# Дали можете да забележите измама?

Кога се наоѓаме на интернет, не можеме секогаш да бидеме сигурни дека луѓето се тие што се претставуваат. Да бидеме свесни за нив е еден од најважните чекори за да ги избегнеме тие интернетски измамници. Штом ќе бидете свесни за нивните трикови, би требало да ви биде полесно за забележите измама кога ќе ја видите.

## Имами за кражба на идентитет

Измамите за кражба на идентитет се најчести облици на измама на интернет. Тие може да изгледаат дека се од веродостојна организација и целта им е да ве натераат да ги дадете вашите лични податоци, како на пример вашата банкарска сметка, бројот на кредитна картичка, корисничкото име и лозинките.

### Може да се јават во голем број облици:

- неочекувана е-пошта, текстуални пораки или телефонски повици во кои од вас се бара да ги потврдите, ажурирате или да ги внесете повторно вашите лични податоци,
- итни или заканувачки пораки што ви кажуваат дека нешто необично се случува со вашата сметка, или дека сметката ќе се затвори па треба да кликнете на некоја врска за да го поправите проблемот,
- неочекувана е-пошта што ви бара да отворите или преземете датотека .exe или .zip.

Совет: ако не сте сигурни за пораката што сте ја примиле, побарајте ја на интернет компанијата што се чини дека ви ја пратила пораката и контактирајте со неа директно.

### Не брзајте. Прочитајте ја повторно пораката.

- Кој ви ја прати? Дали се работи за официјална адреса на е-пошта или некоја чудна адреса?
- Кој е примателот на пораката? Ако наместо вашето име во пораката пишува „Почитуван клиенту“, тоа треба да ви биде сомнително.
- Дали содржината на пораката има граматички грешки и е напишана лошо? Ова може да биде знак дека ви ја пратил некој измамник.

### Не треба:

- да кликнувате на која било врска,
- да отворате какви било прилози, бидејќи тие може да содржат компјутерски вируси,
- да ги користите деталите за контакт дадени во пораката бидејќи тие може да бидат лажни.

# Даночни измами и измами поврзани со Medicare

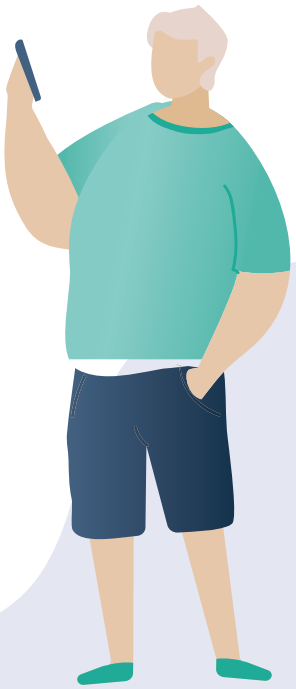
Измамниците се претставуваат дека се вработени во Австралиската даночна управа, Medicare и други владини организации со цел да добијат пари и лични податоци од жртвите преку лажни веб-страници, е-пораки, текстуални пораки и телефонски повици.

Важно е да запомнете дека Австралиската даночна управа (Australian Tax Office - ATO) никогаш нема:

- да ви прати е-пошта или текстуални пораки во кои ви бара лични податоци, како на пример, вашиот даночен број (TFN) или деталите на вашата кредитна картичка или банката,
- да ви бара да платите провизија за да го примите вашиот повраток на данок, или да спречите да бидете уапсени заради затајување данок,
- да ви прати е-пошта со врска до онлајн услуга што ви ги бара личните податоци,
- да ви прати датотеки што треба да ги преземете или да ви побара да преземете софтвер.

## Што можете да направите за да бидете умешни и безбедни?

- Не треба да кликнувате на кои било врски или да преземате какви било прилози.
- Не давајте ги никому вашите лични податоци, како што е даночниот број, датумот на раѓање, банкарската сметка или деталите на вашата кредитна картичка или банката.
- Ако не сте сигурни дали телефонската порака е вистинска, не користете ги дадените детали за контакт, а наместо тоа, извршете пребарување на бројот на организацијата.
- Треба да ја познавате вашата даночна состојба – дали постои веројатност дека треба да добиете повраток на данок или должите плаќања?
- Најавете се на вашата официјална сметка на myGov внесувајќи ја адресата рачно, наместо да кликнувате на врска.
- Проверете дали е-поштата што ја примивте е од вистинска адреса на Австралиската даночна управа што завршува со @ato.gov.au
- Дури и ако изгледа дека се наоѓате на веб-страницата на ATO или на myGov, проверете дали адресата завршува со .gov.au (наместо со, на пример, .com.au, .org.au или .net.au).
- Проверете дали во пораката постојат граматички грешки.
- Кога добивате пораки што не се адресирани директно до вас, тоа треба да ви биде сомнително.



# Измами поврзани со агенции за романтично дружење

Измамниците создаваат лажни онлајн профили на социјалните мрежи или веб-страниците за наоѓање партнери за да воспостават контакт со жртвите. Нивната цел е се здобијат со вашата доверба пред да ви побараат пари.

### Што можете да направите за да бидете умешни и безбедни?

**Треба да бидете внимателни со:**

- луѓе кои многу брзо искажуваат длабоки чувства за вас пред да ви побараат пари или „заем“,
- луѓе кои избегнуваат да се сретнат лично со вас и наоѓаат изговори зошто не можат да патуваат за да ве видат,
- луѓе чии онлајн профили не се совпаѓаат со она што ви го кажале за себе.

**Треба да:**

- извршите пребарување на Google за да проверите дали нивните слики се навистина нивни, или биле земени од друго место на интернет. Одете на images.google.com и кликнете на иконата со камера
- треба да станете сомнителни кога ќе почнат да спомнуваат „проблеми со пари“ или дека им треба парична помош за „итен случај“.

**Не треба:**

- да им пренесувате пари на лица со кои сте контактирале само преку телефон или е-пошта,
- да праќате лични податоци како што се датумот на раѓање, детали на банка или кредитна картичка.

# Измами од техничка поддршка

Овие измами обично почнуваат со повик или е-пошта што доаѓа од голема, добро позната организација што ве информира дека имате проблем со компјутерот или со интернетот и дека тие можат да го поправат.

### Што можете да направите за да бидете вешти и безбедни?

- Не дозволувајте им далечински пристап до вашиот компјутер.
- Не давајте им лични податоци како што се вашата банкарска сметка или детали на кредитна картичка.
- Не купувајте софтвер преку повик или е-пошта што не сте ги побарале.
- Игнорирајте ги скок-пораките што ви велат да ја повикате техничката поддршка.

**Големите организации очекуваат да ги повикате кога имате проблем со вашата интернет-врска или со компјутерот. Тие нема да ве повикаат.**

# Ми треба помош, се сомневам дека сум жртва на измама

Ако сметате дека сте биле жртва на измама, не треба да се чувствувате засрамено и да не кажувате никому. Постојат чекори што можете да ги направите за да го поправите проблемот:

- контактирајте со вашата банка и запрете го измамникот да врши какви било други плаќања,
- пријавете ја измамата кај Австралиската комисија за конкуренција и потрошувачи на scamwatch.gov.au; тие можат да ви помогнат со дополнителни совети
- подигнете ја свеста. Ако познавате некого друг кој можеби е жртва на измама, информирајте го.

Ако не сте сигурни дали некоја порака што сте ја примиле е навистина од Австралиската даночна управа, или сте биле жртва на измама поврзана со данок, повикајте ја **Дежурната линија за измама** поврзана со **Даночната управа (ATO Scam Hotline)** на **1800 008 540**.

Бидете во тек со измамите поврзани со Даночната управа посетувајќи ја веб-страницата ato.gov.au/scams

Ако сте загрижени дека вашите лични податоци биле откриени или злоупотребени, контактирајте со Австралиската служба за национален идентитет и кибер-поддршка (Australia's National Identity and Cyber Support Service) **IDCARE** на **1300 432 273** или idcare.org

**Запомнете:**

секогаш постои некој што може да ви помогне, тоа може да бидат луѓето од scamwatch.gov.au, или пријател или семеен член со технички знаења, или дури и локален компјутерски клуб.

Измамите имаат за цел да ја злоупотребат вашата добра природа, но интернетот може да биде безбедно место што можете да го истражувате ако сте внимателни со личните податоци онлајн, ако користите здрав разум кога праќате пари некому и ако се штитите.


## Најдете време да ја разгледате веб-локацијата Be Connected

Be Connected е една богата веб-локација со бесплатни ресурси специјално дизајнирани да им помогнат на постарите Австралијци да се поврзат безбедно онлајн и да вршат со самодоверба навигација низ дигиталниот свет. Исто така, локацијата е корисна за семејствата и организациите во заедницата што сакаат да им помогнат на постарите лица да пристапат до сите придобивки од интернетот.

beconnected.esafety.gov.au