



РЕПУБЛИКА СРПСКА
МИНИСТАРСТВО ПРОСВЈЕТЕ И КУЛТУРЕ

Трг Републике Српске1, Бања Лука, тел: 051/338-461, факс: 051/338-853, www.vladars.rs,
e-mail: mp@mp.vladars.rs

Број: 07.03/052-8214/26
Датум: 12.10.2026. године

ОСНОВНИМ И СРЕДЊИМ ШКОЛАМА
н/р директора

ПРЕДМЕТ: Позив на такмичење – „Како бити сигуран на интернету“, доставља се

Поштовани,

Поводом Међународног дана сигурнијег интернета у 2027. години, Министарство просвјете и културе и Републички педагошки завод организују такмичење под називом:

„Како бити сигуран на интернету“.

Потребно је да информисете наставнике и ученике у Вашој школи о такмичењу и ономе што оно нуди и предвиђа, као и да их подстакнете да размишљају о овој теми.

Интернет је важан дио живота у модерном свијету. Када се дјеца/ученици пријаве на интернет код куће или у школи, када користите свој мобилни телефон, када се придруже некој од друштвених мрежа - интернет отвара свијет пун забаве, нових информација и нових пријатеља за дружење. Но, са свим могућностима које интернет доноси, важно је знати како бити сигуран када користите интернет и шта је потребно урадити како би се обезбиједили. Опасности су различите - нпр. крађа лозинке и приступ личним подацима; крађа идентитета; лажно представљање и слично. Такве ситуације се могу догодити свакоме, без обзира на старост. Једини начин да ово спријечимо јесте да водимо рачуна о сигурности, а то је могуће само ако знамо како. Важна нам је сигурност наших ученика, али и њихових пријатеља, родбине, вршњака и то ученицима треба јасно дати до знања.

Такмичење „Како бити сигуран на интернету“ усмјерено је управо на ту тему и иницира размишљање, како о опасностима које вребају на интернету, тако и о начинима заштите, односно начинима сигурног кориштења интернета. Ове године потребно је размишљати о томе шта је то што дјеца и млади требају знати о сигурности на интернету: како заштитити своју безбједност, које су ризични облици понашања на интернету, како заштитити личне податке и сл.

Потребно је да ученици израде квиз на тему Безбједности на интернету или сертификат који би се након успјешно завршеног квиза додјељивао учесницима.

Такмичење је предвиђено за три категорије:

- **МЛАЂИ ОСНОВНОШКОЛСКИ УЗРАСТ** (ученици од 1. до 5. разреда) - **такмиче се у изради сертификата, који би могао бити додјељен учесницима након успјешно завршеног квиза.** Сертификат треба да буде тематски везан за квиз Сигурност на интернету. Може да буде приказан као идејно рјешење на које ће накнадном обрадом бити додати потребни елементи

(простор за име и презиме, назив квиза, датум и сл. – није дакле потребно да ученици креирају ове елементе).

- **СТАРИЈИ ОСНОВНОШКОЛСКИ УЗРАСТ** (ученици од 6. до 9.разреда) - такмиче се у изради квиза, који треба да буде више усмјерен на препознавање опасних ситуација на интернету и правилно реаговање.

Примјери тема:

- Како направити јаку лозинку?
- Које личне податке не треба дијелити?
- Како препознати непознату или сумњиву поруку?
- Шта урадити ако те неко вријеђа или узнемирава на интернету?
- Зашто не треба прихватати захтјеве за пријатељство од непознатих особа?
- Како безбједно користити фотографије и друштвене мреже?
- Коме се обратити ако се догоди проблем?
- Примјер конкретног питања - Препознати која је од неколико приказаних ситуација безбједна, а која опасна.

- **СРЕДЊОШКОЛЦИ** - такмиче се у изради квиза, који треба да захтијева анализу ситуације, препознавање преваре и доношење исправне одлуке.

Примјери тема:

- Препознавање phishing порука и лажних веб-страница;
- Двофакторска аутентификација;
- Крађа идентитета;
- Управљање дигиталним трагом;
- Приватност на друштвеним мрежама;
- Онлајн преваре и социјални инжењеринг;
- Провјера поузданости информација;
- Безбједност јавних Wi-Fi мрежа;
- Заштита налога и уређаја;
- Одговорно коришћење вјештачке интелигенције;
- Примјер конкретног питања - Ученици добијају реалан сценарио, нпр. сумњиву SMS поруку или имејл, и треба да објасне који су знакови опасности и шта би предузели.

Квизове је потребно израдити употребом алата *Microsoft Forms* и треба да садрже 15 до 20 питања, уз употребу најмање три различите врсте питања.

Приједлоге сертификата достављати поштом или мејлом. За квизове је потребно имејлом доставити линк и QR код, путем којег је истом могуће приступити, као и преглед питања, те тачне одговоре и кратко објашњење за свако питање (као текстуални документ у прилогу мејла).

Радове је потребно слати на адресу:

Републички педагошки завод

Подручна канцеларија у Фочи

Цара Душана бб

73300 Фоча

Република Српска

са напоменом Пријава на такмичење „Како бити сигуран на интернету“

или на имејл адресу: a.stankovic@rpz-rs.org.

Уз достављање радова обавезно је доставити пријаву која треба да садржи: име аутора, школу, разред, те име наставника - ментора.

У свакој категорији биће проглашена три најбоља рада.

Рок за слање радова је 25. децембар 2026. године.

С поштовањем,

Достављено:

1. Именованим
2. Архиви



МИНИСТАР

Боривоје Голубовић