

Најдобрите 10 совети како да се заштитите од

Измами со лажно претставување

Macedonian | Македонски



Be Connected
Every Australian online.



SCAMWATCH

Измамите денес стануваат сè пософистицирани. Порано беше лесно да се забележат измамници поради лош правопис и граматика, но новата технологија го отежнува нивното откривање.



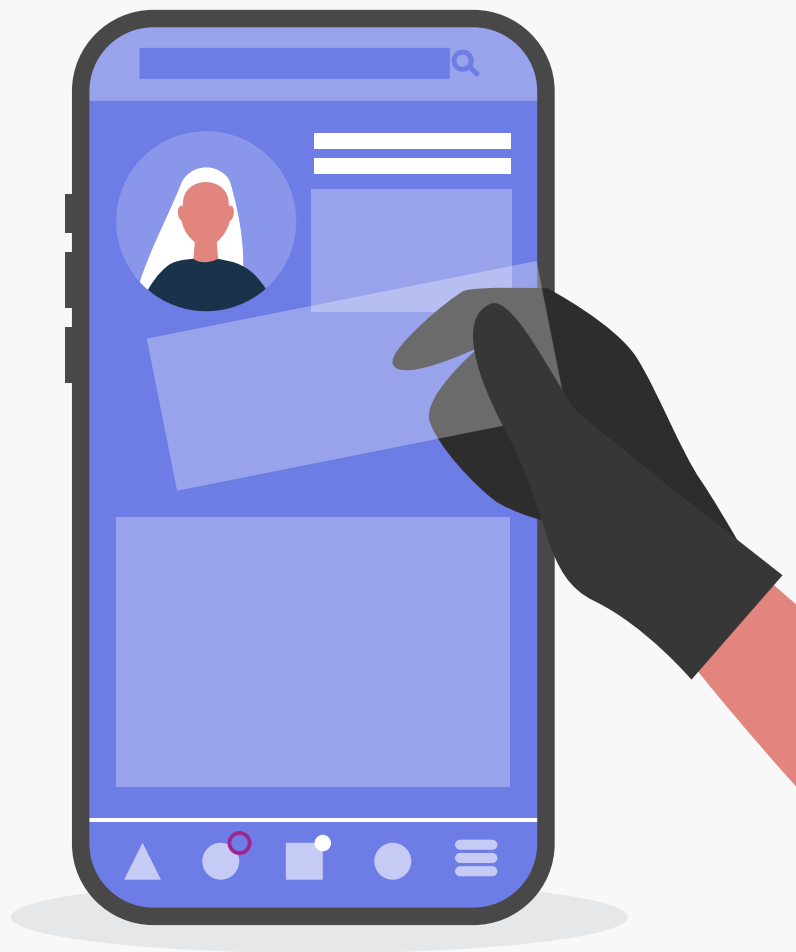
Националниот центар за борба против измами (National Anti-Scam Centre) соработува со владата, експертите од индустријата, органите за спроведување на законот и организациите во заедницата во борбата против измамите. Но, постојат и чекори што вие можете да ги преземете за да се заштитите од измама. Една од најдобрите заштитни мерки е да бидете во тек со новите измами и измамите што се јавуваат за да можете да ги препознаете знаците.

Be Connected, во партнерство со Scamwatch на Националниот центар за борба против измами, ви го дава овој прирачник кој ќе ви помогне да ги препознаете измамите со лажно претставување, да се заштитите од нив и да знаете каде да побарате помош доколку некогаш станете жртва на измама.

Сите примери дадени во овој прирачник се вистински измами.

Во овој прирачник

- [Што е измама со лажно претставување?](#)
- [Што е создавање на лажен профил \(spoofing\)?](#)
- [Чести измами со лажно претставување](#)
- [Најдобрите 10 совети како да се заштитите](#)
- [Каде да се обратите за помош](#)



Што е измама со лажно претставување?

Измамите со лажно претставување се наменети да изгледаат како да се од легитимни организации што ги познавате. Тие може да изгледаат како да се од вашата банка, давател на интернет услуги, владина агенција, трговец на мало, или дури тоа може да биде измамник кој се преправа дека е пријател или член на семејството.

Преправајќи се дека се некој на кого му верувате, измамниците создаваат чувство дека станува збор за итна работа со цел да ве измамат да платите пари или да дадете лични податоци, како што се важни лозинки, податоци за кредитни картички или банкарска сметка.

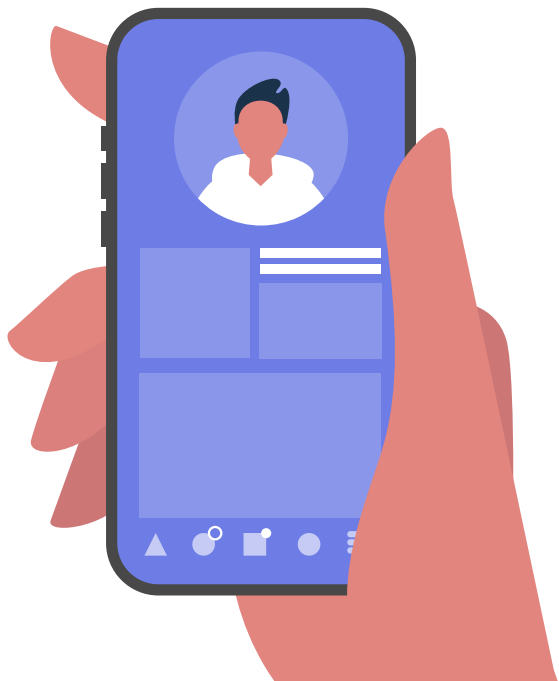
Измамниците користат различни методи за да стапат во контакт со вас, вклучувајќи текстуални пораки, телефонски повици, имејли, објави на социјалните мрежи и лажни веб-страници што изгледаат исто како официјални веб-страници.



Што е создавање на лажен профил (spoofing)?

Измамниците можат да се претстават како организации што ги познавате, користејќи технологија за да прикажат дека нивниот повик или порака доаѓа од доверлив извор. Ова е познато како создавање на лажен профил.

Бидете претпазливи со измамите и бидете сомничави кон ненајавен контакт кој бара лични податоци, како што се лозинка или некаков вид плаќање. Директно контактирајте ја организацијата од која тврди дека е за да потврдите.



Постојат различни видови техники на создавање лажен профил, вклучувајќи:

- 01. Создавање на лажна идентификација на повикувач (Caller ID spoofing):** измамниците го менуваат својот идентитет на повикувач (caller ID) за да се прикаже телефонски број различен од оној што го користат, со што повикот изгледа како да доаѓа од легитимен број.
- 02. Создавање на лажни СМС пораки (SMS spoofing) или алфа-ознаки:** измамниците го менуваат својот телефонски број за да се прикаже како име на компанија (на пример, AusPost). Тоа може да предизвика текстуалната порака да се појави во истиот разговор или нишка како и вистинските пораки од некоја организација.
- 03. Создавање на лажен имејл (Email spoofing):** измамниците ја менуваат својата имејл адреса или името на испраќачот за да изгледа дека имејлот е од доверлив извор. Тие можат да го фалсификуваат името што се прикажува во полето 'From' (Од) или имејл адресата, честопати со промена или додавање буква или број на легитимното име на доменот (на пример, @amaz0n.com наместо @amazon.com).

Чести измами со лажно претставување

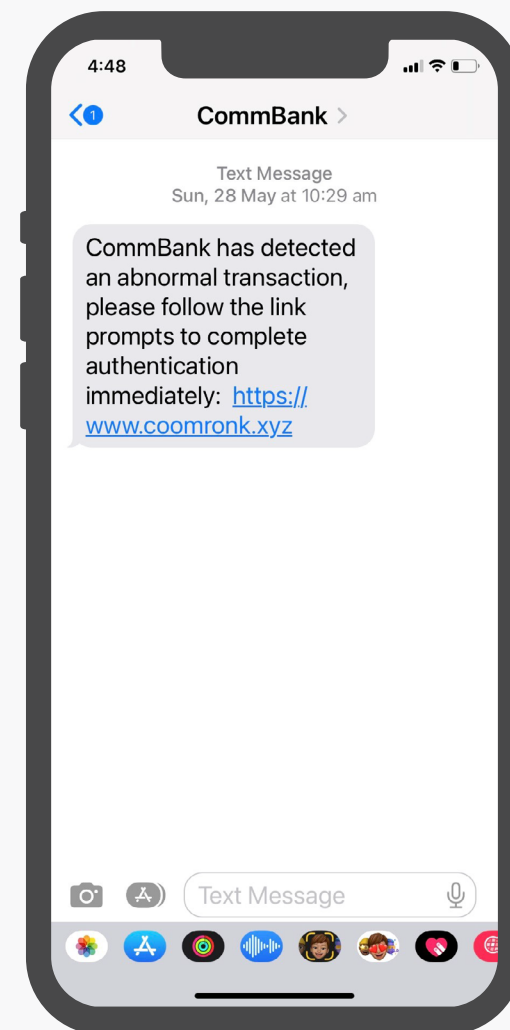
Измами со лажно претставување за банкарски работи

- Добивате телефонски повик или СМС порака од некој што тврди дека е од одделот за безбедност на вашата банка. Ве информира за сомнителна трансакција, тврдејќи дека вашата сметка е компромитирана. Ве убедува да префрлите пари на друга сметка за да ги „заштитите“ или за „понатамошна истрага“.
- Добивате текстуална порака или имејл со барање да кликнете на линк (врска) за да ги потврдите деталите за вашата сметка. Линкот ве води до лажна веб-страница наменета да ги земе вашето корисничко име, лозинка и други лични податоци.

i Како знаете дека се работи за измама?

Иако вашата банка може да ве контактира доколку постои некоја сомнителна активност на вашата сметка, таа никогаш нема да побара од вас да префрлите средства на друга сметка. Ниту, пак, ќе побара какви било податоци за сметката или лични податоци, вклучувајќи ја вашата лозинка, ПИН кодот или еднократна лозинка преку ненајавена СМС порака, имејл или телефонски повик.

Измамниците можат да направат телефонскиот број да изгледа како да е од повикувач од вашата банка, но не сметајте на ова како доказ за тоа со кого разговарате. Исто така, може да изгледа дека тие имаат информации за вас, но сите податоци што ги поседуваат веројатно се добиени со измама.



Пример на текст од лице кое се претставува како вработен од банка од лажен број, со кој бара од вас да кликнете на линк за да ги потврдите вашите податоци.

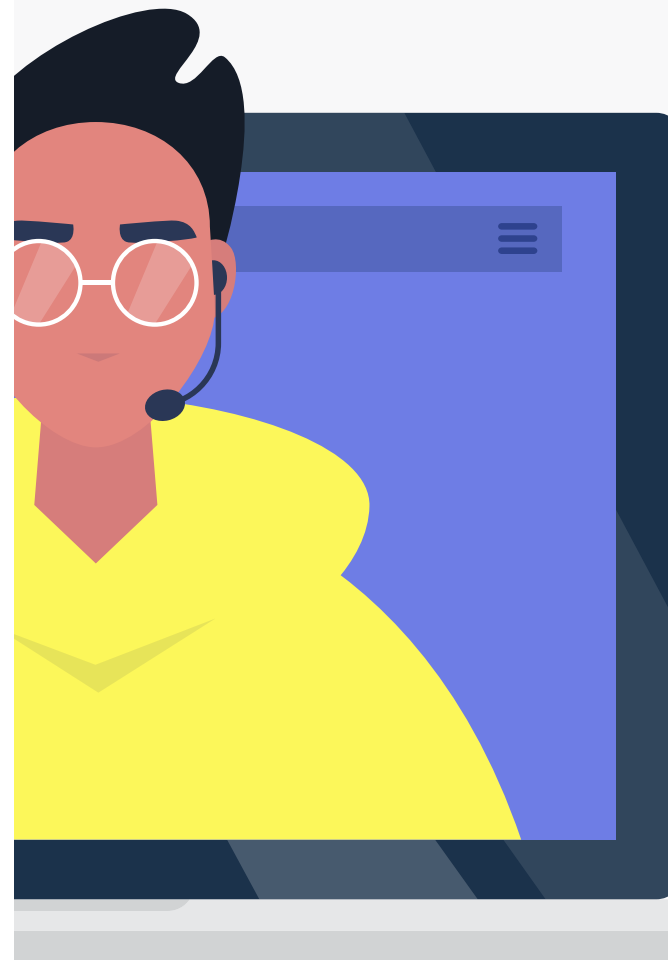
Измами во врска со техничка поддршка

- Повикувач кој се претставува како претставник на давател на интернет услуги, телекомуникациска или компјутерска компанија, ве информира за проблем со вашиот интернет или компјутер. Може да каже дека имало нелегален упад во компјутерот, дека има вирус, дека работи бавно или дека интернетот наскоро ќе биде исклучен. Ве насочува да преземете апликација или софтвер за да му дадете далечински пристап до вашиот компјутер за да може да го „поправи“.
- На екранот на вашиот компјутер се појавува порака со предупредување, со која се бара веднаш да се јавете на наведениот телефонски број за помош во врска со проблем што е откриен.

i Како знаете дека се работи за измама?

Легитимните компании никогаш нема да се јават за да ве информираат за проблем со вашата интернет-врска или компјутер (тие очекуваат вие да ги контактирате доколку има проблем). Тие никогаш нема да побараат од вас да преземете каков било софтвер или апликација што им дава пристап до вашиот уред.

Затворете ги сомнителните пораки што се јавуваат ненадејно (pop-up messages) со тоа што ќе кликнете на „x“ во горниот десен агол од рамката. Ако тоа не помогне, обидете се да кликнете надвор од рамката или да ја затворите веб-страницата на која се појавува. Ако пораката сè уште не е затворена, обидете се да ги држите копчињата ALT и F4 на вашиот Windows компјутер за да го затворите веб-прелистувачот. На Apple компјутер, изберете „Force Quit“ (присилно исклучување) од менито на Apple и изберете го прелистувачот што сакате да го затворите.



Измами за привремено блокирање на сметка

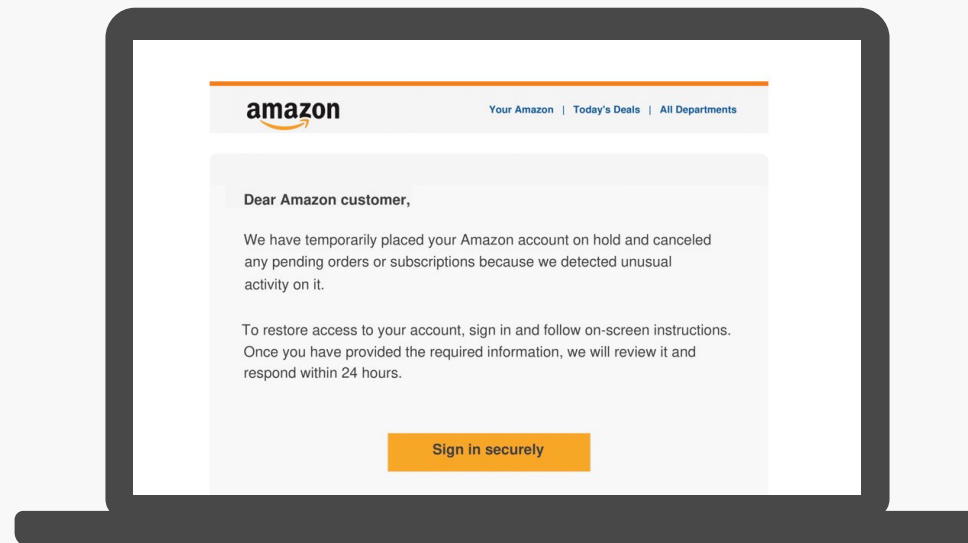
Добивате имејл или текстуална порака во која се тврди дека е од организација што ја познавате, како што се Amazon, PayPal или Netflix. Ве известуваат дека вашата сметка е привремено блокирана поради сомнителна активност и дека ќе треба да кликнете на линк за да го потврдите вашиот идентитет за да знаат дека тоа навистина сте вие.

Измамниците користат тактика на заплашување за да ве насочат да одите на лажна веб-страница која прибира лични податоци како што се вашето корисничко име, лозинка и детали за банкарската или кредитната картичка.

i Како знаете дека се работи за измама?

Amazon, PayPal и Netflix никогаш нема да побараат лични податоци како што се вашите лозинки, податоци за банкарска или кредитна картичка преку линк, ненајавено во имејл или СМС порака. Иако организациите се разликуваат во начинот на кој ги контактираат клиентите, најдобро е да не ризикувате и секогаш да ги третирате ваквите имејли, текстуални пораки или повици со претпазливост.

Доколку не сте сигурни дали пораката е навистина од компанијата од која тврди дека е, контактирајте ја компанијата директно така што ќе ги побарате нејзините податоци за контакт онлајн. Никогаш не ги користете податоците за контакт што ви се дадени во текстуалната порака, имејл или при телефонски повик.



Пример за имејл со измама во кој се тврди дека е од Amazon и ве поттикнува да кликнете на линкот за да ги наведете вашите лични податоци.

Внимавајте на тактики за заплашување

Измамниците користат тактики на заплашување за да создадат чувство на итност за да ве натераат да дејствувате. Следуваат неколку работи што можат да ги кажат за да го привлечат вашето внимание:

- Откриена е необична активност на сметката
- Неовластени обиди за најавување
- Вашата сметка е блокирана/заклучена
- Вашето плаќање беше одбиено
- Не можеме да ги потврдиме вашите податоци за наплата

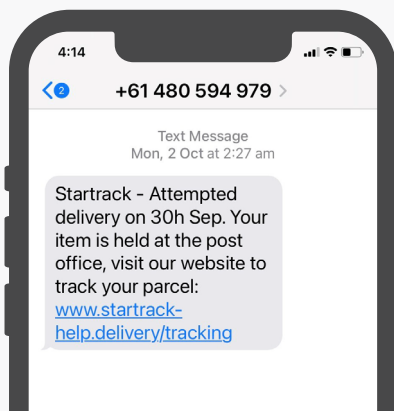
Измами за неуспешен обид за испорака

Добивате имејл или СМС порака во која се тврди дека е од Australia Post или курирска служба како што е FedEx, со која ве информираат дека има проблем или застој со доставата на вашиот пакет. За да го добиете вашиот пакет, ќе треба или да платите за трошоци за испорака или да ги „ажурирате“ вашите податоци“.

i Како знаете дека се работи за измама?

Australia Post, FedEx и другите легитимни курирски служби никогаш нема да испратат СМС порака, имејл или да се јават по телефон за да побараат лични податоци или плаќање. Доколку очекувате испорака, најдобро е да ја следите вашата испорака преку нивната безбедна апликација или преку услугата за онлајн следење во имејлот за потврда на вашата нарачка. Доколку немате имејл, јавете се директно во курирската служба и прашајте за статусот на вашата пратка.

Пример за текстуална порака во која се тврди дека е од курирска служба.



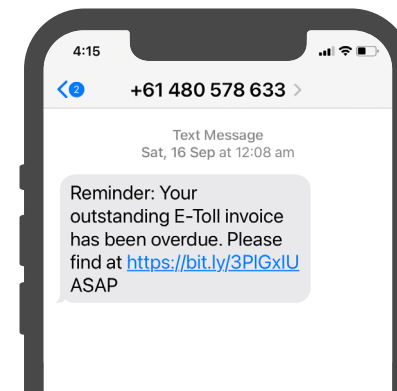
Измами во врска со патарина

Добивате СМС порака од оператор на патарина со која ве известува дека доцните со плаќањето на патарината. За да избегнете плаќање на казна, треба веднаш да преземете мерки, па затоа ви испраќа линк за да го организирате плаќањето, кој ве води до лажна веб-страница дизајнирана да ги украде вашите финансиски податоци.

i Како знаете дека се работи за измама?

Ако ви е испратена СМС порака во која се тврди дека имате задоцнета сметка за патарина или недоволно средства на сметката, можеби станува збор за измама. Посетете ја веб-страницата или апликацијата на операторот за патарини за да се најавите на вашата сметка и да ја проверите вашата неодамнешна активност.

Пример за измама во врска со патарина со текстуална порака.



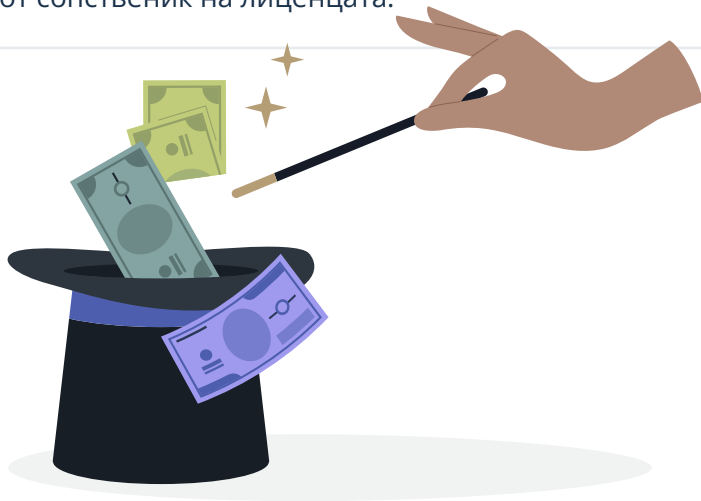
Измами за лажни инвестиции

Забележувате неверојатна инвестициска можност која се чини дека е поддржана од позната личност или финансиски инфлуенсер (влијателна личност). Ветува загарантиран висок приход со мал или никаков ризик. Кога ќе се распрашате, ќе бидете упатени кон веб-страница со професионален изглед и ќе добиете софистициран промотивен материјал.

i Како знаете дека се работи за измама?

Ако некоја понуда ви изгледа премногу добра за да биде вистина, веројатно е така. Измамниците користат тактика на висок притисок за да ве убедат да дејствувате брзо за да не „пропуштите нешто“. Внимавајте на имејли, веб-страници или реклами со препораки и претерани ветувања за голема заработувачка.

„Советникот“ кој ви помага може да тврди дека не му е потребна австралиска лиценца за финансиски услуги (AFS). Доколку ви ја достави, секогаш проверете дали лицето со кое имате работа е вистинскиот сопственик на лиценцата.



Измами со лажни веб-страници

Гледате реклама на Фејсбук за позната марка на скара што се продава за 100 долари, а нејзината редовна цена е 900 долари. Кликнувате на линкот за веб-страницата на продавачот и откривате дека има провизија од 2,99% за плаќање со кредитна картичка, па затоа избирате да платите со директен банкарски трансфер за да добиете дополнителен попуст од 5%. Добивате потврдасо имејл, но не и скара.

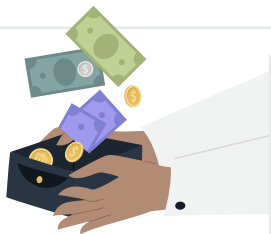
i Како знаете дека се работи за измама?

На лажните веб-страници има цени кои се премногу добри за да бидат вистински, необични начини на плаќање и други знаци за предупредување како што е URL-адреса која се обидува да изгледа како URL-адреса на официјална продавница (на пример, webberbbqs.com наспроти вистинската weber.com).

Измамниците може да плаќаат и за реклами на социјалните мрежи и пребарувачите (search engines) како што е Google (познати како спонзорирани реклами), затоа бидете внимателни кога кликувате на реклами од овој вид.

Најдобрите 10 совети како да се заштитите

- 01.** Внимавајте на ненајавени повици. Оставете ги повиците од телефонски броеви што не ги препознавате да одат во говорната пошта (voicemail).



- 02.** Застанете и размислете пред да дадете лични или финансиски податоци преку ненајавени пораки. Запрашајте се: дали пораката може да биде лажна?

- 03.** Пазете се од имејли во кои се користи тактика на заплашување. Проверете го името и имејл адресата што се прикажани. Дали се исти? На пример, во полето 'From' (Од) пишува 'Amazon Support' (Служба на Amazon за поддршка), но имејл адресата е amazonsupport830@gmail.com



- 04.** Не верувајте во текстуална порака само затоа што се појавува во истата нишка како и други пораки од организација што ја познавате. Пораката сè уште може да биде измама.

- 05.** Доколку не сте сигурни за пораката или повикот што сте го примиле, контактирајте ја организацијата од која се тврди дека доаѓа. Контактирајте ја преку нејзината официјална веб-страница или безбедна апликација на вашиот паметен телефон или таблет.

- 06.** Никогаш не ја давајте вашата лозинка, ПИН или еднократен код на никого преку телефон, дури и ако лицето тврди дека е од вашата банка или од владина агенција и гласно ги чита податоците за вашата сметка.



- 07.** Никогаш не кликувајте на линкови во СМС пораки. Иако е можно дека некои од нив се безбедни, најдобро е да не се ризикува. Истото важи и за прилозите и линковите во имејли, освен ако сте сигурни кој е испраќачот.

- 08.** Никогаш не ги следете упатствата од ненајавен повикувач кој сака да преземете апликација или да инсталирате софтвер што му овозможува пристап до вашиот уред. Веднаш спуштете ја слушалката.

- 09.** Никогаш не се најавувајте на вашите онлајн сметки преку линк во имејл или СМС порака. Наместо тоа, внесете ја URL-адресата на компанијата во вашиот веб-прелистувач или користете ја нивната безбедна апликација за пристап до вашата сметка.



- 10.** Пред да извршите онлајн плаќање, секогаш проверете ја URL-адресата на веб-страницата (дали е тоа официјалната страница?), проверете дали се наведени необични методи на плаќање и дали информациите се лошо формулирани или пак недостасуваат информации во деловите 'About Us' (За нас), 'Shipping and Returns' (Испорака и враќање на стока) и во другите делови што се наоѓаат на дното од веб-страницата.

Доколку некогаш се сомневате, пребарајте на интернет така што ќе го внесете името на организацијата или веб-страницата за која станува збор и зборот „scam“ (измама).

Мислите дека сте биле измамени?

Каде да се обратите за помош

Измата може да биде финансиски и емоционално исцрпувачка, па затоа е важно да побарате помош и да дејствувате брзо. Постојат неколку чекори што можете да ги преземете:

1. Веднаш контактирајте ја вашата банка за да спречите какви било понатамошни трансакции.
2. Контактирајте ја IDCARE, бесплатна служба за поддршка на луѓе кои биле жртви на измама или кражба на идентитет. Јавете се на 1800 595 160 или посетете ја веб-страницата idcare.org
3. Веднаш променете ги лозинките и осигурајте се дека тие се силни.
4. Пријавете ја изматата на Scamwatch за да ги предупредите другите: scamwatch.gov.au/report-a-scam
5. Добијте поддршка за себе. Доколку не се чувствувате пријатно да разговарате со пријателите или семејството, контактирајте ги Lifeline или Beyond Blue за доверлив разговор. А ако сте изгубиле значителна сума пари, обратете се на Националната телефонска линија за помош во врска со долгови (National Debt Helpline).

Beyond Blue: 1300 22 4636 (24/7) или посетете ја веб-страницата beyondblue.org.au

Lifeline: 13 11 14 (24/7) или посетете ја веб-страницата lifeline.org.au

National Debt Helpline: 1800 007 007 (во работни денови од 9:30 наутро до 4:30 попладне) или посетете ја веб-страницата ndh.org.au

За повеќе информации

Кликнете на плочките подолу за да дознаете повеќе:



[Little Book of Scams \(Мала книга на измами\)](#) е меѓународно призната алатка која ќе ви помогне да дознаете повеќе за голем број вообичаени измами и како можете да се заштитите од нив.

Посетете ја веб-страницата на [Scamwatch](#) за да бидете во тек со најновите измами и совети за тоа како да се заштитите од нив.



3а Be Connected

Be Connected е иницијатива на австралиската влада која се фокусира на подобрување на дигиталните вештини и самодовербата на постарите Австралијци, како и на нивната безбедност на интернет преку бесплатни компјутерски часови, кратки онлајн курсеви и многу други активности на различни теми. Со веб-страницата и образовната содржина на Be Connected управува [Претседателот на Комисијата за онлајн безбедност \(eSafety Commissioner\)](#).



3а Scamwatch

Scamwatch го води Националниот центар за борба против измами, кој беше формиран за да ја направи Австралија потешка цел за измамниците. Ја подигнува свеста за измамите преку подучување на заедницата за тоа како да препознава, избегнува и пријавува измами. Центарот за борба против измами споделува информации од пријави за измами и соработува со владата, органите за спроведување на законот и приватниот сектор за да ги отежне и спречи измамите.