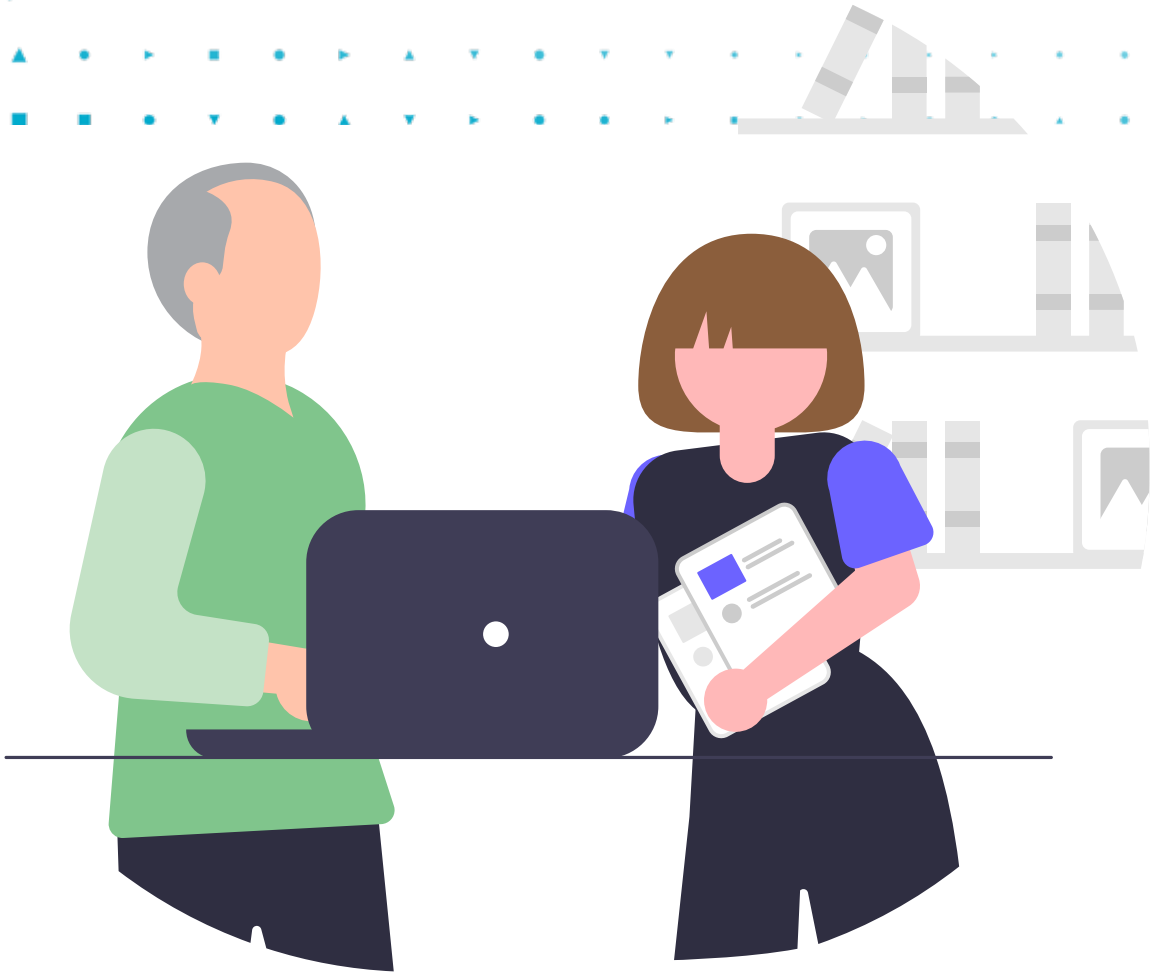
ACSC Australian Cyber Security Centre

Australian Government
Australian Signals Directorate



كيفية استخدام الإنترنت بأمان

دليل لكبار السن

cyber.gov.au

المقدمة

يتيح لك الاتصال بالإنترنت البقاء على اتصال بالأصدقاء والأهل والتعرف على بعض الموضوعات بل وحتى ممارسة الألعاب.

تمامًا مثل ربط حزام الأمان قبل القيادة، يجب أن تتخذ بعض الخطوات قبل استخدام الإنترنت لتكون أكثر أمانًا.

يريد مركز الأمن السيبراني الأسترالي (ACSC) التأكد من أن الجميع آمنون عندما يتصلون بالإنترنت. تتناول هذه الوثيقة بعض ممارسات الأمن السيبراني الأساسية التي يمكنك استخدامها لحماية نفسك عند الاتصال بالإنترنت.

يقدم المركز الأسترالي للأمن السيبراني، بصفته جزءًا من مديرية الإشارات الأسترالية (ASD)، المشورة والمساعدة والاستجابات التشغيلية لمنع واكتشاف ومعالجة التهديدات السيبرانية لأستراليا. 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 cyber.gov.au

الأمن السيبراني لكبار السن

النصيحة 1: قم بتحديث جهازك

يشبه تحديث برامجك القيام بصيانة سيارتك. من شأنه تحسين أداء جهازك وجعله أكثر أمانًا.

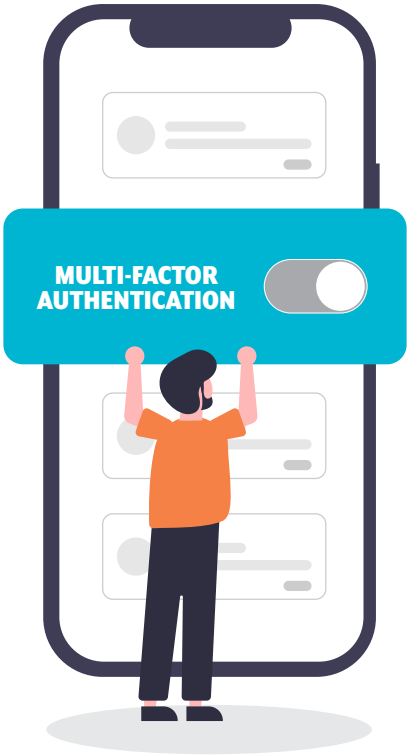
دائمًا ما يجد مجرمو الإنترنت طرقًا جديدة لاختراق الأجهزة. من شأن ضبط جهازك ليقوم بتثبيت التحديثات تلقائيًا أن يصلح أي نقاط ضعف في برامجك وإبعاد المخترقين.

للعثور على دليلنا التفصيلي خطوة بخطوة لتشغيل التحديثات التلقائية:

1. قم بزيارة **cyber.gov.au**
2. انقر على **الأفراد والعائلات**
3. انقر على **أدلة تفصيلية خطوة بخطوة**
4. ابحث **تشغيل التحديثات التلقائية**
5. اختر ما بين أجهزة أبل أو ويندوز.

هل كنت تعلم أن:
ستضيف التحديثات أيضًا ميزات جديدة إلى جهازك وتجعله يعمل بشكل أسرع.

النصيحة 2: قم بتشغيل المصادقة متعددة العوامل



المصادقة متعددة العوامل على حسابك تشبه ما تفعله شاشة المراقبة الأمنة بمنزلك. تحميك من المجرمين الذين يحاولون الاقتحام.

مع تنشيط المصادقة متعددة العوامل، تحتاج إلى تقديم أجزاء متعددة من المعلومات للوصول إلى حسابك. على سبيل المثال، قد تحتاج إلى إدخال كلمة المرور الخاصة بك ورمز رسالة نصية لتسجيل الدخول إلى ملفك على وسائل التواصل الاجتماعي.

تصعب الطبقات المتعددة الاختراق على مجرمي الإنترنت. قد يتمكنون من حل جزء واحد، مثل كلمة المرور الخاصة بك، لكنهم سيظلون بحاجة إلى الحصول على أجزاء أخرى من اللغز للوصول إلى حسابك.

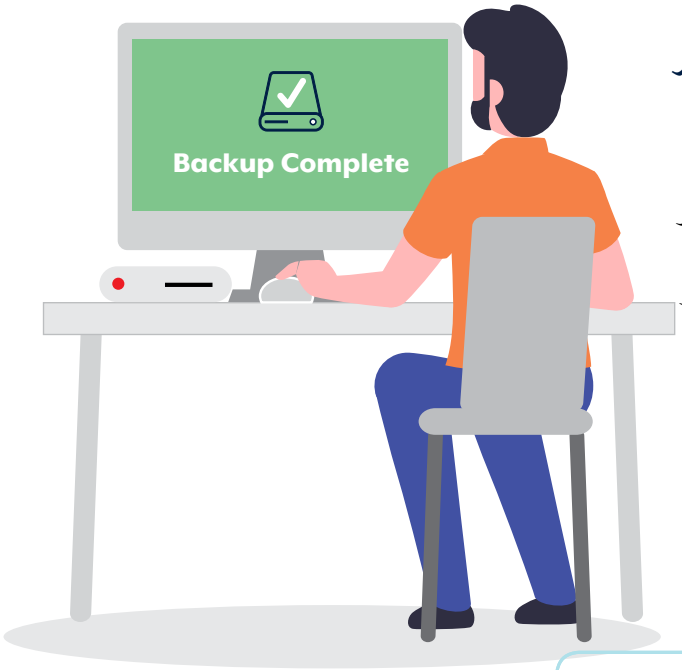
للعثور على دليلنا التفصيلي خطوة بخطوة بشأن المصادقة مزدوجة العوامل:

1. قم بزيارة **cyber.gov.au**
2. انقر على **الأفراد والعائلات**
3. انقر على **أدلة تفصيلية خطوة بخطوة**
4. ابحث **تشغيل المصادقة مزدوجة العوامل**
5. اختر الدليل المناسب لنوع حسابك (مثل فيسبوك أو جيميل أو معرف أبل).

تذكر:

إذا كنت بحاجة إلى مساعدة في تشغيل المصادقة متعددة العوامل، فاطلب المساعدة من أحد الأصدقاء أو أفراد العائلة.

النصيحة 3: قم بإجراء نسخ احتياطي لجهازك.



إجراء "نسخ احتياطي" هو صنع نسخة من ملفاتك المهمة ووضعها في مكان آمن. إنه مثل نسخ الصور الثمينة للاحتفاظ بها في مكان آمن في حالة فقد النسخ الأصلية.

عند إجراء نسخ احتياطي لجهاز الكمبيوتر أو الهاتف أو الجهاز اللوحي، يتم حفظ نسخ من ملفاتك على الإنترنت أو على جهاز منفصل. الاحتفاظ بنسخة احتياطية من ملفاتك المهمة والصور العزيزة عليك سيمنحك راحة البال.

إذا حدث خطأ ما بجهازك أو تعرضت للاختراق من قبل مجرمي الإنترنت، فيمكنك بسهولة استعادة ملفاتك من النسخ الاحتياطية.

للعثور على دليلنا التفصيلي خطوة بخطوة للنسخ الاحتياطي واستعادة ملفاتك:

1. قم بزيارة **cyber.gov.au**
2. انقر على **الأفراد والعائلات**
3. انقر على **أدلة تفصيلية خطوة بخطوة**
4. ابحث **النسخ الاحتياطي واستعادة ملفاتك**
5. اختر ما بين أجهزة أبل أو ويندوز.

هل كنت تعلم أن:

مع إجراء نسخ احتياطي لجهازك بانتظام أنه سيكون بإمكانك الوصول دائمًا إلى أحدث ملفاتك.

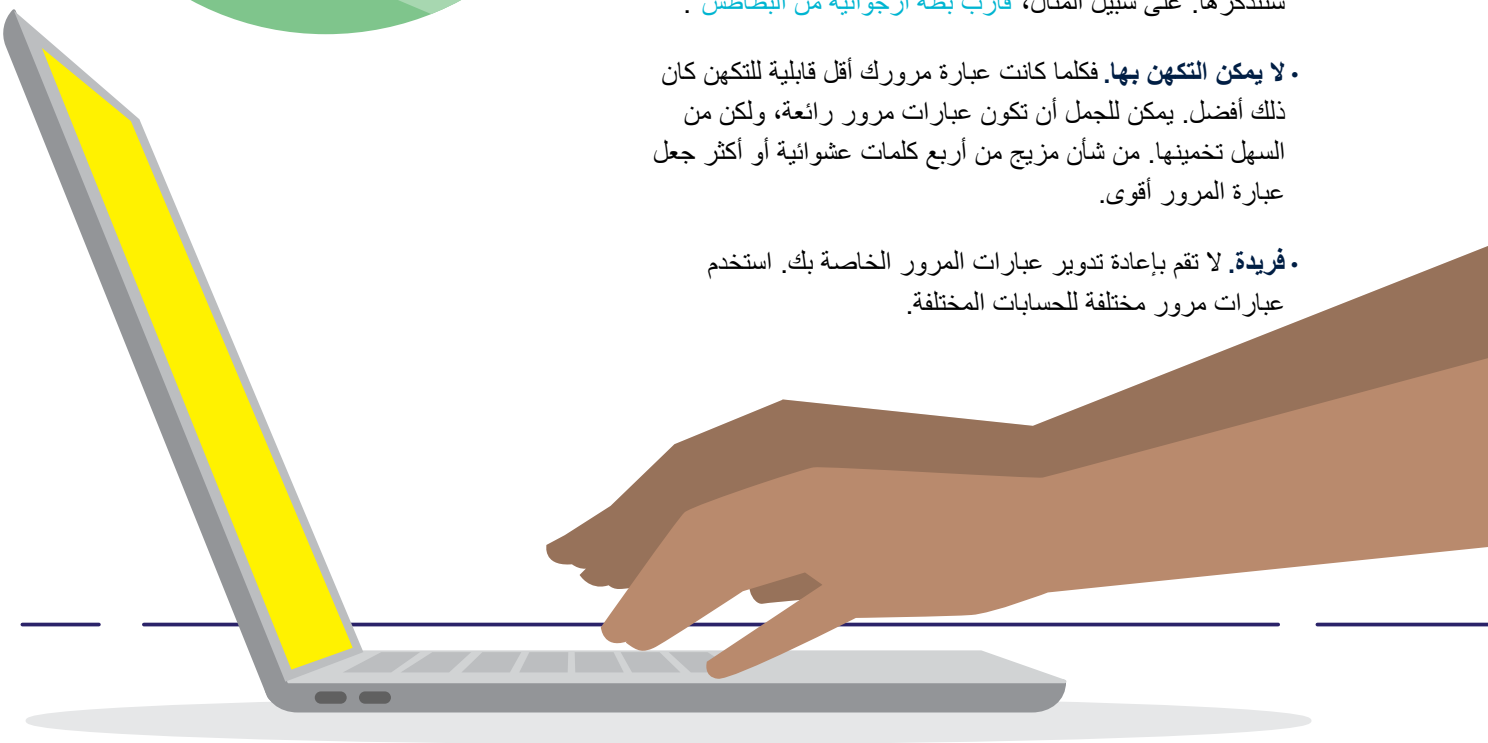
النصيحة 4: استخدم عبارة مرور

إذا أقفلت كلمة مرور حسابك، فإن عبارة المرور تقدم نظام أمان خاصًا بها! إنها نُسخ أقوى وأكثر أمانًا من كلمات المرور.

عندما لا يمكنك تشغيل المصادقة متعددة العوامل، استخدم عبارة مرور لتأمين حسابك. تستخدم عبارات المرور أربع كلمات عشوائية أو أكثر لتصبح كلمة المرور الخاصة بك. هذا يجعل تخمينها صعبًا على مجرمي الإنترنت ولكن يسهل عليك تذكرها.

عندما تقوم بإنشاء عبارة مرور، اجعلها:

- **طويلة.** فكلما كانت أطول كان ذلك أفضل. فليكن هدفك جعلها 14 حرفًا على الأقل. من الرائع أن تكون أربع كلمات عشوائية أو أكثر ستتذكرها. على سبيل المثال، "قارب بطة أرجوانية من البطاطس".
- **لا يمكن التكهن بها.** فكلما كانت عبارة مرورك أقل قابلية للتكهن كان ذلك أفضل. يمكن للجمل أن تكون عبارات مرور رائعة، ولكن من السهل تخمينها. من شأن مزيج من أربع كلمات عشوائية أو أكثر جعل عبارة المرور أقوى.
- **فريدة.** لا تقم بإعادة تدوير عبارات المرور الخاصة بك. استخدم عبارات مرور مختلفة للحسابات المختلفة.



تعرف على المزيد عن إنشاء كلمات مرور آمنة في موقع
/cyber.gov.au/acsc/view-all-content/publications
creating-strong-passphrases

النصيحة 5: تعرف على الحيل وأبلغ عنها.

كلما أسرعت في الإبلاغ عن عمليات الاحتيال، كان بإمكاننا التصرف بشكل أسرع.

إذا كنت تعتقد أن شخصًا ما يحاول استخدام الإنترنت في خداعك، فمن الأفضل أن تتصرف بشكل استباقي وبحذر بدلًا من المخاطرة بالتعرض للاستغلال.

إذا بدا الأمر جيدًا لدرجة يصعب تصديقها، فمن المرجح أن يكون كذلك. فبينما قد تقول رسالة ما أنك فزت بجائزة أو أن جهاز الكمبيوتر الخاص بك يحتوي على فيروس، فإن هذه الرسالة ليست فريدة بالنسبة لك.

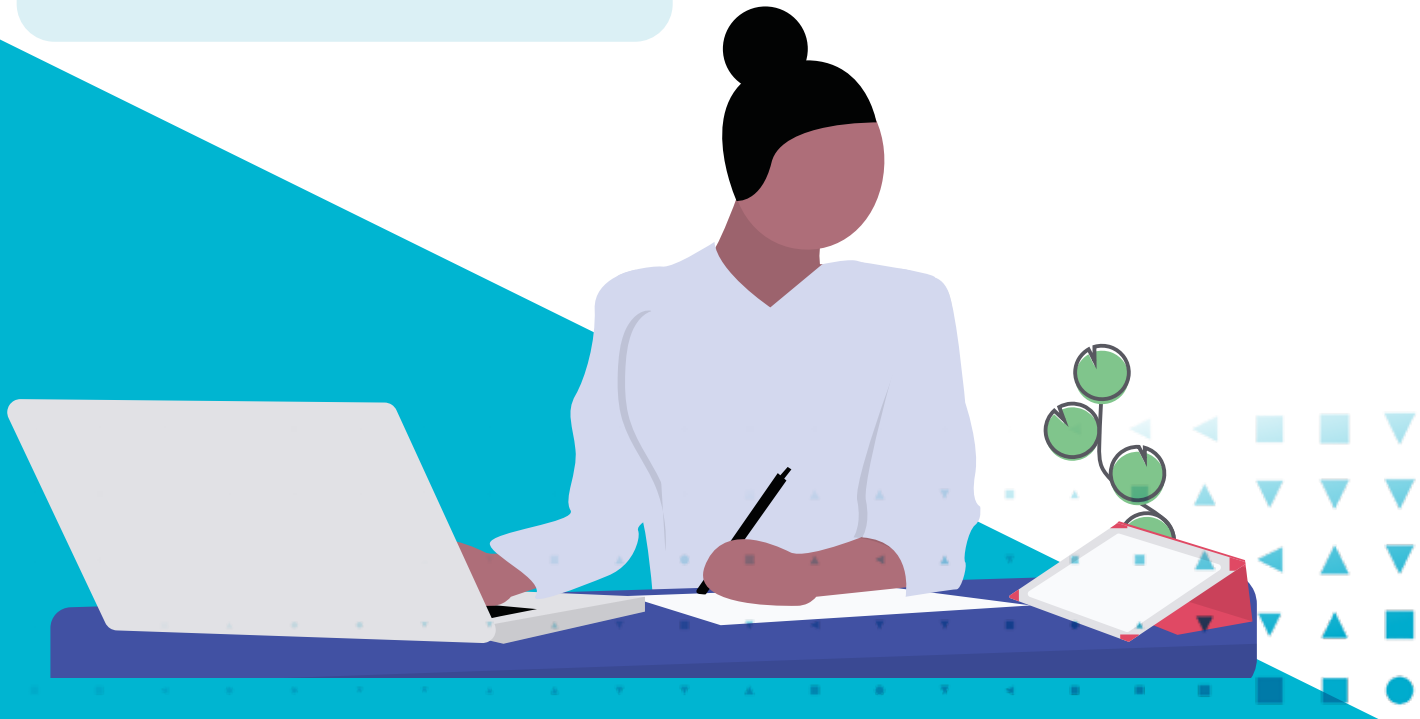
قد تكون قادمة من محتال يريد استغلالك.

قم بزيارة موقع **scamwatch.gov.au** وموقع **cyber.gov.au** للإبلاغ عن الاحتيال.

هل كنت تعلم أن:

يتسم مجرمو الإنترنت بالمكر وقد يستخدمون اسمًا وعنوان بريد إلكتروني مألوفين. كن حذرًا إذا:

- **طُلب منك دفع فاتورة على وجه السرعة**
- **طُلب منك تغيير التفاصيل أو كلمة المرور الخاصة بك**
- **طُلب منك النقر على رابط أو فتح مرفق.**



الختام

بعد أن أصبحت الآن مسلحًا بالمعرفة لاستخدام الإنترنت بشكل أكثر أمانًا، يمكنك التصفح بثقة والاستمتاع بوقتك على الإنترنت.

فقط تذكر أن مجرمي الإنترنت يبتكرون دائمًا
طرقًا جديدة لاستهداف الأشخاص.

لا يضر مطلقًا أن تراجع معرفتك بالأمن السيبر
اني من وقت لآخر وتتعلم
طرقًا جديدة للبقاء آمنًا.

نصائح إضافية

هل تريد معرفة المزيد من طرق البقاء آمنًا عبر الإنترنت؟ اطلع على النصائح التالية.

فكر فيما تنشره.

فكر جيدًا في المعلومات التي تشاركها عبر الإنترنت ومن سيطلع عليها. لا تقبل طلبات صداقة إلا من الأشخاص الذين تعرفهم في الحياة الواقعية.

احصل على تنبيهات بشأن التهديدات الجديدة.

اشترك في خدمة التنبيهات المجانية الخاصة بنا. من شأن هذا إبلاغك كلما وجدنا تهديدًا إلكترونيًا جديدًا.

كما سيعطيك نصائح حول ما يجب فعله في حالة حدوث هجوم.

تحدث عن الأمن السيبراني مع عائلتك وأصدقائك.

بعد أن أصبحت الآن ماهرًا في مجال الأمن السيبراني، شارك ما تعلمته مع عائلتك وأصدقائك. يمكن لمعرفتك أن تساعدهم في الخروج من موقف أثناء استخدام الإنترنت!

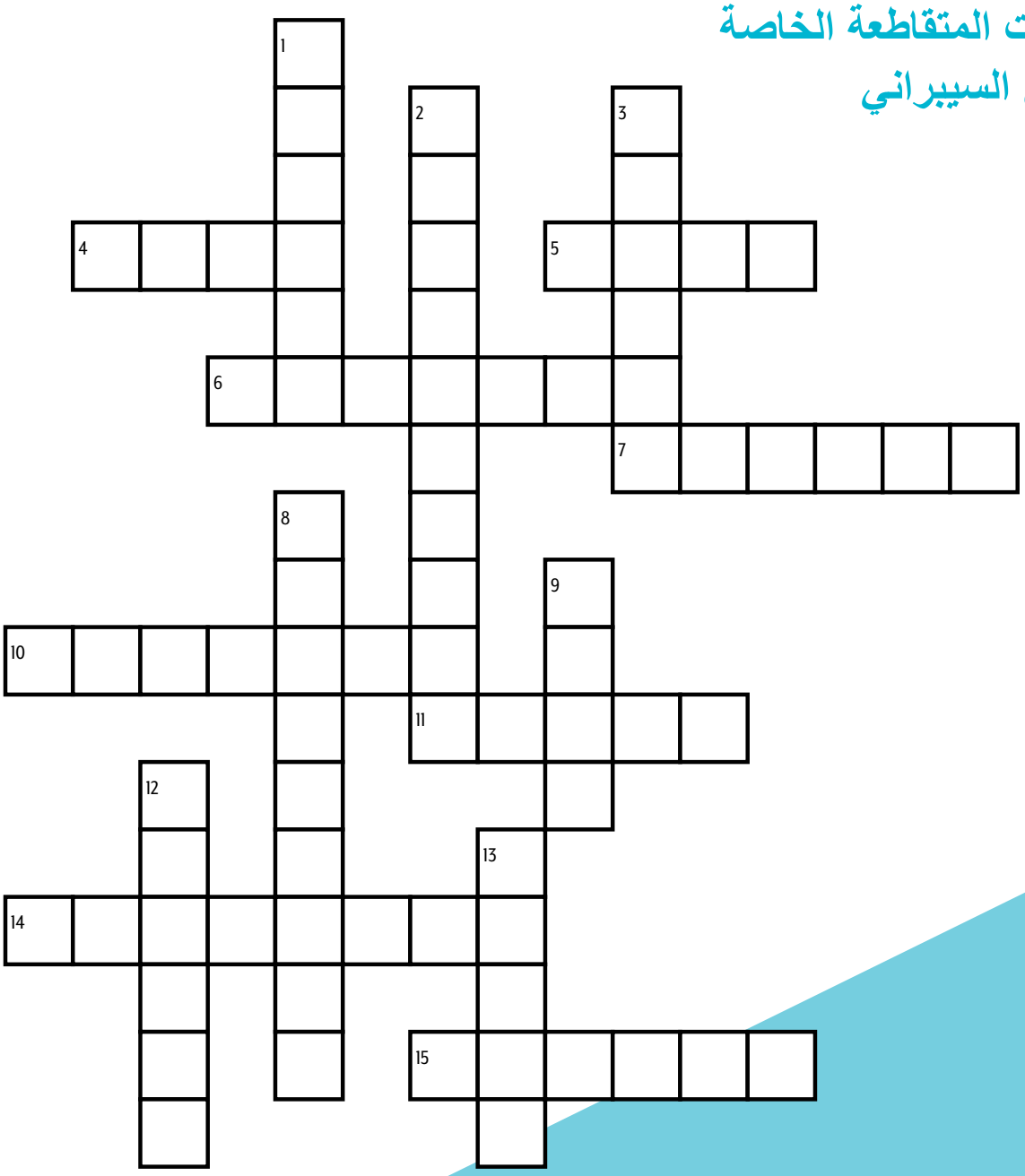
تجنب شبكات Wi-Fi العامة عند إجراء المعاملات المصرفية أو التسوق عبر الإنترنت.

تعد شبكات Wi-Fi العامة رائعة لمشاهدة مقاطع الفيديو أو قراءة المواقع الإلكترونية ولكن اجعل أي نشاط عبر الإنترنت يتضمن أموالًا في شبكة الإنترنت الخاصة بمنزلك. قد تكون شبكات Wi-Fi العامة محفوفة بالمخاطر.

أبلغ عن الهجمات والحوادث الإلكترونية للحفاظ على أمن أستراليا.

إذا كنت تعتقد أنك وقعت ضحية لجريمة إلكترونية، فتصرف بسرعة. ستجد المزيد من النصائح على موقع cyber.gov.au

الكلمات المتقاطعة الخاصة بالأمن السيبراني



رأسي

1. متصل بالإنترنت
2. كلمة مرور قوية
3. شخص يستخدم أجهزة الكمبيوتر لسرقة البيانات
8. برامج تدمر الفيروسات
9. حيلة أو خدعة
12. نسخة من ملفات جهاز الكمبيوتر الخاص بك
13. يتعلق بأجهزة الكمبيوتر أو يتضمنها

أفقي

4. تقنية الشبكات اللاسلكية
5. الوكالة الرائدة في أستراليا للأمن السيبراني
6. وثيقة على شبكة الويب العالمية
7. تقديم معلومات عن شيء ما
10. إصدارات جديدة من البرامج أو محسّنة وأكثر أمانًا
11. بريد إلكتروني
14. حالة عدم وجود خطر أو تهديد
15. أداة يمكنها الاتصال بالإنترنت

أدلة إضافية

لمزيد من المعلومات، يُرجى الاطلاع على سلسلة *الأمن السيبراني الشخصي* الخاصة بنا:
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 جميع الأدلة الثلاثة على موقع **cyber.gov.au**

ملحوظات

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

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

ACSC Australian Cyber Security Centre

Australian Government
Australian Signals Directorate