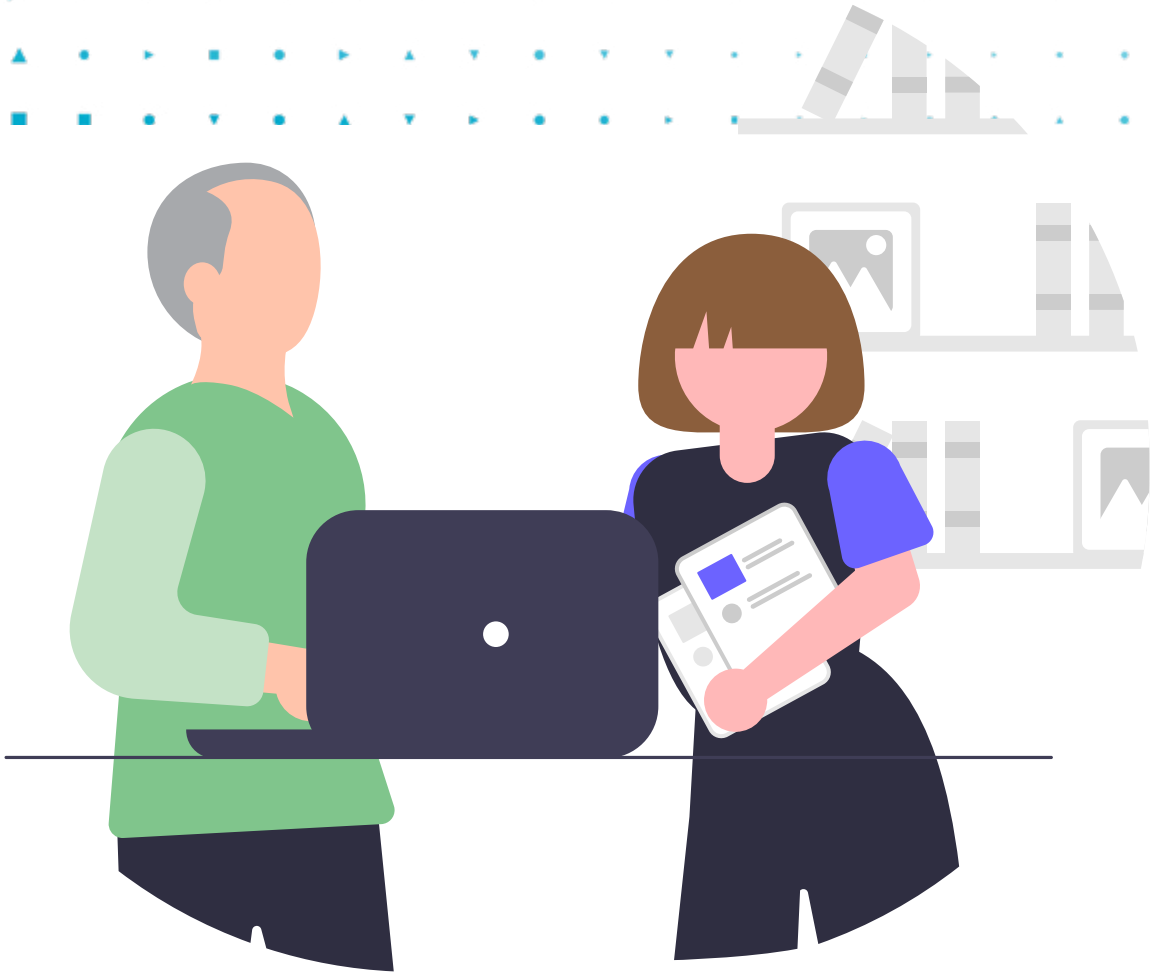
ASD AUSTRALIAN SIGNALS DIRECTORATE

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

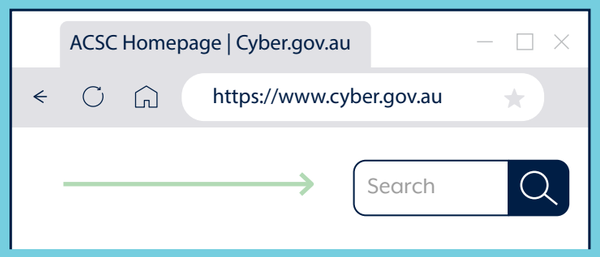
الأمن السيبراني لكبار السن

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 مزيد من المعلومات، ابحث عن'Updates' على cyber.gov.au



هل كنت تعلم أن:

قد تضيف التحديثات أيضًا مميّزات جديدة إلى جهازك وتجعله يعمل بشكل أسرع.

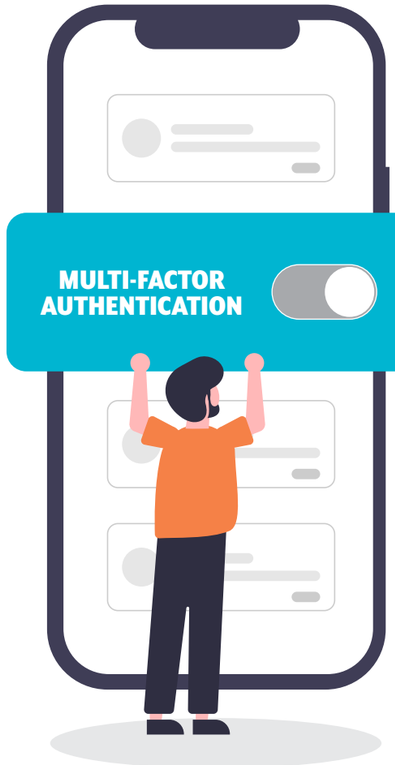
النصيحة 2: قم بتشغيل المصادقة متعددة العوامل

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 مزيد من المعلومات، ابحث عن 'Multi-factor authentication' أو 'MFA' على cyber.gov.au



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 مزيد من المعلومات، ابحث عن 'Backups' على cyber.gov.au

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 تُعِد استخدام عبارات السرّ الخاصة بك. استخدم عبارات سرّ مختلفة لحسابات مختلفة. إذا كنت تعاني من تذكّر جميع عبارات السرّ الخاصة بك، فكّر في استخدام مدير كلمة السرّ. مع مدير كلمة السّر، ما عليك سوى تذكّر كلمة سرّ واحدة، ويهتمّ مدير كلمة السرّ بالباقي. ابحث عن 'password manager' على cyber.gov.au للمزيد من النصائح.

اعرف المزيد حول إنشاء عبارات سرّ آمنة عن طريق البحث في 'Passphrases' على cyber.gov.au

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.

تذكر أن المحتالين غالبًا ما يتظاهرون بأنهم شخص أو منظمة تثق بها. كن مرتاباً إذا تلقيت رسالة تبدو وكأنها من شخص تثق به، ولكنه يستخدم رقم هاتف أو عنوان بريد إلكترونياً أو ملف تعريف على وسائل التواصل الاجتماعي جديداً. قبل الردّ، تحقّق من صحة هوية الشخص أو المنظمة التي تراسلك من خلال الاتصال بهم عبر قناة يمكنك الاعتماد عليها. على سبيل المثال، إذا تلقيت رسالة نصية تبدو وكأنها من أحد أولادك، ولكنها تأتي من رقم جديد، فلا تردّ. أرسل له رسالة على وسائل التواصل الاجتماعي للتحقّق من أنه قام بالفعل بتغيير رقم هاتفه أولاً.

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 السيبراني 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 في ما 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!

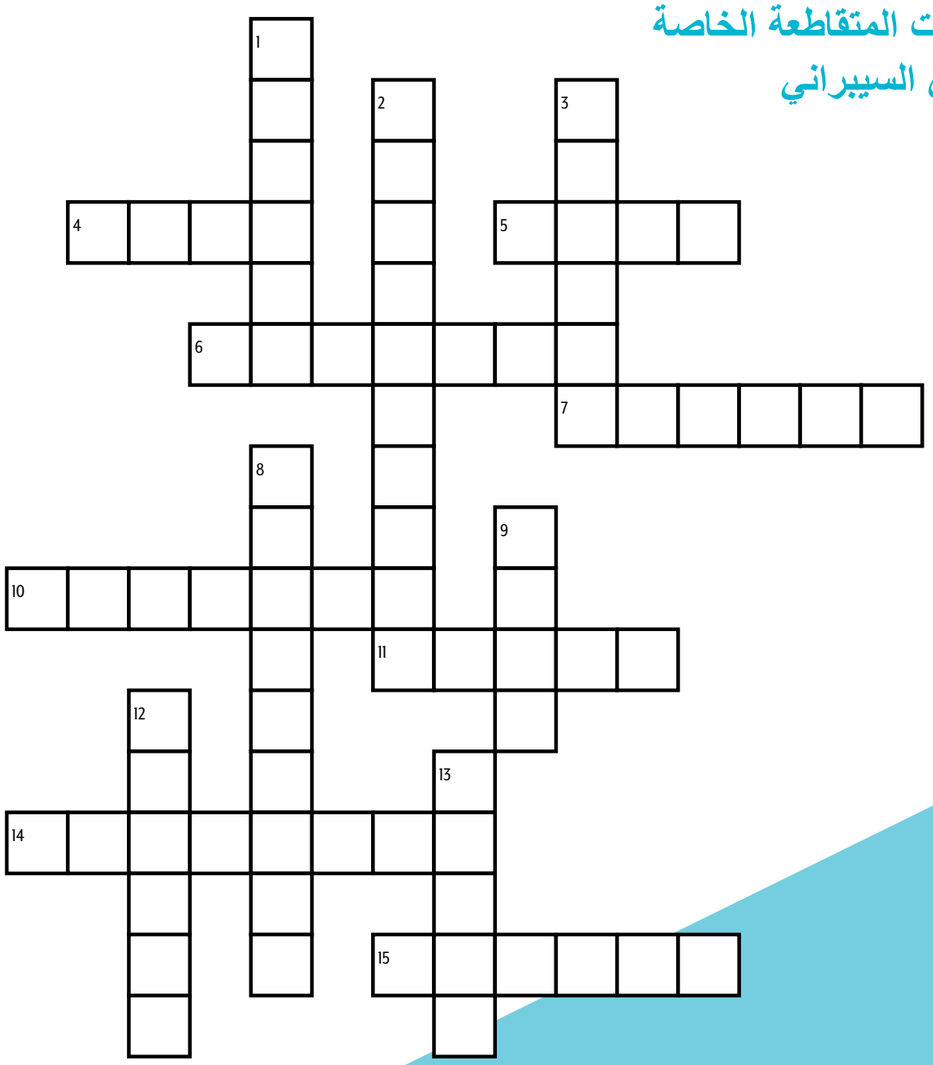
تجنب شبكات Wi-Fi العامة عند إجراء المعاملات المصرفية أو التسوق عبر الإنترنت.

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. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

أفقي

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

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**

إجابات الكلمات المتقاطعة

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

ملحوظات

إخلاء المسؤولية

المادة الواردة في هذا الدليل هي ذات طابع عام ولا ينبغي اعتبارها مشورة قانونية أو الاعتماد عليها للمساعدة في أي ظرف معين 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 إلكتروني، 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