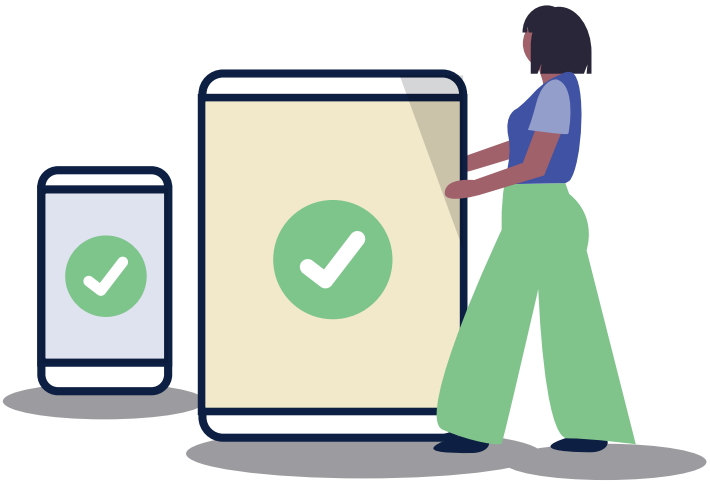
- **الحسابات المصرفية والمالية عبر الإنترنت**
- **حسابات البريد الإلكتروني**

إذا كان لديك الكثير من حسابات البريد الإلكتروني، فامنح الأولوية لتلك المرتبطة بالخدمات المصرفية عبر الإنترنت أو الخدمات الهامة الأخرى.

يمكنك عادةً تغيير كلمة المرور الخاصة بك إلى عبارة مرور قوية وفريدة من خلال قائمة إعدادات حسابك.

"تذكر: لا تُعد استخدام عبارة المرور عبر حسابات متعددة".

لمزيد من النصائح حول كيفية إنشاء عبارات مرور قوية،راجع دليل المركز الأسترالي للأمن السيبراني *إنشاء عبارات مرور قوية* المتاح على cyber.gov.au.



قم بتأمين جهازك المحمول

تُستخدم الهواتف الذكية والأجهزة اللوحية اليوم للاتصال والتسوق والعمل والبنوك والأبحاث وتتبع اللياقة وإكمال مئات المهام الأخرى في أي وقت ومن أي مكان.

ماذا يمكن أن يحدث إذا تعرض جهازي المحمول للاختراق أو الضياع أو السرقة؟

- قد يستخدمه مجرمو الإنترنت لسرقة أموالك أو هويتك، باستخدام المعلومات المخزنة على جهازك بما في ذلك حسابات وسائل التواصل الاجتماعي والبريد الإلكتروني.
- قد تفقد بيانات لا يمكن الاستغناء عنها مثل الصور أو الملاحظات أو الرسائل (إذا لم يتم نسخها احتياطيًا).
- قد يستخدم مجرم الإنترنت رقم هاتفك للاحتيال على أشخاص آخرين.

كيف أقوم بتأمين جهازي المحمول؟

تأمين الجهاز:

- قم بإقفال جهازك بعبارة مرور أو كلمة مرور أو رقم تعريف شخصي أو رمز مرور. صعّب عملية التخمين - يسهل على مجرمي الإنترنت استنتاج تاريخ ميلادك وأنماط القفل الخاصة بك. استخدم عبارة مرور للحصول على الأمان الأمثل (انظر الصفحة 6). قد تفكر أيضًا في استخدام التعرف على الوجه أو بصمة الإصبع لإلغاء قفل جهازك.
- تأكد من ضبط جهازك على الإقفال تلقائيًا بعد فترة قصيرة من عدم النشاط.
- لا تشحن جهازك في محطة شحن عامة وتجنب أجهزة الشحن من أطراف ثالثة.
- تعامل مع هاتفك كأنه محفظتك، وحافظ على سلامته معك في جميع الأوقات.

تأمين البرامج والتطبيقات:

- استخدم ميزة التحديث التلقائي بجهازك لتثبيت التطبيق الجديد وتحديثات نظام التشغيل بمجرد توفرها (راجع الصفحة 5).
- اضبط الجهاز ليطلب عبارة/كلمة مرور قبل تثبيت التطبيقات. يمكن أيضًا استخدام أدوات الرقابة الأبوية لهذا الغرض.
- تحقق من أذونات الخصوصية بعناية عند تثبيت تطبيقات جديدة على جهازك، خاصة للتطبيقات المجانية. فقط قم بتثبيت التطبيقات من البائعين ذوي السمعة الطيبة.

تأمين البيانات:

- قم بتمكين وظائف الإقفال والمسح عن بُعد، إذا كان جهازك يدعمها.
- تأكد من إزالة البيانات الشخصية تمامًا من جهازك قبل بيعه أو التخلص منه.

تأمين الاتصال:

- قم بإيقاف تشغيل Bluetooth و Wi-Fi عندما لا تستخدمهما.
- تأكد من أن جهازك لا يتصل تلقائيًا بشبكات Wi-Fi الجديدة.

قم بتطوير طريقة تفكيرك فيما يتعلق بالأمن السيبراني

لا يقتصر الأمن السيبراني الشخصي على تغيير الإعدادات فحسب، بل يتعلق أيضًا بتغيير تفكيرك وسلوكياتك.

احترس من عمليات الاحتيال السيبرانية

يعرف عن مجرمين الإنترنت استخدام البريد الإلكتروني أو الرسائل أو وسائل التواصل الاجتماعي أو المكالمات الهاتفية لمحاولة الاحتيال على الأستراليين. قد يتظاهرون بأنهم فرد أو منظمة تعتقد أنك تعرفها، أو تعتقد أنك يجب أنه يجب أن تثق بها.

تحاول رسائلهم ومكالماتهم خداعك للقيام بإجراءات محددة، مثل:

- **الكشف عن تفاصيل الحساب المصرفي وكلمات المرور وأرقام بطاقات الائتمان**
- **منح الوصول عن بعد لجهاز الكمبيوتر**
- **فتح مرفق قد يحتوي على برمجيات خبيثة**
- **إرسال الأموال أو بطاقات الهدايا**

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

كيف أتعرف على رسائل الاحتيال؟

قد يكون من الصعب التعرف على رسائل الاحتيال. غالبًا ما يستخدم مجرمو الإنترنت أساليب معينة لخداعك. قد تشمل رسائلهم:

- **السلطة** – هل تدعي الرسالة أنها من شخص مسؤول، في البنك الذي تتعامل معه على سبيل المثال؟
- **الأهمية** – هل يتم إخبارك بوجود مشكلة، أو أن لديك وقتًا محدودًا للرد أو الدفع؟
- **المشاعر** – هل تجعلك الرسالة تشعر بالذعر أو الخوف أو التفاؤل أو الفضول؟
- **الندرة** – هل تعرض الرسالة شيئًا غير متاح بكثرة، أو تعدك بصفقة جيدة؟
- **الأحداث الجارية** – هل الرسالة عن قصة إخبارية جارية أو حدث كبير جارٍ؟

لمعرفة المزيد حول كيفية اكتشاف رسائل التصيد أو الاحتيال، أجب عن الاختبار على الموقع الإلكتروني الخاص بالمركز الأسترالي للأمن السيبراني cyber.gov.au.

ماذا أفعل إذا تلقيت رسالة احتيال؟

إذا تلقيت رسالة احتيال أو مكالمة هاتفية، فيجب عليك تجاهلها أو حذفها أو الإبلاغ عنها إلى وحدة "مراقبة الاحتيال" التابعة للمركز الأسترالي للأمن السيبراني على الموقع scamwatch.gov.au

يمكنك أيضًا الاتصال بالخط الساخن للأمن السيبراني التابع للمركز الأسترالي للأمن السيبراني على **1300 CYBER1** (1300292371) إذا كنت قلقًا بشأن الأمن السيبراني الخاص بك.

إذا كنت قد تعرضت لعملية احتيال وتعتقد أن حساباتك المصرفية أو بطاقات الائتمان أو الخصم المباشر الخاصة بك قد تكون في خطر، فاتصل على الفور بالمؤسسة المالية التي تتعامل معها. فقد يتمكنون من إغلاق حسابك أو إيقاف معاملة ما.

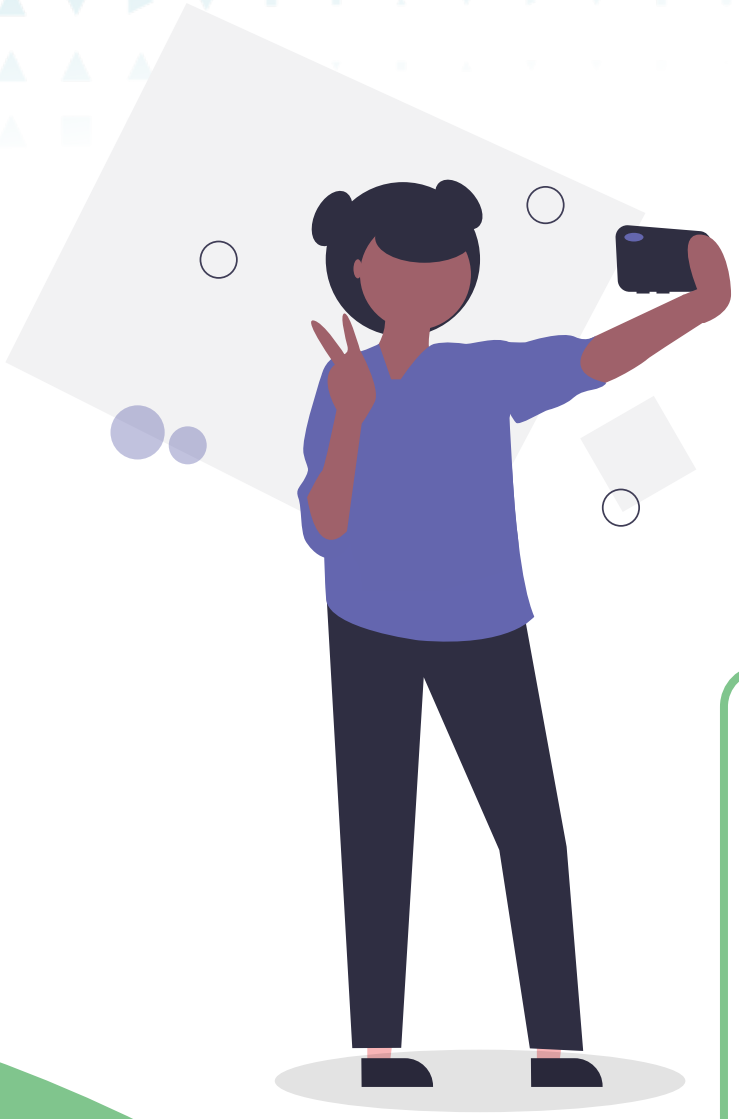
ماذا لو لم أكن متأكدًا مما إذا كانت الرسالة احتيالية؟

إذا كنت تعتقد أن رسالة أو مكالمة ما قد تكون بالفعل من مؤسسة تثق بها (مثل البنك الذي تتعامل معه)، فابحث عن طريقة اتصال يمكنك الوثوق بها. ابحث عن الموقع الرسمي أو اتصل برقم هاتفهم المعلن أو زر متجرهم أو فرعهم.
لا تستخدم الروابط أو تفاصيل الاتصال الموجودة في الرسالة المرسلة إليك أو المعطاة لك عبر الهاتف حيث إنها قد تكون احتيالية.

إذا كنت تعتقد أنك ضحية لجريمة سيبرانية، فأبلغ عنها من خلال ReportCyber التابع للمركز الأسترالي للأمن الأسترالي على الموقع cyber.gov.au أو اتصل بالخط الساخن للأمن السيبراني على 1300 CYBER1 (1300 292 371).

ابق على اطلاع بأحدث التهديدات: اشترك في خدمة التنبيهات المجانية الخاصة بالمركز الأسترالي للأمن السيبراني على الموقع cyber.gov.au والتي سترسل لك تنبيهًا عندما نحدد تهديدًا سيبرانيًا جديدًا.

توقف وفكر قبل أن تشارك شيئًا على



وسائل التواصل الاجتماعي

فكر قبل أن تشارك شيئًا على الإنترنت! يمكن لمجرمي الإنترنت استخدام المعلومات التي نشرتها علنًا على حساب/حسابات وسائل التواصل الاجتماعي الخاصة بك في عمليات الاحتيال والهجمات السيبرانية.

تذكر أن الإنترنت دائم ولا يمكنك أبدًا إزالة ما تم نشره بالكامل.

كيف يمكنني التوقف والتفكير قبل النشر؟

- **فكر:** كيف يمكن لمجرم الإنترنت استخدام هذه المعلومات لاستهدافي أو استهداف حساباتي؟
- **فكر:** هل سأكون مرتاحًا لعرض هذه المعلومة أو الصورة لشخص غريب تمامًا خارج الإنترنت؟

ما هي المعلومات التي يجب أن أتجنب مشاركتها؟

تجنب مشاركة المعلومات (بما في ذلك الصور) عبر الإنترنت التي يمكن لمجرمي الإنترنت استخدامها من أجل: التعرف عليك أو التلاعب بك من خلال عملية احتيال أو استنتاج أسئلة استرداد حسابك. قد يشمل ذلك:

- **مكان الميلاد وتاريخ الميلاد**
- **العنوان ورقم الهاتف**
- **صاحب العمل وتاريخ العمل**
- **المكان الذي درست فيه**
- **أي معلومات شخصية أخرى** يمكن استخدامها لاستهدافك

قائمة مرجعية موجزة

هل أكملت كل شيء في هذا الدليل؟

استخدم هذه القائمة المرجعية المفيدة لتتبع تقدمك:

- **قمت بتشغيل التحديثات التلقائية لجميع أجهزتي:**
  - الكمبيوتر (المكتبي والمحمول)
  - الهاتف الجوال
  - الحاسوب اللوحي
- **قمت بتنشيط المصادقة متعددة العوامل لحساباتي الأكثر أهمية:**
  - جميع حساباتي المصرفية والمالية عبر الإنترنت (على سبيل المثال، البنك الذي تتعامل معه، PayPal)
  - جميع حسابات البريد الإلكتروني الخاصة بي (مثل Gmail و Outlook و Hotmail و Yahoo!)
- **أقوم بإجراء نسخ احتياطي لأجهزتي بانتظام:**
  - الكمبيوتر (المكتبي والمحمول)
  - الهاتف الجوال
  - الحاسوب اللوحي
- **أستخدم عبارات مرور قوية وفريدة في حساباتي الأكثر الأهمية وغير المحمية بالمصادقة متعددة العوامل:**
  - الحسابات المصرفية والمالية عبر الإنترنت
  - حسابات البريد الإلكتروني
- **قمت بتأمين أجهزتي المحمول:**
  - الحاسوب المحمول
  - الهاتف الجوال
  - الحاسوب اللوحي
- **أستخدم طريقة تفكير آمنة عبر الإنترنت كل يوم:**
  - يمكنني التعرف على رسائل الاحتيال
  - أعرف ما يجب فعله إذا تلقيت رسالة احتيال.
  - أعرف كيف أتحقق مما إن كانت رسالة ما احتيالية إن كنت غير متأكد من ذلك
  - أفكر قبل أن أنقر على الروابط والمرفقات
  - أفكر قبل أن أشارك أي شيء على وسائل التواصل الاجتماعي
- **أعرف من أين يمكنني الحصول على المساعدة إذا كنت ضحية لجريمة إلكترونية أو عملية احتيال**

مسرد

استعادة الحساب

عملية يتم فيها استخدام مجموعة من الأسئلة أو طرق تحقق أخرى لاسترداد أو استعادة الوصول إلى أحد الحسابات لتغيير عبارة/كلمة مرور خاصة بحساب.

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.

السحابة

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

مجرم الإنترنت

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

الجهاز

جهاز حوسبة أو اتصالات. على سبيل المثال، جهاز كمبيوتر أو كمبيوتر محمول أو هاتف محمول أو جهاز لوحي.

نهاية الدعم

تشير نهاية الدعم إلى الموقف الذي تتوقف فيه الشركة عن دعم منتج أو خدمة. يتم تطبيق هذا عادةً على منتجات الأجهزة والبرامج عندما تقوم الشركة بإطلاق إصدار جديد وإنهاء دعم الإصدارات السابقة.

البرمجيات الخبيثة

البرامج الضارة المستخدمة للحصول على وصول غير مصرح به والتحكم في جهاز كمبيوتر المستخدم، وسرقة المعلومات وتعطيل الشبكات.

نظام التشغيل

برنامج مثبت على محرك الأقراص الثابتة بجهاز الكمبيوتر وهو يمكن أجهزة الكمبيوتر من الاتصال ببرامج الكمبيوتر وتشغيلها. أمثلة: Microsoft Windows وApple macOS وiOS وAndroid.

الرمز المادي

جهاز مادي يمكن عادةً وضعه في حلقة مفاتيح، وهو يولّد رمز أمان يستخدم لتأكيد هوية مستخدم الكمبيوتر باستخدام المصادقة متعددة العوامل.

الوصول عن بعد

الوصول والتحكم في الأجهزة والشبكات من موقع بعيد عن مكانها.

البرمجيات

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

الدليل التالي في سلسلة الأمن السيبراني الشخصي.

بعد أن أكملت الآن دليل المركز الأسترالي للأمن السيبراني *الأمن السيبراني الشخصي: الخطوات الأولى* يجب أن تبدأ دليل *الأمن السيبراني الشخصي: الخطوات التالية* والمتاح على موقع cyber.gov.au.

***دليل الأمن السيبراني الشخصي: الخطوات التالية* يوضح الإجراءات التي يمكنك اتخاذها الآن لزيادة مستوى الأمن السيبراني لديك.**

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