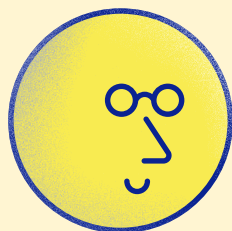


Како да препознаете и избегнете измами



Вашиот водич
за заштита од измами



Australian Government



National
Anti-Scam
Centre



ScamWatch
Stop. Better safe than scammed.

Признание на земјата

АССС им оддава признание на традиционалните сопственици и старатели на земјата низ Австралија и ја препознава нивната постојана поврзаност со копното, морето и заедницата. Ги почитуваме нив и нивните култури, како и нивните старешини – минати, сегашни и идни.

Australian Competition and Consumer Commission
Ngunnawal
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Комонвелт на Австралија 2023 г.

Ова дело е со заштитени авторски права. Покрај секоја негова употреба дозволена според Законот за авторски права од 1968 г. (Copyright Act 1968), целиот материјал содржан во ова дело е обезбеден согласно австралиската лиценца според Creative Commons Attribution 4.0, со исклучок на следното:

- грбот на Комонвелтот
- логата на АССС и АЕР
- сите илустрации, дијаграми, фотографии или графикони за кои Австралиската комисија за конкурентност и потрошувачи не поседува авторски права, но кои може да бидат дел од или се содржани во оваа публикација.

Поединости за условите на соодветната лиценца може да се најдат на веб-страницата на Creative Commons, каде што се наоѓа и целиот правен код за лиценцата CC BY 4.0 AU.

Барањата и прашањата во врска со умножување и права врз изданието треба да се упатат до Director, Corporate Communications, АССС, GPO Box 3131, Canberra ACT 2601.

Важна забелешка

Информациите во оваа публикација се дадени само за општи информативни цели. Тие не претставуваат правен или друг професионален совет и не треба да се толкуваат како законска изјава во која било јурисдикција. Бидејќи ова дело е наменето само како општ водич, тоа може да содржи генерализации. Треба да добиете професионален совет доколку сте загрижени за некоја специфична работа.

АССС ги вложи сите напори во разумни граници да обезбеди тековни и точни информации, но не ја гарантира нивната точност, навременост или комплетност.

Странките кои сакаат повторно да ги објават или на друг начин да ги користат информациите во оваа публикација мора да ја потврдат навременоста и точноста на овие информации пред да ги објават. Ова треба да се направи пред секое издание на публикацијата, бидејќи упатствата на АССС и релевантните преодни закони често се менуваат. Сите прашања што ги имаат странките треба да ги упатат до Director, Corporate Communications, АССС, GPO Box 3131, Canberra ACT 2601.

АССС 05/24_24-13

www.accc.gov.au

Содржина

Достапна е помош	1
Што е измама	3
Едноставни чекори за препознавање и избегнување на измами	4
Измами преку текстуални или СМС пораки	7
Измами преку имејл	11
Измами преку телефон	15
Измами преку веб-страници	19
Измами преку социјалните мрежи, апликации и онлајн пораки	23
Најчестите измами за кои треба да знаете	27
Каде да пријавите измами	31
Повеќе помош и поддршка	33



Овој водич го подготви Националниот центар за борба против измами и ќе ви помогне да препознаете и да се заштитите од штета предизвикана од измами.

Измамата е кривично дело и луѓето кои вршат измами се криминалци. Многу луѓе во Австралија се измамени и губат пари, понекогаш дури и нивната животна заштеда. Измамите ги повредуваат луѓето.

Измамите сè потешко се откриваат, па затоа треба да работиме заедно за да ги спречиме.

Националниот центар за борба против измами работи на тоа да ги заштити Австралијците од измами.

Работиме со владата и индустријата за да најдеме нови начини да ги спречиме измамниците да крадат пари и лични податоци од Австралијците. Следуваат неколку начини на кои го постигнуваме тоа.

Им помагаме на луѓето да препознаваат и избегнуваат измами

Преку Scamwatch, споделуваме најнови информации за измами и начините на кои можете да се заштитите од измами.

Им ја отежнуваме работата на измамниците

Со собирање и споделување информации помеѓу владата и индустријата, им отежнуваме на измамниците да продолжат со нивните злосторства и им олеснуваме на луѓето да пријавуваат измами.



Достапна е помош

Ако го читате ова, големи се шансите дека вие, или некој кого познавате, сте биле измамени. За жал, не сте сами. Измамите стануваат се пософистицирани, што значи дека секој може да биде измамен.

Ако сте биле измамени, важно е брзо да реагирате.

Ако сте изгубиле пари поради измамник, контактирајте ја вашата банка или издавач на картичка.

Контактирајте со IDCARE, [1800 595 160](tel:1800595160), www.idcare.org.

Измамите успеваат бидејќи изгледаат како вистински работи. Измамниците се потпираат на тоа дека не ги забележувате предупредувачките знаци затоа што брзате, затоа што нешто изгледа како добра понуда што не сакате да ја пропуштите или затоа што таа изгледа како да е од некој во кој имате доверба.

Заштитете се од измами следејќи ги овие 3 чекори:

Застанете



Не давајте пари или лични податоци на никого ако не сте сигурни.

Измамниците ќе ви понудат помош или ќе побараат да потврдите кој сте. Тие ќе се преправаат дека се од организации што ги познавате и на кои им верувате, како што се даватели на услуги, полицијата, вашата банка или државни служби.

Проверете



Запрашајте се – дали пораката или повикот можеби се лажни?

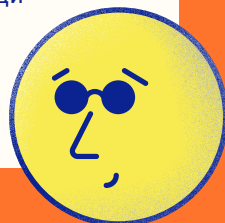
Никогаш не кликувајте на линк (врска) во порака. Контакттирајте само со компании или владата користејќи ги податоците за контакт што ќе ги најдете на нивната официјална веб-страница или апликација. Ако не сте сигурни, кажете „не“, прекинете го телефонскиот разговор или избришете ја пораката.

Пријавете



Реагирајте брзо ако мислите дека нешто не е во ред.

Контактирајте со вашата банка ако забележите невообичаена активност или ако некој измамник ги земе вашите пари или податоци. Побарајте помош и пријавете ја изматата на ReportCyber и Scamwatch. Кога пријавувате измами, им помагате на сите Австралијци со зајакнување на нашата одбрана од измами.



Што е измама

Измама е кога некој ќе ве излаже за да ви ги украде парите или личните податоци.

Измамите се економски кривични дела што ги извршуваат криминалци кои често се многу организирани и софистицирани.

Измамите:

-  ги извршуваат криминалци
-  изгледаат реално
-  проследени се со реални приказни
-  вршат притисок врз вас да дејствувате

Измамата НЕ е:

-  Хакерски упад на компјутер
-  Неправедни услови на договор
-  Вознемирувачки маркетинг пристапи

Важно е да се запамети дека сите негативни искуства не се измами. Можеби сте платиле за производ што никогаш не сте го добиле или сте купиле нешто и сте забележале дека квалитетот е слаб. Иако ова е разочарувачки, тие не се нужно измами. Австралискиот закон за потрошувачи (Australian Consumer Law) им нуди заштита на австралиските потрошувачи при вакви проблеми.

За повеќе информации, посетете www.accc.gov.au/consumers

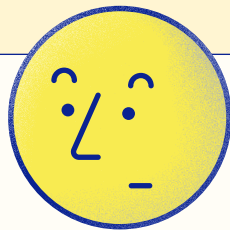
Едноставни чекори за препознавање и избегнување на измами

Измамите можат да ни се случат на сите нас. Измамите се успешни затоа што измамниците создаваат реални приказни за да ви украдат пари и да земат ваши лични податоци.

Измамниците стануваат сè попаметни и користат нови технологии, производи, услуги и големи настани за да ве убедат дека нивните измами се реални.

Може да биде многу тешко да се препознае измама. Следуваат неколку ситуации на кои треба да внимавате. Понекогаш измамниците користат комбинација од овие тактики.

- 1. Можности да заработите или заштедите пари:** Измамниците ќе ве излажат за да верувате дека добивате неверојатна зделка или понуда. Ќе вршат притисок врз вас да дејствувате брзо за да не ја пропуштите можноста. Запомнете дека понудите што изгледаат премногу добри за да бидат вистинити, обично не се добри.
- 2. Тажни приказни и повици за помош:** Измамниците ќе се обидат вашата добрина да ја искористат против вас. Тие ќе споделат со вас приказни за неизмерна тага и трагедија и ќе објаснат зошто им е потребна вашата помош и вашите пари.
- 3. Линкови и прилози:** Измамниците користат линкови за да ве упатат до лажни веб-страници дизајнирани да ги украдат вашите податоци и пари. Измамниците исто така може да побараат од вас да отворите прилози (attachments). Преку овие прилози може да се инсталираат вируси кои ги крадат вашите податоци.



- 4. Притисок за брзо дејствување:** Измамниците не сакаат да почекате и да размислите. Сакаат да ве натераат да дејствувате брзо. Ова може да вклучува закани дека нешто лошо ќе се случи ако не дејствувате брзо.
- 5. Барања да платите на невообичаени или посебни начини:** Измамниците честопати бараат од вас да платите користејќи несекојдневни методи како, на пример, со однапред платени платежни картички (preloaded debit cards), iTunes картички или криптовалути како што е биткоинот. Откако ќе се потрошат тие пари, не можете да ги вратите.
- 6. Барање да отворите нови сметки или PayPal:** Измамниците може да побараат од вас да отворите нова банковна сметка или PayPal за да им платите (или тие да ви платат). Тие може да се преправаат дека се од вашата банка и да побараат од вас да ги префрлите вашите пари на нови сметки за да бидат безбедни.

Ако измамниците успеале да ви ги земат парите, ќе се обидат да добијат повеќе пари од вас. За жал, секоја трета жртва на измама била измамена повеќе од еднаш. Ако сте изгубиле пари со измама, внимавајте на измамници кои нудат да ви помогнат да ги вратите парите. Ова е друг вид на дополнителна измама.



Измами преку текстуални или СМС пораки

Измамниците испраќаат пораки преправајќи се дека се од владата, органи за спроведување на законот, веродостојни компании, па дури и ваши роднини или пријатели.

Овие пораки ќе изгледаат итни и ќе се обидат да ве поттикнат да дејствувате брзо. Тие често содржат линк што ќе ве однесе до лажна веб-страница. Измамниците можат да украдат какви било лични податоци внесени на овие лажни веб-страници и да ги користат за да ви ги земат парите или да извршат измама во ваше име.

За да направат овие пораки да изгледаат како вистински, измамниците го копираат или кријат нивниот телефонски број зад телефонскиот број и идентификацијата на повикувач (caller ID) на легитимни компании или луѓе кои ги познавате.

Лажните пораки дури може да се појават во истата низа на пораки како вистински пораки од организацијата, што прави да биде уште потешко да се препознаат.

Знаци дека некоја порака можеби е измама

Во пораката:



Се бара од вас итно да дејствувате, да извршите плаќање или да префрлите пари.



Се бара од вас да кликнете на врска или да се јавите на број наведен во пораката.



Се бара од вас да се најавите на онлајн сметка со вашето корисничко име и лозинка или да дадете други лични податоци.



Таа е од член на семејството или пријател во која се вели дека неговите/нејзините податоци за контакт се променети.



Содржи закана дека некоја услуга ќе биде прекината или дека ќе ви биде наплатено ако не дејствувате.



Се сугерира дека вие или вашите сметки сте биле хакирани или вклучени во измама.



Се сугерира дека има проблем со вашето плаќање или со испораката на вашиот пакет.

Чекори како да се заштитите од пораки кои содржат измами



1. Ако некое лице што го познавате ви испрати порака за да каже дека има нов телефонски број:
 - а. обидете се да го повикате на постоечкиот број што го имате за него и
 - б. испратете му порака на новиот број со прашање на кое само тој/таа ќе го знае одговорот, за да потврдите дека е тој/таа.
-



2. Никогаш не кликувајте на линкови во пораки.
-



3. Ако пораката е поврзана со веб-страница, не кликувајте на линкот. Наместо тоа, самите пронајдете ја веб-страницата на интернет или користете ја официјалната апликација.
-



4. Не одговарајте на текстуална порака на наведениот телефонски број.
-



5. Јавете се на организацијата или лицето на телефонскиот број што самите сте го нашле, на пример, од веб-страницата на организацијата.
-



Измами преку имејл

Измамниците испраќаат имејли преправајќи се дека се од владата, органите за спроведување на законот и компании. Оставаат впечаток дека се работи за нешто итно за да ве натераат да дејствувате брзо.

Измамниците го користат истото лого и слична имејл адреса како вистинската организација. Измамниците, исто така, може да ја копираат или прикријат нивната имејл адреса зад имејл адресата на организацијата или компанијата за да направат измамничкиот имејл да изгледа пореален.

Знаци дека некој имејл може да биде измама

Со имејлот:



Се бара исплата, но податоците за сметката се нови или променети од последната исплата што сте ја направиле.



Се бара од вас да се најавите на онлајн сметка со вашето корисничко име и лозинка или да дадете други лични податоци.



Имејлот е неочекуван и вклучува прилог со покана да го отворите.



Се бара од вас да ги потврдите вашите банкарски податоци за да ви бидат вратени или исплатени пари што не ги очекувате.



Се тврди дека има информации за вас или ваши слики и се заканува дека ќе ги објави.



Ви се нуди помош да ви бидат вратени пари или да добиете обештетување поради повреда на правото на заштита на личните податоци (data breach) или кражба на идентитет.

Чекори кои можете да ги преземите да се заштитите од измами преку имејл

1. Потврдете дека имејлот е вистински така што:



- а. ќе го контактирате лицето или организацијата директно, користејќи ги податоците за контакт што самите сте ги нашле, на пример, на веб-страницата на организацијата или
- б. ќе пристапите до организацијата преку нејзината официјална апликација (никогаш преку линк).



- ### 2. Веднаш прекинете ги сите контакти со секој што се обидува да ви се заканува или да ве заплашува.

- ### 3. Никогаш не давајте лични податоци или не плаќајте на некој што ви нуди:



- а. обештетување или помош да си ги вратите парите од претходна измама или повреда на правото на заштита на личните податоци или
- б. добивки, награди или наследство.



- ### 4. Кога можете, користите мулти-фактор автентикација. Таа обезбедува дополнителен слој на заштита и значи дека измамникот треба да ја знае вашата лозинка за имејл и PIN-бројот испратен на вашиот телефон за да добие пристап до вашата имејл сметка.



Измами преку телефон

Измамниците се јавуваат и тврдат дека се од добро познати организации. Ова вклучува државни организации, органи за спроведување на законот, инвестициски и правни фирми, банки и даватели на телекомуникациски услуги.

Оставаат впечаток дека се работи за нешто итно, за да ве натераат да дејствувате брзо. Тие може да се обидат да ве убедат да им ги дадете вашите лични податоци или податоците за вашата банковна сметка или да им дадете пристап до вашиот компјутер.

Повикувачот можеби веќе има некои податоци за вас, како што се вашето име или адреса, што прави повикот да изгледа вистински.

Знаци дека некој телефонски повик може да биде измама

Повикувачот:



Бара исплата или бара да префрлите пари на нова сметка.



Ја бара вашата лозинка, PIN-број, еднократен код или други безбедносни податоци.



Ги бара вашите финансиски податоци, како што се податоци за вашата кредитна картичка или банкарски податоци.



Бара од вас да направите нешто на вашиот мобилен телефон или компјутер, на пример, да инсталирате софтвер или да пристапите до безбедна сметка.



Тврди дека е од органите за спроведување на законот и ви се заканува со итно апсење или депортирање.



Вели дека вашата банковна или други онлајн сметки биле хакирани или вклучени во измама.

Чекори кои можете да ги преземите да се заштитите од измами преку телефон

1. Потврдете дека повикот е вистински со тоа што:



- a. ќе го контактирате лицето или организацијата директно, користејќи ги податоците за контакт што самите сте ги нашле, на пример, на веб-страницата на организацијата или
- б. ќе пристапите до организацијата преку нејзината официјална апликација (никогаш преку линк).



2. Ако не знаете кој е повикувачот или ако ви се заканува или заплашува, веднаш прекинете го телефонскиот разговор.



3. Никогаш не инсталирајте софтвер што на некој му дава пристап до вашиот компјутер или уред.



4. Можете да игнорирате повици од броеви што не ги знаете или да ги оставите да одат во говорната пошта.



Добро е да се знае!

Сè уште може да примате лажни повици дури и ако имате скриен број или сте регистрирани во регистарот „Не се јавувај“ (Do Not Call register).



Измами преку веб-страници

Измамниците можат да се преправаат онлајн дека се кој било, вклучително од владата, вистинска компанија, познати личности или вашите пријатели или роднини.

Тие можат да креираат лажни веб-страници за да изгледаат како добро познати брендови. Тие може да се претставуваат како познати личности и да оставаат впечаток дека поддржуваат некои производи или услуги. Овие веб-страници може да содржат лажни позитивни коментари за да ве измамат да им верувате.

Може да видите лажни реклами или прозорчиња (pop-up windows) кои содржат лажни предупредувања или пораки за грешки кога сте онлајн.

Знаци дека некоја веб-страница може да содржи измама

На веб-страницата:



Се нуди продажба на артикли по значително пониски цени од вообичаените или во споредба со други веб-страници.



Ви покажува како да заработите пари брзо и лесно, со мал ризик или напор.



Содржи итно предупредување или порака за грешка со која се бара да кликнете на линкот.



Се бара плаќање на невообичаен или специфичен начин, на пример со картички за подароци или криптовалути како што е биткоинот.



Има само позитивни коментари.

Чекори кои можете да ги преземете да избегнете измама на веб-страница



1. Споредете ги цените. Ако понудата е премногу добра за да биде вистинита, тогаш веројатно не е.



2. Пребарајте информации за организацијата или лицето со кое имате работа пред да ги дадете вашите пари или лични податоци.



3. Не верувајте во коментари што се напишани на самата веб-страница. Пребарајте ја веб-страницата или името на компанијата и зборот „scam“ („измама“) или „reviews“ („коментари“).



4. Ако на вашиот екран се појави порака со предупредување или грешка, не кликувајте на неа, туку одете директно на апликацијата на која тоа се однесува за да проверите дали е вистинска.



5. Ажурирајте го уредот што го користите за онлајн купување со вклучување на „automatic updates“ („автоматски ажурирања“) за вашиот оперативен систем и апликации.



Добро е да се знае!

Практични начини да се заштитите онлајн се достапни на www.cyber.gov.au



Измами преку социјалните мрежи, апликации и онлајн пораки

Ако некој што не го познавате ве контактира на социјалните мрежи, на платформа за пораки како што се WhatsApp или WeChat или преку апликација, тоа може да биде измама.

Измамниците кои се преправаат дека се некој друг, често ја користат вистинската фотографија на личноста или официјалното лого на организацијата која се преправаат дека ја претставуваат, за да го отежнат препознавањето на измамата.

Измамниците на социјалните мрежи ќе отворат лажни профили и ќе се преправаат дека се од владата, вистинска компанија, работодавач, инвестициска компанија, па дури и пријател, роднина или личност за која сте романтично заинтересирани.

Тие може лажно да се претставуваат како познати личности и да оставаат впечаток дека промовираат производи или услуги.

Измамниците исто така можат да научат многу за вас од информациите што ги споделувате на вашите сметки на социјалните мрежи. Тие можат да ги користат овие информации за да се обидат да ги погодат лозинките на вашите сметки или да ве имаат за цел за други измами.

Знаци дека некоја социјална мрежа или апликација содржи измама

Сопственикот на профилот на социјалната мрежа или апликација:



Ви покажува како да заработите пари брзо и лесно, со мал ризик или напор.



Ве поканува да учествувате на натпревар или ви нуди понуда која трае ограничено време.



Бара да префрлите разговор од апликација, на пример од апликација за запознавање на партнери, во приватен разговор или имејл.



Сугерира дека позната личност одобрува или поддржува некој производ или услуга.



Вели дека некој ќе купи нешто што продавате без претходно да го види и тоа по повисока цена.



Се заканува дека ќе сподели приватна фотографија од вас, освен ако не му платите пари.



Ве контактира за да ви понуди работа.



Добро е да се знае!

Информации за тоа како да бидете безбедни на различни платформи на социјалните мрежи може да се најдат на www.esafety.gov.au.

Чекои кои можете да ги преземете за да избегнете измами на социјалните мрежи и апликации



1. Проверете дали профилот можеби е лажен. Дали сметката е активна? Колку пријатели/следбеници има и колку постови објавува онлајн?



2. Пребарајте го името на сопственикот на профилот онлајн заедно со зборот „scam“ („измама“).



3. Никогаш не прифаќајте работа што ви е понудена без да имате интервју или дискусија за вашето искуство, погодност и препораки. Проверете податоци за лицето кое нуди работа и компанијата или за поединецот што ја нуди позицијата. Контактирајте ја агенцијата за вработување преку телефонски броеви што сте ги нашле со независно пребарување на интернет. Не плаќајте пари однапред само за да обезбедите да добиете работа.



4. Примајте совети за инвестирање само од некој што поседува австралиска лиценца за финансиски услуги (Australian Financial Services license) и проверете дали компанијата или веб-страницата се наоѓа на порталот на Комисијата на Меѓународната организација за хартии од вредност (International Organization of Securities Commission's - IOSCO) за предупредувања за инвеститори.



5. Никогаш не давајте пари на лице што сте го запознале само онлајн. Измамниците честопати велат дека живеат во странство и дека не можат да се сретнат со вас лично.



6. Никогаш не испраќајте интимни слики од себе на некој што сте го запознале само онлајн.

За повеќе информации во врска со измами, вклучително и други начини на кои измамниците можат да ве контактираат, на пример, лично и по пошта, посетете го [Scamwatch](#).



Најчестите измами за кои треба да знаете

Следуваат неколку од најчестите видови на измами за кои треба да бидете свесни. Можете да најдете повеќе информации за секој од овие видови на измами, вклучително за знаците за предупредување и чекорите како да се заштитите, на веб-страницата на [Scamwatch](#).

Измами со лажно претставување

Измамниците ве лажат за да мислите дека се од доверливи организации како што се полицијата, владата, банките и добро познати компании. Тие дури може да се преправаат дека се ваш пријател или член на семејството. Измамниците бараат информации за вас така што ви испраќаат имејли или пораки во кои лажно се преставуваат (phishing). Тие се дизајнирани да ги украдат вашите податоци. Тие се обидуваат да ве убедат да им ги дадете вашите лични податоци преправајќи се дека се од официјална организација или некој што го познавате и во кој имате доверба.

Измамниците користат технологија за да направат нивните повици или пораки да изгледаат како да доаѓаат од легитимен телефонски број. Тие можат да направат текстуалните пораки да се појавуваат во истата нишка на разговор како вистинските пораки од некоја организација.

Инвестициски измами

Измамниците користат убедлив маркетинг и нова технологија за да направат нивната инвестициска понуда да звучи премногу добро за да се пропушти. Тие ви ветуваат големи дивиденди со мал или никаков ризик. Тие често користат тактики на вршење на притисок за да ве натераат да дејствувате брзо, за да можат да ви ги украдат парите.

Измами за работа и вработување

Измамниците нудат работа која е високо платена со малку труд. Тие се преправаат дека вработуваат во име на компании од висок профил и онлајн платформи за пазарење. Понекогаш работата што ја наведуваат не ни постои. Измамниците, исто така, се претставуваат лажно како добро познати агенции за вработување. Нивната цел е да ви ги украдат парите и личните податоци. Тие може да побараат од вас однапред да платите за да можете да работите за нив.

Измами со продукти и услуги

Измамниците се претставуваат како купувачи или продавачи, за да ви ги украдат парите. Тие отвараат лажни веб-страници или профили на легитимни веб-страници за малопродажба и нудат производи или услуги по цени што изгледаат премногу добри за да бидат вистинити. Тие објавуваат лажни реклами и лажни коментари. Тие може да користат украдени логоа, името на доменот „.com.au“ и украден австралиски деловен број (ABN). Тешко е да се препознаат овие измами.

Измамниците, исто така, се преправаат дека се компании што ги познавате и на кои им верувате, за да ви испраќаат лажни сметки. Тие дури можат да ги променат деталите на легитимни фактури, така што клиентите на крајот ќе му платат на измамникот наместо вам.

Романтични измами

Измамниците ветуваат љубов, состаноци или пријателство за да ви ги украдат парите. Тие прават сè за да ве убедат дека врската е вистинска и ве манипулираат да им дадете пари.

Измамниците ве наоѓаат на социјалните мрежи, апликациите и веб-страниците за запознавање на партнери или за игри. Тие исто така можат да ви испраќаат текстуални пораки или имејли. Тие се кријат зад лажни профили и идентитети, понекогаш на познати личности. Откако ќе стекнете доверба во нив, тие ќе имаат „итен случај“ и ќе побараат помош од вас. Тоа често се барања за пари или други производи.

Измами со закани и изнудување пари

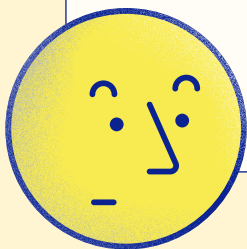
Измамниците се преправаат дека се од веродостојна организација и тврдат дека треба да платите пари или дека во спротивно ќе се случи нешто лошо. Тие може да ви се закануваат со апсење, депортирање или дури физичка повреда доколку не се согласите веднаш да им платите.

Тие исто така може да ве уценуваат со закана дека ќе споделуваат голи фотографии или видео записи што сте им ги испратиле, освен ако не им испратите пари.

Измами со неочекувани пари

Измамниците се обидуваат да ве убедат дека ви се должат пари или имате право на пари или добивки што не сте ги очекувале.

Измамникот бара од вас да платите наплата или да ги дадете вашите банкарски податоци или податоци за вашиот идентитет пред да можете да ги добиете парите или добивките. За жал, не постојат гратис пари.





Каде да пријавите измами

Работиме на тоа Австралија да стане потешка цел за измамниците преку подигање на свеста за тоа како да се препознаат, избегнуваат и пријавуваат измамите.

Споделуваме информации од извештаите за измами и работиме со владата, органите за спроведување на законот и приватниот сектор, за да ги попречиме и спречиме измамите.

Помогнете им на другите со тоа што ќе ги пријавите измамите на Scamwatch. Пријавете го вашето искуство со измама преку формуларот за пријавување на веб-страницата на Scamwatch, www.scamwatch.gov.au

Запамтете, ако сте жртва на измама, важно е брзо да реагирате.

- Ако сте изгубиле пари поради измамник, контактирајте ја вашата банка или издавач на картичка.
- Контактирајте со ID CARE: 1800 595 160 | idcare.org



Повеќе помош и поддршка

Да се биде жртва на измама може да биде неиздржливо. Важно е да се запамети дека ова може да му се случи на секого и дека е достапна поддршка.

Ако вие или некој што го познавате бил измамен, разговарајте со некого за тоа. Можете да побарате поддршка од семејството, пријателите, вашиот доктор по општа пракса (GP) или некоја од следните служби за поддршка.

Lifeline: 13 11 14 | lifeline.org.au

или преку онлајн разговор за поддршка при криза (24 часа во денот, 7 дена во неделата)

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

или преку онлајн разговор (24 часа во денот, 7 дена во неделата)

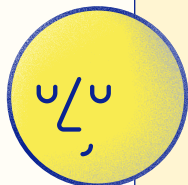
Kids Helpline: 1800 55 1800 | kidshelpline.com.au

(24 часа во денот, 7 дена во неделата)

Финансиските последици од измамите може да бидат поразителни и да ви го променат животот.

Ако имате финансиски потешкотии, можете да разговарате со советник за финансии преку Националната телефонска линија за помош околу долгови ([National Debt Helpline](https://nationaldebthelpline.org.au)) на:

1800 007 007 од 9:30 ч. наутро до 4:30 ч. попладне, од понеделник до петок, или ако се приклучите на „Разговор во живо“ (Live Chat) од 9:00 ч. наутро до 8:00 ч. навечер, од понеделник до петок.



scamwatch.gov.au