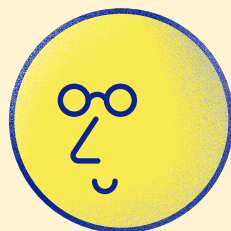


نحوه شناسایی و جلوگیری از کلاهبرداری

راهنمای شما برای محافظت
از خود در برابر کلاهبرداری



ScamWatch

Stop. Better safe than scammed.



Australian Government



**National
Anti-Scam
Centre**

تصدیق کشور

ACCC (کمیسون رقابت و مصرف کنندگان استرالیا) مالکان و متولیان سنتی کشور در سراسر استرالیا را به رسمیت می شناسد و ارتباط مستمر آنها با زمین، دریا و جامعه را به رسمیت می شناسد. ما به آنها و فرهنگ آنها احترام می گذاریم. و به بزرگان آنها در گذشته، حال و آینده.

Australian Competition and Consumer Commission

Ngunnawal

23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

Commonwealth of Australia 2023 ©

حق چاپ این اثر محفوظ است. علاوه بر هرگونه استفاده مجاز تحت قانون حق چاپ 1968، تمام مطالب موجود در این اثر تحت مجوز Creative Commons Attribution 4.0 استرالیا ارائه شده است، به استثنای موارد زیر:

- نشان مشترک المنافع
- آرم های ACCC و AER
- هر تصویر، نمودار، عکس یا گرافیکی که کمیسون رقابت و مصرف کنندگان استرالیا دارای حق چاپ آن نیست، اما ممکن است بخشی از این نشریه باشد یا در آن موجود باشد.

جزئیات شرایط مجوز مربوطه در وب سایت Creative Commons و همچنین کد قانونی کامل مجوز CC BY 4.0 AU موجود است.

درخواست ها و پرس و جوهای مربوط به بازتولید و حقوق باید به Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT ارسال شود.

اطلاعیه مهم

اطلاعات این نشریه فقط برای راهنمایی عمومی است. این اطلاعات به منزله مشاوره حقوقی یا سایر مشاوره های حرفه ای نیست و نباید به عنوان بیانیه قانون در هیچ حوزه قضایی به آن استناد کرد. از آنجا که این فقط به عنوان یک راهنمای کلی در نظر گرفته شده است، ممکن است شامل کلیات باشد. اگر نگرانی خاصی دارید باید مشاوره حرفه ای دریافت کنید.

ACCC تمام تلاش معقول خود را برای ارائه اطلاعات دقیق و جاری انجام داده است، اما هیچ تضمینی در مورد دقیق بودن، به روز بودن یا کامل بودن آن اطلاعات ارائه نمی کند.

طرف هایی که مایل به انتشار مجدد یا استفاده دیگری از اطلاعات این نشریه هستند، باید قبل از انتشار، این اطلاعات را از نظر به روز بودن و دقیق بودن بررسی کنند. این بررسی باید قبل از هر ویرایش انجام شود، زیرا دستورالعمل ACCC و قوانین انتقالی مربوطه اغلب تغییر می کنند. هر گونه سؤالی که اشخاص دارند باید به Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601 ارسال شود.

ACCC 05/24_24-13

www.accc.gov.au

فهرست

1	حمایت در دسترس است
3	کلاهبرداری چیست
4	اقدامات ساده برای شناسایی و جلوگیری از کلاهبرداری
7	کلاهبرداری پیامکی یا SMS
11	کلاهبرداری از طریق ایمیل
15	کلاهبرداری های تلفنی
19	کلاهبرداری های وب سایت
23	کلاهبرداری های مبتنی بر رسانه های اجتماعی، اپ و پیام رسانی آنلاین
27	کلاهبرداری های برتر که باید درباره آنها بدانید
31	کجا می توان کلاهبرداری ها را گزارش کرد
33	کمک و پشتیبانی بیشتر



این راهنما توسط مرکز ملی مبارزه با کلاهبرداری نوشته شده است و به شما کمک می کند آسیب های ناشی از کلاهبرداری را شناسایی کرده و از خود در برابر آن محافظت کنید.

کلاهبرداری جرم است و افرادی که کلاهبرداری می کنند مجرم هستند. بسیاری از مردم استرالیا مورد کلاهبرداری قرار می گیرند و پول خود را از دست می دهند، حتی گاهی اوقات پس انداز زندگی خود را. کلاهبرداری به زندگی مردم آسیب می زند.

شناسایی کلاهبرداری ها سخت تر می شود، بنابراین باید برای جلوگیری از آنها با یکدیگر همکاری کنیم.

مرکز ملی مبارزه با کلاهبرداری تلاش می کند تا استرالیایی ها را از کلاهبرداری در امان نگه دارد.

ما با دولت و صنایع کار می کنیم تا برای جلوگیری از سرقت پول و اطلاعات شخصی استرالیایی ها توسط کلاهبرداران راه های جدیدی پیدا کنیم. در اینجا برخی از راه های رسیدن به این هدف آورده شده است.

ما به افراد کمک می کنیم کلاهبرداری را شناسایی کرده و از آن جلوگیری کنند

از طریق **Scamwatch** ما اطلاعات به روز در مورد کلاهبرداری ها و راه های محافظت از خود در برابر کلاهبرداری را به اشتراک می گذاریم .

ما کلاهبرداران را مختل می کنیم

با جمع آوری و به اشتراک گذاری اطلاعات در سراسر دولت و صنایع، ادامه جرایم کلاهبرداران را دشوار تر و گزارش کردن کلاهبرداری را برای افراد آسان تر می کنیم.



حمایت در دسترس است

اگر در حال خواندن این مطلب هستید، به احتمال زیاد شما یا شخصی که می شناسید مورد کلاهبرداری قرار گرفته است. متأسفانه، شما تنها نیستید. کلاهبرداری ها به طور فزاینده ای پیچیده می شوند، به این معنی که هر کسی می تواند مورد کلاهبرداری قرار بگیرد.

اگر مورد کلاهبرداری قرار گرفته اید، مهم است که سریع اقدام کنید.

اگر پول خود را به یک کلاهبردار از دست داده اید، با بانک یا ارائه دهنده کارت خود تماس بگیرید.

با IDCARE، 1800 595 160، www.idcare.org تماس بگیرید.

کلاهبرداری ها به این دلیل موفق می شوند که واقعی به نظر می رسند. کلاهبرداران متکی بر این هستند که شما علائم هشدار دهنده را تشخیص ندهید زیرا عجله دارید، چیزی شبیه معامله خیلی خوبی است که نمی خواهید از دست بدهید یا به نظر می رسد از طرف شخصی است که به او اعتماد دارید.

با انجام 3 اقدام زیر از خود در برابر کلاهبرداری محافظت کنید:

توقف کنید



اگر مطمئن نیستید پول یا اطلاعات شخصی را به کسی ندهید. کلاهبرداران به شما پیشنهاد کمک می‌کنند یا از شما می‌خواهند تأیید کنید که چه کسی هستید. آنها وانمود می‌کنند که از سازمان‌هایی هستند که شما می‌شناسید و به آنها اعتماد دارید، مانند ارائه دهندگان خدمات، پلیس، بانک یا خدمات دولتی شما.

چک کنید

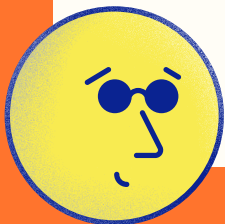


از خود بپرسید - ممکن است پیام یا تماس جعلی باشد؟ هرگز روی لینک در پیام کلیک نکنید. تنها با استفاده از اطلاعات تماسی که از وب‌سایت یا اپ رسمی آن‌ها پیدا می‌کنید، با کسب‌وکارها (بیزینس‌ها) یا دولت تماس بگیرید. اگر مطمئن نیستید، «نه» بگویید، قطع کنید یا حذف کنید.

گزارش بدهید



اگر حس می‌کنید چیزی اشتباه است، سریع عمل کنید. اگر متوجه فعالیت غیرعادی شدید یا اگر یک کلاهبردار پول یا اطلاعات شما را گرفت، با بانک خود تماس بگیرید. به دنبال کمک باشید و کلاهبرداری را به **ReportCyber** و **Scamwatch** گزارش دهید. هنگامی که کلاهبرداری را گزارش می‌کنید، با تقویت دفاع ما در برابر کلاهبرداری به همه استرالیایی‌ها کمک می‌کنید.



کلاهبرداری چیست

کلاهبرداری زمانی است که شخصی شما را فریب می دهد تا پول یا اطلاعات شخصی شما را بدزدد.

کلاهبرداری ها جرایم اقتصادی هستند که توسط مجرمانی که اغلب بسیار سازماندهی شده و پیچیده هستند انجام می شوند.

کلاهبرداری ها:

-  توسط مجرمان اداره می شوند
-  واقعی به نظر می رسند
-  همراه با داستان های باورپذیرند
-  شما را تحت فشار قرار می دهند تا اقدامی انجام دهید

کلاهبرداری شامل موارد زیر نیست:

-  رویکردهای بازاریابی مزاحم
-  شرایط قرارداد
ناعادلانه
-  هک
کامپیوتر

مهم است که به یاد داشته باشید که همه تجربیات منفی کلاهبرداری نیستند. ممکن است برای محصولی که هرگز دریافت نکرده اید پول پرداخت کرده باشید یا چیزی خریده باشید و متوجه شده باشید که کیفیت پایینی دارد. اگرچه این ناامیدکننده است، اما اینها لزوماً کلاهبرداری نیستند. قانون مصرف کنندگان استرالیا از مصرف کنندگان استرالیایی در این گونه مسائل حمایت می کند.

برای اطلاعات بیشتر به www.accc.gov.au/consumers مراجعه کنید.

اقدامات ساده برای شناسایی و جلوگیری از کلاهبرداری

کلاهبرداری ممکن است برای همه ما اتفاق بیفتد. کلاهبرداری ها به این دلیل کار می کنند که کلاهبرداران داستان های قابل باوری برای سرقت پول شما و به دست آوردن اطلاعات شخصی شما خلق می کنند.

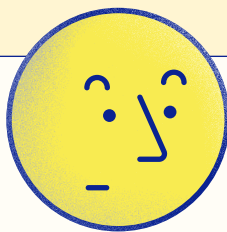
کلاهبرداران باهوش تر می شوند و از فناوری، محصولات، خدمات و رویدادهای مهم جدید بهره می برند تا شما را متقاعد کنند که کلاهبرداری های آنها واقعی است.

تشخیص کلاهبرداری می تواند بسیار سخت باشد. در اینجا چند موقعیت وجود دارد که باید مراقب آنها باشید. گاهی اوقات کلاهبرداران از ترکیبی از این تاکتیک ها استفاده می کنند.

1. فرصت هایی برای کسب یا پس انداز پول: کلاهبرداران شما را فریب می دهند تا فکر کنید یک معامله یا پیشنهاد باورنکردنی دریافت می کنید. آنها شما را تحت فشار قرار می دهند که سریع عمل کنید تا فرصت را از دست ندهید. به یاد داشته باشید، معاملاتی که برای واقعی بودن بیش از حد خوب به نظر می رسند، معمولاً همینطور هستند.

2. داستان های غم انگیز و فریاد کمک: کلاهبرداران سعی می کنند از طبیعت خوب شما علیه شما استفاده کنند. آنها داستان های دلشکستگی و تراژدی را با شما در میان می گذارند و توضیح می دهند که چرا به کمک و پول شما نیاز دارند

3. لینک ها و پیوست ها: کلاهبرداران از لینک هایی استفاده می کنند تا شما را به وب سایت های کلاهبرداری بفرستند که برای سرقت اطلاعات و پول شما طراحی شده اند. کلاهبرداران همچنین ممکن است از شما بخواهند فایل های پیوست را باز کنید. اینها می توانند ویروس هایی را نصب کنند که اطلاعات شما را می دزدند.



4. فشار برای اقدام سریع: کلاهبرداران نمی خواهند که شما وقت صرف کرده و به مسائل فکر کنید. آنها می خواهند شما را تحت فشار قرار دهند تا سریع عمل کنید. این می تواند شامل تهدیدهایی باشد که اگر سریع عمل نکنید اتفاق بدی رخ خواهد داد.

5. درخواست هایی برای این که به روش های غیر معمول یا خاص پرداخت کنید: کلاهبرداران اغلب از شما می خواهند با استفاده از روش های غیرمعمول مانند کارت های نقدی از پیش بارگذاری شده، کارت های iTunes یا ارز مجازی مانند بیت کوین پرداخت کنید. وقتی این پول خرج شد، نمی توانید آن را پس بگیرید.

6. درخواست برای راه اندازی حساب های جدید یا PayID: کلاهبرداران ممکن است از شما بخواهند که یک حساب بانکی یا PayID جدید ایجاد کنید تا به آنها پرداخت کنید (یا توسط آنها پرداخت شود). آنها ممکن است وانمود کنند که بانک شما هستند و به شما بگویند که پول خود را به حساب های جدید منتقل کنید تا آن را ایمن نگه دارید.

اگر کلاهبرداران موفق شده اند پول شما را بگیرند، سعی خواهند کرد پول بیشتری از شما بگیرند. متأسفانه، از هر سه قربانی کلاهبرداری، یک نفر بیش از یک بار مورد کلاهبرداری قرار گرفته است. اگر در اثر کلاهبرداری پول خود را از دست داده اید، مراقب کلاهبردارانی باشید که به شما پیشنهاد کمک می کنند تا پول خود را پس بگیرید. این یک نوع دیگر از کلاهبرداری های بعدی است.



کلاهبرداری پیامکی یا SMS

کلاهبرداران پیام‌هایی را ارسال می‌کنند که وانمود می‌کنند از طرف دولت، مجری قانون، مشاغل مورد اعتماد یا حتی خانواده شما هستند.

این پیام‌ها فوری به نظر می‌رسند و سعی می‌کنند شما را وادار کنند به سرعت عمل کنید. آنها اغلب یک لینک دارند که شما را به یک وب‌سایت کلاهبرداری می‌برد. کلاهبرداران می‌توانند هر گونه اطلاعات شخصی وارد شده در این وب‌سایت‌های کلاهبرداری را بدزدند و از آن برای برداشتن پول یا ارتکاب کلاهبرداری به نام شما استفاده کنند.

برای اینکه این پیام‌ها واقعی به نظر برسند، کلاهبرداران شماره تلفن خود را در پشت شماره تلفن و شناسه تماس‌گیرندگان مشاغل قانونی یا افرادی که می‌شناسید کپی یا پنهان می‌کنند.

پیام‌های کلاهبرداری حتی می‌توانند در زنجیره پیام‌های واقعی آن سازمان ظاهر شوند و تشخیص آنها را سخت‌تر کند.

نشانه هایی که یک پیام ممکن است کلاهبرداری باشد

پیام:

از شما می خواهد که اقدام فوری انجام دهید، مبلغی را بپردازید یا پولی را انتقال دهید.



از شما می خواهد که روی یک لینک کلیک کنید یا با شماره ای که در پیام ارائه شده است تماس بگیرید.



از شما می خواهد که با نام کاربری و رمز عبور خود به یک حساب آنلاین وارد شوید یا اطلاعات شخصی دیگری را ارائه دهید.



از طرف یکی از اعضای خانواده یا دوست است که می گوید اطلاعات تماسشان تغییر کرده است.



تهدید می کند که در صورت عدم اقدام، سرویسی را متوقف می کند یا از شما هزینه دریافت می کند.



وانمود می کند که شما یا حساب های شما هک شده یا درگیر کلاهبرداری شده اید.



وانمود می کند که مشکلی در پرداخت یا تحویل بسته شما وجود دارد.



کام هایی برای محافظت از خود در برابر کلاهبرداری های پیام رسانی

1. اگر شخصی که می شناسید پیامی بفرستد تا بگوید شماره تلفن جدیدی دارد:



- a. سعی کنید با شماره موجودی که از او دارید تماس بگیرید و
- b. به شماره جدید یک سوال که فقط او پاسخش را می داند بفرستید تا چک کنید او کسی که می گوید هست یا نه.

2. هرگز روی پیوندهای موجود در پیام ها کلیک نکنید.



3. اگر پیامی به یک وب سایت لینک دارد، روی آن لینک کلیک نکنید. در عوض، خودتان وب سایت را به صورت آنلاین جستجو کنید یا از اپ رسمی استفاده کنید.



4. با استفاده از شماره تلفن ارائه شده به پیامک پاسخ ندهید.



5. با شماره تلفنی که خودتان پیدا کرده اید، مانند وب سایت سازمان، دوباره با سازمان یا شخص تماس بگیرید.





کلاهبرداری از طریق ایمیل

کلاهبرداران ایمیل هایی را ارسال می کنند که وانمود می کنند از طرف دولت، مجری قانون و مشاغل هستند. آن ها کاری می کنند که موضوع فوری به نظر برسد تا شما سریع اقدام کنید.

کلاهبرداران از همان آرم و آدرس ایمیل مشابه سازمان واقعی استفاده می کنند. کلاهبرداران همچنین می توانند آدرس ایمیل خود را در پشت آدرس ایمیل یک سازمان یا بیزینس کپی یا پنهان کنند تا ایمیل کلاهبرداری واقعی تر به نظر برسد.

نشانه هایی که یک ایمیل ممکن است کلاهبرداری باشد

ایمیل:

درخواست پرداخت می کند اما جزئیات حساب جدید است یا از آخرین پرداختی که انجام داده اید تغییر کرده است.



از شما می خواهد که با نام کاربری و رمز عبور خود به یک حساب آنلاین وارد شوید یا اطلاعات شخصی دیگری را ارائه دهید.



غیرمنتظره بود و شامل یک پیوست با دعوت به باز کردن آن است.



از شما می خواهد جزئیات بانکی خود را تأیید کنید تا بازپرداخت یا پولی را که انتظار ندارید دریافت کنید.



ادعا می کند که اطلاعاتی درباره شما یا تصاویری از شما دارد و تهدید به انتشار آنها می کند.



پیشنهاد می کند که برای بازیابی پول یا دریافت غرامت نقض داده های شما یا سرقت هویت به شما کمک کند.



اقداماتی که می توانید برای محافظت از خود در برابر کلاهبرداری های ایمیل انجام دهید

1. بررسی کنید که ایمیل واقعی است یا خیر:

- a. تماس مستقیم با شخص یا سازمان با استفاده از اطلاعات تماسی که خودتان پیدا کرده اید، مانند وب سایت سازمان یا
- b. دسترسی به یک سازمان از طریق اپ رسمی آنها (هرگز از طریق لینک این کار را نکنید).



2. فوراً ارتباط خود را با هر کسی که سعی در تهدید یا ارباب شما دارد قطع کنید.



3. هرگز اطلاعات شخصی ندهید یا به کسی که به شما موارد زیر را پیشنهاد می کند پول ندهید:

- a. غرامت یا کمک به بازیابی از کلاهبرداری قبلی یا نقض داده ها یا
- b. برنده شدن ها، جوایز یا یک ارث.



4. در صورت امکان از احراز هویت چند عاملی استفاده کنید. این یک لایه حفاظتی اضافی را فراهم می کند و به این معنی است که یک کلاهبردار باید رمز عبور ایمیل شما و یک شماره پین ارسال شده به تلفن شما را بداند تا به حساب ایمیل شما دسترسی پیدا کند.





کلاهبرداری های تلفنی

کلاهبرداران با ادعای اینکه از سازمان های معروف هستند تماس می گیرند. این شامل سازمان های دولتی، مجری قانون، سرمایه گذاری و شرکت های حقوقی، بانک ها و ارائه دهندگان مخابرات می شود.

آن ها طوری وانمود می کنند که اقدام سریع شما ضروری به نظر برسد. آنها ممکن است سعی کنند شما را متقاعد کنند که اطلاعات شخصی یا حساب بانکی خود یا دسترسی به رایانه خود را به آنها بدهید.

ممکن است تماس گیرنده از قبل اطلاعاتی درباره شما داشته باشد، مانند نام یا آدرس شما، که باعث می شود تماس واقعی به نظر برسد.

علائمی که نشان می دهند تماس تلفنی ممکن است کلاهبرداری باشد

تماس گیرنده:

درخواست پرداخت می کند یا از شما می خواهد که پول را به یک حساب جدید منتقل کنید.



رمز عبور، پین، کد یکبار مصرف یا برخی اطلاعات امنیتی دیگر را از شما می خواهد.



از شما جزئیات مالی مانند جزئیات کارت اعتباری یا بانکی را می خواهد.



از شما می خواهد که یک اقدام را در تلفن همراه یا رایانه خود انجام دهید، مانند نصب نرم افزار یا دسترسی به یک حساب امن.



ادعا می کند که از مجریان قانون است و شما را به دستگیری یا اخراج فوری تهدید می کند.



می گوید بانک یا سایر حساب های آنلاین شما هک شده یا درگیر کلاهبرداری شده است.



اقداماتی که می توانید برای محافظت از خود در برابر کلاهبرداری های تلفنی انجام دهید

1. بررسی واقعی بودن تماس توسط یکی از موارد زیر:

- a. تماس مستقیم با شخص یا سازمان با استفاده از اطلاعات تماسی که خودتان پیدا کرده اید، مانند وب سایت سازمان یا
- b. دسترسی به یک سازمان از طریق اپ رسمی آنها (هرگز از طریق لینک این کار را نکنید).



2. اگر مطمئن نیستید تماس گیرنده کیست یا شما را تهدید یا ارباب می کند، فوراً تلفن را قطع کنید.



3. هرگز نرم افزاری را نصب نکنید که به شخصی اجازه دسترسی به رایانه یا دستگاه شما را می دهد.



4. می توانید تماس ها از شماره هایی را که نمی شناسید نادیده بگیرید یا اجازه دهید تماس ها به پست صوتی بروند.



خوب است بدانید!

حتی اگر شماره خصوصی داشته باشید یا در لیست «تماس نگیرید» **Do Not Call** هستید، همچنان می توانید تماس های کلاهبرداری دریافت کنید.





کلاهبرداری های وب سایت

کلاهبرداران می توانند وانمود کنند که هر شخص آنلاینی هستند، از جمله دولت، یک بیزینس واقعی، افراد مشهور یا دوستان یا خانواده شما.

آنها می توانند وب سایت های جعلی ایجاد کنند تا شبیه برندهای معروف شوند. آنها ممکن است وانمود کنند افراد مشهور هستند و به نظر برسد که در حال تایید کالا یا خدمات هستند. این وب سایت ها می توانند حاوی نظرات جعلی باشند تا باعث شوند شما به آنها اعتماد کنید.

ممکن است هنگام آنلاین بودن، بنرهای تبلیغاتی جعلی یا پنجره های pop-up حاوی هشدارهای جعلی یا پیام های خطا را مشاهده کنید.

نشانه هایی که یک وب سایت ممکن است یک کلاهبرداری باشد

وبسایت:

اقدام را با قیمت هایی که از حد معمول یا در مقایسه با سایت های دیگر بسیار پایین تر است برای فروش ارائه می دهد.



به شما درباره راهی برای کسب درآمد سریع و آسان با ریسک یا تلاش کم می گوید.



حاوی یک هشدار یا پیام خطای فوری است که از شما می خواهد روی یک لینک کلیک کنید.



درخواست پرداخت به روش های غیرمعمول یا خاص مانند کارت های هدیه یا ارزهای دیجیتال مانند بیت کوین را دارد.



فقط شامل نظرات مثبت است.



اقداماتی که می توانید برای جلوگیری از کلاهبرداری وب سایتی انجام دهید

1. قیمت ها را مقایسه کنید. اگر پیشنهادی خوب تر از آن به نظر می رسد که واقعی باشد ، احتمالاً همینطور است.



2. قبل از دادن پول یا اطلاعات شخصی خود در مورد سازمان یا شخصی که با او سر و کار دارید تحقیق کنید.



3. به نظرات نوشته شده در خود وب سایت اعتماد نکنید. نام وب سایت یا بیزینس و کلمه «کلاهبرداری» یا «بازینی» را جستجو کنید.



4. اگر اخطار یا پیام خطایی روی صفحه نمایش شما ظاهر شد، روی آن کلیک نکنید، در عوض مستقیماً به اپلیکیشن مورد نظر بروید تا واقعی بودن آن را بررسی کنید.



5. با فعال کردن «به روزرسانی های خودکار» برای سیستم عامل و اپ هایتان، ابزاری را که برای خرید آنلاین استفاده می کنید به روز نگه دارید.



خوب است بدانید!

راه های عملی برای محافظت از خود به صورت آنلاین در www.cyber.gov.au موجود است.





کلاهبرداری های مبتنی بر رسانه های اجتماعی، اپ و پیام رسانی آنلاین

اگر فردی که نمی شناسید در رسانه های اجتماعی، یک پلتفرم پیام رسانی مانند واتس اپ یا وی چت یا از طریق یک اپ با شما تماس بگیرد، ممکن است کلاهبرداری باشد.

کلاهبرداری که وانمود می کنند شخص دیگری هستند، اغلب از عکس واقعی شخص یا لوگوی رسمی سازمانی که وانمود می کنند هستند استفاده می کنند تا تشخیص کلاهبرداری را سخت تر کنند.

کلاهبرداران در رسانه های اجتماعی پروفایل های جعلی ایجاد می کنند و وانمود می کنند که از دولت، یک بیزینس واقعی، کارفرما، شرکت سرمایه گذاری یا حتی یک دوست، عضو خانواده یا علاقه مند عاشقانه هستند. آنها ممکن است وانمود کنند افراد مشهور هستند و به نظر برسد که در حال تبلیغ کالا یا خدمات هستند.

کلاهبرداران همچنین می توانند از جزئیاتی که در حساب های رسانه های اجتماعی خود به اشتراک می گذارید چیزهای زیادی درباره شما بیاموزند. آنها می توانند از این اطلاعات برای حدس زدن رمزهای عبور حساب شما یا هدف قرار دادن سایر کلاهبرداری ها استفاده کنند.

نشانه های کلاهبرداری در رسانه های اجتماعی یا اپلیکیشن

پروفايل يا اپليکيشن رسانه اجتماعی:

به شما درباره راهی برای کسب درآمد سریع و آسان با ریسک یا تلاش کم می گوید.



از شما دعوت می کند تا در یک مسابقه یا پیشنهاد زمانی محدود شرکت کنید.



درخواست انتقال مکالمه از اپی مانند اپ دوستیابی به چت یا ایمیل خصوصی.



اشاره می کند که یک شخص معروف محصول یا خدماتی را تایید یا از آن حمایت می کند.



می گوید شخصی چیزی را که شما می فروشید بدون اینکه اول آن را ببیند و با قیمتی بالا خواهد خرید.



تهدید می کند که یک تصویر خصوصی از شما را به اشتراک می گذارد مگر اینکه به آنها پول پرداخت کنید.



با شما تماس می گیرد تا شغلی را به شما پیشنهاد کند.



خوب است بدانید!

اطلاعات مربوط به نحوه ایمن ماندن در پلتفرم های مختلف رسانه های اجتماعی را می توان در www.esafety.gov.au یافت.



اقداماتی که می توانید برای جلوگیری از کلاهبرداری های مبتنی بر رسانه های اجتماعی و اپ ها انجام دهید

1. بررسی کنید که آیا پروفایل ممکن است جعلی باشد. آیا اکانت فعال است؟ آنها چند دوست/فالوور دارند و چقدر آنلاین پست می کنند؟



2. نام پروفایل را به همراه کلمه «کلاهبرداری» (scam) به صورت آنلاین جستجو کنید.



3. هرگز کاری را که به شما پیشنهاد شده است بدون مصاحبه یا گفتگو در مورد تجربه، شایستگی و مراجع خود انتخاب نکنید. در مورد استخدام کننده و بیزینس یا فردی که این شغل را ارائه می دهد تحقیق کنید. از طریق شماره تلفن هایی که از یک جستجوی اینترنتی مستقل تهیه شده است، با آژانس کاریابی تماس بگیرید. فقط برای تضمین شغلی از قبل پول پرداخت نکنید.



4. فقط از کسی که دارای مجوز خدمات مالی استرالیا است مشاوره سرمایه گذاری بگیرید و بررسی کنید که نام یک شرکت یا وب سایت در پورتال هشدارهای سرمایه گذاران سازمان بین المللی کمسیون اوراق بهادار (IOSCO) نباشد.



5. هرگز به کسی که فقط آنلاین با او آشنا شده اید پول ندهید. کلاهبرداران اغلب می گویند که در خارج از کشور زندگی می کنند و نمی توانند شخصاً شما را ملاقات کنند.



6. هرگز تصاویر شخصی خود را برای کسی که فقط به صورت آنلاین با او ملاقات کرده اید ارسال نکنید.



برای اطلاعات بیشتر در مورد کلاهبرداری ها از جمله راه های دیگری مانند حضوری و از طریق پست، که کلاهبرداران ممکن است با شما تماس بگیرند، به [Scamwatch](#) مراجعه کنید.



کلاهبرداری های برتر که باید درباره آنها بدانید

در اینجا برخی از رایج ترین انواع کلاهبرداری را برای شما آورده ایم که باید از آنها آگاه باشید. می توانید اطلاعات بیشتری در مورد هر یک از این نوع کلاهبرداری ها، از جمله علائم هشدار دهنده و اقدامات محافظت از خود را، در وب سایت [Scamwatch](#) بیابید.

کلاهبرداری های جعل هویت

کلاهبرداران شما را فریب می دهند تا فکر کنید از سازمان های قابل اعتمادی مانند پلیس، دولت، بانک ها و بیزینس های معروف هستند. آنها حتی می توانند وانمود کنند که دوست یا عضو خانواده شما هستند. کلاهبرداران با ارسال ایمیل یا پیام های فیشینگ اطلاعاتی را درباره شما جستجو می کنند. اینها برای سرقت اطلاعات شما طراحی شده اند. آنها سعی می کنند با وانمود کردن اینکه از یک سازمان رسمی یا شخصی که می شناسید و به او اعتماد دارید هستند، شما را متقاعد کنند که اطلاعات شخصی خود را به آنها بدهید. کلاهبرداران از فناوری استفاده می کنند تا به نظر برسد که تماس ها یا پیام هایشان از یک شماره تلفن قانونی است. آنها می توانند پیام های متنی را در همان رشته مکالمه به عنوان پیام های واقعی از یک سازمان نشان دهند.

کلاهبرداری های سرمایه گذاری

کلاهبرداران از بازاریابی متقاعد کننده و فناوری جدید استفاده می کنند تا پیشنهاد سرمایه گذاری خود را آنقدر خوب جلوه دهند که نمی توان آن را از دست داد. آنها به شما وعده سودهای کلان با ریسک کم یا بدون ریسک می دهند. آن ها اغلب از تاکتیک های فشار استفاده می کنند تا شما را مجبور کنند سریع عمل کنید، بنابراین می توانند پول شما را بدزدند.

شغل و کلاهبرداری شغلی

کلاهبرداران مشاغل را ارائه می دهند که با تلاش اندک درآمد خوبی دارند. آنها وانمود می کنند که از طرف شرکت های مطرح و پلتفرم های خرید آنلاین استخدام می کنند. گاهی اوقات، شغلی که فهرست می کنند حتی وجود ندارد. کلاهبرداران همچنین وانمود می کنند که آژانس های استخدام شناخته شده هستند. هدف آنها سرقت پول و اطلاعات شخصی شماست. آنها ممکن است از شما بخواهند که از قبل پول بپردازید تا بتوانید برای آنها کار کنید.

کلاهبرداری محصولات و خدمات

کلاهبرداران به عنوان خریدار یا فروشنده ظاهر می شوند تا پول شما را بدزدند. آنها وب سایت ها یا پروفایل های جعلی را در سایت های فروشگاه های قانونی راه اندازی می کنند که محصولات یا خدماتی را با قیمت هایی ارائه می کنند که خوب تر از آن است که واقعی باشد. آنها تبلیغات جعلی و نظریات جعلی ارسال می کنند. آنها ممکن است از آرم های دزدیده شده، یک نام دامنه **com.au** و شماره بیزینس استرالیایی (ABN) به سرعت رفته استفاده کنند. تشخیص این کلاهبرداری ها سخت است.

کلاهبرداران همچنین به عنوان بیزینس هایی ظاهر می شوند که شما آنها را می شناسید و به آنها اعتماد دارید تا صورتحساب های جعلی را برای شما ارسال کنند. آنها حتی می توانند جزئیات فاکتورهای قانونی را تغییر دهند تا مشتریانان به جای شما به کلاهبردار پرداخت کنند.

کلاهبرداری های عاشقانه

کلاهبرداران از وعده عشق، قرار گذاشتن، یا دوستی برای سرقت پول شما استفاده می کنند. آنها تمام تلاش خود را می کنند تا شما را متقاعد کنند که این رابطه واقعی است و شما را گول می زنند تا به آنها پول بدهید.

کلاهبرداران شما را در رسانه های اجتماعی، اپ های دوستیابی یا بازی و وب سایت ها پیدا می کنند. آنها همچنین ممکن است برای شما پیامک یا ایمیل ارسال کنند. آنها پشت پروفایل ها و هویت های جعلی، که گاهی اوقات مربوط به افراد مشهور است، پنهان می شوند. هنگامی که به آنها اعتماد کنید، آنها یک "وضعیت اضطراری" خواهند داشت و از شما کمک خواهند خواست. این اغلب درخواست هایی برای پول یا سایر محصولات است.

تهدید و کلاهبرداری اخاذی

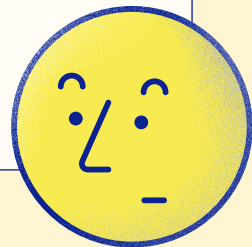
کلاهبرداران وانمود می کنند که از یک سازمان قابل اعتماد هستند و ادعا می کنند که باید پول بپردازید وگرنه اتفاق بدی رخ خواهد داد. آنها ممکن است شما را به دستگیری، اخراج از کشور یا حتی آسیب جسمی تهدید کنند، در صورتی که با پرداخت فوری آنها موافقت نکنید.

آنها همچنین می توانند با تهدید به اشتراک گذاری تصاویر یا ویدیوهای برهنه ای که برایشان ارسال کرده اید در صورت عدم ارسال پول برای آنها، از شما باج گیری کنند.

کلاهبرداری های پول غیرمنتظره

کلاهبرداران سعی می کنند شما را متقاعد کنند که شما پولی یا جایزه ای را طلب دارید یا مستحق دریافت آن هستید که انتظارش را ندارید.

کلاهبردار از شما می خواهد قبل از جمع آوری پول یا جایزه، مبلغی را پرداخت کنید یا اطلاعات بانکی یا هویتی خود را ارائه دهید. متأسفانه پول مجانی وجود ندارد.





کجا می توان کلاهبرداری ها را گزارش کرد

ما در تلاش هستیم تا با افزایش آگاهی در مورد نحوه شناسایی، اجتناب و گزارش کلاهبرداری، استرالیا را به هدف سخت تری برای کلاهبرداران تبدیل کنیم.

ما اطلاعات گزارش های کلاهبرداری را به اشتراک می گذاریم و با دولت، مجری قانون و بخش خصوصی برای ایجاد اختلال و جلوگیری از کلاهبرداری کار می کنیم.

با گزارش دادن به Scamwatch به دیگران کمک کنید. تجربه کلاهبرداری خود را از طریق فرم گزارش در وب سایت [Scamwatch www.scamwatch.gov.au](http://www.scamwatch.gov.au) گزارش دهید.

به یاد داشته باشید، اگر قربانی یک کلاهبرداری هستید، مهم است که سریع عمل کنید.

■ اگر پول خود را به یک کلاهبردار از دست داده اید، با بانک یا ارائه دهنده کارت خود تماس بگیرید.

■ با idcare.org | 1800 595 160 ID CARE تماس بگیرید



کمک و پشتیبانی بیشتر

قربانی کلاهبرداری بودن می تواند احساسی طاقت فرسا داشته باشد. مهم است که به یاد داشته باشید که ممکن است برای هر کسی اتفاق بیفتد و پشتیبانی در دسترس است.

اگر شما یا کسی که می شناسید مورد کلاهبرداری قرار گرفته اید، در مورد آن با کسی صحبت کنید. می توانید از خانواده، دوستان، پزشک عمومی یا یکی از سرویس های حمایتی زیر کمک بگیرید.

Lifeline: 13 11 14 | lifeline.org.au

یا چت پشتیبانی بحران آنلاین (24 ساعت شبانه روز، 7 روز هفته)

Beyond Blue: 1300 22 4636 | beyondblue.org.au

یا چت آنلاین (24 ساعت شبانه روز، 7 روز هفته)

Kids Helpline: 1800 55 1800 | kidshelpline.com.au

(24 ساعت شبانه روز، 7 روز هفته)

اثرات مالی کلاهبرداری می تواند ویرانگر باشد و زندگی را تغییر دهد.

اگر با مشکلات مالی مواجه هستید، می توانید از طریق خط تلفن ملی بدهی با یک مشاور مالی

صحبت کنید:

1800 007 007 از 9:30 صبح تا 4:30 بعد از ظهر دوشنبه تا جمعه

یا از دوشنبه تا جمعه از ساعت 9:00 صبح تا 8:00 بعد از ظهر به چت زنده دسترسی داشته باشید.

33

scamwatch.gov.au