معلومات مهم در مورد کلاهبرداری برای مشتریان.

مشتریان محترم

اعتماد و امنیت برای ما یک اولویت است.

بعضی اوقات مواردی را می بینیم که یک مشتری تحت فشار، اجبار یا فریب شخص ثالث یک معامله مالی را انجام داده است. گاهگاهی مجرمان مشتری را تا به یک شعبه همراهی می کنند یا از طریق تلفون دستورالعمل هایی را می دهند تا از انجام یک معامله مالی اطمینان یابند.

این کلاهبرداری ها به اشکال مختلفی انجام می شود و می تواند بسیار پیچیده باشد. مشتریان باید هوشیار و آگاه باشند و هرگونه فعالیت مشکوک را گزارش دهند.

علائم هشدار دهنده و بیرق های سرخ.

کلاهبرداران اغلب سعی می کنند احساس فوریت ایجاد کنند. آنها این کار را با وارد کردن فشار بر مشتری با دادن مهلت های کوتاه مدت، موارد عاجل کاذب، تهدید به اقدام قانونی یا معرفی کردن خود به عنوان نماینده نیروی پولیس، یک بانک یا یک اداره دولتی، انجام می دهند.

انواع کلاهبرداری ها.

کلاهبرداری های رایج عبارتند از:

- فناوری معلوماتی و دسترسی از راه دور (به کمپیوتر، تلفون موبایل یا سایر دستگاه های الکترونیکی شما)
- سرمایه گذاری
- دوستیابی و روابط عاشقانه
- پول یا برنده شدن های غیر منتظره
- موسسات خیریه جعلی
- خرید یا فروش
- کار و به کار گماشتن
- تهدیدها و اخاذی
- کوشش های دیگر برای به دست آوردن معلومات شخصی شما

ما هرگز از طریق تلفون یا ایمیل از شما PIN، رمز عبور (password) یا کد پیام کوتاه (NetBank (NetBank SMS Code) نخواهیم خواست.
اگر تماسی از طرف کسی دریافت میکنید که ادعا میکند که از کمونولت بنک (CommBank) است و از شما این معلومات را درخواست میکند یا هر کسی که در صداقت و واقعی بودن او مطمئن نیستید، پیش از هر گونه اقدام به ما زنگ بزنید.

از کجا معلومات بیشتر بدست آورید.

تعدادی از منابع آنلاین با آموزش و معلومات بیشتر درباره کلاهبرداری های رایج وجود دارد، از جمله
www.commbank.com.au/scams و
www.scamwatch.gov.au.

همچنین میتوانید در وب سایت CommBank برای 'Savvy & Safe' یک نسخه از راهنمای ما را که جهت کمک به مشتریان سالخورده طراحی شده است تا آنان بدرفتاری با سالخوردگان، کلاه برداری و فریب را بدانند و از انها اجتناب کنند. اگر در دسترسی به هر یک از منابع فوق نیاز به کمک دارید، لطفاً به یک شعبهٔ CommBank مراجعه کنید.

ما اینجا هستیم که کمک کنیم.

اگر معاملات غیر مجاز یا رفتار غیرعادی را در حساب بانکی خود شناسایی کردید یا اگر بخواهید معلوم کنید که آیا یک تماس از CommBank حقیقی است یانه در هر وقت می توانید به شمارهٔ **13 2221 (به شمارهٔ 3283 9999 2 61+ از خارج از استرالیا) زنگ بزنید یا به یکی از شعبات محلی بانک مراجعه کنید.**

همچنین می توانید از طریق شماره 919 023 1800با تیم کلاهبرداری بانک تماس بگیرید. گزینه 2 و سپس گزینه 1 را انتخاب کنید (دوشنبه تا جمعه 8 صبح - 7 عصر ، شنبه تا یکشنبه 8 صبح - 4 عصر به وقت سیدنی) .

اگر به پشتیبانی عاطفی و روانی نیاز دارید ، لطفاً با شماره تلفون 793 360 1300 با خدمات پشتیبانی مشتری (Customer Support Service) تماس گرفته و وقت بگیرید.
خدمات پشتیبانی مشتری یک خدمات مشاوره تلفونی کوتاه مدت و محرمانه است که در اختیار مشتریان کمونولت بانک و Bankwest مستقر در استرالیا قرار دارد.

با تشکر
CommBank

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

کلاهبرداری فناوری معلومات و دسترسی از راه دور

شما ممکن است:

- از کسی که ادعا می کند از یک موسسه مالی، شرکت مخابرات یا مرکز مشاوره فناوری اطلاعات است ، یک تماس ناخواسته دریافت کنید. آنها ممکن است از قبل مشخصات شما را داشته باشند.
- از شما خواسته می شود یک برنامه ای را نصب کنید یا کد خاصی را بخوانید. از این روش اغلب برای فراهم کردن دسترسی از راه دور استفاده می شود تا کلاهبردار دستگاه شما را ببیند و کنترل کند.
- با شما تماس گرفته می شود که در گرفتن مجرمان کمک کنید.

کلاهبرداری سرمایه گذاری و شغلی

به شما ممکن است:

- محصولات سرمایه گذاری مانند سهام یا ارز رمزگذاری شده (cryptocurrency) که یک میزان بسیار خوبی نفع را برای سرمایهٔ شما تضمین می کنند، پیشنهاد شود.
- فرصتی برای کار پیشنهاد شود که آنقدر خوب است که نمی تواند واقعی باشد. این ممکن است شامل دریافت پول از کسب و کار یا "مشتریان" آنها و انتقال این پول به افراد بعدی باشد.
- خواسته می شود که دیگران را در شغل یا سرمایه گذاری جذب کنید.

کلاهبرداری در رابطه

شما ممکن است:

- با کسی که از طریق ملاقات عشقی آنلاین یا رسانه های اجتماعی ملاقات کرده و رابطه برقرار کرده اید اکنون به صورت عاجل پول می خواهد.
- از شما خواسته می شود برای انتقال بین المللی پول (IMT) ثبت نام کنید و در مورد چگونگی ارسال پول به خارج از کشور هدایت داده می شوید. توضیحات IMT ممکن است با مشخصات گیرنده مورد نظر مطابقت نداشته باشد.

کلاهبرداری پول غیر منتظره

شما ممکن است:

- یک نامه، ایمیل ، زنگ یا بطور ناگهانی یک پیام (up-pop) در کمپیوتر خود درباره برنده شدن در قرعه کشی، ارث بردن یا موارد مشابه دریافت کنید.
- به شما گفته میشود که شما مستحق پولی هستید اما باید ابتدا پول آزاد سازی، بطور مثال فیس قانونی آن را بپردازید.

کلاهبرداری تهدید و مجازات

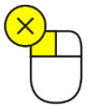
شما ممکن است:

- کسی که ادعا می کند کارمند کلاهبرداری در بانک، پولیس، ادارهٔ مهاجرت یا مالیات (ATO) است با شما تماس می گیرد.
- به شما گفته می شود که بل/ جریمه پرداخت نشده یا مالیات از موعد گذشته دارید.
- به مجازاتی تهدید شوید که اگر پرداخت نکنید زندانی یا از کشور اخراج می شوید.

کلاهبرداری بل های جعلی/ ایمیل به خطر افتاده

شما ممکن است:

- یک اطلاع یا بل دریافت می کنید که به یک تامین کننده شناخته شده از طریق یک حساب جدید پرداخت کنید.
- از تأمین کننده تان اخطار دریافت می کنید مبنی بر اینکه هرگز پرداختی از شما دریافت نکرده است.



خرید/ فروش

شما ممکن است:

- اجناسی را بصورت آنلاین خریداری کنید و پس از پرداخت پول اجناس را دریافت نکنید.
- یک توله سگ / حیوان خانگی را بصورت آنلاین خریداری کنید اما پس از پرداخت پول حیوان خانگی را دریافت نکنید.

موسسات خیریه جعلی

شما ممکن است:

- کسی با شما تماس می گیرد که ادعا میکند از یک موسسه خیریه است یا به پول نیاز دارد تا به یک طفلی که مریض است کمک کند.