



Australian Government



Одмах предузимајте мере.
Будите безбедни.

Како да будете безбедни када сте онлајн

Поједностављена верзија



Укратко о овом водичу



Ми смо Влада Аустралије.

Ми смо написали овај водич.



Неке речи смо написали **подебљаним** словима.

Ове речи објашњавамо.

Списак ових речи се такође налази на страници 28.



Можете замолити некога коме верујете да вам помогне:

- да прочитате овај водич.
- да сазнате више информација.



Ово је кратак преглед другог водича и написан је поједностављеним језиком.

Укључује само најважније идеје.



Тај други водич можете наћи на нашем веб-сајту.

www.actnowstaysecure.gov.au

Шта се налази у овом водичу?

Чему служи овај водич	4
Обезбедите своје налоге	6
Проверите подешавања како бисте заштитили своје податке	10
Заштитите своје уређаје	16
Онлајн преваре	20
Реците нешто	25
Списак речи	28
Контактирајте нас	30

Чему служи овај водич



Сви морамо да размишљамо о томе како да будемо безбедни када смо онлајн.

То се зове **сајбер** безбедност.



Сајбер значи нешто што има везе са интернетом.



Овај водич објашњава шта можете да урадите да бисте се заштитили када сте онлајн.

На пример, од **сајбер криминала**.



Сајбер криминал је када криминалци користе интернет за криминал.

На пример, могу да користе интернет:

- да вам украду личне податке
- да преузму ваше онлајн налоге или профиле.

Сајбер криминал може да се догоди на било ком уређају.



То укључује ваш:

- компјутер
- паметни телефон
- паметни сат.



Постоје ствари које можете урадити како бисте се заштитили од сајбер криминала.



У наставку ћемо вам објаснити шта можете урадити.

Обезбедите своје налоге



Треба да размислите о томе како можете да обезбедите своје онлајн налоге.

Користите јаке лозинке у облику различитих фраза



Лозинка у облику фразе је јача врста лозинке.

Веома је тешко другим људима да је погоде.



Коришћење јаких лозинки у облику различитих фраза је један од најбољих начина да заштитите своје налоге.



Пожељно је да за сваки онлајн налог користите другачију фразу као лозинку.



Јаке лозинке у облику фразе се састоје од:

- 4 или више неповезаних речи
- 15 или више слова и бројева.



Можете укључити и нека велика слова.



Такође можете користити симболе, као што су:

- цртица
- ознака за долар
- ознака @, која је део имејл адресе.



Не би требало да користите ваше личне податке као део фразе коју користите као лозинку.



На пример:

- ваш датум рођења
- имена чланова ваше породице или кућних љубимаца.

Додајте још који корак за пријављивање на налоге



Своје онлајн налоге можете заштитити **вишефакторском аутентификацијом (MFA)**.

MFA је када сваки пут користите 2 или више различитих начина да се пријавите на свој налог.



На пример, можда ће прво бити потребно да унесете своју лозинку у облику фразе.

А затим уносите шифру коју добијете путем телефона.

Можда ћете моћи да изаберете:



- да имате апликацију на телефону путем које ћете добити шифру



- да добијете шифру путем имејла



- да добијете шифру путем SMS поруке.



MFA отежава другим људима да уђу у ваше онлајн налоге.

Чак иако открију вашу лозинку у облику фразе.

Проверите подешавања како бисте заштитили своје податке



Можете проверити да сте подесили уређај тако да вам штити личне податке када сте онлајн.



То укључује подешавања:

- на вашим онлајн налозима
- на уређајима
- у апликацијама.



Можете:

- променити подешавања
- изабрати којим апликацијама дозвољавате да користе ваше податке.

Можете пронаћи подешавања на вашем уређају тако што ћете:



- потражити иконицу која личи на зупчаник
- или
- укупати 'подешавања' у поље за претраживање на вашем уређају.



Можете пронаћи подешавања у апликацији или на онлајн налогу тако што ћете ући у мени.

Ознака за мени обично изгледа као 3 праве линије.



Нека од ових подешавања могу поделити податке о томе:

- ко сте
- где се налазите
- где живите.



Ако делите те податке када сте онлајн, тиме ризикујете да будете жртва сајбер криминала.



Сајбер криминалци могу искористити ове податке да се представе као ви.

На пример, могу да користе следеће податке:



- где живите



- имена чланова ваше породице



- имена ваших кућних љубимаца.



Можете подесити своје налоге тако да само људи које познајете могу да виде ваш профил на друштвеним медијима.

На пример, ваш профил на Фејсбуку.



Оваква подешавања се обично називају подешавања за приватност.



Такође можете да контролишете **подешавања за локацију**.

Подешавања за локацију показују где се налази ваш уређај.



Подешавања за локацију можете укључити или искључити.

Такође можете изабрати апликације које могу да користе ваша подешавања за локацију.



То можете урадити за:

- ваше онлајн налоге
- уређаје
- апликације.

Неке апликације вас такође могу питати да ли дозвољавате:



- да користе вашу камеру



- да виде ваше фотографије.



Дозволите коришћење камере и приступ фотографијама само оним апликацијама које су вам познате.

Заштитите своје уређаје



Требало би да размислите о томе како можете да заштитите своје уређаје како бисте били безбедни када сте онлајн.

На пример, ваш телефон или паметни сат.



Ово је важно за уређаје који имају приступ интернету.

Ажурирајте своје уређаје



Можете ажурирати своје уређаје како бисте били безбедни када сте онлајн.

На пример, ваш телефон и лаптоп.



То се на вашем уређају можда зове ажурирање софтвера.



Ажурирања помажу уређају да се заштити од сајбер криминала.



Можете наместити уређај тако да се сам ажурира.



На нашем веб-сајту можете сазнати више о томе како да ажурирате своје уређаје.

[www.actnowstaysecure.gov.au/
cyber-safe-actions](http://www.actnowstaysecure.gov.au/cyber-safe-actions)

Јавне Wi-Fi мреже



Треба да будете опрезни када користите **јавну Wi-Fi мрежу**.



Јавна Wi-Fi мрежа је бесплатан бежични интернет који можете да користите на јавним местима.



На пример:

- у кафићу
- на аеродрому
- у хотелу.



Треба да будете опрезни са подацима које уносите на веб-сајт док користите јавну Wi-Fi мрежу.



На пример, ваше:

- банковне податке
- имејл налоге
- профиле на друштвеним медијима.



Неки сајбер криминалци могу користити јавну Wi-Fi мрежу:

- да прате шта радите онлајн
- да украду ваше податке.

То је зато што:



- свако може да користи ту мрежу



- теже је заштитити уређаје.



На нашем веб-сајту можете сазнати више о томе како да будете безбедни док користите јавну Wi-Fi мрежу.

www.actnowstaysecure.gov.au/cyber-safe-actions

Онлајн преваре



Онлајн превара је када неко покуша:

- да вас насамари
- да вам узме новац.



Онлајн преварант је неко ко се бави онлајн преварама.

Онлајн преваранти могу вас преварити путем:



- SMS поруке или телефонског позива
- имејла
- друштвених медија
- веб-сајта.



Могу деловати пријатељски.

Али могу да вас насамаре тако да им ви откријете своје податке.

Они то могу искористити:



- да се пријаве на ваше онлајн налоге



- да се представе као ви



- да вам украду новац.

Онлајн преваранти такође могу:



- да отворе лажне налоге како би вас насамарили



- да поделе линкове и рекламе са вама како бисте кликнули на њих.

Како да препознате онлајн превару

Можда је у питању онлајн превара ако:



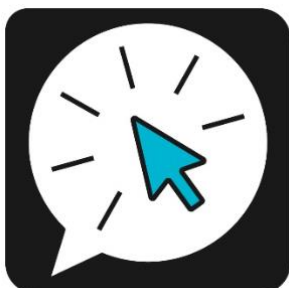
- се тражи да урадите нешто на брзину



- нуди вам се пуно новца



- тражи се новац од вас



- тражи се да кликнете на линк.



Онлајн преваранти такође могу да се представљају да су организација коју познајете и којој верујете.

На пример, ваша банка.



Онлајн преваранти то раде да бисте им открили ваше личне податке.



Треба да прекинете разговор са особом ако мислите да је онлајн преварант.



Треба да проверите да ли је та особа заиста она за коју се представља.

Можете контактирати ту особу или организацију тако што ћете користити податке којима верујете и које сте сами пронашли.



Реагујте брзо како бисте се заштитили ако посумњате да нешто није како треба.

Пријављивање онлајн превара



Служба против онлајн превара, Scamwatch, помаже Аустралијанцима да:

- разумеју онлајн преваре
- пријаве онлајн преваре.



Служба Scamwatch такође помаже Аустралијанцима који су били жртве онлајн превара.



Можете пријавити онлајн преваре преко веб-сајта службе Scamwatch.

www.scamwatch.gov.au/report-a-scam

Реците нешто



Треба да пренесете то што знате како би други људи могли да се заштите када су онлајн.

То укључује:



- пријављивање сајбер криминала



- дељење онога што знате са породицом и пријатељима.



У наставку ћемо вам објаснити како можете да кажете нешто.

Пријављивање сајбер криминала

Пријављивање сајбер криминала помаже влади:



- да научи како сајбер криминалци покушавају да нападну људе



- да заштити више људи.



Можете пријавити сајбер криминал преко веб-сајта ReportCyber.

www.cyber.gov.au/report

Разговарајте са породицом и пријатељима о томе како да будете безбедни када сте онлајн



Треба да поделите своје савете о томе како да будете безбедни када сте онлајн са својом породицом и пријатељима.

Такође можете да научите нешто од њих.



Можете да заштитите себе и друге око себе тако што ћете поделити то што знате о томе како да будете безбедни када сте онлајн.



Ово је такође важно ако делите уређаје са другима.

Списак речи

У овом списку се објашњава значење речи које су написане **подебљаним** словима у овом водичу.



Сајбер

Сајбер значи нешто што има везе са интернетом.

Сајбер криминал



Сајбер криминал је када криминалци користе интернет за криминал.

На пример, могу да користе интернет:

- да вам украду личне податке
- да преузму ваше онлајн налоге.



Подешавања за локацију

Подешавања за локацију показују где се налази ваш уређај.



Вишефакторска аутентификација (MFA)

MFA је када сваки пут користите 2 или више различитих начина да се пријавите на свој налог.



Лозинка у облику фразе

Лозинка у облику фразе је јача врста лозинке.

Веома је тешко другим људима да је погоде.



Јавна Wi-Fi мрежа

Јавна Wi-Fi мрежа је бесплатан бежични интернет који можете да користите на јавним местима.



Онлајн преваре

Онлајн преваре су када неко покуша:

- да вас насамари
- да вам узме новац.



Онлајн преваранти

Онлајн преварант је неко ко се бави онлајн преварама.

Контактирајте нас



Можете позвати информативну линију за сајбер безбедност у Аустралији (Australian Cyber Security Hotline).

1300 292 371



Можете посетити наш веб-сајт.

www.actnowstaysecure.gov.au



Можете пријавити сајбер криминал преко веб-сајта ReportCyber.

www.cyber.gov.au/report



Група за приступ информацијама (The Information Access Group) је саставила овај документ на поједностављеном језику користиће фотографије за комерцијалну употребу и наменске слике. Ове слике се не могу поново користити без одобрења. За све упите у вези са сликама, посетите www.informationaccessgroup.com. Наведите посао број 6342.
