Малата црна книшка за измами

Џебен водич кој ви помага да можете да ги забележите, да ги избегнете и да се заштитите себеси од измамите

Малата црна книшка за измами

Џебен водич кој ви помага да можете да ги забележите, да ги избегнете и да се заштитите себеси од измамите

ISBN 978 1 920702 00 7

Австралиска комисија за конкурентност и потрошувачи
(Australian Competition and Consumer Commission)
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Федерална влада/Комонвелтот на Австралија 2016 г.

Ова дело претставува авторско право. Дополнително на секаква негова употреба дозволена согласно *Законот за авторски права од 1968 г.,* целиот материјал содржан во рамките на ова издание е обезбеден согласно австралиската лиценца според Creative Commons Attribution 3.0, со исклучок на следното:

- грботот на Федералната влада/Комонвелтот
- логото на Австралиската комисија за конкурентност и потрошувачи (ACCC) и логото на Регулаторното тело за енергетика на Австралија (AER)
- сите прикази, дијаграми, слики или графици за кои Австралиската комисија за конкурентност и потрошувачи не поседува авторски права, а кои може да претставуваат составен дел од или се содржани во ова издание.

Поединостите за условите за поседување на соодветната лиценца може да се најдат на местото на интернет на Creative Commons, а таму се наоѓа и целиот законик за лиценцата CC BY 3.0 AU.

Барањата и прашањата поврзани со умножување и права врз изданието треба да се упатат до Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601, или пак на местото на интернет publishing.unit@accc.gov.au.

ACCC 12/16_1129

www.accc.gov.au

Содржина

Вовед	2
Најчестите измами од коишто треба да се чувате	3
Измами со љубовни и романтични средби	4
Измами со инвестирање пари	6
Измами со закани и казни	8
Измама со неочекувани пари	10
Измами со награди и лотарија	12
Измами со купување преку интернет, со реклами и со наддавања	14
Измами насочени кон компјутерите и мобилните уреди	16
Крадење на идентитет	18
Измами со работни места и вработување	20
Измами за добротворни и медицински цели	22
Измами на компании	24
Како функционираат измамите—анатомија на една измама	26
Златното правило за да се заштитите себеси	32
Каде да најдете помош и поддршка	34
Каде да пријавите измама	36

Вовед

Секоја година измамите ги чинат Австралијците, бизнисите и економијата стотици милиони долари и причинуваат емоционална штета на жртвите и на нивните семејства.

Најдобар начин да се заштитите себеси е преку свесност и едукација за нивното постоење. Ова ново издание на *Малата црна книшка со измами* ви го овозможува Австралиската комисија за конкурентност и потрошувачи (ACCC), како национална агенција за заштита на потрошувачите. Малата црна книшка со измами е меѓународно признаена како важна алатка за потрошувачите и за малите бизниси за да дознаат за измамите од типот на:

- најчестите измами на кои треба да се внимава
- различните начини на коишто измамниците можат да стапат во контакт со вас
- алатките што ги користат измамниците за да ве измамат
- предупредувачките знаци
- како да се заштитите, и
- каде можете да побарате помош.

Малата црна книшка со измами може да се најде на интернет на www.accc.gov.au/littleblackbookofscams.

—пријавете се на местото Scamwatch

За да бидете секогаш еден чекор понапред од измамниците, осознајте повеќе на местото на интернет на Комисијата ACCC наречено Scamwatch—www.scamwatch.gov.au—таму можете да се пријавите преку бесплатни електронски пораки да добивате предупредувања за новите измами кои имаат за цел да ги измамат потрошувачите и малите бизниси. Scamwatch исто така можете да го следите и на Twitter на @scamwatch_gov или на http://twitter.com/scamwatch_gov.

Најчестите измами од коишто треба да се чувате

Сите се подложни на измами така што на сите им се потребни информации околу тоа како да препознаат измама и како да избегнат да бидат измамени. Некои луѓе мислат дека само лековерните и алчните стануваат жртви на измами. Вистината е дека измамниците се паметни и ако не знаете од што да се пазите, секој може да стане жртва на измама.

Дали сте примиле понуда што била предобра за да биде вистинита, можеби телефонски повик каде ви нудат да ви помогнат да го поправите компјутерот или пак некоја закана дека треба да платите пари што не ги должите, итно известување од вашата банка или добавувач на телекомуникациски услуги во врска со некаков проблем со вашата сметка, или дури и покана да 'станете пријатели' или да се поврзете со некого преку интернет? Измамниците знаат како да ве намамат за да го добијат тоа што го сакаат.

Стануваат сè попаметни, ги следат новитетите за да ги злоупотребат новите технологии, новите производи или услуги и најважните големи настани за да создадат приказни во коишто може да поверувате и кои ќе ве убедат да дадете пари или лични поединости.

Меѓутоа, благодарение на десетици илјади пријави за измами што пристигнуваат секоја година, Комисијата ACCC изготви список на чести измами за да ги разоткрие тајните и тактиките коишто измамниците не сакаат да ги знаете.

Измами со љубовни и романтични средби

Измамите со љубовни и романтични средби секоја година ја чинат Австралија милиони и можат да уништат единки и семејства.

Како функционира измамата

Измамниците кои работата со **љубовни и романтични средби** отвораат лажни профили на веродостојни места на интернет за љубовни средби, на мобилни апликации или пак на друштвени платформи како што е Facebook, притоа користејќи фотографии и идентитети што често пати се украдени од други лица. Ги користат овие профили за да пробаат да почнат врска со вас и тоа може да трае со месеци или дури и со години, само со цел да дојдат до вашите пари. Измамникот ќе побара пари за да му се помогне со некаква болест, повреда, патни трошоци или пак некаква криза во семејството. Тие се бесчувствителни и ќе ве лажат за да ја искористат вашата добрина.

Измамниците обично се некаде во странство и имаат изговор зошто се таму, на пример дека отслужуваат воен рок, дека работат како инженери или пак дека се грижат за некој пријател или за роднина. Тие никој пат не се тоа што се претставуваат дека се, а некои итри измамници може дури и да ви праќаат мали подароци. Тоа е само дел од нивниот голем план за подоцна од вас да извлечат повеќе пари.

Заштитете се

- Никогаш не му праќајте пари и не му откривајте лични поединости на некого кој само што сте го запознале преку интернет.
- Внимавајте кога некој ваш обожавател од интернет бара да комуницирате надвор од платформата за љубовни средби или друштвена мрежа после само неколку ‘контакти’ или разговори – може да се работи за измамник.
- Пребарајте слики од вашиот обожавател за да утврдите дали навистина се работи за оној кој се вели дека е. Можете да користите сервис за пребарување слики како што е Google или пак TinEye.
- Бидете внимателни кога споделувате интимни фотографии или видеа преку интернет. Измамниците се познати по тоа што ги уценуваат своите жртви со користење слики или видеа од вас коишто вие не сакате никој друг да ги види.

Измами со инвестирање пари

‘Инвестирање пари без ризик’ или пак можност за несреќа?

Како функционира измамата

Измамите со инвестирање пари доаѓаат во многу облици како што се купување на крипто валути, тргување со бинарни опции, деловни вложувања, шеми за пензионирање, управувани фондови и продажба или купување акции или имот. Со цел да ги прикријат своите лажни дејствија измамниците ги маскираат ‘можностите за заработка’ со брошури и места на интернет што изгледаат професионално. Често пати почнуваат со ненадеен телефонски повик или електронска порака од измамникот кој нуди некоја можност ‘што не се пропушта’, или ‘ќе донесе огромен поврат на пари’ или ‘загарантирано успева’. Измамниците обично работат од странство и не поседуваат австралиска лиценца за финансиски услуги.

Измамите со компјутерски софтвери за предвидување ви ветуваат дека точно ќе ги предвидат движењата на берзите, резултатите од трки со коњи, од спортски натпревари или пак од лотарија. Тие едноставно претставуваат еден облик на коцкање маскирано во инвестиции. Повеќето од овие шеми или програми не работат и купувачите не можат да си ги повратат парите. Во многу од случаите давателот на услугата едноставно исчезнува.

Измамите со пензии ви нудат порано да ги земете парите од заштедениот фонд од вториот задолжителен пензиски столб, често во облик на пензиски фонд што лично го управувате или пак за одреден надоместок. Измамникот може да побара да се согласите на некоја приказна што ќе ви овозможи порано пуштање на вашите пари од фондот и тогаш, во улога на ваш финансиски советник, ќе го измами вашиот пензиски фонд да му ги исплати парите од вашиот фонд директно на него. Откако ќе ги добие вашите пари, измамникот може да ви наплати огромен 'надоместок' за услугата или пак да ви украде сè.

Заштитете се

- Не дозволувајте никој да ве притиска да донесувате одлуки во врска со вашите пари или инвестиции – особено ако се работи за ненадејна понуда.
- Пред да ги дадете парите, самите истражете ја компанијата за инвестиции и проверете на www.moneysmart.gov.au за да видите дали поседува австралиска лиценца за финансиски услуги. Запрашајте се: ако некој странец знае тајна како да се заработат пари, зошто би ја споделил со други?

Ако уште не сте во години за пензионирање, внимавајте на понудите што нудат лесно пристапување до парите од вашиот заштеден фонд од вториот задолжителен пензиски столб. Ако порано и противзаконски пристапите до парите за вашата пензија, може да треба да плаќате казни согласно даночниот законик.

Измами со закани и казни

Ако некое владино тело или пак позната компанија ви побара да платите пари за нешто, застанете, размислете и два пати проверете за што се работи.

Како функционира измамата

Наместо да ви нудат некоја награда, пари или попуст, овие измами користат закани создадени да ве исплашат за да им ги дадете парите. Измамникот може да ви се јави и да ви се закaнува со **апсење** или пак да ви прати електронска порака во којашто тврди дека должите пари за **казна за брзо возење, некој долг кон управата за даноци** или пак некоја **неплатена сметка.**

За време на телефонскиот повик измамникот ќе ве притиска веднаш да платите и ќе ви каже дека ако одбиете да платите дома ќе ви дојде полиција. Измамниците се познати по тоа што целат на ранливи луѓе во нашата заедница, како што се новопристигнатите доселеници. Се преправаат дека се службеници од Одделот за доселеништво и на жртвите им се заканувaат со **депортирање** доколку не платат надоместок за да се исправат грешките во нивните визи за престој. Има една многу слична измама каде измамникот се преправа дека е од австралиската даночна управа и им кажува на жртвите дека имаат неплатен долг за данок.

Измамниците исто така се преправаат дека се некоја **сигурна и етаблирана компанија** како што се вашите даватели на банкарски услуги, гас, електрична енергија или телефонски услуги. Ќе ви се заканува дека ќе прекине со испорака на услугата или дека ќе ви наплатат високи казни ако веднаш не ја платите сметката. Некој пат може да се престави како деловно лице од австралиската пошта изјавувајќи дека треба да отидете да подигнете пратка и ако не го сторите тоа ќе ви се наплаќа надоместок за чување за секој ден за којшто нема да платите. Во секој случај, ќе се трудат да ве уплашат и да ве натераат да го сторите тоа што го бараат без да подзастанете да размислите и да проверите дали приказната е вистинита.

Ако измамата е испратена по електронска пошта, најверојатно ќе има прилог или линк до лажно место на интернет кадешто ќе ви се бара да симнете доказ за постоењето на ‘сметката’, ‘казната’ или пак ‘поединости за испорака на пратката’. Ако го отворите прилогот или ако го снимите документот вашиот компјутер ќе се зарази со малициозен софтвер (видете на страна 16).

Заштитете се

- Не дозволувајте лице што ви се заканува по телефон да врши притисок врз вас. Застанете, размислете и проверете дали приказната е вистинита.
- Ниедна владина агенција или вам позната компанија нема да побара да платите преку невообичаени методи на плаќање како што се картички за подарок, преку жичен трансфер на пари или со Биткоини.
- Потврдете го идентитетот на лицето кое стапило во контакт со вас така што ќе се јавите директно во дотичната организација — пронајдете го преку независен извор како што е телефонски именик, од некоја мината сметка или со пребарување на интернет.
- Не ги користете поединостите за контакт што се наведени во електронските пораки или што ви се дадени за време на телефонскиот разговор. Сепак пронајдете ги преку независен извор на информации.

Измама со неочекувани пари

Ако некој ви бара да платите пред да го добиете производот или очекуваните пари, добро размислете.

Како функционира измамата

Измамниците ненадејно ви кажуваат дека имате право да добиете некакви пари, скапоцени камења, злато или пак вредни акции, но дека морате **да платите однапред** за да ги добиете. Никогаш нема да го добиете тоа што ви било ветено и секој пат ќе има изговор зошто треба да платите повеќе. Ако го платите надоместокот, ќе си ги изгубите парите.

Кај **измамите со попусти или поврат на пари** измамникот ви кажува дека некој ви должи пари заради преплатени даноци, банкарски провизии или пак некој вид на компензација. Меѓутоа, пред да ги добиете парите треба да платите мал административен надоместок.

Кај **измамите со наследство**, измамниците настапуваат како адвокати, банкари или странски службени лица и ви кажуваат дека може да остварите право на големо наследство или ви нудат удел во некоја разработена шема бидејќи го носите истото име и презиме како некое починато лице. Често користат документи како оние што ги поседуваат службените лица и ви бараат да платите надоместоци и даноци пред да го добиете наследството. Може да ви ги побараат и личните поединости за да ја пополнат ‘потребната документација’. Тоа значи дека покрај парите може да ви го украдат и идентитетот.

Има измами познати како **нигериски измами** што може да потекнале од Западна Африка, но може да дојдат и од било каде во светот. Кај нив измамниците ви кажуваат дека треба да им помогнете да спасат големо богатство коешто тие очајно се обидуваат да го изнесат од својата земја. Може да велат дека богатството е голем износ на пари, злато или вредни средства што ги оставила нивната корумпирана влада или властите и дека ако се согласите да ги прифатите ќе ви дадат голем удел од

истите кога ќе биде безбедно да се направи тоа. Како и кај сите останати измами, ќе ви кажат дека пред да ви ги пратат парите прво треба да платите даноци, банкарски провизии или надоместоци за да се извршат проверки за спречување тероризам или за перење пари.

Овие измами често доаѓаат од странство и бараат да платите преку жичен трансфер, но може да бараат и трансфер на парите преку банка или преку други методи.

Ако паднете на овие измами, од измамникот никогаш нема да добиете ништо и ќе ги изгубите сите пари што сте ги испратиле.

Заштитете се

- Запомнете дека не постојат шеми со кои брзо ќе се збогатите: ако звучи предобро за да биде вистинито тогаш веројатно е така.
- Избегнувајте секакви договори со странец кој бара плаќање однапред преку платен налог, преку жичен трансфер на пари, преку меѓународен трансфер на средства, преку однапред наполнета платежна картичка или преку електронски валути. Многу ретко можат да се повратат парите што се испратени на ваков начин.
- Ако некоја непожелна електронска порака ви изгледа сомнителна, едноставно избришете ја. Не кликајте на никакви линкови.
- Владините оддели, банките или комуналните служби никогаш нема да стапат во контакт со вас и да бараат да плаќате однапред со цел да добиете поврат на пари или пак попуст.
- Ако не сте сигурни, независно проверете го идентитетот на лицето кое ве контактира. Не ги користете поединостите за контакт во пораката што ви е испратена-најдете ги точните поединости за контакт преку независен извор од типот на телефонски именик или преку пребарување на интернет.
- Истражете на интернет така што ќе ги внесете точно истите зборови од понудата — на овој начин може да се откријат многу измами.

Измами со награди и лотарија

Немојте да се мамите по некоја добивка како изненадување — само измамник може да ви понуди таква неочекувана добивка.

Како функционира измамата

Преку овие измами се обидуваат да ве намамат однапред да дадете пари или да ги откриете вашите лични поединости со цел да добиете некоја награда од лотарија, од наградна игра или од натпревар во којшто никогаш не сте учествувале. Измамниците ви кажуваат дека треба да платите надоместок или даноци пред да ја пратат вашата 'добивка' или награда. Може исто така да треба да се јавите или да пратите порака на телефонски број со висока претплата за да си ја побарате наградата.

Кај **измамите со гребење** добивате електронска порака со светкави брошури и неколку картички на гребење при што една од нив носи добивка. За да бидат поуверливи, често ќе наведат дека се работи за втора или за трета награда. Кога ќе се јавите да си ја побарате наградата, измамниците ќе побараат да платите некаков надоместок или данок пред да ја подигнете добивката.

Измамите со лотарија може да ги користат имињата на вистински лотарии од странство за да ви кажат дека сте добиле пари, иако никогаш не сте играле таква лотарија. Измамниците обично бараат надоместок или данок за да ви ги пуштат парите. Исто така ќе ви кажат дека им требаат и вашите лични поединости за да докажат дека сте вистинскиот добитник, но подоцна ќе ги искористат истите за да ви го украдат идентитетот или да украдат пари од вашата банковна сметка.

Кај **лажните ваучери и картички со подароци** измамниците ви праќаат електронска порака или текстуална порака или пак порака преку друштвена мрежа велејќи дека сте добиле картичка со подарок од добро позната трговска компанија, но и дека треба да дадете некои поединости пред да си го земете подарокот. Ова е обид да се дојде до личните

податоци коишто можат да се искористат за крадење на идентитетот или пак за да станете цел на некоја друга измама. Ваквите понуди се исто така познати по тоа во вашиот уред внесуваат софтвер што ве уценува да платите пари за да се одблокира уредот (видете страна 17).

Кај **измамите со наградни патувања** измамниците ви кажуваат дека сте добиле бесплатен одмор или авионска карта. Во суштина, она што сте го добиле е шанса да платите за престој или за ваучер за авионски лет. Овие ваучери за патување обично имаат скриени надоместоци и услови, или пак може да бидат лажни и безвредни. Исто така, измамниците може да ви нудат прекрасни пакети за одмор со снижени цени коишто воопшто не постојат.

Заштитете се

- Запомнете: не можете да добиете пари на лотарија или од натпревар освен ако не сте се пријавиле да учествувате во играта.
- Натпреварите и лотариите не бараат да плаќате надоместок за да си ја подигнете наградата—пребарајте на интернет така што ќе ги користите точно истите зборови од понудата. Тоа може да помогне да откриете дека се работи за измама.
- Внимателно размислете пред да се јавите или да пратите текстуална порака на телефонски број што почнува на ‘19’—тие наплаќаат високи тарифи.

Измами со купување преку интернет, со реклами и со наддавања

И измамниците ја сакаат леснотијата со која се врши купување преку интернет.

Како функционира измамата

Потрошувачите и бизнисите сè повеќе купуваат и продаваат преку интернет. За жал, измамниците го користат интернетот за да најдат жртви.

Измамниците може да создадат многу уверливи **лажни места за продажба на интернет** што изгледаат многу вистинито, а тоа го прават и на друштвените мрежи како Facebook. Најголемиот предзнак дека некое место за продажба на интернет е измама е начинот на кој се плаќа – внимавајте ако се бара да платите преку жичен трансфер или преку други невообичаени методи на плаќање.

Кај **измамите со наддавање преку интернет** измамникот ви кажува дека сте добиле втора шанса да купите некој производ за којшто сте наддавале бидејќи победникот се откажал. Измамникот ќе побара да платите на друго место а не преку методот за безбедно плаќање на официјалното место на интернет за наддавање; ако го сторите тоа, ќе ги изгубите парите, а местото на интернет каде било наддавањето нема да може да ви помогне.

Измамата со рекламирање преку веродостојни регистрирани места на интернет е чест вид на измама која ги напаѓа и купувачите и продавачите. Купувачите треба да внимаваат на измамници кои поставуваат лажни реклами на веродостојни места на интернет наменети за рекламирање. Ваквите реклами може да бидат за било што, од изнајмување простор до рекламирање домашни миленичиња, користени автомобили или фотоапарати, а цените обично се евтини. Ако покажете дека сте заинтересирани за некој производ, измамникот може да ви

каже дека е на пат или дека се преселил во странство и дека откако ќе платите некој агент ќе ви го достави производот. По плаќањето нема да го примите производот, ниту пак ќе можете да стапите во контакт со продавачот.

Кај продавачите, измамникот со реклами ќе одговори на вашата реклама со дарежлива понуда. Ако ја прифатите, измамникот ќе плати со чек или со платен налог. Но, износот што го примате е поголем од она што сте се договориле. Кај оваа измама на **плаќање повеќе пари**, 'купувачот' може да ви каже дека се работи за грешка и ќе побара да му го вратите вишокот преку трансфер на пари. Измамникот се надева дека вие ќе префрлите пари пред да откриете дека чекот е одбиен и дека платниот налог бил лажен. Вие ќе ги изгубите парите, а и производот што сте го продале доколку веќе сте го испратиле.

Заштитете се

- Дознајте со кој точно си имате работа. Ако се работи за австралиски малопродажник, ќе бидете во многу подобра позиција да го разрешите проблемот ако нешто тргне наопаку.
- Проверете дали продавачот го бие добар глас, дали има политика на враќање пари или пак служба за разрешување на поплаки од корисници.
- Избегнувајте зделки каде се бара плаќање однапред преку платен налог, преку жичен трансфер, преку меѓународен трансфер на средства, со однапред наполнета платежна картичка или со електронска валута. Парите што се испратени на ваков начин ретко се враќаат. Никогаш не праќајте пари, не давајте кредитни картички или поединости за сметки на интернет на никого кој не го познавате или на кој не му верувате, и никогаш не откривајте такви податоци преку електронска порака.
- Плаќајте само преку методот за безбедно плаќање на местото на интернет – барајте адреса на интернет што почнува со 'https' и со знак со затворен катанец.
- Никогаш не прифаќајте чек или платен налог за плаќање што е на поголем износ од она што сте се договориле, и не префрлајте пари никому.

Измами насочени кон компјутерите и мобилните уреди

Запомнете: сè што се поврзува на интернет е подложно на измама.

Како функционира измамата

Измамниците кои го користат далечинскиот пристап ви се јавуваат на телефон велејќи ви дека компјутерот ви е заразен со вируси. Ако ги следите нивните инструкции, тоа ќе им дозволи да пристапат до вашиот компјутер и да го контролираат и од него ќе можат да крадат податоци или да инсталираат малициозни софтвери. Може исто така да ве убедат да купите ‘anti-virus’ софтвер за заштита од вируси за којшто обично се испоставува дека е прескап или пак е бесплатно достапен на интернет.

Malware е термин кој се однесува на сите видови на малициозни софтвери што може да се инсталираат на вашиот компјутер или на други уреди и вклучува вируси, шпионски софтвери, софтвери што ве уценуваат да платите за да се одблокира уредот познати како ransomware, тројански коњи и софтвери што снимаат сè што се притиска на тастатурата познати како keystroke loggers.

Софтверите што снимаат сè што се притиска на тастатурата или keystroke loggers и шпионските софтвери им овозможуваат на измамниците да го снимат точно она што го пишувате на тастатурата за да ви ги откријат лозинките и банковните поединости и да ги испратат било каде кај што тие сакаат. Откако истите ќе се инсталираат, измамниците може да ги контролираат вашата електронска пошта и интернет сметки на друштвените мрежи и да присвојат било која информација од вашиот уред, вклучително и лозинки. Исто така може да ги користат вашите интернет сметки за да испратат повеќе измами до вашите пријатели и семејството.

Софтверот што ве уценува да платите за да се одблокира уредот или ransomware претставува друг вид на малициозен софтвер којшто го енркиптира или заклучува вашиот уред за да ве спречи да го користите додека не се плати за да се отклучи. Плаќањето не ви гарантира дека истиот ќе се отклучи и дека ќе биде чист од скриени вируси, коишто исто така можат да се рашират и да заразат и други компјутери и уреди во вашата мрежа.

Малициозниот софтвер често се доставува по електронска пошта и може да изгледа дека доаѓа од веродостоен извор, како на пример од давател на комунални услуги, од владина агенција или дури од полицијата која наводно ви пишува парична казна. Не кликајте на линкот и не отворајте никакви прилози за кои не сте апсолутно сигурни што се. Така може да снимите малициозен софтвер. Ваквите измами ги напаѓаат и поединците и компаниите.

Заштитете се

- Бидете претпазливи со опциите за бесплатно симнување музика, игри, филмови и пристап до интернет места за возрасни. Тие можат да инсталираат штетни програми без вие да знаете.
- Чувајте ги заштитени вашите канцелариски мрежи, компјутери и мобилни уреди. Ажурирајте го софтверот за заштита, менувајте ги лозинките и на редовна основа зачувувајте резервни копии на вашите податоци. Чувајте ги резервните копии со податоци надвор од уредот и надвор од интернет. На местото на интернет www.staysmartonline.gov.au е објаснето како да правите резервни копии од податоците и како да ги заштитите вашите мобилни уреди.
- Не ги отворајте прилозите и не кликајте на линкови или на пораки од друштвените мрежи што се ги добиле од непознати лица – едноставно избришете ги.

Крадење на идентитет

Во сите измами има потенцијал да се украде нечиј идентитет. Кога се заштитувате себеси од измами тоа подразбира и безбедно чување на вашите лични податоци.

Крадењето идентитет е закана што постои во секоја измама

Повеќето луѓе ги поврзуваат измамите со измамнички обиди да ви земат пари. Меѓутоа, вашите податоци исто така им се вредни на измамниците. Измамниците ги крадат вашите лични поединости за да вршат измамнички дејствија како на пример да извршат неовластено купување од вашата кредитна картичка, или пак за да го користат идентитетот за да отворат банковна сметка или сметка за телефон. Можат да земат кредит или пак да извршат други противзаконски деловни работи во ваше име. Можат дури и да им ги продадат вашите податоци на други измамници за да се користат за други противзаконски работи понатаму.

Откако ќе ви го украдат идентитетот тоа може да ве уништи и финансиски и емоционално. Може да бидат потребни месеци да си го повратите идентитетот, а влијателниот удар од тоа што ви бил украден може да трае со години.

Фишинг измама—измамникот ненадејно стапува во контакт со вас преку електронска пошта, телефон, Facebook или преку текстуална порака преправајќи се дека доаѓа од легитимна компанија како што е банка, или пак давател на телефонски или интернет услуги. Ве насочува на лажна верзија на местото на интернет на компанијата и бара да ги обелодените вашите лични поединости за да се потврдат записите за корисникот заради настаната техничка грешка. Може да ви се јави и да глуми малопродажник на луксузна стока и да ви каже дека некој се обидува да ја искористи вашата кредитна картичка. Ве советува да стапите во контакт со вашата банка но не спушта од кај него и ја остава линијата отворена. Кога пробувате да се јавите во банката сè уште зборувате со измамникот кој симулира вистински повик, имитира банкарски службеник и бара да му ги кажете поединостите за сметката и заштитните лозинки. Во секој случај, измамникот ја презема секоја информација што ќе му ја дадете и ја користи за да пристапи до вашата сметка.

Лажни анкети— во замена за тоа да пополните анкета на интернет измамниците нудат награди или добивки како што се картички со подароци од познати малопродажни места. Со анкетата се бара да одговорите на низа прашања, вклучително и откривање на важни идентификациски или банковни поединости.

Како дел од секоја измама—измамниците често бараат лични податоци во други измами. Во измамата со лотарија измамниците често бараат број на возачка дозвола или на пасош за 'да го докажат вашиот идентитет пред да можат да ви ги пуштат парите од наградата'. Кај измамите со љубовни и романтични средби може да ви побараат податоци 'за да се спонзорира нивното пријавување за добивање виза за да ве посетат во Австралија'.

Запомнете: Давање на лични податоци на измамник може да биде исто толку лошо како и давањето пари. Чувајте си ги личните поединости за себе и чувајте ги заштитени.

Заштитете се

- **Размислете два пати за она што го кажувате и што го правите во интернет околина**

  Бидете внимателни со споделувањето информации за себе на интернет, вклучително и на друштвените мрежи, на блогови и на други форуми на интернет. Застанете и размислете пред да пополните некоја анкета, пред да влезете во некој натпревар, пред да кликнете на некој линк или на прилог, па дури и кога 'прифаќате пријател', 'кога ставате 'like'' или кога 'споделувате' нешто на интернет.

- **Бидете претпазливи со секакво барање за вашите поединости или за пари**

  Служејќи се со имињата на добро познати компании или владини оддели, измамниците ќе пробаат да ве измамат да им ги предадете вашите податоци. Ако мислите дека се работи за измама, не одговарајте, проверете во телефонскиот именик или истражете на интернет за да ги проверите поединостите за контакт на организацијата. Никогаш не ги користете поединостите за контакт што ви се дадени во оригиналното барање.

Ако сте дале лични податоци за идентификување на измамници, стапете во контакт со IDCARE на 1300 432 273.

Измами со работни места и вработување

Големи приходи—загарантирани? Малку е веројатно!

Како функционира измамата

Измамите со работни места и вработување вклучуваат понуди за работа од дома или воспоставување и инвестирање во некоја ‘деловна можност’. Откако првин ќе платите однапред, измамниците ветуваат работа, висока плата или голем поврат на инвестицијата. Ова плаќање може да биде за потребите на ‘деловен план’, за курс за обука, за софтвер, за униформи, за безбедносна дозвола, за даноци и надоместоци. Ако го платите надоместокот може да не добиете ништо или пак не она што сте го очекувале или што ви било ветено.

Некои понуди за работни места може да бидат покритие за активности за **незаконско перење пари**, каде се бара да делувате во улога на ‘управител на сметки’ или ‘личен помошник’, да примате исплати на вашата банковна сметка за одредена провизија, а потоа да ги префрлате парите на некоја странска компанија.

Измамите со работни места често се промовираат преку непожелни спам електронски пораки или преку реклами на добро познати места на интернет за рекламирање и за барање работа – дури и на владини места на интернет за барање работа.

Голема опасност кај овие измами со работни места е тоа што може да ви побараат многу лични податоци што не треба да ги откривате, вклучително и вашиот даночен број и копии од вашиот пасош и од возачката дозвола. Овие податоци подоцна може да се искористат за крадење на идентитет.

Заштитете се

- Бидете претпазливи со понуди или со шеми кои изјавуваат дека гарантираат приход или пак бараат да платите однапред.
- Никогаш не се согласувајте да префрлате пари за некој друг – тоа е перење пари и претставува незаконско дејствие.
- Кога се пријавувате за некое работно место не го давајте вашиот даночен број, ниту возачка дозвола или пасош. Може ќе треба да ги дадете ваквите податоци, но само откако ќе почнете да работите.

Перењето пари е кривично дело: не се согласувајте да префрлате пари за непознато лице.

Измами за добротворни и медицински цели

Измамниците се бесчувствителни и може да ве нападнат во очајни времиња кога ви треба помош.

Како функционира измамата

Измамниците ги злоупотребуваат луѓето кои сакаат да донираат за добротворни цели или пак да најдат решение на некој здравствен проблем.

Кај **измамите за добротворни цели** измамниците собираат пари преправајќи се дека работат за некоја легитимна иницијатива или добротворна организација, или пак за некоја лажна којашто самите ја создале. Често пати измамниците користат прилика да настапат после некоја природна катастрофа или криза што била објавена на вести.

Овие измами ги пренасочуваат многу потребните донации далеку од веродостојните добротворни организации. Добротворните организации мора да бидат регистрирани од владата — донирајте безбедно со тоа што прво ќе ја проверите нивната регистрација.

Измамите со чудотворни лекови нудат низа производи и услуги коишто може да изгледаат како легитимна алтернативна медицина, и обично ветуваат брзо и делотворно закрепнување од сериозни медицински заболувања. Третманите често се промовираат со користење на лажни сведоштва од луѓе кои биле 'излечени'.

Измамите со средства за слабеење ветуваат драматично слабеење со мал или со никаков напор. Овој вид на измама може да вклучува некоја необична или ограничена исхрана, револуционерна вежба, некој уред ‘уништувач на маснотии’, новооткриени апчиња, лепенки или креми. Може да ви бараат однапред да платите голем износ на пари или да потпишете долгорочен договор за редовно да ви праќаат залихи.

Лажните аптеки на интернет нудат фалсификувани лекови и медицински препарати по многу ниски цени, а понекогаш ги даваат и без рецепта од лекар. Овие лекови може да содржат мали количини или пак воопшто да немаат активни состојки, а тоа може да доведе до смртни последици по лицата кои ги користат.

Заштитете се

- Ако ви пристапи собирач на средства за добротворни цели на улица, побарајте да ви покаже документ за идентификација. Ако имате било каков сомнеж за тоа кое е лицето, не плаќајте.
- Проверете го списокот на регистрирани добротворни организации при Австралиската непрофитна асоцијација на добротворни организации (Australian Charities Not for Profit Association).
- Посоветувајте се со својот матичен лекар доколку размислувате за некоја понуда за ‘чудесен лек’ или за ‘лек кој делува веднаш’ поврзана со медицински препарати, додатоци во исхраната или други третмани.
- Запрашајте се: ако ова е навистина чудесен лек, зарем вашиот матичен лекар немало да ви каже за него?

Измами на компании

Измамниците ја злоупотребуваат зафатеноста и брзото темпо на многу компании за да ги измамат.

Како функционира измамата

Измамите што ги напаѓаат компаниите доаѓаат во секакви скриени облици и најголема е веројатноста да нападнат во најзафатените времиња од работењето, како што е крајот на финансиската година.

Измамата со лажни сметки е најчестиот трик што измамниците го користат против компаниите. Измамниците издаваат лажни сметки за непожелно или за неовластено регистрирање во именици, реклами, производи или услуги. **Измамата со деловниот именик** е добро познат пример, при што добивате сметка за да бидете регистрирани во наводно добро познат деловен именик. Измамниците ве прелажуваат да се потпишете со тоа што ја маскираат понудата како неплатена фактура или бесплатно вметнување во именикот, но со скриен договор за претплата испишан со мали букви.

Измамата со име на домен е уште еден трик што го користат измамниците, при што ве прелажуваат да потпишете за регистрација на интернет домен што не сте го барале, а кој е многу сличен на вашиот. Може исто така да добиете и лажно известување за обновување на претплатата за вистинското име на вашиот домен и да платите без да приметите.

Кај **измамата со канцелариски материјал** вие примате производи што не сте ги порачале и ви наплатуваат за нив. Овие измами често работат со производи или услуги што редовно ги порачувате, како на пример канцелариски материјал и средства за чистење. Измамниците обично се јавуваат во вашата компанија и се преправаат дека веќе била направена порачка на некоја услуга или производ.

Кај **измамата со преусмерување на исплата** измамникот користи податоци што ги добил со хакирање на вашиот компјутерски систем. Потоа се претставува како еден/една од вашите редовни даватели на услуги и ви кажува дека ги сменил/а банковните поединости. Може да ви каже дека неодамна ја сменил/а банката, а може да користи и копирани меморандуми и обележје на марката за да ве увери дека се веродостојни. Ќе ви даде број на нова банковна сметка и ќе ве замоли сите идни плаќања да ги вршите на таа сметка, соодветно. Оваа измама често се открива само откако вашиот редовен давател на услугата ќе праша зошто не им е платено за услугата.

Софтверите што ве уценуваат да платите за да се одблокира уредот познати како **ransomware** можат да имаат огромно разорно дејство за било која компанија. Најдобрата одбрана е на редовна основа да зачувувате редовни копии од вашите податоци и резервните копии да ги чувате надвор од уредите и надвор од интернет. За повеќе поединости видете на страна 17.

Заштитете се

- Немојте веднаш да се согласувате на понудите и зделките – секој пат побарајте да добиете понуда на писмено и побарајте независен совет ако зделката вклучува пари, време или долгорочно обврзување со договор.
- Никогаш немојте да му ги давате банковните, финансиските и сметководствените поединости за вашата компанија на некое лице кое неочекувано стапило во контакт со вас и кое не го познавате, ниту му верувате.
- Делотворните постапки за управување може многу да придонесат за спречување на измамите—имајте јасно дефинирани процеси за утврдување на веродостојноста и плаќање на сметките и фактурите и многу внимателно проверувајте ги барањата за промена на банковни поединости.
- Обучете ги вработените да препознаваат измами.
- Зачувувајте резервни копии од вашите деловни податоци надвор од уредите и надвор од интернет.
- Бидете претпазливи со електронски пораки што бараат промена на поединостите за плаќање. Секој пат потврдете ја вистинитоста на промените во поединостите за плаќање директно со самата компанија или со дотичниот поединец.

Како функционираат измамите—анатомија на една измама

Повеќето измами следат една иста шема и откако еднаш ќе ја сфатите, ќе ви биде полесно да ги воочите триковите што ги користи измамникот.

Ако ги погледнете внимателно сите различни видови на измами наведени во оваа книга, наскоро ќе приметите дека повеќето измами поминуваат низ три фази: (1) пристап; (2) комуникација; и (3) плаќање.

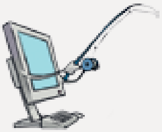
Разбирањето на основните составни делови на измамите ќе ви помогне да ги избегнете шемите на измами што моментално се вртат и да бидете на штрек за новите измами што ќе се појават во иднина.

1. Пристапот: начин на кој ви ја ‘продава’ приказната

Кога ви пристапуваат измамниците, тоа секој пат е пропратено со приказна измислена за да ве натера да поверувате во лага. Измамникот ќе се преправа дека е некој кој не е, како на пример владин службеник, стручен инвеститор, службеник од лотарија или дури и романтичен обожавател.

За да ви ги ‘продадат’ лагите, измамниците ќе користат низа методи на комуникација.

Преку интернет



Измамниците демнат позади анонимноста на околината на интернет.

Електронската порака е омилениот метод на претставување на измамата, којшто обезбедува евтин и едноставен начин за комуникација во голем обем. Електронските пораки со ‘фишинг’ намери (Phishing emails) што ‘се во лов’ на вашите лични податоци е најчестиот вид на измама со електронска порака.

Платформите на друштвените мрежи, местата на интернет за љубовни средби и форумите на интернет им овозможуваат на измамниците да ‘ви станат пријатели’ и да влезат во вашиот личен живот за да пристапат до вашите лични податоци коишто потоа може да бидат искористени против вас или против вашето семејство и пријатели.

Измамниците го користат **купувањето преку интернет,** како и **местата на интернет за рекламирање и за наддавање** за да ги напаѓаат купувачите и продавачите. Притоа првичниот контакт обично се прави преку добро познато и препознаено место на интернет или преку лажно место на интернет коешто изгледа како вистинско. Барајте да плаќате преку заштитени опции за плаќање и бидете претпазливи со невообичаени методи на плаќање како што е жичен пренос, со Биткоини или преку однапред наполнета платежна картичка. Кредитните картички обично нудат одредена заштита.

Измамниците се јавуваат и преку телефон и преку СМС пораки.

Измамниците користат **телефонските повици** и се јавуваат во домовите и во компаниите во многу разни измами, од типот на измами со закани за неплатени даноци до нудење награди или 'помош' околу компјутерски вируси. Достапноста на евтини телефонски повици со протоколи за пренесување на глас преку интернет (Voice Over Internet Protocol - VOIP) значи дека повикувачките центри може да работат од странство со телефонски броеви што личат како да се локални броеви. Идентификувањето на повикувачот лесно може да се маскира и претставува еден од многуте трикови коишто ги користат измамниците за да ве убедат дека се некој друг.

Измамниците ги користат **текстуалните СМС** пораки за да испраќаат цела низа измами, вклучително и измами со натпревари и со награди. Ако одговорите, може да ви биде наплатена висока тарифа или пак да испадне дека сте се согласиле на услуга за претплата. Побезбедно е да не одговарате и да не кликате на линковите во текстуалните пораки освен ако знаете од кој доаѓаат. Тие исто така може да содржат прилози или линкови до малициозни софтвери скриени во слики, песни, игри или пак апликации.

Внимавајте—некои измамници буквално ќе ви се појават на врата за да пробаат да ве измамат.

Кај **измамите од врата на врата** измамникот обично промовира производи или услуги коишто не се испорачуваат на друг начин или се со многу лош квалитет. Може дури и да ви наплатат за завршена работа којашто не сте ја сакале или кога не сте се согласиле за истата. Една од честите измами од врата на врата ја прават сомнителните трговци кои одат од место во место и прават лошо извршени поправки во домовите или едноставно ви ги земаат парите и бегаат.

Веродостојните компании може да продаваат услуги и добра од врата на врата, но мораат јасно да се идентификуваат и себе и компанијата и да се придржуваат кон други правила. Кога се работи за практиката на продавање од врата на врата, имате посебни права, вклучително и шанса да се премислите – дознајте повеќе на www.accc.gov.au/doortodoor.

Измамниците може да се претставаат како вработени во лажна **добротворна организација** за собирање донации. Тие ги злоупотребуваат неодамнешните настани како што се поплави и шумски пожари. Пред да дадете донација побарајте документ за идентификација и погледнете го нивниот службен приемник со евиденција за донациите.

Масовното испраќање пораки сè уште се користи за праќање **измами со лотарии и со наградни игри, со инвестициски можности, за нигериски измами** и **за лажни писма за наследство.** Светкавата брошура не е гаранција дека понудата е легитимна.

Без разлика на методот што го користат за да ви ја ‘продадат’ измамата, нивната приказна секогаш е мамката и ако загризете измамникот ќе проба да ве однесе во следната фаза.

2. Комуницирање и замајување со приказни

Ако им дадете шанса да зборуваат со вас, ќе почнат да користат трикови од нивната **богата палета на замки** за да ве убедат да си ги дадете парите.

'Алатките' што ги користат измамниците може да вклучат:

- измамниците коваат детални, но сепак **уверливи приказни** за да го добијат тоа што го сакаат.
- Тие ги користат вашите **лични податоци** за да ве натераат да верувате дека и претходно сте се сретнале со нив и прават измамата да изгледа легитимна.
- Измамниците може **редовно да ве контактираат** за да стекнете доверба во нив и за да ве убедат дека ви се пријател, партнер или пак лице заинтересирано за љубовна врска.
- Тие **си поигруваат со вашите чувства** користејќи ја возбудата што ја носи победата, ветувањето за вечна љубов, изразеното сочувство за несреќен настан, вината дека не им помагате или стравот од апсење или добивање казна.
- Измамниците обожаваат да создаваат **чувство на итност** за да немате време да размислите за работите и за да изреагирате врз основа на чувствата, а не на логиката.
- Слично, тие користат **тактики за продажба така што вршат голем притисок** велејќи дека се работи за ограничена понуда, дека цените ќе пораснат или дека пазарот ќе се придвижи и понудената можност ќе исчезне.
- Измамата може да ги има сите обележја на вистински бизнис и да користи **светкави брошури** со технички изрази поткрепен со канцеларии, повикувачки центри и професионално место на интернет.
- Со пристап до интернет и со паметен софтвер на измамниците им е лесно да создаваат фалсификати коишто **изгледаат како официјални документи.** Некој документ што изгледа како да има владино одобрение или кога е полн со правни изрази може да Ѝ придаде лажна важност на измамата.

Алатките на измамниците се создадени за да ве натераат да си ја смалите одбраната, да стекнете доверба во приказната и да дејствувате брзо или неразумно и да продолжите до последната фаза – плаќање пари.

3. Праќање на парите

Понекогаш најголемиот знак што ќе го добиете дека се работи за измама е начинот на кој измамникот ви бара да платите.

Барањето пари може да се случи по само неколку минути од почетокот на измамата или пак после месеци поминати во внимателно намамување. Измамниците имаат свои претпочитани начини на кои ќе сакаат да им испратите пари.

Познато е дека измамниците ги насочуваат жртвите до нивната најблиска локација каде можат да проследат **парична дознака** за да ги испратат парите (пошта, сервис за жичен пренос, па дури и во банка). Познати се по тоа што ја држат отворена телефонската линија, даваат специфични инструкции, а може дури и да испратат такси за да помогнат да се заврши работата. Измамниците се спремни да примат пари на секаков можен начин, а тоа може да вклучува **директен трансфер преку банка, претходно наполнета дебитна картичка, картичка со подароци, картички од Google Play, од Steam, или од iTunes** или со виртуелна валута како што е **Биткоин.** Секое едно барање за плаќање преку невообичаен метод е знак кој издава дека се работи за дел од измама.

Кредитните картички обично нудат одредена заштита. Исто така треба да ги барате опциите за безбедно плаќање каде на адреса на место на интернет се појавува претставката 'https' и каде местото има симбол со затворен катанец.

Не праќајте пари на некој кој само што сте го запознале преку интернет или преку телефон – особено ако лицето е во странство.

Имајте на ум дека измамниците може исто така да побараат плаќање во облик на вредна стока и скапи подароци како што се накит или електронски уреди. Плаќање пари на измамници не е единствената работа за која треба да се грижите – ако помогнете да се пренесат пари за непознато лице може без ваше знаење да бидете вклучени во **незаконски дејствија за перење пари.**

Златното правило за да се заштитите себеси

Бидете свесни за фактот дека постојат измами. Кога се соочувате со непоканети контакти од луѓе и компании, независно дали се преку телефон, преку пошта, преку електронска пошта, лично или на некоја друштвена мрежа, секогаш имајте ја во предвид можноста дека нивното пристапување може да биде со цел да ве измамат. Запомнете, ако изгледа предобро за да биде вистинито, најверојатно е така.

Осознајте со кого си имате работа. Ако си имате работа со некој кој само што сте го запознале преку интернет или пак ако сте несигурни за веродостојноста на некоја компанија, поминете некое време да истражите подлабоко. Направете пребарување на слики преку сервисот на Google или пребарајте на интернет дали има други лица коишто имале работа со тоа лице или со таа компанијата.

Не отворајте сомнителни текстови, pop-up прозорци или пораки — избришете ги. Доколку не сте сигурен/на, потврдете го идентитетот на лицето што ве контактирало преку независен извор од типот на телефонски именик или со пребарување на интернет. Не ги користете поединостите за контакт што ви се дадени во испратената порака.

Чувајте ги заштитени вашите лични поединости. Ставете клуч на поштенското сандаче и исечете ги на ситни парчиња сметките и другите важни документи пред да ги исфрлите. Чувајте ги на безбедно место лозинките и пин-боевите од картичките. Внимавајте колку лични податоци споделувате на друштвените мрежи. Измамниците може да ги искористат вашите податоци и слики за да создадат лажен идентитет или за да ве нападнат со измама.

Бидете претпазливи со невообичаените методи на плаќање. Измамниците често бараат плаќањата да се извршат преку жичен трансфер, преку претходно наполнети платежни картички, а дури и преку картички за Google Play, за Steam, или за iTunes и со Биткоини. Сите овие се скоро секогаш знак дека се работи за дел од измама.

Заштитете ги вашите мобилни уреди и компјутери. Секогаш користете заштита со лозинка, не споделувајте пристап со другите (ниту далечински пристап), ажурирајте ги софтверите за заштита и правете резервни копии од податоците. Заштитете ја вашата WiFi мрежа со лозинка и избегнувајте да користите јавни компјутери или WiFi hotspots кога пристапувате до банкарски услуги на интернет или пак кога давате лични податоци.

Внимателно бирајте лозинка. Бирајте лозинки коишто другите тешко би ги погодиле и ажурирајте ги редовно. Силната лозинка треба да биде мешавина од големи и мали букви, од бројки и симболи. Не користете иста лозинка за секоја сметка/профил и не ја споделувајте лозинката со никого.

Бидете претпазливи со секакви барања за вашите податоци или за пари. Ако некого не познавате или ако не му верувате, никогаш не праќајте пари и не давајте број на кредитна картичка, поединости за сметки на интернет ниту пак копии од лични документи. Не се согласувајте да пренесувате пари или стока за некој друг: перењето пари се смета за кривично дело.

Внимавајте кога купувате преку интернет. Бидете претпазливи со понуди коишто изгледаат предобро за да бидат вистинити, и секој пат користете сервис за купување преку интернет којшто го знаете и на којшто му верувате. Размислете два пати пред да се одлучите да користите виртуелни валути (како Биткоини)—тие не ги поседуваат истите заштити како другите методи за вршење трансакции, што значи дека нема да можете да си ги вратите парите откако еднаш ќе ги префрлите.

Каде да најдете помош и поддршка

Ако сте изгубиле пари преку измама или ако сте ги дале вашите лични податоци на некој измамник, најверојатно нема да си ги вратите парите. Меѓутоа, постојат чекори што можете веднаш да ги преземете за да ја ограничите штетата и за да се заштитите себеси од натамошни загуби.

Стапете во контакт со вашата банкарска или кредитна установа

Ако сте префрлиле пари или сте дали лични банковни податоци на некој измамник, веднаш стапете во контакт со вашата банкарска или кредитна установа. Тие може ќе можат да го стопираат преносот на пари или чекот, или пак да ја затворат вашата сметка доколку измамникот ги има поединостите за сметката. Ако вашата кредитна картичка била искористена лажно, давателот на услугите за кредитни картички можеби ќе може да изврши 'враќање на исплатата' или 'charge back' (односно да направи обратна трансакција).

Повратете си го украдениот идентитет

Ако се сомневате дека сте жртва на крадење на идентитет, важно е брзо да дејствувате за да го намалите ризикот од финансиска загуба или од други штети.

Стапете во контакт со **IDCARE**—бесплатна служба финансирана од владата што им нуди поддршка на жртвите на криминалот со крадење идентитети. Службата IDCARE може да ви помогне да разработите план за реагирање за да ги преземете соодветните чекори за поправање на нанесената штета на вашата репутација, на кредитната историја и на идентитетот. Посетете го местото на интернет на IDCARE на www.idcare.org или јавете се на 1300 432 273.

Пријавете се да добиете **Сертификат за жртви кој го издава Федералната влада (Commonwealth Victims' Certificate)**—сертификатот ќе ви послужи како поткрепа на вашата изјава дека сте биле жртва на крадење на идентитетот и може да се искористи да помогне повторно да се воспостават вашите претходни овластувања во владините и во финансиските институции. За да дознаете повеќе околу заштитата и обновувањето на вашиот идентитет посетете го Министерството на јавниот обвинител на www.ag.gov.au (или јавете се на 02 6141 6666).

Стапете во контакт со служба за советување или за поддршка

Ако вие самите или некој кој го познавате сте биле измамени или пак ако патите од емоционален стрес или депресија, ве молиме поразговарајте со вашиот матичен лекар, со локалните здравствени работници или со некој на кој му верувате. Исто така можете да размислите да стапите во контакт со некоја од службите за советување и за поддршка, како што се:

Службата **Lifeline**—кога ви е потребна поддршка во време на криза, стапете во контакт со Lifeline на 13 1114 (24/7) или посетете го местото www.lifeline.org.au

Службата **Beyondblue**—за информации во врска со депресија или анксиозност, стапете во контакт со beyondblue на 1300 224 636 или посетете го местото www.beyondblue.org.au

Линијата за помош **Kids helpline**—служба за поддршка преку телефон или преку интернет за млади лица на возраст од пет до 25 години. Јавете се на Kids helpline на 1800 551 800 или посетете го местото www.kidshelpline.com.au

Финансиско советување Австралија (Financial Counselling Australia)—доколку сте во финансиска криза јавете се на 1800 007 007 за да позборувате со бесплатен финансиски советник, или пак посетете го местото www.financialcounsellingaustralia.org.au.

Каде да пријавите измама

Со пријавување измама кај соодветните власти можете да им помогнете и на другите. Вашата информација ќе им помогне на овие организации да изградат подобра слика за најновите измами и да ги предупредат другите луѓе околу тоа на што треба да внимаваат.

Следните организации примаат пријави за одредени видови на измами.

Scamwatch

Пријавете измама во Комисијата ACCC преку Scamwatch—посетете го местото на интернет www.scamwatch.gov.au

Бидете чекор понапред од измамниците

Бидете чекор понапред од измамниците—посетете го местото на интернет Scamwatch за во целост да ги разберете измамите коишто ги напаѓаат австралиските потрошувачи и малите бизниси. Дознајте повеќе за тоа како функционираат измамите, како да се заштитите себеси и што да сторите доколку сте биле измамени.

Регистрирајте се во службата за пријавување на Scamwatch за да добивате бесплатни електронски пораки за новите измами што моментално се во оптек.

www.scamwatch.gov.au

Следете ги Scamwatch на Twitter на @scamwatch_gov или на местото на интернет http://twitter.com/Scamwatch_gov

Ако наидете на измама на некое место на интернет или на некоја платформа на друштвена мрежа, пријавете ја истата на самото место на интернет за да може да се истражи и да се отстрани. Ако измамниците се претставуваат како некоја легитимна организација како што е некој владин оддел или банка, известете ги за да можат да ги предупредат и другите.

Други установи

Исто така треба да размислите да ја пријавите измамата и во други установи коишто специфично се занимаваат со одредени видови на измами.

Вид на измама	Установа
Компјутерски криминал или Cybercrime	Австралиска мрежа за пријавување на компјутерски криминал преку интернет - Australian Cybercrime Online Reporting Network (ACORN)—посетете го местото на интернет www.acorn.gov.au
Финансиски и инвестициски измами	Австралиска комисија за акции од вредност и инвестиции - Australian Securities and Investments Commission (ASIC) — посетете го местото на интернет www.moneysmart.gov.au или јавете се на информативната телефонска линија на ASIC на 1300 300 630
Измами и кражби	Вашата локална полициска станица—јавете се на 13 1444
Непожелни spam електронски пораки и СМС пораки	Австралиско тело за комуникации и медиуми - Australian Communications and Media Authority (ACMA)—посетете го местото на интернет www.acma.gov.au или јавете се во Центарот за услуги за корисници при ACMA на 1300 850 115
Измами поврзани со даноци	Австралиска даночна управа - Australian Taxation Office (ATO)—за да пријавите измама со данок или за да утврдите дали е веродостојно некое лице кое стапило во контакт со вас во име на даночната управа: • јавете се на 1800 008 540 или препратете ја електронската порака што содржи измама со данок на адресата ReportEmailFraud@ ato.gov.au
Банкарство	Вашата банка или финансиска институција

Стапете во контакт со локалната установа за заштита на потрошувачи

Иако Комисијата ACCC е национална установа која се занимава со општите случаи од областа на заштита на потрошувачи, ваквите установи во државите и териториите исто така можат да ви помогнат.

Канцеларија за регулаторни служби при Територијата на главниот град на Австралија (Australian Capital Territory Office of Regulatory Services)	www.accesscanberra.act.gov.au 13 2281
Служба за потрошувачки работи на Австралија (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
Фер тргување на Нов Јужен Велс (New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
Служба за потрошувачки работи на Северна Територија (Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
Канцеларија за фер тргување во Квинсленд (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
Служби за потрошувачи и бизнис заедница во Јужна Австралија (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
Служби за потрошувачи, градежништво и работнички услуги на Тасманија (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
Министерство за рударство, индустриска регулатива и безбедност на Западна Австралија (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

Повеќе информации

Австралиската влада поседува одлични ресурси за тоа како постојано да бидете заштитени и безбедни на интернет.

- Услуга на интернет Stay Smart—www.staysmartonline.gov.au
- Место на интернет CyberSmart—www.cybersmart.gov.au
- Водичи на интернет Stay Smart—достапни на www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au