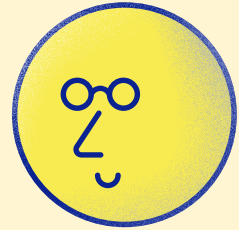


كيفية اكتشاف وتجنب عمليات الاحتيال

دليلك لحماية نفسك
من عمليات الاحتيال



ScamWatch

Stop. Better safe than scammed.



Australian Government



**National
Anti-Scam
Centre**

الاعتراف بالبلد

تعترف لجنة ACCC المفوضية الأسترالية للمنافسة وشؤون المستهلك بالمالكين والأوصياء التقليديين للأرض في جميع أنحاء أستراليا وتقرّ ارتباطهم المستمر بالأرض والبحر والمجتمع. نقدم احترامنا لهم ولثقافتهم؛ ولشيوخهم ماضياً وحاضراً ومستقبلاً.

Australian Competition and Consumer Commission

Ngunnawal

23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© كومونولث أستراليا 2023

يخضع هذا العمل لحقوق التأليف والنشر. بالإضافة إلى أي استخدام مسموح به بموجب قانون حقوق التأليف والنشر لعام 1968، تم توفير جميع المواد المتضمنة في هذا العمل بموجب ترخيص Creative Commons Attribution 4.0 Australia. باستثناء:

- درع الكومونولث
- شعارات ACCC و AER
- أي رسم توضيحي، أو رسم تخطيطي، أو صورة فوتوغرافية، أو رسم بياني لا تمتلك المفوضية الأسترالية للمنافسة وشؤون المستهلك حقوق الطبع والنشر له، ولكنها قد تكون جزءاً من هذا المنشور أو متضمنة فيه.

توفر تفاصيل شروط الترخيص ذات الصلة على موقع Creative Commons الإلكتروني، وكذلك المدونة القانونية الكاملة لترخيص CC BY 4.0 AU.

يجب توجيه الطلبات والاستفسارات المتعلقة بالنسخ والحقوق إلى Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ملاحظة مهمة

المعلومات الواردة في هذا المنشور هي للإرشاد العام فقط. ولا تشكل مشورة قانونية أو مشورة مهنية أخرى، ولا ينبغي الاعتماد عليها كبيان للقانون في أي ولاية قضائية. ولأن المقصود منه فقط أن يكون دليلاً عاماً، فقد يحتوي على تعميمات. يجب عليك الحصول على المشورة المهنية إذا كان لديك أي مخاوف محددة.

بذلت المفوضية الأسترالية للمنافسة وشؤون المستهلك (ACCC) كل جهد معقول لتوفير معلومات حديثة ودقيقة، ولكنها لا تقدم أي ضمانات فيما يتعلق بدقة تلك المعلومات أو حداتها أو اكتمالها.

يجب على الأطراف التي ترغب في إعادة نشر المعلومات الواردة في هذا المنشور أو استخدامها بطريقة أخرى، التحقق من هذه المعلومات للتأكد من صحتها ودقتها قبل النشر. ينبغي أن يتم ذلك قبل كل طبعة منشورة، حيث تغير إرشادات المفوضية الأسترالية للمنافسة وشؤون المستهلك والتشريعات الانتقالية ذات الصلة بشكل متكرر. يجب توجيه أي استفسارات من قبل الأطراف إلى Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

Canberra ACT 2601

ACCC 05/24_24-13

www.accc.gov.au

المحتويات

1	المساعدة متاحة
3	ما هي عملية الاحتيال
4	خطوات بسيطة لاكتشاف عمليات الاحتيال وتجنبها
7	الرسائل النصية أو الرسائل النصية القصيرة الاحتيالية
11	عمليات الاحتيال عبر البريد الإلكتروني
15	عمليات الاحتيال الهاتفية
19	عمليات الاحتيال على موقع الانترنت
23	عمليات الاحتيال على وسائل التواصل الاجتماعي والتطبيقات والرسائل عبر الانترنت
27	أهم عمليات الاحتيال التي يجب أن تعرفها
31	أين يمكن الإبلاغ عن عمليات الاحتيال
33	مزيد من المساعدة والدعم



تم كتابة هذا الدليل من قبل المركز الوطني لمكافحة الاحتيال وسيساعدك على التعرف على وحماية نفسك من الضرر الناجم عن عمليات الاحتيال.

عملية الاحتيال جريمة والأشخاص الذين يقومون بعمليات الاحتيال هم مجرمون. يتعرض العديد من الأشخاص في أستراليا للاحتيال ويخسرون أموالهم، وأحياناً حتى مدخراتهم. عمليات الاحتيال تؤذي حياة الناس.

أصبح اكتشاف عمليات الاحتيال أكثر صعوبة، لذا يتعين علينا العمل معاً لإيقافها.

يعمل المركز الوطني لمكافحة الاحتيال على حماية الأستراليين من عمليات الاحتيال.

نحن نعمل مع الحكومة والقطاع لإيجاد طرق جديدة لمنع المحتالين من سرقة الأموال والمعلومات الشخصية من الأستراليين. فيما يلي بعض الطرق التي نحقق بها ذلك.

نحن نساعد الأشخاص على اكتشاف عمليات الاحتيال وتجنبها

من خلال **Scamwatch** نشارك أحدث المعلومات حول عمليات الاحتيال والطرق التي يمكنك من خلالها حماية نفسك من عمليات الاحتيال.

نحن نقوم بتعطيل عمل المحتالين

من خلال جمع المعلومات الاستخبارية ومشاركتها عبر الحكومة والقطاع، فإننا نجعل من الصعب على المحتالين مواصلة جرائمهم ونسهل على الأشخاص الإبلاغ عن عمليات الاحتيال.



المساعدة متاحة

إذا كنت تقرأ هذا، فمن المحتمل أنك أنت أو شخص تعرفه قد تعرض للاحتيال. لسوء الحظ، أنت لست وحدك. أصبحت عمليات الاحتيال معقدة بشكل متزايد مما يعني أنه يمكن خداع أي شخص.

إذا تعرضت للاحتيال، فمن المهم أن تتصرف بسرعة.

إذا خسرت أموالاً بسبب محتال، فاتصل بالمصرف الذي تتعامل معه أو مزود البطاقة.

اتصل بـ www.idcare.org، 1800 595 160، IDCARE

تنجح عمليات الاحتيال لأنها تبدو وكأنها حقيقية. يعتمد المحتالون على عدم اكتشافك لعلامات التحذير لأنك في عجلة من أمرك، أو لأن الشيء يبدو وكأنه صفقة كبيرة لا تريد تفويتها، أو لأنه يبدو أنه من شخص تثق به.

احمِ نفسك من عمليات الاحتيال باتباع الخطوات الثلاث التالية:

توقف



لا تعط المال أو المعلومات الشخصية لأي شخص إذا لم تكن متأكداً.

سيعرض عليك المحتالون مساعدتك أو يطلبون منك التحقق من هويتك. سوف يتظاهرون بأنهم من مؤسسات تعرفها وتتق بها مثل مقدمي الخدمات أو الشرطة أو المصرف الذي تتعامل معه أو الخدمات الحكومية.

دقق



اسأل نفسك – هل يمكن أن تكون الرسالة أو المكالمة مزيفة؟

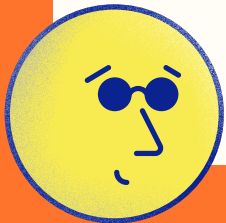
لا تنقر أبداً على رابط في رسالة. اتصل فقط بالشركات أو الحكومة باستخدام معلومات الاتصال التي تجدها بنفسك من موقعها الإلكتروني أو تطبيقها الرسمي. إذا لم تكن متأكداً، فقل "لا"، أو قمر بإنهاء المكالمة أو الحذف.

بلّغ



تصرف بسرعة إذا شعرت بخطب ما.

اتصل بالمصرف الذي تتعامل معه إذا لاحظت نشاطاً غير عادي أو إذا حصل أحد المحتالين على أموالك أو معلوماتك. اطلب المساعدة وبلّغ عن عملية الاحتيال إلى ReportCyber وScamwatch. عند الإبلاغ عن عمليات الاحتيال، فإنك تساعد جميع الأستراليين من خلال بناء دفاعنا ضد عمليات الاحتيال.



ما هي عملية الاحتيال

تحدث عملية الاحتيال عندما يخدعك شخص ما لسرقة أموالك أو معلوماتك الشخصية.

عمليات الاحتيال هي جرائم اقتصادية يديرها مجرمون غالبًا ما يكونون منظمين ومتطورين للغاية.

عمليات الاحتيال:

يديرها مجرمون ✓

تبدو حقيقية ✓

تأتي مع قصص قابلة للتصديق ✓

تضغط عليك لاتخاذ إجراء ✓

عملية الاحتيال ليست:

قرصنة لكمبيوتر ✗ شروط عقد غير عادلة ✗ أساليب التسويق المضايقة ✗

من المهم أن تتذكر أنه ليست كل التجارب السلبية عبارة عن عمليات احتيال. ربما تكون قد دفعت ثمن منتج لم تستلمه مطلقًا أو اشتريت شيئًا ما ووجدت أن الجودة كانت سيئة. في حين أن هذا أمر مخيب للآمال، إلا أن هذه ليست بالضرورة عمليات احتيال. يوفر قانون المستهلك الأسترالي الحماية للمستهلكين الأستراليين فيما يتعلق بهذا النوع من المشكلات.

لمزيد من المعلومات قم بزيارة www.accc.gov.au/consumers

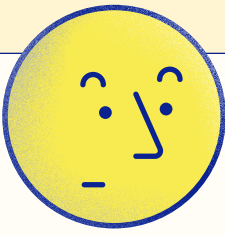
خطوات بسيطة لاكتشاف عمليات الاحتيال وتجنبها

يمكن أن تحدث عمليات الاحتيال لنا جميعًا. تتجس عمليات الاحتيال لأن المحتالين يقومون بإنشاء قصص قابلة للتصديق لسرقة أموالك والحصول على معلوماتك الشخصية.

أصبح المحتالون أكثر ذكاءً ويستفيدون من التكنولوجيا الحديثة والمنتجات والخدمات والأحداث الكبرى لإقناعك بأن عمليات الاحتيال التي يقومون بها حقيقية.

قد يكون من الصعب جدًا اكتشاف عملية احتيال. فيما يلي بعض المواقف التي يجب الانتباه إليها. يستخدم المحتالون أحيانًا مجموعة من هذه الأساليب.

- 1. فرص لكسب أو توفير المال:** سوف يخدعك المحتالون للاعتقاد بأنك تحصل على صفقة أو عرض رائع. سوف يضغطون عليك لتصرف بسرعة حتى لا تفوتك الفرصة. تذكر أن الصفقات التي تبدو جيدة جدًا لدرجة يصعب تصديقها، عادةً ما تكون كذلك.
- 2. قصص حزينة ومناشدات طلبا للمساعدة:** سيحاول المحتالون استخدام طبيعتك الطيبة ضدك. سوف يشاركونك قصص الحزن والمأساة معك ويشرحون سبب حاجتهم لمساعدتك ولمالك.
- 3. الروابط والمرفقات:** يستخدم المحتالون الروابط لإرسالك إلى مواقع الإنترنت الاحتيالية المصممة لسرقة معلوماتك وأموالك. قد يطلب منك المحتالون أيضًا فتح المرفقات. يمكن لهذه المرفقات تثبيت فيروسات تسرق معلوماتك.



4. **الضغط للتحرك بسرعة:** لا يريد المحتالون منك أن تأخذ وقتك وتفكر في الأمور. إنهم يريدون الضغط عليك للتصرف بسرعة. يمكن أن يشمل ذلك التهديد بحدوث شيء سيء إذا لم تتصرف بسرعة.

5. **طلبات الدفع بطرق غير عادية أو محددة:** غالبًا ما يطلب منك المحتالون الدفع باستخدام طرق غير شائعة مثل بطاقات الخصم المحملة مسبقًا أو بطاقات iTunes أو العملة الافتراضية مثل البتكوين / Bitcoin. وبمجرد إنفاق هذه الأموال، لا يمكنك استعادتها.

6. **طلب إنشاء حسابات جديدة أو PayID (معارف الدفع):** قد يطلب منك المحتالون إنشاء حساب مصرفي جديد أو PayID من أجل الدفع لهم (أو الدفع لك). قد يتظاهرون بأنهم المصرف الذي تتعامل معه ويطلبون منك تحويل أموالك إلى حسابات جديدة للحفاظ عليها آمنة.

إذا نجح المحتالون في أخذ أموالك، فسيحاولون الحصول على المزيد من المال منك. ولسوء الحظ، تم خداع واحد من كل ثلاثة ضحايا للاحتيال أكثر من مرة. إذا خسرت المال بسبب عملية احتيال، فكن حذرًا من المحتالين الذين يعرضون مساعدتك في استعادة أموالك. هذا نوع آخر من عمليات الاحتيال اللاحقة.



الرسائل النصية أو الرسائل النصية القصيرة الاحتيالية

يرسل المحتالون رسائل تبدو وكأنها من الحكومة أو وكالات إنفاذ القانون أو الشركات الموثوقة أو حتى من عائلتك أو أصدقائك.

ستبدو هذه الرسائل عاجلة وستحاول دفعك إلى التصرف بسرعة. غالبًا ما يكون لديهم رابط ينقلك إلى موقع إنترنت احتيالي. يمكن للمحتالين سرقة أي معلومات شخصية يتم إدخالها على مواقع الاحتيال هذه واستخدامها للاستيلاء على أموالك أو ارتكاب عمليات نصب باسمك.

لجعل هذه الرسائل تبدو حقيقية، يقوم المحتالون بنسخ أو إخفاء رقم هاتفهم خلف رقم الهاتف ومعرف المتصل الخاص بشركات مشروعة أو الأشخاص الذين تعرفهم.

يمكن أن تظهر الرسائل الاحتيالية في نفس سلسلة الرسائل مثل الرسائل الحقيقية من المؤسسة، مما يزيد من صعوبة اكتشافها.

علامات على أن الرسالة قد تكون عملية احتيال

الرسالة:

تطلب منك اتخاذ إجراء فوري، أو إجراء بالدفع، أو تحويل الأموال.



تطلب منك النقر على رابط أو الاتصال بالرقم الموجود في الرسالة.



يطلب منك تسجيل الدخول إلى حساب عبر الإنترنت باستخدام اسم المستخدم وكلمة المرور الخاصة بك أو تقديم معلومات شخصية أخرى.



رسالة من أحد أفراد العائلة أو الأصدقاء تفيد بأن تفاصيل الاتصال الخاصة بهم قد تغيرت.



تهدد بإيقاف الخدمة أو فرض رسوم عليك إذا لم تتصرف.



تشير إلى تعرضك أنت أو حساباتك للاختراق أو التورط في عملية نصب.



تشير إلى وجود مشكلة في الدفع أو تسليم طردك.



خطوات لحماية نفسك من الرسائل الاحتيالية

1. إذا أرسل شخص تعرفه رسالة ليخبرك أن لديه رقم هاتف جديد:



- a. حاول الاتصال بهم على رقمهم الموجود لديك، و
- b. قم بمراسلتهم على الرقم الجديد بسؤال هم فقط من يعرفون الإجابة عليه، للتأكد من هويتهم.

2. لا تنقر أبداً على الروابط الموجودة في الرسائل.



3. إذا كانت الرسالة مرتبطة بموقع انترنت، فلا تنقر فوق الرابط. بدلاً من ذلك، ابحث عن موقع الإنترنت بنفسك على الإنترنت، أو استخدم التطبيق الرسمي.



4. لا ترد على رسالة نصية باستخدام رقم الهاتف المزود.



5. اتصل مرة أخرى بالمنظمة أو الشخص على رقم الهاتف الذي وجدته بنفسك، مثلاً من موقع المنظمة على الانترنت.





عمليات الاحتيال عبر البريد الإلكتروني

يرسل المحتالون رسائل بريد إلكتروني تبدو وكأنها من الحكومة ووكالات إنفاذ القانون والشركات. يجعلون الأمر يبدو عاجلاً لجعلك تتصرف بسرعة.

يستخدم المحتالون نفس الشعار وعنوان بريد إلكتروني مشابهًا للمنظمة الحقيقية. يمكن للمحتالين أيضًا نسخ أو إخفاء عنوان بريدهم الإلكتروني خلف عنوان البريد الإلكتروني لمؤسسة أو شركة لجعل البريد الإلكتروني الاحتيالي يبدو أكثر واقعية.

علامات بأن البريد الإلكتروني قد يكون عملية احتيال

البريد الإلكتروني:

يطلب الدفع، ولكن تفاصيل الحساب جديدة أو تغيرت منذ آخر دفعة قمت بها.



يطلب منك تسجيل الدخول إلى حساب عبر الإنترنت باستخدام اسم المستخدم وكلمة المرور الخاصة بك أو تقديم معلومات شخصية أخرى.



كان غير متوقع ويتضمن مرفقًا مع دعوة لفتحه.



يطلب منك تأكيد بياناتك المصرفية لاسترداد أموالك أو أموال لا تتوقعها.



يدعي أن لديه معلومات عنك أو صور لك ويهدد بنشرها.



عروض لمساعدتك في استرداد الأموال أو الحصول على تعويض عن اختراق البيانات أو سرقة الهوية.



الخطوات التي يمكنك اتخاذها لحماية نفسك من عمليات الاحتيال عبر البريد الإلكتروني

1. تأكد من أن البريد الإلكتروني حقيقي عن طريق إما:

- a. الاتصال بالشخص أو المؤسسة مباشرةً باستخدام تفاصيل الاتصال التي وجدتها بنفسك، مثل موقع الانترنت الخاص بالمنظمة أو،
- b. التواصل مع مؤسسة عبر تطبيقها الرسمي (وليس عبر رابط أبدأ).



2. توقف فورًا عن التواصل مع أي شخص يحاول تهديدك أو تخويفك.



3. لا تقدم أبدًا تفاصيل شخصية أو تدفع لأي شخص يعرض عليك:

- a. التعويض أو المساعدة في التعافي من عملية احتيال سابقة أو خرق للبيانات، أو
- b. المكاسب أو الجوائز أو الميراث.



4. استخدم المصادقة متعددة العوامل عندما تستطيع ذلك. يوفر هذا طبقة

إضافية من الحماية ويعني أن المحتال يجب أن يعرف كلمة مرور بريدك الإلكتروني ورقم التعريف الشخصي الذي تم إرساله إلى هاتفك للوصول إلى حساب بريدك الإلكتروني.





عمليات الاحتيال الهاتفية

يتصل المحتالون مدعين أنهم من منظمات معروفة. ويشمل ذلك المنظمات الحكومية ووكالات إنفاذ القانون وشركات الاستثمار والمحاماة والبنوك ومقدمي خدمات الاتصالات.

يجعلون الأمر يبدو عاجلاً لجعلك تتصرف بسرعة. وقد يحاولون إقناعك بتزويدهم بتفاصيل حسابك الشخصي أو المصرفي، أو الوصول إلى جهاز الكمبيوتر الخاص بك. قد يكون لدى المتصل بالفعل بعض التفاصيل عنك، مثل اسمك أو عنوانك، مما يجعل المكالمة تبدو حقيقية.

علامات على أن المكالمة الهاتفية قد تكون عملية احتيال

المتصل:

يطلب منك الدفع أو يطلب منك تحويل الأموال إلى حساب جديد.



يطلب منك كلمة المرور أو الرقم السري أو الرمز المستخدم لمرة واحدة أو بعض المعلومات الأمنية الأخرى.



يطلب منك تفاصيلك المالية، مثل بطاقة الائتمان أو التفاصيل المصرفية.



يطلب منك إكمال إجراء على هاتفك المحمول أو جهاز الكمبيوتر الخاص بك مثل تثبيت البرامج أو الوصول إلى حساب آمن.



يدعي أنه من وكالات إنفاذ القانون ويهددك بالاعتقال الفوري أو الترحيل.



يشير إلى أن المصرف الذي تتعامل معه أو حساباتك الأخرى على الإنترنت قد تم اختراقها أو تورطها في عمليات نصب.



الخطوات التي يمكنك اتخاذها لحماية نفسك من عمليات الاحتيال عبر الهاتف

1. تأكد من أن المكالمة حقيقية عن طريق:

- a. الاتصال بالشخص أو المؤسسة مباشرةً باستخدام تفاصيل الاتصال التي وجدتها بنفسك، مثل موقع الانترنت الخاص بالمنظمة أو،
- b. التواصل مع مؤسسة عبر تطبيقها الرسمي (وليس عبر رابط أبدأ).



2. إذا لم تكن متأكدًا من هوية المتصل أو إذا كان يهددك أو يخيفك، قم بإغلاق الخط على الفور.



3. لا تقم مطلقًا بتثبيت برنامج يسمح لأي شخص بالوصول إلى جهاز الكمبيوتر أو الجهاز الخاص بك.



4. يمكنك تجاهل المكالمات الواردة من أرقام لا تعرفها أو السماح للمكالمات بالانتقال إلى البريد الصوتي.



من الجيد ان تعلم!

لا يزال بإمكانك تلقي مكالمات احتيالية حتى إذا كان لديك رقم مخفي أو كنت مسجلًا في سجل عدم الاتصال.





عمليات الاحتيال على موقع الانترنت

يمكن للمحتالين التظاهر بأنهم أي شخص على الإنترنت، بما في ذلك الحكومة أو شركة حقيقية أو المشاهير أو أصدقائك أو عائلتك.

يمكنهم إنشاء مواقع إنترنت مزيفة لتبدو وكأنها علامات تجارية معروفة. قد ينتحلون شخصية أشخاص مشهورين ويجعلون الأمر يبدو وكأنهم يوافقون على السلع أو الخدمات. يمكن أن تحتوي هذه المواقع على تقييمات زائفة لتجعلك تثق بها.

قد ترى لافتات إعلانية زائفة أو نوافذ منبقة تحتوي على تحذيرات أو رسائل خطأ زائفة عند تصفح الإنترنت.

علامات على أن موقع الانترنت قد يكون عملية احتيال

الموقع:

يعرض سلعاً للبيع بأسعار أقل بكثير من المعتاد أو مقارنة بالمواقع الأخرى.



يخبرك عن طريقة لكسب المال بسرعة وسهولة مع القليل من المخاطرة أو الجهد.



يحتوي على تحذير عاجل أو رسالة خطأ تطلب منك النقر فوق رابط.



يطلب الدفع بطرق غير معتادة أو محددة مثل بطاقات الهدايا أو العملات المشفرة مثل البيتكوين.



يتضمن التقييمات الإيجابية فقط.



الخطوات التي يمكنك اتخاذها لتجنب عمليات الاحتيال على موقع الانترنت

1. قارن الأسعار. إذا بدا العرض جيداً لدرجة يصعب تصديقه، فمن المحتمل أن يكون كذلك.



2. ابحث عن المنظمة أو الشخص الذي تتعامل معه قبل إعطاء أموالك أو معلوماتك الشخصية.



3. لا تعتمد على التقييمات المكتوبة على الموقع نفسه. ابحث عن موقع الإنترنت أو اسم المصلحة التجارية وكلمة "احتيال" أو "تقييمات".



4. إذا ظهرت رسالة تحذير أو خطأ على شاشتك، فلا تنقر عليها، بل انتقل بدلاً من ذلك إلى التطبيق الذي تشير إليه مباشرةً للتحقق مما إذا كانت حقيقية.



5. حافظ على تحديث الجهاز الذي تستخدمه للتسوق على الإنترنت من خلال تمكين "التحديثات التلقائية" لنظام التشغيل والتطبيقات لديك.



من الجيد ان تعلم!
تتوفر الطرق العملية لحماية نفسك على الإنترنت
على www.cyber.gov.au





عمليات الاحتيال على وسائل التواصل الاجتماعي والتطبيقات والرسائل عبر الإنترنت

إذا اتصل بك شخص لا تعرفه على وسائل التواصل الاجتماعي، أو منصة مراسلة مثل WhatsApp أو WeChat، أو عبر أحد التطبيقات، فقد يكون ذلك عملية احتيال.

غالبًا ما يستخدم المحتالون الذين يتظاهرون بأنهم شخص آخر الصورة الحقيقية للشخص أو الشعار الرسمي للمنظمة التي يتظاهرون بها، وذلك لجعل عملية الاحتيال أكثر صعوبة في اكتشافها.

سيقوم المحتالون على وسائل التواصل الاجتماعي بإنشاء ملفات تعريف مزيفة والتظاهر بأنهم من الحكومة، أو شركة حقيقية، أو صاحب عمل، أو شركة استثمار، أو حتى صديق أو أحد أفراد العائلة أو اهتمامات رومانسية.

قد ينتحلون شخصية أشخاص مشهورين ويجعلون الأمر يبدو وكأنهم يروجون للسلع أو الخدمات. يمكن للمحتالين أيضًا معرفة الكثير عنك من التفاصيل التي تشاركها على حساباتك على وسائل التواصل الاجتماعي. يمكنهم استخدام هذه المعلومات لتخمين كلمات مرور حسابك أو استهدافك بعمليات احتيال أخرى.

علامات الاحتيال على وسائل التواصل الاجتماعي أو التطبيقات

ملف تعريف وسائل التواصل الاجتماعي أو التطبيق:

يخبرك عن طريقة لكسب المال بسرعة وسهولة مع القليل من المخاطرة أو الجهد.



يدعوك للدخول في مسابقة أو عرض لفترة محدودة.



يطلب نقل محادثة من تطبيق مثل تطبيق المواعدة إلى الدردشة الخاصة أو البريد الإلكتروني.



يقترح أن شخصًا مشهورًا يؤيد أو يدعم منتجًا أو خدمة.



يقول إن شخصًا ما سيشتري شيئًا تبيعه دون أن يراه أولاً وبسعر مرتفع.



يهدد بمشاركة صورة خاصة لك ما لم تدفع له المال.



يتصل بك ليعرض عليك وظيفة



من الجيد ان تعلم!

يمكن العثور على معلومات حول كيفية البقاء آمنًا على منصات التواصل الاجتماعي المختلفة على www.esafety.gov.au



الخطوات التي يمكنك اتخاذها لتجنب عمليات الاحتيال عبر وسائل التواصل الاجتماعي والتطبيقات

1. تحقق مما إذا كان ملف التعريف الشخصي مزيّفًا. هل الحساب نشط؟ كم عدد الأصدقاء/المتابعين لديهم وكم عدد منشوراتهم على الإنترنت؟



2. ابحث عن اسم الملف الشخصي على الإنترنت مع كلمة "احتيال".



3. لا تقبل أبدًا الوظيفة التي عُرضت عليك دون إجراء مقابلة أو مناقشة حول خبرتك ومدى ملاءمتك ومراجعك. ابحث عن مسؤول التوظيف والشركة أو الفرد الذي يعرض الوظيفة. اتصل بوكالة التوظيف على أرقام الهواتف التي تم الحصول عليها من بحث مستقل على الإنترنت. لا تدفع المال مقدمًا فقط للحصول على وظيفة.



4. لا تأخذ نصيحة استثمارية سوى من شخص لديه ترخيص للخدمات المالية الأسترالية وتأكد من عدم ذكر اسم الشركة أو موقع الإنترنت على بوابة تسيّيات المستثمرين التابعة للمنظمة الدولية لهيئات الأوراق المالية (IOSCO).



5. لا تعطي المال أبدًا لشخص قابلته على الإنترنت فقط. كثيرًا ما يقول المحتالون إنهم يعيشون في الخارج ولا يمكنهم مقابلتك شخصيًا.



6. لا ترسل أبدًا صورًا حميمة لك إلى شخص تعرفت عليه على الإنترنت فقط.



لمزيد من المعلومات حول عمليات الاحتيال بما في ذلك الطرق الأخرى التي قد يتصل بها المحتالون بك، مثل التواصل الشخصي أو من خلال البريد، قم بزيارة [Scamwatch](#).



أهم عمليات الاحتيال التي يجب أن تعرفها

فيما يلي بعض أنواع الاحتيال الأكثر شيوعًا التي يجب أن تكون على دراية بها. يمكنك العثور على مزيد من المعلومات حول كل نوع من أنواع عمليات الاحتيال هذه، بما في ذلك العلامات التحذيرية والخطوات اللازمة لحماية نفسك، على موقع [Scamwatch](#) الإلكتروني.

عمليات احتيال عبر انتحال الشخصية

يخدعك المحتالون بجعلك تعتقد أنهم ينتمون إلى مؤسسات موثوقة مثل الشرطة والحكومة والمصارف والشركات المعروفة. يمكنهم حتى التظاهر بأنهم صديقك أو أحد أفراد أسرتك. يبحث المحتالون عن معلومات عنك عن طريق إرسال رسائل بريد إلكتروني أو رسائل تصيديه. هذه مصممة لسرقة معلوماتك. يحاولون إقناعك بمنحهم معلوماتك الشخصية من خلال التظاهر بأنهم من منظمة رسمية أو شخص تعرفه وتتق به.

يستخدم المحتالون التكنولوجيا لجعل مكالماتهم أو رسائلهم تبدو وكأنها واردة من رقم هاتف شرعي. يمكنهم جعل الرسائل النصية تظهر في نفس سلسلة المحادثة كرسائل حقيقية من مؤسسة.

عمليات الاحتيال الاستثمارية

يستخدم المحتالون التسويق المقنع والتكنولوجيا الجديدة لجعل مقترحهم الاستثماري يبدو جيدًا للغاية بحيث لا يمكن تفويته. يعدونك بأرباح كبيرة مع أخطار قليلة أو معدومة. غالبًا ما يستخدمون أساليب الضغط لجعلك تنصرف بسرعة، حتى يتمكنوا من سرقة أموالك.

عمليات الاحتيال عبر الوظائف والتوظيف

يقدم المحتالون وظائف ذات أجر جيد وبجهد قليل. يتظاهرون بأنهم يقومون بالتوظيف نيابة عن شركات رفيعة المستوى ومنصات التسوق على الإنترنت. في بعض الأحيان، الوظيفة التي يدرجونها غير موجودة. كما يتحلل المحتالون صفة وكالات التوظيف المعروفة. هدفهم هو سرقة أموالك ومعلوماتك الشخصية. قد يطلبون منك دفع المال مقدماً حتى تتمكن من العمل معهم.

عمليات الاحتيال المتعلقة بالمنتجات والخدمات

يتظاهر المحتالون بأنهم مشترين أو بائعون لسرقة أموالك. يقومون بإنشاء مواقع إنترنت أو ملفات تعريف مزيفة على مواقع بيع بالتجزئة مشروعة مقدّمين منتجات أو خدمات بأسعار جيدة جداً لدرجة يصعب تصديقها. ينشرون إعلانات وهمية وتقييمات وهمية. وقد يستخدمون الشعارات المسروقة واسم النطاق **com.au**. ورقم تجاري أسترالي مسروق (ABN). من الصعب اكتشاف هذه الحيل.

يتظاهر المحتالون أيضاً بأنهم شركات تعرفها وتثق بها لإرسال فواتير مزيفة إليك. يمكنهم أيضاً تغيير تفاصيل الفواتير الشرعية بحيث ينتهي الأمر بالعملاء إلى الدفع للمحتال بدلاً منك.

عمليات الاحتيال الرومانسية

يستخدم المحتالون الوعد بالحب أو المواعدة أو الصداقة لسرقة أموالك. إنهم يبذلون قصارى جهدهم لإقناعك بأن العلاقة حقيقية ويتلاعبون بك لمنحهم المال.

يعثر عليك المحتالون على مواقع التواصل الاجتماعي أو تطبيقات المواعدة أو الألعاب. وقد يرسلون لك رسائل نصية أو بريداً إلكترونياً. إنهم يختبئون وراء الملفات الشخصية والهويات المزيفة، وأحياناً لأشخاص مشهورين. بمجرد أن تثق بهم، سيكون لديهم "حالة طوارئ" ويطلبون مساعدتك. سيكون هذا غالباً طلبات للحصول على أموال أو منتجات أخرى.

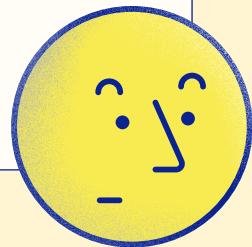
التحديات وعمليات الابتزاز

يتظاهر المحتالون بأنهم من منظمة موثوقة ويزعمون أنك بحاجة إلى دفع المال وإلا سيحدث شيء سيئ. قد يهددونك بالاعتقال أو الترحيل أو حتى الأذى الجسدي، إذا لم توافق على الدفع لهم على الفور. يمكنهم أيضًا ابتزازك من خلال التهديد بمشاركة الصور أو مقاطع الفيديو العارية التي أرسلتها إليهم ما لم ترسل إليهم أموالًا.

عمليات احتيال عبر أموال غير متوقعة

يحاول المحتالون إقناعك بأنك مستحق أو يحق لك الحصول على أموال أو مكاسب لم تكن تتوقع الحصول عليها.

يطلب منك المحتال دفع رسوم أو تقديم تفاصيل حسابك المصرفي أو هويتك قبل أن تتمكن من تحصيل الأموال أو المكاسب. لسوء الحظ، لا يوجد أموال مجانية.





أين يمكن الإبلاغ عن عمليات الاحتيال

نحن نعمل على جعل أستراليا هدفًا أكثر صعوبة للمحتالين من خلال زيادة الوعي حول كيفية التعرف على عمليات الاحتيال وتجنبها والإبلاغ عنها.

نحن نشارك المعلومات من تقارير عمليات الاحتيال ونعمل مع الحكومة ووكالات إنفاذ القانون والقطاع الخاص لتعطيل ومنع عمليات الاحتيال.

ساعد الآخرين من خلال إبلاغ Scamwatch. قم بالإبلاغ عن تجربتك مع الاحتيال من خلال نموذج الإبلاغ الموجود على موقع Scamwatch الإلكتروني www.scamwatch.gov.au

تذكر، إذا كنت ضحية لعملية احتيال، فمن المهم أن تتصرف بسرعة.

■ إذا خسرت أموالاً بسبب محتال، فاتصل بالمصرف الذي تتعامل معه أو مزود البطاقة.

■ اتصل بـ idcare.org | ID CARE: 1800 595 160



مزيد من المساعدة والدعم

إن كونك ضحية عملية احتيال يمكن أن يكون أمرًا مرهقًا. من المهم أن تتذكر أنه يمكن أن يحدث لأي شخص، وأن الدعم متاح.

إذا تعرضت أنت أو أي شخص تعرفه للاحتيال، فتحدث إلى شخص ما حول هذا الموضوع. يمكنك طلب الدعم من العائلة، أو الأصدقاء، أو طبيب العائلة، أو إحدى خدمات الدعم التالية.

لايف لاين Lifeline: 13 11 14 | lifeline.org.au

أو دردشة الدعم عند الأزمات على الإنترنت (24 ساعة في اليوم، 7 أيام في الأسبوع)

بيوند بلو Beyond Blue: 1300 22 4636 | beyondblue.org.au

أو الدردشة على الإنترنت (24 ساعة في اليوم، 7 أيام في الأسبوع)

خط مساعدة الأطفال Kids Helpline: 1800 55 1800 | kidshelpline.com.au

(24 ساعة في اليوم، 7 أيام في الأسبوع)

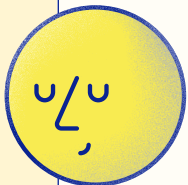
يمكن أن تكون التأثيرات المالية لعمليات الاحتيال مدمرة وتغير مجرى الحياة.

إذا كنت تعاني من ضائقة مالية، يمكنك التحدث مع مستشار مالي من خلال خط المساعدة الوطني الخاص

بالديون National Debt Helpline:

1800 007 007 من الساعة 9:00 صباحًا حتى 4:30 مساءً من الاثنين إلى الجمعة

أو قم بالوصول إلى الدردشة المباشرة من الساعة 9:00 صباحًا حتى 8:00 مساءً من الاثنين إلى الجمعة



scamwatch.gov.au