MKSafeNet

Безбедност на интернетот

Разбирање на ризиците, учење безбедни практики и стануване одговорни дигитални граѓани

Зошто е важна безбедноста на Интернет?

Интернетот е моќна алатка, но доаѓа со ризици. Ајде да истражиме како да останеме безбедни.

Што ќе покриеме

- Ризици на интернетот
- Безбедни однесувања онлајн
- Сајбер-насилство и како да се справиме
- Зачувување на личните информации
- Поставување онлајн граници

Тинејџерите поминуваат во просек **7+ часа дневно** на интернет. Како да останеме безбедни во овој дигитален пејзаж?

Кои се опасностите?

- **Сајбер-насилство**
- **Фишинг измами**
- **Несоодветна содржина**
- **Онлајн предатори**

Што е сајбер-малтретирање?

Користење на технологија за вознемирување, заканување или засрамување некого. Тоа може да се случи на социјалните медиуми, платформите за игри или преку апликации за пораки.

Знаци на сајбер малтретирање

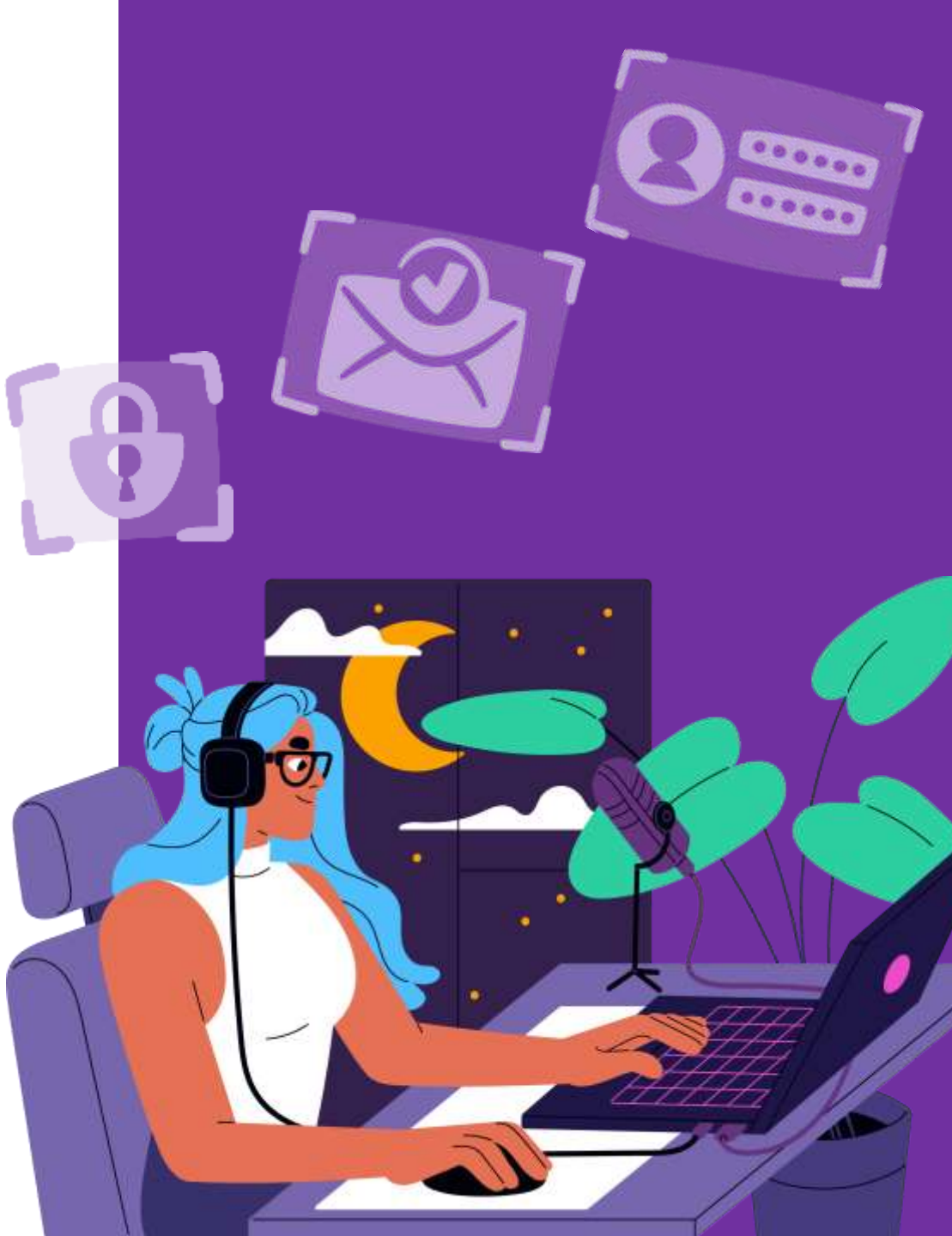
- Постојани навредливи пораки
- Ширење лажни информации
- Исклучувајќи ги другите онлајн
- Повлекување од семејството и пријателите
- Избегнување на училиште, клубови, спортови или активности

MKSafeNet

Како да се заштитиме?

Чекори на преземање

- **Не одговарајте и не возвраќајте**
- **Зачувајте докази (скриншотови)**
- **Блокирајте/пријавете го лицето**
- **Разговарајте со возрасно лице на кое му верувате**



MKSafeNet

Што се фишинг измами?

Фишинг е кога измамниците ве намамуваат да дадете свои лични информации, како лозинки или банкарски податоци.

Како да забележите измама?

Прво, важно е да барате сомнителни линкови. Потоа, треба да проверите дали има граматички грешки. И на крај, треба да бидете сигурни дека нема да споделувате лични информации без да го потврдите изворот.

Лажни едукативни платформи

Лажните едукативни платформи се една од најчестите онлајн измами насочени кон ученици, наставници и родители. Овие измами обично се дизајнирани така што имитираат вистински образовни платформи како **Google Classroom, Microsoft Teams, Moodle или Zoom** и имаат за цел да ги украдат корисничките податоци или финансиски информации.

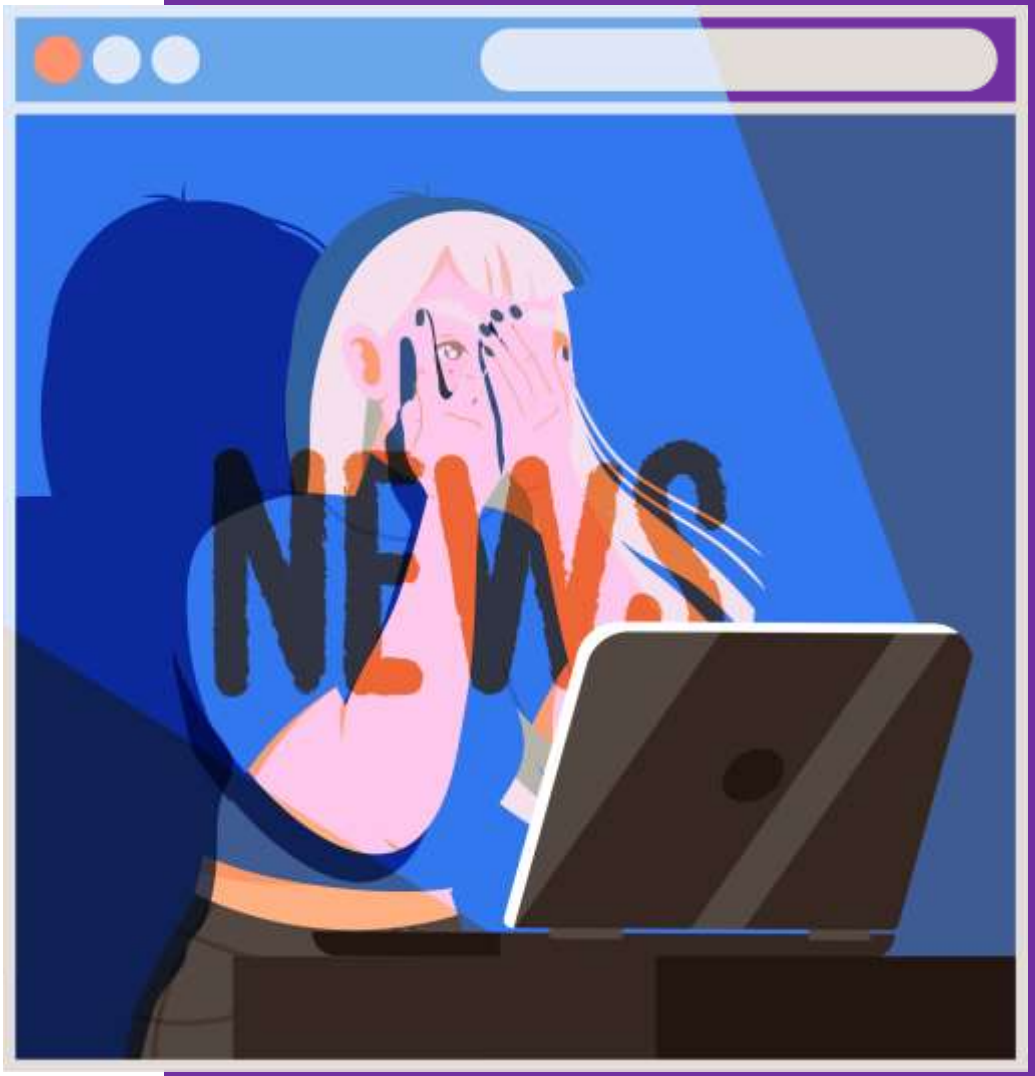
Измамниците може да испратат малициозен софтвер преку платформата, кој може да ги зарази уредите на корисниците и да предизвика сериозни безбедносни проблеми. Како резултат на тоа, учениците може да загубат пристап до своите акаунти, што може да доведе до злоупотреба на нивните лични податоци. Дополнително, наставниците може да бидат измамени да споделат доверливи информации, што може да загрози и други ученици, училишни системи или административни податоци.

Како да се заштитите од интернет измами?

- Никогаш не споделувајте лични информации преку е-пошта, телефон или пораки со непознати лица.
- Проверувајте дали веб-страницата има „https“ во URL-то и безбедносен сертификат пред да правите онлајн плаќања.
- Користете силни лозинки и двофакторска автентикација каде што е можно.
- Не кликнувајте на сомнителни линкови или прилози во е-пошта.
- Информирајте се за најновите измами и користете софтвер за антивирусна заштита.
- Ако станете жртва на измама, веднаш пријавете ја ситуацијата кај надлежните органи или платформата каде што се случила измамата.

Справување со несоодветна содржина

Ако видите нешто вознемирувачко или несоодветно, главната работа што мора да ја направите е да не се занимавате со тоа. Пријавувањето на платформата помага да се отстранат содржините од тој тип.



MKSafeNet

Приватност онлајн

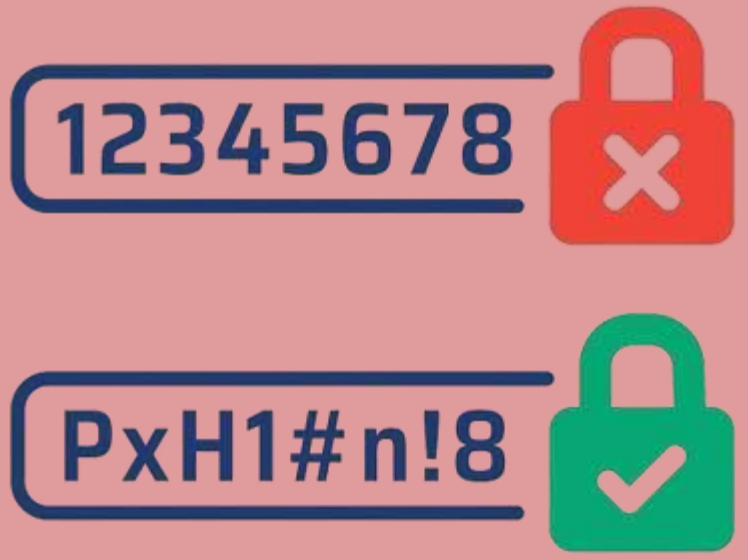
MKSafeNet

Зошто е важна приватноста?

Вашите лични податоци се вредни. Нивната заштита ве штити од кражба на идентитет и онлајн предатори.

Креирање безбедни лозинки

- **Користете мешавина од букви, бројки и симболи**
- **Избегнувајте користење на лични податоци**
- **Редовно менувајте ги лозинките**
- **Не ги споделувајте лозинките со други**



Ризици од прекумерно споделување

Објавувањето премногу информации може да ве направи ранливи на измами или предатори. Чувајте ги деталите за вашиот живот приватно.

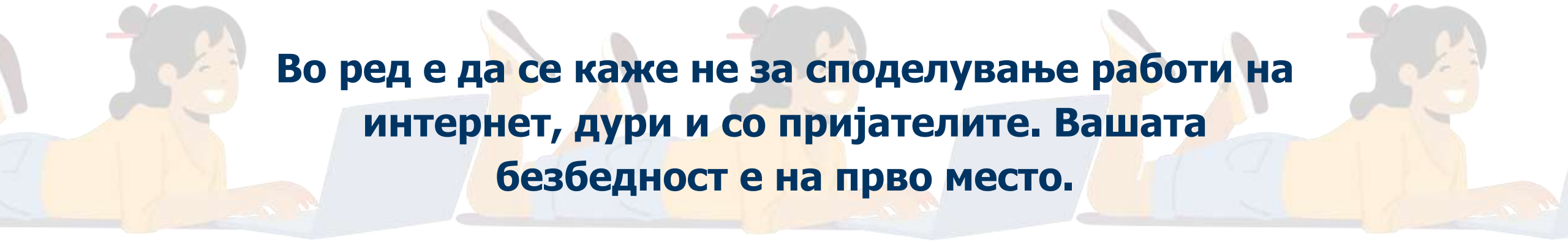
Останување безбедни на социјалните медиуми

- **Поставете ги вашите профили приватни**
- **Бидете внимателни кој прифаќате како пријател или следбеник**
- **Размислете пред нешто да објавите**
- **Дознајте како да пријавите, блокирате и филтрирате содржина**

MKSafeNet

Онлајн граници

Поставување граници



Во ред е да се каже не за споделување работи на интернет, дури и со пријателите. Вашата безбедност е на прво место.

Безбедност при ‘гејминг’ - Паметно играње

- **Не споделувајте лични информации со други играчи**
- **Пријавете ги навредливите играчи**
- **Внимавајте на купувањата во играта**
- **Користете VPN кога играте онлајн**

Што е ’grooming’?

’Grooming’ е кога некој гради доверба за да ве искористува или да ви наштети. Научете да препознавате сомнителни однесувања.

Свесност за време пред екранот

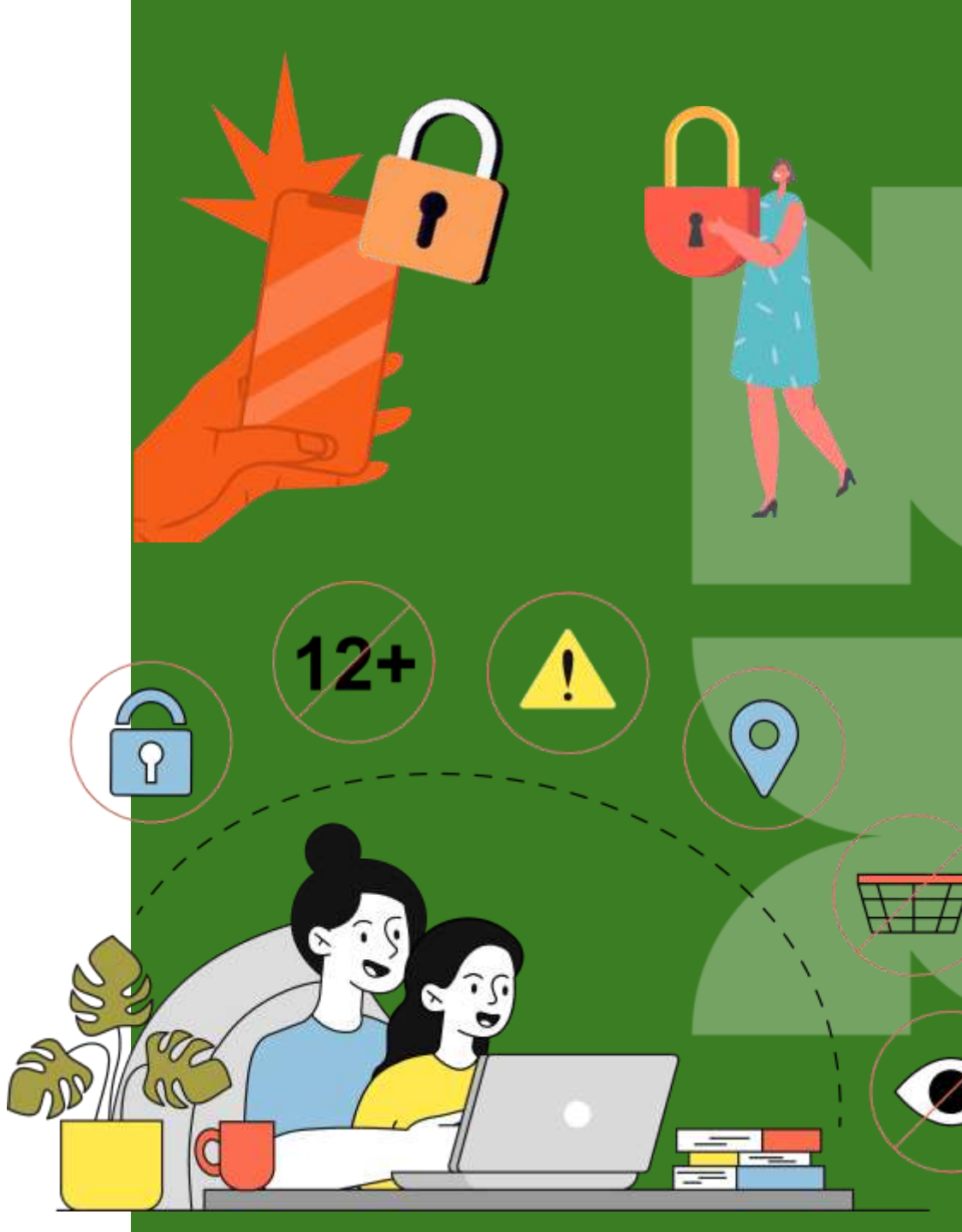
Балансот е клучен. Премногу време поминато пред екранот може да влијае на вашето ментално и физичко здравје.

MKSafeNet

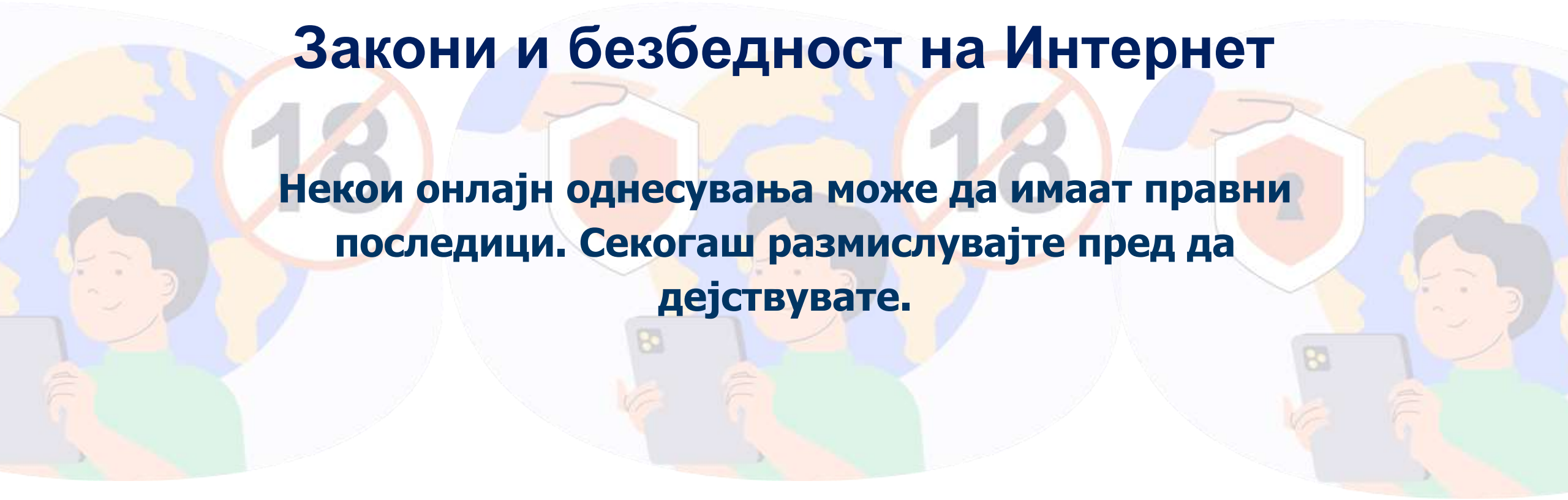
Основи на сајбер безбедноста

Заштита на вашите уреди

- **Користете антивирусен софтвер**
- **Избегнувајте јавен Wi-Fi без VPN.**
- **Одржувајте го софтверот ажуриран**
- **Исчистете го кешот и историјата на прелистување**



Закони и безбедност на Интернет



Некои онлајн однесувања може да имаат правни последици. Секогаш размислувајте пред да дејствувате.

Улогата на родителите и старателите

Родителите и старателите може да помогнат децата да останат безбедни на интернет. Тие треба да ја контролираат и да бидат во тек со нивната онлајн активност.

MKSafeNet

MKSafeNet
2025

Дигитален отпечаток и социјални мрежи

Што е дигиталниот отпечаток?

Дигиталниот отпечаток ги вклучува сите информации што ги оставаме зад себе на интернет, како објави, слики и коментари. Треба да се внимава какви содржини се споделуваат, бидејќи тие може да влијаат на професионалниот углед.

Редовно пребарување на своето име на интернет е добра практика за да се уверите дека дигиталниот отпечаток е во согласност со професионалните стандарди.

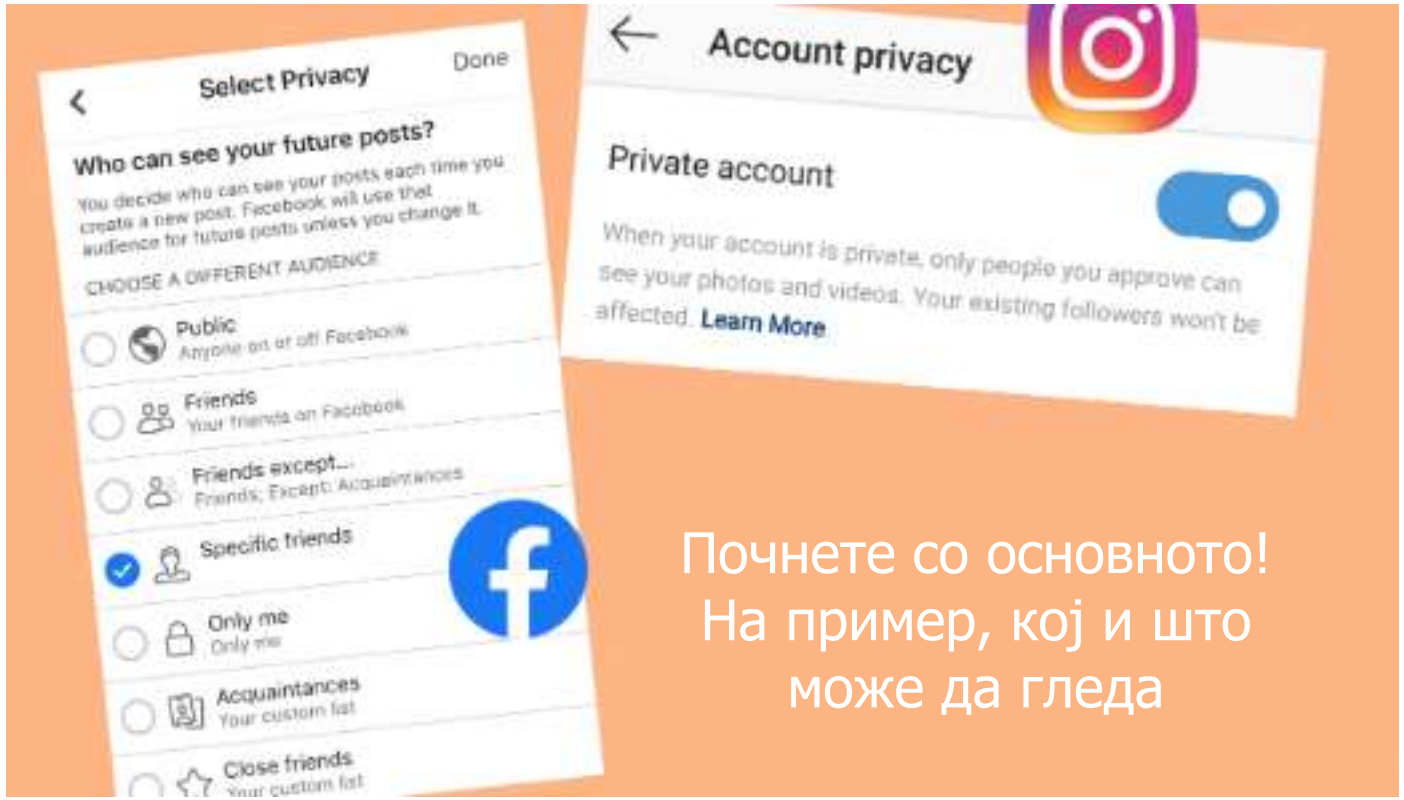
Приватност на профили на социјални мрежи

Наставниците треба да ги постават своите профили на социјалните мрежи како приватни за да ги заштитат личните информации. Користете поставки за ограничување на пристапот само на пријатели или блиски контакти. Избегнувајте додавање ученици на лични профили и создадете професионални страници доколку треба да споделувате образовни содржини. Ова ќе ви помогне да ги одделите личниот живот и професионалната кариера.

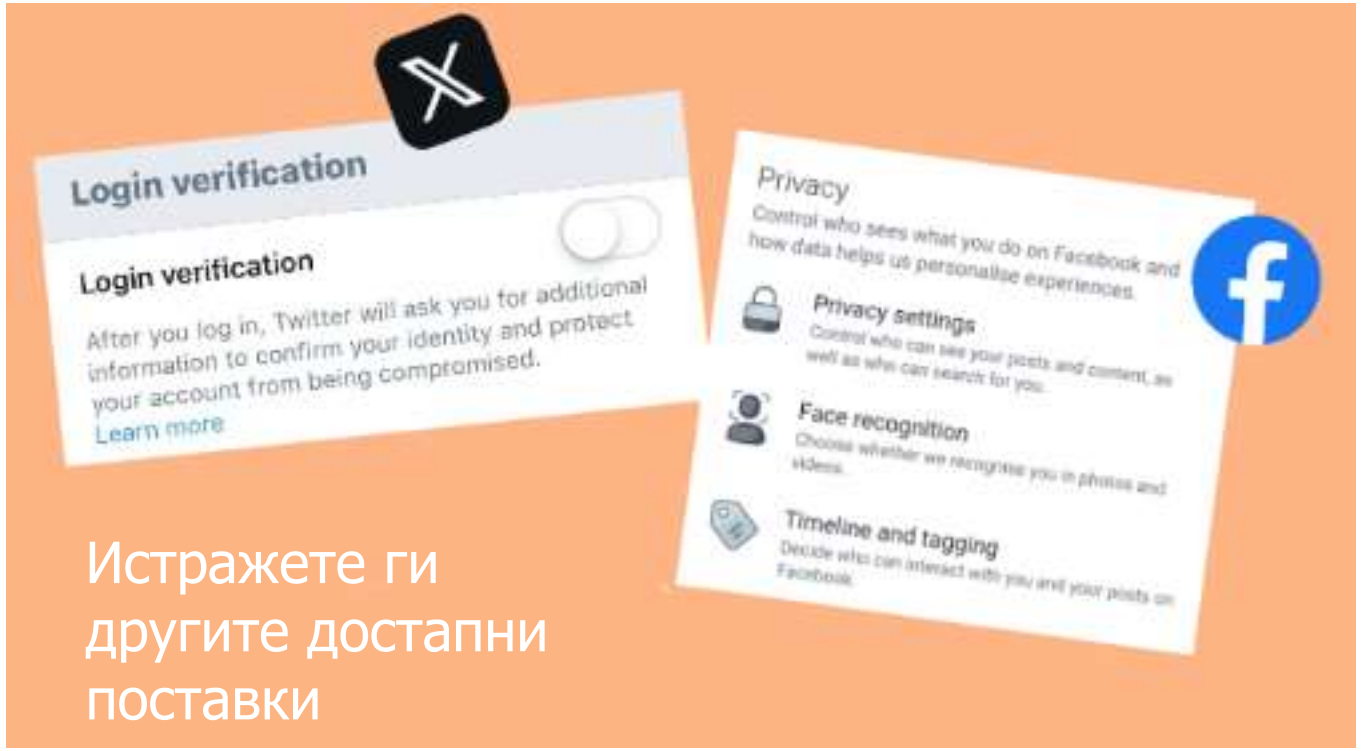
Менаџирање на поставки за приватност

Барај ги следниве симболи

Менаџирање на поставки за приватност



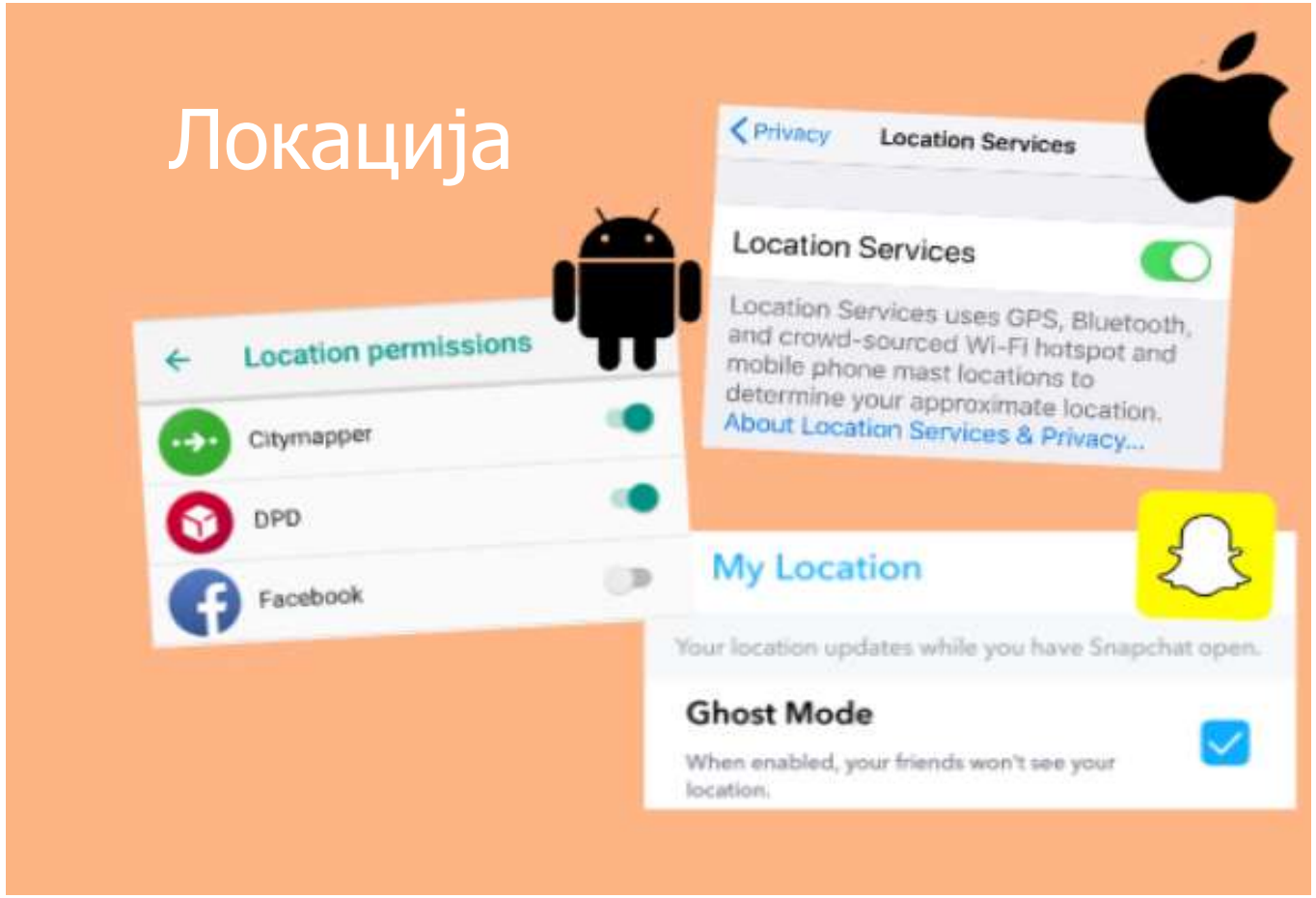
Менаџирање на поставки за приватност



Истражете ги другите достапни поставки

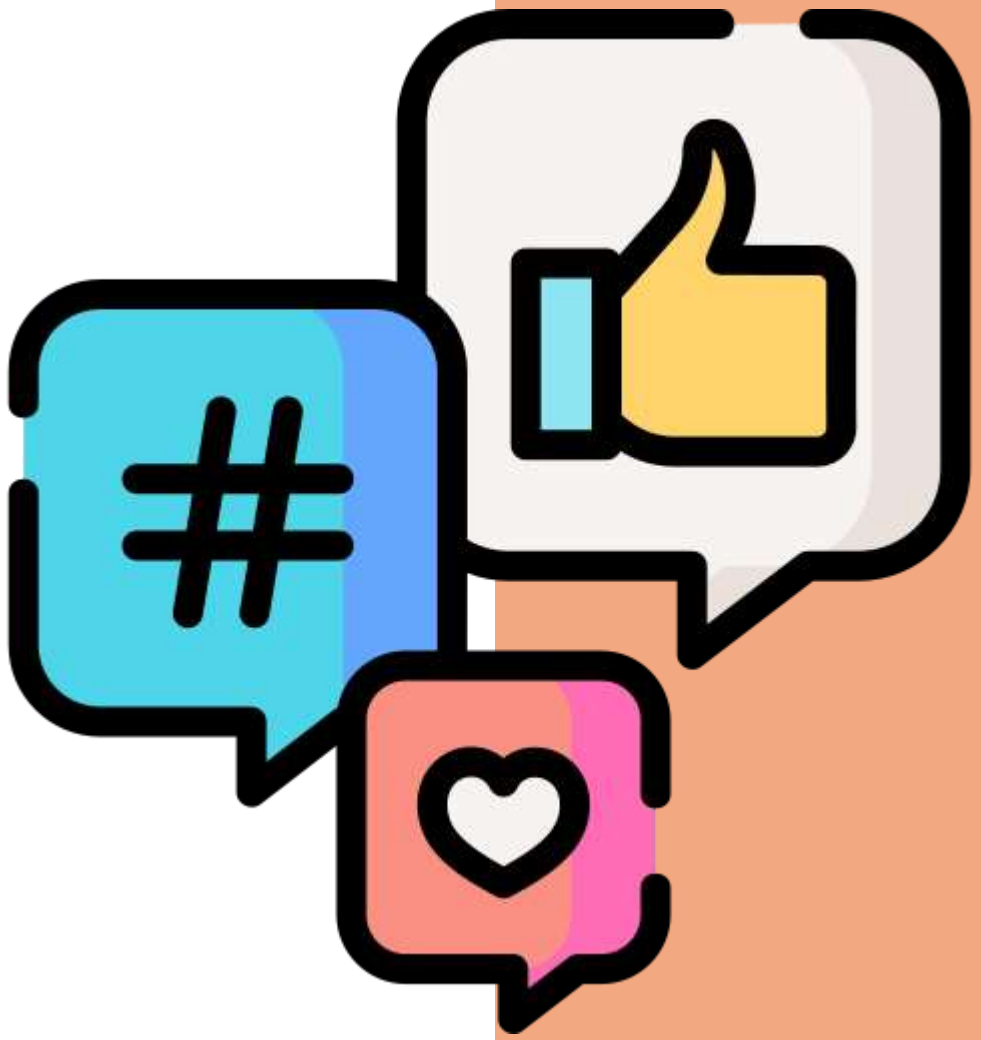
MKSafeNet

Менаџирање на поставки за приватност



Комуникација со ученици преку социјални мрежи – дозволено или не?

Комуникацијата со ученици преку социјални мрежи треба да биде строго регулирана или целосно избегнувана. Ако е дозволено, користете професионални и етички стандарди, како и платформи создадени за образовна комуникација. Не користете лични профили за споделување информации или наставни материјали. Подобро е да користите официјални училишни платформи кои нудат поголема заштита и транспарентност.



MKSafeNet

MKSafeNet
2025

Заштита на чувствителни податоци

Зачувување и споделување на ученички податоци

Ученичките податоци треба да се чуваат на безбедни места, како што се заштитени сервери или локални уреди. При споделување, користете заштитени платформи и осигурете се дека само овластени лица имаат пристап. Избегнувајте праќање чувствителни податоци преку несигурни канали, како јавни е-пошти или неавтентицирани апликации.

Користење сигурни платформи за комуникација (Google Classroom, Microsoft Teams...)

Сигурните платформи за комуникација овозможуваат безбедно споделување на информации и работа со ученици. Избегнувајте употреба на непроверени апликации кои немаат соодветна заштита или приватност.

Наставниците треба да ги конфигурираат платформите со силни лозинки и опции за контрола на пристапот.

Редовно проверувајте ги поставките за приватност и ажурирајте ги апликациите за да останат сигурни.

Шифрирање на документи и датотеки

Шифрирањето на документите овозможува заштита на информациите дури и ако документите се украдени или несакано споделени. Користете алатки за шифрирање при праќање чувствителни датотеки преку интернет. Осигурете се дека само оние кои го имаат шифрирачкиот клуч можат да ги отворат датотеките. Овој пристап додава дополнителен слој безбедност и е клучен за заштита на доверливи информации.

Справување со загуба или кражба на податоци

Заштитата од загуба или кражба на податоци е клучна во дигиталното образование. Редовното правење резервни копии на чувствителни информации и нивното чување на безбедни платформи помага во спречување на загуби. При сомнителна активност, ИТ службите треба веднаш да бидат известени. Наставниците и учениците треба да користат сигурни уреди, да избегнуваат јавни Wi-Fi мрежи и секогаш да се одјавуваат по користење на училишните платформи. Ажурираниот антивирусен софтвер и добрите безбедносни поставки дополнително ја зголемуваат заштитата.

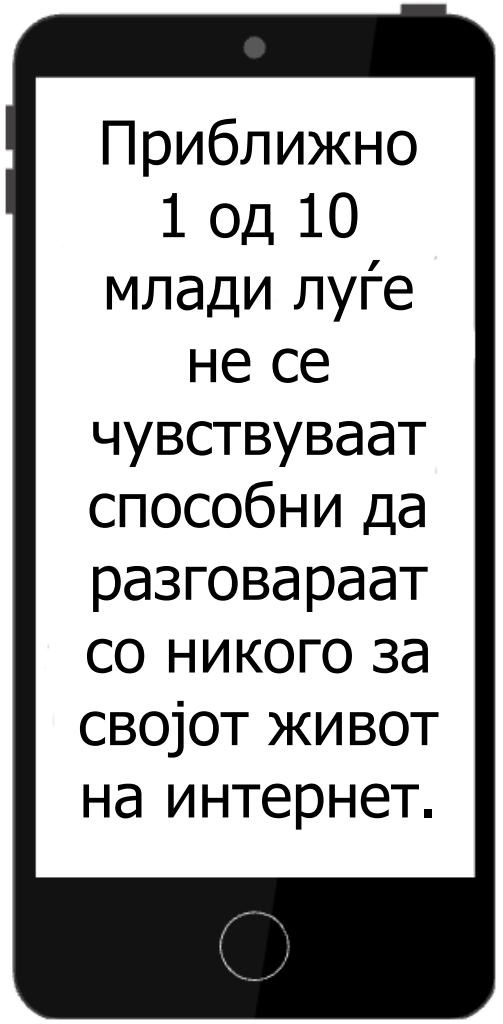
MKSafeNet

MKSafeNet
2025

Зајакнување на дигиталната безбедност

Зошто е вака?

- загрижени се дека ќе западнат во неволја на училиште или дома
- засрамени се
- немаат зборови или средства за објаснување
- не се сигурени што ќе се случи ако му кажат на возрасен
- загрижени се да не ги наречат „кодош“
- не може да видат како возрасен може да им помогне
- не ги препознаваат проблематичните онлајн ситуации



Безбедноста на интернет е битно прашање

Секое обелоденување или инцидент во врска со безбедноста на интернет треба да доведе до користење на вообичаените процедури за заштита.

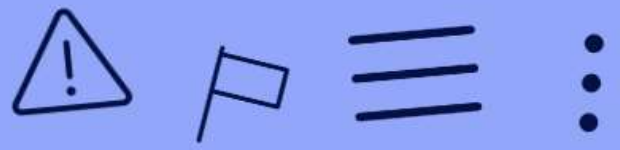
Секој инцидент каде што детето е изложено на ризик од непосредна повреда или каков било инцидент што вклучува несоодветни слики треба итно да се пренасочи до надлежните заштитни органи.

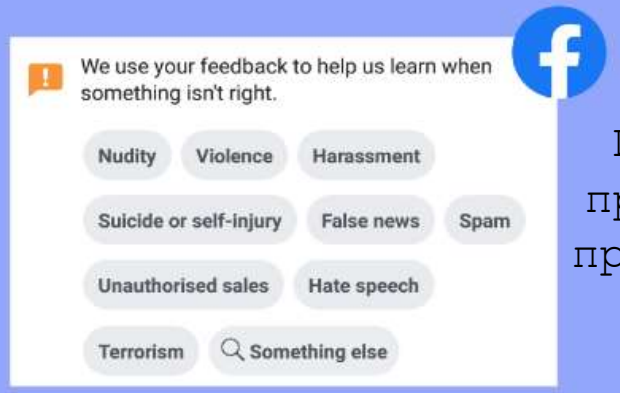
Прашања што треба да се земат во предвид:

- Како да пријавите било каква штетна онлајн содржина?
- Како, кога и на кој начин родителите треба да бидат вклучени?
- Како можете да продолжите да ги поддржувате и едуцирате сите вклучени млади луѓе?

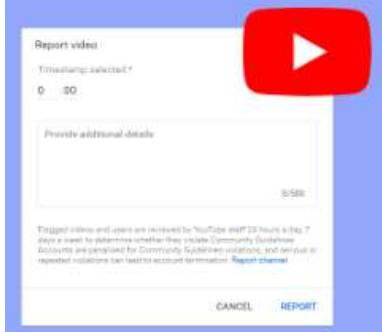
Процес на пријавување

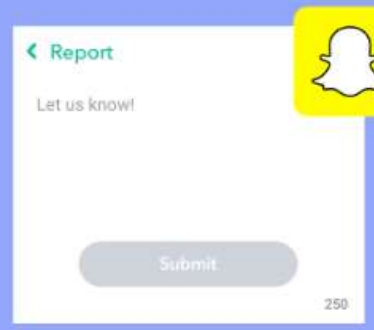
Побарајте ги овие симболи на објавата, коментарот или корисничкиот профил што сакате да го пријавите

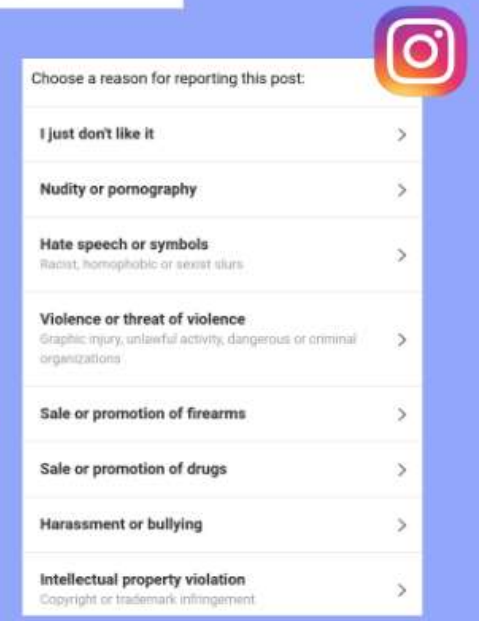




Изберете причина за пријавување







Пополнете го формуларот со колку што е можно повеќе детали и испратете за да го информирате безбедносниот тим на платформата.

Уште еден начин на пријавување и информирање

Наскоро ќе биде достапна македонската платформа за поддршка при онлајн безбедност!

www.mksafenet.mk

Превентивни мерки

Што сакаат да прават онлајн децата и младите со кои што работите? Кои сервиси и уреди ги користат?

Онлајн светот може да биде интересен и инспиративен. Тој им нуди огромен број на можности на младите. Како и да е, важно е да се менаџираат и минимизираат ризиците и штетите кои ги носи со себе.

Потребите на младите треба да бидат клучен дел од успешното обезбедување на онлајн безбедност.

Што правеше за време на викендот? Дали беше онлајн?

Започнете го разговорот полека - не мора да биде како лекција.

Кои апликации се најпопуларни во вашата генерација?

Разговарајте со нив генерално ако избегнуваат приватни разговори.

Ајде да го разгледаме/прочитаме ова заедно - што мислиш?

Користете видеа, приказни итн. како поттик за разговор.

Наставници

- Создадете култура на отворен разговор со вашите ученици - поставувајте прашања, бидете заинтересирани.
- Признајте дека младите го користат интернетот на поинаков начин од возрасните.
- Најдете каде безбедноста на интернет се совпаѓа на вашата улога.
- Користете соодветни ресурси - има многу бесплатни!
- Препознајте ја безбедноста на интернет низ училиште. Креирајте прикази, прославувајте специјални настани.

Родители и старатели

- Споделете совет во вашите канали за комуникација.
- Разговарајте со родителите/старателите кога веќе се присутни (на пр. родителска, спортски настан итн.)
- Испратете информативни летоци и списанија.

Неосудувачкиот пристап е клуч

- Користете неутрален јазик и избегнувајте да бидете критични кон интересите на учениците на интернет.
- Фокусирајте се на клучните ризици и на достапната поддршка, а не на изборите на младите.
- Создадете безбеден простор и кажете им на учениците дека нема да бидете лути или вознемирени, туку би сакале да ги поддржите во безбедно и одговорно користење на интернетот.

Наместо

"Ти си уште мал"

"Како може да бидеш толку невнимателен?"

Кажете...

"Ти благодарам што ми кажа. Ајде да размислиме што може да направиме за да помогнеме."

Следни чекори

- Започнете разговор со децата со кои работите.
- Истражувајте ресурси за возрастите на кои што предавате.
- Оддржувајте интерактивни предавања.
- Поставете постери во вашите училници/кабинети/ходници.
- Користете примери од реалниот живот.
- Прегледајте го вашиот дигитален отпечаток и поставките за приватност.

Останете безбедни, останете паметни!
Интернетот е одлично место - ако го користите паметно.

Ви благодариме!