أفضل عشر نصائح لحماية نفسك ضد

عمليات الاحتيال بانتحال الشخصية

العربية | Arabic

Australian Government | National Anti-Scam Centre | SCAMWATCH | Australian Government | Be Connected Every Australian online.

أصبحت عمليات الاحتيال اليوم أكثر تعقيدًا وتطورًا بشكل متزايد. في السابق، كانت الأخطاء الإملائية والنحوية تجعل من السهل اكتشافها، لكن التكنولوجيا الجديدة تعني أن عمليات الاحتيال أصبحت أكثر صعوبة في الكشف.

تعاون المركز الوطني لمكافحة الاحتيال (National Anti-Scam Centre) مع الحكومة وخبراء الصناعة وهيئات إنفاذ القانون ومنظمات المجتمع لمكافحة الاحتيال. لكن هناك أيضًا خطوات يمكنك اتخاذها لحماية نفسك من التعرض للاحتيال. أحد أفضل وسائل الحماية هو البقاء على اطلاع بأحدث الاحتيالات الحديثة حتى تتمكن من التعرف على العلامات.

تعاونت هيئة Be Connected مع مركز Scamwatch التابع لمركز مكافحة الاحتيال الوطني لتقديم هذا الدليل لمساعدتك في اكتشاف عمليات الاحتيال بانتحال الشخصية وحماية نفسك منها ومعرفة أين تذهب للحصول على المساعدة إذا وجدت نفسك ضحية للاحتيال.

جميع الأمثلة المقدمة في هذا الدليل هي عمليات احتيال حقيقية.

في هذا الدليل

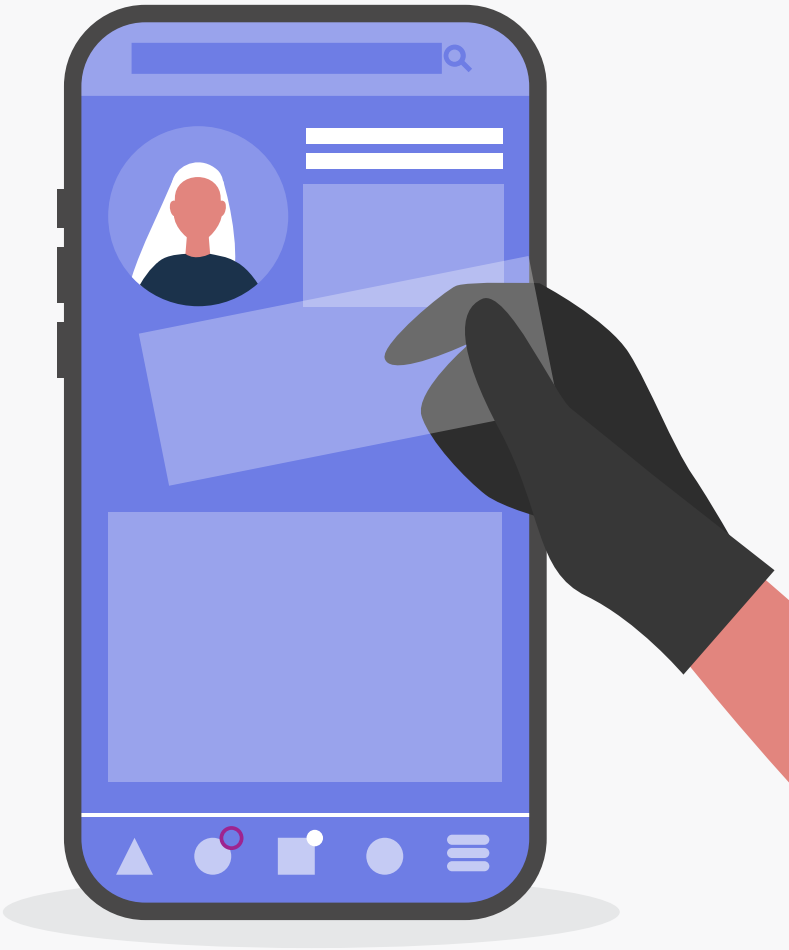
- ما هي عمليات الاحتيال بانتحال الشخصية؟
- ما هو الانتحال؟
- عمليات الاحتيال بانتحال الشخصية الشائعة
- أفضل عشر نصائح لحماية نفسك
- أين تذهب للحصول على المساعدة

ما هو الاحتيال بانتحال الشخصية؟

تم تصميم عمليات الاحتيال بانتحال الشخصية لتبدو وكأنها من جهات شرعية تعرفها. قد تبدو وكأنها صادرة من البنك أو مزود خدمة الإنترنت أو وكالة حكومية أو بائع تجزئة أو حتى محتال يتظاهر بأنه صديق أو أحد أفراد الأسرة.

من خلال التظاهر بأنه شخص تثق به، يلجأ المحتالون إلى استخدام إحساس الشعور بالعجلة لخداعك وحثك على دفع المال أو تقديم معلومات شخصية، مثل كلمات المرور المهمة أو تفاصيل بطاقة الائتمان أو التفاصيل المصرفية.

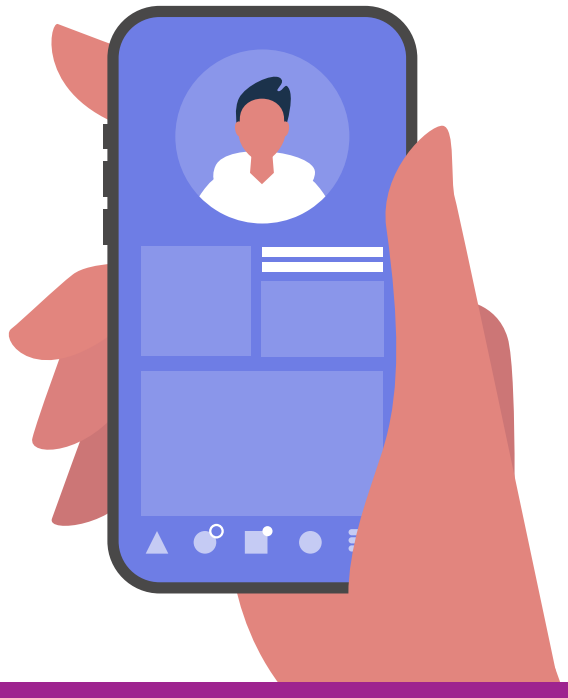
يستخدم المحتالون مجموعة من الأساليب للتواصل معك، بما في ذلك الرسائل النصية والمكالمات الهاتفية ورسائل البريد الإلكتروني ومنشورات وسائل التواصل الاجتماعي والمواقع الإلكترونية المزيفة التي تبدو متطابقة مع المواقع الرسمية.



ما هو الانتحال؟

يمكن للمحتالين انتحال شخصيات مؤسسات تعرفها وذلك باستخدام التكنولوجيا لجعل مكالمتهم أو رسالتهم تبدو وكأنها تأتي من مصدر موثوق. يُعرف هذا بالانتحال.

كن واعيًا بأساليب الاحتيال واطرح الأسئلة حول أي تواصل غير مرغوب فيه يطلب منك معلومات شخصية، مثل كلمة المرور أو أي شكل من أشكال الدفع. تواصل مباشرةً مع الجهة التي تزعم أنها المرسل للتأكد.



هناك أنواع مختلفة من تقنيات الاحتيال، بما في ذلك:

.01 **تزييف مُعرّف المتصل:** يغير المحتالون مُعرّف المتصل الخاص بهم ليظهر رقم هاتف مختلف عن الرقم المستخدم، مما يجعل المكالمة تبدو وكأنها تأتي من رقم شرعي.

.02 **تزييف الرسائل النصية (اسم المرسل الرسمي أو علامات ألفا):** يقوم المحتالون بتغيير رقم هاتفهم ليظهر كاسم عمل تجاري (على سبيل المثال، AusPost). يمكن ذلك أن يجعل الرسالة النصية تظهر في نفس المحادثة أو السلسلة مثل الرسائل الحقيقية المرسلة من منظمة ما.

.03 **تزييف البريد الإلكتروني:** يقوم المحتالون بتغيير عنوان بريدهم الإلكتروني أو اسم المرسل لجعل البريد الإلكتروني يبدو وكأنه من مصدر موثوق. قد يزيفون اسم المرسل الظاهر في حقل "من" أو عنوان البريد الإلكتروني، غالبًا عن طريق تغيير أو إضافة حرف أو رقم إلى اسم نطاق شرعي (على سبيل المثال، @amaz0n.com بدلًا من @amazon.com).

عمليات الاحتيال بانتحال الشخصية الشائعة

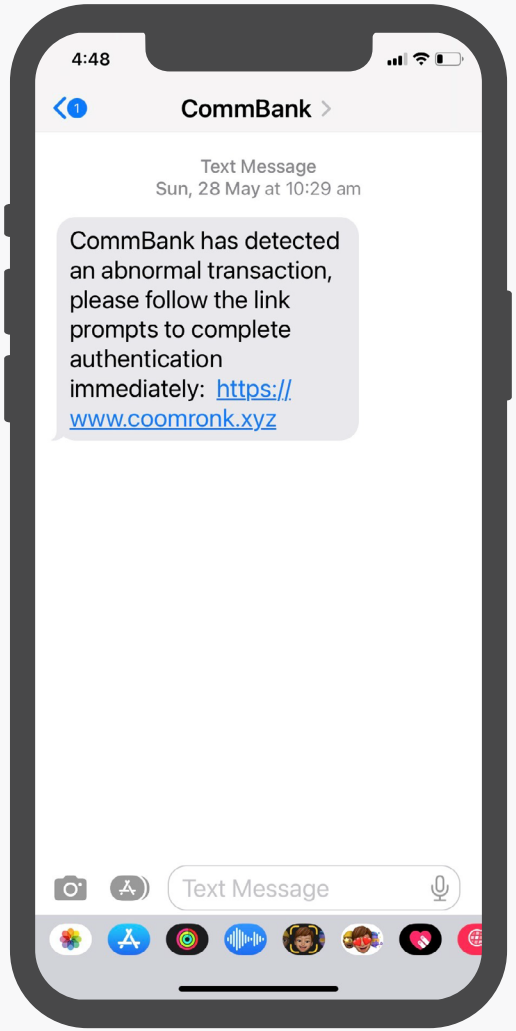
عمليات الاحتيال بانتحال شخصية مصرف

- تتلقى مكالمة أو رسالة نصية من شخص يزعم أنه من قسم الأمن في المصرف. يخبرك بوجود معاملة مشبوهة، مدعيًا أن حسابك المصرفي قد تم اختراقه. يحثك على تحويل الأموال إلى حساب آخر "للحفاظ عليها آمنة" أو "لإجراء مزيد من التحقيق".
- تتلقى رسالة نصية أو بريدًا إلكترونيًا يطلب منك النقر على رابط للتحقق من تفاصيل حسابك. يأخذك الرابط إلى موقع مزيف مصمم لالتقاط اسم المستخدم وكلمة المرور ومعلوماتك الشخصية الأخرى.

كيف تعرف أنها عملية احتيال؟

بينما قد يتصل بك المصرف إذا كان هناك نشاط مشبوه على حسابك، فإنه لن يطلب منك أبدًا تحويل الأموال إلى حساب آخر. لن يطلب أي حساب أو تفاصيل شخصية، بما في ذلك كلمة المرور أو الرقم السري أو رمز المرور لمرة واحدة في رسالة نصية أو بريد إلكتروني أو مكالمة هاتفية غير مطلوبة.

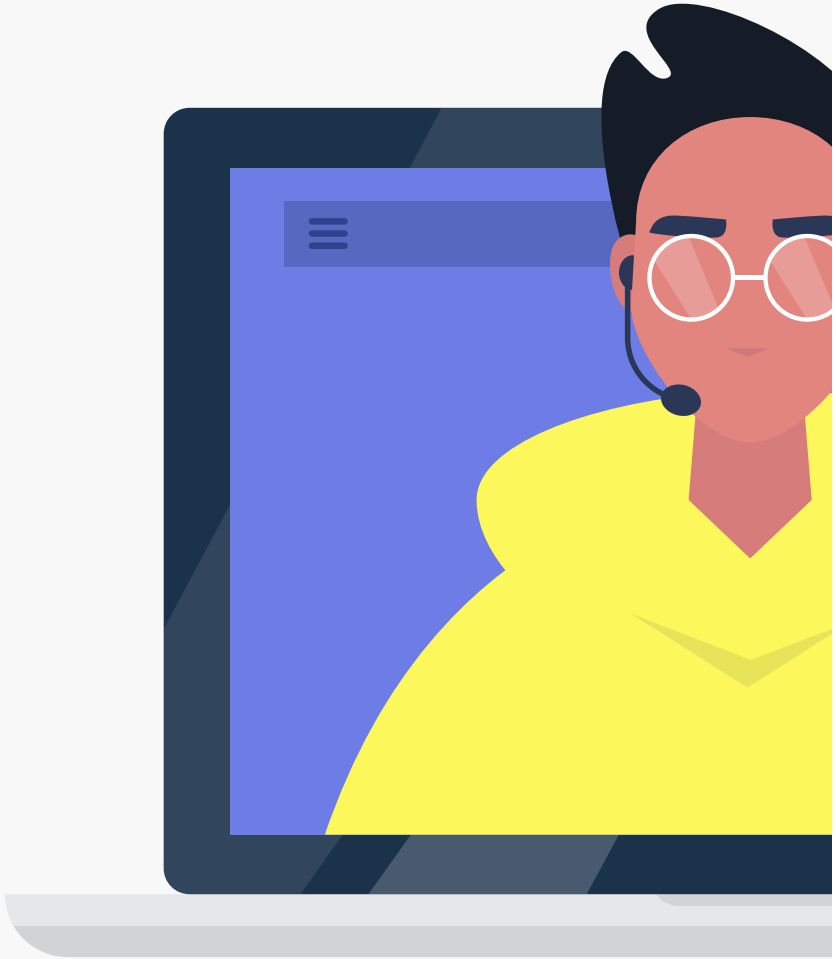
يمكن للمحتالين جعل رقم الهاتف يبدو كمعرف المتصل الخاص بالمصرف، لكن لا تأخذ ذلك كدليل على من تتحدث إليه. قد يبدو أن لديهم معلومات عنك، لكن من المحتمل أن تكون تلك التفاصيل قد تم الحصول عليها بطريقة احتيالية.



مثال على رسالة نصية بانتحال شخصية مصرف من رقم مزيف تطلب منك النقر على رابط للتحقق من تفاصيلك.

عمليات احتيال دعم التقنية

- مُتصل يدّعي أنه من مزود خدمة الإنترنت أو شركة اتصالات أو حواسيب، يبلغك بوجود مشكلة في الإنترنت أو جهاز الحاسوب الخاص بك. قد يقولون إنه تم اختراقه أو يحتوي على فيروس أو يعمل ببطء أو على وشك أن يتم فصله. يوجهونك لتنزيل تطبيق أو برنامج لمنحهم إمكانية الوصول إلى جهازك من على عن بُعد حتى يتمكنوا من "إصلاحه".
- تظهر رسالة تحذير على شاشة جهازك تحثك على الاتصال فورًا بالرقم المدرج للحصول على المساعدة بشأن مشكلة تم اكتشافها.



كيف تعرف أنها عملية احتيال؟

الشركات الشرعية لن تتصل بك أبدًا لتخبرك أن هناك مشكلة في اتصال الإنترنت أو جهاز الحاسوب الخاص بك (يتوقعون منك الاتصال بهم عندما تكون هناك مشكلة). لن يطلبوا منك أبدًا تنزيل أي نوع من البرامج أو التطبيقات التي تمنحهم إمكانية الوصول إلى جهازك.

قم بإغلاق الرسائل المنبثقة المشبوهة بالنقر على علامة "x" في الزاوية العلوية اليمنى من المربع. إذا لم ينجح ذلك، حاول النقر خارج المربع أو أغلق صفحة الإنترنت التي تظهر عليها. إذا لم تختفِ الرسالة المنبثقة، حاول الضغط على مفاتيح ALT و F4 على جهاز الحاسوب الذي يعمل بنظام ويندوز (Windows) لإغلاق متصفح الإنترنت. على جهاز حاسوب Apple، اختر إنهاء قسري من قائمة Apple واختر المتصفح الذي تريد إغلاقه.

عمليات احتيال تعليق الحساب

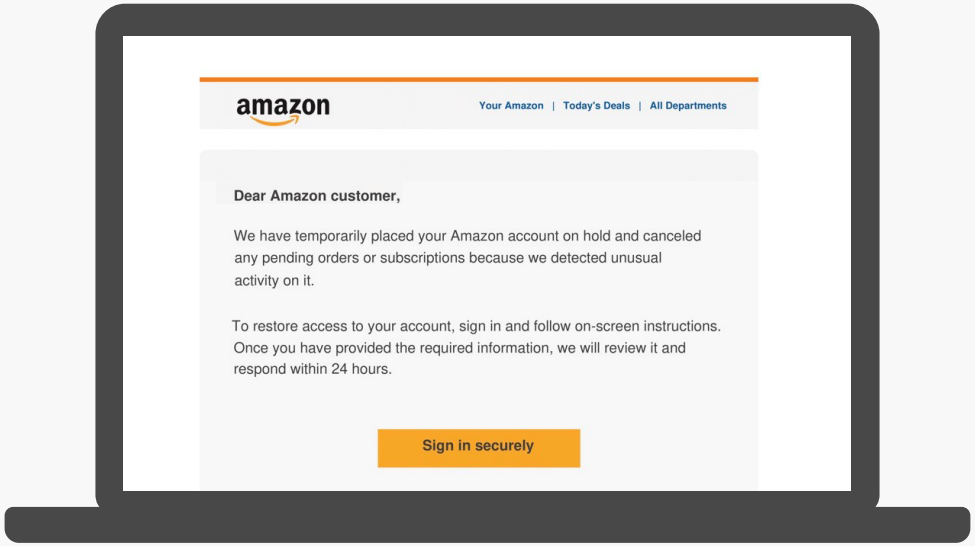
تتلقى رسالة بريد إلكتروني أو رسالة نصية تدّعي أنها من جهة تعرفها، مثل Amazon أو PayPal أو Netflix. تبلّغك بأنه قد تم تعليق حسابك بسبب نشاط مشبوه وأنك ستحتاج إلى النقر على رابط لتأكيد هويتك حتى يتأكدوا من أنك أنت بالفعل.

يستخدم المحتالون أساليب تخويف لتوجيهك إلى موقع إلكتروني مزيف يلتقط تفاصيل شخصية مثل اسم المستخدم وكلمة المرور وتفاصيل المصرف أو بطاقة الائتمان.

كيف تعرف أنها عملية احتيال؟

لن تطلب Amazon أو PayPal أو Netflix منك أبدًا معلومات شخصية مثل كلمات المرور أو التفاصيل المصرفية أو تفاصيل بطاقة الائتمان من خلال رابط في بريد إلكتروني أو رسالة نصية غير مطلوبة. بينما تختلف الجهات في نهجها في التواصل مع العملاء، فمن الأفضل توخي الحيطة دائمًا وأن تتعامل مع هذه الأنواع من الرسائل الإلكترونية أو الرسائل النصية أو المكالمات بحذر.

إذا لم تكن متأكدًا مما إذا كانت الرسالة صادرة فعلًا من الجهة التي تدّعي أنها منها، فتواصل مباشرة معه تلك الجهة من خلال البحث عن تفاصيل الاتصال الخاصة بها عبر الإنترنت. لا تستخدم أبدًا بيانات الاتصال الواردة في نص الرسالة أو البريد الإلكتروني أو المكالمة الهاتفية.



مثال على بريد إلكتروني احتيالي يدعي أنه من Amazon يحثك على النقر على الرابط لتقديم معلوماتك الشخصية.

انتبه لأساليب التخويف

يستخدم المحتالون أساليب التخويف لخلق شعور بالعجلة لجعلك تتصرف. إليك بعض العبارات التي قد يستخدمونها لجذب انتباهك:

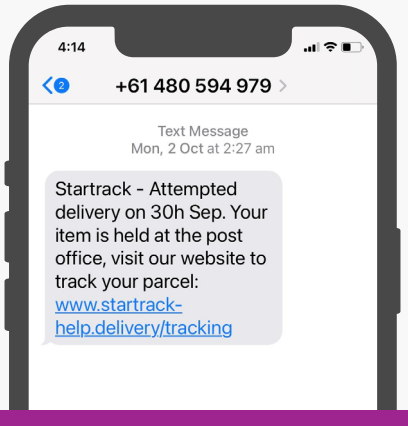
- تم اكتشاف نشاط غير عادي في الحساب
- محاولات تسجيل دخول غير مصرح بها
- حسابك محظور / مقفل
- تم رفض دفعتك
- لا يمكننا التحقق من معلومات الفاتورة الخاصة بك

عمليات احتيال محاولات تسليم غير ناجحة

تتلقى بريدًا إلكترونيًا أو رسالة نصية تدّعي أنها من Australia Post أو شركة توصيل مثل FedEx تخبرك أن هناك مشكلة أو تأخير في تسليم طردك. لتلقي الطرد، ستحتاج إلى دفع تكلفة الشحن أو "تحديث بياناتك".

كيف تعرف أنها عملية احتيال؟

لن تقوم هيئة البريد الأسترالي Australia Post وشركة خدمات شحن البضائع FedEx وغيرها من شركات النقل الشرعية أبدًا بإرسال نصوص أو رسائل بريد إلكتروني أو إجراء اتصالات هاتفية لطلب معلومات شخصية أو طلب دفع أموال. إذا كنت تتوقع استلام طرد، فمن الأفضل أن تتبع التسليم من خلال تطبيقهم الآمن أو من خلال خدمة التتبع الإلكتروني المدرجة في بريد تأكيد استلام طلبك الإلكتروني. إذا لم تكن تتوقع طردًا، اتصل بشركة النقل مباشرة للاستفسار عن حالة الطرد.



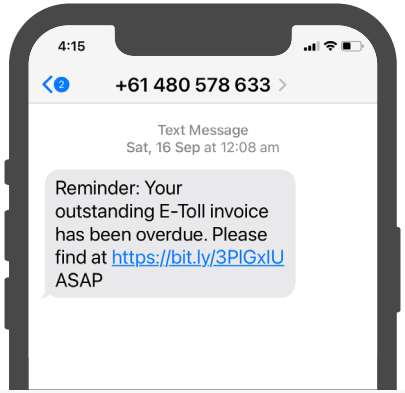
مثال على رسالة نصية تدعي أنها من شركة توصيل.

عمليات احتيال الطرق السريعة ذات الرسوم

تتلقى رسالة نصية من إحدى شركات الطرق السريعة تبلغك بأن دفعة رسوم المرور الخاصة بك متأخرة. وتحتاج لاتخاذ إجراء فوري لتجنب دفع غرامة، لذا يرسلون لك رابطًا لترتيب الدفع ولكنه يأخذك لموقع مزيف مصمم لسرقة تفاصيلك المالية.

كيف تعرف أنها عملية احتيال؟

إذا تم إرسال رسالة نصية إليك تدّعي أن لديك حساب رسوم طريق متأخر الدفع أوأن الرصيد غير كافي، فقد يكون ذلك احتيالًا. قم بزيارة موقع شركة تشغيل الطرق أو التطبيق لتسجيل الدخول إلى حسابك للتحقق من نشاطك الأخير.



مثال على نص احتيالي لطريق سريع.

عمليات احتيال الاستثمار الوهمية

ترى فرصة استثمارية مذهلة يبدو أنها مؤيدة من قبل شخصية مشهورة أو شخص مؤثر في مجال التمويل. تقدم وعد بعائد مرتفع مضمون قليل المخاطر أو بدون مخاطر. عندما تستفسر، يتم توجيهك إلى موقع إلكتروني يبدو احترافيًا وتتلقى من خلاله مواد ترويجية متطورة.

كيف تعرف أنها عملية احتيال؟

إذا كانت الصفقة تبدو جيدة جدًا لدرجة يصعب تصديقها، فمن المحتمل أن تكون كذلك. يستخدم المحتالون أساليب الضغط الشديد لإقناعك بالتصرف بسرعة حتى لا "تفوّت الفرصة". احذر من رسائل البريد الإلكتروني أو المواقع الإلكترونية أو الإعلانات التي تحتوي على شهادات ووعود مُبالغ فيها بعوائد كبيرة.

قد يدعي "المستشار" الذي يساعدك أنه لا يحتاج إلى ترخيص خدمات مالية أسترالية (AFS). إذا قدم ترخيصًا، تحقق دائمًا من أن الشخص الذي تتعامل معه هو الحائز الحقيقي على الترخيص.

عمليات احتيال المواقع الوهمية

ترى إعلانًا على Facebook لعلامة تجارية مشهورة لمشواة تُباع بسعر 100 دولار بينما سعرها العادي 900 دولار. تنقر على رابط موقع البائع وترى أن المدفوعات بواسطة بطاقة الائتمان تفرض رسومًا بنسبة 2.99%، لذا تختار الدفع عن طريق التحويل المصرفي المباشر للحصول على خصم إضافي بنسبة 5%. تتلقى بريدًا إلكترونيًا للتأكيد ولكن لا يوجد مشواة.

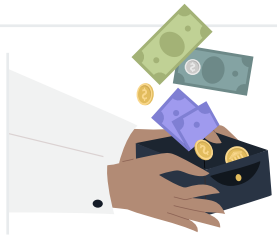
كيف تعرف أنها عملية احتيال؟

المواقع المزيفة تعرض أسعارًا تبدو مغرية جدًا بشكل غير واقعي وتطلب طرق دفع غير معتادة وتظهر فيها علامات تحذيرية أخرى مثل عنوان رابط URL يحاول أن يبدو مثل عنوان رابط URL لمتجر رسمي (على سبيل المثال، webberbbqs.com مقابل weber.com الحقيقي).

يمكن للمحتالين أيضًا الدفع مقابل الإعلانات على وسائل التواصل الاجتماعي ومحركات البحث مثل Google (المعروفة بالإعلانات المموّلة)، لذا كن حذرًا عند النقر على هذه الأنواع من الإعلانات.

أفضل عشر نصائح لحماية نفسك

.01 احذر من المكالمات غير المرغوب فيها. دع المكالمات من أرقام الهواتف التي لا تعرفها تذهب إلى البريد الصوتي.



.02 توقف وفكر قبل أن تقدم تفاصيل شخصية أو مالية عبر اتصالات لم تطلب الاتصال بها. اسأل نفسك: هل يمكن أن يكون مزيفًا؟

.03 احذر من رسائل البريد الإلكتروني التي تستخدم أساليب التخويف. تحقق من اسم العرض وعنوان البريد الإلكتروني. هل يتطابقان؟ على سبيل المثال، قد يُظهر حقل "من" أنه من دعم Amazon ولكن عنوان البريد الإلكتروني هو amazonsupport830@gmail.com

.04 لا تثق في رسالة نصية لمجرد أنها تظهر في نفس السلسلة مع رسائل أخرى من منظمة تعرفها. قد لا تزال تكون رسالة احتيالية.

.05 إذا كنت غير متأكد من رسالة أو مكالمة تلقيتها، فاتصل بالمنظمة التي تدعي أنها منها. تواصل عبر موقعهم الرسمي أو تطبيقهم الآمن على الهاتف الذكي أو الجهاز اللوحي.

.06 لا تفصح أبدًا عن كلمة المرور الخاصة بك أو الرقم السري أو رمز لمرة واحدة لأي شخص عبر الهاتف، حتى لو ادعى أنه من المصرف أو وكالة حكومية وقرأ معلومات عن حسابك.

.07 لا تضغط أبدًا على الروابط في الرسائل النصية. بينما قد يكون من الممكن أن تكون بعض الروابط غير ضارة، من الأفضل أن تكون حذرًا. ينطبق نفس الشيء على المرفقات والروابط في رسائل البريد الإلكتروني ما لم تكن متأكدًا من المرسل.

.08 امتنع تمامًا عن اتباع تعليمات أي متصل لم تطلب الاتصال به يطلب منك تنزيل تطبيق أو تثبيت برنامج يمنحهم الوصول إلى جهازك. أغلق الخط على الفور.

.09 تَجنّب تمامًا تسجيل الدخول إلى حساباتك الإلكترونية عبر الإنترنت من خلال رابط في بريد إلكتروني أو رسالة نصية. بدلًا من ذلك، أدخل عنوان الرابط URL الخاص بالشركة في متصفح الإنترنت أو استخدم تطبيقها الآمن للوصول إلى حسابك.

.10 قبل إجراء أي دفعة عبر الإنترنت، تحقق دائمًا من عنوان الرابط URL الخاص بالموقع (هل هو الموقع الرسمي؟)، وابحث عن طرق الدفع غير المعتادة والمعلومات المكتوبة بصياغة رديئة أو الناقصة في قسم "نبذة عنا" والشحن والإرجاع وغيرها من الأقسام الموجودة في أسفل الموقع.

إذا كنت في شك، قم بالبحث عبر الإنترنت عن طريق إدخال اسم المنظمة أو الموقع المعني وكلمة "احتيال".

هل تعتقد أنك تعرضت للاحتيال؟

أين تذهب للحصول على المساعدة

يمكن أن يتسبب التعرض للاحتيال في أضرار مالية وعاطفية، لذا من المهم طلب المساعدة والتصرف بسرعة. هناك عدة خطوات يمكنك اتخاذها:

1. اتصل بالمصرف على الفور لوقف أي معاملات أخرى من الحدوث.
2. اتصل بـ IDCARE، وهي خدمة دعم مجانية للأشخاص الذين تأثروا بالاحتيالات أو سرقة الهوية. اتصل على الرقم 160 595 1800 أو قم بزيارة موقع idcare.org
3. قم بتغيير كلمات المرور الخاصة بك على الفور وتأكد من أنها قوية.
4. قم بالإبلاغ عن الاحتيال إلى Scamwatch لتحذير الآخرين: scamwatch.gov.au/report-a-scam
5. احصل على الدعم لنفسك. إذا لم تشعر بالراحة في التحدث إلى الأصدقاء أو العائلة، فاتصل بـ Lifeline أو Beyond Blue للدردشة بسرية. وإذا فقدت مبلغًا كبيرًا من المال، تحدث إلى خط المساعدة الوطني للديون (National Debt Helpline).

Beyond Blue على الرقم 4636 22 1300 (على مدار الساعة طوال أيام الأسبوع) أو تفضل بزيارة beyondblue.org.au

Lifeline على الرقم 14 11 13 (على مدار الساعة طوال أيام الأسبوع) أو تفضل بزيارة lifeline.org.au

الخط الوطني للديون (National Debt Helpline) على الرقم 007 007 1800 (خلال أيام الأسبوع، من 9:30 صباحًا إلى 4:30 مساءً) أو تفضل بزيارة ndh.org.au

للمزيد من المعلومات

انقر على المربعات أدناه لاستكشاف:

كتيب عمليات الاحتيال هو أداة معترف بها دوليًا لمساعدتك على معرفة المزيد عن أنواع عمليات الاحتيال الشائعة وكيف يمكنك حماية نفسك منها.

تفضل بزيارة موقع Scamwatch الإلكتروني للبقاء على اطلاع بأحدث عمليات الاحتيال والنصائح حول كيفية حماية نفسك منها.

Australian Government | Be Connected
Every Australian online.

نبذة عن Be Connected (ابقَ على تواصل)

Be Connected هي مبادرة حكومية أسترالية تهدف إلى بناء المهارات الرقمية والثقة والسلامة على الإنترنت لكبار السن المقيمين في أستراليا من خلال دروس الحاسوب المجانية والدورات القصيرة عبر الإنترنت، والمزيد حول مجموعة من المواضيع. تتم إدارة موقع Be Connected ومحتوى التعلم بواسطة مفوض السلامة الإلكترونية.

Australian Government | National Anti-Scam Centre | SCAMWATCH

نبذة عن Scamwatch (رصد الاحتيالات)

يدير المركز الوطني لمكافحة الاحتيال Scamwatch الذي تم إنشاؤه لجعل أستراليا هدفًا أصعب للمحتالين. يزيد الوعي حول عمليات الاحتيال من خلال تعليم المجتمع كيفية التعرف على أساليب عمليات الاحتيال وتجنبها والإبلاغ عنها. يشارك مركز مكافحة عمليات الاحتيال المعلومات من تقارير عمليات الاحتيال ويعمل مع الحكومة وهيئات إنفاذ القانون والقطاع الخاص لتعطيل ومنع عمليات الاحتيال.