اطلاعات مهم برای مشتریان درباره کلاهبرداری ها.

مشتری گرامی،

اعتماد و امنیت برای ما در اولویت است.

گاه و بیگاه، شاهد مواردی هستیم که یک مشتری از جانب شخص ثالثی تحت فشار بوده، به زور مجبور شده یا مورد سواستفاده قرار می گیرد تا یک تبادل مالی انجام بدهد. برخی اوقات خلافکاران همراه مشتری به شعبه می آیند یا دستورالعملی را پشت تلفن در اختیار او قرار می دهند تا اطمینان بیابند که تبادل مالی انجام شده است.

این کلاهبرداری ها می توانند به اشکال مختلف و بسیار پیچیده باشند. مشتری ها باید آگاه و هوشیار باشند و هر گونه فعالیت مشکوک را گزارش کنند.

علائم هشداردهنده و نشانه های خطر.

کلاهبرداران اغلب حس ضرورت را ایجاد می کنند. آنها این کار را با فشار بر مشتریان از طریق سررسید کوتاه مدت، موارد اضطراری دروغین، تهدیدات به اقدام قانونی یا تظاهر به نماینده بودن از سوی نیروهای پلیس، بانک یا یک اداره دولتی انجام می دهند.

انواع کلاهبرداری ها.

کلاهبرداری های رایج شامل این موارد می شوند:

- فناوری اطلاعاتی و دسترسی از راه دور (به کامپیوتر، موبایل یا سایر وسایل الکترونیکی تان)
- سرمایه گذاری
- دوستیابی و رابطه عاشقانه
- پول غیر منتظره و برنده شدن
- سازمان های خیریه جعلی
- خرید یا فروش
- کار و اشتغال
- تهدیدات و اخاذی
- تلاش های دیگر برای دستیابی به اطلاعات شخصی تان

ما هرگز از شما PIN، کلمه عبور یا کد اس ام اس نت بانک تان را از طریق تلفن یا ایمیل نمی پرسیم. اگر تماسی از فردی دریافت کردید که ادعا می کند از بانک CommBank است و این اطلاعات را از شما می خواهد یا فردی با شما تماس گرفت که مطمئن نیستید واقعی است، آن کار را انجام ندهید و با ما تماس بگیرید تا پیش از هر اقدامی، تائید شود.

محل یافتن اطلاعات بیشتر.

تعدادی منابع آنلاین جهت آموزش و کسب اطلاعات بیشتر در مورد کلاهبرداری های در حال حاضر وجود دارد از جمله www.commbank.com.au/scams و www.scamwatch.gov.au

همچنین می توانید در وب سایت بانک، 'Savvy & Safe' را برای یک نسخه از راهنمای ما جستجو کنید که جهت کمک به مشتریان مسن تر تهیه شده است تا انها سواستفاده از افراد مسن، کلاهبرداری و تقلب را درک کرده و از آنها اجتناب کنند. اگر نیاز به کمک برای دسترسی به هر یک از منابع فوق دارید، لطفا به یکی از شعبات بانک CommBank مراجعه کنید.

ما اینجا برای کمک به شما هستیم.

اگر متوجه هرگونه تبادل غیرمجاز یا رفتار غیرمعمول در حساب های بانکی تان شدید، یا نیاز به تایید حقیقی بودن تماس از بانک CommBank را دارید، می توانید با ما هر زمانی با شماره **13 2221 (3283 9999 2 61+ برای تماس از خارج از استرالیا) تماس بگیرید**، یا **به شعبه محلی تان مراجعه کنید.**

همچنین می توانید با تیم کلاهبرداری بانک به شماره 1800023919 تماس بگیرید. گزینه 2 را انتخاب کنید، سپس گزینه 1 (دوشنبه تا جمعه 8 صبح تا 7 بعد از ظهر، شنبه تا یکشنبه 8 صبح تا 4 بعد از ظهر به وقت سیدنی).

اگر نیاز به حمایت روحی و روانی دارید، لطفا با خدمات حمایت از مشتریان ما به شماره 1300360793 تماس گرفته و وقت ملاقات بگیرید.
خدمات حمایت از مشتریان، خدمات مشاوره تلفنی کوتاه مدت و محرمانه است که برای مشتریان بانک کامنولت و بانک وست (Bankwest) مستقر در استرالیا، موجود می باشد.

با سپاس
CommBank

برای خلاصه ای از انواع کلاهبرداری های رایج، لطفا به صفحه 2 مراجعه کنید.

کلاهبرداری های مربوط به فناوری اطلاعاتی و دسترسی از راه دور

ممکن است:

- تماس تلفنی ناگهانی از فردی دریافت کنید که ادعا می کند از یک موسسه مالی، شرکت مخابراتی یا مرکز پشتیبانی فناوری اطلاعات است. آنها ممکن است جزئیات شما را از قبل داشته باشند.
- از شما درخواست شود که برنامه ای را نصب کنید یا کد خاصی را بخوانید. این تکنیک اغلب برای دادن دسترسی از راه دور بکار می رود تا فرد کلاهبردار بتواند وسیله شما را ببیند و کنترل کند.
- با شما تماس گرفته شود تا در دستگیری خلافکاران کمک کنید.

کلاهبرداری های مربوط به سرمایه گذاری و کار

ممکن است:

- به شما موارد سرمایه گذاری مانند سهام یا ارز دیجیتال پیشنهاد شود که نرخ بسیار خوبی را برای سود سرمایه گذاری تان تضمین می کند.
- فرصت کاری به شما پیشنهاد شود که خوب تراز آنی است که بتواند حقیقتش داشته باشد. این مورد ممکن است شامل دریافت وجوهی از یک کسب و کار یا "مشتریان" شان و انتقال آن وجوه به حساب دیگر باشد.
- از شما درخواست شود که سایرین را برای کار یا سرمایه گذاری بکار بگیرید.

کلاهبرداری های مربوط به روابط

ممکن است:

- شما رابطه با فردی برقرار کرده اید که از طریق دوست یابی آنلاین یا رسانه اجتماعی با او آشنا شده اید و در حال حاضر این فرد درخواست پول فوری می کند.
- از شما درخواست بشود تا برای انتقال های بین المللی پول (IMT) ثبت نام کنید و دستورالعمل های مربوط به نحوه انتقال پول به خارج از استرالیا داده شود. توضیحات IMT ممکن است با جزئیات دریافت کننده مورد نظر هماهنگ نباشد.

کلاهبرداری های غیر منتظره مربوط به پول

ممکن است:

- نامه، ایمیل، تماس تلفنی یا نوشته ای را روی کامپیوتر خود در مورد برنده شدن لاتاری، ارثیه یا موردی مشابه دریافت کنید.
- به شما گفته شود که شما مستحق دریافت پولی هستید اما برای آزاد کردن پول، ابتدا باید پولی را مانند هزینه های قانونی، پرداخت کنید.

کلاهبرداری همراه با تهدید و مجازات

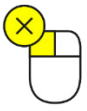
ممکن است:

- فردی با شما تماس بگیرد و ادعا کند که از کارکنان کلاهبرداری بانک، پلیس، اداره مهاجرت یا اداره مالیات است.
- به شما گفته شود که قبوض/ جریمه های پرداخت نشده یا مالیات معوقه دارید.
- شما را با مجازاتی مانند زندان یا اخراج از کشور تهدید کنند در صورتیکه پول را پرداخت نکنید.

صورتحساب های ساختگی / کلاهبرداری های مربوط به ایمیل به خطر افتاده

شما ممکن است:

- نامه یا صورتحسابی را برای پرداخت به یک حساب جدید برای یک تامین کننده تثبیت شده دریافت کنید.
- نامه ای از تامین کننده تان دریافت کنید که آنها هرگز پرداختی را دریافت نکرده اند.



خرید/ فروش

شما ممکن است:

- کالاهایی را آنلاین خریداری کنید ولی پس از پرداخت کالا را دریافت نکنید.
- توله سگ/ حیوان خانگی را آنلاین خریداری کنید ولی پس از پرداخت حیوان را دریافت نکنید.

سازمان های خیریه قلابی

ممکن است:

- توسط شخصی با شما تماس گرفته شود که ادعا کند از یک سازمان خیریه می باشد یا نیاز به پول برای کمک به کودکی دارد که بیمار است.