ЛЕКЦИЈА 4

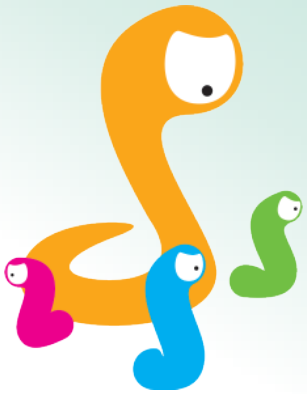
Будите безбедни на мрежи

Интернет нуди бесконачне могућности и може вам олакшати живот. Чак и домаћи задатак може брже да се уради, посебно када је у питању прикупљање информација.

Али све има своју цену. Пошто је интернет огроман, постоји ризик од штетних програма који се називају **Малвер** (MALicious softWARE). Њихова улога је да наруше функционисање рачунара, да прикупе осетљиве информације или приступе приватним рачунарским системима. Да поменемо само неколико врста малвера: вируси, тројански коњ, црви, спајвер (енгл. spyware) - шпијунски софтвер, адвер (енгл. adware) - рекламни софтвер.

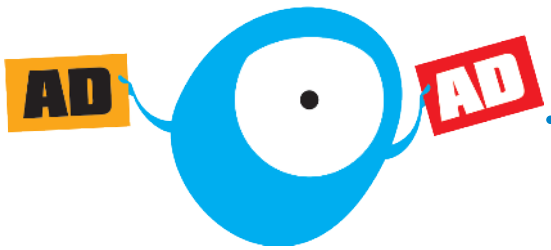
Вирус је програм који може да се умножава и шири са једног рачунара на други. Сврха овог програма је да оштети ваш рачунар, да обрише датотеке или да спречи правилно функционисање рачунара. Вирусе стварају људи који врло добро познају рачунарско програмирање и умрежавање.

Тројански коњ изгледа као нормалан и безопасан програм. Његова сврха је да се злонамерним особама омогући неовлашћени приступ вашем рачунару. Тројанци немају намеру да се копирају или заразе друге датотеке, већ обично краду информације са вашег рачунара.



Црв се умножава како би се проширио на друге рачунаре, углавном кроз мрежу.

Спајвер (Шпијунски софтвер) прикупља информације о корисницима без њиховог знања. Шпијунски софтвер је скривен од корисника и веома га је тешко открити.



Адвер (рекламни софтвер) вам показује рекламе без ваше дозволе. Ове рекламе могу бити у облику искачућег прозора (енгл. pop-up), у корисничком окружењу програма.

Како да се заштитите приликом рада на интернету?

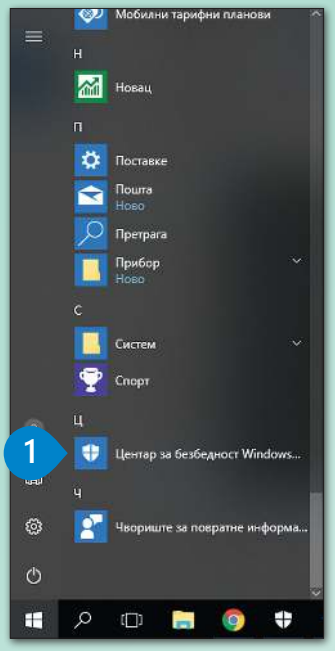
Морате да имате инсталиран **антивирусни програм** на рачунару и да проверите да ли је увек ажуриран за нови малвер.

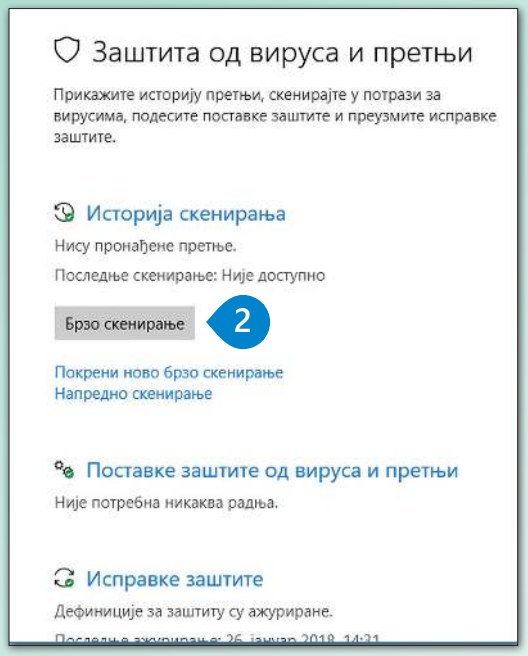
Антивирусни програм стално проверава штетне програме. Такође, можете да извршите и **скенирање** како бисте били сигурни да је рачунар чист и безбедан. Овако се то ради:

Да бисте отворили Центар за безбедност:

> Отворите **Центар за безбедност** (енгл. Microsoft Security Essentials) на рачунару и кликните на картицу Заштита од вируса и претњи. 1

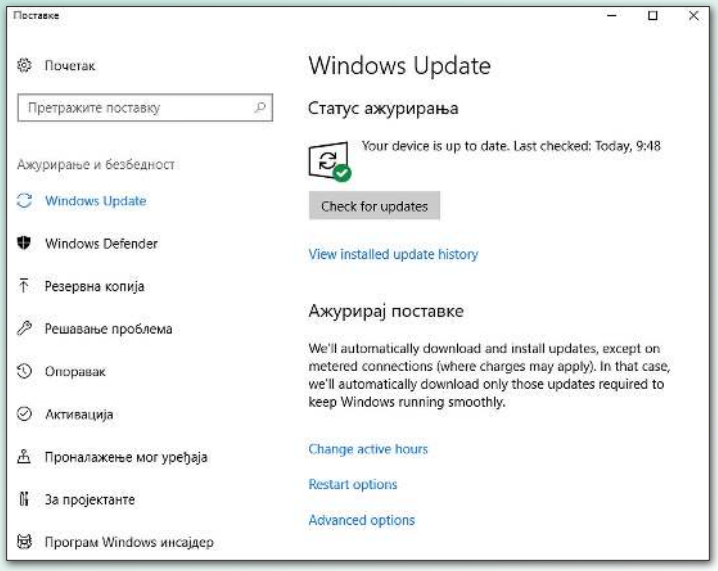
> Кликните на дугме **Брзо скенирање** (енгл. Quick scan). Ако изаберете пуно скенирање, може да ће процес потрајати сатима док се не заврши. 2





Како ажурирати антивирусни програм

Антивирусни програм може да проверава постојање малвера на рачунару само ако зна за њих. Свакодневно се појављују нови штетни програми, тако да морате бити повезани на интернет и ажурирати антивирусни програм скоро сваког дана.



Шта још треба да знате?

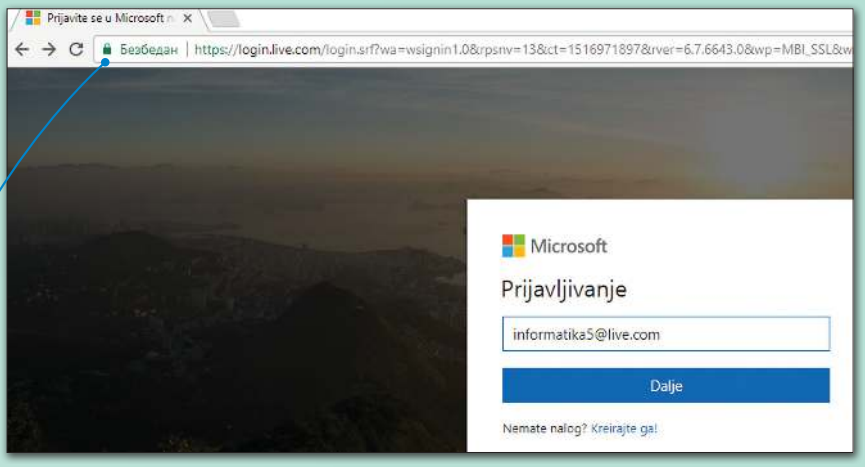
Увек ажурирајте софтвер на свом рачунару. Можда ће вашем оперативном систему бити потребно ажурирање за решавање проблема.

Безбедна комуникација

Добар начин избегавања вируса јесте посета безбедних и поузданих веб-страница. На пример, ако желите да купите књигу, идите у проверене онлајн-књижаре као што је, на пример, Амазон. Начин да се провери да ли је веб-локација поуздана је икона **Катанац** (енгл. Padlock) на траци за унос веб-адресе, поред адресе веб-сајта.

Када видите иконицу **Катанац** (енгл. Padlock) сва комуникација између вас и веб-локације је шифрована. Једноставним речима, ако упишете лозинку електронске поште и она гласи на пример 3x@mple, пренеће се као 3wrt93is0932959dsfwsdf34sfsrq3, тако да нико не може да је разуме осим вашег рачунара и сервера веб-сајта.

Да ли то значи да када видим **Катанац** икону могу да уносим било какву информацију? Одговор је – НЕ! Иако видите **Катанац**, и даље морате бити врло пажљиви и сигурни да верујете веб-сајту са којим ћете поделити своје личне информације.



Реците својим пријатељима за икону Катанца. Побрините се да је потраже када купују преко интернета. Свакако се у случају куповине преко интернета договарајте са неким од старијих укућана.

Корисничко име и лозинка

Сваки пут када се налазите на неком интернет налогу, од вас се тражи **корисничко име и лозинка**. Зашто су они тако важни и зашто су нам потребни?

Знате ли да постоје ормарићи у које можете сместити ствари, закључати их и унети шифру? То је начин да заштитите своје ствари. Потребна вам је иста заштита и за ваше ствари на интернету. На пример, потребан вам је лични налог када комуницирате са другима. То је једини начин да ваши пријатељи препознају ко сте. Ваше **корисничко име** (енгл. username) може бити право име или надимак. Да бисте заштитили овај налог, потребна вам је тајна **лозинка** (енгл. password) коју знате само ви (а можда и ваши родитељи).

Хајде да видимо како можете да креирате јаку лозинку:

> Лозинка мора бити довољно дуга. Лозинку са 4 знака је веома лако разбити. Користите лозинке које садрже најмање 8 до 10 знакова.

> Избегавајте уобичајене речи као што су љубав, мама, тата, фудбал... На вама је да смислите оригиналну лозинку.

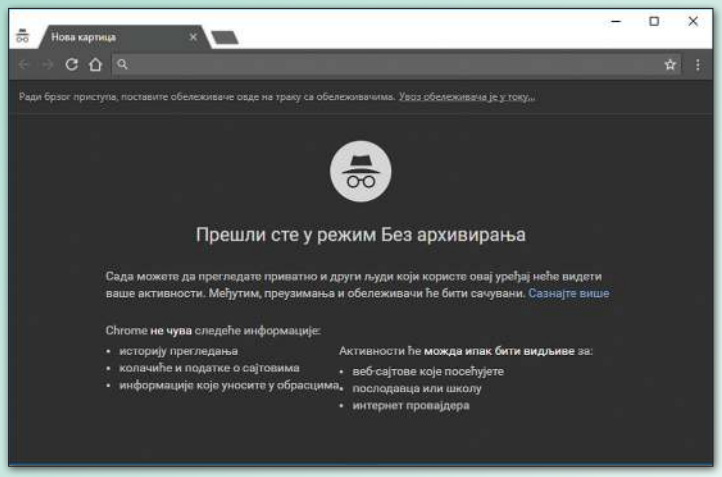
> Не користите исту реч/фразу за своје корисничко име и за лозинку! Такође, не користите личне информације: рођендан, омиљени тим, број телефона, итд.

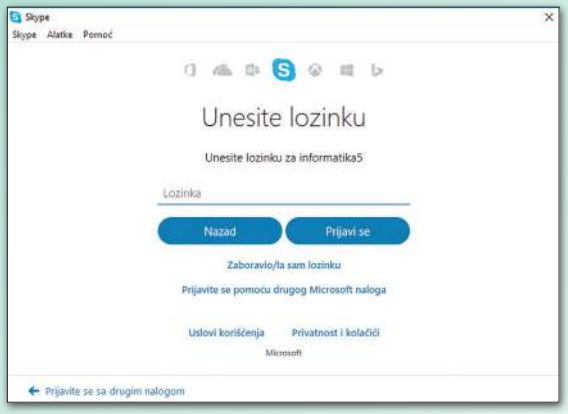
> Користите и симболе и бројеве. Биће много теже да неко погоди вашу лозинку ако је Be0gr@d1# уместо само Београд.

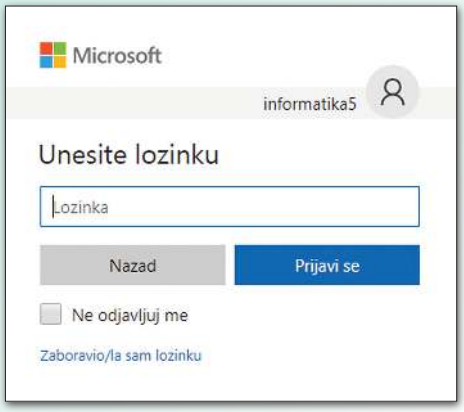
> Једноставан начин стварања јаких лозинки које можете лако да запамтите је да смислите реч или фразу и замените самогласнике симболима и бројевима. На пример, уместо markodigitalkids, пробајте m@rk0d!G!T@lk!ds. Тешко је погодити, али ћете је запамтити.

> Ако користите неки важан налог, мењајте лозинку сваких 6 до 12 месеци.

Уколико сте приступали свом налогу преко нечијег туђег рачунара, обавезно проверите да ли сте се одјавили кад завршите рад. Најбезбедније је да у случају рада на туђем рачунару користите прозор "без архивирања" (енгл. Incognito window) јер на тај начин, кад затворите прозор, у рачунару неће остати запамћено ваше корисничко име, лозинка, историја прегледања...







Не користите исту лозинку свуда. Ако неко сазна вашу лозинку, он ће имати приступ свим вашим налозима. И не остављајте белешке са својом лозинком поред екрана рачунара!

Користите лозинке и за мобилне телефоне и таблете како бисте заштитили поруке, слике и сл.