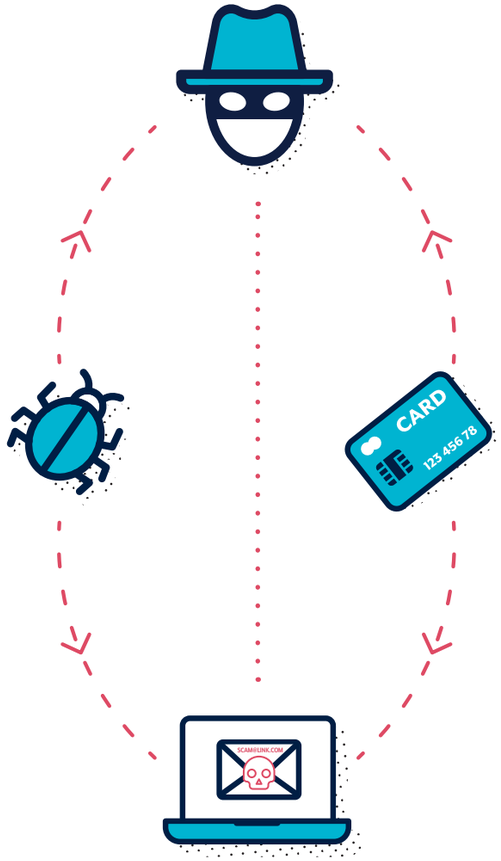
خطوات سهلة

لتأمين أجهزتك وحساباتك

قلل من مخاطر استهدافك
من قبل مجرمي الإنترنت باتباع هذه الخطوات

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre



لمزيد من المعلومات حول اكتشاف الرسائل المحتالة، راجع منشور الكشف عن الرسائل المهندسة اجتماعيًا التابع لمركز أمن الإنترنت الأسترالي (ACSC)، وابق على اطلاع من خلال الاشتراك في خدمة التنبيهات الخاصة بمركز ACSC على الموقع **cyber.gov.au**

5. احترس من عمليات الاحتيال

يستخدم المجرمون على الإنترنت البريد الإلكتروني والرسائل القصيرة والمكالمات الهاتفية ووسائل التواصل الاجتماعي لخداعك كي تفتح مُرفقًا أو تزور موقعًا على الإنترنت أو تكشف عن تفاصيل تسجيل الدخول إلى حسابك أو عن معلومات حساسة أو تحول أموالًا أو بطاقات الهدايا. صُممت هذه الرسائل لتبدو وكأنها مرسلة من أفراد أو مؤسسات تعتقد أنك تعرفها، أو تعتقد أنها محل ثقة.

لاكتشاف الرسائل المحتالة، توقف وفكر:

- **سلطة:** هل الرسالة تدعي أنها من مسؤول؟
- **الاستعجال:** هل أخبرتَ بأن لديك وقتًا محدودًا للرد؟
- **العواطف:** هل تجعلك الرسالة تشعر بالذعر أو الخوف أو التفاؤل أو الفضول؟
- **ندرة:** هل الرسالة تقدم شيئًا ما غير متوفر؟
- **الأحداث الجارية:** هل هذه الرسالة متعلقة بالأخبار الحالية أو الأحداث الكبرى أو أوقات محددة خلال العام (مثل فترة الإقرارات الضريبية)؟

للتحقق من شرعية الرسالة:

- راجع أمرًا يمكنك الوثوق به. اطلع على الموقع الرسمي أو قم بتسجيل الدخول إلى حسابك أو اتصل برقم هاتفهم المعلن. لا تستخدم الروابط أو تفاصيل الاتصال في الرسالة المرسلة إليك أو المعطاة عبر الهاتف.
- تحقق لمعرفة إن كان المصدر الرسمي قد أخبرك بالأمور التي لن يطلبها منك مطلقًا.
فعلى سبيل المثال، ربما أخبرك مصرفك الذي تتعامل معه أنه لن يطلب منك أبدًا الإفصاح عن كلمة المرور الخاصة بك.

قم بالإبلاغ عن الهجمات والحوادث عبر الإنترنت للحفاظ على أمن أستراليا.

اشترك
في خدمة التنبيهات المجانية لدينا
cyber.gov.au

بلّغ عن
جرائم الإنترنت إلى REPORTCYBER:
cyber.gov.au/report

للاتصال:
اتصل على الرقم 1300CYBER1 أو
اطلع على الموقع **cyber.gov.au**
هذا الرقم متاح للاستخدام داخل أستراليا فقط.

تابعنا

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1.قم بتحديث أجهزتك

يقوم مجرمو الإنترنت باختراق الأجهزة باستخدام نقاط الضعف المعروفة في الأنظمة أو التطبيقات. تشتمل التحديثات على تعزيزات أمنية لإصلاح نقاط الضعف هذه. قم بتشغيل التحديث تلقائيا بحيث يتم ذلك بدون تصرف منك.

قم بتشغيل التحديث التلقائي على جميع أجهزتك:

- الهاتف الجوال
- الحاسوب المحمول
- الحاسوب

تحقق بانتظام من وجود تحديثات لكل من:

- التطبيقات
- البرامج
- الأجهزة الذكية

2. شغّل المصادقة المتعددة العوامل (MFA)

تعمل MFA على تحسين أمنك من خلال تصعيب وصول مجرمي الإنترنت إلى ملفاتك أو حسابك.

قم بإعداد MFA بدءًا من حساباتك الأكثر أهمية:

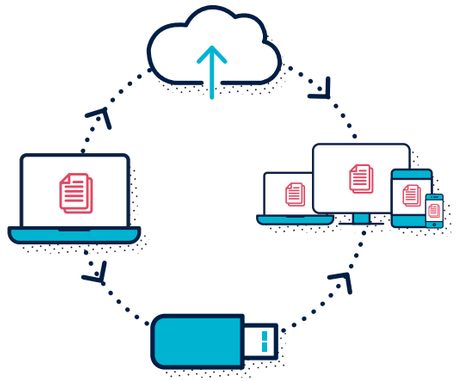
- حسابات البريد الالكتروني
- حسابات المعاملات المصرفية على الإنترنت والحسابات التي تختزن تفاصيل الدفع
- وسائط التواصل الاجتماعي

3.قم بعمل نسخة احتياطية من محتويات أجهزتك

النسخة الاحتياطية هي نسخة رقمية من المعلومات المخزنة على جهازك، مثل الصور والمستندات ومقاطع الفيديو والبيانات الخاصة بالتطبيقات. يمكنك حفظها على جهاز تخزين خارجي أو على السحابة. يسمح إعداد النسخ الاحتياطية باستعادتك لملفاتك في حالة فقدت جهازك أو سرق منك أو أتلف.

قم بعمل النسخة الاحتياطية من محتويات أجهزتك بانتظام:

- الهاتف الجوال
- الحاسوب المحمول
- الحاسوب
- الحاسوب اللوحي



4.قم بتعيين عبارات دخول آمنة

في الحالات التي لا تتوفر فيها MFA، غالبًا ما تكون عبارات الدخول الآمنة هي الأمر الوحيد الذي يحمي معلوماتك وحساباتك من المجرمين.

تستخدم عبارة الدخول أربع كلمات عشوائية أو أكثر ككلمة السر الخاصة بك. قم بتغيير كلمات السر الخاصة بك إلى عبارات الدخول وتأكد من كونها:

- طويلة: فكلما كانت عبارة الدخول أطول كلما كان ذلك أفضل. اجعل طولها 14 حرفًا على الأقل
- لا يمكن التكهن بها: استخدم مزيجًا عشوائيًا من كلمات لا صلة لها ببعضها البعض
- فريدة: لا تعيد استخدام عبارات الدخول على حسابات متعددة