



Australian Government

تصرف الآن. حافظ على أمنك.

كيف تبقى آمناً على الإنترنت

نسخة سهلة القراءة



كيفية استخدام هذا الدليل

نحن الحكومة الأسترالية.

قمنا بكتابة هذا الدليل.



كتبنا بعض الكلمات بخط عريض.

وسوف نشرح معنى هذه الكلمات.

يوجد أيضاً قائمة بهذه الكلمات في الصفحة 28.



يمكنك أن تطلب المساعدة من شخص تثق به من أجل:

- قراءة هذا الدليل

- العثور على مزيد من المعلومات.



إن هذا الدليل هو ملخص مُبسّط لدليل آخر.

ويحتوي فقط على أهم الأفكار.



يُمكنك العثور على الدليل الآخر على موقعنا الإلكتروني:

www.actnowstaysecure.gov.au



ماذا يوجد في هذا الدليل؟

4 حول هذا الدليل

6 حافظ على أمان حساباتك

10 تحقق من إعداداتك لحماية معلوماتك

16 قُم بحماية أجهزتك

20 عمليات الاحتيال

25 تحدث واطلب المساعدة

28 قائمة الكلمات

30 اتصل بنا

حول هذا الدليل

جميعنا بحاجة إلى التفكير في كيفية البقاء آمنين على الإنترنت.

نسمي هذا بالأمن السيبراني.



كلمة **سايبير** تعني أن الشيء له علاقة بالإنترنت.



يشرح هذا الدليل بعض الأشياء التي يمكنك القيام بها لحماية نفسك على الإنترنت.

على سبيل المثال، الحماية من **الجرائم الإلكترونية**.



تحدث الجرائم الإلكترونية عندما يستخدم المجرمون الإنترنت للقيام بجرائم.

على سبيل المثال، قد يستخدمون الإنترنت من أجل:

- سرقة معلوماتك الشخصية
- السيطرة على حساباتك أو ملفاتك على الإنترنت.



يمكن أن تحدث الجرائم الإلكترونية على أي جهاز:

وهذا يشمل:

- الحاسوب
- الهاتف الذكي
- الساعة الذكية.



هناك أشياء يمكنك القيام بها للبقاء آمناً من الجرائم الإلكترونية.



سنقوم بشرح ما يمكنك القيام به في الصفحات التالية.



حافظ على أمان حساباتك

يجب أن تفكر في كيفية الحفاظ على أمان حساباتك على الإنترنت.



قُم باستخدام عبارات مرور قوية ومختلفة لكل حساب

عبارة المرور هي نوع أقوى من كلمة المرور.

ويصعب جداً على الآخرين تخمينها.



استخدام عبارات مرور قوية ومختلفة هو من أفضل الطرق لحماية حساباتك.



يجب أن تستخدم عبارة مرور مختلفة لكل حساب من حساباتك على الإنترنت.



تشمل عبارات المرور القوية:

- 4 كلمات عشوائية أو أكثر
- 15 حرفاً ورقماً أو أكثر.



يمكنك استخدام بعض الأحرف الكبيرة.



مكنك أيضاً استخدام رموز مثل:

- شَرْطَة (-)
- رمز الدولار (\$)
- رمز @ في البريد الإلكتروني.



يجب ألا تستخدم أي معلومات شخصية في عبارات المرور الخاصة بك.



على سبيل المثال:

- تاريخ ميلادك
- أسماء أفراد عائلتك أو حيواناتك الأليفة.



قُم بإضافة خطوات إضافية لتسجيل الدخول إلى حساباتك

يمكنك حماية حساباتك على الإنترنت باستخدام

المصادقة متعددة العوامل (MFA).

المصادقة متعددة العوامل هي استخدام طريقتين مختلفتين أو أكثر لتسجيل الدخول إلى حسابك في كل مرة.



على سبيل المثال، قد تحتاج أولاً إلى إدخال عبارة المرور الخاصة بك

ثم تقوم بإدخال رمز يصلك على هاتفك.



قد يكون لديك خيار:

- تحميل تطبيق على هاتفك ليعطيك الرمز.



- استلام الرمز عبر البريد الإلكتروني.



- استلام الرمز عبر رسالة نصية.



إن المصادقة المتعددة العوامل تجعل الوصول إلى حساباتك على الإنترنت أمراً صعباً على الآخرين. حتى لو تمكنوا من معرفة عبارة المرور الخاصة بك.



تحقق من إعداداتك لحماية معلوماتك

يمكنك التأكد من أن إعداداتك تحمي معلوماتك على الإنترنت.



يشمل ذلك الإعدادات على:

- حساباتك عبر الإنترنت
- أجهزتك
- تطبيقاتك.



يمكنك:

- تغيير إعداداتك
- اختيار التطبيقات التي يمكنها استخدام معلوماتك.



يمكنك العثور على الإعدادات على جهازك عن طريق:

- البحث عن رمز الترس

أو

- كتابة كلمة "الإعدادات" في شريط البحث على جهازك.



يمكنك العثور على الإعدادات في تطبيق أو حساب عبر الإنترنت من خلال فتح القائمة.

وغالبًا ما تظهر القائمة على شكل ثلاثة خطوط مستقيمة.



يمكن أن تشارك بعض هذه الإعدادات معلومات عن:

- من أنت
- أين أنت
- أين تقطن.



يمكن أن يعرّضك مشاركة هذه المعلومات عبر الإنترنت
لخطر الجرائم الإلكترونية.



يمكن لمجرمي الإنترنت استخدام معلوماتك لتقمّص
هويتك والتظاهر بأنهم أنت.



على سبيل المثال، قد يستخدمون معلومات مثل:

- مكان سكنك



- أسماء أفراد عائلتك



- أسماء حيواناتك الأليفة.



يمكنك ضبط حساباتك بحيث لا يتمكن من رؤية ملفاتك
على وسائل التواصل الاجتماعي إلا الأشخاص الذين
تعرفهم.



على سبيل المثال، ملفك الشخصي على فيسبوك.



تُسمى هذه الإعدادات عادةً "إعدادات الخصوصية".



يمكنك أيضاً التحكم في **إعدادات الموقع**.

تُظهر إعدادات الموقع مكان وجود جهازك.



يمكنك تشغيل إعدادات الموقع أو إيقافها.

كما يمكنك اختيار التطبيقات التي يمكنها استخدام إعدادات موقعك.

يمكنك القيام بذلك في:

- حساباتك عبر الإنترنت
- أجهزتك
- تطبيقاتك.



قد تطلب منك بعض التطبيقات أيضاً السماح لها ب :

- استخدام الكاميرا الخاصة بك



- رؤية صورك.



يجب أن تسمح فقط للتطبيقات التي تثق بها وتعرفها
باستخدام الكاميرا والصور الخاصة بك.



قُم بحماية أجهزتك

يجب أن تفكر في كيفية حماية أجهزتك للمساعدة
في الحفاظ على سلامتك عبر الإنترنت.
على سبيل المثال، هاتفك أو ساعتك الذكية.



هذه الخطوة مهمة خاصةً للأجهزة المتصلة بالإنترنت.



قُم بتحديث أجهزتك

يمكنك تحديث أجهزتك للحفاظ على سلامتها عبر
الإنترنت.
على سبيل المثال، هاتفك المحمول وجهاز الحاسوب
المحمول.



قد يُطلق جهازك على ذلك اسم "تحديث البرمجيات".



تساعد التحديثات الجهاز على حماية نفسه من الجرائم الإلكترونية.



يمكنك ضبط الجهاز ليقوم بالتحديث تلقائياً.



يمكنك معرفة المزيد حول كيفية تحديث أجهزتك على موقعنا الإلكتروني.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)



شبكات الإنترنت اللاسلكي العامة

يجب أن تكون حذراً عند استخدام شبكات الإنترنت اللاسلكي العامة واي فاي



شبكة الإنترنت اللاسلكي العامة هي إنترنت لاسلكي مجاني يمكنك استخدامه في الأماكن العامة.



على سبيل المثال في:

- مقهى
- مطار
- فندق.



يجب أن تكون حذراً بشأن المعلومات التي تُدخلها
إلى موقع إلكتروني عند استخدام أي شبكة إنترنت
لاسلكي عامة.



على سبيل المثال:

- تفاصيل حسابك البنكي
- حسابات البريد الإلكتروني الخاصة بك
- ملفاتك على وسائل التواصل الاجتماعي.



يمكن لبعض مجرمي الإنترنت استخدام شبكة الإنترنت
اللاسلكي العامة من أجل:

- مراقبة ما تفعله عبر الإنترنت
- سرقة معلوماتك.



وذلك لأن:

- بإمكان أي شخص استخدامها



- يكون من الصعب حماية أجهزتك.



يمكنك معرفة كيفية البقاء آمناً عند استخدام شبكة الإنترنت اللاسلكي العامة على موقعنا الإلكتروني:

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)



عمليات الاحتيال

تُسميها **عملية احتيال** عندما يحاول شخص ما:

- خداعك
- أخذ أموالك.



المحتال هو الشخص الذي يقوم بعمليات الاحتيال.



قد يحاول المحتالون خداعك من خلال:

- رسالة نصية أو مكالمة هاتفية
- بريد إلكتروني
- وسائل التواصل الاجتماعي
- مواقع الإنترنت.



قد يبدو ودودين.

لكنهم قد يخدعونك لتزودهم بمعلوماتك.



يمكنهم استخدام هذه المعلومات لـ:

- الدخول إلى حساباتك على الإنترنت



- انتحال شخصيتك



- سرقة أموالك.



قد يقوم المحتالون أيضاً بـ:

- إنشاء حسابات مزيفة لخداعك



- مشاركة روابط وإعلانات لتنقر عليها.



كيف تكتشف عملية احتيال

قد تكون عملية احتيال إذا:

- طُلب منك القيام بشيء بسرعة



- عُرض عليك الكثير من المال



- طُلب منك المال



- طُلب منك النقر على رابط.



قد ينتحل المحتالون أيضاً صفة مؤسسة تعرفها وتثق بها.



على سبيل المثال: البنك الذي تتعامل معه.

يقوم المحتالون بذلك لكي تشاركهم معلوماتك الشخصية.



يجب عليك التوقف عن التواصل مع الشخص إذا كنت تعتقد أنه محتال.



يجب عليك التأكد من أن الشخص هو فعلاً من يدّعي أنه هو.



يمكنك التواصل مع الشخص أو المؤسسة باستخدام معلومات موثوقة قمت بالعثور عليها بنفسك.

اتخذ إجراءً سريعاً لحماية نفسك إذا شعرت أن هناك أمراً مريباً.



الإبلاغ عن عملية احتيال

يساعد موقع Scamwatch الأستراليين على:

- فهم عمليات الاحتيال
- الإبلاغ عن عمليات الاحتيال.



كما يساعد موقع Scamwatch الأستراليين الذين
تعرضوا لعمليات احتيال.



يمكنك الإبلاغ عن عملية احتيال عبر موقع Scamwatch
الإلكتروني:

www.scamwatch.gov.au/report-a-scam



تحدث واطلب المساعدة

يجب أن تعبر عن مخاوفك وتُحدّر الآخرين عن كيفية حماية أنفسهم على الإنترنت.



يشمل ذلك:

- الإبلاغ عن الجرائم الإلكترونية



- مشاركة ما تعرفه مع العائلة والأصدقاء.



سنشرح كيف يمكنك التعبير عن مخاوفك والإبلاغ في الصفحات التالية.



الإبلاغ عن الجرائم الإلكترونية

إن الإبلاغ عن الجرائم الإلكترونية يساعد الحكومة على:

- التعرف على كيفية محاولة المجرمين الإلكترونيين مهاجمة الأشخاص



- حماية المزيد من الأشخاص.



يمكنك الإبلاغ عن الجرائم الإلكترونية عبر موقع

.ReportCyber

www.cyber.gov.au/report



تحدث مع العائلة والأصدقاء حول كيفية البقاء آمناً على الإنترنت

يجب عليك مشاركة نصائحك حول البقاء آمناً على الإنترنت مع عائلتك وأصدقائك. ويمكنك أيضاً التعلم منهم.



يمكنك حماية نفسك ومن حولك من خلال مشاركة ما تعرفه عن كيفية البقاء آمناً على الإنترنت.



هذا الأمر مهم أيضاً إذا كنت تشارك الأجهزة مع الآخرين.



قائمة الكلمات

تشرح هذه القائمة معنى الكلمات المكتوبة بخط عريض في هذا الدليل.

سايبير

تعني كلمة "سايبير" شيئًا له علاقة بالإنترنت.



الجريمة الإلكترونية

الجريمة الإلكترونية هي عندما يستخدم المجرمون

الإنترنت لارتكاب الجرائم.

على سبيل المثال، قد يستخدمون الإنترنت من أجل:

- سرقة معلوماتك الشخصية
- السيطرة على حساباتك عبر الإنترنت.



إعدادات الموقع

تُظهر إعدادات الموقع مكان وجود جهازك.



المصادقة متعددة العوامل (MFA)

وهي عندما تستخدم طريقتين مختلفتين أو أكثر لتسجيل الدخول إلى حسابك في كل مرة.



عبارة المرور

عبارة المرور هي نوع أقوى من كلمة المرور. ويصعب جداً على الآخرين تخمينها.



شبكة الإنترنت اللاسلكي العامة واي فاي

هو إنترنت لاسلكي مجاني يمكنك استخدامه في الأماكن العامة.



الاحتيال عمليات

نُسميه احتيلاً عندما يحاول شخص ما:

- خداعك
- أخذ أموالك.



المحتال

المحتال هو شخص يقوم بعمليات احتيال.



اتصل بنا

يمكنك الاتصال بالخط الساخن الخاص بالأمن السيبراني
في أستراليا.

1300 292 371



يمكنك زيارة موقعنا الإلكتروني.

www.actnowstaysecure.gov.au



يمكنك الإبلاغ عن الجرائم الإلكترونية عبر موقع

ReportCyber

www.cyber.gov.au/report



أعد فريق "Information Access Group" هذا المستند

السهل القراءة باستخدام صور فوتوغرافية جاهزة وصور

مخصصة. ولايجوز استخدام الصور بدون إذن.

للاستفسار عن الصور، يرجى زيارة موقع

www.informationaccessgroup.com.



أذكر رقم الوظيفة: 6342