Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

КАКО БЕЗБЕДНО ДА КОРИСТИТЕ ИНТЕРНЕТ

ПРИРАЧНИК ЗА ПОСТАРИ ЛИЦА

cyber.gov.au

Вовед

Интернетот ви овозможува да одржувате контакти со пријателите и семејството, да учите на нови теми, па дури и да играте игри.

Исто како што го ставате сигурносниот појас пред да возите, треба да преземете мерки пред да користите интернет за бидете побезбедни.

Австралискиот центар за сајбер безбедност (Australian Cyber Security Centre - ACSC) сака да осигура сите луѓе да бидат безбедни кога се онлајн. Во овој документ се опфатени некои основни работи за сајбер безбедноста кои можете да ги правите за да се заштитите кога користите интернет.

Австралискиот центар за сајбер безбедност (ACSC), како дел од Австралиската управа за разузнавање (Australian Signals Directorate - ASD), нуди совети, помош и оперативни одговори за спречување, откривање и санирање на сајбер закани на Австралија. ACSC е тука за да помогне Австралија да стане најсигурно место за поврзување на интернет.
За повеќе информации, упатства и совети во врска со сајбер безбедноста, посетете ја веб-страницата cyber.gov.au

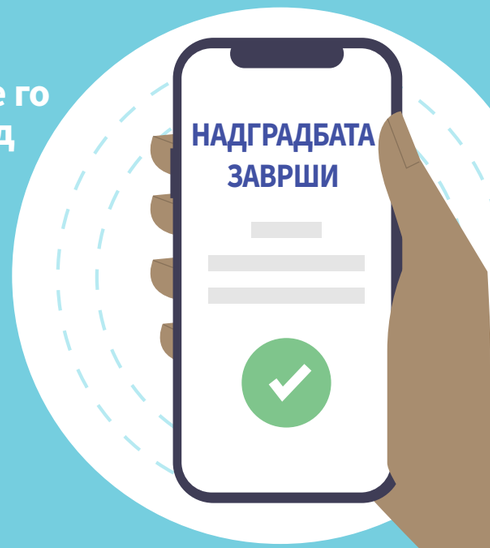
Сајбер безбедност за постари лица

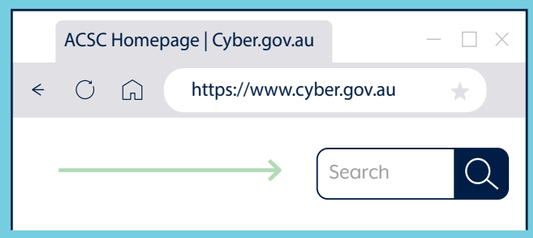
Совет бр.1: Надградувајте го софтверот на вашиот уред

Надградувањето на софтверот е како сервисирање на вашата кола. Ја подобрува работата на вашиот уред и го прави побезбеден.

Сајбер криминалците секогаш наоѓаат нови начини незаконски да влегуваат во уредите. Со автоматско инсталирање на надградби на вашиот уред може да се отстранат сите слабости во вашиот софтвер и да се спречи хакерите да влезат во вашиот уред.

За да најдете повеќе информации, барајте 'Updates' на cyber.gov.au.





ДАЛИ ЗНАЕВТЕ:
Со ажурирањето може исто така да бидат додадени нови функции на вашиот уред и да го направат побрз.

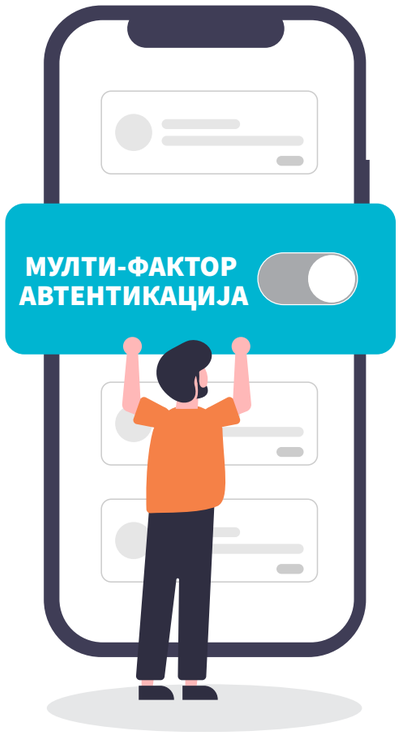
Совет бр.2: Вклучете ја мулти-фактор автентикацијата

Мулти-фактор автентикацијата на вашата сметка е исто што и безбедносната мрежа на прозорците и вратите во вашиот дом.
Таа ве штити од криминалци кои се обидуваат да провалат.

Кога мулти-фактор автентикација е активирана, треба да дадете повеќе информации за да имате пристап на вашата сметка. На пример, можеби ќе треба да ја внесете вашата лозинка и шифра во форма на текстуална порака за да се најавите на вашиот профил на социјалните медиуми.

Повеќекратните слоеви им отежнуваат на сајбер криминалците незаконски да влезат во вашата сметка. Тие можеби ќе успеат да откријат еден дел, на пример, вашата лозинка, меѓутоа сè уште ќе треба да ги најдат другите парчиња од сложувалката за да имаат пристап до вашата сметка.

За да најдете повеќе информации, барајте 'Multi-factor authentication' или 'MFA' на cyber.gov.au



ЗАПАМТЕТЕ:

Ако ви треба помош да ја вклучите мулти-фактор автентикацијата, побарајте да ви помогне пријател или член од семејството.

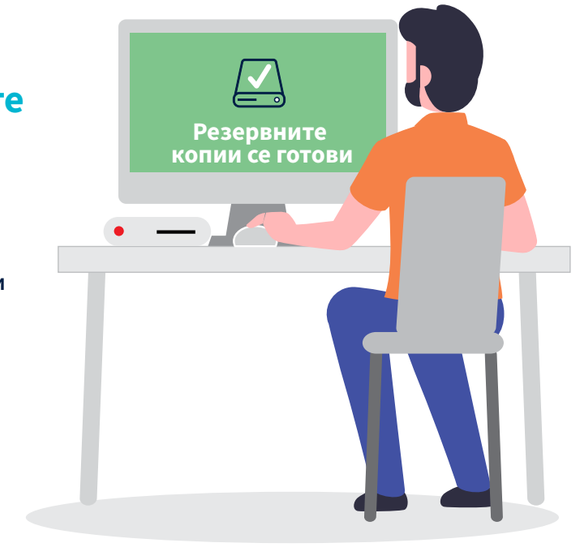
Совет бр.3: Правете резервни копии на податоците во вашите уреди

Тоа е кога правите копија на вашите важни датотеки и ги ставате на сигурно место.
Исто е како да фотокопирате драгоцени фотографии за да ги чувате во сеф во случај да ги изгубите оригиналите.

Кога правите резервни копии на податоците во вашиот компјутер, телефон или таблет, тие се зачувуваат онлајн или на друг уред. Ќе бидете спокојни ако имате резервни копии на вашите датотеки и драги фотографии.

Ако се случи нешто со вашиот уред или ако во сметката незаконски ви влезат сајбер криминалци, можете лесно да ги обновите вашите датотеки од резервните копии.

За да најдете повеќе информации, барајте 'Backups' на cyber.gov.au



ДАЛИ ЗНАЕВТЕ:

Со редовното правење на резервни копии на податоците во вашиот уред секогаш ќе имате пристап до вашите најнови датотетки.

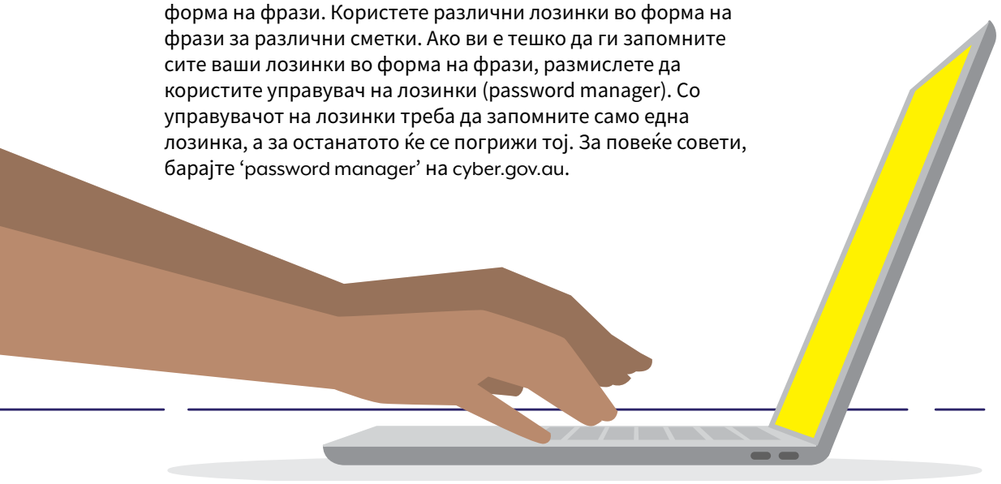
Совет бр.4: Користете лозинка во форма на фраза

Ако лозинката од еден збор става катанец на вашата сметка, лозинката во форма на фраза ѝ дава сопствен безбедносен систем! Овие лозинки се појаки и побезбедни верзии на лозинките од единечни зборови.

Кога не можете да ја вклучите MFA, користете лозинка во форма на фраза за да ја обезбедите вашата сметка. За лозинка се користи фраза од четири или повеќе случајно избрани зборови. Ова им отежнува на сајбер криминалците да ја погодат, но за вас ќе биде лесна да ја запамтите.

Кога креирате лозинка во форма на фраза, направете ја:

- **Долга.** Колку е подолга фразата, толку подобро. Стремете се фразата да има најмалку 14 букви. Одлично ќе биде ако изберете четири или повеќе случајно избрани зборови кои ќе ги запамтите. На пример, “чамец од компир со виолетова патка”.
- **Непредвидлива.** Колку помалку може да се предвиди вашата лозинка во форма на фраза, толку подобро. Реченициите може да бидат одлични лозинки, но тие полесно се предвидуваат. Лозинката ќе биде посилна ако е комбинација од четири или повеќе случајно избрани зборови.
- **Единствена.** Не ги користете повторно вашите лозинки во форма на фрази. Користете различни лозинки во форма на фрази за различни сметки. Ако ви е тешко да ги запомните сите ваши лозинки во форма на фрази, размислете да користите управувач на лозинки (password manager). Со управувачот на лозинки треба да запомните само една лозинка, а за останатото ќе се погрижи тој. За повеќе совети, барајте ‘password manager’ на cyber.gov.au.



Дознајте повеќе како се создаваат сигурни лозинки ако барате ‘Passphrases’ на cyber.gov.au

Совет бр.5: Препознавајте и пријавувајте измами

Колку побрзо ќе пријавите измама, толку побрзо ќе можеме да реагираме.

Ако верувате дека некој се обидува да користи интернет за да ве измами, подобро е да бидете проактивни и претпазливи отколку да бидете искористени.

Ако звучи премногу добро за да биде вистина, тогаш веројатно не е. Иако пораката може да вели дека сте добиле награда или дека вашиот компјутер има вирус, пораката не ви е испратена само вам.

Таа можеби доаѓа од измамник кој сака да ве искористи.

Запамтете, измамниците често ќе се преправаат дека се поединец или организација на кои им верувате. Бидете сомнителни ако примите порака што изгледа како да е од некој на кого му верувате, но користи нов телефонски број, имејл адреса или профил на социјалните мрежи. Пред да одговорите, проверете дали лицето или организацијата што ви ја испраќа пораката се тие што велат дека се така што ќе ги контактирате преку канал во кој можете да имате доверба. На пример, ако примите текстуална порака што изгледа како да е од некое од вашите деца, но е од нов број, не одговарајте. Испратете им порака на социјалните мрежи за прво да проверите дали навистина го сменил/а телефонскиот број.

ДАЛИ ЗНАЕВТЕ:

Сајбер криминалците се итри и може да користат познато име и имејл адреса. Бидете претпазливи ако:

- **од вас се бара итно да платите сметка**
- **од вас се бара да ги смените вашите податоци или лозинка**
- **од вас се бара да притиснете на врска или да отворите прилог.**

Заклучок

Сега кога сте ‘вооружени’ со знаење како побезбедно да користите интернет, можете да пребарувате со доверба и да продолжите да уживате во времето што го поминувате онлајн.

Само запамтете, сајбер криминалците секогаш изнајдуваат нови начини да ги измамуваат луѓето.

Никогаш нема да ви наштети одвреме навреме да го освежувате вашето познавање на сајбер безбедноста и да научите нови начини како да бидете безбедни.

Бонус совети

Сакате ли да научите нови начини како да бидете безбедни онлајн? Погледнете ги следните совети.

Размислете за тоа што го објавувате.

Внимателно размислете за информациите кои ги споделувате онлајн и кој ќе ги види. Прифаќајте барања за пријателство само од лица кои ги познавате во вистинскиот живот.

Добивајте предупредувања за нови закани.

Пријавете се да ја користите нашата бесплатна услуга за предупредување. Со тоа ќе бидете информирани секогаш кога ќе откриеме нови сајбер закани.

Преку услугата исто така ќе добивате совети што да правите ако бидете нападнати.

Разговарајте со семејството и пријателите за сајбер безбедноста.

Сега кога сте вешти за сајбер безбедноста, споделете го вашето знаење со семејството и пријателите. Вашето знаење може да им помогне да излезат од незгодна ситуација во иднина!

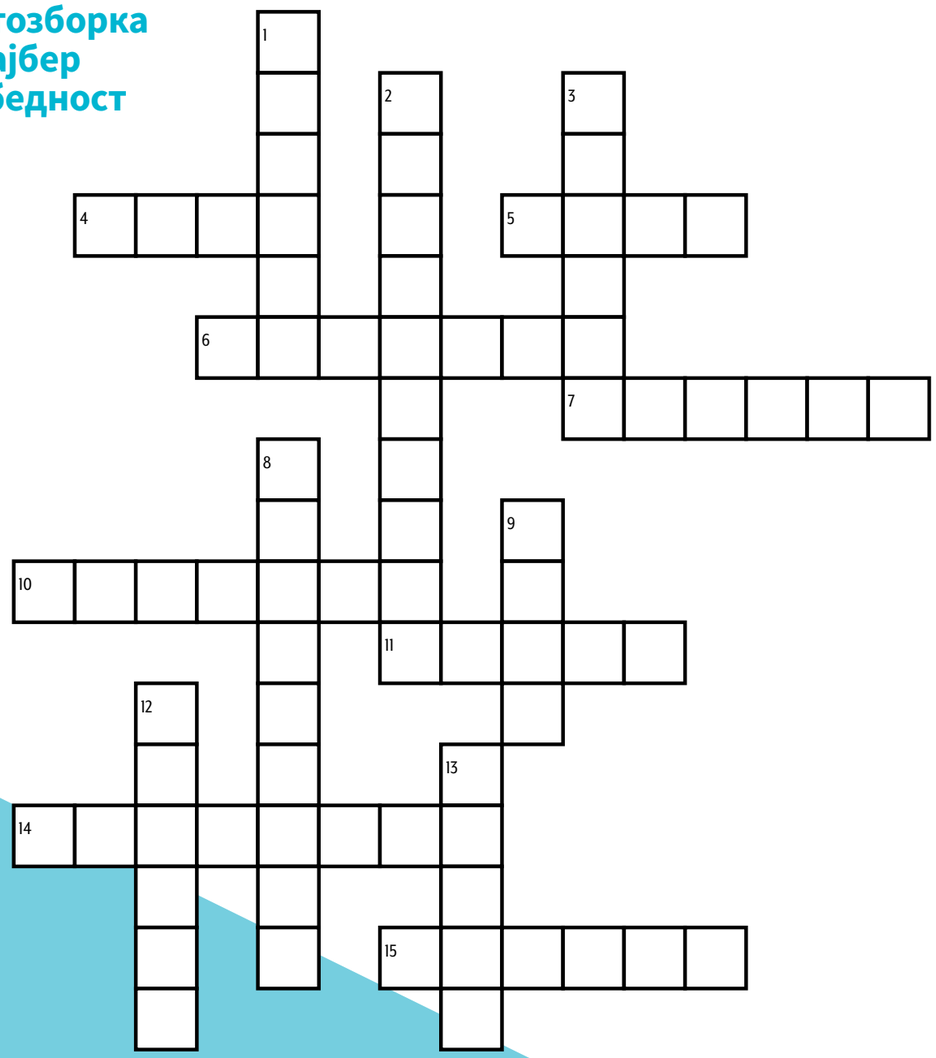
Кога вршите банкарски работи или пазарите онлајн, избегнувајте да користите јавна Wi-Fi мрежа.

Јавната Wi-Fi мрежа е одлична за гледање на видео записи или читање на веб-страници, но сите работи во врска со пари правете ги преку домашниот интернет. Јавните Wi-Fi мрежи можат да бидат ризични.

Пријавете сајбер напади и инциденти за Австралија да биде безбедна.

Ако мислите дека сте биле жртва на сајбер криминал, делувајте брзо. Повеќе совети има на cyber.gov.au

Крстозборка за сајбер безбедност



ВЕРТИКАЛНО

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computerw's files
13. Relating to, or involving computers

ХОРИЗОНТАЛНО

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Дополнителни прирачници

За понатамошни информации, ве молиме прегледајте ја нашата серија на прирачници, *Personal Cyber Security (Лична сајбер безбедност)*: три прирачници наменети да им помогнат на обичните Австралијци да ги разберат основите на сајбер безбедноста и како да преземат мерки да се заштитат од чести сајбер закани.

Сите три прирачници можете да ги најдете на **cyber.gov.au**

Одговори на крстозборката

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Забелешки

Одрекување од одговорност

Материјалот во овој водич е од општ карактер и не треба да се смета како правен совет или материјал на кој можете да се потпирате за помош во било кои одредени околности или итни ситуации. За сите важни работи треба да побарате совети од соодветно независно професионално лице за вашите сопствени околности.

Комонвелтот не прифаќа никаква одговорност или обврска за каква било штета, загуба или трошоци кои произлегуваат поради доверба во информациите во овој водич.

За повеќе информации или за да пријавите инцидент во врска со сајбер безбедноста, контактирајте нè на:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Овој број е достапен за користење само во Австралија.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre