

احموا أنفسكم من العمليات الاحتيالية

تحتل الثقة والأمان صدارة أولوياتنا في بنك CommBank. لاحظنا في الآونة الأخيرة ازدياد عمليات الاحتيال المالي التي تستهدف العملاء حيث يقوم المُخادعون بالضغط عليهم أو خداعهم لإرسال الأموال لهم. وعمليات الاحتيال هذه قد تكون متطورة وتأخذ أشكالاً مختلفة. من المهم توخي الحذر واليقظة وإبلاغنا عن أي نشاط مشبوه. راجعوا الموقع الإلكتروني commbank.com.au/safe لمعرفة المزيد حول طرق حماية أنفسكم والإبلاغ عن عملية احتيال.

عملية المصادقة والتحقق

- أكملوا عملية التحقق الأمني في تطبيق CommBank.
- شغلوا ميزة المصادقة متعددة العوامل التي توفر عامل حماية إضافي لإثبات هويتكم.
- استخدموا ميزة CallerCheck للتحقق من هوية المتصلين الذين يزعمون أنهم من البنك.
- استخدموا ميزة CustomerCheck في الفرع لكي تؤكّدوا هويتكم لموظفينا.
- ستُحدّركم ميزة NameCheck في حال كانت تفاصيل الحساب لا تبدو صحيحة عند الدفع للمرة الأولى.

كلمة المرور ومعلوماتكم الشخصية

- لا تعطوا أبداً كلمات المرور أو أرقام التعريف الشخصية (PIN) لأي شخص آخر، وتوخّوا الحذر عند مشاركة المعلومات الشخصية.
- لا تعطوا أبداً رمز NetCode لأي شخص حتى لموظفي بنك CommBank.
- يمكنكم تغيير كلمة المرور لحسابكم مع البنك عبر بوابة NetBank الإلكترونية وتطبيق CommBank في أي وقت.
- استخدموا كلمات مرور قوية وغَيروها بانتظام. يُرجى زيارة الموقع الإلكتروني commbank.com.au/password-security للاطلاع على نصائحنا حول إنشاء كلمة مرور قوية.

أمن الجهاز وعملية الدفع

- حدّثوا برنامج مكافحة الفيروسات باستمرار لحماية جهاز الكمبيوتر من المخاطر الشائعة.
- ادفعوا باستخدام طرق الدفع الآمنة كتمرير البطاقة فوق القارئ أو إدخالها فيه.
- لا تشاركوا الأجهزة التي تحتوي على محفظتكم الرقمية مع أي شخص آخر.

البريد الإلكتروني والرسائل الهاتفية وتصفح الإنترنت

- لا تنقروا أبداً على الروابط الإلكترونية في رسائل البريد الإلكتروني أو الرسائل الهاتفية المشبوهة.
- إذا راودتكم الشكوك حول رسالة ما، فتكلّموا عنها مع شخص تثقون به أو اتصلوا بالمنظمة مباشرة من خلال وسائل الاتصال الرسمية الخاصة بها.
- أقفلوا الخط إذا سمعتم رسالة مُسجّلة أو مشبوهة أو تهديدية من أطراف ثالثة.
- توخّوا الحذر عند التعامل مع أشخاص ومؤسسات لا تعرفونها عبر وسائل التواصل الاجتماعي والمنصات عبر الإنترنت.

توقّفوا. تحققوا. لا تردّوا.

لا تردّوا. هل الرسالة تبدو مُريبة؟ إذا راودتكم الشكوك فإن أفضل شيء يمكنكم فعله هو التوقّف، وأخذ نفس عميق. **تحقّقوا.** اسألوا شخصاً تثقون به أو اتصلوا بالمنظمة مباشرة من خلال وسائل الاتصال الرسمية الخاصة بها. **لا تردّوا.** أقفلوا الخط في وجه المتصل أو احذفوا رسالة البريد الإلكتروني أو احظروا رقم الهاتف. غيِّروا كلمات المرور.

إن كنتم تعتقدون أنكم وقعتم ضحية عملية احتيال، اتصلوا ببنك CommBank على الفور على الرقم 13 22 21، أو على الرقم 61 2 9999 3283 إن كنتم خارج أستراليا.

إذا كانت لغتكم الإنجليزية ضعيفة، يمكنكم استخدام خدمة الترجمة الخطية والشفهية المجانية التي تقدّمها الحكومة لمساعدتكم على التواصل معنا، وهي تقدّم خدمات الترجمة بأكثر من 150 لغة. يمكننا ترتيب هذه الخدمة عندما تتصلون بنا أو عندما تزورونا في الفرع.

يجب عليكم معرفة ما يلي: نحن لن نرسل إليكم أبداً رسالة عبر البريد الإلكتروني أو رسالة هاتفية تطلب فيها معلومات مصرفية كرقم العميل NetBank أو كلمة المرور أو رمز NetCode، كما أننا لن نرسل إليكم أبداً رابطاً لتسجيل الدخول مباشرة من البريد الإلكتروني أو الرسالة الهاتفية. استخدموا دائماً متصفح الإنترنت لزيارة موقعنا commbank.com.au من خلال كتابته في شريط العنوان أو استخدموا تطبيق CommBank للدخول إلى الخدمات المصرفية بشكل آمن. إذا وصلكم رسالة من CommBank تبدو مُريبة، أرسلوها إلينا إلى العنوان التالي hoax@cba.com.au واحذفوها مباشرة بعد ذلك. Commonwealth Bank of Australia (بنك كومونولث أستراليا) رقم العمل التجاري الأسترالي 48 123 123 124 ورقم ترخيص الخدمات المالية الأسترالية ورخصة الائتمان الأسترالية 234945.



معلومات مهمة حول عمليات الاحتيال الشائعة



بريد المصلحة التجارية الإلكتروني الذي تعرّض للاختراق

قد يستهدف المحتالون المصالح التجارية من خلال إرسال رسائل عبر البريد الإلكتروني من عنوان اخترقوه، أو قد يرسلون رسائل تبدو وكأنها موجهة من شخص تثقون به كالمساعد أو العميل أو المحامي أو المدير أو الجهة الموردة.

إليك بعض النصائح لحماية أنفسكم:

- قبل أن تدفعوا للمرة الأولى أو في حال تغيّرت تفاصيل الدفع، اتصلوا بالمنظمة على رقم الهاتف الرسمي الخاص بها لتأكيد هذه التفاصيل أولاً.
- استخدموا ميزة NameCheck عند الدفع لمعرفة ما إذا كان اسم الحساب يتطابق مع رقم BSB (البنك-الولاية-الفرع) ورقم الحساب المحدّد.
- درّبوا الموظفين لكي يتعرّفوا على عمليات التصيد الاحتيالية والإبلاغ عنها.



عمليات التصيد الاحتيالية عبر البريد الإلكتروني ورسائل الهاتف

يرسل المحتالون رسائل إلى بريدكم الإلكتروني أو إلى هاتفكم قد تتضمن رابطاً يوجّهكم إلى موقع إلكتروني احتيالي أو تطلب منكم معلومات شخصية حسّاسة.

إليك بعض النصائح لحماية أنفسكم:

- لا تنقروا أبداً على الروابط الإلكترونية في رسائل البريد الإلكتروني أو الرسائل الهاتفية المشبوهة.
- يمكنكم التأكد من صحة الرسالة عن طريق الاتصال بالمنظمة مباشرة وذلك باستخدام وسائل الاتصال الرسمية الخاصة بها.
- بلّغوا عن أي رسائل مشبوهة موجهة من CommBank إلى hoax@cba.com.au.

حيل الاستثمار (تتضمّن العملات الرقمية المُشفّرة)



يعمل المحتالون على إغراء الأفراد من خلال قطع وعود عليهم بتحقيق عوائد مالية عالية، وغالباً ما تتم هذه العمليات باستخدام العملات الرقمية المُشفّرة أو الفرص الاستثمارية الأخرى. قد يحاول المحتالون الاتصال بكم عبر مكالمات هاتفية أو رسالة إلى البريد الإلكتروني أو من خلال منصات التواصل الاجتماعي.

إليك بعض النصائح لحماية أنفسكم:

- إذا بدا الأمر جيداً لدرجة قد يصعب تصديقها فهو على الأغلب كذلك.
- احذروا من العروض التي لم تطلبوها وإلحاح الأشخاص لكي تستثمروا أو تتصرّفوا بسرعة.
- تحققوا من شرعية الشركة أو الوسيط من خلال استخدام الموقع الإلكتروني لهيئة الأوراق المالية والاستثمارات الأسترالية (ASIC).

حيل التحكم عن بعد



عندما يتصل بكم محتال يدّعي أنه من شركة أو مؤسسة تعرفونها وتثقون بها ويحاول الوصول إلى حساباتكم أو جهازكم.

إليك بعض النصائح لحماية أنفسكم:

- لا تنزّلوا أبداً برنامجاً يخوّل متصلاً من طرف ثالث الوصول عن بعد إلى جهازكم بناءً على طلبه أو بضغط منه.
- يمكنكم دائماً معاودة الاتصال بالمؤسسة باستخدام تفاصيل الاتصال المشروعة والتي يمكنكم العثور عليها على موقعها الإلكتروني الرسمي.
- إذا تلقيتكم مكالمات من شخص يدّعي أنه من بنك CommBank، يمكنكم دائماً أن تطلبوا منا تأكيد شرعية المكالمات عبر ميزة CallerCheck الموجودة في التطبيق.



معلومات مهمة حول العمليات الاحتيالية الشائعة



حيل فرص التوظيف

تُعرض عليكم وظيفة تتطلب جهداً قليلاً أو لا تتطلب أي جهد على الإطلاق غير أنها ستحقق لكم مكاسب مالية عالية، أو تُعدكم بكسب المال بسرعة.

إليك بعض النصائح لحماية أنفسكم:

- تحققوا من الشركة والعرض من خلال القنوات الرسمية، وابحثوا عنها عبر الإنترنت للتأكد من شرعيتها وما إذا كانت تتاجر في الوقت الحالي.
- احذروا من العمل الذي يُعرض عليكم عبر وسائل التواصل الاجتماعي أو من خلال وسائل الدردشة المشفرة أو رسائل البريد الإلكتروني أو الهاتف أو الرسائل الواردة من أشخاص لم تقابلوهم من قبل أو شركات لا تعرفونها.
- إن الشركات الشرعية لا تطلب منكم أبداً دفع دفعة مقدماً ولا تستخدم معلوماتكم المصرفية الشخصية لتسهيل الحصول على أموال الشركة أو للتجارة.



التهديدات والعقوبات

ينتحل المحتالون صفة السلطات أو المؤسسات الموثوقة لابتزاز الأموال من خلال التهديد بفرض غرامات أو اتخاذ إجراءات قانونية.

إليك بعض النصائح لحماية أنفسكم:

- اقفلوا الخط إذا ما هددكم المتصل واتصلوا بالمؤسسة مباشرة.
- إن المؤسسة الشرعية لن تطلب منكم أبداً الدفع بطرق غير مُعتادة من خلال البطاقات الشرائية أو بطاقات المتاجر أو قسائم iTunes أو التحويلات البنكية أو عملات بيت كوين.
- اتصلوا بالشرطة إذا كنتم خائفين على سلامتكم.

حيل إقامة العلاقات



يُنشئ المحتالون صفحات شخصية زائفة بهدف تكوين علاقات مع الضحايا لدفعهم لإرسال الأموال أو المعلومات الشخصية.

إليك بعض النصائح لحماية أنفسكم:

- لا ترسلوا أبداً الأموال أو تشاركوا كلمات المرور أو تفاصيل بطاقة الائتمان أو الحساب المصرفي مع أي شخص لا تثقون به.
- ابحثوا عن شريككم المُحتمل عبر الإنترنت من خلال Google أو تطبيقات التواصل الاجتماعي. أجروا بحثاً عكسياً عن الصور لمعرفة ما إذا كان شخص آخر يمتلك الصور التي تم إرسالها إليكم.
- تحدثوا إلى أفراد العائلة والأصدقاء حول علاقتكم عبر الإنترنت، فقد يتمكنوا من تقديم وجهة نظر مختلفة ويتعرفوا على إشارات تحذيرية لربما لم تلاحظونها.

حيل التسوق عبر الإنترنت



يُنشئ المحتالون متاجر أو إعلانات عبر الإنترنت لجذب المتسوقين لشراء منتجات غير موجودة أو زائفة.

إليك بعض النصائح لحماية أنفسكم:

- لا تتسوقوا إلا عبر المواقع الإلكترونية الآمنة والتي تتمتع بسمعة جيدة وتوحيّوا الحذر من أي عرض جيد لدرجة قد يصعب تصديقها.
- استخدموا طرق الدفع الآمنة وتجنبوا التحويلات المباشرة للبائعين.
- لا تتسرعوا أو تشعروا بالضغط للشراء لأن "العرض محدود" أو بسبب بدء "العدّ التنازلي" لنهاية التنزيلات.