2020-1-DE02-KA227-ADU-008321

https://creativecommons.org/licenses/by-sa/4.0/

BY SA

Co-funded by the Erasmus+ Programme of the European Union

Брошура на

....

за користење алатки за ИКТ

Создадена од партнерите на
проектот „ДИГИТАЛИЗИРАЈ - алатки за возрасни
Роми да користат интернет и да го промовираат
образованието“

Партнерски организации:

Amaro Foro e.V.

EGYÜTT HATÓ
KÖZÖSSÉGÉPÍTŐ EGYESÜLET

PARUDIMOS

RROMA

- Моја брошура за користење алатки за ИКТ -

Проект „Дигитализирај - алатки за возрасни Роми да користат интернет и да го промовираат образованието“

Овој документ е создаден во рамките на проектот „Дигитализирај - алатки за возрасни Роми да користат интернет и да го промовираат образованието“ имплементиран од Amaro Foro e.V., Együttható Egyesület, Nevo Parudimos и RROMA. Проектот е поддржан од програмата Еразмус+ на Европската Унија. Број на проект: 2020-1-DE02-KA227-ADU-008321. Поддршката на Европската комисија за производството на оваа публикација не претставува одобрување на содржината, која ги одразува ставовите само на авторите и Комисијата не може да биде одговорна за каква било употреба на информациите содржани во неа.

Автор: YOZKAN, Pelin - Együttható Egyesület

Co-funded by the Erasmus+ Programme of the European Union

Amaro Foro e.V.

EGYÜTT HATÓ KÖZÖSSÉGÉPÍTŐ EGYESÜLET

NEVO PARUDIMOS

RROMA

- Содржина-

ОСТАНЕТЕ БЕЗБЕДНИ НА ДРУШТВЕНИТЕ МЕДИУМИ

ЗАШТИТА НА ПОДАТОЦИ И ДИГИТАЛЕН ОТПЕЧАТОК

ИНТЕРНЕТ-НАСИЛНИШТВО

ГОВОР НА ОМРАЗА ПРЕКУ ИНТЕРНЕТ

КУПУВАЊЕ ПРЕКУ ИНТЕРНЕТ И ЕЛЕКТРОНСКО БАНКАРСТВО

ПРИСТАП ДО УСЛУГИ ПРЕКУ ИНТЕРНЕТ

Еве ги нашите 10 најдобри совети за да останете безбедни на друштвените медиуми:

Совет бр. 1

Користете силна лозинка

Направете ги вашите лозинки единствени!

Користете различна лозинка за секоја Ваша сметка на интернет. Повторната употреба на лозинки е ризична!

Facebook Instagram Tiktok Банкарска сметка

Доколку некој ја добие Вашата лозинка за една сметка, тој би можел да пристапи до Вашата е-пошта, адреса, па дури и до Вашите пари.

Совет
бр. 1

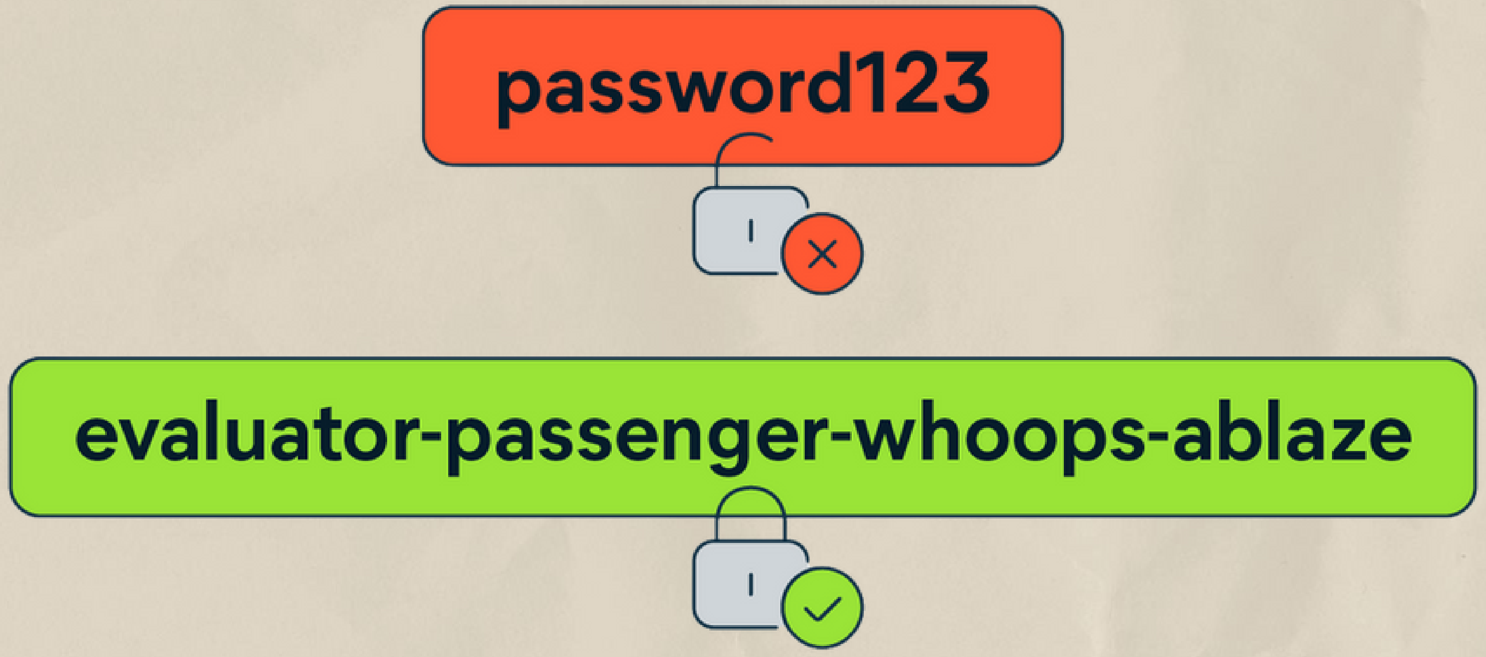
Користете силна лозинка

Направете ја вашата лозинка подолга и полесна за помнење!

Долгите лозинки се посилни, затоа вашата лозинка нека содржи најмалку 12 знаци.

Обидете се да користите:

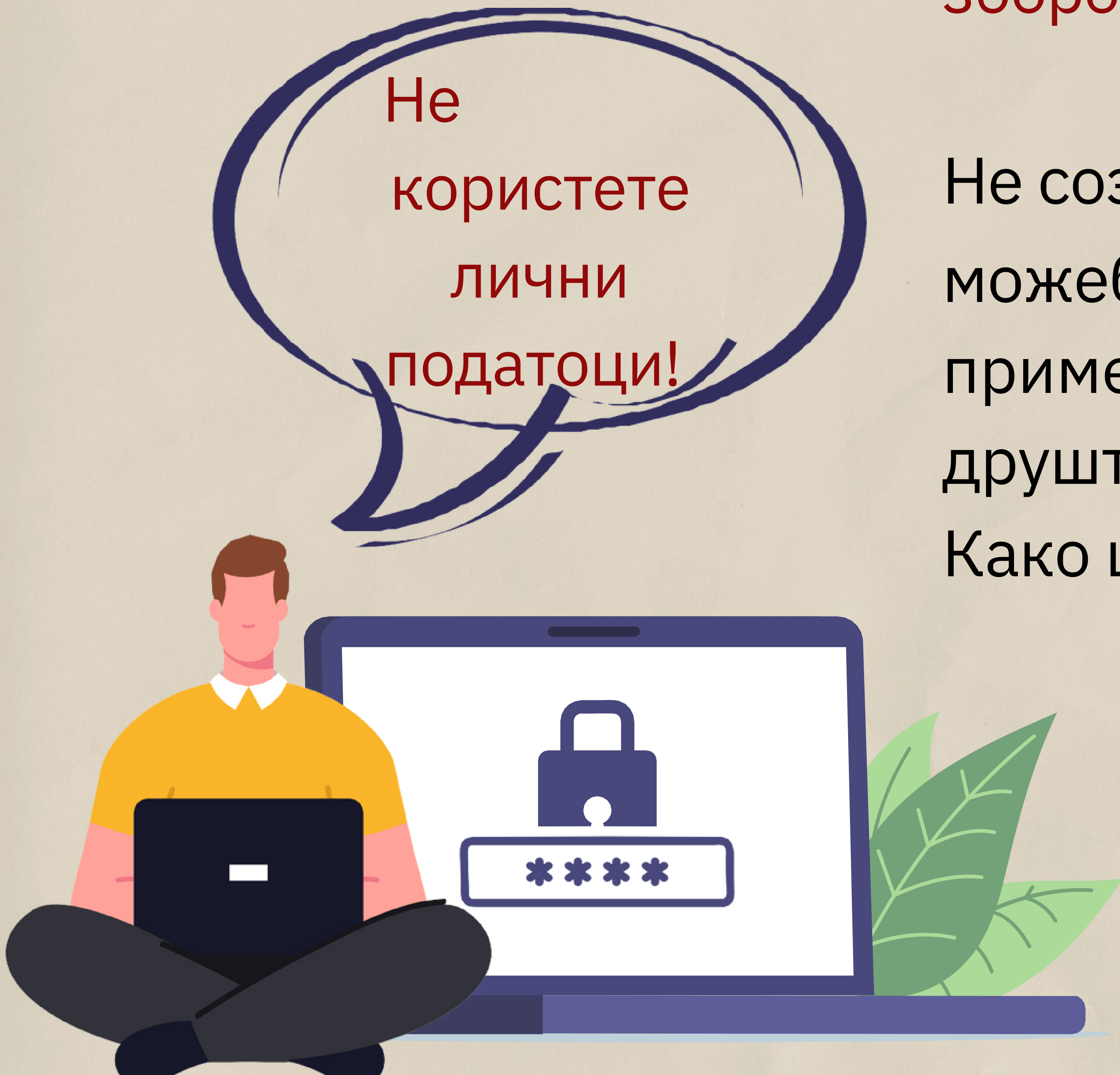
- Стихови од музичка нумера или поема
- Впечатлив цитат од филм или говор
- Низа зборови кои имаат посебно значење за Вас - Кратенка: Направете лозинка користејќи ја
прватa буква од секој збор во реченицата.



Совет бр. 1

Користете силна лозинка

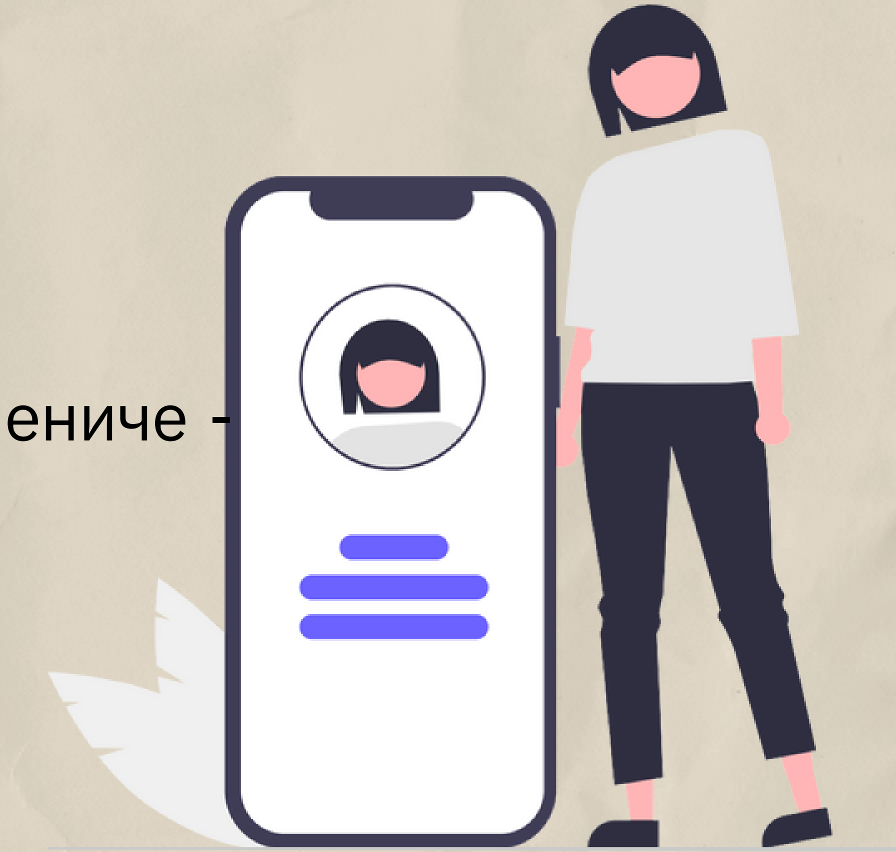
Избегнувајте лични информации и често употребувани зборови!



Не создавајте лозинки од информации што другите можеби ги знаат или би можеле лесно да ги дознаат (на пример, достапните информации на вашиот профил на друштвените мрежи).

Како што се:

- Вашиот прекар или иницијали
- Името на Вашето дете или домашно милениче
- Важни родендени или години
- Името на вашата Улица
- Броевите од Вашата адреса



Совет
бр. 1

Користете силна лозинка

Не користете вообичаени, едноставни зборови, фрази и шаблони кои лесно се погодуваат!

Примери:

- Очигледни зборови и фрази како што се „лозинка“ или „Вашето име“
- Редослед како „abcd“ или „1234“
- Шаблони со низа од букви на тастатурата како „qwerty“ или „qazwsx“

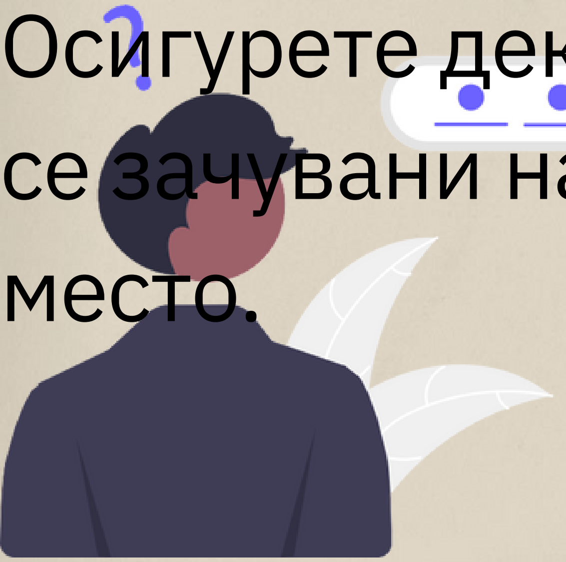
Совет бр. 1

Користете силна лозинка

Чувајте ги лозинките безбедни!

Откако ќе создадете силна лозинка, преземете чекори да ја зачувате безбедна: Чекор I. Сокријте ги напишаните лозинки:

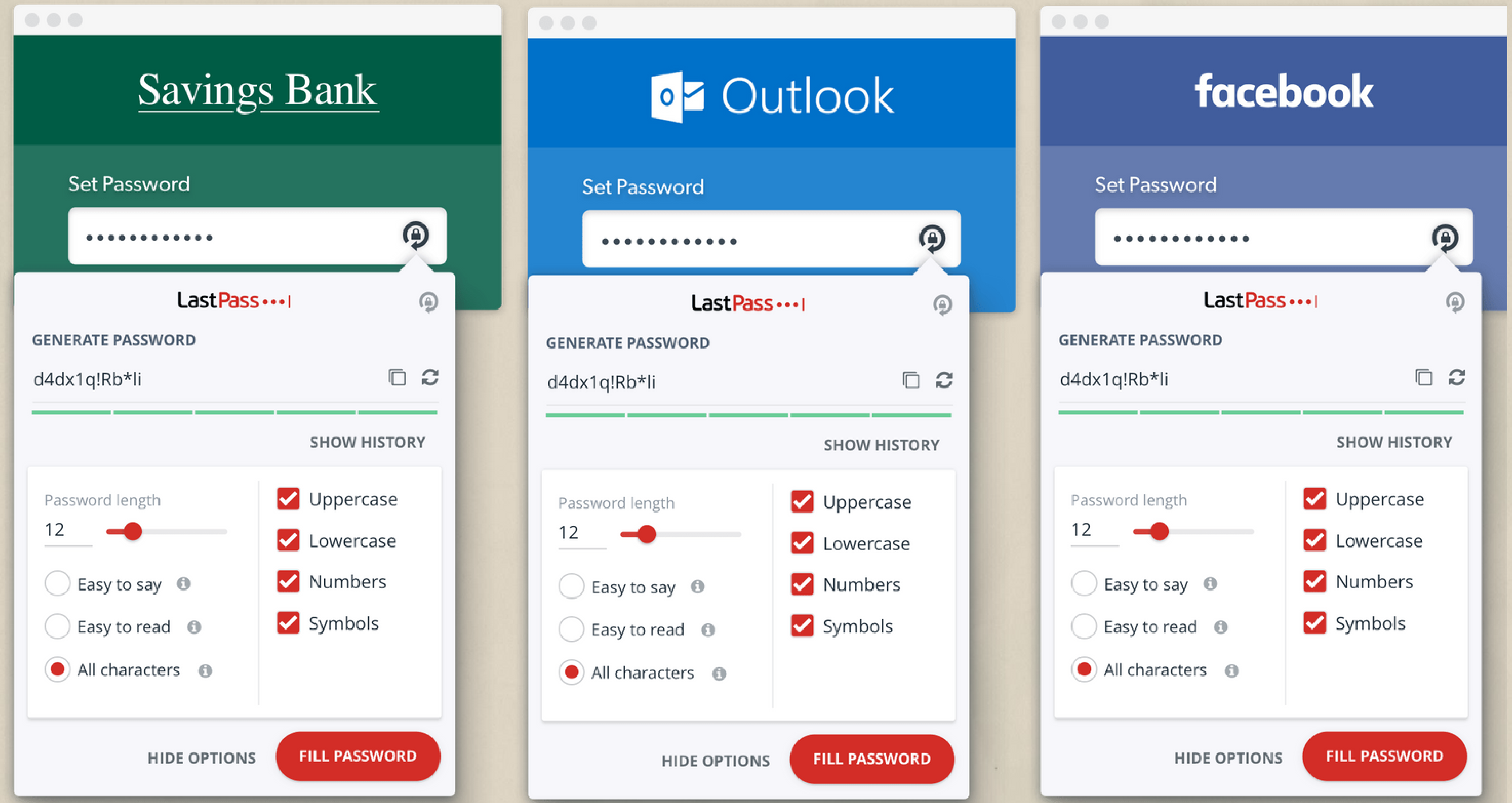
Доколку треба да ја запишете лозинката за да ја запомните, не ја оставајте на компјутерот или на работната маса. Осигурете дека сите напишани лозинки се зачувани на скришно или заклучено место.



Совет бр. 1

Користете силна лозинка

Чекор II. Управувајте со Вашите лозинки преку алатка:



Еден начин за безбедно зачувување и запомнување на лозинките е да користите алатка која ја складира Вашата листа со кориснички имиња и лозинки во шифрирана форма. Некои од овие алатки дури и ќе Ви помогнат со автоматско пополнување на информациите за вас на одредени веб-локации. (На пример: LastPass.)

Совет

бр. 2

Заштитете го Вашиот уред со лозинка

Поставувањето лозинка на Вашиот мобилен уред ќе помогне да ги задржите неовластените корисници подалеку од уредот и може да помогне доколку Вашиот уред некогаш се изгуби или биде украден. Секогаш кога ќе го вклучите или разбудите уредот, ќе биде побарано да ја внесете лозинката пред да можете да го користите уредот. Во делот „Безбедност“ на Вашиот паметен уред се дадени неколку можности за избор на тип на заклучување:

Препознавање на лицето - може да го покажете Вашето лице за да го потврдите Вашиот идентитет. Едноставно препознава еден човек како единствен сопственик на уредот, а истовремено го ограничува пристапот на другите луѓе.

Шара - можете да нацртате шара поврзувајќи ги точките за да го отклучите вашиот уред

Препознавање отпечаток од прст - Ова претставува уште една форма на биометриска безбедност, како што е случајот со препознавање лице.

PIN - можете да внесете шифра од 4 цифри (6 цифри кај некои уреди) за да го отклучите Вашиот уред

Совет

бр. 3

Редовно ажурирајте го Вашиот уред

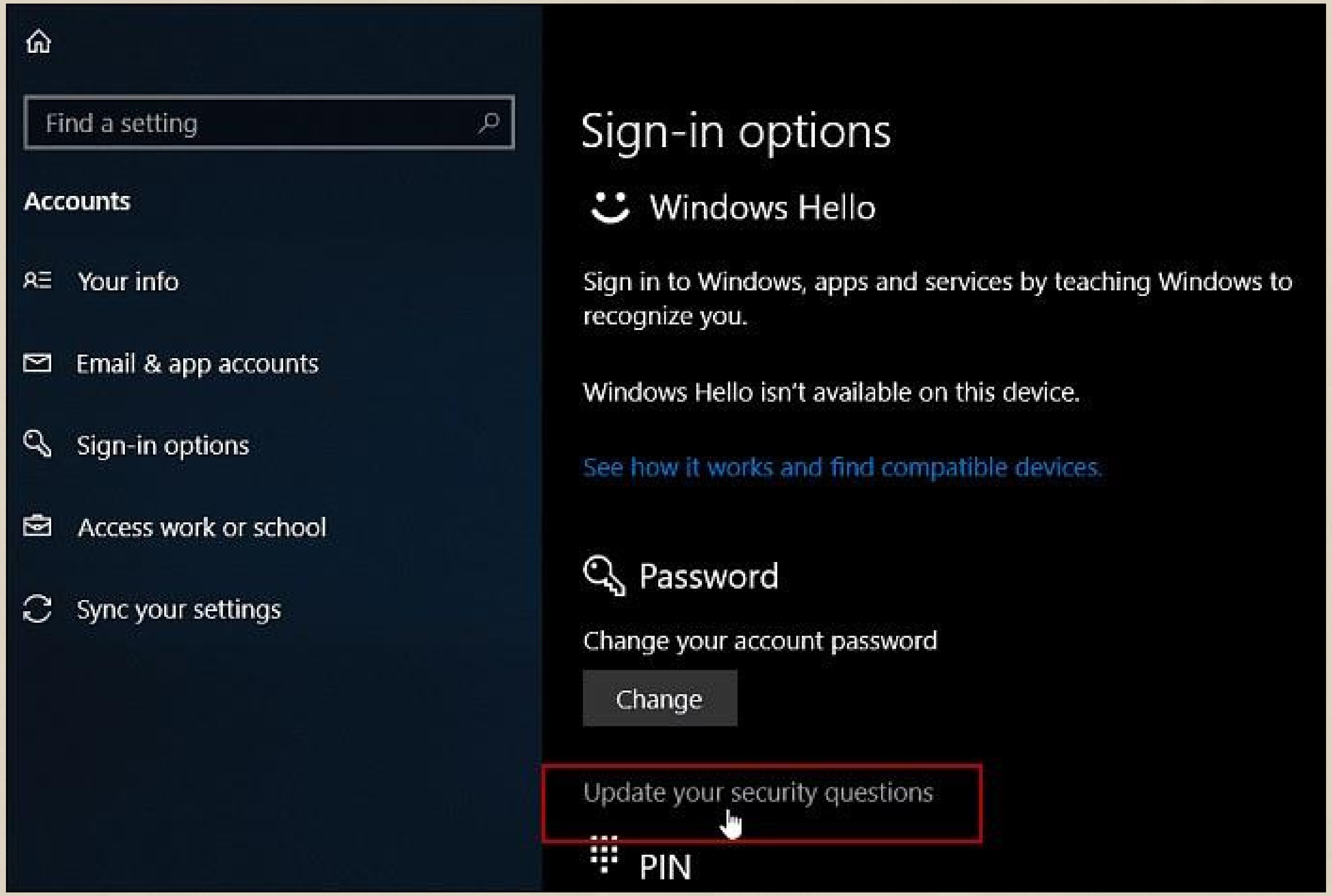
Развивачите на компјутерски софтвер објавуваат ажурирања за да ги одржат производите безбедни. Редовно ажурирајте го софтверот на Вашиот уред за да не биде ранлив на злонамерен софтвер.

Исто така, заштитете го компјутерот со инсталирање антивирусен софтвер за заштита.

Совет

бр. 4

Поставете безбедносни одговори



Безбедносните прашања се направени за да се осигури безбедноста на Вашата корисничка сметка. Исто така, тие се користат и за Ваша идентификација доколку ја заборавите лозинката и не можете да пристапите до Вашата сметка. Оваа опција е достапна на повеќето страници на друштвените медиуми.

Совет
бр. 5

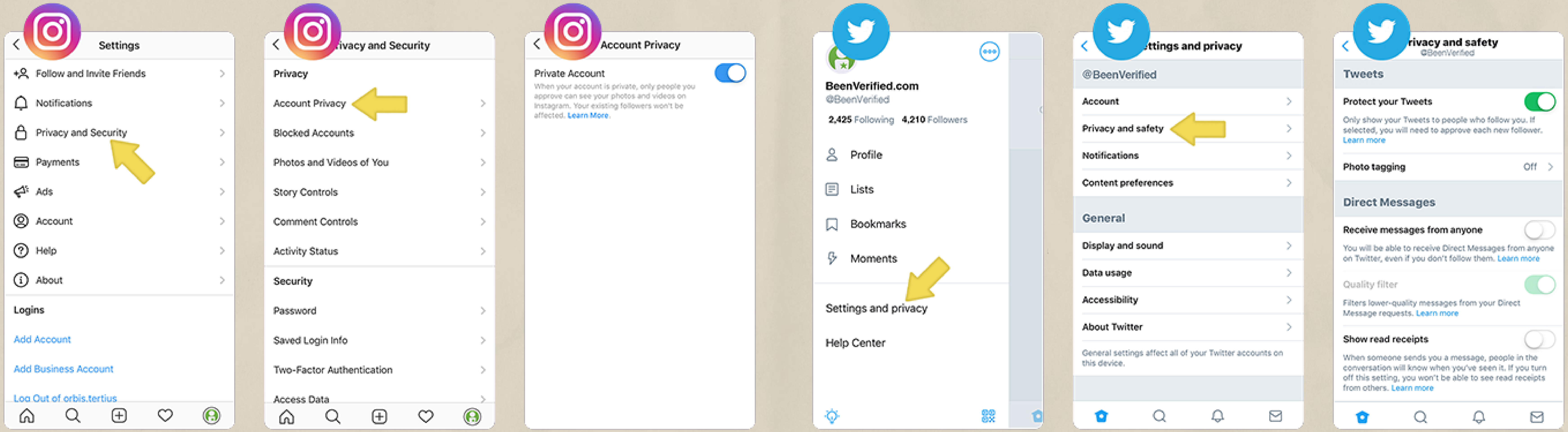
Научете ги поставките за приватност

Запознајте се со политиките за приватност за кој било уред, апликација или услуга што ја користите!

Некои апликации ќе побараат дозвола за пристап до фотографии и други лични информации. Бидете информирани со цел да не споделувате нешто што не сакате.

Совет
бр. 6

Поставете ги Вашите профили како приватни



Сериозно размислете околу тоа кои лица сакате да ги гледаат Вашите објави и споделените лични информации. Размислете да ги поставите Вашите профили на единствено пријатели/следбеници. Кога ќе го поставите вашиот профил како приватен, единствено прифатените следбеници имаат пристап до содржината што ја објавувате.

Совет
бр. 7

Внимавајте што споделувате

Дури и при силни поставки за приватност, важно е да го имате предвид фактот дека она што го објавувате на интернет никогаш не е навистина приватно и може некаде да биде споделено. Токму затоа, важно е секогаш да размислите пред да објавите.

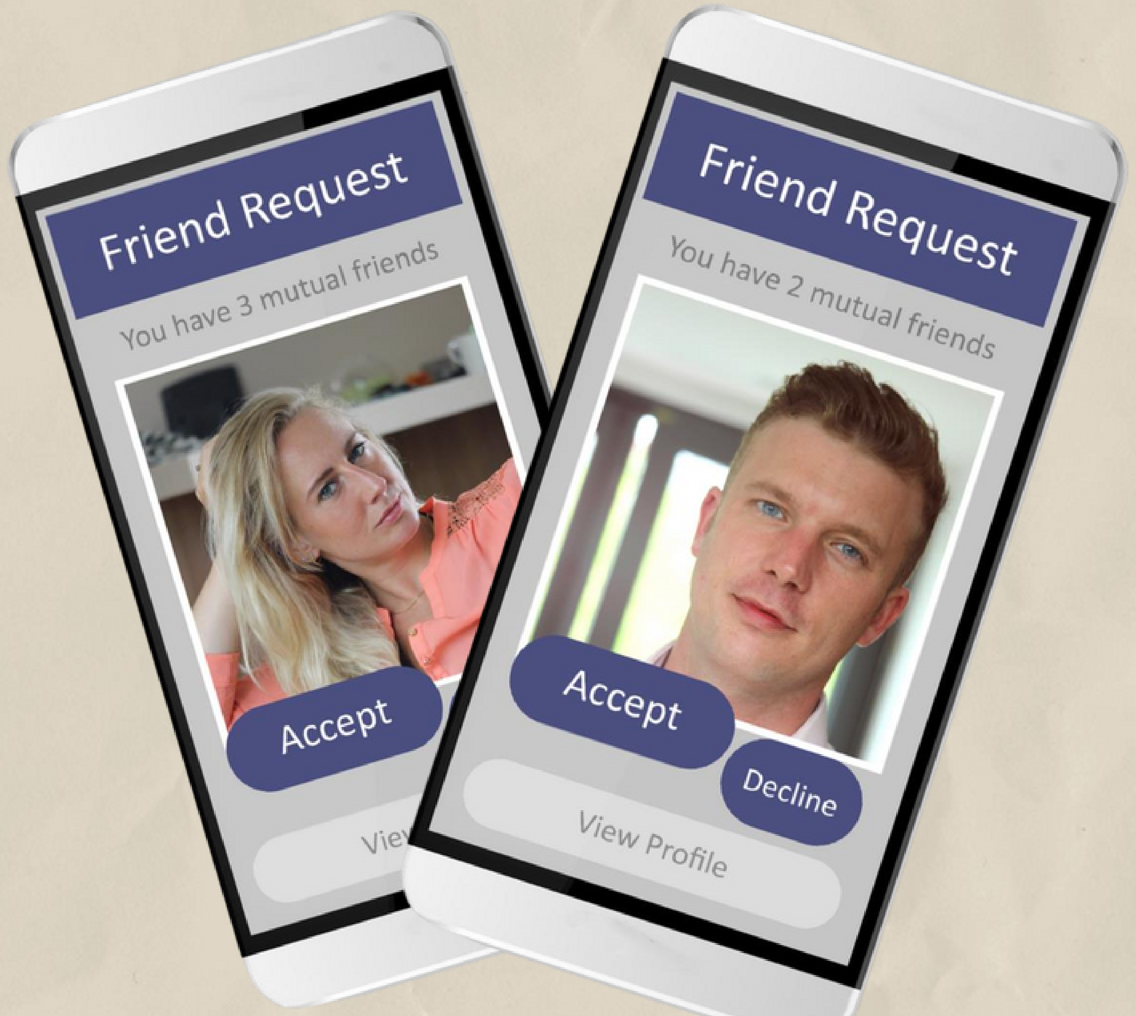
Совет

бр. 8

Бидете селективни во однос на барањата за пријателство

Доколку не ја познавате личноста, не прифаќајте го барањето!

Дури и кога ја познавате личноста, разгледајте го профилот за да бидете сигурни дека тоа не е лажна сметка преку која некое лице се обидува да пристапи до Вашите чувствителни информации. Кибернетичките злосторници на интернет може да се претставуваат како луѓе што ги познавате. Нивната цел е преку измама да изнудат пари од луѓето, да спроведуваат политичка пропаганда или да вршат дејствија поради бројни други злобни причини.



Совет бр. 9

Бидете претпазливи кога кликате на врските

Внимавајте на веб-локациите или е-поштата што содржат сомнителни врски. Некои веб-локации може да користат квизови, бесплатни понуди или лажни приказни за да Ве намамат да кликнете на нив и потоа да ги украдат Вашите лични податоци.

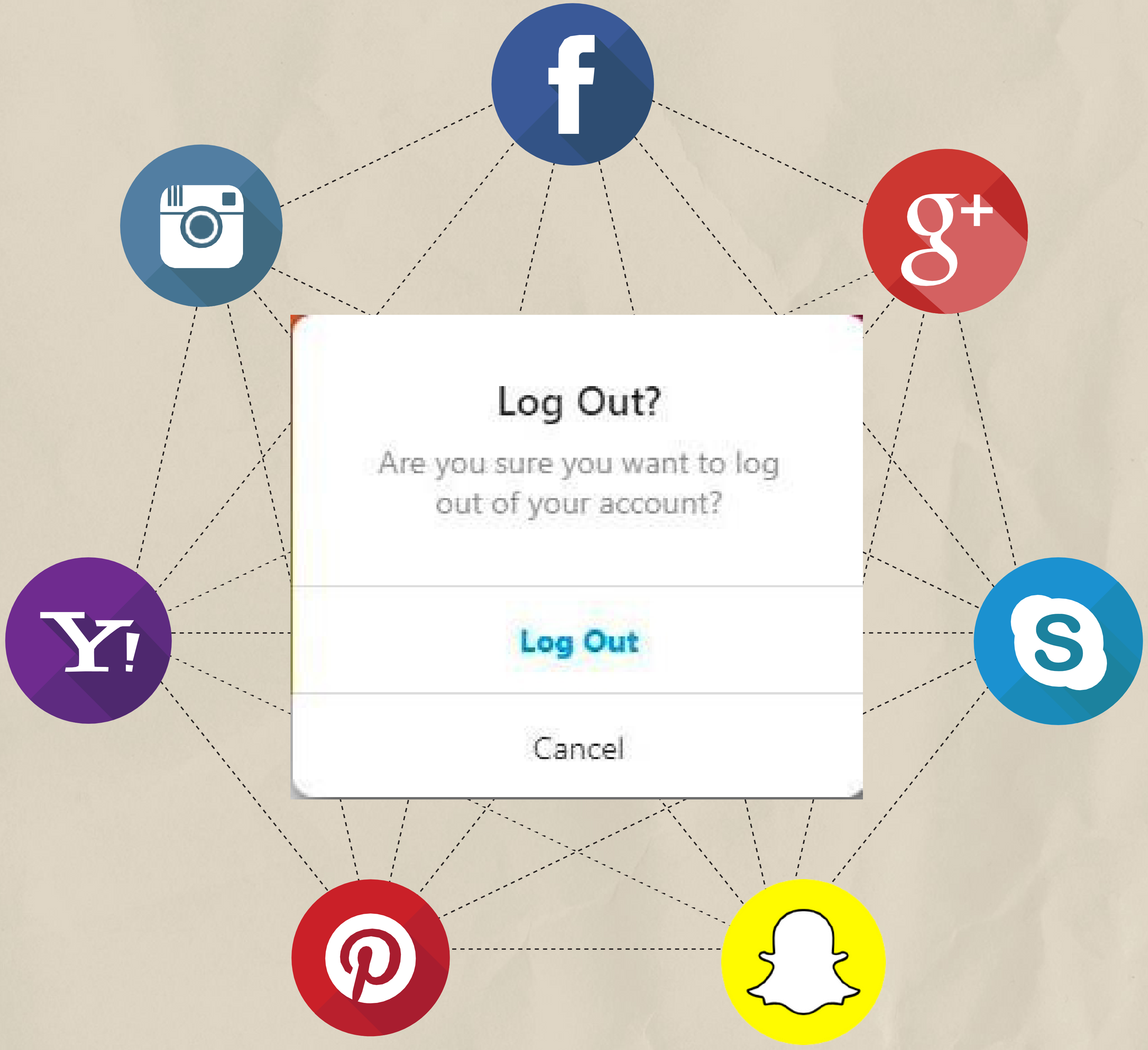
Проверете ја веродостојноста на веб-локацијата!

Можете да направите проверка така што ќе погледнете дали има мала икона за заклучување или „https“ пред URL. Буквата „s“ во „https“ значи „безбедно“, а заклучувањето значи дека е конкретната веб-локација е потврдена како безбедна од страна на Вашиот прегледувач.

Совет
б р. 10

Одјавете се кога ќе завршите

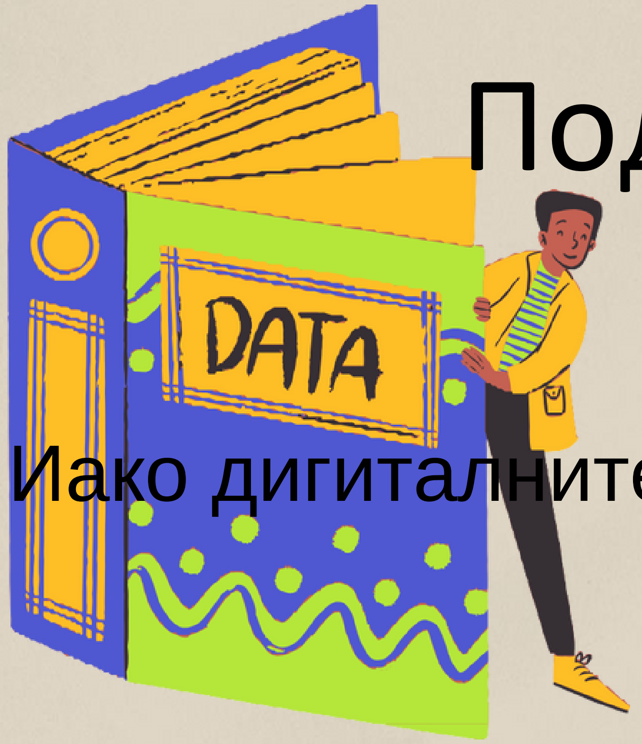
Не дозволувајте прегледувачот да ги запомни Вашите детали за пријавување. Многу побезбедно е повторно да ги внесувате вашите податоци секогаш кога ќе се пријавувате, дури и доколку тоа трае малку подолго.



Заштита на податоци и дигитален отпечаток:

„Што оставате зад себе?“

Што се дигитални податоци?



Податоци: *„Информации што се зачуваат на компјутерски систем“*

Иако дигиталните платформи се промовираат како „бесплатни“ тоа не е така. Компаниите за друштвени медиуми остваруваат профит од пребарувањето на податоци - корисниците плаќаат за услугите со своите податоци и со својата приватност.

Целта на овие компании е да направат секој да споделува што е можно повеќе информации за себе и да собираат што е можно повеќе податоци од секого. Овие податоци потоа ги претвораат во бази на податоци за ефикасни, добро насочени реклами.

Кои податоци се собираат од Вашиот уред додека прегледувате на Интернет?

Термини што се ги пребарувале

Демографски информации (односно, датум на раѓање, пол, итн.)

Име на прегледувачот (односно, Chrome, Firefox, итн.) и други информации како на пример, стандарден јазик

Артикли во Вашите кошнички за пазарење и артикли што ги гледате и купувате

Информации за вашиот компјутерски систем, десктоп компјутер или мобилен уред, моделите на централната процесна единица (CPU) и графичката процесорска единица (GPU), резолуцијата на екранот, итн.

Имињата на Вашите пријатели, колку често посетувате ресторан, итн. - размислете какви информации има Facebook за вас, каде одите и со кого, итн.

Локација

ИП -адреса

Движења со глувчето, кликања со глувчето и други дејства на прегледувачот

Видеа на YouTube што сте ги гледале

Период од денот кога претпочитате да пребарувате на Интернет

Веб-локации што сте ги посетиле

Како да управувате со Вашиот дигитален отпечаток?

Дигитален отпечаток: „Онаштогооставатезадсебе.“

„Дигитален отпечаток“ претставува всушност целото ваше присуство на интернет - сите информации, објави, слики и податоци што ги оставате на интернет, без разлика дали тоа го правите намерно или не. Колку повеќе информации оставате на интернет, толку повеќе луѓето можат да дознаат за Вас. Некои луѓе можат да ги користат тие информации за да утврдат што би можело да Ве интересира да купите или за други злонамерни цели, како што се обидот недозволено да се пристапи до Вашите сметки на интернет и обидот да се пристапи до лозинки, банкарски информации итн.

Како да управувате со Вашиот дигитален отпечаток?

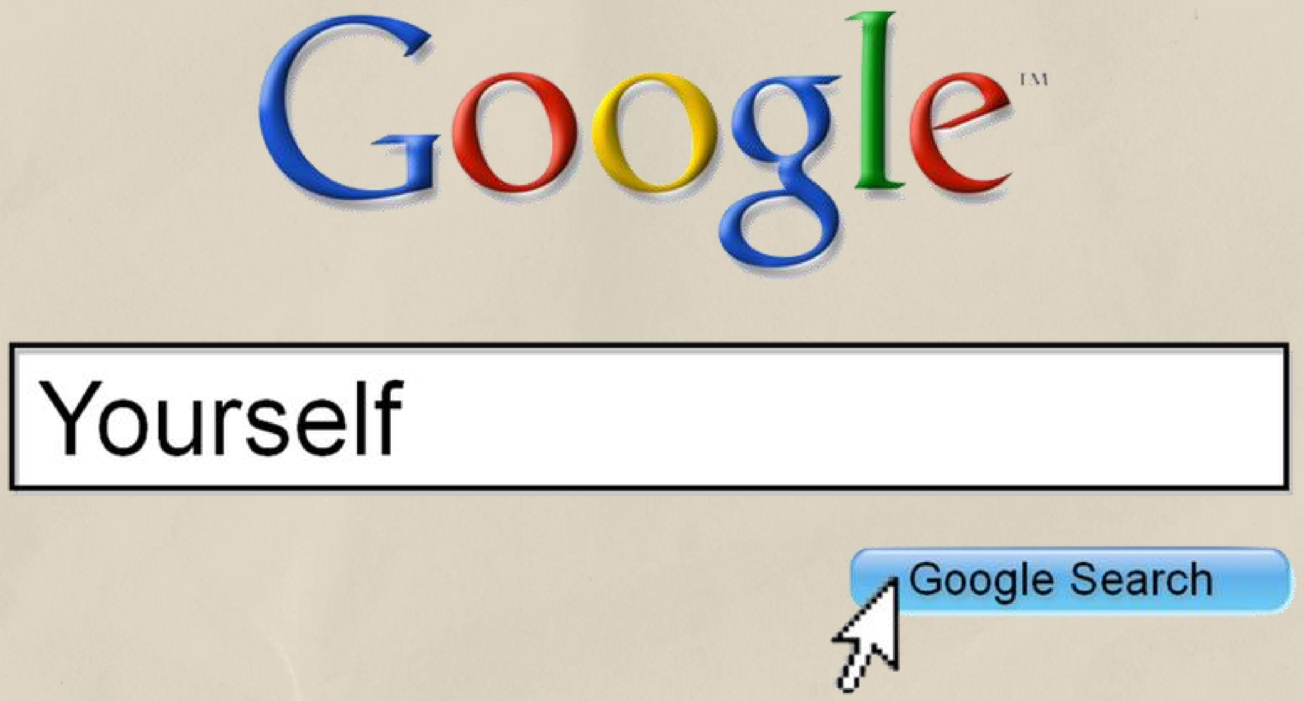
Дигиталните отпечатоци, вклучително мета податоците и содржината, влијаат врз безбедноста, приватноста и довербата. Како што интернетот станува сè повеќе распространет и позастапен, станува уште поважно да се размислува за тоа што може да се случи со сопственоста на фотографиите што ги поседувате и содржината што ја пишувате. Можеби дури и ќе бидете цел на кражба на дигитален идентитет.

Запомнете дека она што се споделува на интернет обично останува таму, па дури и доколку ги избришете објавите, ќе има трага од податоци што сте ги оставиле зад себе.

Еве ги првите 10работи што може да се направат за да се намали и да се управува со Вашиот дигитален отпечаток

Како да управувате со Вашиот дигитален отпечаток?

1. Пребарувајте за себе така што ќе го внесете Вашето име и презиме на интернет за да видите што ќе се појави.

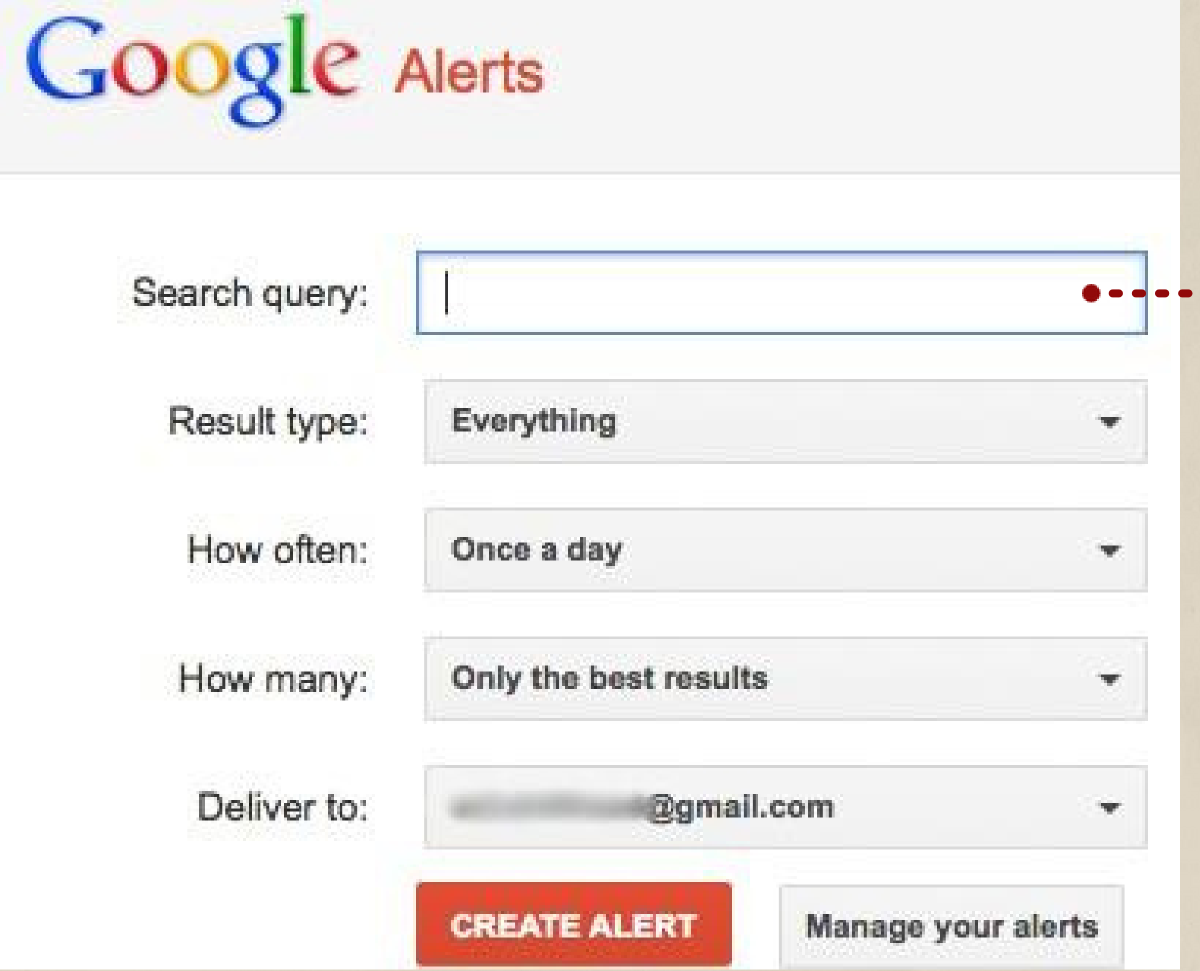


Мора да знаете точно каков е Вашиот дигитален отпечаток за добро да управувате со истиот. Пребарувајте за себе на неколку различни пребарувачи (Google, Yahoo итн.) за да ги видите резултатите што се појавуваат. Направете список на сè што сакате да отстраните или подобрите.

Како да управувате со Вашиот дигитален отпечаток?

2. Поставете Google предупредувања за Вашето лично име!

На овој начин, ќе добиете известување доколку нешто каде сте споменати се појави на интернет.

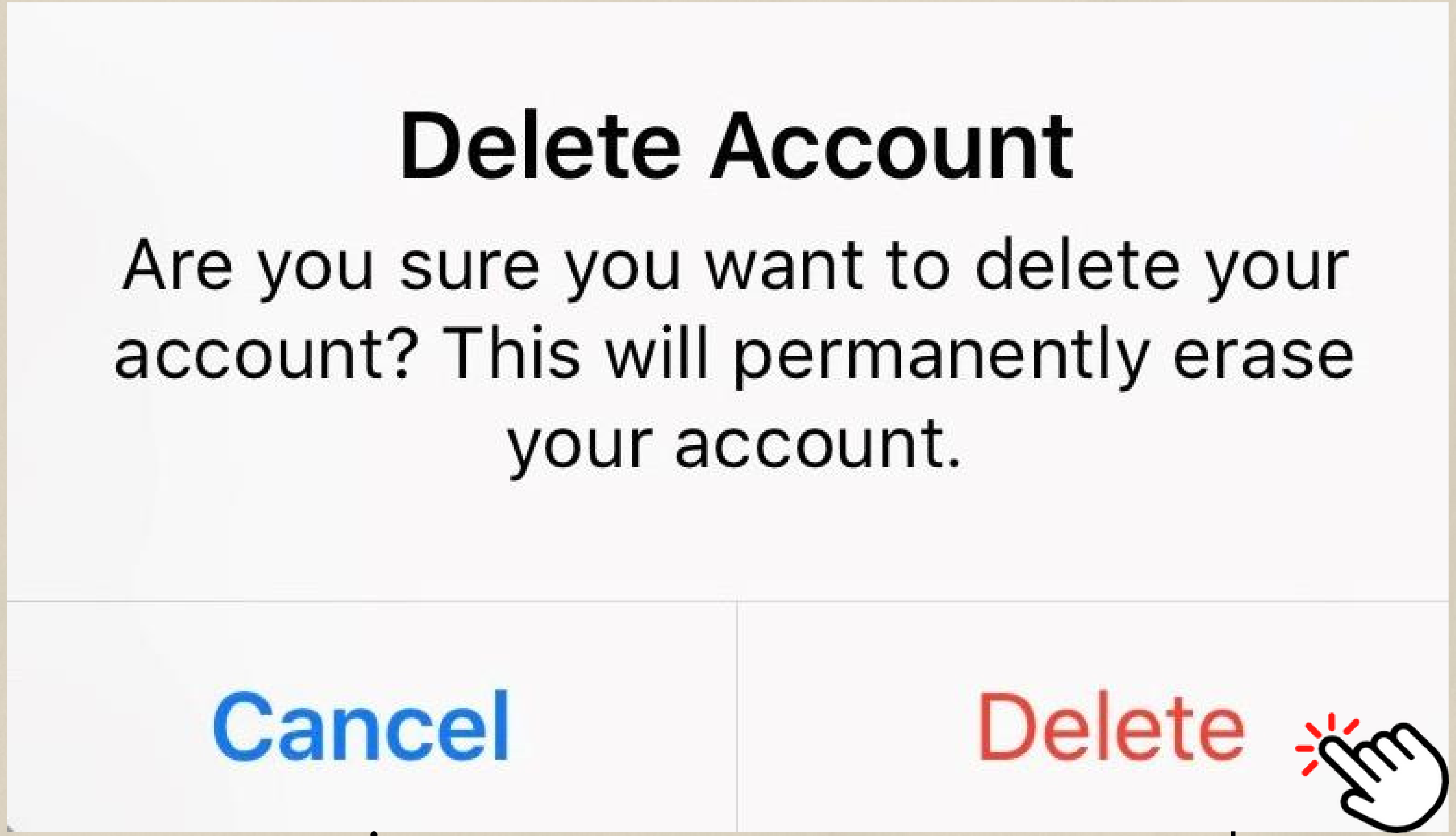


Не можете секогаш да контролирате што се покажува
на интернет. За повеќе помош, контактирајте го
пребарувачот каде
се појавуваат резултатите и замолете да ги
Внесете избришат спорните објави. На пример, Google
го дозволува да пријавите лични или приватни
Вашето информации што се појавуваат на нивниот
име пребарувач преку посета на страницата Google
тука! Support.

Како да управувате со Вашиот дигитален отпечаток?

3. Избришете ги профилите или сметките што повеќе не ги користите и поставете ги опциите на Вашата сметка како приватни.

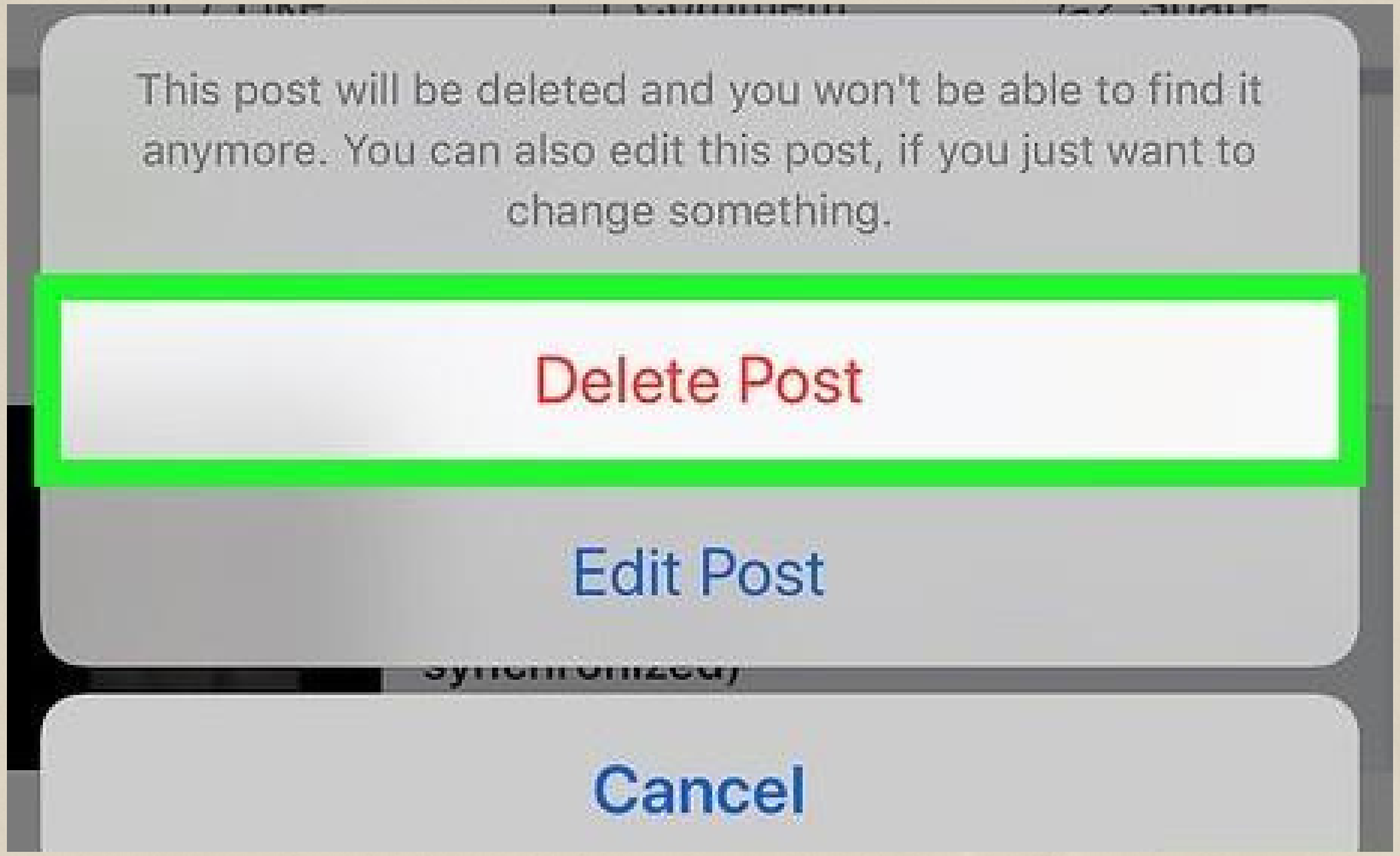
Нема потреба да чувате сметки што не ги користите. Со чување на сите овие сметки само се зголемува количеството на информации за Вас на интернет. Ова го нарушува Вашето присуство на интернет, затоа затворете или избришете ги сите сметки што повеќе не ги користите.



Дополнително, прилагодете ги поставките на приватни кај сите преостанати платформи за да контролирате и ограничите кој може да ги гледа Вашите објави.

Како да управувате со Вашиот дигитален отпечаток?

4. Избришете сè што сметате дека Ви го нарушува угледот.



Можеби ќе најдете некои непримерни објави кога ќе пребарувате за себеси. Тоа значи дека кое било лице, потенцијално, може да ги види објавите, што може да предизвика штета во личниот и професионалниот живот. Општо земено, сомнителната содржина вклучува вулгарности, експлицитни фотографии, пиење алкохол или груби коментари. Избришете ги доколку се појават и воздржете се од објавување на такви содржини во иднина.

Како да управувате со Вашиот дигитален отпечаток?

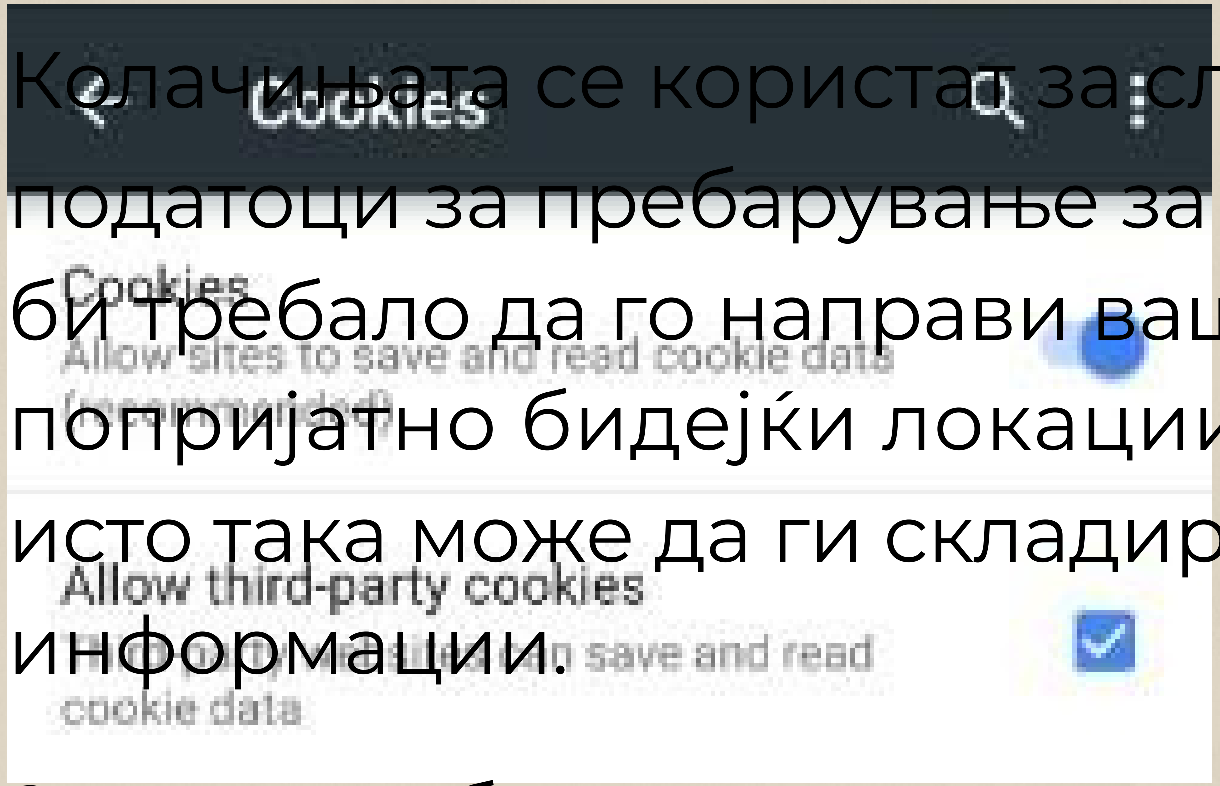
5. Размислете пред да објавите.

Размислете за сите последици од објавите што сте ги направиле и споделете единствено работи што Ве покажуваат во позитивно, професионално светло. Обидете се да избегнете да објавувате нешто доколку се чувствувате возбудено или луто. Можеби не размислувате за поголемите последици од она што го кажувате.

Запомнете дека користењето на поставките за приватност не е замена за да бидете внимателни во врска со тоа што објавувате. Избегнувајте да споделувате несоодветни објави, дури и доколку вашите сметки се заклучени.

Како да управувате со Вашиот дигитален отпечаток?

6. Бришете ги колачињата на секои неколку месеци за да ги избришете податоците за следење.



Колачињата се користат за следење на Вашите податоци за пребарување за одредени локации. Ова би требало да го направи вашето веб-искуство попријатно бидејќи локациите ќе Ве запаметат, но исто така може да ги складираат Вашите лични информации.

За да го избегнете ова, создадете навика да ги бришете колачињата на вашиот веб-прегледувач на секои неколку месеци за да отстраните сè што би можело да ја следи Вашата активност.

Како да управувате со Вашиот дигитален отпечаток?

7. Внимавајте на сомнителни пораки и е-пошта за кражба на идентитетот.

На пораките со скратена URL-адреса кои содржат изјави како „О; Боже погледнете ја оваа слика од Вас...“ или „Дали сте разбрале што зборуваат за Вас...“ не треба да им се верува. Не кликајте на врските што се наоѓаат во таквите текстови.

Проблем се и е-поштите за кражба на идентитетот. Станува збор за измамнички комуникации при што испраќачите лажно се претставуваат како доверлива организација како што е Facebook, и ќе се обидат да Ве натера да се пријавите и да ви ги украде податоците.

Како да управувате со Вашиот дигитален отпечаток?

8. Препознајте ги измамниците.

Не секој на друштвените мрежи ќе биде оној којшто се претставува дека е. Може да има луѓе кои се преправаат дека се некој друг и би можеле да Ви нанесат штета. На пример, тие можеби ќе сакаат да Ве измамат да споделите приватни или лични информации што би можеле да ги искористат против Вас. Откако ќе го прифатите пријателството преку интернет, тоа не мора да биде трајно. Редовно прегледувајте ги Вашите контакти и отстранете ги сомнителните контакти.

Како да управувате со Вашиот дигитален отпечаток?

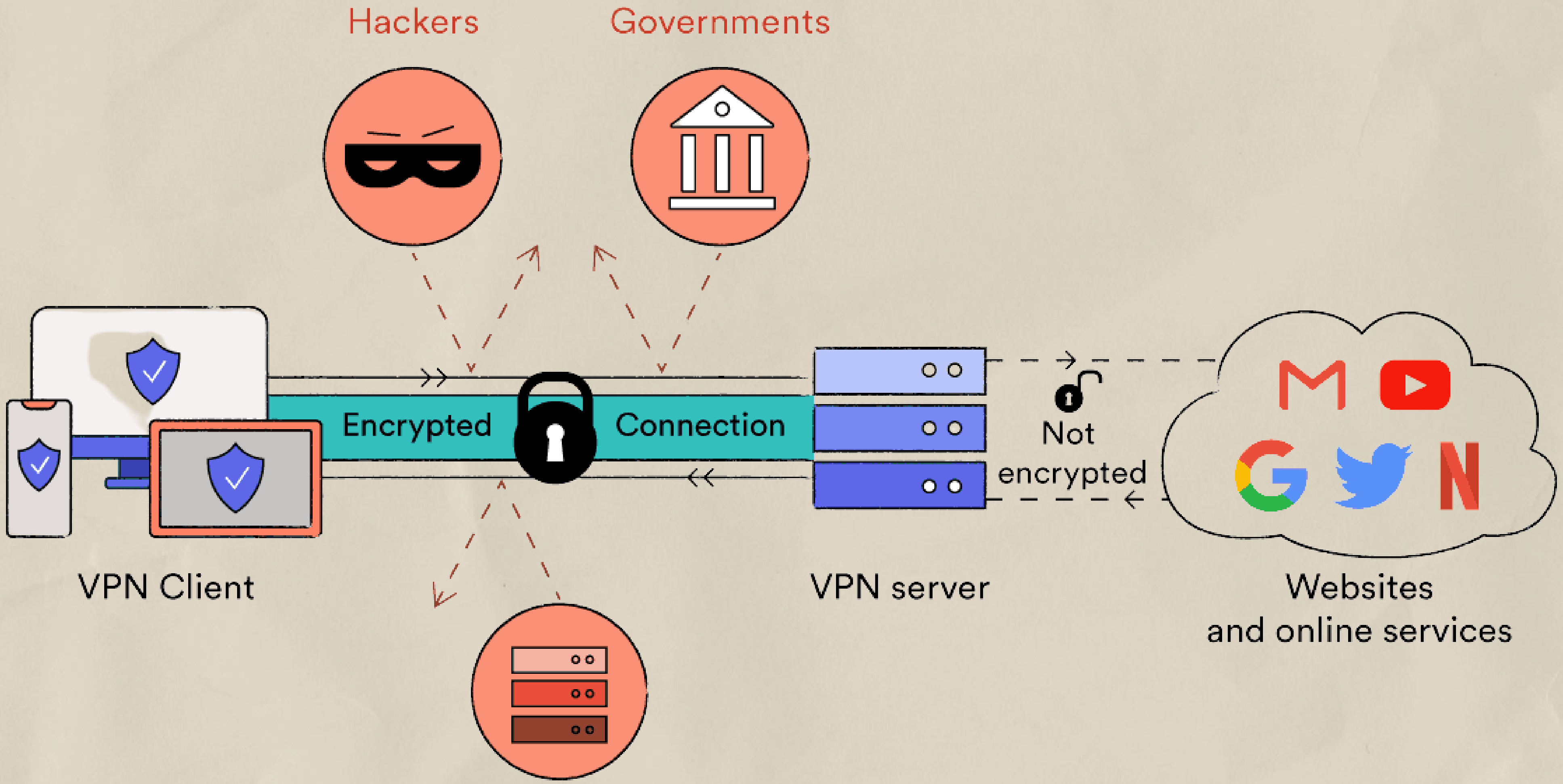
9. Редовно ажурирајте го Вашиот софтвер.

Застарениот софтвер може да им овозможи на хакерите задна врата за пристап до Вашите приватни информации. Редовното ажурирање на антивирусната програма и другите програми значи дека добивате безбедносни поправки кои ќе помогнат да се поправат или отстранат грешките во Вашиот систем. Може да поставите програмите и апликациите да се ажурираат автоматски за да бидете сигурни дека го имате инсталирано најновиот софтвер.

Како да управувате со Вашиот дигитален отпечаток?

10Користете алатки за виртуелна приватна мрежа.

ЗадајазаштититеВашатаприватностможете да користите алатки против следењеприватнипребарувачиилианонимнипрегледувачи. Виртуелни приватни мрежимаскирајтејавашатаИПадресаза (VPN) да, можете да ги задржите како приватнивашаталокацијаисторијатанапрегледување и другите информации.



New Tab

Интернет-насилништво и говор на омраза преку интернет

Што значи интернет-насилништво?

Како да се заштитите?

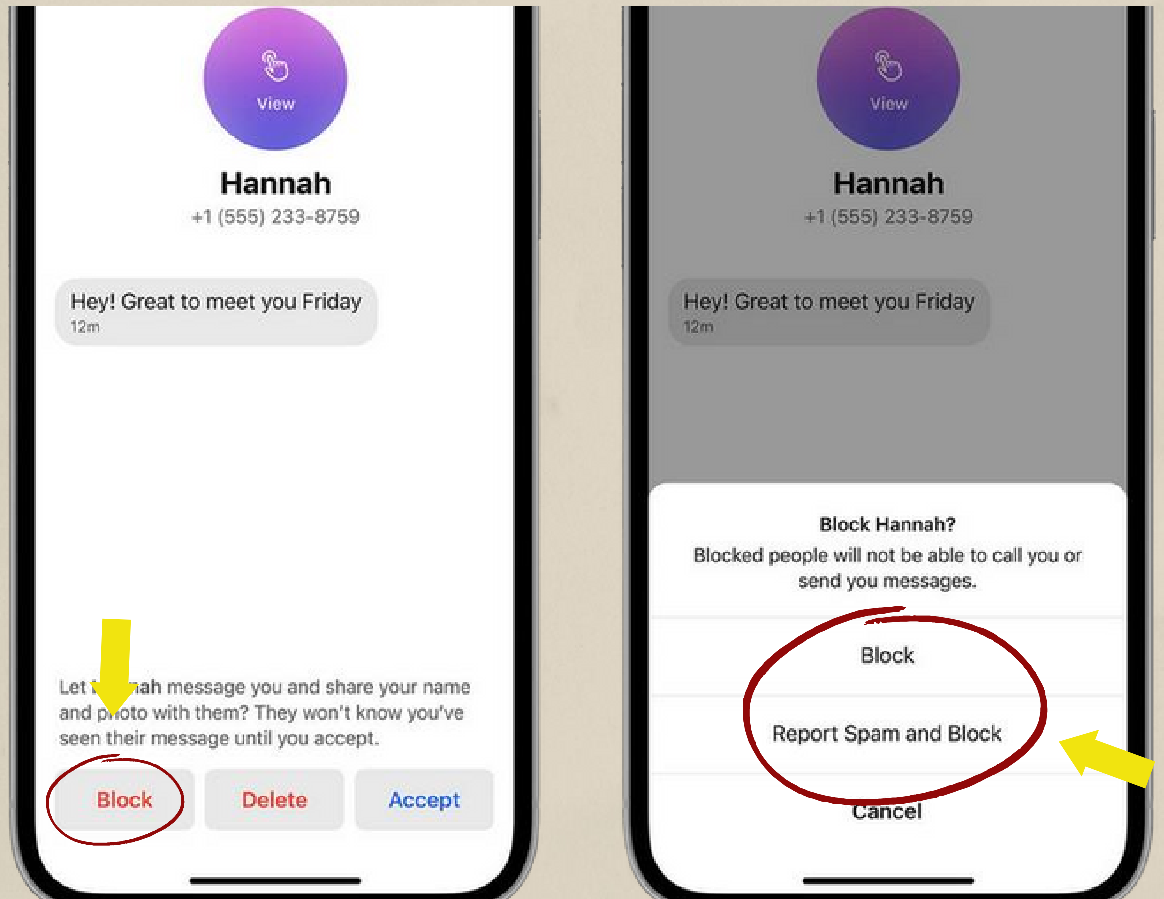
Како да ги заштитите другите?

Што значи интернет-насилништво?

Постојат многу друштвени платформи каде што луѓето создаваат и споделуваат различни содржини. Една од најголемите опасности од овие активности е што корисниците често се однесуваат непромислено поради потребата за поврзување, внимание и препознавање. Она што инаку не би го направиле во реалниот живот се прави многу полесно на интернет, со помала непријатност. Таа злоупотреба на информатичките технологии со намера да им наштети на другите се нарекува интернет-насилништво.

Како да се спречи интернет-насилништвото?

Виртуелните корисници ги злоупотребуваат друштвените платформи за да ги вознемируваат своите таканаречени „пријатели“. Понекогаш овие луѓе користат лажни идентитети и сметки или прибегнуваат кон користење алатки за анонимизирање за да го сокријат својот идентитет со цел да ги малтретираат другите зад виртуелните маски.



Постојат 7 едноставни чекори за да се спречи интернет-насилништвото:

Зголемете ја Вашата приватност. Не споделувајте премногу.
Не одговарајте на пораките. Зборувајте со некого.
Блокирајте го лицето или луѓето. Зачувајте ги доказите.
Пријавете го случајот на платформите/властите.

Бидете свесни за влијанието на Вашите објави врз другите

Понекогаш луѓето мислат дека тоа што го прават е безопасно или само обична шега кога објавуваат видео запис или слика што може некого да засрами или пак кога споделуваат совети за алтернативна медицина од недоверливи ресурси итн.

Но, вистината е дека дигиталниот свет е вистински свет со реални последици. Откако ќе објавите нешто, ја губите контролата врз друштвените, трауматските и психолошките ефекти врз поединецот настанати како резултат на Вашите споделувања.

Не ги злоупотребувајте друштвените мрежи за да ги засрамувате и да вршите насилство врз другите луѓе!

Секогаш поставете си ги следните прашања пред да притиснете на „испрати“!

Размислете за овие 10 прашања пред да објавите нешто.

1. Дали подоцна ќе се чувствувам добро или поинаку во врска со тоа ?
2. Зошто го објавувам ова?
3. Дали би го кажал ова директно?
4. Може ли ова да биде сфатено поинаку?
5. Дали сум љубезен?
6. Дали [illegible] си се допаднал себеси?
7. Дали е ова навистина приватно?
8. Имам ли дозвола?
9. Дали е законски?
10. Дали е ова точно?

Електронско банкарство и купување преку интернет

Што е електронско банкарство?

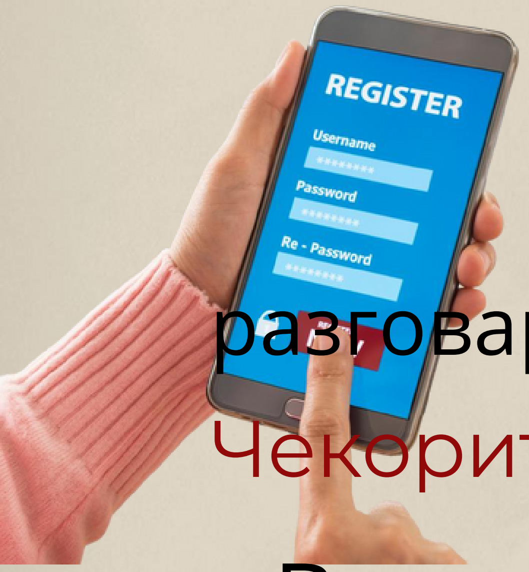
Електронското и мобилното банкарство претставуваат безбеден начин да управувате со Вашите финансии од удобноста на домот или кога сте надвор од домот.

За што можам да користам електронско банкарство?

- *Проверка на состојбата на Вашата трансакциска сметка.*
- *Плаќање сметки*
- *Проверка на Вашите изводи од сметката.*
- *Да префрлите парични средства на друго лице.*
- *Да префрлате парични средства помеѓу Вашите банкарски сметки*
- *Да поставите или откажете автоматско повлекување парични средства од сметката и трајни налози.*

Како да поставам електронско банкарство?

Сè додека имате уред со пристап до Интернет и банкарска сметка одобрена за електронско банкарство, лесно е да започнете:



За да пристапите до електронско банкарство, прво ќе треба да се регистрирате преку веб-локацијата на Вашата банка. Секоја банка има различен процес за поставување електронско банкарство и треба да разговарате со лице вработено во Вашата банка.

Чекорите може да го вклучуваат следното:

• Внесување лични податоци и податоци за Вашата банкарска сметка (број на банката и број на трансакциска сметка).

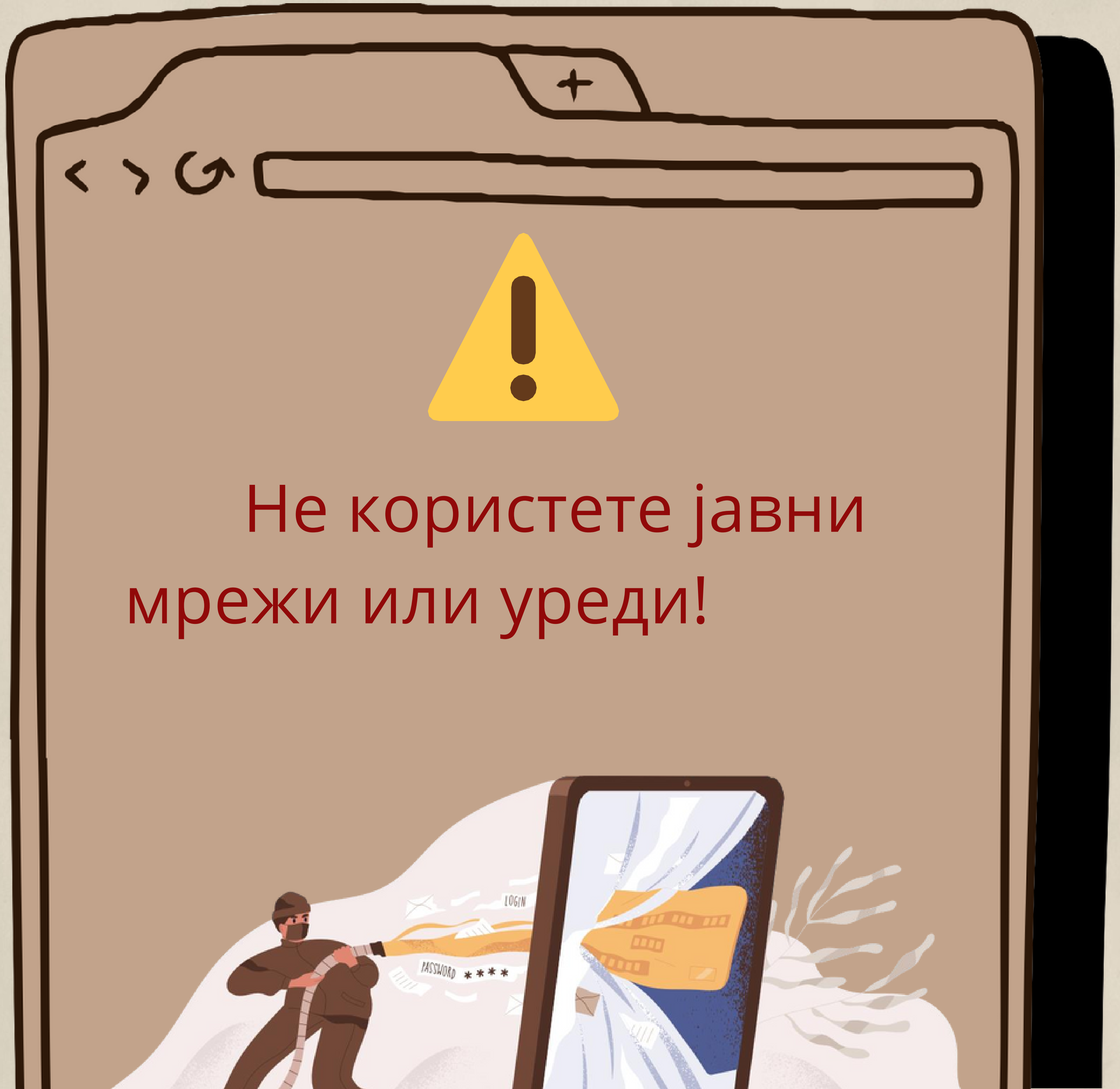
• Може да Ве контактира лице од банката и да Ви постави неколку прашања за да го потврди Вашиот идентитет и да испрати код за активација или текстуална порака.

• Поставување корисничко име и безбедна лозинка или код за лозинка.

Што можам да направам за да ги одржам моите парични средства и мојот идентитет безбедни?

1. Користете единствено безбедни Wi-Fi мрежи и уреди за пристап до Вашето електронско банкарство.

Доколку користите јавни мрежи, како што се тие во кафулињата или железничките станици, можеби е возможно луѓето на истата мрежа да пристапат до Вашите податоци. Исто така, бидете внимателни кога користите јавен компјутер за пристап до Вашето електронско банкарство. Можеби немаат соодветно ниво на безбедносен софтвер.



Што можам да направам за да ги одржам моите парични средства и мојот идентитет безбедни?

2. Користете различни детали за пријавување и лозинки за електронски банкарски сметки.

Не користете ниту еден од деталите за пријава на електронско банкарство за други портали или услуги на интернет. Погрижете се да создадете силна лозинка и редовно да ја менувате.

3. Не ги давајте никому деталите за пријавување поврзани со Вашето електронско банкарство.

Чувајте ги кај себе, исто како и сите ПИН-кодови и други чувствителни информации за автентикација.

Што можам да направам за да ги одржам моите парични средства и мојот идентитет безбедна?

4. Внимавајте кому префрлате парични средства.

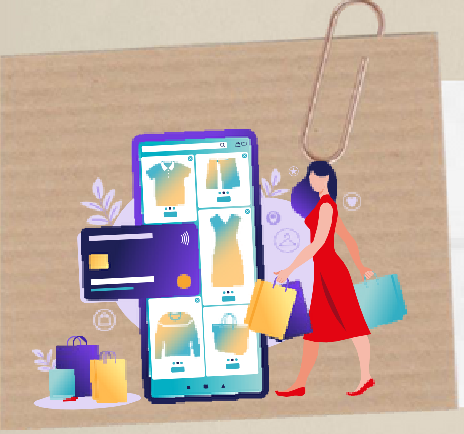
Префрлајте парични средства на субјекти на кои им верувате. Префрлените парични средства вообичаено не може да Ви бидат вратени без експлицитна дозвола од страната што ги примила.

Што можам да направам за да ги одржам моите парични средства и мојот идентитет безбедни?

5. Користете софтвер за заштита од кражба на идентитет или VPN.

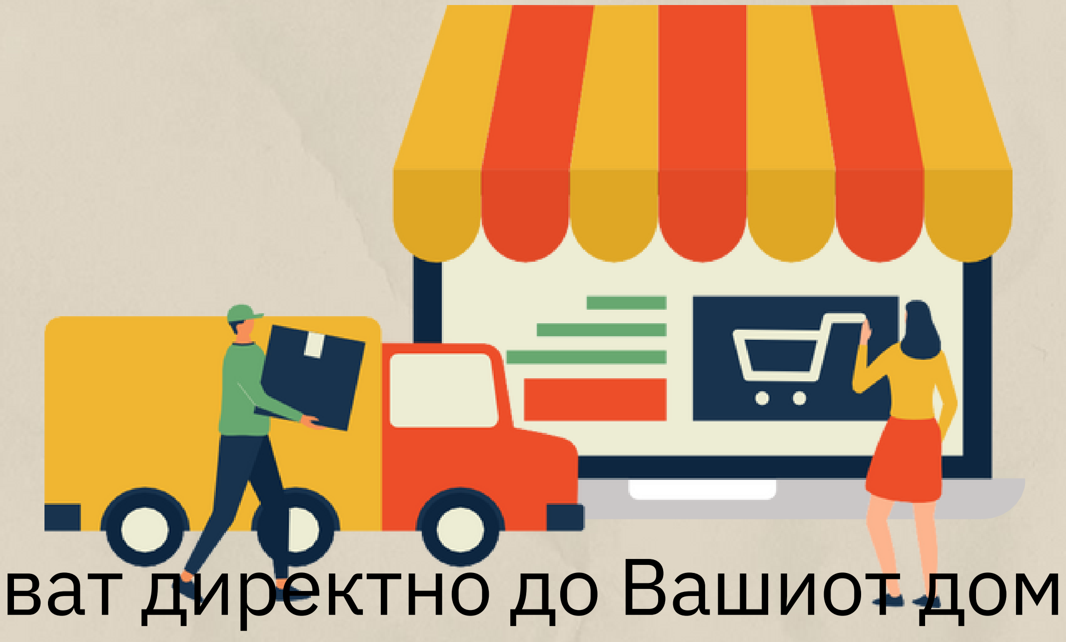
Размислетезапреземањесофтверзазаштитаодкражбанаидентитет. Тоа е услугакојагошифрираВашетоинтернетповрзувањезада го одржува безбедноОвиеуслугичестоможедаопфататнеколкузаштитни мерки спакуванивоеднавклучувајќи инадзорналозинка

- : , VPN .

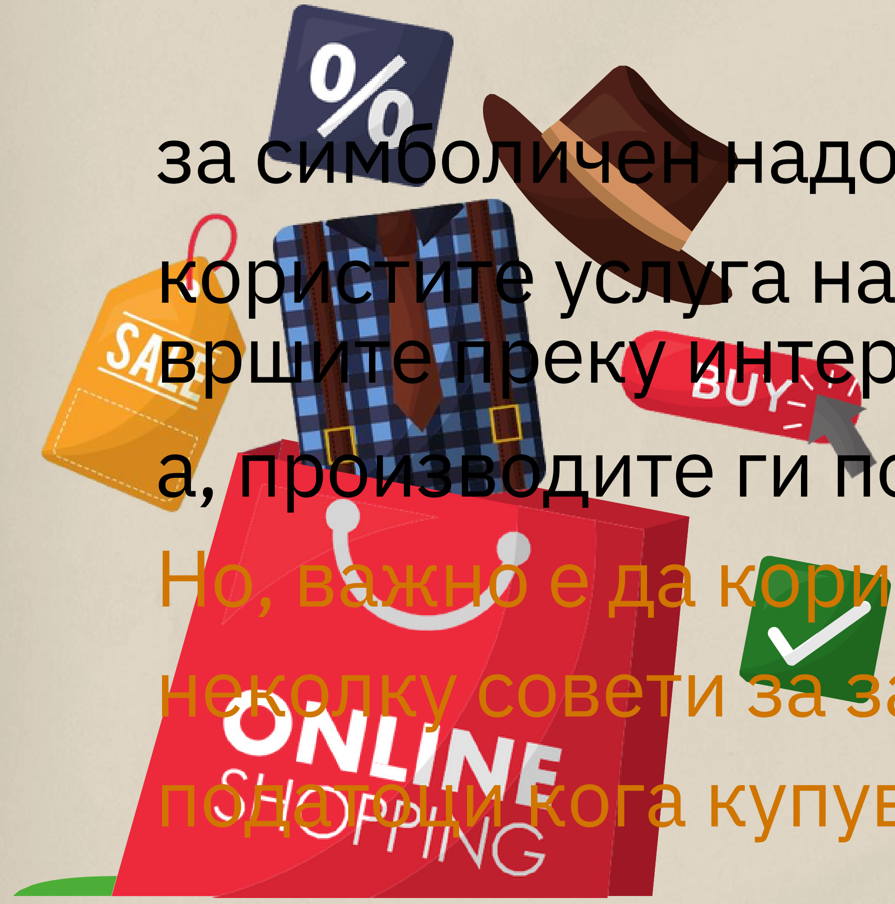


Безбедно купување преку интернет

Купувањето преку интернет може многу да го олесни животот и да ја отстрани обврската за одење во супермаркет или трговски центар. Можете да купувате преку интернет од повеќето супермаркети, продавници на познати брендови, како и помали самостојни продавници.



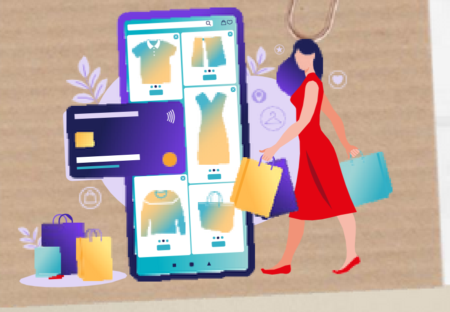
Вообичаено, производите може да се достават директно до Вашиот дом



за симболичен надоместок или бесплатно, или можете, исто така, да користите услуга наречена „кликни и подигни“ при што нарачката ја вршите преку интернет

а, производите ги подигнувате во продавницата.

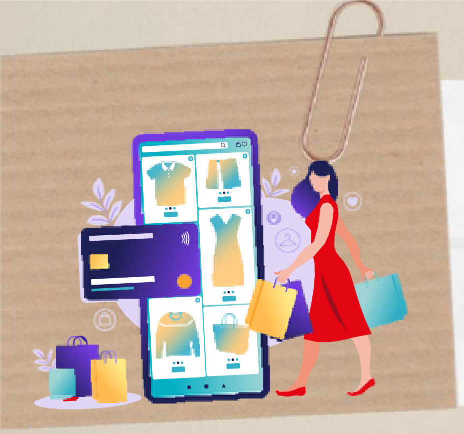
Но, важно е да користите безбедни и оригинални веб-локации. Еве неколку совети за заштита на Вашите парични средства и лични податоци кога купувате преку интернет.



Безбедно купување преку интернет

Совет бр. 1: Внимателно изберете ја веб-локацијата од каде ќе купувате и купувајте од реномирани трговци на мало.

Купувајте кај трговци на мало на мало со добра репутација, на пример, добро познати супермаркети, продавници на познати брендови или продавници со развиена трговија преку интернет. Побарајте ги целосните детали за контакт на компанијата. Реномираните компании секогаш ги прикажуваат овие информации на својата веб-локација. Пребарајте го името на компанијата на интернет за да видите дали некој имал проблеми со конкретниот трговец на мало.



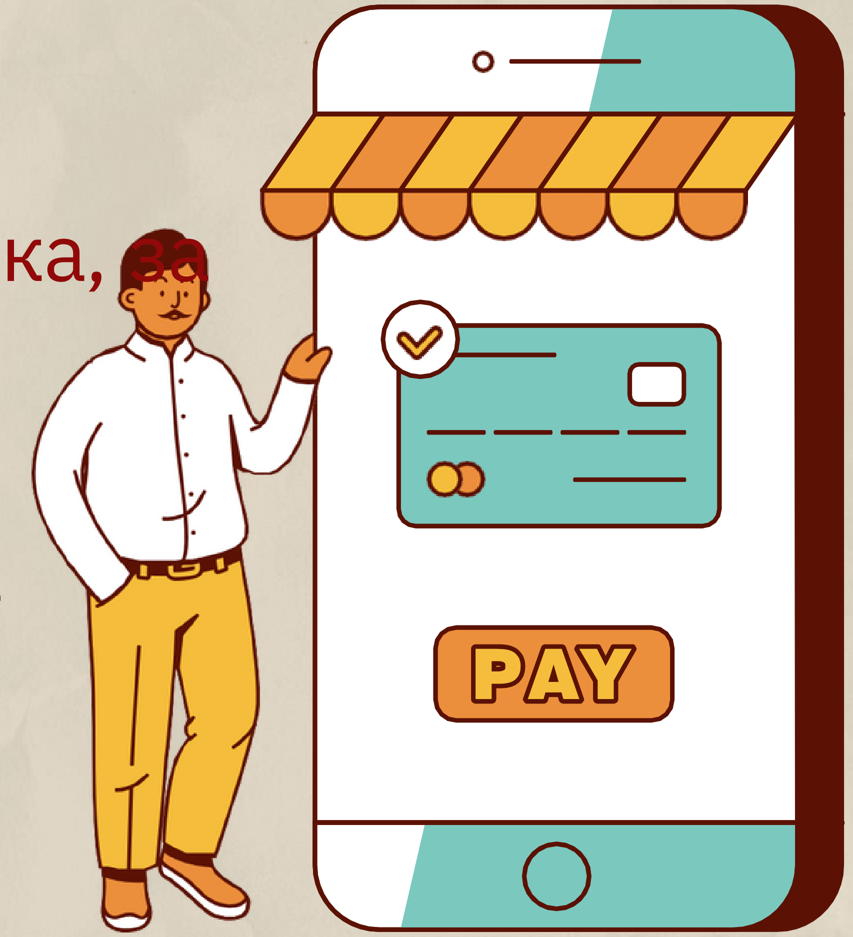
Безбедно купување преку интернет

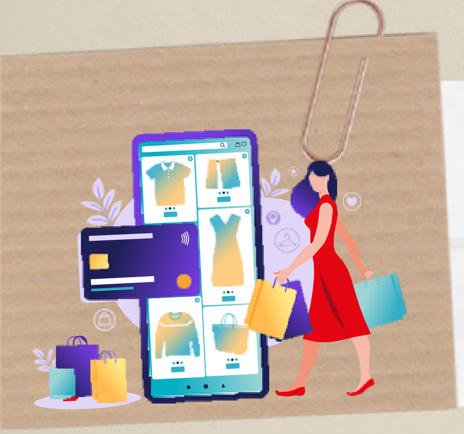
Совет бр. 2: Истата картичка користете ја единствено за интернет трансакции.

Редовно проверувајте го изводот од банката за оваа картичка за какви било невообичаени трансакции и веднаш контактирајте ја Вашата банка доколку забележите проблем.

Совет бр. 3: Користете кредитна картичка, наместо дебитна картичка, за трансакции преку интернет.

Тоа ќе обезбеди дополнителна заштита. Доколку трошокот за Вашето купување ја надминува вредноста од 100 британски фунти и притоа користите кредитна картичка, продавачот и субјектот кој Ви ја издал картичката се подеднакво одговорни за евентуални проблеми.



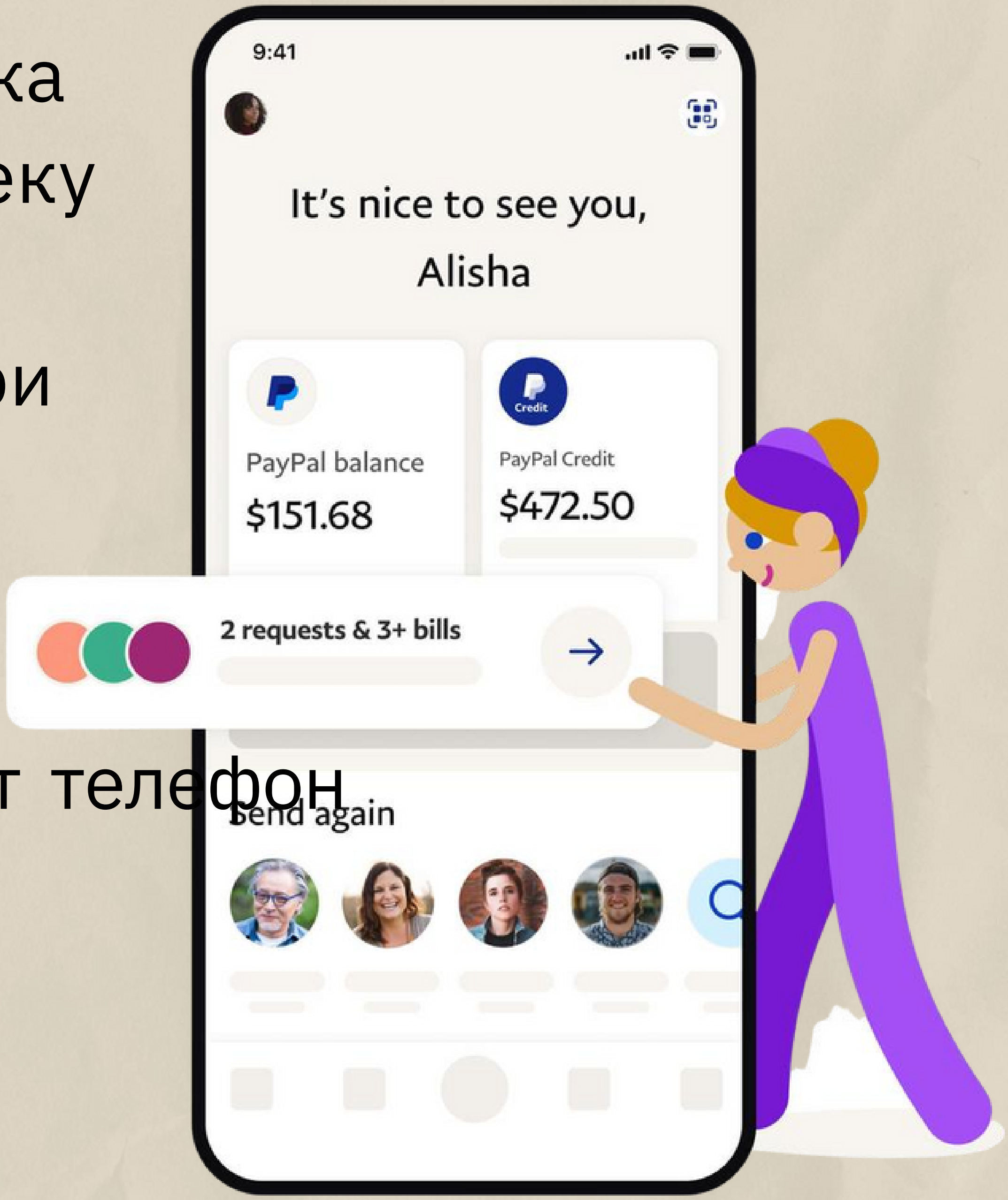


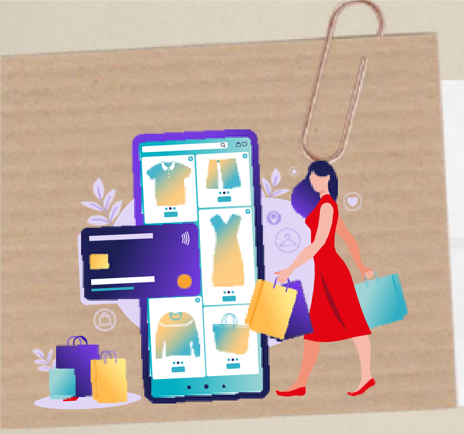
Безбедно купување преку интернет

Совет бр. 4: Размислете за користење сметка на PayPal.

Ова е електронска сметка што ја поврзувате со Вашата банкарска сметка или платежна картичка за да платите при купување преку интернет. Доколку не сакате да користите кредитна картичка, PayPal претставува безбедна опција и има поголема заштита при плаќање отколку дебитната картичка.

Преземете ја апликацијата на Вашиот телефон или регистрирајте се бесплатно преку интернет. После тоа, можете да ја користите како опција за плаќање при Вашите купувања.

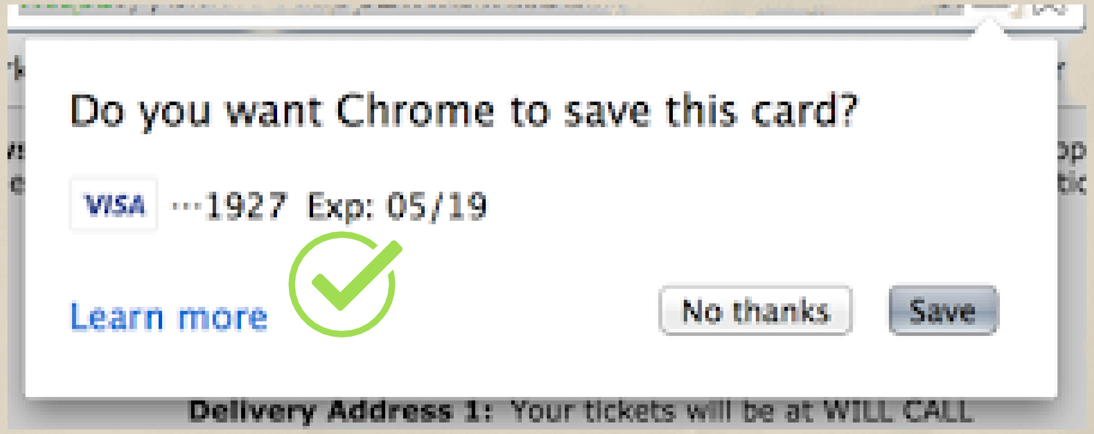




Безбедно купување преку интернет

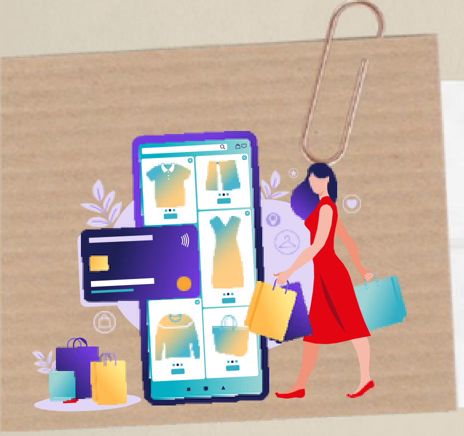
Совет бр. 5: Не ги зачувувајте деталите за Вашата картичка.

Понекогаш веб-локацијата или Вашиот интернет-прегледувач бара од Вас да ги зачувате деталите за Вашата картичка за следниот пат.



Никогаш не го правете тоа на споделен компјутер и осигурете дека

Вашиот уред е заштитен со лозинка, ПИН-код или пријавување со отпечаток од прст доколку ги зачувате деталите за Вашата картичка.



Безбедно купување преку интернет

6. Не наседнувајте на измами преку е-пошта

Може да добиете е-пошта или текстуални пораки кои нудат неверојатно поволни цени или тврдат дека има проблем при испорака на пакетите. Избришете ги сомнителните пораки од непознати испраќачи. Исто така, не отворајте прилози или не кликајте на врски во пораките бидејќи тие би можеле да го заразат Вашиот компјутер или телефон со вируси и друг злонамерен софтвер.

Безбедно купување преку интернет

7. Следете ја испораката.

Откако ќе извршите купување преку интернет, следете го за да бидете сигурни дека е испратено до Вашата адреса. Доколку трговецот одбие да даде информации за испорака или да одговори на Вашите барања за статусот на вашата нарачка, контактирајте со издавачот на Вашата кредитна картичка за помош. Тие може да ја сторнираат наплатата од Вашата сметка и да го разгледаат проблемот.

Uslugi gov.mk

Македонски Телеком

EVN

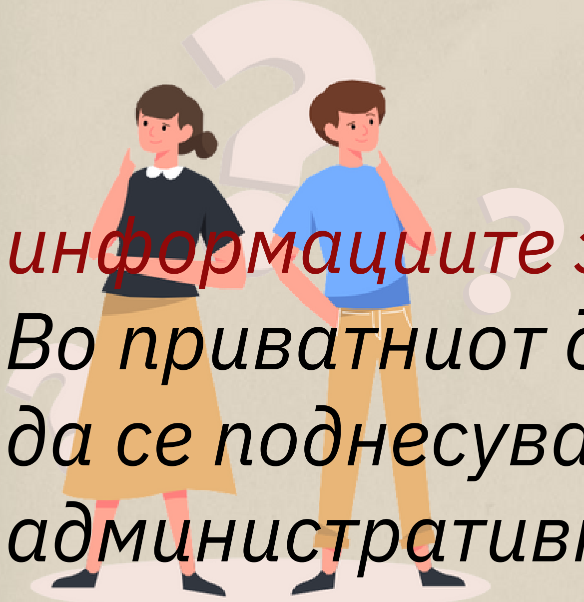
ОНЛАЈН ПРИСТАП ДО УСЛУГИ

КОИ СЕ ДЕЛ ОД ЈАВНИТЕ ЕЛЕКТРОНСКИ УСЛУГИ ВО СЕВЕРНА МАКЕДОНИЈА?

Uslugi.gov.mk -Националниот портал за е-услуги

Националниот портал за е-услуги е електронска платформа преку која можат да се добијат информации за јавните административни услуги од сите институции во државата и директно да се користат јавни административни услуги кои се достапни како е-услуги.

Порталот се состои од јавен и приватен дел. Во јавниот дел, кој е достапен за сите може да се најдат детални информации за тоа како да се заврши било која административна услуга од било која институција, вклучувајќи ги надлежните органи за услугата, потребните обрасци, поднесоци, услови, докази, рокови, информациите за плаќање, законската регулатива, итн.



Во приватниот дел, пак, кој е достапен само за регистрирани и идентификувани корисници, можат да се поднесуваат барања за добивање на одредена е-услуга, да се платат надоместоци и административни такси, да се следи статусот на постапката, и да се преземат други чекори кои овозможуваат завршување на одредена административна услуга директно онлајн, од комфорот на домот.

Услугите можат да се пребаруваат според категорија и поткатегорија, животеннастан, надлежен орган, со користење на алатка за пребарување, или пак според азбучен редослед. Сите услуги кои се достапни за завршување како е-услуги се означени со специјален „е“ знак и можат да се најдат директно на овој линк.

Регистрација, ЕЕБГ и eID

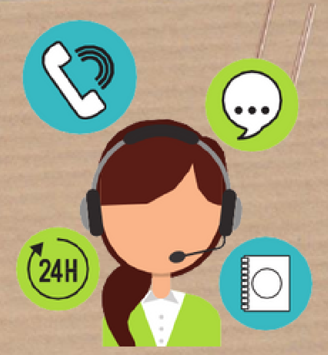
За пристапување во приватниот дел на Порталот и извршување на е-услуги, потребно е да се креира кориснички профил, односно eID профил, кој има неколку нивоа: основно, ниско и високо. eID е средств електронска идентификација и претставува кориснички профил за конкретно физичко лице.

При процесот на регистрација, eID профилот се поврзува со идентитетот на граѓанинот еднократно. Поврзувањето се прави со лично присуство и проверка на личните податоци, со помош на документи за лична идентификација, и со потврда во Централниот Регистар на Население (ЦРН).

Сите граѓани можат да се регистрираат бесплатно на следната врска > http://bit.ly/UslugiGovMkRegister
Важно е да се истакне дека граѓаните кои имаат кориснички сметки во УЈП можат директно да добијат eID профил со ниско ниво, кое им овозможува пристап до речиси сите е-услуги. Сè што треба да направат е да се најават со нивното корисничко име и лозинка од УЈП на следниот линк.

Број на достапни услуги

На порталот Uslugi.gov.mk се достапни информации за повеќе од 700 услуги и 1289 институции. Од услугите, 127 во овој момент се електронски, а овој број постојано ќе се зголемува во иднина согласно тековната дигитализација на институциите и органите.



Македонски Телеком

Македонски Телеком АД (скратливо АД Македонски телекомуникации) енајголемо трговско друштво за телекомуникации во Македонија, со седиште во Скопје.. „Македонски Телеком“ нуди широк опсег на телекомуникациски услуги и услуги од забавен карактер, како што се мобилни и фиксни телефонски услуги, опсег на услуги за интернет пристап вклучувајќи широкопојасен интернет (ADSL), IPTV производи и управува со националната телефонска мрежа.

За да платите онлајн сметка потребно е да пристапите на нивната страна на следниот линк:

https://www.telekom.mk/privatni-korisnici.nspx#

Потоа ќе најдете поле насловено „Телеком услуги“' и ќе ја селектирате опцијата

,,Плати брзо''

Плати онлајн сметки со Телеком

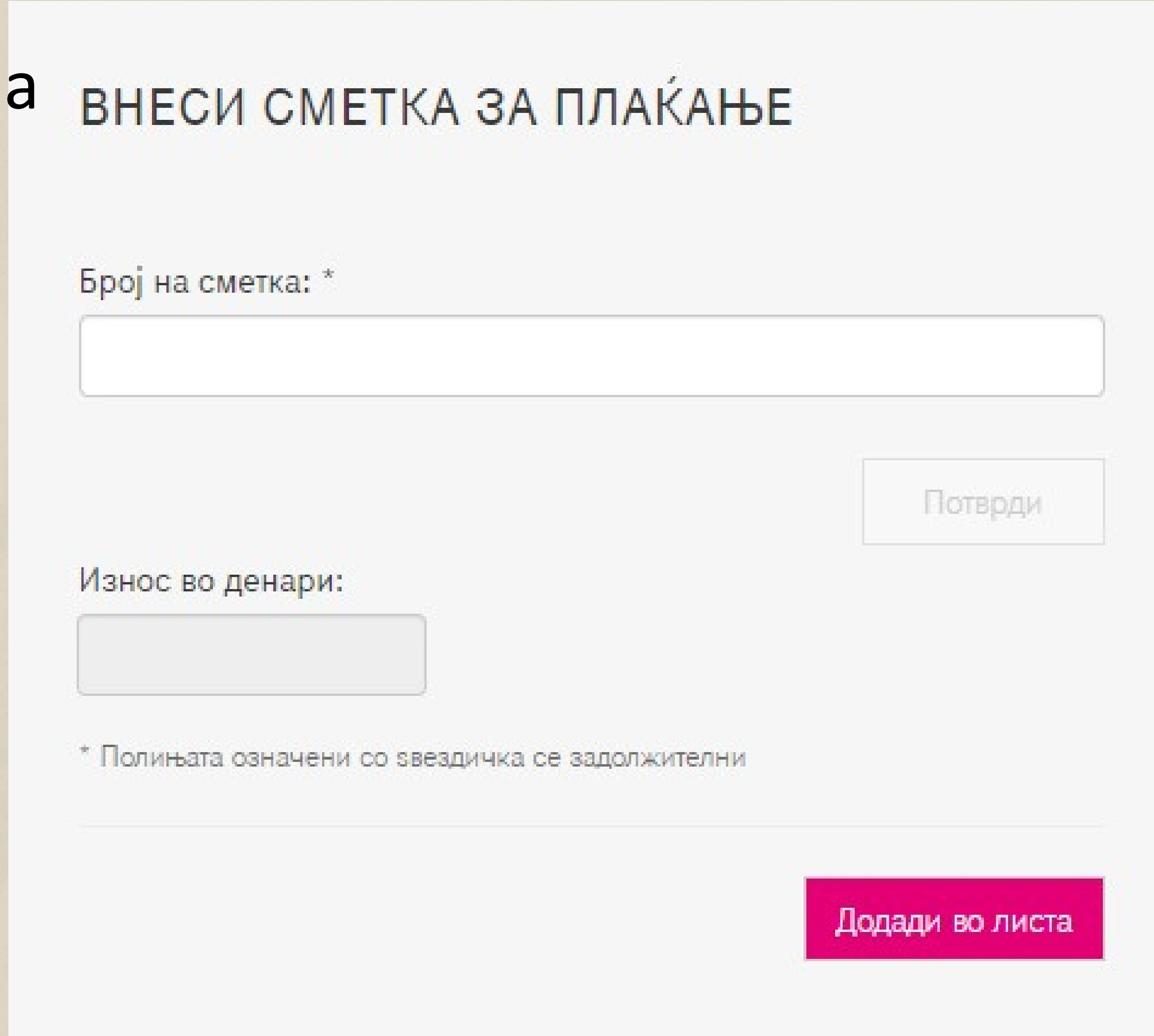
Откако ќе се најдете на страната Плати сметка, имате четири чекори кои треба да ги следите за да платите сметка:

1. Го внесуваме бројот на сметка и износот во денари

2. Ги внесуваме податоците за плаќање

3. Потоа потврдуваме на банката дека ја одобруваме исплатата на сметката.

4. Потврдуваме на снабдувачот со услуги се согласуваме со плаќањето на услугата



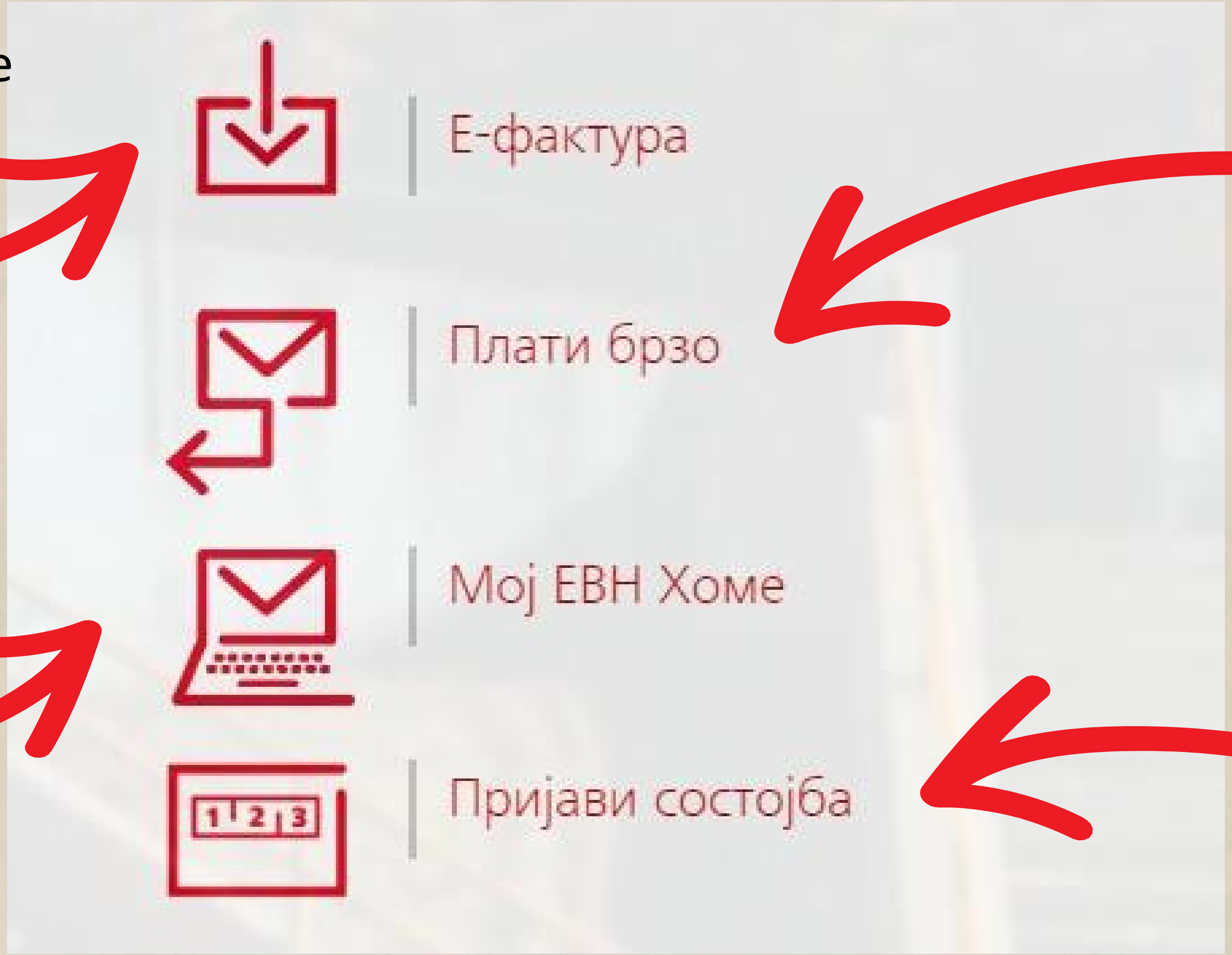
Плати ЕВН сметки за струја онлајн

ЕВН АД е македонско акционерско друштво за производство, трговија и дистрибуција

на електрична енергија.

Со оваа опција имате можност на брз и практичен начин да ја платите вашата сметка онлајн

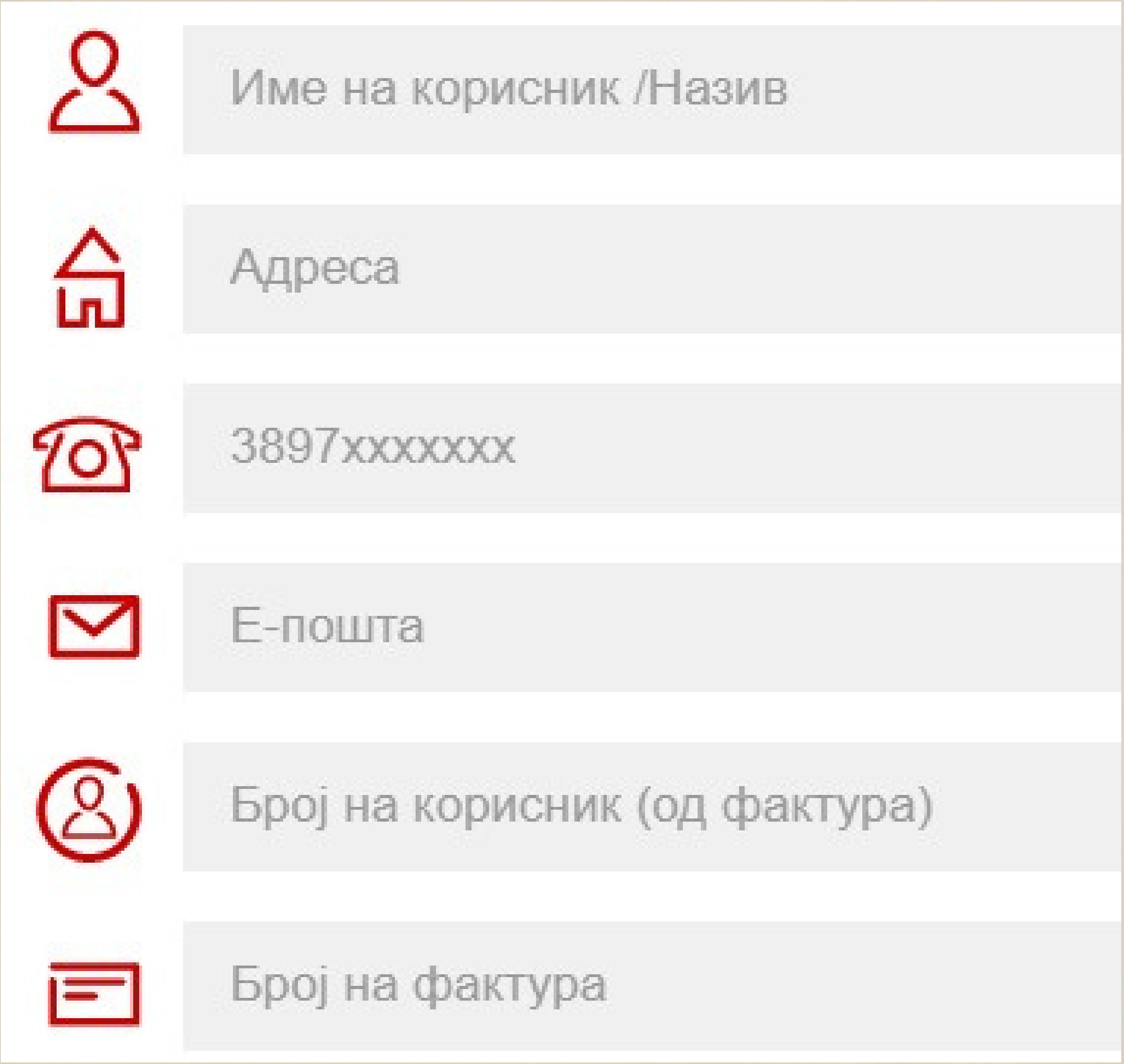
Со оваа опција можете сметките за потрошена електрична енергија по пат на електронска пошта.



Со оваа опција можете да креирате свој профил и да се најавите

Оваа опција ви овозможува сами да ја пријавите состојбата на вашето броило

Е-фактура



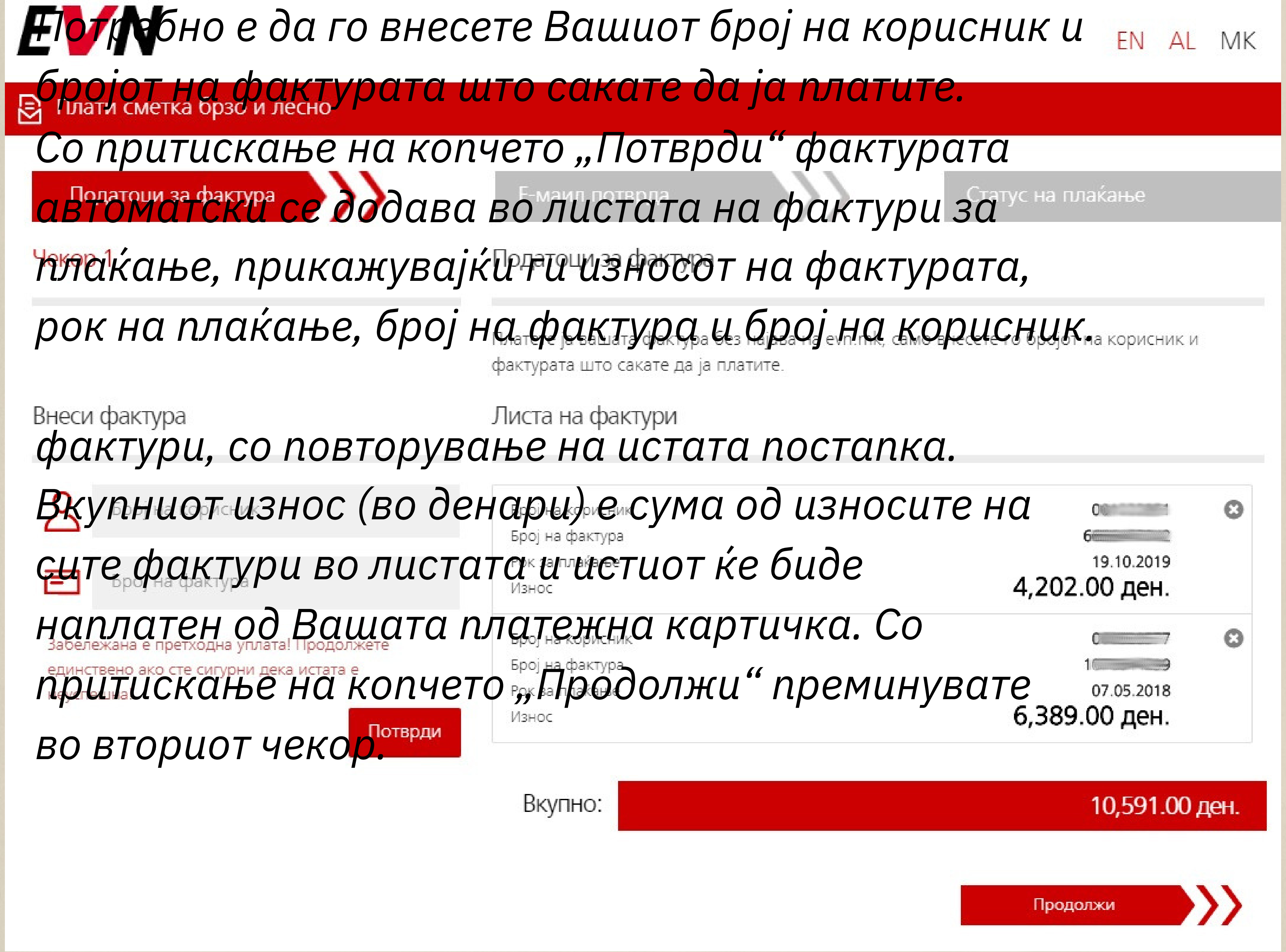
За да ги добивате Вашите фактури за електрична енергија во Вашето електронски сандаче, потребно е само да ги пополните следните податоци на формуларот:

Со притискање на копчето „Прати“, Вашето барање ќе биде регистрирано и обработено од наша страна, а на Вашата е-адреса ќе добиете потврда за успешно праќање на податоците.

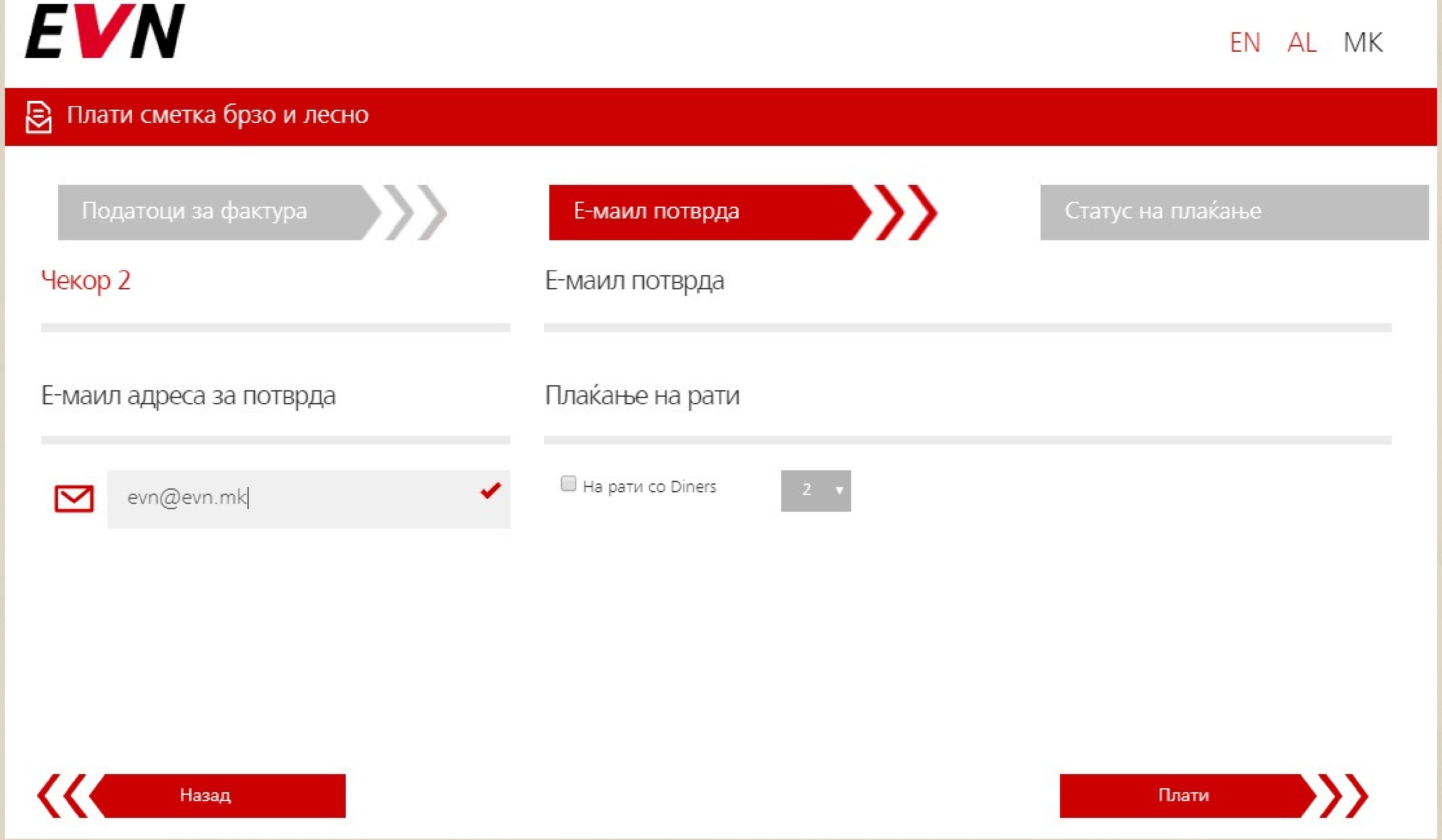
https://www.youtube.com/watch?v=0oAiZ6FK8-k

Плати брзо ЕВН онлајн

Услугата Брзо плаќање овозможува брзо и без регистрација на нашиот портал да ги платите своите фактури

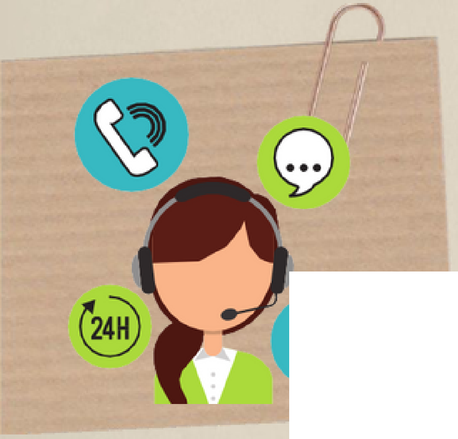


- *Потребно е да го внесете Вашиот број на корисник и бројот на фактурата што сакате да ја платите.*
- *Со притискање на копчето „Потврди“ фактурата автоматски се додава во листата на фактури за плаќање, прикажувајќи ги износот на фактурата, рок на плаќање, број на фактура и број на корисник.*
- *Услугата овозможува едновремено плаќање на повеќе фактури, со повторување на истата постапка.*
- *Вкупниот износ (во денари) е сума од износите на сите фактури во листата и истиот ќе биде наплатен од Вашата платежна картичка. Со притискање на копчето „Продолжи“ преминувате во вториот чекор.*



Чекор 2 – внесување на е-пошта адреса за потврда

- *За да продолжите со плаќањето и добиете потврда за уплатата, задолжително ја внесувате својата е-адреса.*
- *Доколку плаќате со Diners кредитна картичка, можете да одберете својот долг да го платите на рати со одбирање на полето „на рати со Diners“ и одбирање на бројот на рати.*
- *По притискање на копчето „Плати“, продолжувате со плаќањето.*



EVN

Информации за плаќањето

Трговец	EVN MAKEDONIJA
Интернет страница	http://www.evn.mk/
Износ	MKD 480,00

Податоци за платежна картичка

Број на картичка	123412341234
CVV2/CVC2	•••
Датум на истек	1 / 2019

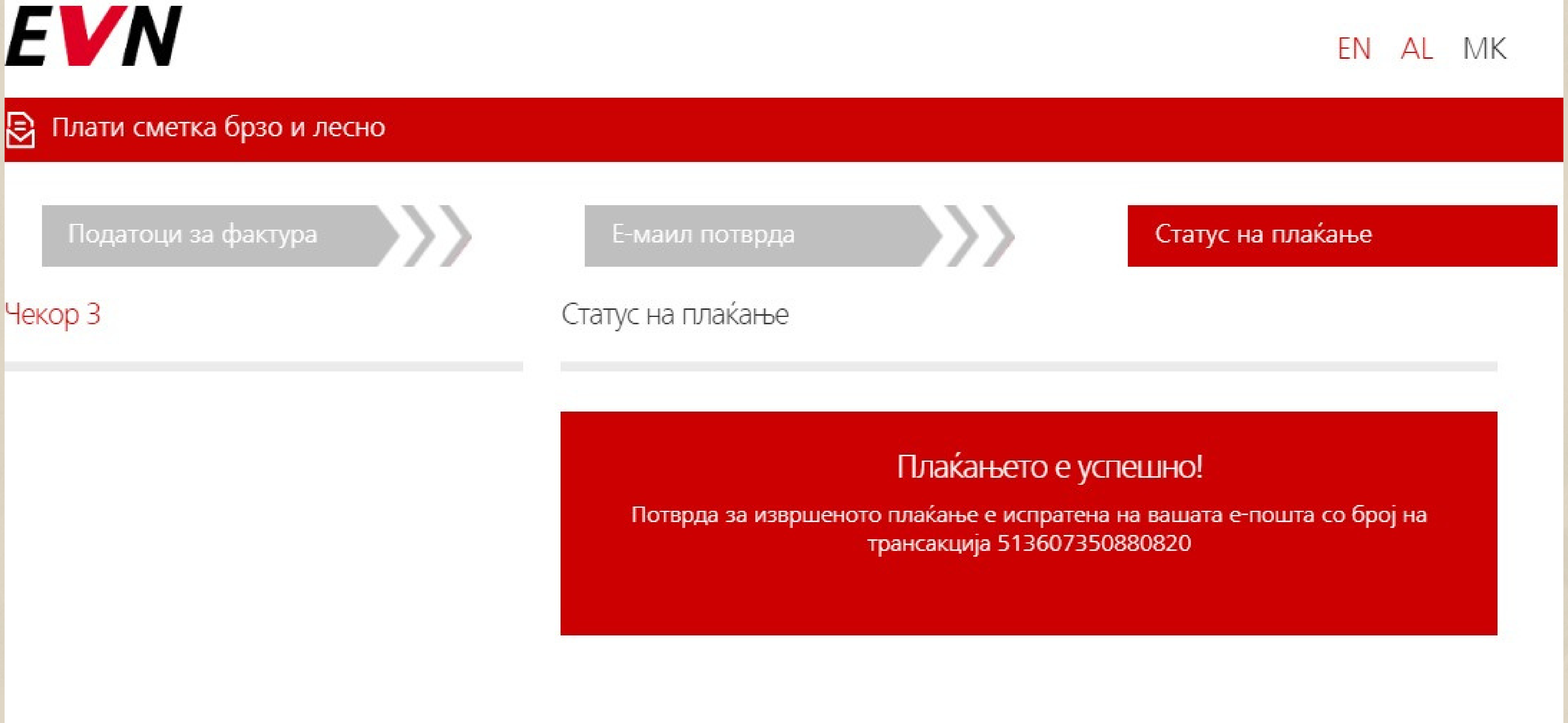
Потврди   Откажи

GODADDY.COM® VERIFIED & SECURED
Mastercard SecureCode
Verified by VISA

Copyright ©2018 NLB Tutunska Banka

Чекор 3 – Внес на податоци за платежна картичка

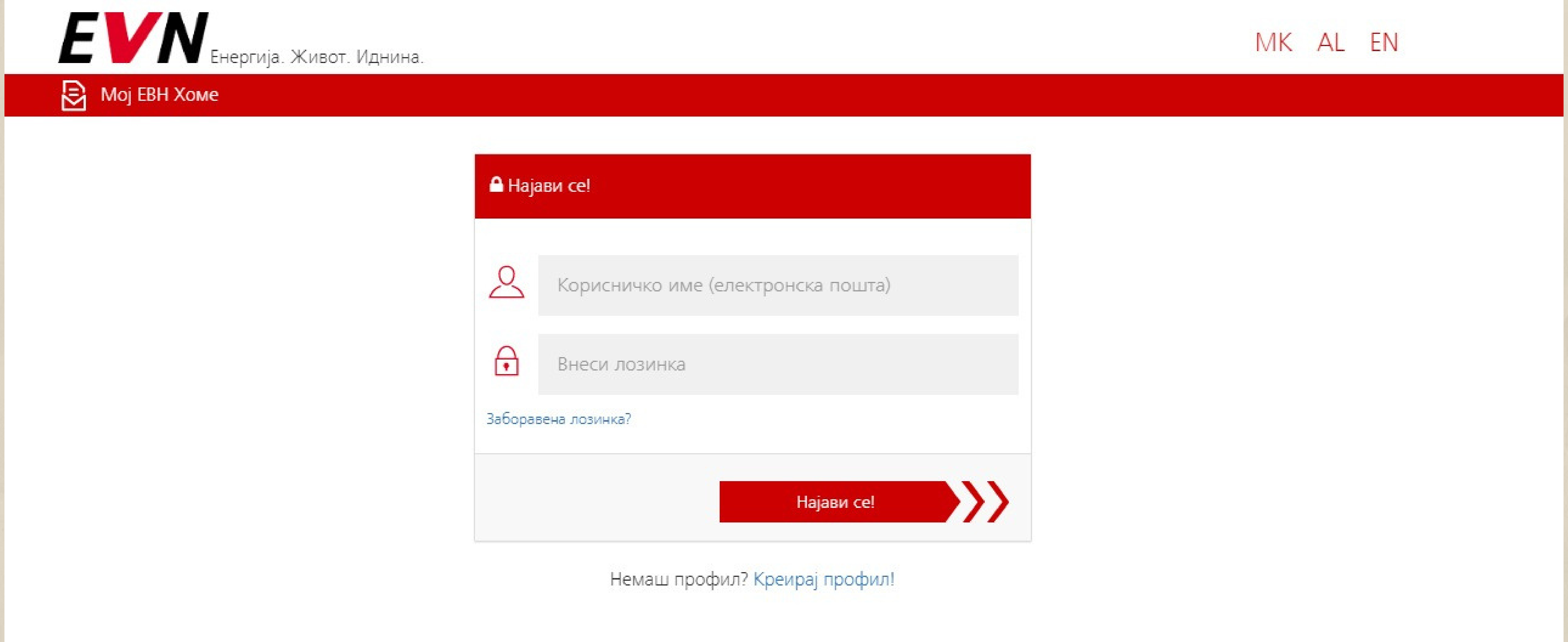
- Внесувате податоци од Вашата платежна картичка за да се реализира платежната трансакција.
- Додека сте пренасочени на веб страницата на НЛБ Банка, ЕВН нема увид во податоците што ги внесувате.
- На оваа страница имате можност да ги потврдите внесените податоци и да продолжите понатаму, или да се откажете од електронското плаќање сметки. Се уште се наоѓате на страницата на НЛБ Банка



Чекор 4 – Статус од платежната трансакција

- ***По извршување на плаќањето, повторно сте пренасочени на веб страницата на ЕВН, каде што ќ добиете информација за успешноста на трансакцијата.***
- ***На Вашата е-адреса ќе добиете потврда за трансакцијата односно информација за успешноста на истата. https://www.youtube.com/watch?v=Cn3b-Y_BPeA***

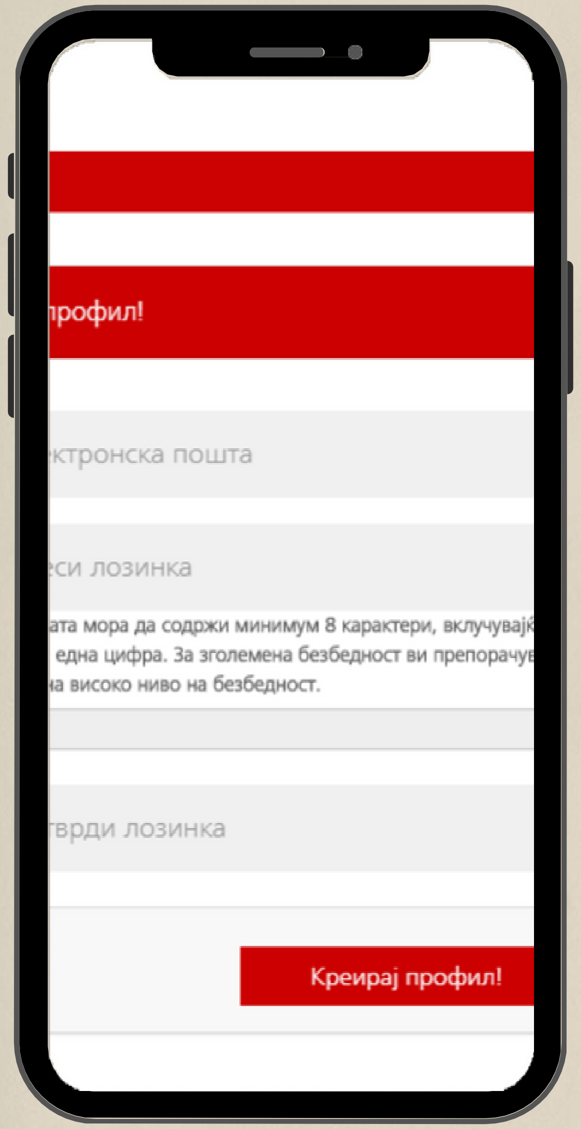
Регистрација и најава - Мој ЕВН Хоме

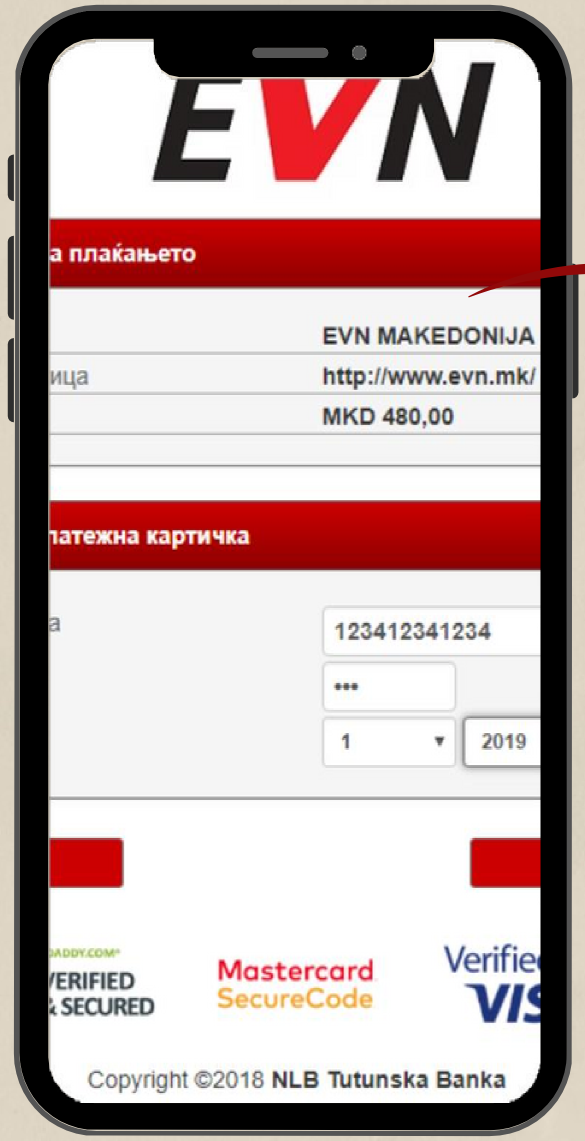


Доколку сте веќе регистриран корисник, со внесување на вашето корисничко име и лозинка, и избирање на полето „Најави се“ започнувате со користење на нашите онлајн услуги.

Корисници регистрирани за услугата „Е-пункт“ која е сега надградена и преименувана во Мој ЕВН Хоме можат да се пријават со електронската пошта како корисничко име и истата лозинка.

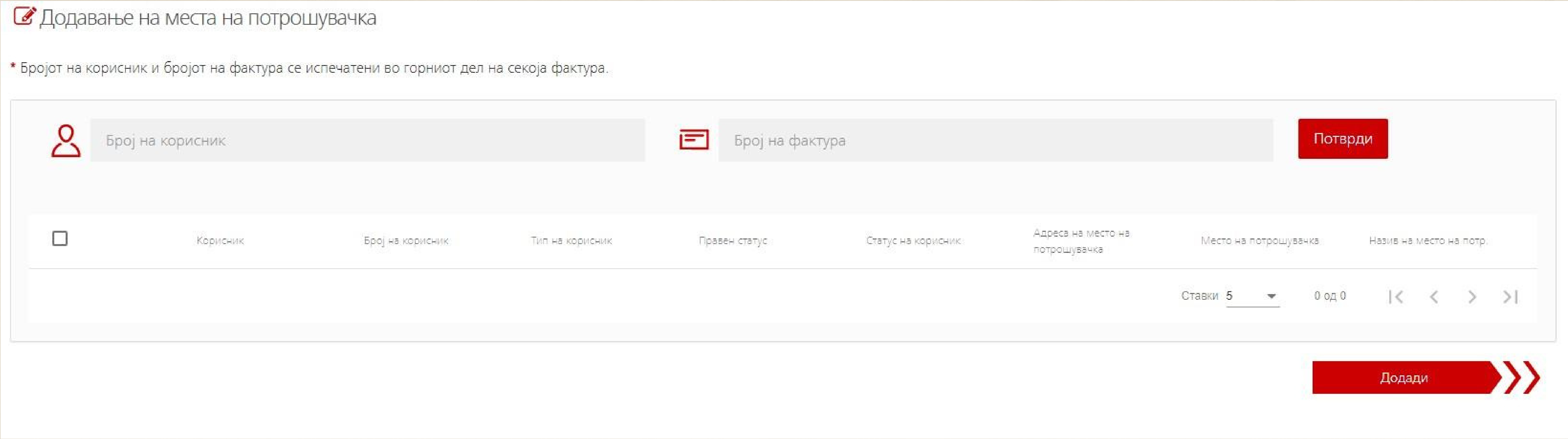
За регистрација на профил на Мој ЕВН Хоме, притиснете на „Регистрирај се“ и внесете валидна електронска пошта и лозинка со минимум 8 карактери, вклучувајќи една буква и една цифра и на крај притиснете „Креирај профил“.





На Вашата електронска пошта ќе пристигне порака за активација. Со притискање на линкот Вашиот профил е финално креиран и можете да преминете кон најава на Мој ЕВН Хоме.

Мој ЕВН Хоме е услуга наменета за корисниците домаќинства.



За да почнете да го користите вашиот кориснички профил, најпрво треба да го уредите, односно да додадете кориснички броеви/места на потрошувачка за кои ви се потребни услугите на Мој ЕВН Хоме.

1. ***Одберете ја опцијата од левото мени насловена „Места на потрошувачка" и во десниот дел притиснете го полето „+ Додај мерно место".***

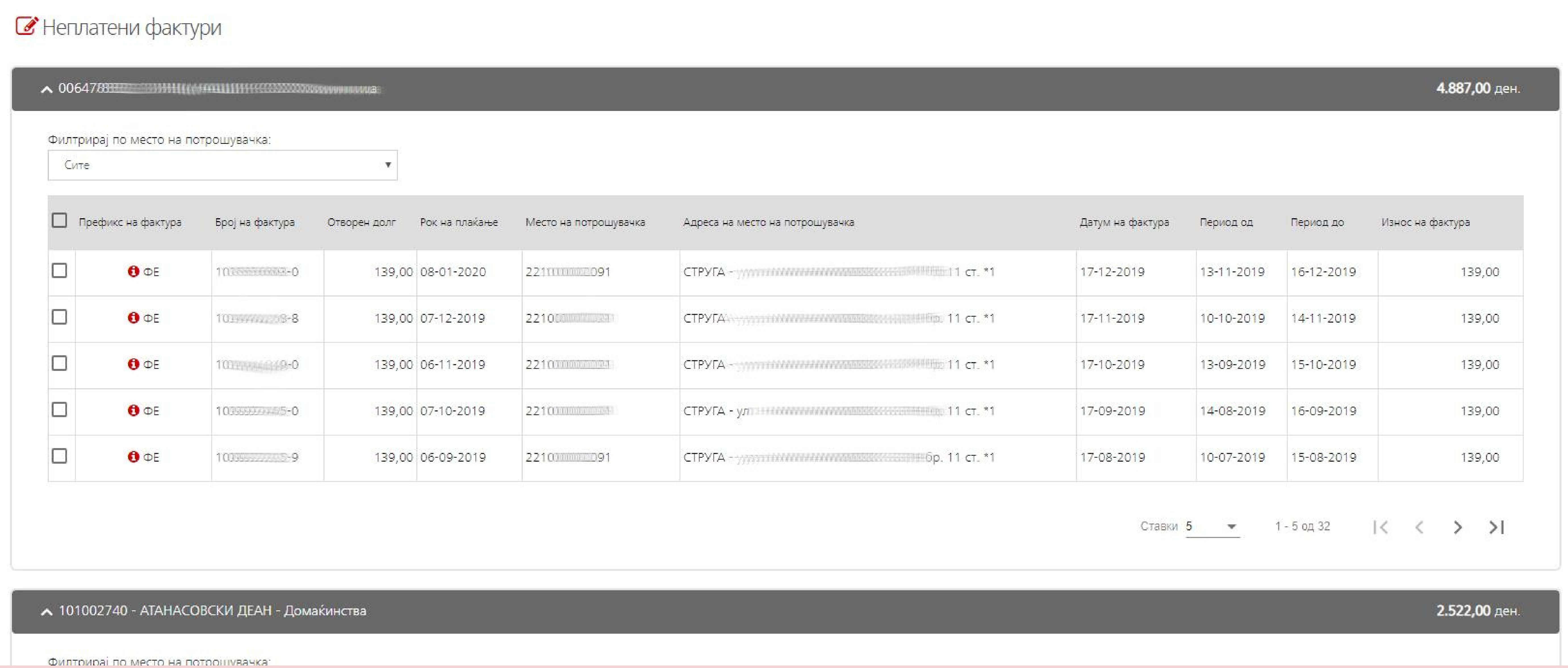
2. ***Во двете полиња потребно е да внесете:***

- Број на корисник (горен десен агол на фактурата за електрична енергија)

- Број на фактура (под бројот на корисник на фактурата за електрична енергија)

За финализација на барањето, одберете „Потврди".

Возможно е додавање на повеќе места на потрошувачка во еден кориснички профил. Исто така едно место на потрошувачка може да биде додадено во повеќе профили. Ова е особено поволно за сопственици на имот што се дава под наем, но и закупци на имот. Местата на потрошувачка исто така има опција да се избришат од профилот. Тоа може да го направите со избирање на иконата која изгледа како канта за отпадоци.



Неплатени фактури

^ 006478[illegible] — 4.887,00 ден.

Филтрирај по место на потрошувачка:

Сите

	Префикс на фактура	Број на фактура	Отворен долг	Рок на плаќање	Место на потрошувачка	Адреса на место на потрошувачка	Датум на фактура	Период од	Период до	Износ на фактура
☐	ФЕ	10[illegible]-0	139,00	08-01-2020	221[illegible]091	СТРУГА - [illegible] 11 ст. *1	17-12-2019	13-11-2019	16-12-2019	139,00
☐	ФЕ	10[illegible]-8	139,00	07-12-2019	2210[illegible]	СТРУГА [illegible] 11 ст. *1	17-11-2019	10-10-2019	14-11-2019	139,00
☐	ФЕ	10[illegible]-0	139,00	06-11-2019	2210[illegible]	СТРУГА - [illegible] 11 ст. *1	17-10-2019	13-09-2019	15-10-2019	139,00
☐	ФЕ	10[illegible]-0	139,00	07-10-2019	2210[illegible]	СТРУГА - ул [illegible] 11 ст. *1	17-09-2019	14-08-2019	16-09-2019	139,00
☐	ФЕ	10[illegible]-9	139,00	06-09-2019	2210[illegible]091	СТРУГА - [illegible] бр. 11 ст. *1	17-08-2019	10-07-2019	15-08-2019	139,00

Ставки 5 — 1 - 5 од 32

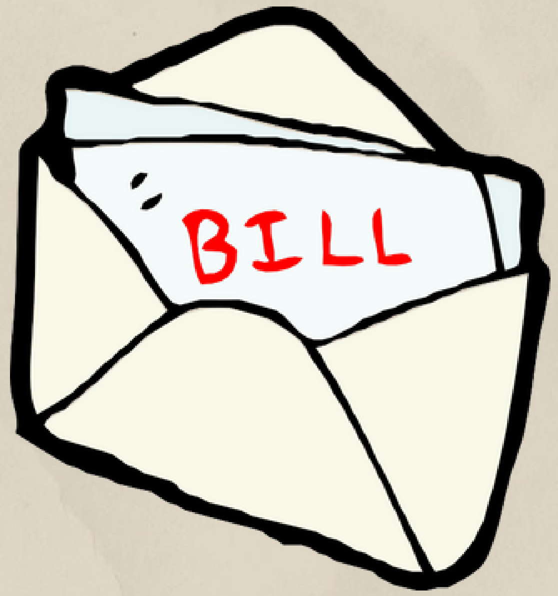
^ 101002740 - АТАНАСОВСКИ ДЕАН - Домаќинства — 2.522,00 ден.

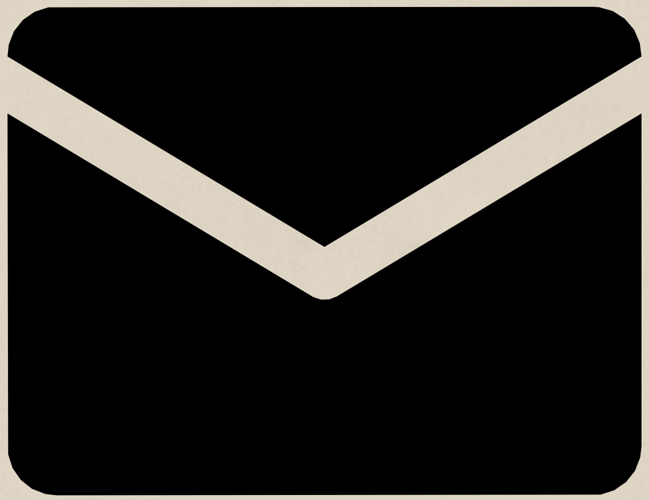
Филтрирај по место на потрошувачка:

Во овој дел можете да ги погледнете тековните неплатени фактури за регистрираните места на потрошувачка во Вашиот профил. Изберете кои фактури сакате да ги платите со одбирање на квадратчињата во најлевата колона од табелата.

Во најдолниот лев агол, до полето „Вкупно за наплата“ е прикажан збирот на селектираните фактури во денари. Со одбирање на опцијата „Плати”, можете да платите една или повеќе фактури одеднаш, за еден или повеќе кориснички броеви односно места на потрошувачка. Постои и опција за плаќање на рати со Diners.

Мој ЕВН Хоме нуди опција за преземање на електронски копии од фактурите за електрична енергија. Откако ќе го изберете менито „Копија од фактура“ пред Вас добивате табела со преглед на платени и неплатени фактури. Во најдесната колона, со притискање на симболот за „.pdf“, можете да преземете било која фактура од листата





Во „Преглед на трансакции“ можете да ги погледнете сите претходни успешни и неуспешни обиди за плаќање на фактурите за електрична енергија преку вашиот профил на Мој ЕВН Хоме (претходно Е-пункт). За неуспешни уплати, причината е наведена во делот „Опис на грешка”.

РЕФЕРЕНЦИ

БИДИ БЕЗБЕДЕН НА ДРУШТВЕНИТЕ МЕДИУМИ

https://safety.google/security/security- tips/

https://us.norton.com/internetsecurity- privacy-password-security.html

https://www.kidscape.org.uk/advice/a dvice-for-young-people/dealing-with- cyberbullying/staying-safe-on-

social- media/

https://www.facebook.com/help/1220 06714548814

ЗАШТИТА НА ПОДАТОЦИ И ДИГИТАЛЕН ОТПЕЧАТОК

https://www.gov.uk/data-protection

https://www.familylives.org.uk/advice/your-family/online-safety/digital- footprints

https://www.security.org/digital- safety/

https://staysafeonline.org/online- safety-privacy-basics/5-ways-spot- phishing-emails/

РЕФЕРЕНЦИ

ИНТЕРНЕТ-НАСИЛНИШТВО

https://www.researchgate.net/publicat i on/358402280_Bullying_Cyberbullying_and_Hate_Speech

https://www.unicef.org/end-violence/how-to-stop-cyberbullying

https://www.kidscape.org.uk/advice/a dvice-for-young-people/dealing-with-cyberbullying/think-before-you-post/

https://www.brandwatch.com/reports/ cyberbullying-2016/

ЕЛЕКТРОНСКО БАНКАРСТВО И КУПУВАЊЕ ПРЕКУ ИНТЕРНЕТ

https://www.ageuk.org.uk/globalassets/age-uk/documents/digital-instruction-guides/a-beginners-guide-to-staying-safe-online.pdf

https://www.consumerfinance.gov/about-us/blog/online-mobile-banking-tips-beginners/

https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/

ПРИСТАП ДО ЈАВНИ СЕРВИСИ ПРЕКУ ИНТЕРНЕТ

https://evnonline.mk/index/evnhome

https://www.youtube.com/watch?v=PQl0w7zOY

dc https://www.telekom.mk/privatni-

korisnici.nspx

https://uslugi.gov.mk/

Р
Е
Ф
Е
Р
Е
Н
Ц
И

SCAN ME

SCAN ME

Проект „ДИГИТАЛИЗИРАЈ - алатки за возрасни Роми [redacted] интернет и да го промовираат образованието“

Amaro Foro e.V.
facebook.com/AmaroForo/
instagram.com/amaro_foro/

EGYÜTT HATÓ KÖZÖSSÉGÉPÍTŐ EGYESÜLET
facebook.com/EgyuttHato/
instagram.com/egyutthato/

NEVO PARUDIMOS
facebook.com/NevoParudimos/
instagram.com/nevoparudimos/

RROMA
facebook.com/rromassn.org/
instagram.com/rromassn/

SCAN ME

SCAN ME