



حماية معلوماتك الشخصية عبر الإنترنت

يطلب منك كل تطبيق أو منصة وسائط اجتماعية أو موقع إلكتروني تقريبًا بعض المعلومات الشخصية على الأقل. تتضمن معلوماتك الشخصية أي تفاصيل أو بيانات يمكن استخدامها لتحديد هويتك، مثل التفاصيل التي تحدد مكان وجودك أو مكان إقامتك، وغيرها من التفاصيل المحددة الفريدة. من المهم دائمًا التفكير مرتين في مشاركة المعلومات الشخصية.

حماية معلوماتك الشخصية مهمة

تُعد حماية معلوماتك الشخصية أمرًا مهمًا للغاية حيث يمكن للمحتالين ولصوص الهوية استخدامها لانتحال شخصيتك. يمكنهم إنشاء حسابات مزيفة باسمك والتصرف بطرق يمكن أن تؤثر عليك الآن أو في المستقبل. قد يشمل ذلك الاحتيال، مثل سرقة الأموال من حسابك المصرفي أو الحصول على قرض باسمك.

قد يستخدم المحتالون معلوماتك من تلقاء أنفسهم أو في سياق مع معلومات أخرى. يمكن أن يشمل ذلك الأشياء اليومية الخاصة بك، مثل:

وثائق الهوية

- رخصة القيادة
- جواز السفر
- شهادة الميلاد
- بطاقة مديكير
- التأشيرة الأسترالية أو
- شهادة الجنسية
- بطاقة الهجرة ImmiCard

المعلومات الشخصية

- الاسم الكامل
- عنوان المنزل
- رقم الهاتف
- تاريخ الميلاد
- رقم رخصة القيادة
- تفاصيل الحساب المصرفي
- عنوان البريد الإلكتروني
- أسماء المستخدم وكلمات المرور



كن على دراية بما تشاركه

وسائل التواصل الاجتماعي

من الجيد تجنب مشاركة المعلومات الشخصية على حسابات وسائل التواصل الاجتماعي الخاصة بك. يمكن للمحتالين معرفة الكثير عنك من خلال التفاصيل التي تشاركها عبر الإنترنت. في بعض الأحيان يقومون بإنشاء منشورات تضم اختبارات أو أسئلة مصممة لخداعك لمشاركة معلوماتك الشخصية. وهم يستخدمون هذه المعلومات لتخمين كلمات مرور حسابك أو استهدافك بعمليات احتيال أخرى.

استخدام التطبيقات

قم بتنزيل التطبيقات فقط من متاجر التطبيقات الرسمية، واقرأ سياسات الخصوصية والمراجعات قبل تنزيل أي شيء. يمكنك أيضًا تقييد المعلومات التي يمكن للتطبيقات الوصول إليها. تطلب بعض التطبيقات الوصول بلا ضرورة إلى قوائم جهات الاتصال والكاميرا والتخزين والموقع والميكروفون. راجع أذونات التطبيق واضبطها في قائمة الإعدادات على جهازك الذكي.

تذكر: اقبل طلبات الصداقة فقط من الأشخاص الذين تعرفهم في الحياة الواقعية، واجعل حساباتك على وسائل التواصل الاجتماعي خاصة، وراجع من يمكنه رؤية ما تشاركه.

حافظ على أمان معلوماتك

استخدم أمان الجهاز

يعد استخدام برامج الأمان على جهاز الكمبيوتر الخاص بك أحد أبسط الطرق لحماية نفسك وخصوصيتك. يتضمن الأمان الجيد للكمبيوتر تثبيت برامج مكافحة التجسس وبرامج مكافحة الفيروسات وبرامج جدار الحماية ذات السمعة الطيبة. يجب عليك أيضًا تحديث أدوات وتطبيقات الأمان عبر الإنترنت من خلال تمكين التحديثات التلقائية. استخدم أقفال الشاشة التلقائية والموقوتة أو شاشات التوقف المحمية بكلمة مرور، واحصل على قفل تلقائي بعد فشل محاولات تسجيل الدخول المتعددة.

عبارات المرور

حافظ على أمان حساباتك باستخدام عبارات مرور قوية. عبارات المرور هي الإصدار الأكثر أمانًا من كلمات المرور وتتكون من أربع كلمات عشوائية أو أكثر.

حاول التفكير في عبارة مرور مختلفة لكل حساب من حساباتك ولا تعيد تدوير أجزاء من أي عبارات مرور قديمة.

عند اختيار عبارة المرور الخاصة بك، اجعلها:

- **طويلة** - 14 حرفًا على الأقل
- **لا يمكن التنبؤ بها** - استخدم أربع كلمات عشوائية أو أكثر بأرقام ورموز وأحرف كبيرة وصغيرة
- **فريدة** - لا تعيد استخدام عبارات المرور الخاصة بك

على سبيل المثال، أصفر لذا مرحبًا نبات < Yell*w-SOheyPl@nt!

نصيحة: يمكن أن يساعدك تطبيق إدارة كلمات المرور أيضًا في إنشاء وتخزين عبارات مرور معقدة يصعب على الآخرين تخمينها أو اختراقها. يمكنك العثور على معلومات حول **تطبيقات إدارة كلمات المرور** وكيفية إعدادها على موقع Be Connected الإلكتروني.

نصيحة: تحقق من قوة كلمة المرور باستخدام اختبار قوة كلمة المرور لحكومة نيو ساوث ويلز على الموقع nsw.gov.au/id-support-nsw/be-prepared/passwords

المصادقة متعددة العوامل

من الجيد دائماً تشغيل المصادقة متعددة العوامل لحساباتك. تضيف المصادقة متعددة العوامل (المعروفة أيضاً باسم المصادقة ذات الخطوتين) طبقة إضافية من الأمان. هذا يعني أنه عند تسجيل الدخول إلى حساب باستخدام كلمة المرور الخاصة بك، قد يُطلب منك القيام بخطوة إضافية لتأكيد هويتك - مثل إدخال رمز من رسالة نصية أو استخدام تعريف التعرف على الوجه.

تسوق بأمان عبر الإنترنت

عند التسوق عبر الإنترنت، تأكد من استخدام البائعين الموثوق بهم وابحث عن تقييمات العملاء. قبل إدخال معلوماتك الشخصية، تحقق من أن الموقع الإلكتروني يستخدم "https" في بداية اسم العنوان الخاص به أو يحتوي على رمز أمان، عادةً ما يكون قفلاً صغيراً مقفلاً، على متصفحه للإشارة إلى أنه موقع إلكتروني أكثر أماناً. عند إجراء عملية شراء، استخدم طريقة دفع آمنة مثل PayPal أو BPAY أو بطاقتك الائتمانية.

استخدم اتصال آمن

عندما تحتاج إلى الوصول إلى حسابات مهمة أو إرسال معلومات حساسة أو إدخال كلمات مرور، اتصل بشبكة إنترنت موثوق بها، مثل المنزل أو العمل، أو باستخدام بيانات المحمول الخاصة بك إذا كانت متوفرة. شبكة الواي فاي العامة ليست آمنة مثل شبكة الواي فاي في المنزل أو العمل.

عمليات الاحتيال وخروقات البيانات

احم نفسك من عمليات الاحتيال

يعد الوعي بعمليات الاحتيال وكيفية عملها إحدى الخطوات المهمة لتجنبها. يتظاهر المحتالون بأنهم من مؤسسة أو شخص تعرفه لمحاولة خداعك لتسليم معلوماتك الشخصية. وتسمى عمليات الاحتيال هذه انتحال الهوية.

تذكر:

توقف - لا تعطي المال أو المعلومات الشخصية لأي شخص إذا لم تكن متأكدًا
غالبًا ما يطلب منك المحتالون التحقق من هويتك أو يطلبون منك إجراء دفع.

فكر - اسأل نفسك هل يمكن أن تكون الرسالة أو المكالمات مزيفة؟

احذر من المكالمات والرسائل ورسائل البريد الإلكتروني غير المتوقعة. إذا لم تكن متأكدًا من رسالة ما، فاتصل بالمؤسسة مباشرةً باستخدام رقم الهاتف الموجود على الموقع الإلكتروني الخاص بها.

الحماية - تصرف بسرعة إذا شعرت بخطأ ما

اتصل بالبنك الذي تتعامل معه إذا لاحظت نشاطًا غير عادي أو إذا حصل المحتال على أموالك أو معلوماتك.

نصيحة: تفضل بزيارة موقع Be Connected للحصول على **دليل عمليات الاحتيال** المجاني الخاص بانتحال الهوية الذي تم تطويره مع Scamwatch.

خروقات البيانات

يحدث خرق البيانات عندما يتم الوصول إلى المعلومات الشخصية التي تحتفظ بها المؤسسة أو الكشف عنها دون إذن، أو فقدانها. تتحمل العديد من المؤسسات والوكالات الحكومية مسؤولية قانونية لإخبارك إذا كانت معلوماتك الشخصية متورطة في خرق للبيانات من المحتمل أن يتسبب لك في ضرر جسيم.

إذا كانت معلوماتك متورطة في خرق للبيانات، فتأكد من التصرف بسرعة والحصول على المشورة المقدمة

من **مكتب مفوض المعلومات الأسترالي**

Office of the Australian Information

Commissioner. يعتمد الإجراء الذي تتخذه على

المعلومات المعنية. احتفظ بسجل لما تفعله. يمكنك

أيضًا الحصول على دعم ومشورة مجانية من **IDCARE**.

لمعرفة ما إذا كان موقع إلكتروني أو تطبيق تستخدمه قد

تعرض لخرق للبيانات، يمكنك التحقق من خدمات مثل

haveibeenpwned.com. إذا حدث ذلك، فقم بتغيير

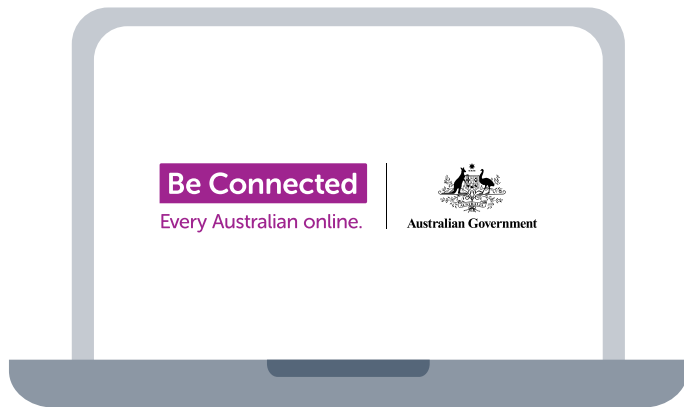
كلمات المرور الخاصة بك على الفور.

الاحتيال على الهوية

إذا كنت تعرف أو تشك في سرقة هويتك:

- قم بتقديم تقرير إلى مركز الأمن السيبراني الأسترالي Australian Cyber Security Centre التابع لمديرية الإشارات الأسترالية Australian Signals Directorate في **ReportCyber**.
- اتصل بالشرطة على الرقم 131 444. اطلب تقرير الشرطة أو الرقم المرجعي كدليل على أنك قدمت تقريرًا.
- إذا كنت تعرف أو تشك في نوع المعلومات الشخصية التي تمت سرقتها، فاتصل بالوكالة أو المنظمة ذات الصلة لإعلامها بذلك.
- أخبر مؤسستك المالية في أقرب وقت ممكن.
- قم بتقديم تقرير إلى المركز الوطني لمكافحة الاحتيال National Anti-Scam Centre في **Scamwatch** إذا كان جزءًا من عملية احتيال.

خذ الوقت الكافي لاكتشاف Be Connected



Be Connected هو موقع إلكتروني شامل يحتوي على موارد مجانية مصممة خصيصًا لدعم كبار السن الأستراليين للاتصال بأمان عبر الإنترنت والتنقل في العالم الرقمي بثقة. الموقع مفيد أيضًا للعائلات والمنظمات المجتمعية التي ترغب في مساعدة أفراد المجتمع الأكبر سنًا في الوصول إلى جميع مزايا الإنترنت.

تفضل بزيارة **beconnected.esafety.gov.au**

تم تطوير هذا البرنامج من قبل السلامة الإلكترونية eSafety كجزء من مبادرة Be Connected.

eSafety
Commissioner


Australian Government

beconnected.esafety.gov.au