هل يمكنكم اكتشاف عملية احتيال؟

على الإنترنت، لا يمكننا دائمًا التأكد من أن الناس هم نفسهم الذين يقولون بأنهم هم. يُعد التعرف على المحتالين عبر الإنترنت إحدى أهم الخطوات لتجنبهم. وبمجرد أن تدركوا خِدعهم، يجب أن يكون من الأسهل اكتشاف عملية احتيال عندما تروا واحدة.

التصيّد الاحتيالي

يعتبر التصيّد الاحتيالي هو الشكل الأكثر شيوعًا من أشكال الاحتيال على الإنترنت. يمكن أن يبدو أنه من منظمة موثوق بها ومصمم لخداعكم لإعطاء تفاصيلكم الشخصية مثل حسابكم المصرفي ورقم بطاقة الائتمان واسم المستخدم و كلمات السر.

ويمكن أن يظهر في أشكال عديدة:

- رسائل بريد إلكتروني أو رسائل نصية أو مكالمات هاتفية غير متوقعة تطلب منكم تأكيد تفاصيلكم الشخصية أو تحديثها أو إعادة إدخالها
- رسائل عاجلة أو تهديدية تخبركم بشيء غير عادي يحدث لحسابكم، أو أنه سيتم إغلاق حسابكم، لذلك تحتاجون إلى النقر على رابط لتصحيحه
- رسائل إلكترونية غير متوقعة تطلب منكم فتح أو تنزيل ملف ".exe" أو ".zip"

نصيحة: إذا لم تكونوا متأكدين من الرسالة التي تلقيتموها، فقوموا بإجراء بحث عبر الإنترنت عن الشركة التي يبدو أنها أرسلت منها واتصلوا بها مباشرة.

تمهّلوا. أعيدوا قراءة الرسالة.

- من هو المرسِل؟ هل يبدوا أنه عنوان بريد إلكتروني رسمي أم عنوان غريب؟
- إلى من تم توجيهه؟ يكون مريبًا إذا كان إلى "عزيزي الزبون" بدلاً من اسمكم.
- هل يحتوي على قواعد نحوية أو تهجئة ضعيفة؟ يمكن أن يكون هذا علامة على أنه من مخادع

لا تقوموا بـ:

- النقر على أي روابط
- فتح أي مرفقات لأنها قد تقوم بتنزيل فيروس الكمبيوتر
- استخدام تفاصيل الاتصال الواردة في الرسالة، فقد تكون مزيفة

حيل الضرائب والميدكير

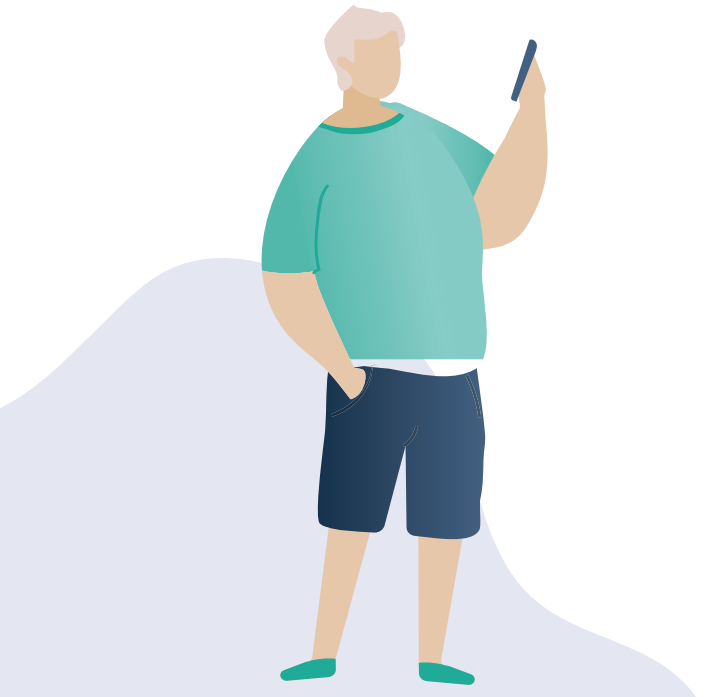
يقوم المحتالون بانتحال هوية مكتب الضرائب الأسترالي و الميديكير والمنظمات الحكومية الأخرى لكسب الأموال والمعلومات الشخصية من الضحايا من خلال مواقع ورسائل بريد إلكتروني ورسائل نصية ومكالمات هاتفية مزيفة.

من المهم أن تتذكروا، أن مكتب الضرائب الأسترالي (ATO) لن يقوم أبدًا بما يلي:

- ارسال لكم بريدًا إلكترونيًا أو رسالة نصية تطلب معلوماتكم الشخصية بما في ذلك بيانات رقم الملف الضريبي (TFN) أو بطاقة الائتمان أو البنك
- الطلب منكم دفع رسوم لتلقي العائد الضريبي، أو للتخلص من إلقاء القبض عليكم بتهمة التهرب الضريبي
- إرسال بريد إلكتروني إليكم يحتوي على رابط لخدمة عبر الإنترنت تطلب تفاصيلكم الشخصية
- إرسال لكم ملفات قابلة للتنزيل أو إخباركم بتثبيت برنامج

ما الذي يمكنكم فعله لتكونوا أذكياء وآمنين؟

- لا تنقروا على أي روابط أو تقوموا بتنزيل أي مرفقات.
- لا تعطوا تفاصيل شخصية مثل رقم ملفكم الضريبي (TFN) أو تاريخ ميلادكم أو تفاصيل حسابكم المصرفي أو تفاصيل بطاقة الائتمان.
- إذا لم تكونوا متأكدين مما إذا كانت رسالة الهاتف حقيقية، فلا تستخدموا تفاصيل الاتصال المقدمة، وبدلاً من ذلك ابحثوا عبر الإنترنت عن رقم المؤسسة.
- إعرفوا وضع شؤونكم الضريبية – هل من المحتمل أن تكونوا مستحقين لعائد ضريبي أو مدينين بدفعة؟
- قوموا بتسجيل الدخول إلى حساب myGov الرسمي الخاص بكم بكتابة العنوان يدويًا بدلاً من النقر فوق رابط.
- تحققوا مما إذا كان البريد الإلكتروني الذي تلقيتموه من عنوان ATO الحقيقي ينتهي بـ @ato.gov.au.
- حتى إذا كان يبدو أنكم على موقع ATO أو myGov، تحققوا من أن العنوان ينتهي بـ gov.au. (بدلاً من com.au. أو org.au. أو net.au. على سبيل المثال).
- ابحثوا عن القواعد والتهجئة السيئة.
- كونوا حذرين من الرسائل التي لا يتم توجيهها إليكم مباشرةً.



الحيل الرومانسية والمواعدة

يقوم المخادعون بإنشاء ملفات تعريف مزيفة عبر الإنترنت على وسائل التواصل الاجتماعي أو مواقع المواعدة للتواصل مع الضحايا. هدفهم هو كسب ثقتكم قبل طلب المال.

ما الذي يمكنكم فعله لتكونوا أذكياء وآمنين؟

ابحثوا عن:

- الأشخاص الذين يعبرون عن مشاعر عميقة لكم بسرعة كبيرة قبل طلب المال، أو "قرض".
- الأشخاص الذين يتجنبون الإلتقاء وجهًا لوجه ويختلقون أسباب لعدم تمكنهم من السفر لرؤيتكم.
- الأشخاص الذين لا يتطابق ملفهم الشخصي عبر الإنترنت مع ما أخبروكم به عن أنفسهم.

قوموا بـ:

- التحقق مما إذا كانت صورهم هي بالفعل صورهم أو إذا تم التقاطها من مكان آخر على الإنترنت من خلال البحث في صور Google. قوموا بزيارة images.google.com وانقروا على أيقونة الكاميرا.
- كونوا متشككين عندما يبدأون في ذكر مشاكل المال أو الحاجة إلى المال لحالة "طارئة".

لا تقوموا بـ:

- تحويل أي أموال إلى شخص ما تحدثتم معه فقط عبر الهاتف أو البريد الإلكتروني.
- إرسال معلومات شخصية مثل تاريخ ميلادكم أو تفاصيل البنك أو بطاقة الائتمان.

حيل الدعم التقني

تبدأ عمليات الاحتيال هذه عادةً بمكالمة أو بريد إلكتروني يبدو أنه من مؤسسة كبيرة ومعروفة لإخباركم أن لديكم مشكلة في الكمبيوتر أو الإنترنت ويمكنهم إصلاحها.

ما الذي يمكنكم فعله لتكونوا أذكياء وآمنين؟

- لا توفروا الوصول عن بعد إلى جهاز الكمبيوتر الخاص بكم.
- لا تزودوهم بمعلومات شخصية مثل حسابكم المصرفي أو تفاصيل بطاقة الائتمان الخاصة بكم.
- لا تشتروا برامج من مكالمة أو بريد إلكتروني غير مرغوب فيه.
- تجاهلوا الرسائل المنبثقة التي تخبركم بالاتصال بالدعم التقني.

تتوقع المؤسسات الكبيرة منكم الاتصال بها عندما تكون هناك مشكلة في الإنترنت أو الكمبيوتر. لن يتصلوا بكم.

ساعدوني، أعتقد أنني وقعت في عملية احتيال

إذا كنتم تعتقدون أنكم وقعتم ضحية لعملية احتيال، لا تشعروا بالحرج ولا تحتفظوا بها لنفسكم هناك خطوات يمكنكم اتخاذها لإصلاح المشكلة:

- اتصلوا بالمصرف الذي تتعاملون معه وأوقفوا أي دفعات أخرى إلى المخادع
- أبلغوا المفوضية الأسترالية للمنافسة والمستهلكين عن عملية الاحتيال على scamwatch.gov.au - يمكنهم مساعدتكم بمزيد من النصائح
- زيادة التوعية. إذا كان هناك أي شخص آخر تعرفونه قد يكون ضحية، فأخبروه بذلك

إذا لم تكونوا متأكدين مما إذا كانت الرسالة التي تلقيتموها هي فعلاً من ATO، أو كنتم ضحية لعملية احتيال تتعلق بالضرائب، اتصلوا **بالخط الساخن لـ ATO** على الرقم **1800 008 540**.

ابقوا على اطلاع على حيل ATO من خلال زيارة ato.gov.au/scams

إذا كنتم قلقين بشأن الكشف عن معلوماتكم الشخصية وإساءة استخدامها، فاتصلوا بخدمة أستراليا للهوية الوطنية والدعم السيبراني **IDCARE** على الرقم **1300 432 273** أو idcare.org

تذكروا:

هناك دائمًا شخص يمكنه المساعدة - سواء كانوا أشخاص في scamwatch.gov.au، أو صديقًا أو أحد أفراد العائلة ذا خبرة تقنية، أو حتى نادي كمبيوتر محلي.

تهدف عمليات الاحتيال إلى الاستفادة من طبيعتكم الجيدة، ولكن يمكن أن يكون الإنترنت مكانًا آمنًا للاستكشاف إذا كنتم حريصين حول مشاركة المعلومات الشخصية عبر الإنترنت، واستخدام الحس السليم بشأن لمن ترسلوا الأموال والبقاء حذرين.

خذوا وقتكم في استكشاف Be Connected

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

beconnected.esafety.gov.au