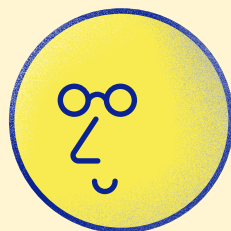


نحوه تشخیص و جلوگیری از فریبکاری

راهنمای شما برای محافظت
از خود در برابر فریبکاری



ScamWatch

Stop. Better safe than scammed.



Australian Government



**National
Anti-Scam
Centre**

قدرتانی کشور

ACCC از مالکان و نگهداران سنتی کشور در سراسر استرالیا قدرتانی می کند و ارتباط مستمر آنها با زمین، دریا و جامعه را به رسمیت می شناسد. ما به آنها و فرهنگ آنها، و به بزرگان آنها در گذشته، حال و آینده احترام می گذاریم.

Australian Competition and Consumer Commission

Ngunnawal

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

Commonwealth of Australia 2023 ©

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

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

جزئیات شرایط مجوز مربوطه در وب سایت Creative Commons موجود است، همانطور که کد قانونی کامل برای مجوز CC BY 4.0 AU است. درخواست ها و پرسش های مربوط به حقوق و پارتولید باید به مدیر ارتباطات شرکتی ACCC به GPO Box 3131، Canberra ACT 2601 ارسال شود.

اطلاعیه مهم

اطلاعات این نشریه فقط برای راهنمایی عمومی است. این مشاوره حقوقی یا سایر مشاوره های حرفه ای را تشکیل نمی دهد و نباید به عنوان بیانیه قانون در هر حوزه قضایی به آن اعتماد کرد. از آنجا که فقط به عنوان یک راهنمای کلی در نظر گرفته شده است، ممکن است شامل کلیات باشد. اگر تگرای خاصی دارید، باید مشاوره حرفه ای دریافت کنید.

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

طرف هایی که مایل به انتشار مجدد یا استفاده دیگر از اطلاعات این نشریه هستند، باید قبل از انتشار این اطلاعات را از نظر جریان و صحت بررسی کنند. این کار باید قبل از هر نسخه انتشار انجام شود، زیرا دستورالعمل ACCC و قوانین انتقال مربوطه مکرراً تغییر میکنند. هر گونه سوالی که طرفین دارند باید به مدیر ارتباطات شرکتی ACCC به GPO Box 3131، Canberra ACT 2601 خطاب شود.

ACCC 05/24_24-13

www.accc.gov.au

فهرست

1	کمک در دسترس است
3	فریکاری چیست
4	اقدامات ساده برای شناسایی و جلوگیری از فریکاری
7	فریکاری از طریق پیام یا SMS
11	فریکاری از طریق ایمیل
15	فریکاری های تلفونی
19	فریکاری های وب سایت
23	فریکاری های براساس برنامه، شبکه اجتماعی و پیام رسانی آنلاین
27	فریکاری های برتر که باید درباره آنها بدانید
31	کجا میتوان فریکاری ها را گزارش داد
33	کمک و حمایت بیشتر



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

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

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

مرکز ملی مبارزه با فریبکاری تلاش می کند تا آسترالیایی ها را از فریبکاری در امان نگهدارد.

ما با دولت و صنعت کار می کنیم تا راه های جدیدی برای جلوگیری از سرقت پول و اطلاعات شخصی از آسترالیایی ها توسط فریبکاران پیدا کنیم. در اینجا برخی از راه های که ما برای رسیدن به این اهداف انجام می دهیم آمده است.

ما به مردم کمک می کنیم فریبکاری را شناسایی کرده و از آن جلوگیری کنند

از طریق Scamwatch ما معلومات تازه در مورد فریبکاری ها و راه هایی را به اشتراک می گذاریم که می توانید از خود در برابر فریبکاری ها محافظت کنید.

ما فریبکاران را مختل می کنیم

با جمع آوری و به اشتراک گذاری اطلاعات در سراسر دولت و صنعت، ادامه جرایم فریبکاری را سخت تر می کنیم و گزارش فریبکاری را برای مردم آسانتر می کنیم.



کمک در دسترس است

اگر در حال خواندن این مطلب هستید، به احتمال زیاد شما یا شخصی که می شناسید فریب داده شده اید. متأسفانه، شما تنها نیستید. فریبکاری ها به طور فزاینده ای پیچیده می شوند، به این معنی که هر کسی می تواند مورد فریبکاری قرار گیرد.

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

اگر پول خود را به یک فریبکار از دست داده اید، با بانک یا فراهم کننده کارت خود تماس بگیرید.

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

فریبکاری ها به این دلیل موفق می شوند که هم شکل چیز واقعی هستند. فریبکاران به این متکی هستند که شما علائم هشدار دهنده را تشخیص نمی دهید زیرا عجله دارید، چیزی شبیه یک معامله عالی است که نمی خواهید از دست بدهید یا به نظر میرسد از طرف شخصی است که به آن اعتماد دارید.

با دنبال کردن این 3 مرحله از خود در برابر فریبکاری ها محافظت کنید:

توقف کنید



اگر مطمئن نیستید پول یا اطلاعات شخصی را به کسی ندهید.
فریبکاران به شما پیشنهاد کمک خواهند کرد یا از شما میخواهند که تأیید کنید چه کسی هستید. آنها اظهار می کنند که از سازمان هایی هستند که شما می شناسید و به آنها اعتماد دارید، مانند ارائه دهندگان خدمات، پولیس، بانک یا خدمات دولتی شما.

بررسی کنید

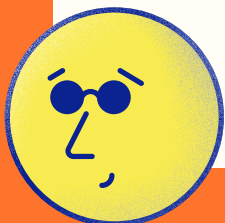


از خود پرسید ممکن است این پیام یا تماس جعلی باشد؟
هرگز روی یک لینک در پیام کلیک نکنید. فقط با استفاده از اطلاعات تماسی که از وب سایت یا برنامه کاربری رسمی آن ها پیدا می کنید، با تجارت ها یا دولت تماس بگیرید. اگر مطمئن نیستید، «نه» بگویید، قطع کنید یا حذف کنید.

گزارش دهید



اگر چیزی اشتباه است، سریع عمل کنید.
اگر متوجه فعالیت غیرعادی شدید یا اگر یک فریبکار پول یا اطلاعات شما را دریافت کرد، با بانک خود تماس بگیرید. به دنبال کمک باشید و فریبکاری را به ReportCyber و Scamwatch گزارش دهید.
هنگامی که فریبکاری را گزارش می دهید، با ایجاد دفاع ما در برابر فریبکاری به همه استرالیایی ها کمک می کنید.



فریبکاری چیست

فریبکاری زمانی است که شخصی شما را فریب می دهد تا پول یا اطلاعات شخصی شما را دزدی کند.

فریبکاری ها جرایم اقتصادی هستند که توسط مجرمانی که اکثراً بسیار سازماندهی شده و پیچیده هستند اداره می شوند.

فریبکاری ها:

- ✓ توسط جنایتکاران اجرا میشوند
- ✓ واقعی به نظر میرسند
- ✓ با داستان های باورکردنی می باشند
- ✓ شما را تحت فشار قرار میدهند تا اقدامی انجام دهید

فریبکاری موارد ذیل نیست:

- ✗ هک کردن کامپیوتر
- ✗ شرایط ناعادلانه قرارداد
- ✗ رویکردهای بازاریابی مزاحم

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

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

اقدامات ساده برای شناسایی و جلوگیری از فریبکاری

فریبکاری ممکن است برای همه ما اتفاق بیفتد. فریبکاری ها کار میکنند زیرا فریبکاران داستان های قابل باوری برای سرقت پول شما و به دست آوردن اطلاعات شخصی شما ایجاد می کنند.

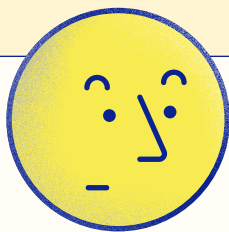
فریبکاران باهوش تر می شوند و از تکنالوژی، محصولات، خدمات و رویدادهای مهم جدید استفاده می کنند تا شما را متقاعد کنند که فریبکاری های شان واقعی است.

تشخیص یک فریبکاری می تواند بسیار سخت باشد. در اینجا چند حالت وجود دارد که باید متوجه آنها باشید. گاهی اوقات فریبکاران از ترکیبی از این تاکتیک ها استفاده میکنند.

1. فرصت هایی برای بدست آوردن یا پس انداز پول: فریبکاران شما را فریب میدهند تا فکر کنید یک معامله یا پیشنهاد باورنکردنی دریافت میکنید. آنها شما را تحت فشار قرار میدهند تا سریع عمل کنید تا آن را از دست ندهید. به یاد داشته باشید، معاملاتی که به نظر خیلی خوب می آیند، معمولاً واقعیت ندارند.

2. داستانهای غم انگیز و فریادهای کمک: فریبکاران سعی میکنند از طبیعت خوب شما علیه خودتان استفاده کنند. آنها داستانهای دلشکستگی و غم انگیز را با شما در میان می گذارند و توضیح میدهند که چرا به کمک شما و پول شما نیاز دارند.

3. لینک ها و پیوست ها: فریبکاران از لینک های برای راجع کردن شما به وب سایت های فریبکاری استفاده می کنند که برای سرقت اطلاعات و پول شما طراحی شده اند. فریبکاران همچنین ممکن است از شما بخواهند پیوست ها را باز کنید. اینها میتوانند ویروس هایی را نصب کنند که اطلاعات شما را می دزدند.



4. فشار برای اقدام سریع: فریبکاران نمی خواهند شما وقت بگذارید 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 ها برای پرداختن به روش های غیر معمول یا خاص: فریبکاران بیشتر اوقات از شما می خواهند با استفاده از روش های غیرمعمول مانند کارت های نقدی پیش پرداخت 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 ها یا PayID های جدید: فریبکاران ممکن است از شما بخواهند که یک حساب بانکی یا PayID جدید ایجاد کنید تا به آنها پرداخت کنید (یا توسط آنها پرداخت شوید). آنها ممکن است اظهار کنند که از طرف بانک شما هستند و به شما بگویند که پول خود را به حساب های جدید منتقل کنید تا آن را امن نگهدارید.

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



فریبکاری از طریق پیام یا SMS

فریبکاران پیام هایی را ارسال می کنند که اظهار می کنند از طرف دولت، مجری قانون، تجارت های مورد اعتماد یا حتی فامیل یا دوستان شما هستند.

این پیام ها فوری به نظر میرسند و سعی میکنند که شما سریع عمل کنید. آنها بیشتر اوقات یک لینک دارند که شما را به یک وبسایت فریبکاری میبرد. فریبکاران میتوانند هر گونه اطلاعات شخصی وارد شده در این وبسایت های فریبکاری را بدزدند و از آن برای برداشتن پول یا ارتکاب فریبکاری به نام شما استفاده کنند.

برای اینکه این پیامها واقعی به نظر برسند، فریبکاران شماره تلفون خود را در پشت شماره تلفون و هویت تماس گیرنده تجارت های قانونی یا افرادی که میشناسید درج یا پنهان می کنند.

پیامهای فریبکاری حتی میتوانند در زنجیره پیامهای واقعی سازمان ظاهر شوند و تشخیص آنها را سخت تر میکند.

نشانه هایی که یک پیام ممکن است فریبکاری باشد

پیام:

از شما میخواهد که اقدام فوری انجام دهید، پرداختی انجام دهید یا پول را انتقال دهید.



از شما میخواهد که روی لینکی کلیک کنید یا با شماره ای که در پیام ارائه شده است تماس بگیرید.



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



از طرف یک دوست یا عضو فامیل است که میگوید اطلاعات تماس شان تغییر کرده است.



تهدید میکند که در صورت عدم اقدام، خدمات را متوقف میکند یا از شما هزینه دریافت میکند.



اظهار میکند که شما یا حساب های شما هک شده یا درگیر فریبکاری شده اید.



اظهار میکند که مشکلی در پرداخت یا تحویل بسته شما وجود دارد.



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

1. اگر شخصی که می شناسید پیامی ارسال کرد تا بگوید شماره تلفن جدیدی گرفته است:



- a. سعی کنید با شماره موجودی که برای آنها دارید تماس بگیرید، و
- b. در شماره جدید به آنها پیام دهید و سوالی پرسید که فقط آنها پاسخ آنها بدانند تا بررسی کنید که آنها چه کسی هستند.

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



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



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



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





فریبکاری از طریق ایمیل

فریبکاران ایمیل هایی را ارسال میکنند که اظهار میکنند از طرف دولت، مجری قانون و تجارت ها هستند. آنها را ضروری شکل میدهند تا شما را وادار به اقدام سریع کنند.

فریبکاران از همان لوگو و آدرس ایمیل مشابه سازمان واقعی استفاده می کنند. فریبکاران همچنین میتوانند آدرس ایمیل خود را در پشت آدرس ایمیل یک سازمان یا تجارت پنهان کنند تا ایمیل فریبکاری واقعی تر به نظر برسد.

نشانه هایی که یک ایمیل ممکن است فریبکاری باشد

ایمیل:

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



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



غیرمنتظره است و شامل یک پیوست با درخواست برای باز کردن آن است.



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



ادعا میکند که اطلاعاتی درباره شما یا تصویری از شما دارد و تهدید به انتشار آنها میکند.



پیشنهاد برای کمک به بازیابی پول یا جبران خسارت برای نقض معلومات یا سرقت هویت میکند.



اقداماتی که میتوانید برای محافظت از خود در برابر فریبکاری های ایمیلی انجام دهید

1. بررسی کنید که ایمیل واقعی باشد، توسط:

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



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



3. هرگز اطلاعات شخصی یا پول به کسی که به شما موارد ذیل را پیشنهاد میکند ندهید:

- a. جبران خسارت یا کمک به بازیابی از فریبکاری قبلی یا نقض اطلاعات یا،
- b. برنده شدن، جوایز یا یک ارث.



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





فریکاری های تلفونی

فریکاران 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 میشود.

آنها را ضروری شکل میدهند تا شما را وادار به اقدام سریع کنند. آنها ممکن است سعی کنند شما را متقاعد کنند که اطلاعات شخصی یا حساب بانکی خود یا دسترسی به کامپیوتر خود را به آنها بدهید. ممکن است تماس گیرنده از قبل اطلاعاتی درباره شما داشته باشد، مانند نام یا آدرس شما، که باعث میشود تماس واقعی به نظر برسد.

نشانه هایکه یک تماس تلفونی ممکن است فریبکاری باشد

تماس گیرنده:

درخواست پرداخت میکند یا از شما میخواهد که پول را به یک حساب جدید منتقل کنید.



از شما رمز عبور، رمز، کد یکبار مصرف یا برخی اطلاعات امنیتی دیگر را میخواهد.



از شما جزئیات مالی مانند جزئیات بانکی یا کریدیت کارت را میخواهد.



از شما میخواهد که یک عمل را در تلفون همراه یا کامپیوتر خود انجام دهید، مانند نصب نرم افزار یا دسترسی به یک حساب امن.



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



میگوید که حساب بانکی یا سایر حساب های آنلاین شما هک شده یا درگیر فریبکاری شده است.



اقداماتی که میتوانید برای محافظت از خود در برابر فریبکاری های تلفونی انجام دهید

1. توسط هرکدام از موارد ذیل بررسی کنید که تماس واقعی باشد:

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



2. اگر مطمئن نیستید تماس گیرنده کیست یا شما را تهدید میکنند یا می ترسانند، فوراً تلفون را قطع کنید.



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



4. شما میتوانید تماس هایی را که شماره آنها را نمی شناسید نادیده بگیرید یا اجازه دهید تماس به پست صوتی برود.



خوب است بدانید!

حتی اگر شماره خصوصی داشته باشید یا در لیست "Do Not Call" ثبت باشید، همچنان ممکن است تماس های فریبکاری دریافت کنید.





فریبکاری های وب سایت

فریبکاران میتوانند آنلاین اظهار کنند که هر کسی باشند، از جمله دولت، یک تجارت واقعی، افراد مشهور یا دوستان یا فامیل شما.

آنها میتوانند وب سایت های جعلی ایجاد کنند تا شبیه مارک های معروف شوند. آنها ممکن است به نام افراد مشهور تظاهر کرده به نظر برسند که در حال تایید اجناس یا خدمات هستند. این وب سایت ها میتوانند حاوی نظرات جعلی باشند تا اعتماد تان را کسب کنند.

ممکن است هنگام آنلاین بودن، شعارهای تبلیغاتی جعلی یا پنجره های حاوی از هشدارهای جعلی یا پیام های خطا را مشاهده کنید.

نشانه هاییکه یک وب سایت ممکن است فریبکاری باشد

وب سایت:

اچناس را با قیمت های بسیار پایین تر از حد معمول یا در مقایسه با سایت های دیگر برای فروش ارائه میکند.



به شما درباره راهی برای کسب درآمد سریع و آسان با خطر یا تلاش کم میگوید.



حاوی یک هشدار یا پیام خطای فوری است که از شما میخواهد 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 میتوانید برای جلوگیری از فریبکاری وب سایت انجام دهید

1. قیمت ها را مقایسه کنید. اگر پیشنهادی فراتر از حقیقت به نظر میرسد، احتمالاً واقعیت ندارد.



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 تجارت و کلمه «فریبکاری» یا «نظرها» را جستجو کنید.



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



5. با فعال کردن «به روزرسانی های خودبخود» برای سیستم عامل و برنامه های کاربری خود، دستگاهی را که برای خرید آنلاین استفاده می کنید به روز نگه دارید.



خوب است بدانید!

روش های عملی برای محافظت از خودتان به صورت آنلاین در www.cyber.gov.au در دسترس است.





فریکاری های مبتنی بر رسانه های اجتماعی، برنامه های کاربری و پیام رسانی آنلاین

اگر فردی که نمی شناسید در رسانه های اجتماعی، یک برنامه پیام رسانی مانند واتس اپ یا وی چت یا از طریق یک برنامه کاربری دیگر با شما تماس میگیرد، ممکن است فریکاری باشد.

فریکارانیکه که اظهار میکنند شخص دیگری هستند، بیشتر از عکس واقعی شخص یا لوگوی رسمی سازمانی که اظهار میکنند هستند استفاده میکنند تا تشخیص فریکاری را سخت تر کنند.

فریکاران در رسانه های اجتماعی حساب های جعلی ایجاد میکنند و اظهار میکنند که از دولت، یک تجارت واقعی، صاحب کار، شرکت سرمایه گذاری یا حتی یک دوست، عضو فامیل یا علاقه مند روماتیک شما هستند.

آنها ممکن است خود را جعل افراد مشهور کنند و به نظر برسد که در حال تبلیغ اجناس یا خدمات هستند.

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

نشانه های فریبکاری در رسانه های اجتماعی یا برنامه کاربری

حساب رسانه های اجتماعی یا برنامه کاربری:

به شما درباره راهی برای کسب درآمد سریع و آسان با خطر یا تلاش کم میگوید.



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



درخواست انتقال مکالمه از یک برنامه مانند دوستیابی به پیام یا ایمیل خصوصی را میکند.



پیشنهاد میکند که یک شخص معروف محصول یا خدماتی را تایید یا حمایت کند.



میگوید شخصی چیزی را که شما می فروشید بدون اینکه اول آن را ببیند و با قیمت بالا خریداری میکند.



تهدید میکند که تصویر خصوصی شما را به اشتراک میگذارد مگر اینکه پولی به آنها بپردازید.



با شما تماس میگیرد تا کاری پیشنهاد کند.



خوب است بدانید!

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



اقداماتی که میتوانید برای جلوگیری از فریبکاری های مبتنی بر رسانه های اجتماعی و برنامه های کاربری انجام دهید

1. بررسی کنید که آیا حساب ممکن است جعلی باشد. آیا این حساب فعال است؟ آنها چند دوست/تعقیب کننده دارند و چقدر آنلاین پُست میگذارند؟



2. نام حساب را به همراه کلمه «scam» به صورت آنلاین جستجو کنید.



3. هرگز کاری را که به شما پیشنهاد شده است بدون مصاحبه یا بحث در مورد تجربه، شایستگی و مراجع خود قبول نکنید. در مورد استخدام کننده و تجارت یا فردی که این وظیفه را پیشنهاد میکند تحقیق کنید. از طریق شماره تلفون هایی که از یک جستجوی اینترنتی مستقل دریافت کرده اید، با سازمان کارایی تماس بگیرید. فقط برای تضمین وظیفه 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 بخش هشدارهای سرمایه گذاران سازمان بین المللی کمیسیون اوراق بهادار (IOSCO) نباشد.



5. هرگز به کسی که فقط آنلاین با او آشنا شده اید پول ندهید. فریبکاران بیشتر اوقات میگویند که در خارج از کشور زندگی میکنند و نمی توانند شخصاً شما را ملاقات کنند.



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



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



فریبکاری های برتر که باید درباره آنها بدانید

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

فریبکاری های جعل هویت

فریبکاران شما را فریب می دهند تا فکر کنید از سازمان های قابل اعتمادی مانند پولیس، دولت، بانک ها و تجارت های معروف هستند. آنها حتی میتوانند اظهار کنند که دوست یا عضو فامیل شما هستند. فریبکاران با ارسال ایمیل یا پیام های جاسوسی (phishing)، معلوماتی را درباره شما جستجو میکنند. اینها برای سرقت اطلاعات شما طراحی شده اند. آنها تلاش میکنند با اظهار کردن اینکه آنها از یک سازمان رسمی یا شخصی که می شناسید و به آن اعتماد دارید، شما را متقاعد میکنند که اطلاعات شخصی خود را به آنها بدهید.

فریبکاران از تکنالوژی استفاده میکنند تا به نظر برسند تماس ها یا پیام هایشان از یک شماره تلفون قانونی است. آنها میتوانند پیام های نوشتاری را در همان سلسله مکالمه به عنوان پیام های واقعی از یک سازمان نشان دهند.

فریبکاری های سرمایه گذاری

فریبکاران از بازاریابی متقاعد کننده و تکنالوژی جدید استفاده میکنند تا پیشنهاد سرمایه گذاری خود را آنقدر خوب جلوه دهند که نمیتوان آنرا از دست داد. آنها به شما قول سودهای بزرگ با خطر کم یا بدون خطر میدهند. آنها اکثراً از تکتیک های فشار استفاده میکنند تا شما را مجبور کنند سریع عمل کنید تا بتوانند پول شما را بدزدند.

فریبکاری های وظیفه ای و کارمندی

فریبکاران وظیفه های را پیشنهاد میکنند که تلاش کم و درآمد خوبی دارند. آنها اظهار میکنند که از طرف شرکت های مطرح و صفحه های فروشات آنلاین استخدام میکنند. گاهی اوقات، وظیفه ای که اعلان میکنند حتی وجود ندارد. فریبکاران همچنین جعل هویت دفتر های کارایی مطرح شده را میکنند. هدف آنها سرقت پول و اطلاعات شخصی شما است. آنها ممکن است از شما بخواهند که از قبل پول بپردازید تا بتوانید برای آنها کار کنید.

فریبکاری های اجناس و خدمات

فریبکاران به عنوان خریدار یا فروشنده ظاهر میشوند تا پول شما را بدزدند. آنها وب سایت ها یا حساب های جعلی را در سایت های فروشندگان قانونی میسازند و اجناس یا خدمات را با قیمت هایی پیشنهاد میکنند که برای واقعی بودن غیر قابل باور است. آنها تبلیغات جعلی و نظریات جعلی پُست میکنند. آنها ممکن است از لوگو های دزدیده شده، نام حوزه ای **com.au** و شماره تجاری استرالیایی (**ABN**) دزدیده شده استفاده کنند. تشخیص این فریبکاری ها سخت است.

فریبکاران همچنین به عنوان تجارت های ظاهر میشوند که شما آنها را می شناسید و به آنها اعتماد دارید تا بیل های جعلی را برای شما ارسال کنند. آنها حتی میتوانند جزئیات بیل های قانونی را تغییر دهند تا مشتریان به جای شما به فریبکاران پرداخت کنند.

فریبکاری های عاشقانه

فریبکاران از وعده عشق، ملاقات یا دوستی برای سرقت پول شما استفاده میکنند. آنها تمام تلاش خود را میکنند تا شما را متقاعد کنند که این رابطه واقعی است و از شما استفاده میکنند تا به آنها پول بدهید.

فریبکاران شما را در رسانه های اجتماعی، برنامه های دوستیابی یا برنامه های کاربری و وب سایت های بازی پیدا میکنند. آنها همچنین ممکن است برای شما پیام یا ایمیل ارسال کنند. آنها پشت حساب ها و هویت های جعلی، گاهی اوقات افراد مشهور، پنهان می شوند. هنگامی که به آنها اعتماد کردید، آنها یک «اضطراب» خواهند داشت و از شما کمک میخواهند. این اکثراً درخواست پول یا سایر اجناس خواهد بود.

فریبکاری های تهدید و اخاذی

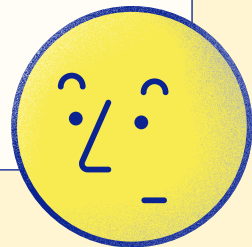
فریبکاران اظهار میکنند که از یک سازمان قابل اعتماد هستند و ادعا میکنند که باید پول بپردازید وگرنه اتفاق بدی رخ خواهد داد. اگر موافقت نکنید که فوراً به آنها پرداخت کنید، آنها ممکن است شما را با دستگیری، اخراج یا حتی آسیب جسمی تهدید کنند.

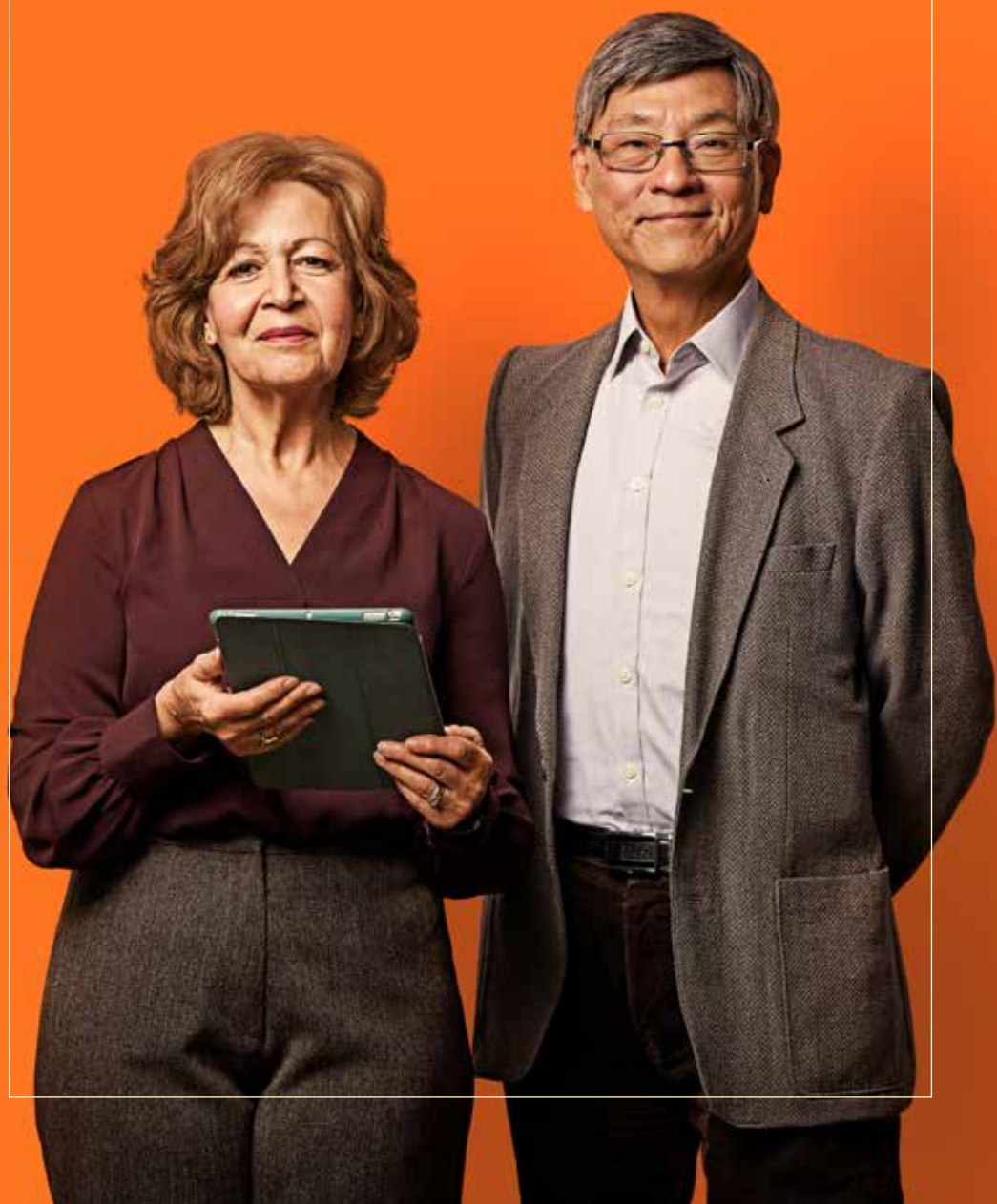
آنها همچنین میتوانند با تهدید به اشتراک گذاری تصاویر برهنه یا ویدیوهایی که برای آنها ارسال کرده اید، از شما باج گیری کنند، مگر اینکه برای آنها پول ارسال کنید.

فریبکاری های غیرمنتظره پول

فریبکاران تلاش میکنند شما را متقاعد کنند که از شما قرض دار اند یا مستحق پول یا جایزه ای هستید که انتظار دریافت آنرا نداشتید.

فریبکار از شما میخواهد قبل از دریافت پول یا جایزه، مبلغی را پرداخت کنید یا اطلاعات بانکی یا هویتی خود را بدهید. متأسفانه پول رایگانی وجود ندارد.





کجا میتوان فریبکاری ها را گزارش داد؟

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

ما اطلاعات گزارش های فریبکاری را به اشتراک میگذاریم و با دولت، مجری قانون و بخش خصوصی برای ایجاد اختلال و جلوگیری از فریبکاری کار میکنیم.

با گزارش دادن به Scamwatch به دیگران کمک کنید. تجربه فریبکاری خود را از طریق فورم گزارش در وب سایت www.scamwatch.gov.au Scamwatch گزارش دهید.

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

■ اگر پول خود را به یک فریبکار از دست داده اید، با بانک یا فراهم کننده کارت خود تماس بگیرید.

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



کمک و حمایت بیشتر

قربانی یک فریبکاری بودن میتواند احساس طاقت فرسای داشته باشد. مهم است که به یاد داشته باشید که این ممکن است برای هر کسی اتفاق بیفتد و کمک در دسترس است.

اگر شما یا شخصی که میشناسید مورد فریبکاری قرار گرفته اید، در مورد آن با کسی صحبت کنید. میتوانید از فامیل، دوستان، داکتر فامیلی یا یکی از خدمات حمایت زیر کمک بگیرید.

Lifeline (لایف لاین): 13 11 14 | lifeline.org.au

یا گفتگوی کمک بحران آنلاین (24 ساعت شبانه روز، 7 روز هفته)

Beyond Blue (بیاند بلو): 1300 22 4636 | beyondblue.org.au

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

Kids Helpline (خط کمک کودکان): 1800 55 1800 | kidshelpline.com.au

(24 ساعت شبانه روز، 7 روز هفته)

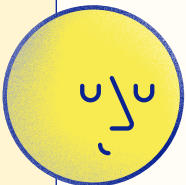
تأثیرات مالی فریبکاری ها میتواند ویرانگر باشد و زندگی را تغییر دهد.

اگر با مشکلات مالی مواجه هستید، میتوانید از طریق خط کمک ملی قرضه

National Debt Helpline با یک مشاور مالی صحبت کنید:

1800 007 007 از ساعت 9:30 صبح الی 4:30 بعد از ظهر، دوشنبه الی جمعه

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



scamwatch.gov.au