

مصون ماندن در مقابل کلاهبرداری

اعتماد و مصونیت برای ما در CommBank اولویت اصلی است. ما شاهد موارد فزاینده ای از مشتریانی هستیم که توسط کلاهبرداران تحت فشار یا مورد فریب قرار میگیرند تا پول برایشان ارسال کنند. این کلاهبرداری ها می توانند پیچیده باشند و به اشکال مختلف ارائه شوند. مهم است که مراقب باشید و اگر چیزی بنظر درست نمی آید به ما اطلاع دهید. برای اطلاع بیشتر در مورد نحوه محافظت از خود و گزارش کلاهبرداری، به وبسایت commbank.com.au/safe مراجعه کنید.

احراز هویت و تایید

- باز سنجی امنیتی را در برنامه (اپ) CommBank تکمیل کنید.
- احراز هویت چند-عاملی را فعال کنید، که یک سنجش اضافی برای اثبات هویت شما اضافه می کند.
- از CallerCheck برای تأیید هویت تماس گیرنده که ادعا میکند از طرف بانک هست، استفاده کنید.
- از CustomerCheck در شعبه ها استفاده کنید تا هویت خود را پیش کارکنان ما اثبات کنید.
- اگر مشخصات حساب در اولین پرداخت به نظر درست نیاید، NameCheck به شما هشدار خواهد داد.

رمز عبور و اطلاعات شخصی

- هرگز رمزهای عبور یا PIN (پین) را به اشتراک نگذارید و هنگام اشتراک گذاری اطلاعات شخصی خود احتیاط کنید.
- هرگز NetCode خود را در اختیار کسی از جمله کارکنان CommBank قرار ندهید.
- هر زمان بخواهید، می توانید رمز عبور خود را در NetBank و اپ CommBank تغییر دهید.
- رمزهای عبور قوی درست کنید و به طور مرتب آنها را تغییر دهید. برای دسترسی به راهنمایی های ما در درست کردن رمز عبور، به commbank.com.au/password-security مراجعه کنید.

امنیت دستگاه و پرداخت

- نرم افزار آنتی ویروس را به روز نگه دارید و از رایانه خود در برابر تهدیدات رایج محافظت کنید.
- از روشهای پرداخت ایمن مانند تماس دادن کارت خود یا وارد کردن آن در دستگاه استفاده کنید.
- دستگاه هایی را که به کارت دیجیتال شما دسترسی دارند، به اشتراک نگذارید.

ایمیل، اس ام اس و آنلاین

- روی لینک های موجود در ایمیل ها یا پیامک های مشکوک کلیک نکنید.
- اگر در مورد پیامی مطمئن نیستید، آن را با فردی که به او اعتماد دارید در میان بگذارید یا مستقیماً با سازمان مربوطه از طریق مشخصات رسمی شان تماس بگیرید.
- تماس های تلفنی خودکار، مشکوک یا تهدیدآمیز اشخاص را قطع کنید.
- مراقب تماسهای ناشناس در رسانه های اجتماعی و پلتفرم های آنلاین باشید.

ادامه ندهید. بررسی کنید. امتناع کنید.

ادامه ندهید. چیزی به نظر غیر عادی می رسد؟ اگر شک دارید، بهترین کار این است که ادامه ندهید. نفسی تازه کنید. **بررسی کنید.** از شخصی که به او اعتماد دارید پرسید یا مستقیماً با سازمانها با استفاده از مشخصات رسمی شان تماس بگیرید. **امتناع کنید.** تلفن تماس گیرنده را قطع کنید، ایمیل را حذف کنید، شماره تلفن را مسدود کنید، رمزهای عبور خود را تغییر دهید.

اگر فکر میکنید قربانی کلاهبرداری شده اید، فوراً با CommBank با شماره 132221 یا 6129999 3283+ از خارج از کشور تماس بگیرید.

اگر انگلیسی زبان اول شما نیست، خدمات ترجمه رایگان دولتی می تواند به شما کمک کند تا با ما ارتباط برقرار کنید. این سرویس با بیش از 150 زبان در دسترس است. زمانی که با ما تماس میگیرید یا به شعبه ما مراجعه میکنید، می توانیم این خدمات را فراهم کنیم.

چیزهایی که باید بدانید: ما هرگز برای شما ایمیل یا پیامکی ارسال نمی کنیم که اطلاعات بانکی مانند شناسه مشتری NetBank، رمز عبور یا NetCode شما را بخواهد، یا لینک برای ورود مستقیم از طریق ایمیل یا پیامک بفرستد. همیشه commbank.com.au را در مرورگر تایپ کنید یا از اپ CommBank برای دسترسی ایمن به بانک خود استفاده کنید. اگر چیزی از طرف CommBank مشکوک به نظر می رسد، آن را به hoax@cba.com.au ارسال کرده و بعد حذف کنید. بانک Commonwealth (کامن ولت) استرالیا ABN 48 123 123 124 AFSL و مجوز اعتباری استرالیا 234945.

اطلاعات مهم در مورد کلاهبرداری های رایج



در خطر افتادن امنیت ایمیل کسب و کار

کلاهبرداران می توانند کسب و کارها را از طریق ایمیل های لو رفته دیگران یا ایمیل هایی که به نظر می رسد از یک شخص قابل اعتماد مانند: دستیار، مشتری، وکیل، مدیر یا تهیه کننده شما ارسال شده اند، هدف قرار دهند.

نکاتی برای محافظت خود:

- قبل از انجام اولین پرداخت یا تغییر مشخصات پرداخت، با شماره تماس رسمی سازمان ها ارتباط بگیرید تا ابتدا مشخصات را تأیید کنند.
- هنگام پرداخت، از امکانات NameCheck استفاده کنید تا ببینید آیا نام حساب با BSB و شماره حساب داده شده مطابقت دارد یا خیر.
- به کارکنان خود آموزش دهید تا اقدامات فیشینگ را شناسایی و گزارش کنند.



فیشینگ و اسمیشینگ

کلاهبرداران از ایمیل های فریبنده یا پیامک های استفاده میکنند که ممکن است حاوی لینکی باشند که شما را به یک وب سایت تقلبی هدایت کنند یا اطلاعات شخصی حساس شما را درخواست کنند.

نکاتی برای محافظت خود:

- روی لینک های موجود در ایمیل ها یا پیامک های مشکوک کلیک نکنید.
- میتوانید درستی یک پیام را با تماس مستقیم با سازمان ها، با استفاده از روشهای تماس رسمی موجود، تأیید اعتبار کنید.
- هرگونه پیام مشکوک از CommBank را به hoax@cba.com.au گزارش دهید.

سرمایه گذاری (از جمله رمزارز)



کلاهبرداران افراد را با وعده سرمایه گذاری با بازدهی بالا جذب میکنند، که اغلب شامل فرصتهای سرمایه گذاری رمزارز یا سایر سرمایه گذاری ها می باشد. کلاهبرداران ممکن است سعی کنند از طریق تلفن، ایمیل یا پلتفرم های رسانه های اجتماعی با شما تماس بگیرند.

نکاتی برای محافظت خود:

- اگر حس میکنید موردی خوبتر از آن است که بتواند واقعی باشد، احتمالاً همینطور هست.
- مراقب پیشنهادات ناخواسته و فشار برای سرمایه گذاری یا اقدام سریع باشید.
- ابتدا مشروعیت شرکت یا کارگزار را در وب سایت ASIC بررسی کنید.

دسترسی از راه دور



این مربوط به موردی میشود که کلاهبردار با شما تماس می گیرد و سعی می کند به حساب ها یا دستگاه شما دسترسی پیدا کند و وانمود می کند که از یک شرکت یا سازمان قابل اعتماد است.

نکاتی برای محافظت خود:

- هرگز نرم افزار دسترسی از راه دور را به درخواست یا تحت فشار شخص تماس گیرنده دانلود نکنید.
- همیشه میتوانید با سازمانها از طریق اطلاعات تماس شان که در وب سایت رسمی آنها یافت میشود، تماس بگیرید.
- اگر تماسی دریافت میکنید که ادعا میکند فردی از CommBank هستید، همیشه میتوانید از ما بخواهید که فرد را از طریق امکانات CallerCheck درون اپ تأیید کنیم.

اطلاعات مهم در مورد کلاهبرداری های رایج



فرصت شغلی

این مربوط به موردی میشود که ظاهراً یک پیشنهاد شغلی نیاز به تلاش اندک یا بدون هیچ تلاشی برای سود مالی بالا دارد، یا وعده کسب درآمد سریع را می دهد.

نکاتی برای محافظت خود:

- شرکت ها و پیشنهاد ها را از طریق کانال های رسمی تأیید اعتبار کنید، و در مورد شرکت ها تحقیق کنید تا مطمئن شوید که آنها قانونی بوده و در حال حاضر فعال هستند.
- مراقب پیشنهادهای شغلی از طریق رسانه های اجتماعی، چت رمزگذاری شده، ایمیل، تلفن یا نامه افرادی که ملاقات نکرده اید یا شرکت هایی که نمی شناسید، باشید.
- یک شرکت قانونی هرگز شما را ملزم به پیش پرداخت یا استفاده از اطلاعات بانکی شخصی خودتان برای تسهیل نقل و انتقال وجوه یا معامله با شرکت نمی کند.



تهدید و جریمه

کلاهبرداران با جعل هویت مسئولین یا سازمان های مورد اعتماد، از طریق تهدید به جریمه یا اقدام قانونی، اخاذی می کنند.

نکاتی برای محافظت خود:

- تلفن تماس گیرندگان تهدید کننده را قطع کنید و مستقیماً با سازمان تماس بگیرید.
- یک سازمان قانونی هرگز از شما نمی خواهد با روشهای غیرعادی مانند کارتهای هدیه یا کارت فروشگاه ها، کوپنهای iTunes، حواله های الکترونیکی یا بیت کوین پرداخت کنید.
- اگر نگران امنیت خود هستید، با خط تلفن police assistance (کمک پلیس) تماس بگیرید.

رابطه



کلاهبرداران برای ایجاد رابطه و فریب قربانیان برای ارسال پول یا اطلاعات شخصی، پروفایل های جعلی ایجاد می کنند.

نکاتی برای محافظت خود:

- هرگز پول نفرستید یا با کسی که به او اعتماد ندارید، رمزهای عبور، کارت اعتباری یا مشخصات حساب خود را به اشتراک نگذارید.
- از طریق Google یا برنامه های رسانه های اجتماعی، در مورد شریک زندگی بالقوه خود تحقیقات خود را بصورت آنلاین انجام دهید. از روش جستجوی معکوس عکس استفاده کنید تا معلوم شود که آیا شخص دیگری صاحب عکسهایی است که به شما ارسال شده اند.
- با خانواده و دوستان خود در مورد رابطه آنلاین خود صحبت کنید. آنها ممکن است بتوانند دیدگاهی بشما ارائه دهند و علائم هشدار دهنده ای را که ممکن است شما متوجه آنها نشده اید، تشخیص دهند.

خرید آنلاین



کلاهبرداران فروشگاه یا آگهی های آنلاین درست می کنند تا خریداران را به خرید محصولات غیرموجود یا جعلی ترغیب کنند.

نکاتی برای محافظت خود:

- فقط از وب سایت های معتبر و ایمن خرید کنید و مراقب هر پیشنهادی باشید که حس میکنید خبتر از آن است که بتواند واقعی باشد.
- از روش های پرداخت ایمن استفاده کنید و از انتقال مستقیم به فروشندگان خودداری کنید.
- عجله نکنید و تحت فشار 'پیشنهادهای محدود' یا 'شمارش معکوس' پایان فروش نباشید.