تجنُّب الإحتيالات

ما هو الاحتيال؟

الهدف من الاحتيال هو خداعك لتعطي أموالك أو تُفصح عن بياناتك الشخصية. تنجح الاحتيالات لأنها تبدو حقيقية وتلبي احتياجاتك ورغباتك.

والأشخاص الذين يقومون بهذه الاحتيالات (المحتالون) يتسمون بسعة الخيال والقدرة على التلاعب؛ وهم يعرفون كيف يضغطون على الأزرار الصحيحة للحصول على الرد الذي يريدونه.

تنشأ العديد من عمليات الاحتيال من خارج أستراليا وبمجرد إرسال المال إلى الخارج فإنه يستحيل استرداده فعلياً.

من هم المستهدفون؟

تستهدف عمليات الاحتيال الجميع بغض النظر عن الخلفية والعمر والدخل. وهي تأخذ أشكالاً عديدة وتصل إليك بطرق عديدة – بالبريد وعلى الإنترنت عبر البريد الإلكتروني والهاتف ومباشرة من الباب للباب.

ما هي أنواع الاحتيالات الموجودة؟

سوف يُجرب المحتالون عدداً من الطرق للحصول على أموالك ومعلوماتك الشخصية، وهذا يشمل:

- **اليانصيب والمراهنات على الخيول والمسابقات** – وسوف يتم إبلاغك في هذه العمليات الاحتيالية بأنك فزت بمسابقة أو يانصيب وسوف يحاولون خداعك لكي تفصح عن بياناتك البنكية والشخصية من أجل الحصول على الجائزة. تذكر أنك إذا لم تكن قد اشتركت من الأساس، فلا يمكنك أن تربح.
- **طلبات تحويل الأموال** – تنطوي هذه الاحتيالات عادة على مساعدة المحتال في تحويل الأموال من خلال حسابك، مقابل حصولك على رسوم. سوف يُطلب منك تقديم بياناتك البنكية والشخصية لإتمام المعاملة، لكن لن يتم إيداع الأموال في حسابك ويكون المحتال قد حصل على بياناتك.
- **الاحتيالات البنكية واحتيالات بطاقات الائتمان والحسابات على الإنترنت** – تهدف عمليات الاحتيال هذه إلى جعلك تكشف عن معلوماتك البنكية والشخصية من خلال إرسال رسائل بريد إلكتروني إليك، يقولون فيها غالباً أنها من بنكك، وتطالبك بتأكيد تفاصيل حسابك، بما في ذلك كلمة المرور.
- **سرقة الهوية** – هي نوع من الاحتيال ينطوي على سرقة هويتك من خلال الحصول على ما يكفي من بياناتك الشخصية بشكل يتيح انتحال شخصيتك عند التعامل مع المؤسسات المالية وخلافه.
- **احتيالات الهواتف الجوالة** – تتم عمليات الاحتيال هذه عادة من خلال الاتصال بك أو إرسال رسالة إلى هاتفك الجوال تعرض عليك خدمة ما. وعند الرد، فقد تشتري خدمة لا تريدها أو لا يمكنك إيقافها. ويؤدي هذا عادة إلى زيادة كبيرة في فواتير الهواتف الجوالة. احذر من عروض نغمات رنين الهاتف التي قد تؤدي بك أيضاً إلى الموافقة عن غير معرفة على استلام نغمات رنين إضافية لا تريدها، مما سوف يكلفك الكثير من المال.
- **الاحتيالات الهرمية** – تعتمد هذه الأنواع من الاحتيالات على تجنيد الأعضاء. سوف يدفع الأعضاء رسوماً للانضمام، مع دفع رسوم العضوية إلى عضو آخر الذي سيتلقى بدوره مالاً من البرنامج. وبمجرد أن يتوقف الأشخاص عن الانضمام، فسوف يتوقف إعطاء الأموال وإذا تم القبض عليك في ذلك الاحتيال الهرمي، فسوف تخسر أموالك.
- **فرص الاستثمار الذهبية** – سوف تعرض عليك هذه الاحتيالات عادة فرصاً استثمارية استناداً إلى معرفة داخلية سرية يمتلكها المحتالون، وكل ما عليك القيام به هو توفير بياناتك البنكية والشخصية للاشتراك. ويمكن أن يتاح لك أيضاً الوصول المبكر إلى معاشك التقاعدي أو خصوماتك أو إستردادات الضريبية الموعودة.
- **المقامرة على الإنترنت** – تنطوي هذه الاحتيالات عادة على الرهان على الخيول، لكنها قد تشمل أشكالاً أخرى من المقامرة، من خلال نظام حاسوبي. دفع بعض الأشخاص ما يصل إلى 20,000 دولار للنظام ليكتشفوا أنه لا يعمل وقد خسروا أموالهم.
- **الاحتيالات الصحية والطبية** - تعرض هذه الاحتيالات منتجات أو خدمات من شأنها أن تشفي مشكلاتك الصحية أو توفر علاجاً بسيطاً. وهذه الأدوية والعلاجات لن تحقق لك أية نتيجة.

كيف يمكنني تجنب الاحتيالات؟

اتبع هذه القواعد الذهبية لتجنب الوقوع ضحية للاحتيالات:

- لا ترد على العروض أو الصفقات أو الطلبات التي تطلب منك إعطاء بياناتك الشخصية. توقف، واستغرق الوقت للتحقق من الطلب أو العرض بشكل مستقل.
- لا ترسل أموالاً أو تعطي بيانات بطاقة الائتمان أو الحساب أو بيانات شخصية أخرى إلى أي شخص يقدم عروضاً أو طلبات لم تطلبها للحصول على معلوماتك.
- لا تعتمد على العبارات المبهرة: ابحث عن أدلة قوية من مصادر مستقلة (وليس تلك المقدمة مع العرض).
- لا ترد مطلقاً على أي من الطلبات غير المتوقعة للحصول على بياناتك الشخصية.
- احرص دائماً على الكتابة في عنوان الموقع الإلكتروني للبنك أو الشركة أو الهيئة محل اهتمامك للتأكد من أنك تسجل الدخول إلى موقع الويب الأصلي.
- لا تفتح رسائل بريد إلكتروني لم تطلبها.
- لا تنقر مطلقاً فوق رابط موجود في رسالة بريد إلكتروني لم تطلبها حيث إنه من المرجح أن يؤدي بك إلى موقع إلكتروني زائف مصمم لخداعك وجعلك تقدم بياناتك الشخصية.
- لا تستخدم مطلقاً أرقام الهاتف المقدمة في طلبات أو عروض لم تطلبها حيث من المرجح أن توصلك بأشخاص زائفين سوف يحاولون الإيقاع بك من خلال الأكاذيب.
- لا ترد على رسائل نصية لم تطلبها من أرقام لا تعرفها.
- احرص دائماً على البحث عن أرقام الهاتف في دليل مستقل عندما تريد التحقق مما إذا كان الطلب أو العرض حقيقياً.
- لا تتصل بأرقام تبدأ بـ 0055 أو 1900 ما لم تكن متأكداً من أنك تعرف مقدار التكلفة.

ماذا لو وقعت ضحية الاحتيال، ما هي الجهة التي يتعين عليَّ إبلاغها؟

إذا وقعت ضحية احتيال مصدره NSW أو إذا كنت تعرف اسم شركة أو متداول ضمن NSW، فيمكنك الإبلاغ عن الاحتيال بتقديم شكوى (Lodge a complaint) إلى مكتب التجارة العادلة بنيوساوث ويلز NSW Fair Trading على الإنترنت، أو الاتصال على الرقم 13 32 20 ، أو التبليغ شخصياً لدى أحد مراكز مكتب التجارة العادلة Fair Trading Centres التابعة لنا.

إذا كان الاحتيال مصدره من خارج NSW أو من دول أجنبية، فيمكنك الإبلاغ عنه من خلال SCAMwatch. SCAMwatch هو موقع إلكتروني تديره Australian Competition and Consumer Commission (ACCC) ويوفر معلومات إلى المستهلكين والشركات الصغيرة حول كيفية التعرف على الاحتيالات وتجنبها والإبلاغ عنها.

لمزيد من المعلومات، يرجى زيارة الموقع www.scamwatch.com.au

www.fairtrading.nsw.gov.au
Fair Trading enquiries على الرقم 13 32 20
المبرقة الهاتفية للصمّ 1300 723 404 (TTY)
خدمة المساعدة اللغوية 13 14 50