ACSC Australian Cyber Security Centre

Australian Government
Australian Signals Directorate

CYBER SECURITY

كتيّب الأمن السيبراني

[دليل الأطفال لاستخدام الإنترنت بأمان!]

cyber.gov.au

المقدمة

صور القطط الهزلية، مقاطع الفيديو للأخطاء، برامج فلترة الوجه - الإنترنت رائع! لسوء الحظ، ليس كل مستخدمي الإنترنت رائعين.

حيث يتصل البعض بالإنترنت فقط للتسبب في المتاعب والسرقة من الآخرين.

يُطلق على هؤلاء مجرمي الإنترنت وهم السبب في أننا يجب أن نتوخى الحذر عندما نستخدم الإنترنت. وحتى نساعدك، أنشأنا هذا الكتيّب. إنه مليء بالنصائح المفيدة التي يمكنك استخدامها لرفع مستوى الأمان الإلكتروني لديك والبقاء آمنًا على الإنترنت!

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

الشخصيات

تعرف على اللاعبين المعنيين عندما يتعلق الأمر بالأمن السيبراني.

البطل

رائع ومدهش ومبهج ومضحك. بطل الأمن السيبراني هو الشخص الذي يقرأ هذا الآن. أنت!

باستخدام هذا الكتيّب، لديك القدرة على التغلب على أي تهديد إلكتروني يواجهك. ولست وحدك، فهناك العديد من المجموعات في أستراليا التي تعمل لحمايتك على الإنترنت.

مركز الأمن السيبراني الأسترالي.

أي نحن! يقدم مركز الأمن السيبراني الأسترالي المشورة والمعلومات حول كيفية حمايتك أنت وعائلتك عند الاتصال بالإنترنت.

نحن نراقب التهديدات السيبرانية على مدار الساعة طوال أيام الأسبوع.

مراقبة الاحتيال

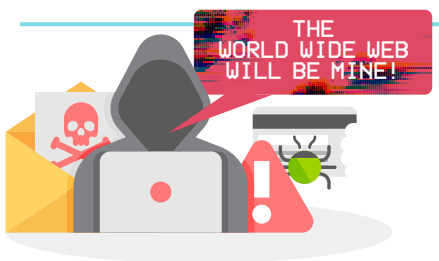
يبين فريق مراقبة الاحتيال للناس كيفية التعرف على عمليات الاحتيال وتجنبها والإبلاغ عنها.

عمليات الاحتيال عبارة عن خطط غير شريفة أو غير قانونية يستخدمها مجرمو الإنترنت لمهاجمة الضحايا غير المتشككين.

مفوض السلامة الإلكترونية

"السلامة الإلكترونية" هي الجهة المنظمة للأمن السيبراني في أستراليا. يمكن تقديم الشكاوى إلى "السلامة الإلكترونية" من أجل إزالة المحتوى الضار.

تقوم "السلامة الإلكترونية" أيضًا بالأبحاث وتقديم المشورة القائمة على الأدلة والموارد والبرامج لتحسين مهارات الأمان عبر الإنترنت.



مجرمو الإنترنت.

مجرمون. محتالون. مخادعون. هؤلاء المجرمون عديمو النفع يستخدمون الإنترنت لتنفيذ جرائمهم.

لا يوجد شيء يحبونه أكثر من إصابة أجهزة الآخرين ونشر الملفات غير القانونية وسرقة الأموال!

كيفية التغلب على التهديدات الإلكترونية.

الخطوة الأولى: قم بتحديث جهازك

التحديثات تمنح جهازك قوة أمنية!

تعمل التحديثات على اكتشاف العيوب في البرامج التي يستخدمها مجرمون الإنترنت لاختراق جهازك وإصلاحها. كما أنها تضيف ميزات جديدة إلى أجهزتك ويمكن أن تجعلها تعمل بشكل أسرع.

قم بزيارة cyber.gov.au لمعرفة كيفية تثبيت التحديثات.

نصيحة: انتبه!
يمكن للبرامج والتطبيقات غير المحدثة أن تجعل جهازك معيبًا ومعرضًا للهجمات السيبرانية

الخطوة الثانية: قم بتشغيل المصادقة متعددة العوامل

تضع المصادقة متعددة العوامل درعًا إضافيًا حول حسابك.

مع تشغيل المصادقة متعددة العوامل، ستحتاج إلى تقديم أنواع متعددة من المعلومات للوصول إلى حسابك. على سبيل المثال، قد تحتاج إلى رمز يتم إرساله برسالة نصية وكلمة المرور لتسجيل الدخول. هذا يعني أنه حتى لو قام أحد مجرمي الإنترنت بتخمين أو سرقة جزء من بيانات تسجيل الدخول الخاصة بك، فستظل محميًا بواسطة درعك الإضافي!

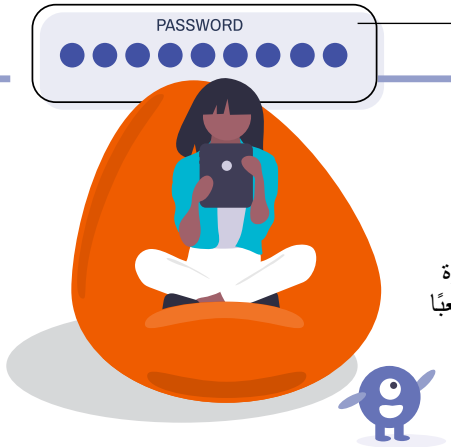
قم بزيارة cyber.gov.au لمعرفة كيفية تشغيل المصادقة متعددة العوامل.

الخطوة الثالثة: قم بإجراء نسخ احتياطي لجهازك.

إجراء نسخ احتياطي لجهازك يشبه حفظ تقدمك في لعبة ما.

وهذا يقوم بعمل نسخة من ملفاتك المهمة في تلك اللحظة في الوقت المناسب ويضعها في مكان آمن. وجود نسخ احتياطية يعني أنه يمكنك استعادة ملفاتك إذا حدث خطأ ما في جهازك.

قم بزيارة cyber.gov.au لمعرفة كيفية إجراء نسخ احتياطي لأجهزتك.



الخطوة الرابعة: استخدم عبارة مرور

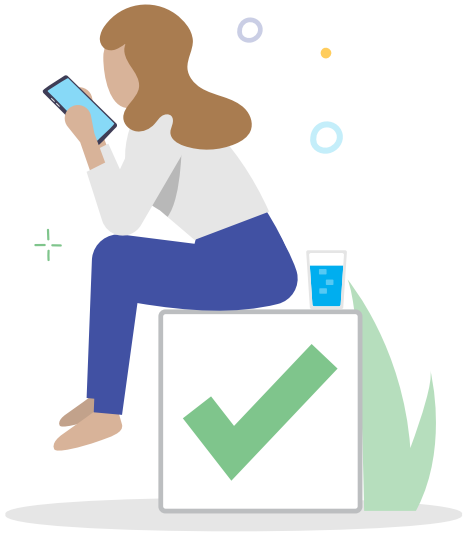
عبارة المرور مثل كلمة المرور ولكن على *مستوى احترافي!*

عندما لا يمكنك تشغيل المصادقة متعددة العوامل، استخدم عبارة مرور. تستخدم عبارة الدخول أربع كلمات عشوائية أو أكثر ككلمة السر الخاصة بك. هذا يجعل تخمينها صعبًا على مجرمي الإنترنت ولكن يسهل عليك تذكرها.

على سبيل المثال، "سماء قارب بطة أرجوانية".

قم بزيارة cyber.gov.au لمعرفة كيفية إنشاء عبارة مرور قوية.

نصيحة: استخدام كلمات كبيرة في عبارة مرورك سيجعلها أكثر صعوبة!



تعرف على الحيل وأبلغ عنها

التغلب على مجرمي الإنترنت يتطلب عملًا جماعيًا.

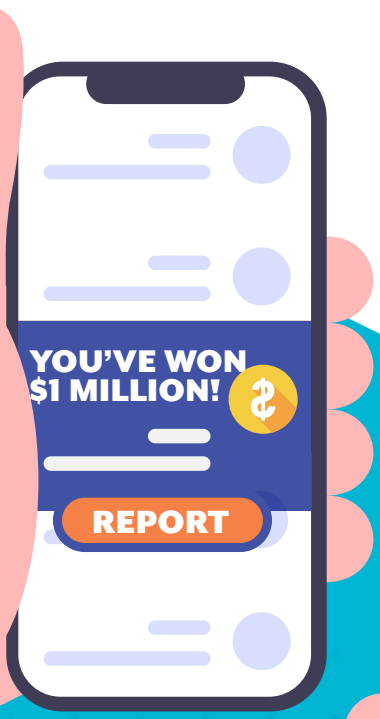
إذا تلقيت رسالة بريد إلكتروني أو رسالة مريبة، فأبلغها إلى مراقبة الاحتيال على الفور.

إذا بدا الأمر جيدًا لدرجة يصعب تصديقها، فمن المرجح أن يكون كذلك.

يتسم مجرمو الإنترنت بالمكر وقد يستخدمون اسمًا وعنوان بريد إلكتروني تعرفهما، ولكن اتبع حدسك. كلما أسرعت في الإبلاغ عن عملية الاحتيال، كان بإمكاننا التصرف بشكل أسرع.

قم بزيارة موقع Scamwatch.gov.au وموقع cyber.gov.au إن كنت تريد الإبلاغ عن شيء مريب.

نصيحة: لا تقم أبدًا بفتح روابط أو ملفات من شخص لا تعرفه.



بعد أن أصبحت الآن ملمًا بمهارات الأمن السيبراني، فأنت على استعداد لتسجيل الدخول مرة أخرى والاستمتاع بالإنترنت بأمان.

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

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

البحث عن الكلمات.

لنر إذا كان يمكنك العثور على جميع كلمات الأمن السيبراني!

T C W V T D T M M J R F R E D
W F Y H A H B U O J X C B N H
C S P A S S P H R A S E P U X
Z C R C B A C K U P S K F W Z
Y A Z K L W G S E C U R I T Y
K M D E V I C E D E F J V X W
Z J X R Q V H L W P K V P V D
V V S W R E P O R T M E S B O
X S I A C S C W O X O M S C C
F G W F Y U H E L M B A A H S
O N L I N E F B Z T A I F N U
M A V V U O I S E E Y L E Q C
W I F I M A L I Q C Y B E R L
E W E M I M E T E G R R T G P
W H D Z G H S E I H S L L C S

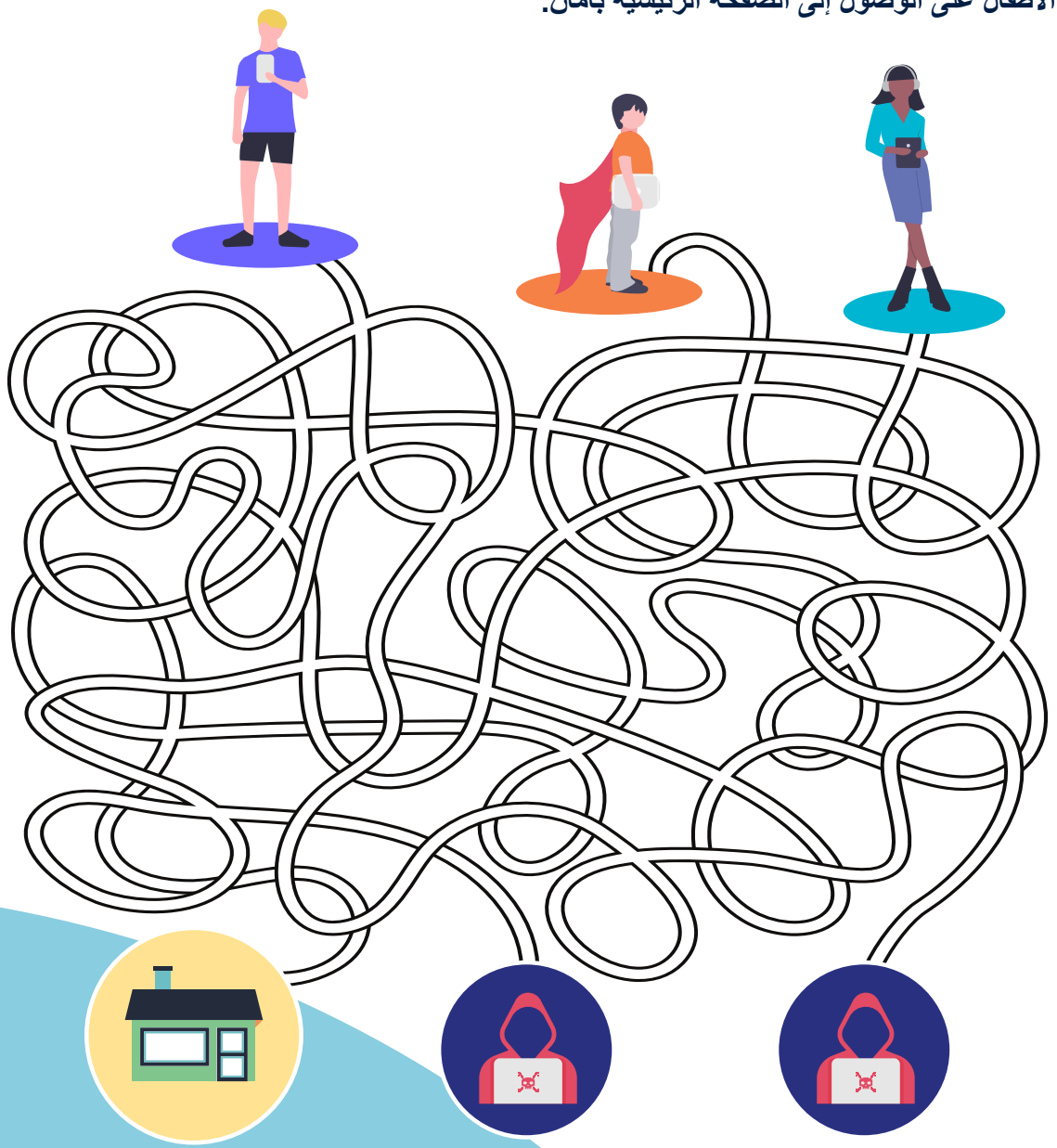
مركز الأمن السيبراني
الأسترالي
النسخ الاحتياطية
سيبراني
جهاز
بريد إلكتروني

ملفات
مخترق
إلكتروني
عبارة مرور
إبلاغ

احتيال
أمن
موقع إلكتروني
WIFI

المتاهة السيبرانية

ساعد الأطفال على الوصول إلى الصفحة الرئيسية بأمان.



BONUS TIPS

هل عرفت ما يلزم لتكون خبيرًا في الأمن السيبراني؟

1. **فكر** فيما تنشره على الإنترنت.
2. **ابق** على اطلاع بالمستجدات مع التنبيهات من مركز الأمن السيبراني الأسترالي.
3. **تحدث** عن الأمن السيبراني مع عائلتك وأصدقائك.
4. **تجنب** شبكات Wi-Fi العامة عند التسوق عبر الإنترنت.

تصفح بأمان!

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**

لمزيد من المعلومات أو للإبلاغ عن حادث أمن إلكتروني، اتصل بنا:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre