

درمان ماندن از فریبکاری ها

اعتماد و امنیت برای ما در CommBank بالاترین اولویت است. ما شاهد موارد فزاینده ای از مشتریانی هستیم که توسط فریبکاران تحت فشار قرار میگیرند یا فریب شان داده می شوند تا برایشان پول روان کنند. این فریبکاری ها می توانند پیچیده بوده و به اشکال مختلفی انجام شوند. مهم است که متوجه بوده و در صورتیکه چیزی درست به نظر نمی رسد به ما اطلاع دهید. برای کسب معلومات بیشتر راجع به نحوه محافظت از خودتان و راپور دادن یک فریبکاری، commbank.com.au/safe را بررسی کنید.

احراز هویت و تصدیق

- بررسی امنیتی را در برنامه کاربری CommBank تکمیل کنید.
- احراز هویت چند-عاملی را فعال کنید، که یک بررسی اضافی برای اثبات هویت تان اضافه می کند.
- از CallerCheck برای تأیید هویت تماس گیرنده هایی که ادعا می کنند از بانک هستند استفاده کنید.
- از CustomerCheck در شعبه استفاده کنید تا خودتان را به کارمندان ما شناسایی کنید.
- اگر جزئیات حساب در پرداخت اولین بار درست به نظر نرسد، NameCheck شما را رهنمایی خواهد کرد.

رمز-عبور و معلومات شخصی

- هرگز رمز-عبور یا PINs را به اشتراک نگذارید و هنگام اشتراک گذاری معلومات شخصی محتاط باشید.
- هرگز NetCode خود را در اختیار کسی حتی کارمندان CommBank قرار ندهید.
- می توانید رمز-عبور خود را در NetBank و برنامه کاربری CommBank هر وقتیکه خواسته باشید تغییر دهید.
- رمزهای-عبور قوی ایجاد کنید و به طور منظم آنها را تغییر دهید. برای راهنمایی های ما راجع به ایجاد رمز-عبور، به commbank.com.au/password-security مراجعه کنید.

امنیت دستگاه و پرداخت

- نرم افزار ضد-ویروس را تازه نگهداشته و از کمپیوتر خود در برابر تهدیدات رایج محافظت کنید.
- از روش های پرداخت امن مانند نزدیک کردن کارت یا وارد کردن کارت خود استفاده کنید.
- دستگاه هایی که به بکسک پول دیجیتال شما دسترسی دارند را به اشتراک نگذارید.

ایمیل، پیام کتبی و آنلاین

- روی پیوندهای موجود در ایمیل یا پیام های کتبی مشکوک کلیک نکنید.
- اگر راجع به پیامی مطمئن نیستید، آن را با شخصی که به آن اعتماد دارید در میان بگذارید یا مستقیماً از طریق جزئیات تماس رسمی با سازمان مربوطه تماس بگیرید.
- تماس های تلفونی خودکار، مشکوک یا تهدیدآمیز از سازمان های ثالث را قطع کنید.
- متوجه تماس های ناشناس در رسانه های اجتماعی و پلتفرم های آنلاین باشید.

توقف کنید. چیک کنید. قبول نکنید.

توقف کنید. آیا کدام چیزی غیر معمولی به نظر می رسد؟ اگر شک دارید، بهترین کار این است که توقف کنید. یک نفس بکشید. **چیک کنید.** از شخصی که به او اعتماد دارید پرسید یا مستقیماً با استفاده از جزئیات رسمی با سازمان مربوطه تماس بگیرید. **قبول نکنید.** تماس شان را قطع کنید، ایمیل را حذف نموده، و نمره های تلفون شان را بلاک کنید. رمزعبور خود را تبدیل کنید.

اگر فکر می کنید قربانی یک فریبکاری شده اید، فوراً با CommBank با نمره 132221، یا از خارج از کشور با نمره +61299993283 تماس بگیرید.

اگر انگلیسی زبان اول تان نیست، خدمات ترجمانی شفاهی و کتبی رایگان دولتی می تواند به شما کمک کند تا با ما ارتباط برقرار کنید. این خدمات به بیش از 150 لسان در دسترس است. وقتی با ما تماس می گیرید یا در شعبه به ما مراجعه می کنید، ما می توانیم این خدمات را ترتیب دهیم.

چیزهایی که باید بدانید: ما هرگز برای شما ایمیل یا پیام کتبی روان نمی کنیم که معلومات بانکی مانند کد شناسایی NetBank، رمز عبور یا NetCode شما را بخواهد؛ یا پیوندی برای ورود مستقیم از طریق ایمیل یا پیام کتبی روان نمی کنیم. همیشه commbank.com.au را در مرورگر تایپ کنید یا از برنامه کاربری 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 روان کرده و آن را حذف کنید. بانک Commonwealth استرالیا 123 124 123 48 ABN و AFSL و مجوز اعتبار استرالیا 234945.

معلومات مهم راجع به فریکاری های رایج



خطر ایمیل کسب و کار

فریکاران می توانند کسب و کارها را با ایمیل هایی از یک آدرس در معرض خطر یا ایمیل هایی که به نظر می رسد از یک مخاطب قابل اعتماد مانند: دستیار، مشتری، وکیل، مدیر یا تامین کننده شما ارسال شده اند، هدف قرار دهند.

نکاتی برای محافظت از خود تان:

- قبل از انجام اولین پرداخت یا تغییر دادن جزئیات پرداخت، با نمره تماس رسمی سازمان مربوطه تماس بگیرید تا ابتدا جزئیات را تصدیق کنید.
- هنگام پرداخت، از ویژگی NameCheck استفاده کنید تا ببینید آیا نام حساب کاربری با BSB و شماره حساب کاربری داده شده مطابقت دارد یا نه.
- به کارمندان تان آموزش دهید تا تلاش های دریافت معلومات غیر قانونی را شناسایی نموده و راپور دهند.

سرمایه گذاری



(از جمله ارزهای دیجیتال)

فریکاران افراد را با وعده بازدهی بالا جذب می کنند، که اکثراً شامل فرصت های سرمایه گذاری ارزهای دیجیتال و غیره می شود. فریکاران ممکن است تلاش کنند از طریق تلفون، ایمیل یا پلتفرم های رسانه های اجتماعی با شما تماس بگیرند.

نکاتی برای محافظت از خود تان:

- اگر بیش از حد خوب به نظر می رسد که درست باشد، احتمالاً همینگونه است.
- متوجه پیشنهادات ناخواسته و فشار برای سرمایه گذاری یا اقدام سریع باشید.
- ابتدا مشروعیت شرکت یا کارگزار را در وب سایت ASIC بررسی کنید.



تماس ها و ایمیل های فریبنده

فریکاران از ایمیل ها یا پیام های متنی فریبنده استفاده می کنند که ممکن است حاوی پیوندی باشد که شما را به یک وب سایت تقلبی هدایت می کند یا معلومات شخصی حساس را طلب می کند.

نکاتی برای محافظت از خود تان:

- روی پیوندهای موجود در ایمیل یا پیام های کتبی مشکوک کلیک نکنید.
- می توانید واقعی بودن یک پیام را با تماس مستقیم با سازمان، با استفاده از روش های تماس رسمی موجود، تأیید کنید.
- هرگونه پیام مشکوک از CommBank را به hoax@cba.com.au راپور دهید

دسترسی از راه دور



جایی که یک فریکار با شما تماس می گیرد و تلاش می کند به حساب ها یا دستگاه شما دسترسی پیدا کند و تظاهر می کند که از یک شرکت یا سازمان قابل اعتماد است.

نکاتی برای محافظت از خود تان:

- هرگز نرم افزار دسترسی از راه دور را به درخواست یا تحت فشار تماس گیرنده شخص ثالث دانلود نکنید.
- همیشه می توانید از طریق معلومات تماس قانونی که در وب سایت رسمی یک سازمان یافت می شود، با آنها تماس بگیرید.
- اگر تماسی دریافت می کنید که ادعا می کند شخصی از CommBank می باشد، همیشه می توانید از ما بخواهید که تماس را از طریق ویژگی CallerCheck داخل برنامه ای تأیید کنیم.

معلومات مهم راجع به فریکاری های رایج



فرصت کاری

جایی که به نظر می رسد یک پیشنهاد کاری نیاز به تلاش اندکی یا بدون هیچ تلاشی برای سود مالی بالا دارد، یا وعده کسب درآمد فوری را می دهد.

نکاتی برای محافظت از خود تان:

- شرکت و پیشنهاد را از طریق کانال های رسمی تأیید کنید، و راجع به شرکت تحقیق کنید تا مطمئن شوید که آنها قانونی هستند و فعلاً هم فعالیت دارند.
- متوجه پیشنهادهای کاری از طریق رسانه های اجتماعی، چت رمزگذاری شده، ایمیل، تلفون یا مکتوب افرادی که ملاقات نکرده اید یا شرکت هایی که نمی شناسید، باشید.
- یک شرکت قانونی هرگز شما را ملزم به پرداخت پیش پرداخت یا استفاده از معلومات بانکی شخصی تان برای تسهیل بودجه یا تجارت شرکت نمی کند.



تهدید و مجازات

فریکاران با جعل هویت مقامات یا سازمان های مورد اعتماد از طریق تهدید به جریمه یا اقدامات قانونی اخاذی می کنند.

نکاتی برای محافظت از خود تان:

- تلفون تماس گیرندگان تهدید کننده را قطع کنید و مستقیماً با سازمان مربوطه تماس بگیرید.
- یک سازمان واقعی هرگز از شما نمی خواهد با روش های غیرعادی مانند کارت های هدیه یا فروشگاه، کوپن های iTunes، حواله های سیمی یا بیت کوین پرداخت کنید.
- اگر نگران امنیت خود هستید، با لین کمکی پولیس تماس بگیرید.

ارتباط



فریکاران برای ایجاد روابط و اعمال نفوذ بر قربانیان برای روان کردن پول یا معلومات شخصی، پروفایل های جعلی ایجاد می کنند.

نکاتی برای محافظت از خود تان:

- هرگز برای کسی که به آن اعتماد ندارید پول نفرستید یا رمز-عبور، کارت اعتباری یا جزئیات حساب خود را به اشتراک نگذارید.
- از طریق Google یا برنامه های رسانه های اجتماعی، شریک بالقوه خود را به صورت آنلاین جستجو کنید. برای اینکه تشخیص دهید که آیا شخص دیگری مالک عکس هایی است که برای شما روان شده است، جستجوی معکوس عکس را امتحان کنید.
- با خانواده و دوستان خود راجع به رابطه آنلاین خود صحبت کنید. آنها ممکن است بتوانند بینش ها و علائم هشدار دهنده شناسایی را ارائه دهند که ممکن است شما متوجه آنها نشده باشید.

خرید آنلاین



فریکاران فروشگاه های آنلاین یا تبلیغاتی ایجاد می کنند تا خریداران را به خرید محصولات غیر-موجود یا جعلی ترغیب کنند.

نکاتی برای محافظت از خود تان:

- فقط از وب سایت های معتبر و ایمن خرید کنید و مراقب هر پیشنهادی باشید که باور نکردنی به نظر می رسد.
- از روش های پرداخت امن استفاده کنید و از انتقال مستقیم به فروشندگان خودداری کنید.
- عجله نکنید و تحت فشار «پیشنهادهای محدود» یا «شمارش برعکس» پایان فروش نباشید.

