

Прирачник
за препознавање лажни профили
на социјалните мрежи

Автори:

Славица Трајковска - Препознавање лажни профили и безбедност на Фејсбук

Јана Ѓелевска - Препознавање лажни профили и безбедност на Инстаграм

Александар Талев - Препознавање лажни профили и безбедност на Твитер

Прирачникот е изработен во рамки на Пилот проект: „Систем за рано предупредување за исчезнати деца“ спроведуван од Новинари за човекови права и управуван од ЕКПАТ Австрија.

Овој материјал е изготвен со помош на Федералното министерство за социјални работи, здравство, грижа и заштита на потрошувачите на Република Австрија. Содржината на овој материјал е исклучива одговорност на авторот и на никој начин не ги одразува ставовите на Федералното министерство за социјални работи, здравство, грижа и заштита на потрошувачите на Република Австрија.

 **Federal Ministry**
Republic of Austria
Social Affairs, Health, Care
and Consumer Protection



Октомври 2022

СОДРЖИНА

Вовед.....	4
А. ПРЕПОЗНАВАЊЕ ЛАЖНИ ПРОФИЛИ И БЕЗБЕДНОСТ НА ФЕЈСБУК.....	6-17
1. Како да останете безбеден на Фејсбук и кои безбедносни можности ви се на располагање...	6
2. Што е Facebook's privacy shortcuts – кратенки за приватност и како да ги пронајдете?.....	6
3. Како да пријавите навредлива содржина?.....	8
3.1. Како да пријавите содржина која вознемирува?.....	8
3.2. Како да пријавите објава?	13
3.3. Како да пријавите вознемирувачки фотографии или видеа?.....	14
3.4. Како да пријавите вознемирувачки пораки преку Месинџер?.....	14
3.5. Како да постапите со пријава ако немате профил на Фејсбук?.....	16
Б. ПРЕПОЗНАВАЊЕ ЛАЖНИ ПРОФИЛИ И БЕЗБЕДНОСТ НА ИНСТАГРАМ.....	18-27
1. Правна рамка.....	18
2. Инстаграм – социјална мрежа	19
3. Политика и услови на приватност	20
4. Безбедност на инстаграм	21
5. Како да препознаам лажен профил на инстаграм?.....	23
5.1. Пребарај ја сликата на профилот.....	23
5.2. Погледнете ги другите следбеници на инстаграм профилот.....	25
5.3. Прочитајте ги описот и коментарите на сликите	25
5.4. Пребарувајте го сопственикот на профилот на други социјални мрежи	25
5.5. Пребарувајте го сопственикот на профилот на интернет пребарувачи	25
6. Начин на пријавување на Инстаграм	26
В. ПРЕПОЗНАВАЊЕ ЛАЖНИ ПРОФИЛИ И БЕЗБЕДНОСТ НА ТВИТЕР.....	28-34
1. Твитер – задржување на вниманието со лажна сметка, бот или трол	28
2. Што претставува лажна сметка?	28
3. Како можам да забележам лажна сметка?.....	29
3.1. Имиња на сметки и адреси на профили.....	29
3.2. Слики на профилот.....	29
3.3. Следбеници, пријатели, претплатници.....	30
3.4. Содржина и онлајн однесување.....	30
4. Што се ботови?	31
4.1. Како можам да забележам ботови?	31
5. Што се тролови?.....	31
5.1. Како да забележам тролови?.....	32
6. Како да блокирате и одблокирате неког на Твитер?.....	33
6.1. Како да блокирате или одблокирате неког користејќи го неговиот Твитер профил.....	33
6.2. Како да одблокирате неког на Твитер користејќи компјутер.....	33
6.3. Како да одблокирате неког на Твитер користејќи ја мобилната апликација.....	33
7. Како да пријавите несоодветен твит или директна порака.....	34

ВОВЕД

Благодарение на ненадејниот пораст на школувањето од далечина, на родителите им стана потешко од кога било да управуваат со дигиталната активност на своите деца. Децата се онлајн почесто отколку што би сакале многу родители. И повеќето родители не можат секогаш да најдат време да внимаваат на дигиталната активност на децата.

Тоа е стрес за родителите кои сакаат да ги заштитат своите деца. Многу истражувања ја покажуваат големината на предизвикот. Еве што се случува со денешните млади:

73% од тинејџерите не можат да го замислат животот без паметен телефон, а половина од нив го носат телефонот во кревет

44% од децата на возраст од 8 до 16 години се постојано онлајн, со предност за забава и апликации за социјални медиуми

40% од децата откриваат чувствителни информации на интернет, вклучувајќи ја и домашната адреса

Третина од младите лажат за својата возраст на интернет

37% од децата доживеале опасности на интернет, вклучувајќи малтретирање, финансиски закани и несоодветна содржина

Како родител, старател, едукатор, не можете да ја надгледувате сè што детето прави на својот паметен телефон и вашиот лаптоп. Дури и да можеш, дали треба? Технологијата ќе игра важна улога во нивните животи од детството до зрелоста. Овие рани години се можност за нив да ги развијат вештините што им се потребни за да останат безбедни на интернет.

Идеалниот пристап е да ги едуцирате и да ги поттикнете децата за да научат како да се чуваат себеси безбедни.

Едуцирајте се за да можете да помогнете во заштитата на децата.

Ако сакате да ги зачувате децата безбедни, прво мора да ги разберете опасностите со кои се соочуваат кога ќе влезат на интернет. Кога сте целосно образовани, можете да им помогнете, да ги оддалечите од ризик, за да можат да се забавуваат и да останат безбедни.

Општо земено, постојат три категории на закани со кои се соочуваат децата кога одат на интернет:

- **Странци:** Предаторите навистина демнат на сајтови кои привлекуваат деца, како што се социјалните медиуми и онлајн игрите. Овие предатори често се преправаат дека се деца, техника позната како Catfishing. Има и хакери и сајбер-криминалци кои ќе таргетираат секого со слаба безбедност, без разлика дали се работи за дете или возрасен. Тие, исто така, може да се обидат да го измамат детето да сподели лозинки или детали за плаќање.

- **Врсници:** Детето може да доживее малтретирање или малтретирање од деца што ги познава. Ова често може да се случи на приватни разговори во социјалните медиуми и апликациите за пораки. Понекогаш, другите деца може да споделуваат приватни информации за вашето дете, што може да предизвика голема вознемиреност. Доколку овие податоци се од сексуална природа, како што се интимните слики, ова може да претставува кривично дело.
- **Себе:** Децата без надзор и самите се ризик на интернет. Тие често кликуваат на копчињата или инсталираат софтвер без да ги разберат последиците од нивните постапки. Тие, исто така, може јавно да објавуваат приватни информации, како што се нивниот датум на раѓање или адреса.

За да се заштитат од овој вид на опасност, треба да поттикнете кај децата правилно користење на интернет и да инсталирате солиден антивирусен софтвер.

Интернет безбедноста е област од информатиката која се занимава со одбрана на компјутери, сервери, мобилни уреди, електронски системи, мрежи и податоци од малициозни (вируси тројанци, црви, итн) напади. Познато е и како безбедност на информатичката технологија или електронска безбедност на информациите. Терминот се применува во различни контексти, од бизнис до мобилни компјутери и може да се подели во неколку вообичаени категории.

- **Мрежна безбедност** е делот каде се врши обезбедување на компјутерска мрежа од натрапници, без разлика дали се целни напаѓачи или малициозен софтвер.
- **Безбедноста на информациите** ги штити интегритетот и приватноста на податоците и при складирање и при трансфер.
- **Оперативната безбедност** ги вклучува процесите и одлуките за ракување и заштита на податоците. Дозволите што ги имаат корисниците при пристап до мрежата и процедурите што одредуваат како и каде може да се складираат или споделуваат податоците, спаѓаат во овој чадор за заштита.
- **Обновувањето на податоците и програмите од катастрофи после напади** дефинираат како да се реагира на инцидент со сајбер-безбедност или кој било друг настан што предизвикува губење на програми или податоци.
- **Образованието за крајните корисници** се однесува на најнепредвидливиот фактор на сајбер-безбедноста: луѓето. Секој може случајно да воведо вирус во инаку безбеден систем со тоа што не ги следи добрите безбедносни упатства. Учењето на корисниците да бришат сомнителни прилози за е-пошта, да не приклучуваат неидентификувани USB-дискови и разни други важни лекции е од витално значење за безбедноста на секој.
- **Безбедноста на работењето на интернет** се фокусира на одржување на софтверот и уредите без закани. Заразена апликација може да обезбеди пристап до податоците место да ги заштити.

Во овој прирачник преку едноставни насоки ќе им презентираме на родителите, старателите, едукаторите, но и на младите корисници директно повеќе начини како да бидат и да останат безбедни на интернет и социјалните мрежи.

А. ПРЕПОЗНАВАЊЕ ЛАЖНИ ПРОФИЛИ И БЕЗБЕДНОСТ НА ФЕЈСБУК

1. Како да останете безбедни на Фејсбук и кои безбедносни можности ви се на располагање?

Еве неколку работи што можете да ги направите за да останете безбедни на Фејсбук:

А) Научете како да ги користите кратенките **privacy shortcuts** и поставките **settings** за приватност на Фејсбук за безбедно споделување и поврзување со други

Б) Научете како да **препознаете чувствителна содржина и однесување** и како да ги **пријавите**

В) Запомнете ги овие едноставни правила за да останете безбедни на интернет:

- Никогаш не ја споделувајте вашата лозинка
- Размислете добро пред да објавите
- Прилагодете ги вашите поставки за приватност и често прегледувајте ги
- Прифатете барања за пријателство само од луѓе кои лично ги познавате
- Пријавете работи што изгледаат сомнително

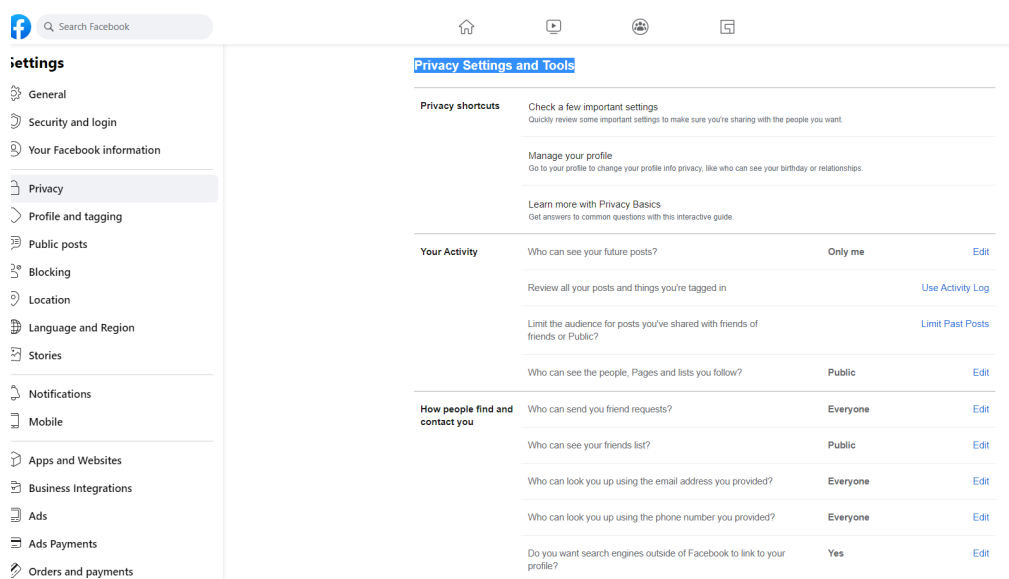
2. Што е Facebook's privacy shortcuts – кратенки за приватност и како да ги пронајдете?

Кратенките за приватност ви даваат брз пристап до некои од најкористените поставки и алатки за приватност.

За да ги најдете вашите кратенки за приватност:

Можете да ги посетите вашите кратенки за приватност **privacy shortcuts** во вашите поставки на Фејсбук - **Privacy Settings and Tools**.

1. Најавете се на вашата сметка на Фејсбук.
2. Кликнете на сликата на вашиот профил.
3. Изберете Поставки и приватност (Settings & Privacy).
4. Кликнете Поставки (Settings) и изберете Приватност (Privacy).



Некои можности со кои кратенките за приватност ви помагаат да управувате:

- **Privacy - Приватност.** Прегледајте ги информациите како што се поставките за вашата локација.
- **Account Security - Безбедност на сметката.** Ажурирајте ги лозинката или предупредувањата.
- **Ad Preferences - Преференци за рекламирање.** Прегледајте ги вашите поставки за реклами и дознајте повеќе за рекламите на Фејсбук.
- **Your Фејсбук Information - Вашите информации на Фејсбук.** Прегледајте некои од вашите информации на Фејсбук користејќи **Access Your Information** - Пристап до вашите информации и **Activity Log** - дневник на активности.
- **Safety - Безбедност.** Користете го Центарот за безбедност за да дознаете за безбедноста на Фејсбук и да најдете корисни информации за теми како малтретирање (bullying).
- **Legal and Policies - политики.** Прегледајте ги политиките на Фејсбук, вклучително и **Privacy Policy** - Политика за приватност и **Community Standards** - стандарди на заедницата.

Имајте на ум, кратенките што ги наоѓате овде може да се променат со текот на времето за да ги одразуваат поставките и алатките што се најрелевантни.

Други начини за управување со вашата приватност

Дознајте повеќе за тоа како да контролирате кој може да гледа што споделувате. Од тука, можете да научите како да:

- изберете публика за вашите идни објави
- промените публиката за вашите минати објави
- ги уредите основните информации на вашиот профил и изберете кој може да ги види
- можете исто така да ги приспособите поставките за приватност за апликации и игри.

3. Како да пријавите навредлива содржина?

Најдобар начин да пријавите навредлива содржина или спам на Фејсбук е со користење на Report link – линкот за извештај во близина на самата содржина. Подолу се дадени неколку примери за тоа како можете да пријавите содржина. Дознајте повеќе за пријавување злоупотреба - **reporting abuse**.

Ако немате сметка или не можете да ја видите содржината што сакате да ја пријавите (на пример: некој ве **блокирал**), **дознајте што можете да направите**.

Профили

3.1. Како да пријавите профил кој вознемирува?

За да пријавите профил:

1. Одете на профилот што сакате да го пријавите со кликување на неговото име во вашата активност - Feed или пребарување.
2. Кликнете  надесно и изберете **Find support or report** - Најдете поддршка или пријавете.
3. За да дадете повратни информации, кликнете на опцијата што најдобро опишува како овој профил ве вознемирува.
4. Во зависност од вашите повратни информации, тогаш можеби ќе можете да поднесете извештај до Мета. За некои видови содржини, Фејсбук не бара од вас да поднесете извештај, но ги користи вашите повратни информации за да им помогне на Фејсбук системите да научат. Кликнете **Done** - Готово.

Ако некој ви досадува на Фејсбук, можете и да го отповикате - **unfriend** или блокирате - **block**.

3.1.1. Како да отфрлите нечиј профил - Unfriend

За да отфрлите нечиј профил од пријател:

1. Одете на тој профил со внесување на името на профилот во лентата за пребарување на врвот на Фејсбук.
2. Кликнете  на врвот на тој профил.
3. Кликнете **Unfriend**, а потоа **Confirm**.

Забелешка: Ако не можете да го најдете профилот што сакате да го отстраните, профилот може да е деактивиран, односно да е избришан.

За да отстраните пријател од деактивиран профил:

1. Кликнете на сликата на вашиот профил во горниот десен агол на Фејсбук.
2. Кликнете **Friends** - Пријатели.
3. Пребарајте го името на профилот.
4. Кликнете *******, а потоа изберете **Unfriend**.

Профилот што сте го исклучиле нема да биде известен. Ако не сакате некој да го гледа вашиот профил, да ве додаде како пријател или да ви испрати порака, можете да го блокирате неговиот профил.

Забелешка: ако отфрлите нечиј профил, исто така и вие ќе бидете отстранети од списокот на пријатели на тој профил. Ако сакате повторно да бидете пријатели со овој профил, ќе треба повторно да го додадете како пријател.

3.1.2. Како да блокирате нечиј Фејсбук профил

Кога блокирате профил на Фејсбук, тој профил повеќе нема да може да прави работи како што се: да ве означува или да гледа работи што ги објавувате на вашата сид. Блокирањето на профилот со кој сте пријатели ќе го отстрани од вашиот профил.

За да блокирате нечиј профил:

1. Кликнете на сликата на вашиот профил во горниот десен агол на Фејсбук.
2. Изберете **Settings & privacy** - Поставки и приватност, а потоа кликнете **Settings** - Поставки.
3. Кликнете на **Blocking** - Блокирање во менито од левата страна.
4. Во делот **Block users** - Блокирај корисници, внесете го името на профилот што сакате да го блокирате и кликнете **Block** - Блокирај.
5. Изберете го конкретниот профил што сакате да го блокирате од списокот што се појавува и кликнете **Block** - Блокирај, а потоа кликнете **Block [name]** - Блокирај [име].

Забелешка: ако не можете да најдете нечиј профил користејќи го овој метод, обидете се да отидете на профилот и да изберете **Block** - Блокирај од ******* менито во долниот десен дел од насловната фотографија.

Имај на ум:

- Кога ќе одблокирате нечиј профил, нема автоматски повторно да бидете пријатели. Ако блокирате профил со кој сте пријатели и потоа го одблокирате, ќе треба да му испратите ново барање за пријателство на тој профил.
- Луѓето нема да бидат известени кога ќе го блокирате нивниот профил.

3.1.3. Да ги видите профилите кои сте ги блокирале

Можете да ги прегледате профилите што сте ги блокирале на Фејсбук во вашите поставки.

За да ги видите профилите што сте ги блокирале:

1. Кликнете на сликата на вашиот профил во горниот десен агол на Фејсбук.
2. Изберете **Settings & privacy** - Поставки и приватност, а потоа кликнете **Settings** - Поставки.

3. На левата страна, кликнете **Privacy** - Приватност, а потоа кликнете **Blocking** - Блокирање.
4. Во делот **Block users** - Блокирај корисници, кликнете **Edit** - Измени, потоа **See your blocked list** - Види ја блокираната листа, за да ја видите листата на профили што сте ги блокирале на Фејсбук. Од тука, можете:
 - **Unblock a profile** - Деблокирајте профил. Кликнете **Unblock** до името на профилот што сакате да го одблокирате.
 - **Block a profile** - Блокирајте профил. Внесете го името на профилот што сакате да го блокирате, потоа кликнете **Block** - Блокирај и изберете **Block [name]** - Блокирај [име] за да потврдите.

3.1.4. Содржина која може да ја видите од блокиран профил

Да. Блокирањето ви овозможува да спречите многу интеракции со нечиј профил на Фејсбук, но сепак може да наидете на содржина што тој ја споделил.

Еве што може да видите:

- **Пораки:** Вашата историја на пораки со профил што сте го блокирале ќе остане во вашето сандаче. Ако блокираниот профил некогаш бил вклучи во разговор со група пријатели, можеби ќе можете да ги видите пораките. Запомнете, можете да напуштите разговор во кој не сакате да бидете дел или да избришете разговор што не ви се допаѓа.
- **Содржина на заеднички пријатели:** постои можност да видите содржина за блокираниот профил преку заеднички пријатели. На пример, ако блокираниот профилзначи заеднички пријател на фотографија, може да го видите ова на временската линија на вашиот пријател.
- **Фотографии:** може да видите фотографии или ознаки од блокираниот профил додадени од други луѓе.
- **Групи:** Профилот што сте го блокирале нема да може да ве додаде во група, но ќе можете да ги видите групите што блокираниот профил ги создал или во кои членува.
- **Настани:** Профилот што сте го блокирале нема да може да ве покани на настан, но ќе можете да гледате настани на кои сте поканети и вие и блокираниот профил.
- **Игри и апликации:** бидејќи игрите и апликациите ги водат надворешни програмери, блокот на Фејсбук нема да важи за нив. Така, може да видите некој чиј профил сте го блокирале додека играте, да игра (на пример: во собата за разговор на играта).
- **Оценки и рецензии на продавачи на Marketplace (е-продавници):** ако блокирате продавач на Marketplace за кој сте оцениле или поднеле оценка, тогаш профилот на продавачот сè уште ќе може да ја гледа, известува и одговара на вашата рецензија.
 - **Купувачи:** ако блокирате продавач на Marketplace за кој сте оцениле или поднеле рецензија, тогаш профилот на продавачот сè уште ќе може да ја гледа, пријави и одговори на вашата рецензија.
 - **Продавачи:** Ако блокирате купувач на Marketplace, тогаш сепак ќе можете да ги гледате оценките и рецензиите оставени од профилот на тој купувач. Сè уште ќе можете да пријавите и да одговорите на тие прегледи.

- **Дополнителни профили:** блокирањето профил нема да се пренесе на други профили што некој може да ги создаде. Сè уште може да ги гледате и да комуницирате со нивните други профили.

3.1.5. Како да блокирам неког да ме следи на Фејсбук?

Ако не сакате одредена личност да ве следи, ќе треба да го блокирате неговиот профил. Имајте на ум дека кога објавувате нешто, можете да изберете со кого ќе го споделите.

3.1.5.1. Одберете кој може да го види вашиот пост

За да изберете кој може да ја гледа вашата објава на Фејсбук, користете го избирачот на публика - **audience selector**.

Изборот на публика може да се најде на повеќето места каде што споделувате содржини на Фејсбук, како што се објави, фотографии и некои информации на вашиот профил.

Одберете ја вашата публика на Фејсбук

Изборот на публика ви овозможува да изберете одредена публика кога објавувате. Вашите опции може да вклучуваат:



Public - Јавно: Кога споделувате нешто со Public, тоа значи дека секој, вклучително и луѓе надвор од Фејсбук, може да го види.



Friends - Пријатели (+ пријатели на кој било означен): Оваа опција ви овозможува да објавувате работи на вашите пријатели на Фејсбук. Ако некој друг е означен во објава, тогаш публиката се проширува за да ги вклучи и означеното лице и нивните пријатели. Ако не сакате вашата фотографија или објава да бидат видливи за пријателите на луѓето што ги означувате, можете да ја прилагодите оваа поставка. Кликнете на **audience selector** - избирачот на публика веднаш до постот, изберете * **Custom** - Прилагодено и отштиктирајте го полето **Friends of those tagged** - Пријатели на означените.



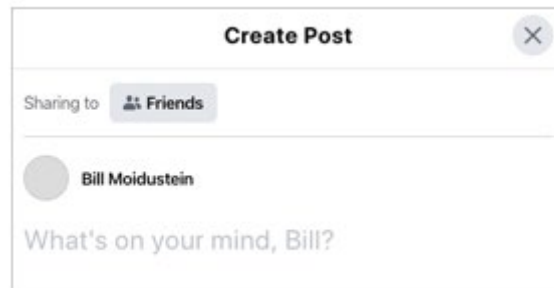
Only Me: Оваа опција ви овозможува да објавувате работи на вашата сид што се видливи само за вас. Објавите со публиката на Only Me ќе се појавуваат во вашата активност, но не и на вашите пријатели. Кога означувате неког во вашата содржина и избирате Only Me, публиката нема да се прошири за да го вклучи лицето што сте го означиле.

* **Custom** - Прилагодено: Кога ќе изберете Прилагодено, можете селективно да споделувате нешто со одредени луѓе или да го скриете од одредени луѓе. Може да споделувате и со одредени списоци со пријатели доколку сте ги поставиле. Custom, исто така, обезбедува опција за споделување со групи или мрежи на кои припаѓате.

За да изберете со кого ќе споделите некој пост:

1. На врвот на вашата активност или профил, кликнете **What's on your mind?** - Што ви е на ум? Оттука, можете да правите работи како што се објавување ажурирање статус, фотографија, видео или пријавување на настан.
2. Под вашето име, кликнете на избирачот на публика (на пример: **Friends -Пријатели**).

3. Кликнете на публиката што сакате да ја види вашата содржина (на пример: Friends, Public or Only Me).



Audience selector - Изборот на публика ќе се појави и на работи што веќе сте ги споделиле, за да можете да видите со кого сте ја споделиле секоја објава. Откако ќе споделите објава, имате опција да промените со кого е споделена.

Промена на публиката на пост на Фејсбук

Можете да го користите избирачот на публика за да промените кој може да ги гледа работите (на пример: објави и фотографии) што ги споделувате на вашиот сид, откако ќе ги споделите. Имајте на ум, кога споделувате нешто на туѓ сид, тие ја контролираат публиката за објавата.

За да ја промените публиката на работите што сте ги споделиле на вашиот сид:

- а. Кликнете на сликата на вашиот профил во горниот десен агол на Фејсбук.
- б. Одете надолу до објавата што сакате да ја уредите.
- в. Кликнете на избирачот на публика веднаш до датумот или времето на објавата. Иконата ќе биде различна во зависност од моменталните поставки на публиката.
- г. Изберете нова публика од опциите што се појавуваат (на пример: Јавно, Пријатели, Само јас).

3.1.6. Да блокирам пораки од профил на Фејсбук

За да блокирате пораки од профил на Фејсбук:

1. Во горниот десен агол на вашиот профил на Фејсбук, кликнете на  Messenger.
2. Отворете го разговорот со профилот што сакате да го блокирате.
3. На врвот на разговорот, кликнете .
4. Кликнете **Block** - Блокирај.
5. Кликнете **Block Messages and Calls** - Блокирај пораки и повици, потоа кликнете **Block** - Блокирај.

Забелешка: Блокирањето пораки од нечиј профил е различно од блокирањето на Фејсбук. Ако блокирате пораки од профил, но не го блокирате на Фејсбук, сепак ќе можете да го видите тој профил на Фејсбук. Во зависност од нивните поставки за приватност, можеби ќе можете да видите работи како што се ажурирањата на нивните статуси, коментари, допаѓања и ознаки на Фејсбук.

3.1.7. Да одблокирам неког на Фејсбук

Кога ќе одблокирате профил, тој профил ќе може да ги гледа вашите објави на Фејсбук што ги споделувате со јавноста. Профилот нема автоматски да стане ваш пријател на Фејсбук. Ако сакате да станете пријатели со профил што сте го одблокирале, ќе треба да испратите барање за пријателство на тој профил.

Забелешка: ако одблокирате профил, нема да можете повторно да го блокирате неколку дена.

Како да одблокирате неког на Фејсбук:

1. Кликнете на сликата на вашиот профил во горниот десен агол на Фејсбук.
2. Изберете **Settings & privacy** - Поставки и приватност, а потоа кликнете **Settings** - Поставки.
3. Во левата колона од вашите Поставки, кликнете на **Blocking** - Блокирање.
4. Во делот **Block Users** - Блокирај корисници треба да видите листа на профили што сте ги блокирале.
5. Кликнете **Unblock** - Деблок до профилот што сакате да го одблокирате.
6. Кликнете **Confirm** - Потврди за да завршите со деблокирање на профилот.

Објави (постови)

3.2. Како да пријавите објава?

За да пријавите објава:

1. Одете на објавата што сакате да ја пријавите.
2. Кликнете  во горниот десен агол на објавата.
3. Кликнете **Find support or report post** - Најди поддршка или пријави објава.
4. За да дадете повратни информации, кликнете на опцијата што најдобро опишува како оваа објава ве вознемирува. Кликнете **Next** -Следно.
5. Во зависност од вашите повратни информации, тогаш можеби ќе можете да поднесете извештај до Мета. За некои видови содржини, не бараме од вас да поднесете извештај, но ги користиме вашите повратни информации за да му помогне на системот да се усоврши. Кликнете **Done**.

3.2.1. Како да пријавите вознемирувачка објава на вашиот сид

1. Кликнете на сликата на вашиот профил во горниот десен агол на Фејсбук.
2. Одете на објавата и кликнете  во горниот десен агол.
3. Кликнете **Find support or report post** - Најди поддршка или пријави објава и потоа кликнете на опцијата што најдобро опишува како оваа објава ве вознемирува.

Можете исто така да го блокирате лицето кое ја објавило оваа содржина на вашиот времеплов.

Фотографии и видеа

3.3. Како да пријавите вознемирувачки фотографии или видеа?

За да пријавите фотографија или видео:

1. Кликнете на фотографијата или видеото за да ја проширите. Ако профилот е заклучен и не можете да ја видите фотографијата со целосна големина, кликнете **Find support or report photo**. - Најдете поддршка или пријавите фотографија.
2. Кликнете  десно од фотографијата или видеото.
3. Кликнете **Find support or report photo** - Најди поддршка или Пријави фотографија, за фотографии или **Report Video** - Пријави видео, за видеа.
4. Изберете ја опцијата што најдобро го опишува проблемот и следете ги упатствата на екранот.

Ако имате проблем да пријавите нешто, ве молиме најавете се од компјутер и користете ги линковите за пријавата.

Пораки

3.4. Како да пријавите вознемирувачки пораки преку Месинџер?

За да пријавите порака што ве вознемирува:

1. Од која било страница на Фејсбук, кликнете на Месинџер во горниот десен агол.
2. Отворете ја пораката.
3. Ако сте ја отвориле пораката како скокачки прозорец, кликнете на  поставки. Ако сте ја отвориле пораката во Message view - приказ на пораки, кликнете на  поставки.
4. Кликнете **Something's Wrong** - Нешто не е во ред.
5. За да дадете повратни информации, кликнете на опцијата што најдобро опишува како оваа порака ве вознемирува.
6. Во зависност од вашите повратни информации, тогаш можеби ќе можете да поднесете извештај до Мета.

Ако мислите дека пораката што сте ја примиле ве вознемирува, може да пријавите.

3.4.1. Што да направам ако некој ме вознемирува со пораки на Фејсбук?

Ако некој профил ви испрати порака на Фејсбук што прави да се чувствувате непријатно, можете да:

- *Блокирате пораки од тој профил.* Овој специфичен профил нема да може да ве контактира (на пример: да ви испраќа пораки или да ви се јави) во Messenger или да ви испраќа пораки преку разговор на Фејсбук.
- *Пријавите заканувачка порака.*
- *Избриши го разговорот.* Имајте на ум дека ова нема да го избрише разговорот од списокот за разговор на другиот профил. Ако сакате да го пријавите разговорот, направете слика од екранот пред да го избришете.

- *Блокирајте го профилот на Фејсбук*

Забелешка: Можете исто така да го пријавите неговиот Фејсбук профил ако мислите дека користи лажен профил или се преправа дека сте вие или некој друг.

Можете исто така да го пријавите користејќи ја апликацијата Messenger. За да дознаете како да пријавите разговори во апликацијата Messenger, посетете го Центарот за помош на Messenger.

Дознајте повеќе за безбедносните алатки и ресурси на Фејсбук. Ако некогаш се чувствувате дека вие или некој што го познавате е во непосредна опасност, контактирајте со локалната служба за спроведување на законот.

3.4.2. Што да направам ако некој ме вознемирува, навредува, напаѓа со пораки на Фејсбук?

Ако сметате дека сте во голема опасност, контактирајте ја полицијата.

Во зависност од тоа колку е сериозна ситуацијата, можете:

- Избришете го профилот на личноста од листата на пријатели.
- Блокирајте го профилот. Ова ќе го спречи профилот да ве додаде како пријател и да ги гледа работите што ги споделувате на вашиот.
- Пријавете го лицето или сите навредливи работи што ги објавува. Фејсбук ги брише постовите ако тие ве вознемируваат и сте ги пријавиле.

3.4.3. Дополнителни совети

Најдобрата заштита од малтретирање е да научите како да го препознаете и како да го спречите. Еве неколку совети:

- **Не возвраќајте.** Повеќето насилници бараат реакција, па не им давајте таква.
- **Не го чувајте во тајност.** Посетете некој кому му верувате, како близок пријател, член на семејството, советник или учител, кој може да ви ја даде потребната помош и поддршка.
- **Документирајте и зачувајте.** Ако некој објавил нешто што не ви се допаѓа, можете да го испечатите или да направите слика од екранот во случај да треба подоцна да го споделите со некој на кој му верувате.

Посетете го **Bullying Prevention Hub** - Центарот за спречување на малтретирање на Фејсбук за повеќе информации, алатки и ресурси.

3.5. Како да постапите со пријава ако немате профил на Фејсбук?

3.5.1. Како да пријавам нешто на Фејсбук ако немам профил или не можам да го видам?

Ако сакате да пријавите нешто што се коси со Community Standards - стандардите на заедницата, но немате профил или не можете да ја видите содржината (на пример: некој ве блокирал, можеби ќе треба да побарате од пријател да ви помогне.

Побарајте пријател со профил да ја пријави содржината користејќи го линкот **Find Support or Report** - Најдете поддршка или Пријави, веднаш до објавата, фотографијата или коментарот на Фејсбук. Имајте на ум дека Фејсбук нема да може да преземе мерки за вашата пријава се додека не ја пронајдат содржината што ја пријавувате. Во вашата пријава, доставете им колку што е можно повеќе детали, вклучувајќи линкови и слики од екранот на содржината што ја пријавувате.

3.5.2. Како да пријавам Фејсбук профил или страна што се претставува дека сум јас или пак што се претставува дека е некој друг?

Профилите и страниците што имитираат други луѓе се спротивни на **Community Standards** - стандарди на заедницата и не се дозволени на Фејсбук.

Ако видите профил или страница што се преправа дека сте вие, некој што го познавате или јавна личност (на пример: славна личност, политичар), ве охрабруваме да го известите Фејсбук. Може да им пријавите лажни профили или страници дури и ако немате профил на Фејсбук.

3.5.2.1. Како да пријавите профил или страница?

Ако имате профил на Фејсбук и сакате да пријавите лажен профил или лажна страница:

1. Одете на лажниот профилот или страницата.
 - Ако не можете да го најдете, обидете се да го побарате името што се користи на профилот или страницата или прашајте ги вашите пријатели дали можат да ви испратат линк до него.
2. Кликнете  под насловната фотографија.
3. Ако пријавувате страница, изберете **Find support or report Page** - Најдете поддршка или пријавете ја страницата. Ако пријавувате профил, изберете **Find support or report profile** - Најди поддршка или пријави профил.
4. Следете ги упатствата на екранот за лажни профили или страници, за да поднесете пријава.

3.5.2.2. Како да пријавите без сметка?

Ако немате Фејсбук профил или го изгубите пристапот до вашата сметка, сè уште можете да пријавите лажна страница или профил.

- Пополнете го формуларот за контакт за да пријавите лажна страница или профил.

Report an Impostor Account

If you don't have a Facebook account and need to report someone who is pretending to be you, please fill out this form.

Which of the following best describes your situation?

☐ Someone is using my email address on their account

☐ Someone created an account for my business or organization

☐ Someone created an account pretending to be me or a friend

Send

Можете исто така да пријавите лажни профили или страници во Messenger.

3.5.2.3. Како да пријавите некој што се претставува дека сте вие или некој друг на Месинџер?

Профилите што се преправаат дека сте вие или некој друг не се дозволени во Месинџер. За да го известите Фејсбук, ако видите профил што се претставува дека сте вие, некој што го познавате или некоја јавна личност (како славна личност или политичар):

Десктоп апликација:

1. Отворете го разговорот.
2. Кликнете  на горниот десен агол.
3. Кликнете **Report** - Пријави.
4. Изберете **Pretending to Be Someone** – Се претставува дека е некој, како ваша опција.
5. Изберете како кој се преправаат дека се и кликнете **Submit Report** - Испрати извештај.

Десктоп (messenger.com):

1. Отворете го разговорот.
2. Во профилот на лицето десно, кликнете **Privacy and Support** - Приватност и поддршка.
3. Кликнете **Report** - Пријави.
4. Изберете **Pretending to Be Someone** – Се претставува дека е некој, како ваша опција.
5. Изберете како кој се претставува дека е, а потоа кликнете **Submit Report** - Испрати извештај.
6. Кликнете **Done** - Готово.

За да пријавите лажно претставување на Фејсбук, посетете го **Фејсбук Help Center** - Центарот за помош на Фејсбук.

Б. ПРЕПОЗНАВАЊЕ ЛАЖНИ ПРОФИЛИ И БЕЗБЕДНОСТ НА ИНСТАГРАМ

1. Правна рамка

Креирањето на лажни профили со користење на лични податоци од друго лице претставува кривично дело во Република Северна Македонија. Доколку постои профил на социјална мрежа кој е креиран со податоци на лице кое е македонски државјанин, истиот треба да се пријави по што министерството за внатрешни работи е задолжено за пронаоѓање на сторителот, како и за иницирање на кривична постапка против истот. Во продолжение е наведен член од Кривичниот законик на Република Северна Македонија во кој има опис на кривичното дело поврзано со заштита на податоците на корисниците на социјалните мрежи и нивната обработка и користење.

Злоупотреба на лични податоци

Член 149

(1) Тој што спротивно на условите утврдени со закон без согласност на граѓанинот прибира, обработува или користи негови лични податоци, ќе се казни со парична казна или со затвор до една година.

(2) Со казна од став 1 се казнува тој што ќе навлезе во компјутерски информатички систем на лични податоци со намера користејќи ги за себе или за друг да осгвари некаква корист или на друг да му нанесе некаква штета.

(3) Ако делото од ставовите 1 и 2 го стори службено лице во вршење на службата, ќе се казни со затвор од три месеци до три години.

(4) Обидот е казнив.

(5) Ако делото од овој член го стори правно лице, ќе се казни со парична казна.

Доколку некој корисник забележи злоупотреба на неговите лични податоци на социјалната мрежа инстаграм од профил кој не е во негова сопственост, истата треба да ја пријави кај надлежните органи на територијата на Република Северна Македонија.

2. Инстаграм – социјална мрежа

Инстаграм е сервис за социјално вмрежување за споделување фотографии и видеа во сопственост на американската компанија Мета Платформи. Апликацијата им овозможува на корисниците да поставуваат фотографии и видеа што може да се уредуваат со филтри и да се организираат со хаштагови и географски ознаки. Објавите може да се споделат јавно или со претходно одобрени следбеници. Корисниците можат да ја прелистуваат содржината на другите корисници по ознака и локација, да гледаат содржини во тренд, како фотографии и да следат други корисници за да ја додадат нивната содржина во лична храна.

Инстаграм првично се одликуваше со тоа што дозволуваше содржината да се вградува само во квадрат (1:1) сооднос од 640 пиксели за да одговара на ширината на екранот на iPhone во тоа време. Во 2015 година ова ограничување беше олеснето со зголемување на 1080 пиксели. Потоа Инстаграм додаде и функции за пораки, можност за вклучување повеќе слики или видеа во една објава и функција Stories - слична на нејзиниот главен конкурент Snapchat - која им дозволуваше на корисниците да ја објавуваат својата содржина на секвенцијален извор, со секоја објава достапна за другите за 24 часа. Од јануари 2019 година Stories дневно ги користат 500 милиони луѓе.

Секој корисник на социјалната мрежа Инстаграм споделува содржина над која има сопственички и авторски права. Инстаграм не е сопственик на текстовите, поддатоците, сликите, фотографиите, видеата, звуците, музичките дела, авторските дела, апликации или други материјали кои корисниците ги објавуваат на или преку Инстаграм сервисот. Сепак, според правилата и условите на користење, со приклучување во социјалната мрежа секој корисник му дава специјално право на Инстаграм да ја користи содржината која ја објавува за свои цели. Во продолжение ќе се објасни подетално кои податоци ги обработува Инстаграм и како може секој корисник да се заштити од злоупотреба на неговите лични податоци на оваа социјална мрежа.

Постојат основни услови за користење на социјалната мрежа кои корисниците на Инстаграм треба да ги прифатат и почитуваат. Во овие услови спаѓаат: минимална возраст од 13 години, забрани за објавување голотија, делумна голотија или сексуално сугестивни фотографии, одговорност за својата корисничка сметка и активноста поврзана со неа. Инстаграм во последните неколку години има воведено начин на родителска контрола на корисници кои не се сеуште полнолетни. Имено при креирање на профил на малолетен корисник родителот може да се наведе како надгледувач над истиот. Родителот може да ги надгледува и брише објавите на своето дете доколку за истите смета дека може да му наштетат на детето. Исто така, родителот има можност да ја ограничи содржината што ја гледа неговото дете на оваа социјална мрежа преку забрана за појавување на содржини со одредена тематика. За дополнителна безбедност имплементиран е систем кој може да го користат покрај родителот и сите корисници, а тоа е забрана за појавување на коментари кои содржат навредливи зборови и фрази. На ваков начин Инстаграм им овозможува на своите корисници да се заштитат себеси од негативното влијание, како и да размислуваат на своето ментално здравје при користење на оваа социјална мрежа. Преку персонализирање на профилот Инстаграм му овозможува на секој корисник да одлучи за начинот на користење на својот профил, како и за степенот на безбедност на истиот.

3. Политика и услови на приватност

Политиката и условите на приватност се задолжителен документ во кој се наведува на што се согласува корисникот кога се приклучува и започнува да ја користи социјалната мрежа Инстаграм во поглед на неговата приватност, безбедност и обработка на неговите лични податоци. Во склоп на политиката за приватност на социјалната мрежа Инстаграм се наоѓа објаснување за начинот на кој Инстаграм ги користи и обработува податоците добиени од корисниците. Во продолжение е прикажан извадок од истата.

Како ги користиме вашите податоци?

Ние ги користиме собраните податоци за да ви обезбедиме персонализирано искуство, вклучително и реклами, заедно со исполнување на други цели што ги објаснуваме детално подолу.

За некои од овие цели, користиме информации од сите наши продукти, како и од сите уреди од кои корисникот е вклучен. Информациите што ги користиме за овие цели автоматски се обработуваат од нашите системи. Но, во некои случаи, ние исто така користиме мануелни прегледи (reviews) за пристап и прегледување на вашите информации.

За да користиме помалку информации што се поврзани со поединечни корисници, во одредени случаи ги анонимизираме или ги генерираме информациите. Може и да го анонимизираме процесот со цел да не ве идентификува. Ние ги користиме овие информации на ист начин на кој ги користиме вашите информации, како што е опишано во овој дел.

Еве како ги користиме вашите информации:

Да ги обезбедиме, персонализираме и подобриме нашите производи

Ги користиме информациите што ги имаме, вклучително и сите што ќе одберете да ги споделите, за да ги обезбедиме и подобриме нашите производи. Ова вклучува персонализирање на функциите, содржината и препораките, како што се вашите Facebook и Instagram почетни страници со вести, приказни и реклами. Не користиме полиња на профили со информации за религиозни ставови, политички ставови или за кого сте „заинтересирани“ во процесот на персонализација.

Во наведениот извадок од политиката за приватност е прикажано како оваа социјална мрежа ги користи информациите кои секој корисник ги објавува на истата. Имено од 4 Јануари 2022 година социјалните мрежи Инстаграм и Фејсбук станаа составен дел од една компанија Meta која има универзална политика на приватност. Како дел од компанијата овие социјални мрежи меѓусебно споделуваат информации за своите корисници, како што се наведува во извадокот од политиката на приватност. Имено во скоп на извадокот овие социјални мрежи се именуваат како продукти и наведено е дека сите информации од корисниците се користат при персонализација низ сите социјални мрежи во склоп на компанијата.

Додека пак за креирање на лажни профили во склоп на нивната политика се наведува следното:

Како не смеете да го користите Инстаграм

Не можете да се претставувате како други или да давате неточни информации.

Не мора да го откривате вашиот идентитет на Instagram, но мора да ни дадете точни и ажурирани информации (вклучувајќи информации за регистрација), кои може да вклучуваат лични податоци. Исто така, не смеете да имитирате некого или нешто што не сте и не можете да креирате сметка за некој друг освен ако немате нивна изречна согласност.

Според политиката, секој корисник не смее лажно да се претставува, но истиот смее да користи псевдоними при креирање на својот профил. Сепак не се наведува која е постапката доколку се пронајде профил кој користи туѓи информации и истиот е лажен. Има начин за пријавување на лажен профил, кој потоа се евалуира од страна на посебен тим вработени во одделот на Instagram и доколку тимот одлучи дека профилот е лажен, истиот ќе биде избришан.

Една од целите кои се наведени во прирачникот за приватност на Инстаграм е креирање на побезбедна мрежа за сите. Во тој дел најголемата препорака е секој корисник да го користи системот за пријавување на несакана содржина преку кој се испраќаат пријави до самата социјална мрежа. Овие пријави се разгледуваат од тим вработени во Инстаграм кои според нивна проценка одлучуваат дали пријавената одржина треба да е избришана или не. Со ваквиот систем на пријавување се овозможува давање на глас на секој корисник и негово директно учество во креирање на побезбедна социјална мрежа.

4. Безбедност на Инстаграм

При креирање на профил на социјалната мрежа Инстаграм, корисникот треба да внимава да остане безбеден при користење на истата. Секој корисник задолжително има корисничко име и лозинка, а сите останати информации кои не се потребни или задолжителни не треба да ги споделува, бидејќи истите можат да се злоупотребат. Корисничкото име може, но и не мора да е името на корисникот, додека пак лозинката треба да е таква што корисникот може лесно да ја запомни но тешка за предвидување од страна на останатите, лозинка која корисникот не ја користи на друго место и лозинка која не е поврзана со корисничкото име или информациите кои се претставени на профилот на корисникот.

Профилот на Инстаграм поседува поставки за истиот да биде побезбеден и за што помалку лични информации на корисникот да бидат достапни за употреба. Поставките кои корисникот може да ги ажурира на својот профил се наоѓаат во делот приватност и безбедност во менито со поставки на профилот. Во ова мени може да се ажурираат следните функционалности:

- Приватност на профилот (Account privacy) – содржините кои ги споделува корисникот на својот профил може да се приватни што значи дека само неговите следбеници ќе може да ги гледаат или јавни што значи дека содржините се отворени и може сите корисници на мрежата да ги гледаат.
- Статус на активност (Activity Status) – доколку оваа поставка е овозможена следбениците на корисникот ќе може да забележат кога профилот бил најавен.
- Споделување приказна (Story sharing) – доколку оваа поставка е овозможена тогаш приказните кои корисникот ги споделува може да се споделени од други корисници.
- Коментари (Comments) – корисникот може да ги скрие коментарите што содржат некој од зборовите или фразите што ќе ги посочи од неговите објави.
- Слика од тебе (Photos of you) – корисникот може да ажурира како неговите фотографии да се додаваат на профилот.
- Два-фактор автентикација (Two-factor authentication)- доколку оваа поставка е овозможена тогаш корисникот при секоја нова најава од некој уред треба истата да ја потврди со помош на својот телефонски број.
- Споменувања (Mentions) - корисникот може да одбере кој може да го споменува во приказните или објавите, може да овозможи сите корисници, само неговите следбеници или никој.
- Содржини (Posts) – корисникот може да подеси да не е видлив бројот на допаѓања кои ги има на своите содржини, исто така може да подеси кој може да го споменува во објавите.
- Контроли за пораки (Message control) – во овој дел има поставки за тоа кој може да му праќа пораки на корисникот и дали за истите прво треба да стасува барање.
- Скриени зборови (Hidden words) -корисникот може да се заштити од вулгарни и навредувачки зборови и фрази, има поставка за криење на коментари кои содржат недолични зборови, поставка за дополнително филтрирање и додавање на фрази кои се навредувачки, како и поставка за криење на сите барања за порака.

За корисникот да биде безбеден и неговите објави за не се злоупотребуваат од други, а истовремено да не биде изложен на лоши и навредливи зборови неговиот профил треба да биде приватен. Од горенаведените поставки за приватност и безбедност овие се неопходни за корисникот да има безбеден профил на Инстаграм

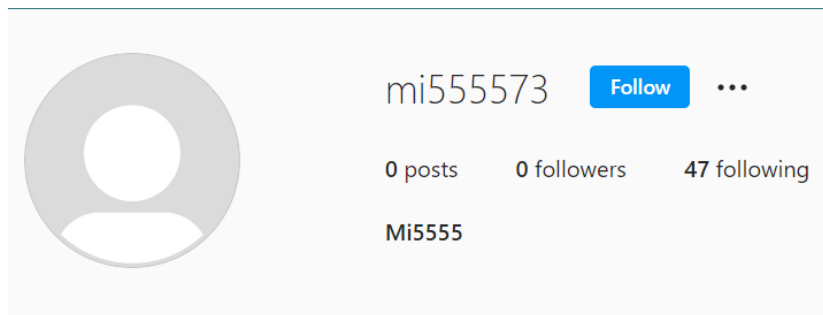
Кога профилот е приватен, содржините се видливи само за следбениците на корисникот. Корисникот притоа треба да внимава кои барања за следбеници ќе ги прифаќа, треба да се прифаќаат барања само од личности кои му се познати на корисникот. За најдобра безбедност корисникот треба да активира два - фактор автентикација, на тој начин никој друг освен корисникот нема да може да влезе во неговиот профил. Препорака е на сите подесувања каде што има опција за сите корисници, да биде избрана опцијата само следбениците на корисникот. Исто така кај подесувањата за пораки, препорачливо е да се праќа барање за порака доколку се обиде да прати порака некој кој не е следбеник на корисникот. Сите други поставки се лични преференци, но секогеш треба да се има на ум дека иако профилот е приватен, корисникот треба да размисли пред да објави било каква содржина на Инстаграм.

5. Како да препознаам лажен профил на инстаграм?

Лажните профили на социјалните мрежи најчесто може да се поделат во две групи

- лажни профили кои користат псевдоними
- лажни профили кои користат лични податоци од други луѓе

Првиот вид на лажни профили е лесно воочлив и често овие профили се користат за пишување на пораки со чие прифаќање на уредот на примачот може да се симне штетен софтвер. Во последно време на Инстаграм овие лажни профили создаваат групи во кои вклучуваат повеќе корисници и на истите им испраќаат пораки. Освен пораки со штетен софтвер, овие профили понекогаш испраќаат пораки за соработка претставувајќи се како личност која доколку направите некоја услуга на социјалната мрежа за истата ќе ви плати, пример собирање одреден број допаѓања или следбеници на некој профил. Лажните профили кои користат псевдоними може лесно да се препознаат, нивното име најчесто е непостоечко и претставува комбинација од букви, броеви и знаци. Често или немаат профилна слика или користат некоја слика од интернет на која нема лице на реален човек. Исто така овие профили најчесто немаат објавено слики на нивниот профил.



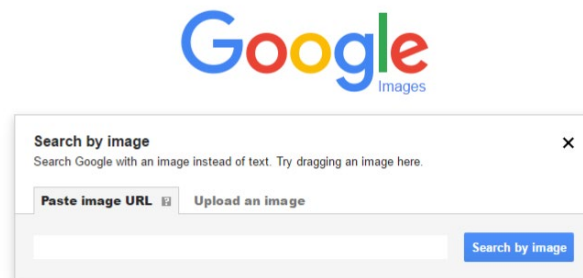
Вториот вид се лажни профили кои користат лични податоци од други лица, во информатиката ваквото претставување како друго лице и собирање на податоци од друго лице се нарекува catfishing. Овие профили се потешки за препознавање, но сепак постојат методи кои може да се искористат за да се препознае дали некој профил, кој изгледа веродостојно е лажен или не.

5.1. ПРЕБАРАЈ ЈА СЛИКАТА НА ПРОФИЛОТ

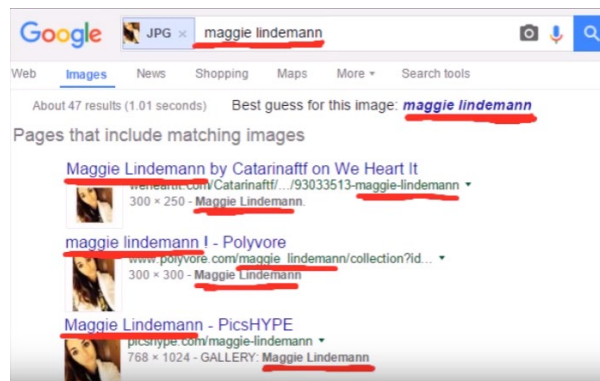
Прво нешто што сакате да го направите откако ќе пронајдете сомнителен профил е да кликнете со десното копче на сликата и да кликнете на „Копирај URL на сликата“. Потоа на вашиот пребарувач да кликнете на иконата камера која се наоѓа десно, како што е прикажано на следната слика:



Со клик на оваа икона ќе ви се отвори следниот поглед



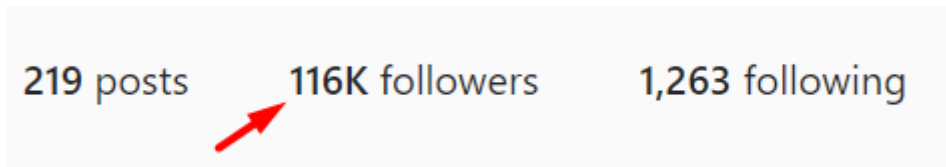
Сега во празното текстуално поле треба да го залепите линкот на сликата што претходно го копиравте и да кликнете на копчето „Пребарувај по слика“.



Пребарувачот ќе ги даде сите резултати каде е присутна оваа слика. Доколку истата ја користи лажен профил, таа ќе се појави како профилна на неколку профили, кои ќе излезат во резултатите од пребарувањето и истите ќе имаат различни лични податоци, како име и презиме на корисникот. Пребарувачот е доволно моќен и за сликата по која пребарува дава препорака за пребарување по име, кое најчесто се користи со дадената слика, препознава лик кој ја користи сликата во склоп на повеќе социјални мрежи на својот профил. На ваков начин најлесно може да се препознае дали некој профил е лажен или не.

5.2. ПОГЛЕДНЕТЕ ГИ ДРУГИТЕ СЛЕДБЕНИЦИ НА ИНСТАГРАМ ПРОФИЛОТ

Лажните профили често имаат голем број на лажни следбеници. Едноставно преку преглед на листата на следбениците на профилот може да се воочи дали истиот е лажен. Имено, овие профили често користат други апликации преку кои се генерираат лажни профили на следбеници кои користат псевдоними и немаат профилна слика. Затоа доколку се провери листата на следбеници и истата содржи голем број на вакви лажни профили, може да се заклучи дека тој профил е лажен.



5.3. ПРОЧИТАЈТЕ ГИ ОПИСОТ И КОМЕНТАРИТЕ НА СЛИКИТЕ

Доколку профилот има свои слики или има слики во кој е споменат, истите може да ги разгледате и со нивна помош да воочите дали тој профил е лажен. Сликите на профилот треба да се конзистентни, имено треба да кореспондираат со личноста која е прикажана на профилната слика. Дали описот на сликите е правилно напишан? Дали следбениците оставаат коментари со кои може да се заклучи дека лично го познаваат лицето позади профилот? Дали коментарите на сликите се од валидни профили? Ако одговорот на овие прашања е да, тогаш тоа е еден знак кој покажува дека тој профил има можност да е реален.

5.4. ПРЕБАРУВАЈТЕ ГО СОПСТВЕНИКОТ НА ПРОФИЛОТ НА ДРУГИ СОЦИЈАЛНИ МРЕЖИ

Големи се шансите дека сопственикот на профилот на Инстаграм што го истражувате има профил на социјалните мрежи на друга платформа. Постојат голем број интернет платформи, кои се дел од нечие секојдневие и за кои е потребан профил, поаѓајќи од потребата за барање работа, па се до купување производи онлјан. Од овие причини огромни се шансите личноста позади профилот на Инстаграм да поседува профил на некоја друга интернет платформа. Ако не можете да најдете профил на друга платформа, можеби е прифатливо да побарате од сопственикот на сметката врска до профилот. Ако сопственикот одбие да обезбеди врска до неговиот профил или ако профилот на друга платформа се чини дека е нелегитимен, тогаш тоа е знак дека сопственикот не го претставува тој или таа точно.

5.5. ПРЕБАРУВАЈТЕ ГО СОПСТВЕНИКОТ НА ПРОФИЛОТ НА ИНТЕРНЕТ ПРЕБАРУВАЧИ

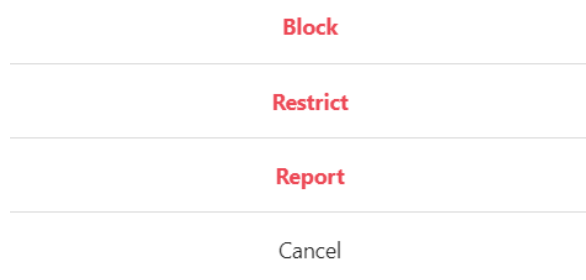
Постојат голем број интернет пребарувачи на кои може да се пребара името на профилот или неговата интернет адреса. Доколку во резултатите на некој пребарувач нема доволни информации за напишаното име, истото може да се пребара во друг интернет пребарувач. Како што беше напоменато за пребарувањето со помош на слика, истото може да се користи за пребарување и со името или некоја друга лична информација за корисникот. Од резултатите

кои ќе ги даде пребарувачот може да се воочи дали дадениот профил е лажен или не. Доколку резултатите се во голем број и постојат голем број профили со исто име, тогаш треба да се пребарува со подетални информации за корисникот.

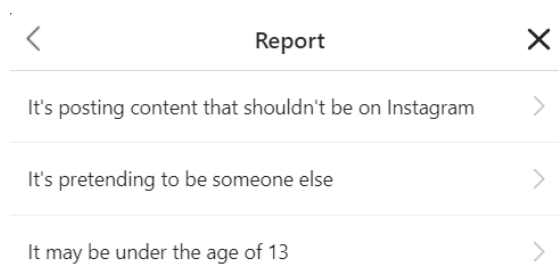
6. Начин на пријавување на Инстаграм

Во случај да откриете дека некој профил на Инстаграм е лажен, доколку објавува несоодветни содржини или личноста која го поседува има помалку од 13 години, истиот треба да го пријавите. Пријавувањето на лажен профил можете да го направите така што

1. Одете на профилот кој сакате да го пријавите
2. Кликнете на трите точки во десниот агол
3. Од наведеното мени кликнете на Report



4. Од менито изберете од која причина сакате да го пријавите профилот



Исто така Инстаграм нуди можност да се пријави и содржина. Начинот на пријавување е ист само наместо на профилот треба да одите на конкретната содржина која сакате да ја пријавите. Во моментов Инстаграм ги нуди следните можности за пријавување на содржина од следните причини:

- Спам

- Голотија или сексуална активност
- Говор на омраза или симболи
- Насилство или опасни организации
- Силеџиство или малтретирање
- Продажба на нелегални или регулирани стоки
- Нарушување на интелектуална сопственост
- Самоубиство или самоповредување
- Нарушувања во исхраната
- Измами
- Лажни информации

Како дополнителна заштита Инстаграм нуди и пријавување на коментари и пораки. Коментарите и пораките се пријавуваат на ист начин како и профилот. Во секој момент доколку сакате да пријавите нешто на Инстаграм, барајте ги трите точки до содржината која сакате да ја пријавите. Тие игледаат вака  или .

За секоја пријава Инстаграм гарантира дека е анонимна, освен ако не пријавувате повреда на лична интелектуална сопственост. Профилот кој го пријавувате или неговата содржина нема да знае кој го пријавил, дури и ако е избришан од социјалната мрежа по пријавата. Доколку сакате да пријавите злоупотреба на ваши лични податоци, освен со обична пријава, тоа може да го сторите и преку пополнување на форма која е достапна во условите за користење на Инстаграм, во која се наведуваат вашите лични податоци или документи за да се докаже дека одреден профил кој не е во ваша сопственост ги користи вашите податоци. Пријавите од секој вид пристигнуваат до вработените во Инстаграм, кои ги ревидираат и донесуваат одлука дали пријавената содржина ќе се избрише или не. Доколку некоја пријава не резултира со бришење на некоја содржина што според вас е нависитна навредлива, тогаш може да се обидете повторно со нова пријава. Најчесто добра практика е доколку и вашиот круг на пријатели го пријави истото, со што ќе бидат пратени повеќе пријави за истата содржина. Често доколку за одредена содржина се пратени повеќе пријави, истата подетално се разгледува и најчесто се брише, имајќи на ум дека истата е навредлива за поголем број корисници. Секогаш кога ќе забележите нешто несоодветно на Инстаграм, пријавете го, со цел социјалната мрежа да стане побезбедна за сите.

В. ПРЕПОЗНАВАЊЕ ЛАЖНИ ПРОФИЛИ И БЕЗБЕДНОСТ НА ТВИТЕР

1. Твитер – задржување на вниманието со лажна сметка, бот или трол

Социјалните мрежи не опкружуваат и постојано се закануваат да го запоседнат секој слободен миг. Во таа намера не се двоумат да ги искористат сите можни начини за привлекување на внимание. Се што може да задржи внимание на корисникот на социјалните мрежи е применливо и важно и се користи без разлика дали е етички, морално исправно. Целта е задржување на вниманието и за постигнување на оваа цел не се бираат средства. Лажните сметки се еден од начините да се одвлече или да се задржи вниманието! Зачинети со ботови и тролови се неверојатно моќно оружје за постигнување на целта - ВАШЕТО ВНИМАНИЕ!

Ако не сте сигурни дали да верувате или не на порака на Фејсбук или Твитер, проучете го нејзиниот извор. Следниве индикатори можат да ви помогнат да процените дали имате работа со лажна сметка, бот или трол.

Во 2014 година, „Вашингтон пост“ објави сторија со наслов „Иронично предупредување: Првиот твит од сметката на Путин му честиташе на Обама? Четири години подоцна, Business Insider објави текст за рускиот претседател Путин кој следи само 19 луѓе на Твитер, од кои еден е мртов веќе пет години. Излегува дека и двата медиума биле измамани од лажен профил на Твитер на англиски јазик кој се претставувал како рускиот претседател Владимир Путин.

Тие не беа единствените почитувани медиумски организации кои ја направија оваа грешка. Поставен во ноември 2012 година, лажниот профил собра речиси милион следбеници до ноември 2018 година, кога конечно беше суспендиран од Твитер поради имитирање на рускиот лидер. Збунувачки, официјалниот, проверен на англиски јазик Твитер на Путин има сличен број на следбеници. Сега веќе непостоечката измамничка сметка главно ги ретвитуваше официјалните изјави на Кремљ, наместо дезинформации. Ова му овозможи да остане неоткриен толку долго.

Лажните сметки од овој вид се повеќе се користат како алатки за информациска војна. За среќа, досега повеќето големи платформи за социјални медиуми се свесни за оваа закана. Не се знае точниот број на лажни сметки на Твитер. Според информации од вработени во Твитер, секоја недела платформата предизвикува меѓу 8,5 и 10 милиони ботови, со автоматско отстранување на две третини од злонамерните сметки. Фејсбук проценува дека 5% од неговите месечни корисници ширум светот се лажни. Социјалната мрежа избриша околу 1,7 милијарди лажни сметки само во вториот квартал од 2021 година.

2.Што претставува лажна сметка?

Според Фејсбук, секој ден платформата блокира милиони обиди за поставување лажни сметки. Фејсбук вели дека таквите сметки се „создадени со злонамерна намера да ги прекршат

нашите политики“. Твитер, пак, го задржува правото трајно да суспендира сметки за имитирање поединци, брендови или организации на погрешен или измамен начин. Во меѓувреме, сметките што имаат слично корисничко име или слика на профилот на другите не се во автоматско прекршување на оваа политика.

3. Како можам да забележам лажна сметка?

Оригиналните сметки на Фејсбук, Твитер и Инстаграм управувани од компании и лица од јавен интерес обично носат син симбол за потврда. Овој симбол ќе го видите на профилните страници на политичарите и познатите личности. Тоа ви помага да ги разликувате, на пример, официјалните профилни страници на основачот на Фејсбук, Марк Цукерберг и шефот на Тесла, Илон Маск, од лажни кои можеби не се лесно видливи како лажни. Неодамна, сепак, Твитер призна дека по грешка потврдил бројни неавтентични сметки.

Кога на сметките им недостасува значка за потврда, обрнете внимание на следните индикатори:

3.1. Имиња на сметки и адреси на профили

Честопати, измамниците ретроактивно ги менуваат своите кориснички имиња на Твитер или Фејсбук откако ќе се регистрираат на платформата. Во овој случај, оригиналното име на сметката на Твитер - на кое му претходи симболот @ - ќе даде инфо дека нешто може да не е во ред. Слично на тоа, различното URL на Фејсбук треба да ве направи сомнителни. Земете ја, на пример, сметка на Фејсбук наводно во сопственост на Илон Маск регистриран на погрешно напишаното корисничко име „Musk“ и „facebook.com/elonreeve.musk.338“. Многу е малку веројатно дека ова е вистинската Фејсбук страница на Илон Маск. Покрај тоа, организациите и лицата од јавен интерес обично ќе се поврзат со нивните вистински сметки на социјалните медиуми.

Ако сакате да ја потврдите автентичноста на сметката регистрирана на лице кое не е во очите на јавноста, користете пребарувачи за да проверите дали споменатата личност е присутна на други социјални мрежи со истото име. Проверете дали користените профилни слики се слични. Исто така, проверете дали се совпаѓаат биографиите на профилот, деталите за контакт и локација. И проверете дали сметките споделуваат слична содржина. Ако можете да откриете голем степен на преклопување, тогаш најверојатно имате работа со вистинска сметка од вистинска личност. На крајот на краиштата, многу е малку веројатно дека лажните сметки со идентично именувани профили и речиси идентична содржина се оперираат на различни социјални мрежи. Имајте на ум дека ова се индикации, а не цврсти докази, за да се процени дали сметката е автентична или не.

3.2. Слики на профилот

Можете исто така да ги проучувате профилните слики за совети (за да дознаете повеќе за

забележување манипулирани слики, видете го објаснувачот во оваа серија), под услов да е достапен. Користете го методот за пребарување на обратна слика (услуга понудена од Google, Bing и Yandex) за да дознаете дали сликата што се користи во профилот прикажува некој друг од она што е тврдено или дали сликата се појавила на друго место на интернет. Сликите со ниска резолуција може да бидат и црвено знаме: многу е малку веројатно дека лицата од јавен интерес ќе користат зрнести слики за нивните официјални профили на социјалните мрежи.

3.3. Следбеници, пријатели, претплатници

Дали е веројатно поранешната германска канцеларка Ангела Меркел има помалку од 4.000 следбеници на Твитер? И колку е веродостојно за војвотката од Кембриџ, Кејт Мидлтон, да има само 52 пријатели на Фејсбук? Ниту една сметка не изгледа особено автентична. Но, фалсификатите не се секогаш толку лесно да се забележат - потсети се на лажната сметка на Елон Маск со над 60.000 следбеници споменати погоре.

За да проверите дали ова може да биде вистинска сметка, вчитајте ја проверената сметка на Маск на Твитер и споредете ја со конкретната сметка на Фејсбук. Додека Маск има над 61 милион следбеници на Твитер, сомнителната сметка на Фејсбук има само 60.000 - така што нешто тука мора да „не штима“. Секогаш треба да бидете сомнителни кога ќе забележите видливо големо несовпаѓање во врска со следбениците, пријателите или претплатниците на некоја личност на различни платформи на социјалните медиуми. „Следбеник“ е корисна алатка за анализа на бројките на следбениците на различни мрежи.

Друг начин да се процени автентичноста на сметката што наводно ја води позната личност е да проверите дали проверените сметки имаат интеракција со неа. Дали соиграчите од истиот спортски клуб, на пример, коментираат за фотографии споделени од сомнителен профил? Или, дали колегите, потврдени сметки, повторно објавуваат содржина споделена од дотичната сметка?

3.4. Содржина и онлајн однесување

Обрнете внимание на тоа кога е креиран профил на социјалните мрежи. Ако беше поставен и беше активен со години, можеше да биде реално. Сепак, ова не е сигурен начин да се измери автентичноста. На крајот на краиштата, лажната сметка на Путин за која се дискутираше погоре, беше активна цели шест години. Проучете го и видот на содржина објавена од сметката. Дали се совпаѓа со личноста, или се чини дека не е карактер? Ако некој постојано ја менува својата или нејзината локација, тоа треба да ги зголеми сомнежите - освен ако поединецот работи како блогер за патувања, воен дописник или во слично својство. Бидете внимателни кога луѓето споделуваат содржина со која се чини дека имаат мала или никаква врска. Германски студент објавува слики на кои наводно е прикажана авганистанска воена зона? Руска пензионерка споделува фотографии од, како што тврди, париските протести против вакцинацијата? Ниту еден случај не изгледа особено веродостоен. И двете би можеле да бидат лажни сметки или барем да споделуваат непроверени дезинформации. Ваквото сомнително однесување е типично и за ботови.

4.Што се ботови?

Ботови, скратено од роботи, неуморно коментираат на објави на Фејсбук, споделуваат содржина или вештачки поттикнуваат онлајн дебата за маргинални или на друг начин занемарени теми. Нивното однесување, како што сугерираше името, наликува на тоа на автоматизирани работи. Меѓутоа, од суштинско значење е да се направи разлика помеѓу добри и лоши ботови. Добрите ботови може автоматски да споделуваат вести или временски прогнози, како и предупредувања за земјотрес или сателитски слики на социјалните мрежи. Спротивно на тоа, лошите ботови се дизајнирани да имитираат вистинска човечка активност за унапредување на одредена агенда. Во зависност од алгоритмот, таквите компјутерски програми може да составуваат и објавуваат објави или коментари на социјалните мрежи, да следат други, па дури и да испраќаат барања за пријателство. Лошите ботови можат да ја искриват реалноста со засилување на одредени политички мислења на платформите на социјалните медиуми и да привлечат вештачко внимание на одредени прашања со постојано споделување невинности или дезинформации и поткопување на конструктивна онлајн дебата. Неодамна, истражувачите од Универзитетот Карнеги Мелон анализираа над 200 милиони твитови испратени во 2020 година во кои разговараа за коронавирус или COVID-19. Тие дојдоа до загрижувачки заклучок : 82% од првите 50 влијателни ретвитари беа ботови; исто така 62% од првите 1.000 ретвитувања.

4.1.Како можам да забележам ботови?

Ботови, како лажни сметки на социјалните мрежи, може да се откријат ако обрнете внимание на:

- Имиња на сметки Корисничките имиња што се состојат од измешани комбинации на букви и зборови може да укажат дека имате работа со бот.
- Слика на профилот Дали на сметката и недостасува профилна слика? Дали покажува некого, но со многу лош квалитет? Ако е така, бидете внимателни.
- Детали за био/сметка на профилот Ретките информации за профилот, неодамнешниот датум на регистрација и сомнителната локација што не се совпаѓа со личноста за која станува збор треба да ве засвонат.
- Однесување на Интернет што се чини дека не е карактеристично за човекот Дали сте забележале една сметка на социјалните мрежи истовремено објавувајќи идентична содржина на различни платформи или под неколку различни објави? Дали сметката објавува безброј груби одговори за многу кратко време или постојано ретвитува содржина? Ако одговорот е да, најверојатно имате работа со бот. Познато е дека ботови обично следат голем број други сметки, додека имаат малку или нема свои следбеници. За да ги проверите броевите на следбениците, размислете да користите алатки како Followerwonk или Botometer

5.Што се тролови?

Троловите се вистински човечки суштества кои покажуваат деструктивно и хиперактивно онлајн однесување, слично како ботови. Тие често се платени да малтретираат одредени јавни личности или медиумски организации. Фејсбук ја опишува таквата насочена акција како

„координирано неавтентично однесување во име на странски или владин актер.“ Такви кампањи може да водат дури и таканаречени фабрики за тролови (за да дознаете повеќе за троловите и нивната улога како агенти на државната пропаганда, видете ја следната статија од оваа серија). Еден од најистакнатите примери на фабрика за тролови е Агенцијата за истражување на Интернет, во Санкт Петербург, Русија. EUvsDisinfo, проект на Европската служба за надворешна акција за спротивставување на дезинформациите, откри дека агенцијата ширела невистини и про-Кремљ пораки на повеќе јазици за време на различни европски и американски изборни кампањи, како и пред неколку референдуми. Агенцијата се здоби со глобална слава кога американските разузнавачки служби објавија извештај во јануари 2017 година во кој се анализираше како работела на манипулирање на американското јавно мислење пред претседателските избори во САД во 2016 година. Оттогаш, Фејсбук напорно ги брише сметките поврзани со агенцијата. Се вели дека фабриките за тролови и таканаречените армии на тролови работат надвор од Индија, Кина, Саудиска Арабија и Мексико. Навистина, во 2020 година, Вашингтон пост откри дека тинејџерите поддржувачи на поранешниот американски претседател Доналд Трамп биле платени да шират дезинформации на социјалните мрежи.

5.1. Како да забележам тролови?

Сметките на трол е потешко да се откријат отколку искрените лажни сметки, бидејќи тие обично се контролирани од вистински човечки суштества. Забележувањето на сметките на трол станува уште поголем предизвик кога тие се поставуваат и одржуваат со години како дел од пошироките трол мрежи. Затоа, не можете лесно да ги идентификувате по нивните сомнителни имиња на профили, неодамнешни датуми на регистрација или сомнителни броеви на следбеници. И покрај тоа, проверете дали има такви потенцијални индикации.

Дополнително, внимателно проучете ја содржината што ја споделува предметната сметка. Дали содржи линкови до веб-локации познати по објавување дезинформации? (За повеќе за откривање дезинформации, видете ја првата статија од оваа серија.) Обрнете внимание на тоа дали корисникот објавува и лични објави заедно со споделување друга содржина. Ако сметката повторно објавува содржини од трета страна, ова може да укаже дека имате работа со трол. Бидете особено сомнителни ако оваа споделена содржина содржи дезинформации.

Проверете дали имате заеднички пријател на одредена социјална мрежа. Потоа контактирајте со оваа личност и распрашајте се за сомнителната сметка. Обрнете внимание и на тоа колку време потенцијалниот трол троши на социјалните мрежи. Дали лицето посветува часови за да коментира одредени онлајн дискусии? Дали поединецот ја објавува истата порака под различни објави на социјалните мрежи или објавува и споделува содржина брзо последователно? Овие би можеле да бидат индикации кои покажуваат дека имате работа со личност чија активност на Facebook, Twitter, Instagram или YouTube е работа, а не хоби.

Еден од најголемите знаци на трол активност е кога личноста за која станува збор не успева да придонесе ништо конструктивно во онлајн дебатата. Ако лицето се фокусира исклучиво на манипулирање со другите и предизвикување негативни емоции, прекинете ја секоја понатамошна дискусија и означете ја сметката на платформата за проверка!

6. Како да блокирате и одблокирате неког на Твитер?

Иако Твитер е одлично место за споделување мислења и за дознавање новости, за време на дискусијата може најдете на некој со кого не сакате да разговарате. Научете како да блокирате корисник на Твитер да ви испраќа пораки, да ги следи вашите активности и да ги гледа вашите твитови. Еве како да го направите блокирањето и деблокирањето чекор по чекор.

6.1. Како да блокирате или одблокирате неког користејќи го неговиот Твитер профил

- Најавете се на Твитер.
- Отворете ја страницата на корисникот што сакате да го блокирате. Ќе го најдете или со впишување на нивното име во пребарувачот или со кликување на фотографијата на нивниот профил во вестите.
- До копчето Следи на десната страна ќе најдете три вертикално подредени точки. Кликнете на нив.
- Во паѓачкото мени ќе најдете Блокирај @[корисничко име]. Кликнете таму.
- Ќе се појави опаѓачко мени со прашањето дали навистина сакате да го блокирате тој корисник. Кликнете на Блокирај.
- Кога сакате да го одблокирате, држете го курсорот на компјутерскиот глушец над Блокиран и кликнете на Одблокирај.

6.2. Како да одблокирате неког на Твитер користејќи компјутер

- Најавете се на Твитер на вашиот компјутер.
- Допрете ја сликичката на вашата фотографија во горниот десен агол и скролувајте до Поставки и приватност – Settings and privacy.
- Во менито лево, кликнете на Блокирани сметки – Blocked accounts.
- Под Сметки - Accounts што сте ги блокирале, ќе се појави список на корисници што сте ги блокирале. За да го одблокирате, поставете го курсорот на компјутерскиот глушец на Блокиран - Blocked.

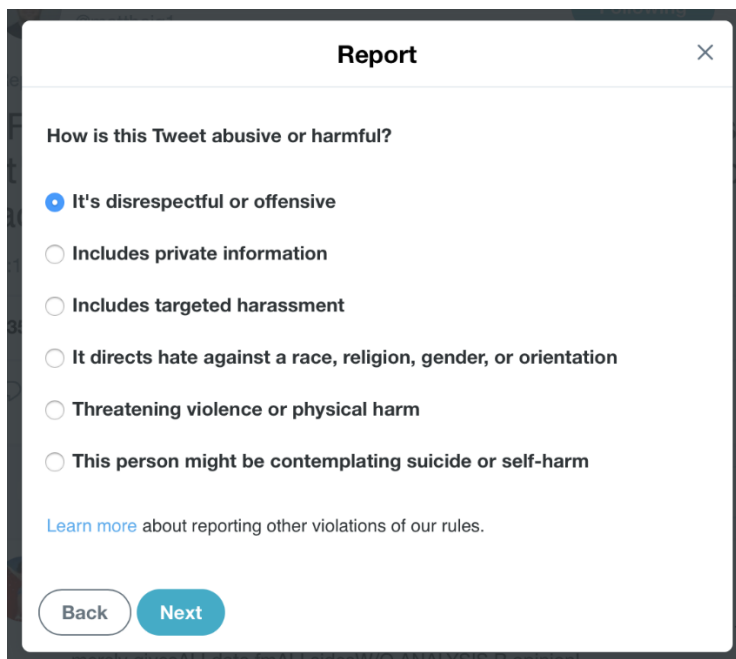
6.3. Како да одблокирате неког на Твитер користејќи ја мобилната апликација

- Отворете го Твитер.
- Повлечете го екранот надесно за да пристапите до менито.
- Во менито лево, допрете Поставки и приватност – Settings and privacy.
- Допрете на Приватност и безбедност – Settings and safety.
- Скролувајте до подменито Безбедност- Safety, пронајдете и допрете Блокирани сметки – Blocked accounts.
- Допрете Блокирано – Blocked и пронајдете го корисникот што сакате да го одблокирате.

7. Како да пријавите несоодветен твит или директна порака

Твитер сигурно ќе се бори со несоодветни сметки или објави уште некое време, а во меѓувреме, она што можете да направите е да ја блокирате и пријавите секоја сомнителна активност што ќе ја забележите на интернет. Тоа може да го направите со следните чекори:

- Одете до твитот што сакате да го пријавите.
- Допрете ја иконата што се наоѓа на врвот на твитот.
- Изберете Пријави твит – Report tweet.
- Ако изберете Тоа е навредливо или штетно – It's abusive or harmful, од вас ќе се побара да обезбедите дополнителни информации за проблемот што го пријавувате.

The image shows a 'Report' dialog box from Twitter. At the top, it says 'Report' with a close button (X) on the right. Below this, the question 'How is this Tweet abusive or harmful?' is displayed. There are six radio button options: 'It's disrespectful or offensive' (which is selected), 'Includes private information', 'Includes targeted harassment', 'It directs hate against a race, religion, gender, or orientation', 'Threatening violence or physical harm', and 'This person might be contemplating suicide or self-harm'. Below the options is a link that says 'Learn more about reporting other violations of our rules.' At the bottom, there are two buttons: 'Back' and 'Next'.

Кога ќе пријавите некој профил на Твитер, Твитер ја анализира жалбата и испраќа е-пошта до вас и до пријавениот профил за дополнително да го истражи случајот. Откако ќе имаат доволно информации и ќе го најдат точни тврдењето, тие или ќе побараат од профилот на Твитер да ја отстрани содржината или ќе го суспендираат нивниот профил.

Проектот е финансиран од Федералното министерство за социјални работи, здравство, грижа и заштита на потрошувачите на Република Австрија

Новинари за човекови права

www.jhrmk.org

Венијамин Мачуковски 2А/3-16, 1000 Скопје,
Република Северна Македонија

 **Federal Ministry**
Republic of Austria
Social Affairs, Health, Care
and Consumer Protection

