

Što znači biti kibernetički siguran?

CARNET – Odjel za Nacionalni CERT





Sadržaj

1. Uvod: pojmovi
2. Što hakeri žele?
3. Kako se zaštитiti?
4. Zaštita podataka
5. Zaključak

Kibernetička sigurnost

„Sustav organizacijskih i tehničkih aktivnosti i mjera kojima se postiže autentičnost, povjerljivost, cjelovitost i dostupnost podataka, kao i mrežnih i informacijskih sustava u kibernetičkom prostoru.”

- *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*

Kibernetički prostor

„Virtualni prostor unutar kojeg se odvija komunikacija između mrežnih i informacijskih sustava te obuhvaća sve mrežne i informacijske sisteme neovisno o tome jesu li povezani na internet.”

- *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*

Kibernetički kriminal

„Činjenje kaznenih djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom informacijskih i komunikacijskih tehnologija.”

- *Nacionalna strategija kibernetičke sigurnosti*

Podatak

„Različite skupine elektroničkih zapisa koji imaju vrijednost za korisnike koji s njima postupaju.”

- *Zakon o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga*

Osjetljivi podaci

„Skupine podataka koje se koriste samo za službene potrebe ili skupine podataka koje su zaštićene odgovarajućim propisima, a pri tome nemaju svojstvo tajnosti (npr. označeni neklasificirani podaci ili osobni podaci).”

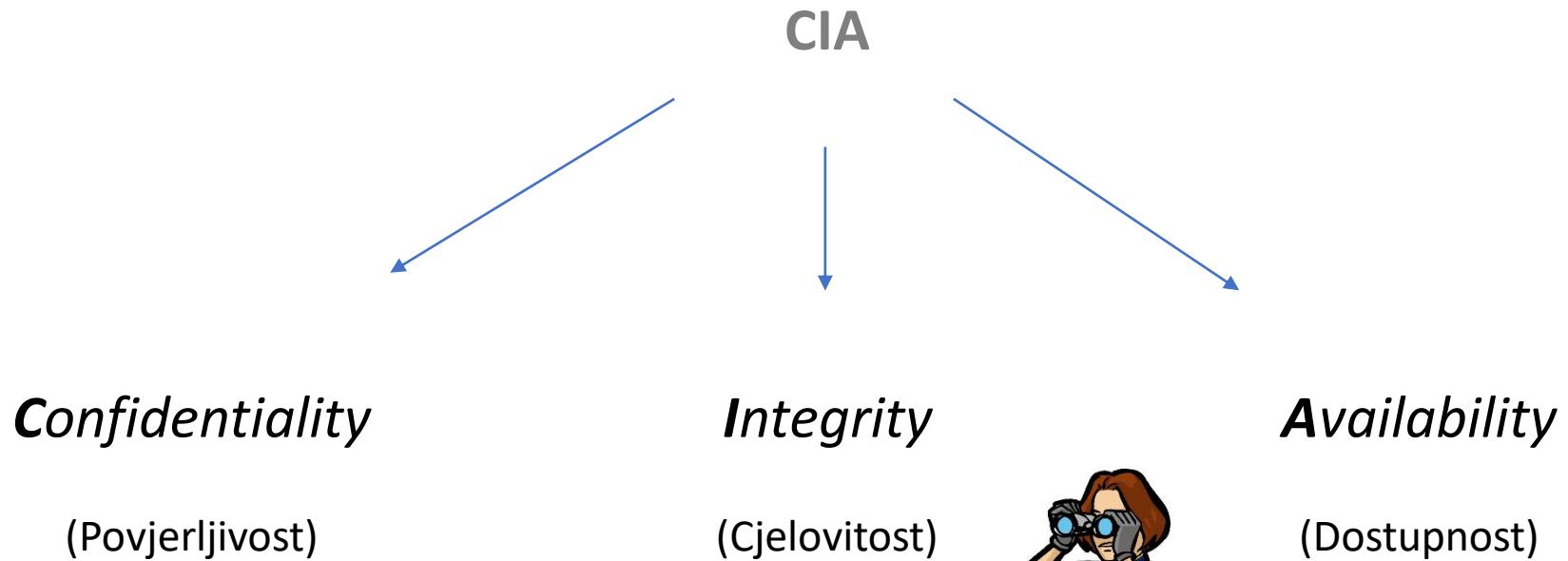
- *Nacionalna strategija kibernetičke sigurnosti*

Digitalni trag

„Jedinstven skup digitalnih aktivnosti, akcija, doprinosa te komunikacije putem interneta i digitalnih uređaja kojih se može uči u trag.“



Osnovna načela informacijske sigurnosti



Povjerljivost

Otkrivanje informacija i podataka isključivo autoriziranim osobama.



Cjelovitost

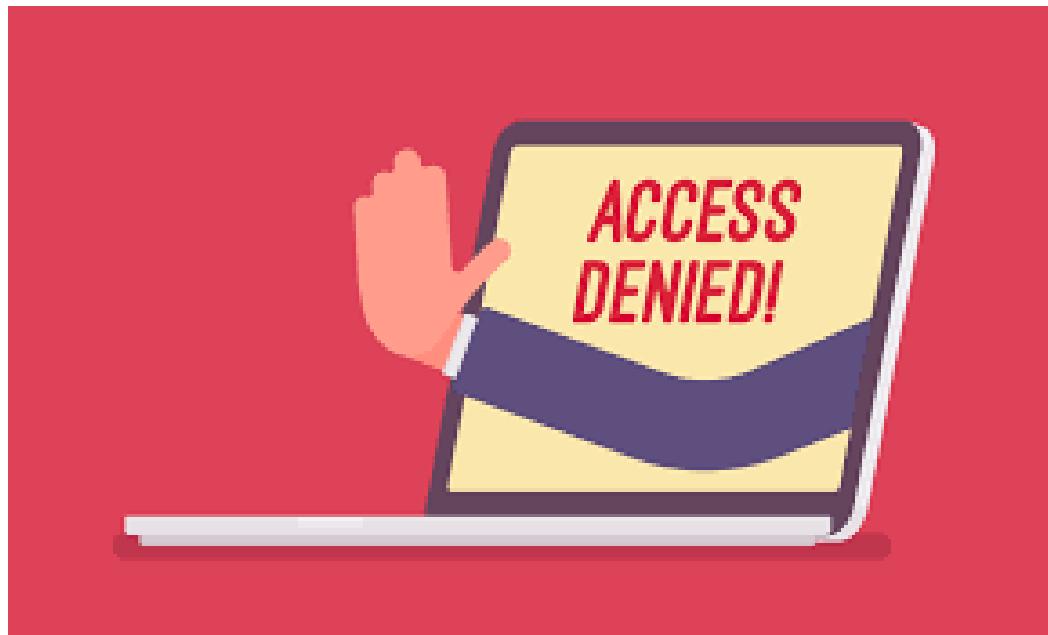
Informacija ima vrijednost samo onda kada je točna

Zaštita informacija od namjerne ili slučajne neovlaštene izmjene.



Dostupnost

Raspoloživost tražene informacije ovlaštenim korisnicima u danom trenutku.



Hakiranje

Malo o povijesti hakiranja

- Alan Turing i Enigma
- Phone Phreaking (zviždanje u slušalicu)



Akteri u kibernetičkoj sigurnosti

HAKER

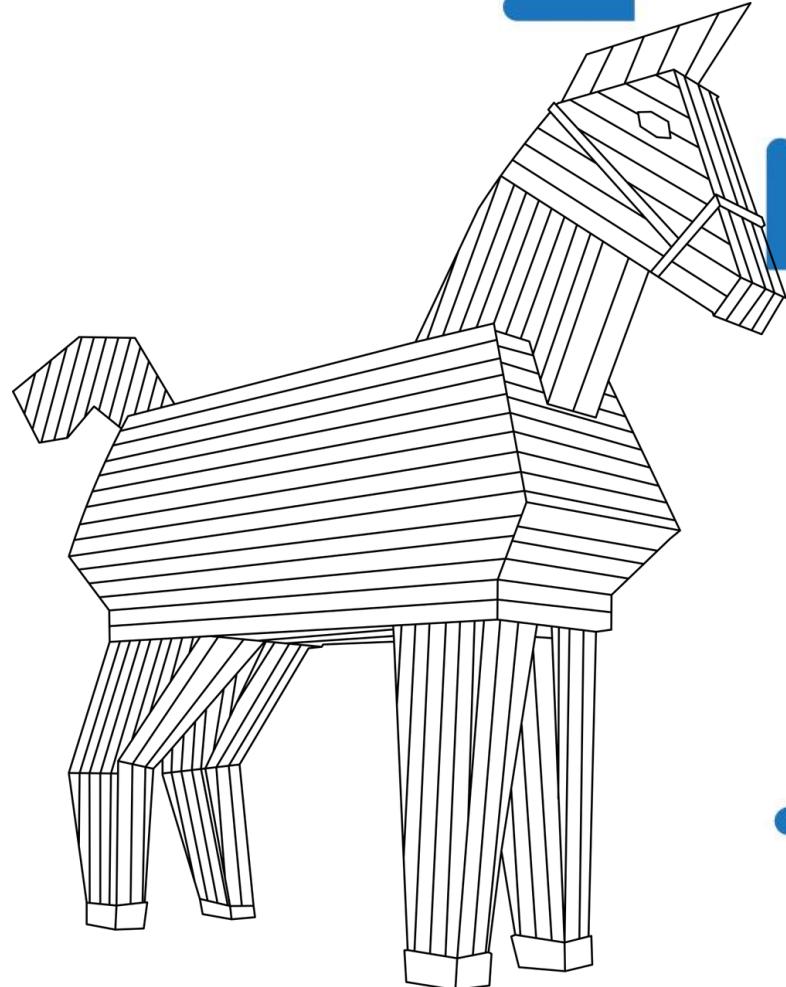


HAKERSKE SKUPINE

- organizirani kriminal,
- najčešće motivirane novčanom dobiti

DRŽAVNO POTPOMOGNUTE SKUPINE

- dobro financirane skupine korištene za složene i precizne napade.
- Motivirane političkim, ekonomskim, tehnološkim i vojnim ciljevima.



Akteri u kibernetičkoj sigurnosti

VRSTE HAKERA



White hat

Grey hat

Black hat

Akteri u kibernetičkoj sigurnosti

VRSTE HAKERA



White hat

Grey hat

Black hat

- Hakeri samoubojice
- Script kiddies
- Cyber teroristi
- Haktivisti

Što hakeri žele?



Što je sve osobni podatak?

MATIČNI PODATCI

- Ime
- Prezime
- Srednje ime
- Inicijali (svi)
- OIB
- JMBG
- Adresa (osobna)
- Datum rođenja
- Ime majke/oca
- Djevojačko ime majke
- Zapis o školovanju
- Zapis o kažnjavanju
- Interni broj/oznaka zaposlenika
- Zapis o internoj evaluaciji
- Elektroničke adrese
- Telefonski brojevi
- Faks brojevi
- Identifikatori na socijalnim mrežama
- Podaci o djeci

OSOBNI DOKUMENTI

- Preslika osobnih dokumenata (iskaznica, putovnica, vozačka dozvola itd.)
- Broj osobne iskaznice
- Broj putovnice
- Broj vozačke dozvole

FINANCIJSKI PODATCI

- Plaća
- Urednost plaćanja računa
- Iznos računa
- Dugovanje
- Broj bankovnog računa (IBAN)
- Trajni nalog/Izravno terećenje/SEPA izravni terećenje
- Račun (engl. *billing account*)
- Porezni broj
- Broj kreditnih/debitnih kartica

POSEBNE KATEGORIJE OSOBNIH PODATAKA

- Rasno ili etničko podrijetlo
- Političko mišljenje
- Vjersko ili filozofsko uvjerenje
- Članstvo u sindikatu
- Genetski i biometrijski podaci
- Podaci o zdravlju
- Podaci o spolnom životu ili seksualnoj orijentaciji

PROMETNI PODATCI

- Telefonski pozivi (ispis telekomunikacijskog prometa)
- Sadržaj telefonskih poziva
- Sadržaj poruka elektroničke pošte
- Sadržaj tekstualnih poruka

AUDIO VIDEO SNIMKE

- Snimke telefonskih razgovora
- Snimke nadzornih kamera
- Fotografija osobe (samo lice)

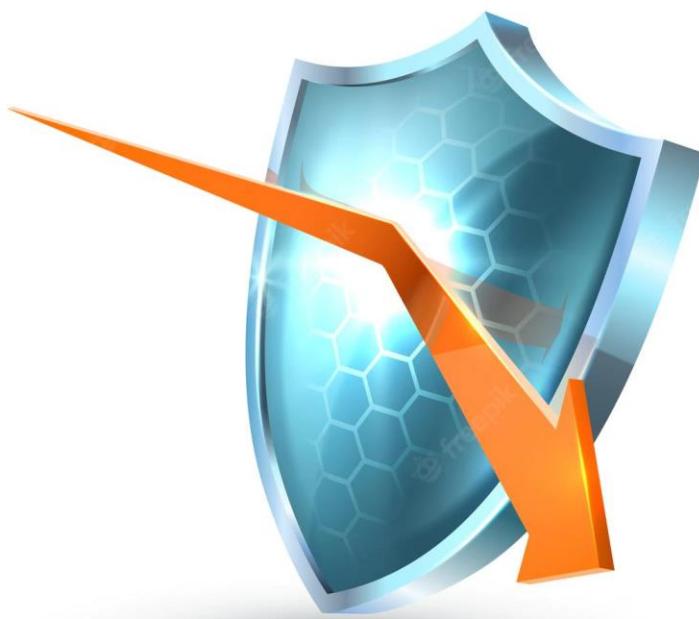
PODATCI O KORIŠTENJU KOJI NISU PROMETNI

- Podaci o navikama
- Podaci o kretanju
- Različiti logovi o korištenju aplikacija/usluga

PODATCI O USLUGAMA I PROIZVODIMA

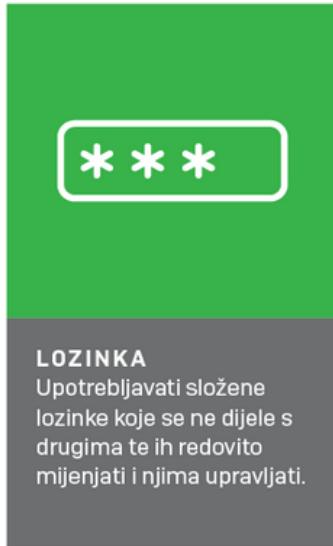
- Usluge/proizvode koje fizička osoba koristi
- Tarife koje fizička osoba koristi
- Serijski broj uređaja (računalo, telefon...)
- IMEI
- IMSI
- Broj registarskih oznaka vozila, broj šasije...
- IP adresa
- Korisnička imena i lozinke
- PIN/PUK brojevi
- Broj OMM (obračunsko mjerno mjesto) za struju/plin

Kako se zaštитити?



Kibernetička higijena

- set pravila
- sigurnosne prakse
- smjernice
- praktični postupci



LOZINKA

Upotrebljavati složene lozinke koje se ne dijele s drugima te ih redovito mijenjati i njima upravljati.



SOFTVER

Sve programe i aplikacije redovito nadograđivati.



PRISTUP

Definirati korisnički pristup sustavu.



HARDVER

Nadograđivati svu opremu te je po potrebi zamijeniti.



INSTALACIJE

Ispravno izvoditi sve nove instalacije, uz dokumentiranje procesa.



SIGURNOSNA KOPIJA

Sigurnosne kopije koje se čuvaju odvojeno od sustava ključne su za minimiziranje štete u slučaju gubitka podataka.

Dobra lozinka



Najmanje 12 znakova



Malo pomiješajte: mala i velika slova, znamenke i posebni znakovi

Ne koristite iste lozinke za različite sustave, pogotovo ne za privatne i poslovne račune



Nikada ne koristite niz znamenaka i/ili slova



Nikada ne koristite osobne informacije poput rođendana, imena svog ljubimca ili naziv ulice



Ne koristite riječi koje možete pronaći u bilo kojem rječniku

Tehnika stvaranja lozinke

- Primjer -

*Tri puta tjedno vježbam u Gymu
od 19 do 20 sati!*

Lozinka:

3*W_Gym_19-20h!

3*W_Gym_19-20h!

Very Strong

15 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:
54 billion years

Review: Fantastic, using that password makes you as secure as Fort Knox.

Upravitelji za lozinke

Prednosti:

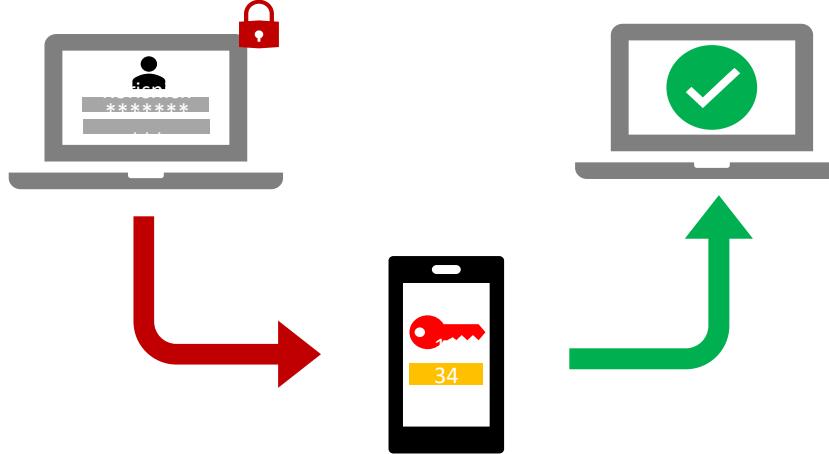
- Jedna lozinka za sve druge lozinke.
- Automatsko stvaranje snažne lozinke.
- Možete imati različite lozinke za svaki račun, a ne morate ih pamtitи.

Nedostaci:

- Jedna lozinka za sve druge lozinke.
- Dobra lozinka nas ne štiti u potpunosti.
- Potrebno je njihovo postavljanje.

Dvofaktorska (2FA) i višestruka autentifikacija (MFA)!

Korisničko ime i lozinka



Kod poslan na vaš
mobilni telefon

Korisnici koji su prethodno aktivirali svoje račune putem ove stranice mogu direktno do svojih računa putem stranice [portal.office.com](#).

Odvedi me na Office365

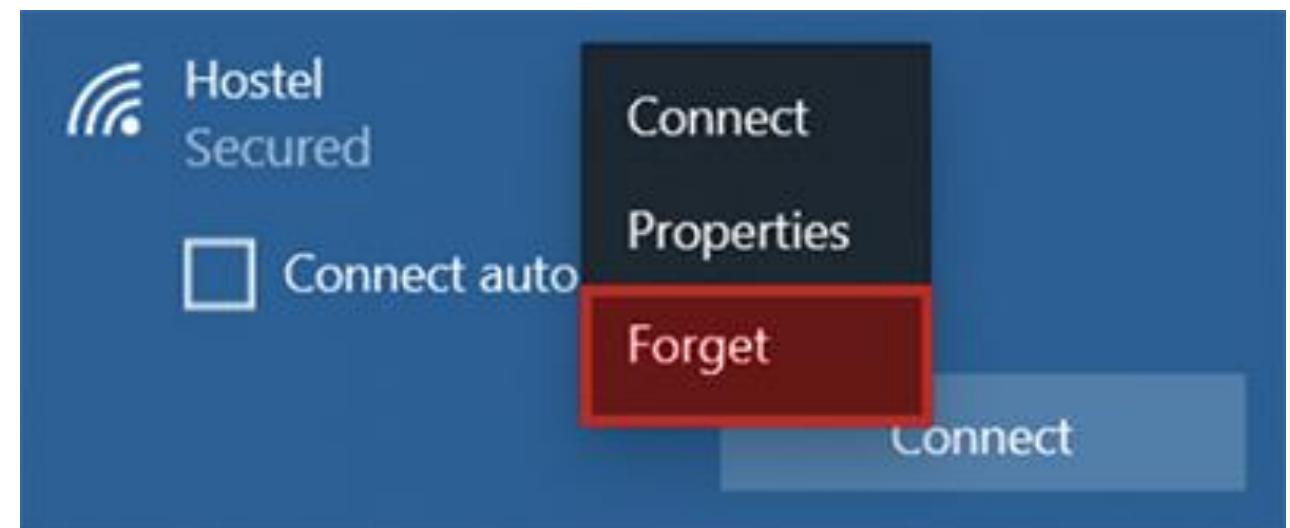
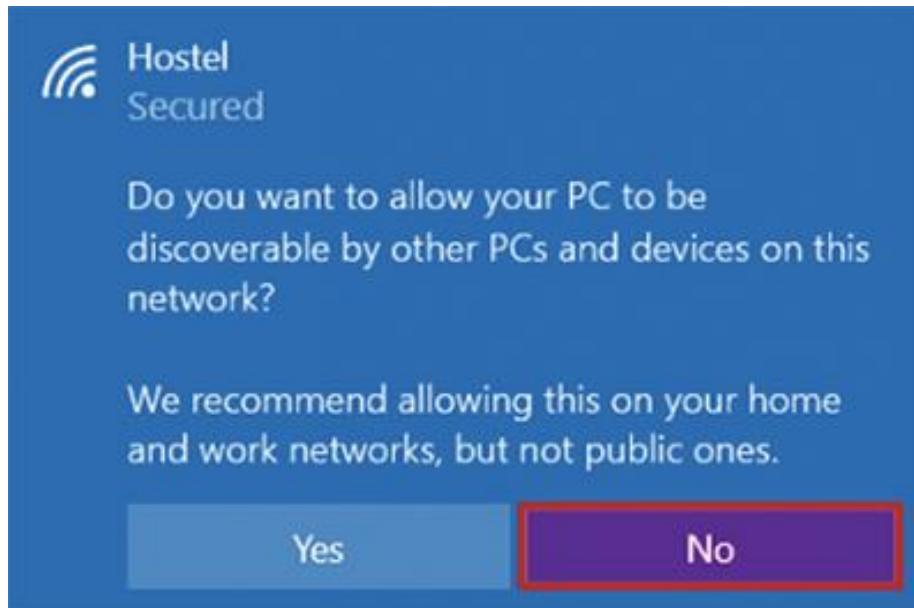
MFA (Multi-factor Authentication): **isključeno**

Multi-faktorska autentifikacija (MFA) služi za prijavu na servise kojima se ne pristupa kroz internet preglednik (MS Office aplikacija, MS Outlook mobilna aplikacija i sl.). U tom slučaju lozinka od AAI@EduHr računa (ime.prezime@skole.hr) kojeg je korisnik dobio od administratora imenika u školi ne vrijedi već je za pristup istima potrebno kreirati zasebnu lozinku pomoću MFA. Dok je uključena MFA, prijava se vrši dodatnom sigurnosnom verifikacijom, telefonski ili putem SMS-a.

[Uključi MFA](#)

Spajanje na Wi-Fi

- Kućnom Wi-Fi-u promijeniti početnu lozinku.
- Ako je moguće izbjegavati spajanje na javni Wi-Fi.
- Kreiranje mobilne pristupne točke.
- Ako nema druge opcije nego spojiti se na javni Wi-Fi:
 - Označiti ga kao javni („public“) Wi-Fi i ne dopuštati da vas drugi uređaji mogu otkriti na toj mreži.
 - Na kraju „zaboraviti“ tu vezu kako se ne bi ponovno automatski spajali.



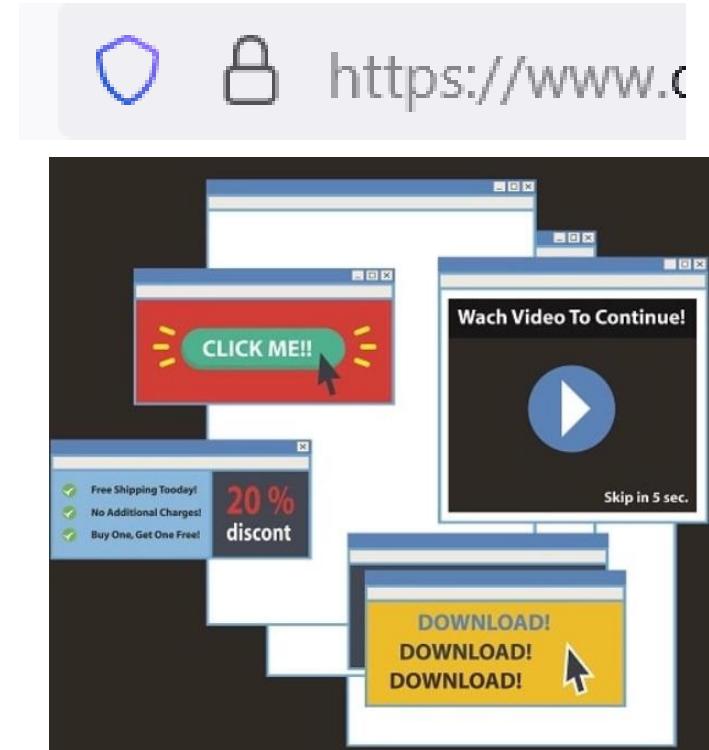
-  General
 -  Speech
 -  Inking & typing personalization
 -  Diagnostics & feedback
 -  Activity history
- App permissions
-  Location
 -  Camera
 -  Microphone
 -  Voice activation
 -  Notifications

Dopuštenja aplikacijama

- Pazite koja dopuštenja dajete aplikacijama.
- Windows dopuštenja – dopuštenja sustavu.
- Dopuštenja aplikacija (lokacija, kamera, mikrofon, slike, kontakti...).
- Dopuštenja uredite i na računalu i na mobitelu.

Sigurno surfanje

- Ima li URL „lokot” i „https://”?
- Blokiranje skočnih prozora
- Ažuriranje preglednika
- Preuzimanje datoteka samo iz sigurnih izvora
- Cjelokupni izgled stranice
- Poseban oprez prilikom online kupovine



Surfanje u anonimnom prozoru preglednika?

- Ne sprema povijest pretraživanja, kolačiće, lozinke i zapis o preuzimanjima lokalno.
 - Korisno za korištenje javnih računala (npr. u knjižnici).
-
- Pružatelj internetske usluge i dalje može pratiti promet mrežom, a to često mogu i druge ustanove na čiju mrežu je uređaj spojen.
 - Ne štiti od hakera, malwarea i drugih izvora opasnosti.





Zaštita digitalnih podataka

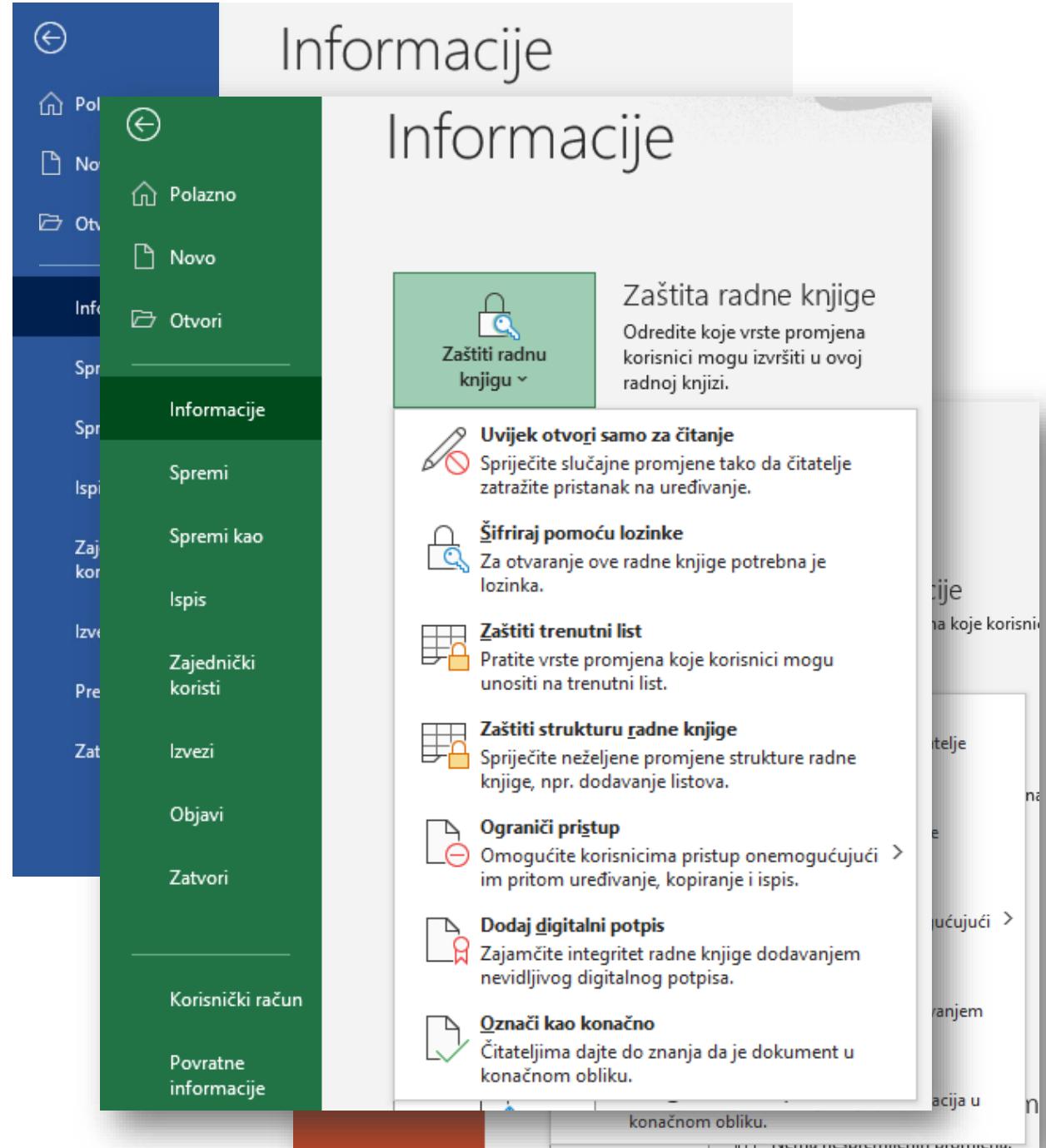
Zašto je
potrebno
zaštiti
datoteke na
računalu?



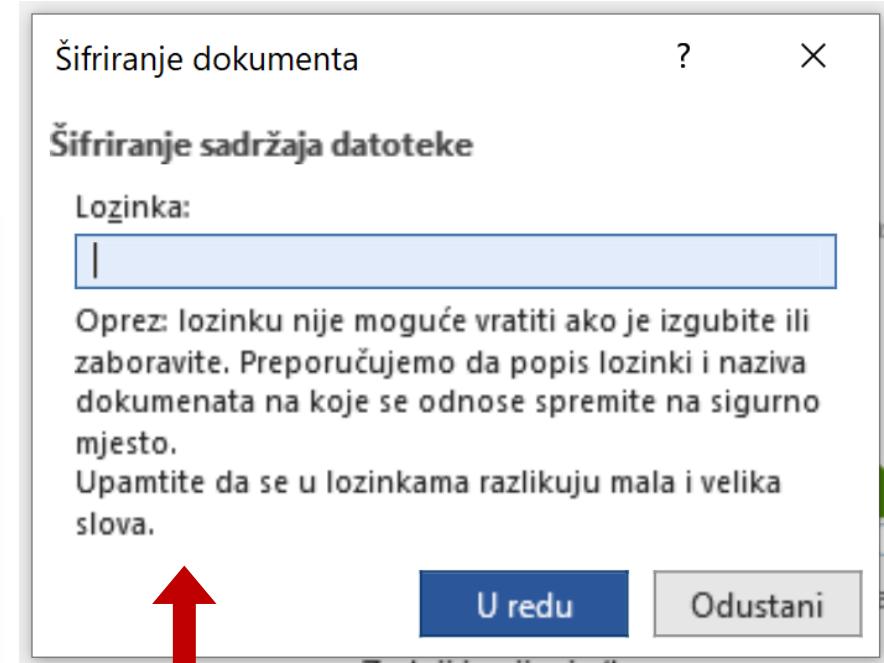
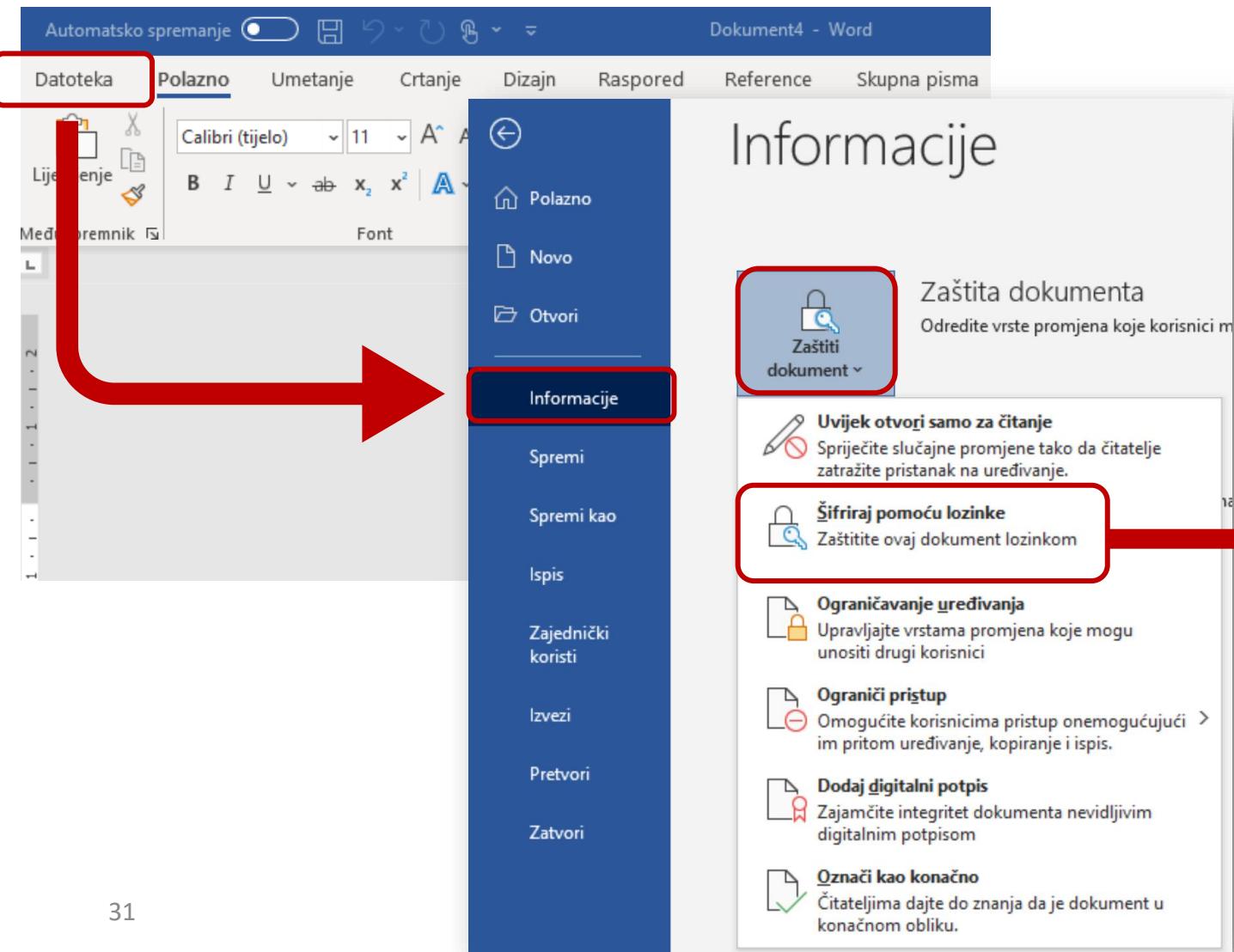
Zaštita Microsoft Office dokumenata

Datoteke stvorene u Wordu, PowerPointu i Excelu moguće je zaštititi:

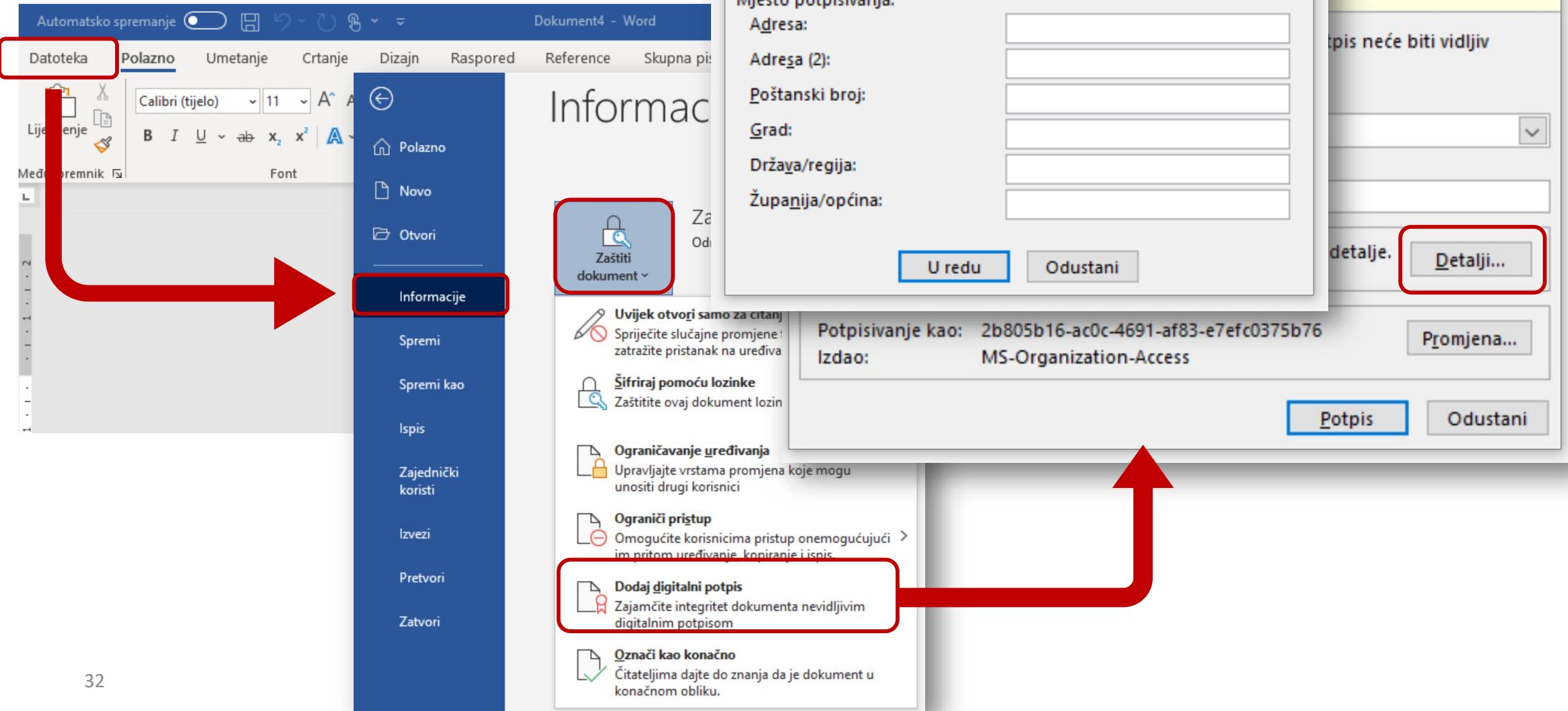
- šifriranjem pomoću lozinke
- ograničavanjem pristupa
- dodavanjem digitalnog potpisa



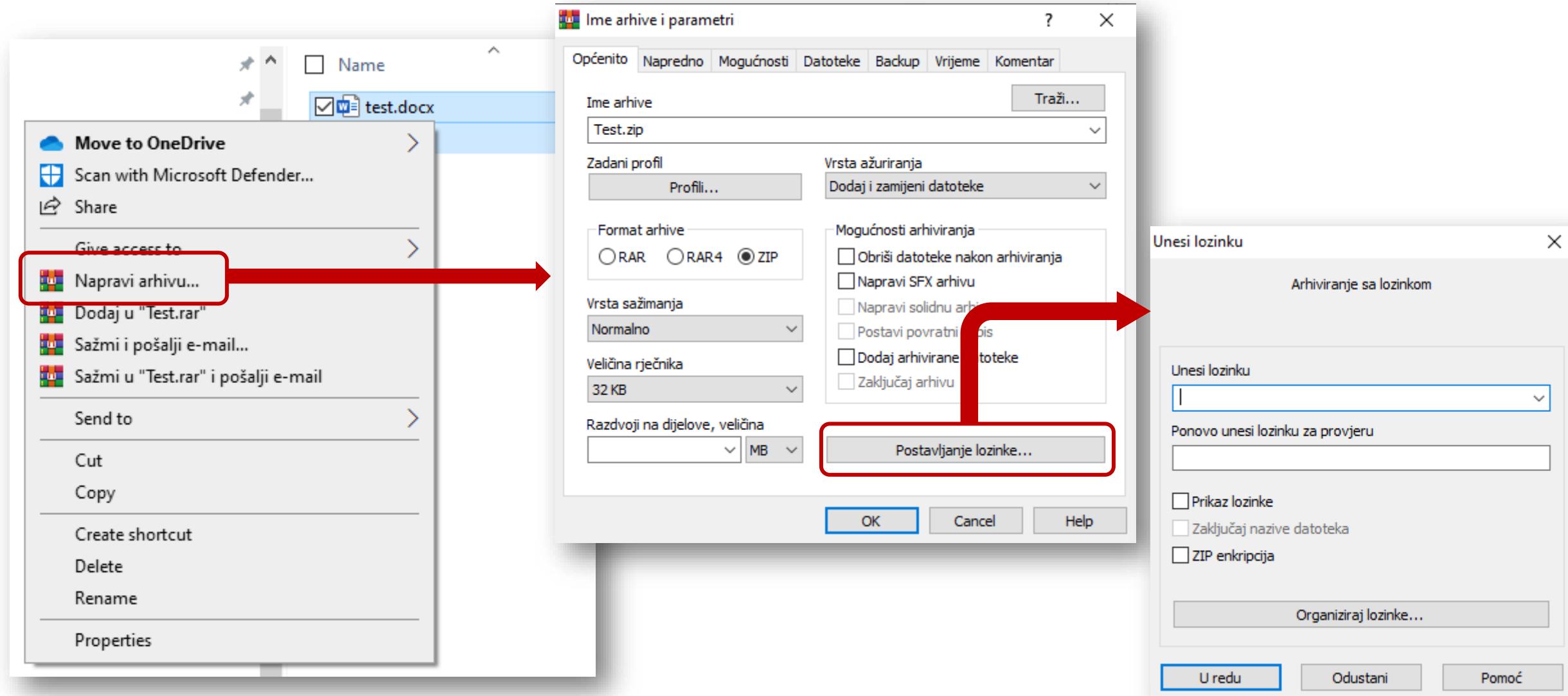
Šifriranje pomoću lozinke



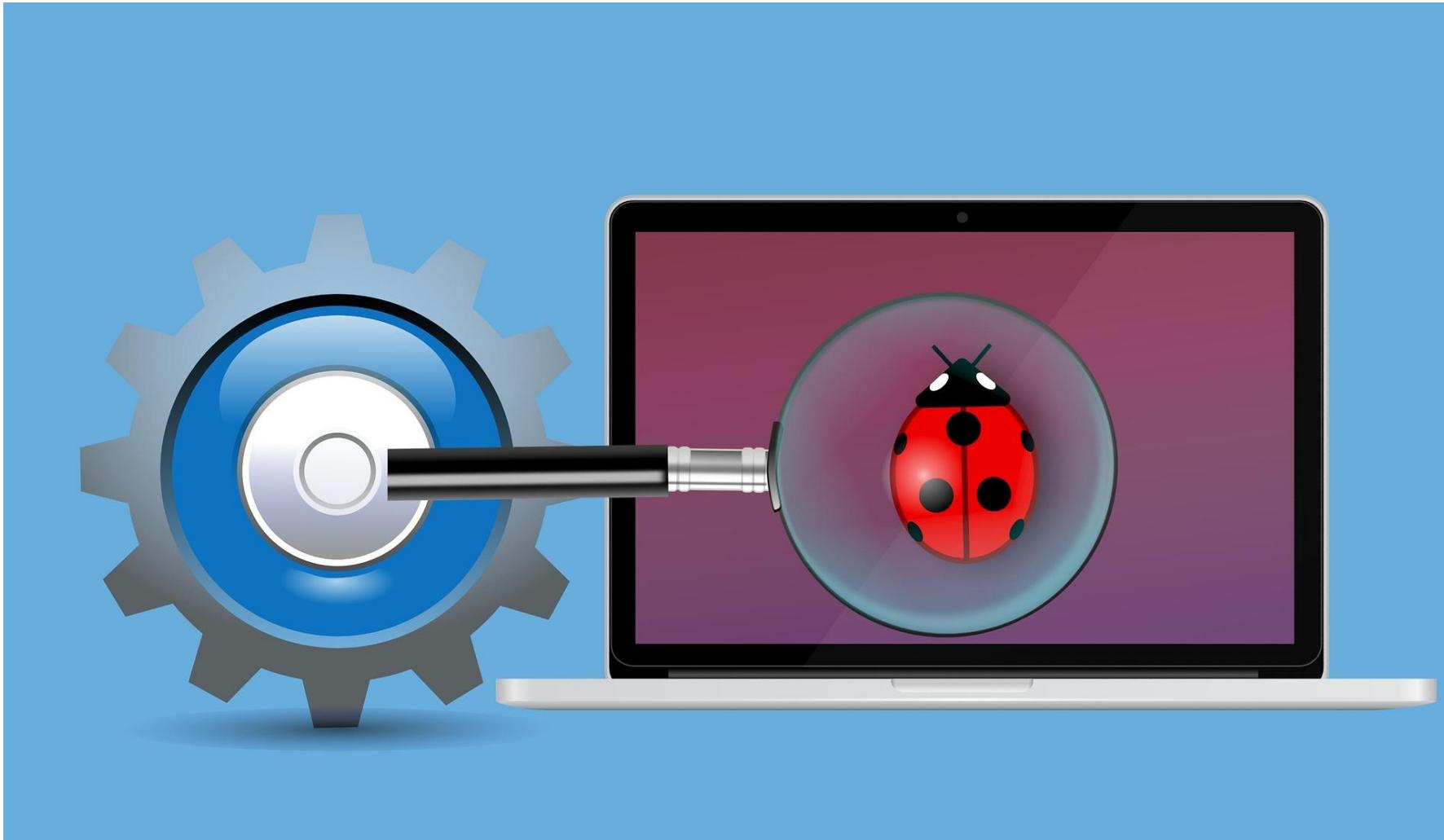
Digitalni potpis



Zaštita komprimiranih datoteka (zip)



Antivirusni programi



Izvor: <https://pixabay.com/illustrations/scan-system-bug-virus-malware-3963099/>

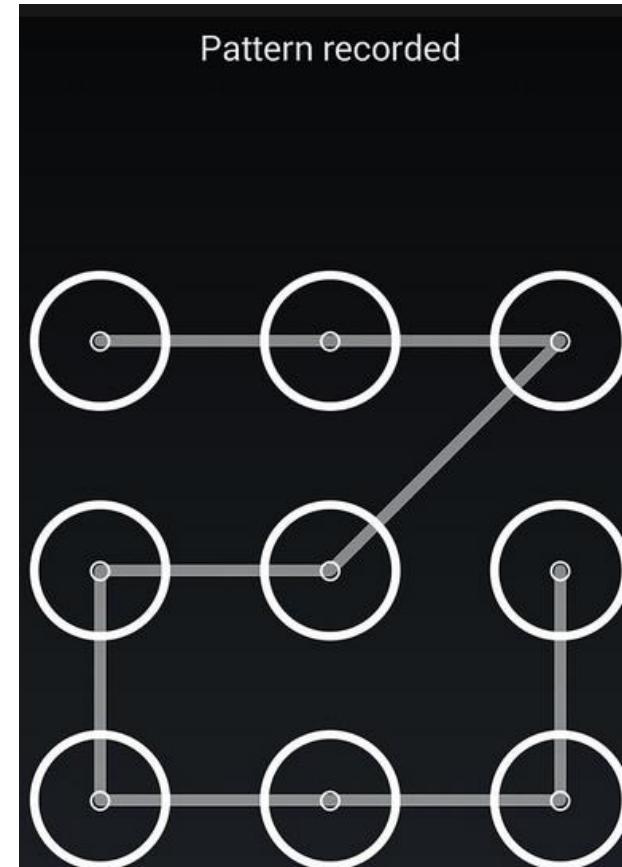
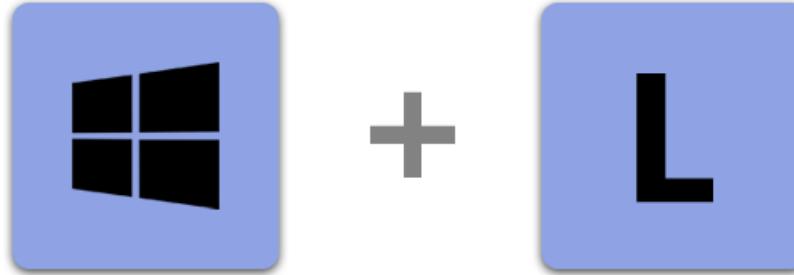
Najpopularniji u

2022. godini:

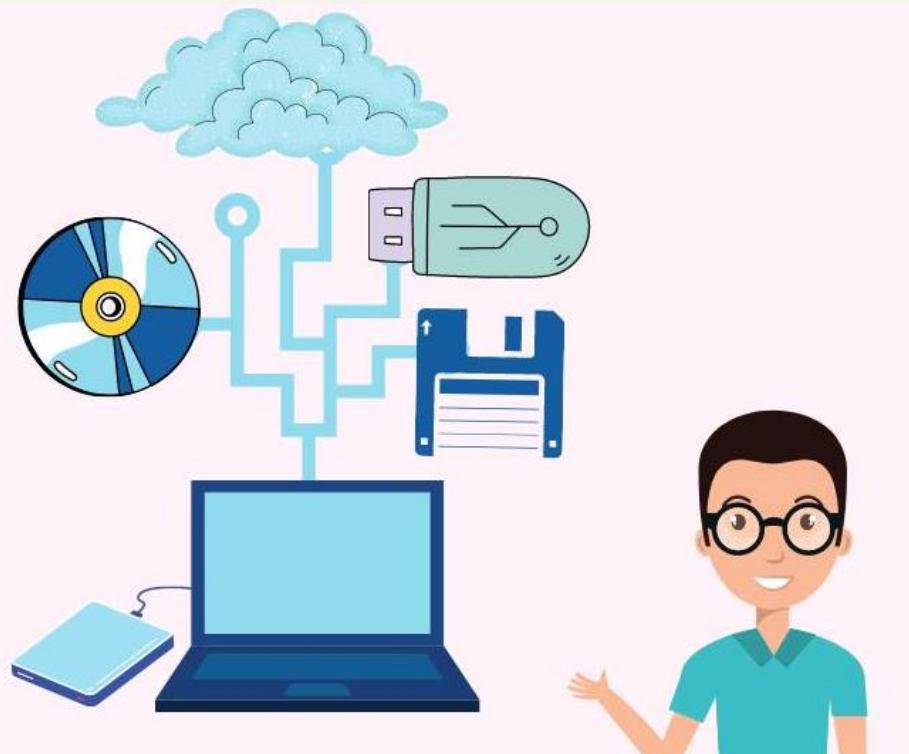
- Norton
- Bitdefender
- Intego
- TotalAV
- McAfee

Zaključavanje uređaja

- Zaključavajte računalo i mobilni telefon kad niste u njihovoj blizini.
- Koristite neki oblik zaštite za otključavanje uređaja.



Izrada sigurnosne kopije!



Ako ne želite izgubiti podatke uvijek je pametno izraditi sigurnosne kopije.

Pravilo 3-2-1:

- 3 kopije
- 2 pohranjene na istoj lokaciji
- 1 pohranjena na drugoj lokaciji

Podaci vrijede više od uređaja na kojem su pohranjeni!

Ažuriranje softvera

- Redovitim ažuriranjem sustava sprečava se iskorištavanje poznatih ranjivosti.
- Uključite automatsko ažuriranje softvera.

Settings

Home

Find a setting

Update & Security

- Windows Update
- Delivery Optimization
- Windows Security
- Backup
- Troubleshoot
- Recovery
- Activation
- Find my device
- For developers
- Windows Insider Program

Windows Update

View configured update policies



You're up to date
Last checked: Today, 0:47

[Check for updates](#)

[View optional updates](#)

Pause updates for 7 days

Visit Advanced options to change the pause period

Change active hours

Currently 8:00 to 17:00

View update history

See updates installed on your device

Advanced options

Additional update controls and settings

Zaključak

- Nikad nismo 100% zaštićeni
- Hakeri mogu iskoristiti svaku informaciju
- Bolje spriječiti nego liječiti
- Rizik se može umanjiti održavanjem kibernetičke higijene
- Tehnologija se razvija, a hakeri osmišljavaju nove metode svaki dan
- Zato moramo zaštititi sebe i svoje podatke
- Biti kibernetički siguran je stalni proces, učenje i usavršavanje...

www.carnet.hr

www.cert.hr

Kontakt:
ncert@cert.hr

Kontakt za prijavu incidenta:
incident@cert.hr

CARNET
CERT.hr
Odjel za Nacionalni CERT
Josipa Marohnića 5
10000 Zagreb
Hrvatska

Telefon: 01-666-1-650
Telefax: 01-666-1-767
