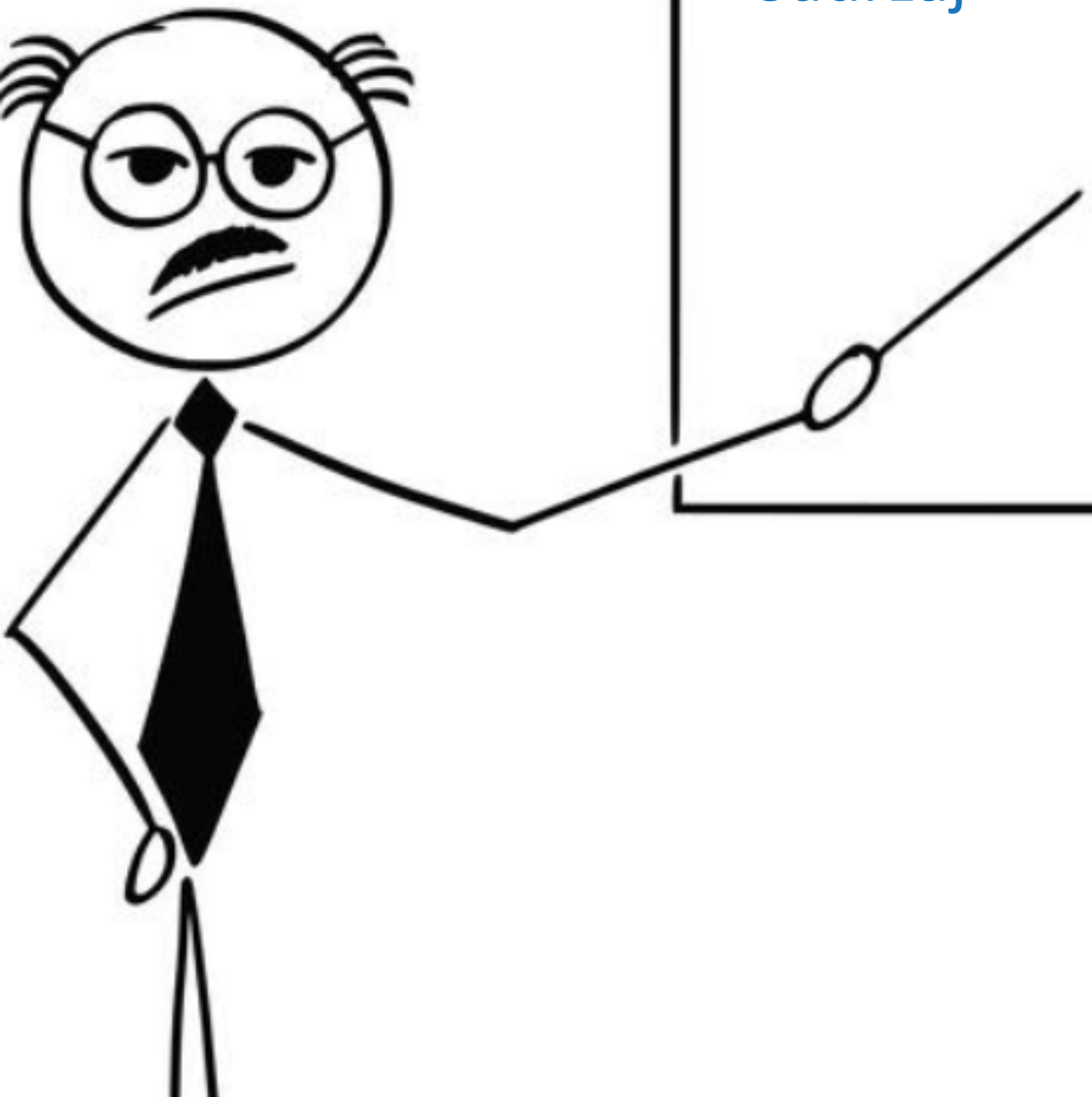
Što znači biti kibernetički siguran?

CARNET – Odjel za Nacionalni CERT

CERT.hr

Sadržaj



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 sustave 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 kojoj se može ući u trag.”

https://www.cert.hr/DIGTrag-InfoG

Osnovna načela informacijske sigurnosti

CIA

***C**onfidentiality*

(Povjerljivost)

***I**ntegrity*

(Cjelovitost)

***A**vailability*

(Dostupnost)

Povjerljivost

Otkrivanje informacija i podataka isključivo autoriziranim osobama.

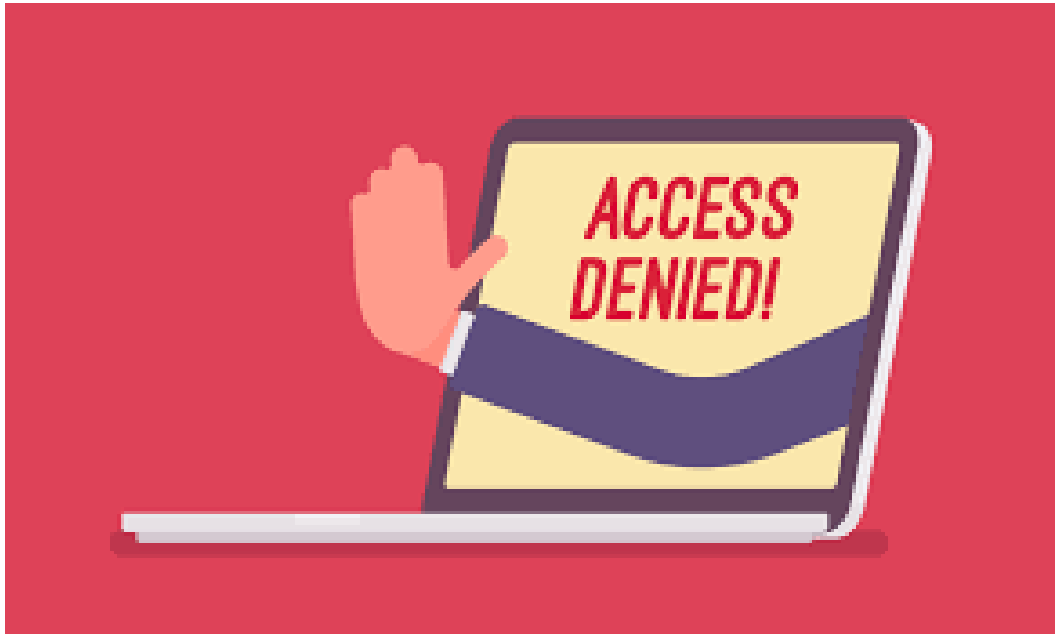
Cjelovitost

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.



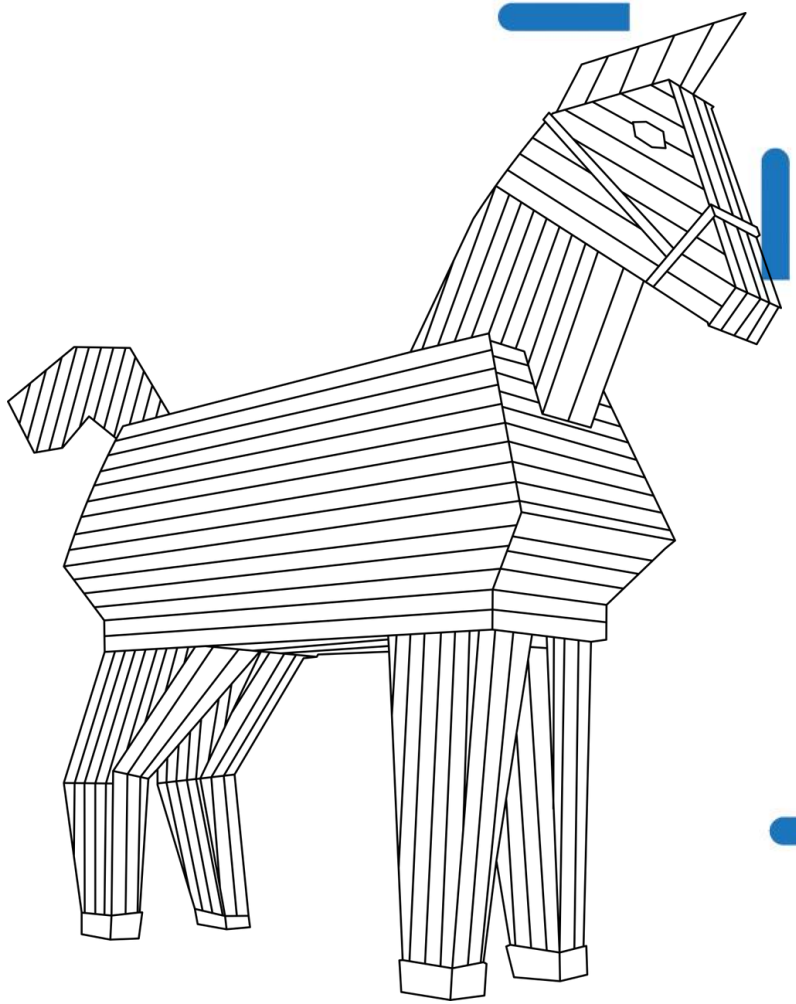
Hakiranje

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
- Zapisi o školovanju
- Zapisi o kažnjavanju
- Interni broj/oznaka zaposlenika
- Zapisi 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)

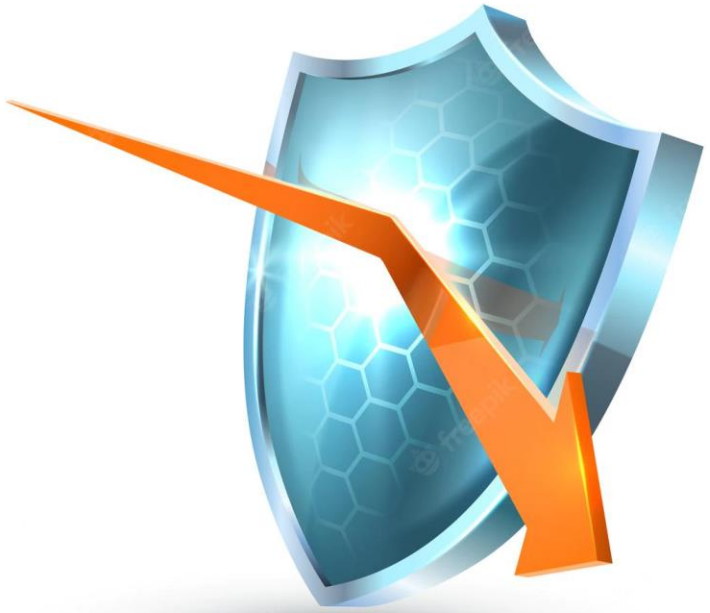
PODATCI O KORIŠTENJU KOJI NISU PROMETNI

- 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 zaštititi?



Kibernetička higijena

- set pravila
- sigurnosne prakse
- smjernice
- praktični postupci

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

1	2	3	4	A	B	C

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

Ne koristite riječi koje možete pronaći u bilo kojem rječniku

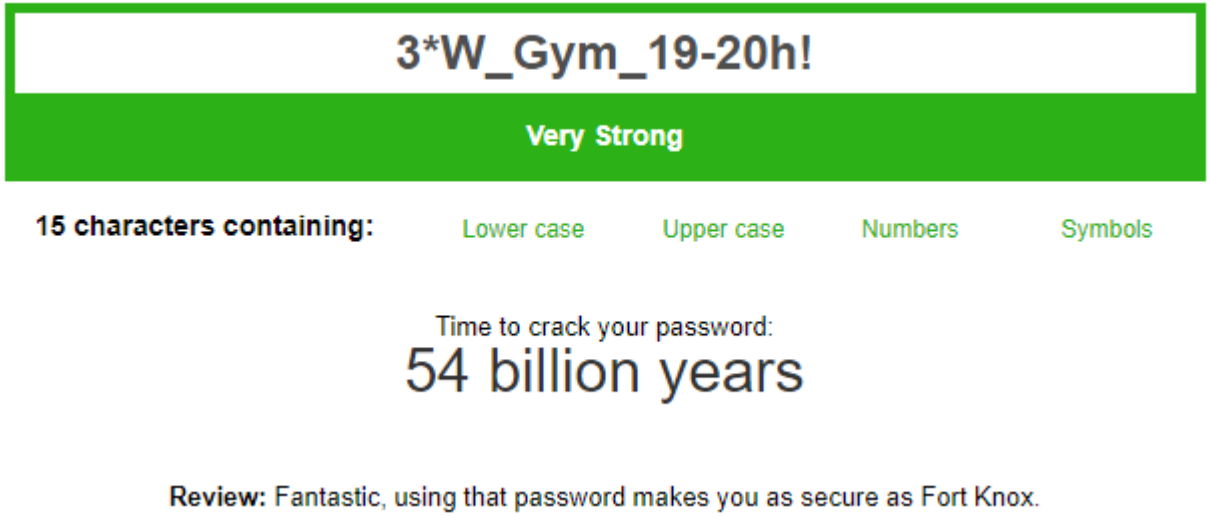
Tehnika stvaranja lozinke

- Primjer -

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

Lozinka:

3*W_Gym_19-20h!



Upravitelji za lozinke

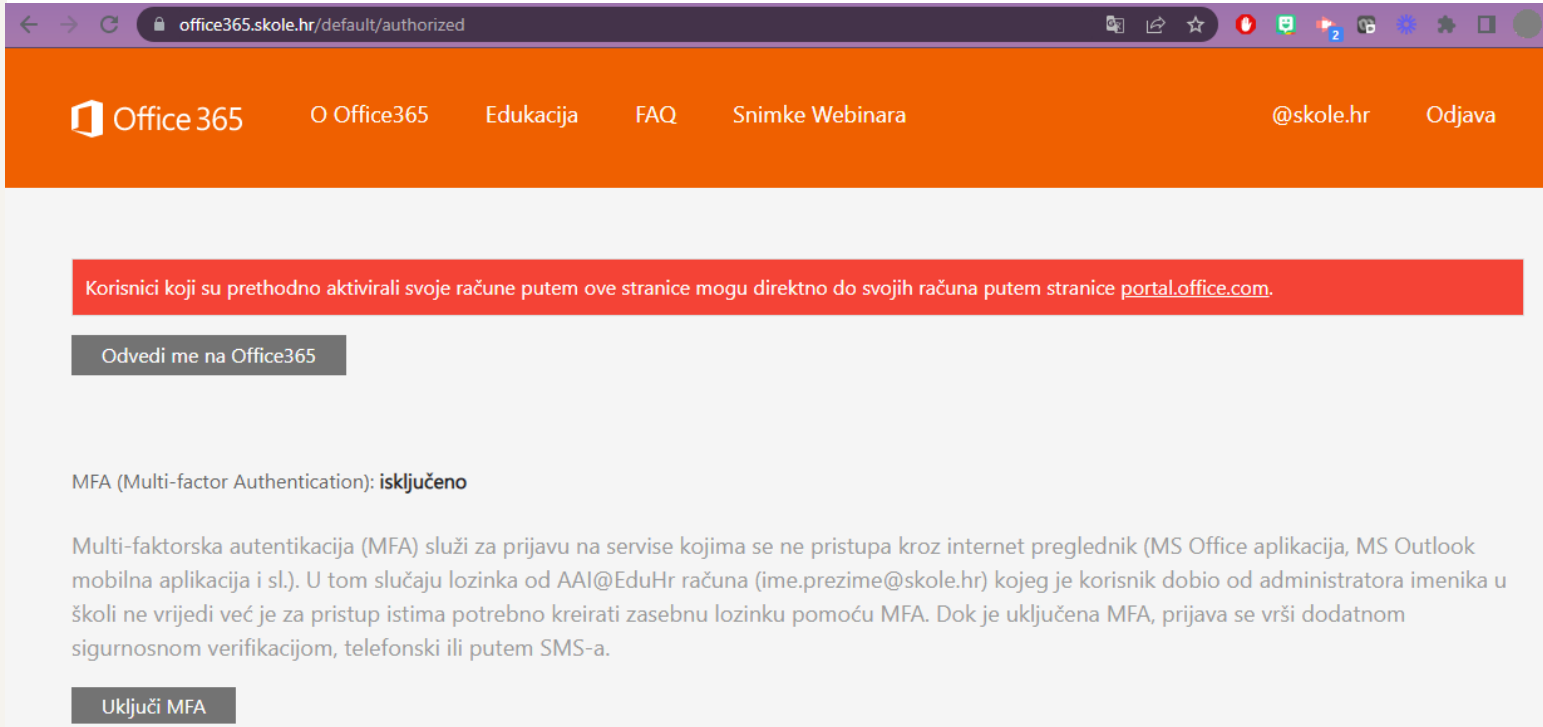
Prednosti:

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

Nedostaci:

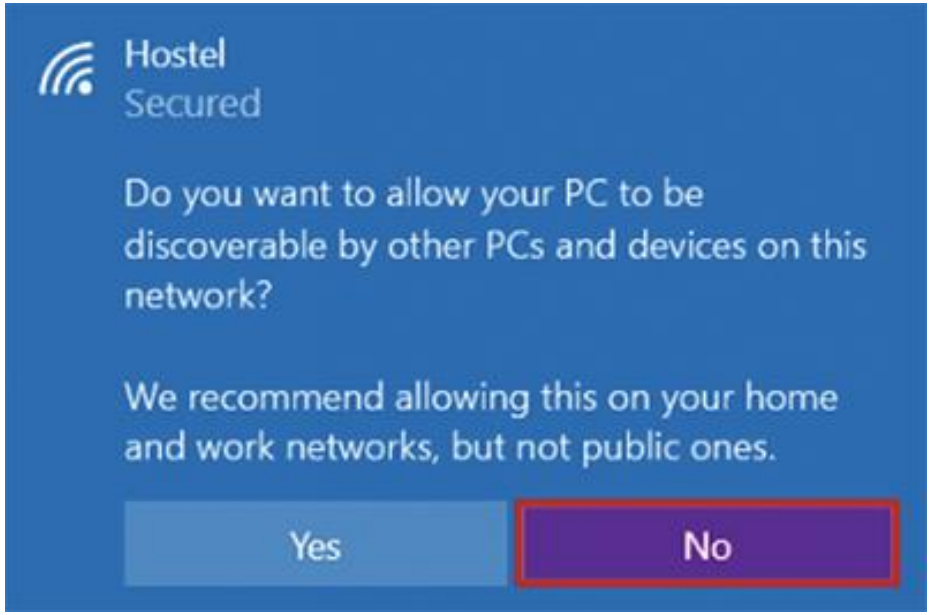
- Jedna lozinka za sve druge lozinke.
- Dobra lozinka nas ne štiti u potpunosti.
- Potrebno je njihovo postavljanje.

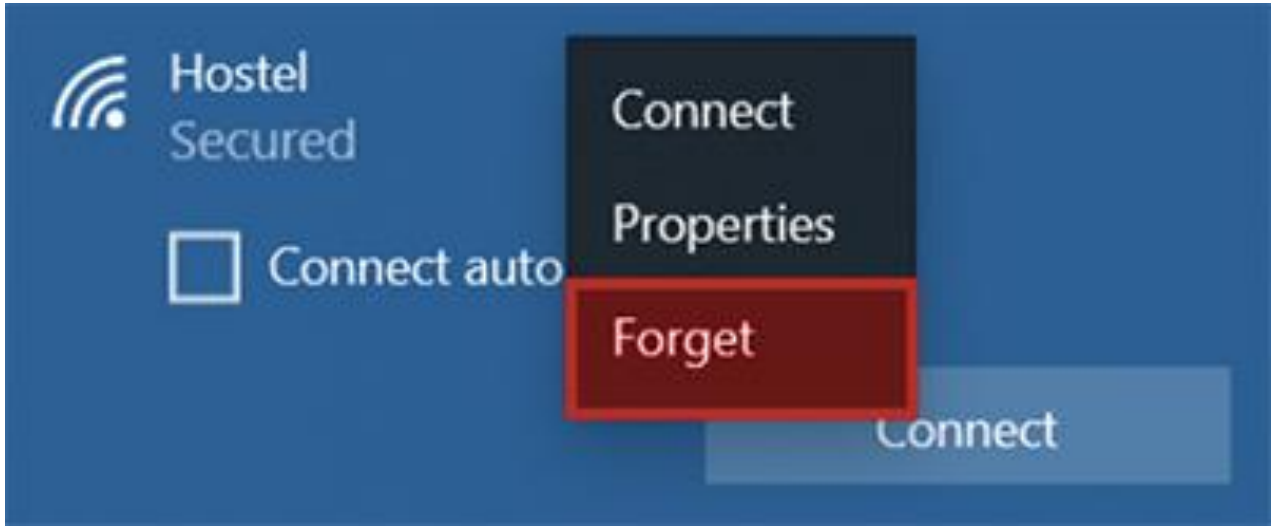
Dvofaktorska (2FA) i višestruka autentifikacija (MFA)!



Spajanje na Wi-Fi

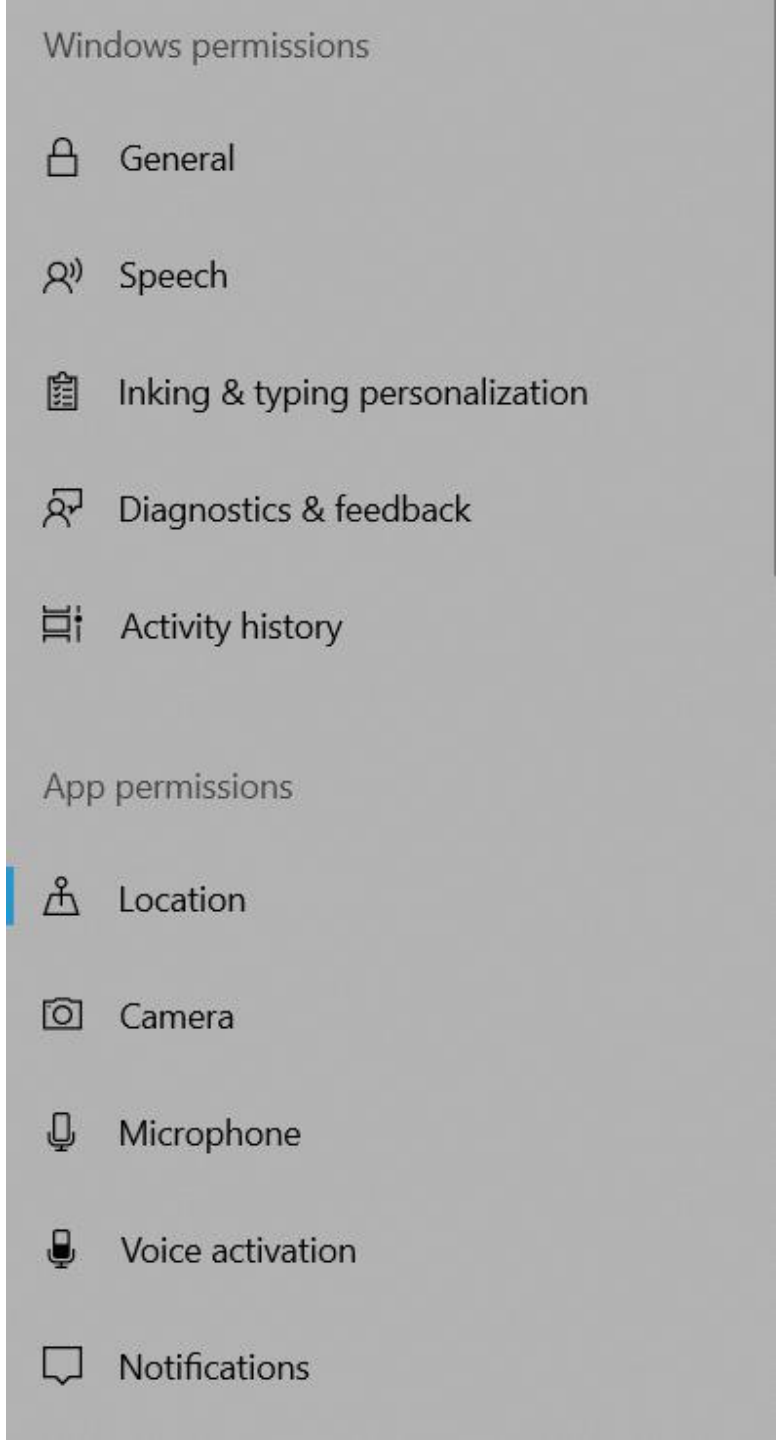
- Kućnom Wi-Fi-u promijeniti početnu lozinku.
- Ako je moguće izbjegavati spajanje na javni Wi-Fi.
- Kreiranje mobilne pristupne točke.
- Ako nema druge opcije nego spojiti se na javni Wi-Fi:
  - Označiti ga kao javni („*public*”) Wi-Fi i ne dopuštati da vas drugi uređaji mogu otkriti na toj mreži.
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





Dopuštenja aplikacijama

- Pazite koja dopuštenja dajete aplikacijama.
- Windows dopuštenja – dopuštenja sustavu.
- Dopuštenja aplikacijama (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.

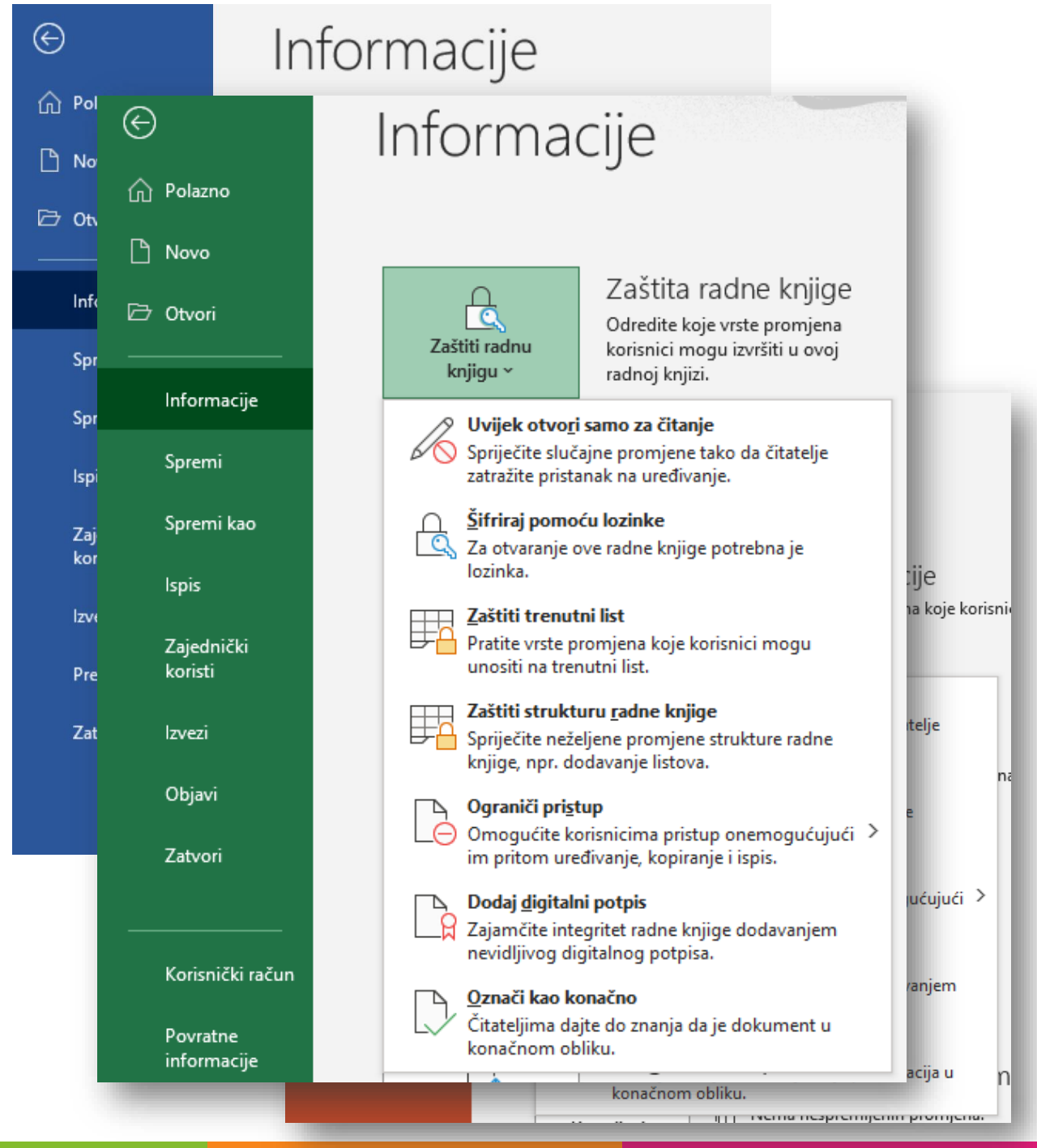
Zaštita digitalnih podataka

Zašto je potrebno zaštititi datoteke na računalu?

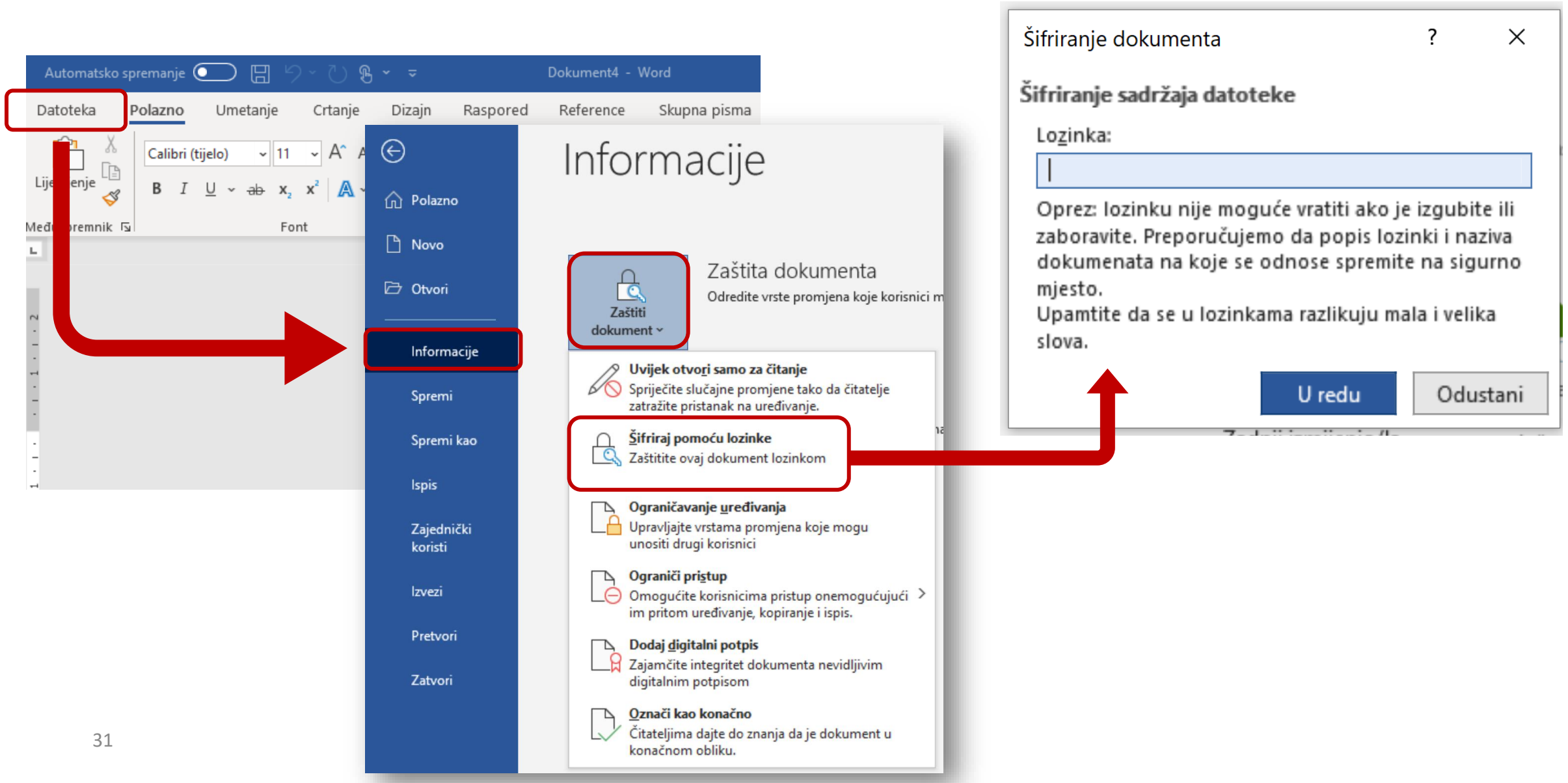
Zaštita Microsoft Office dokumenata

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

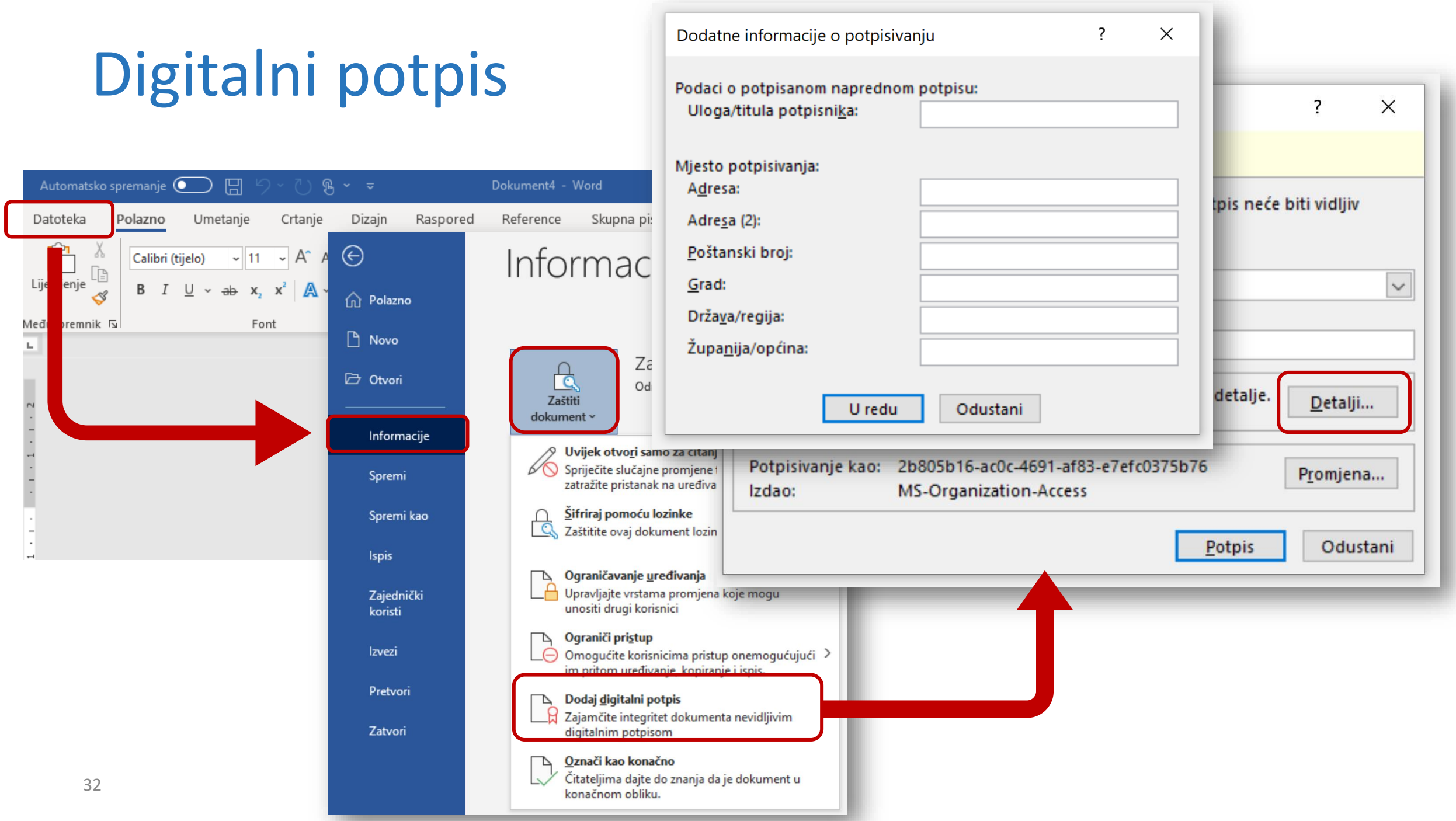
- šifriranjem pomoću lozinke
- ograničavanjem pristupa
- dodavanjem digitalnog potpisa



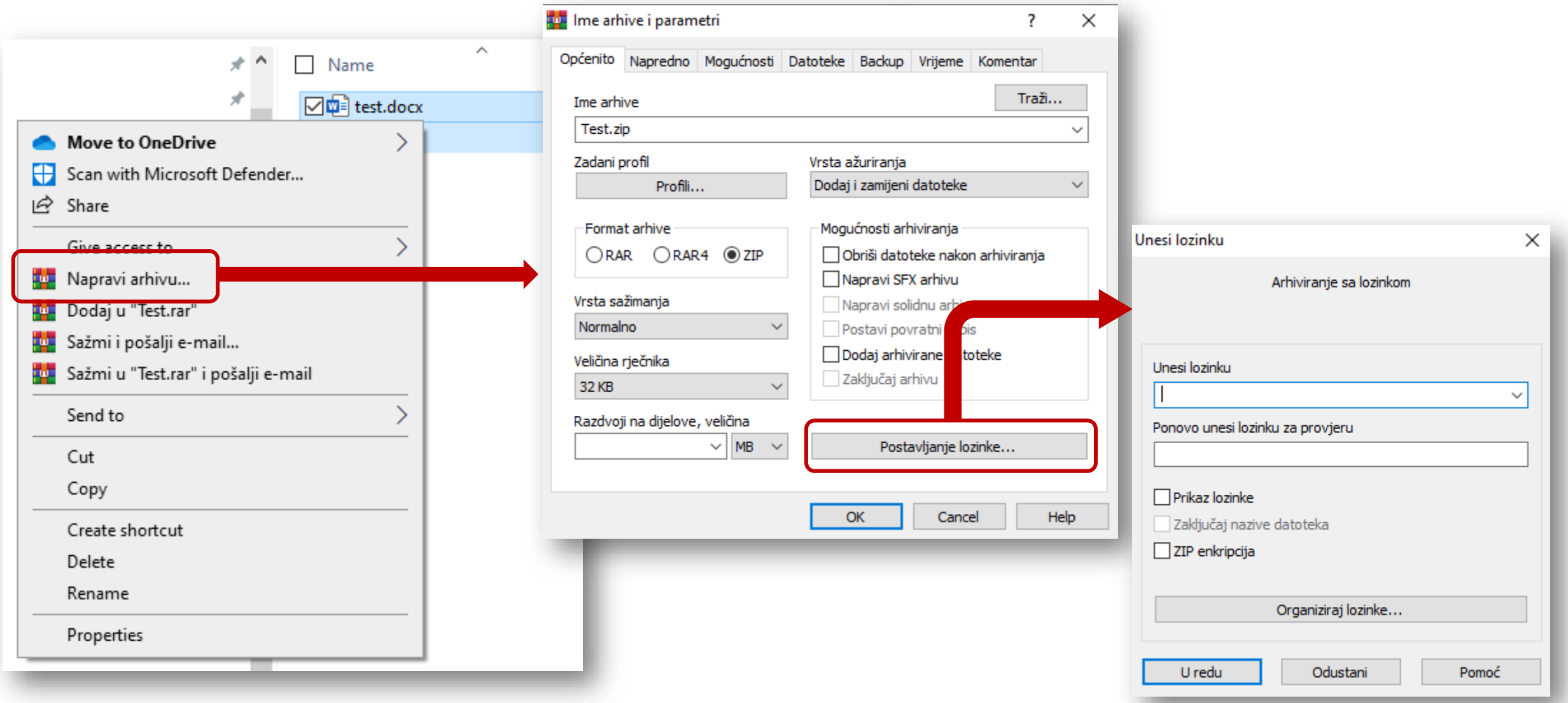
Šifriranje pomoću lozinke



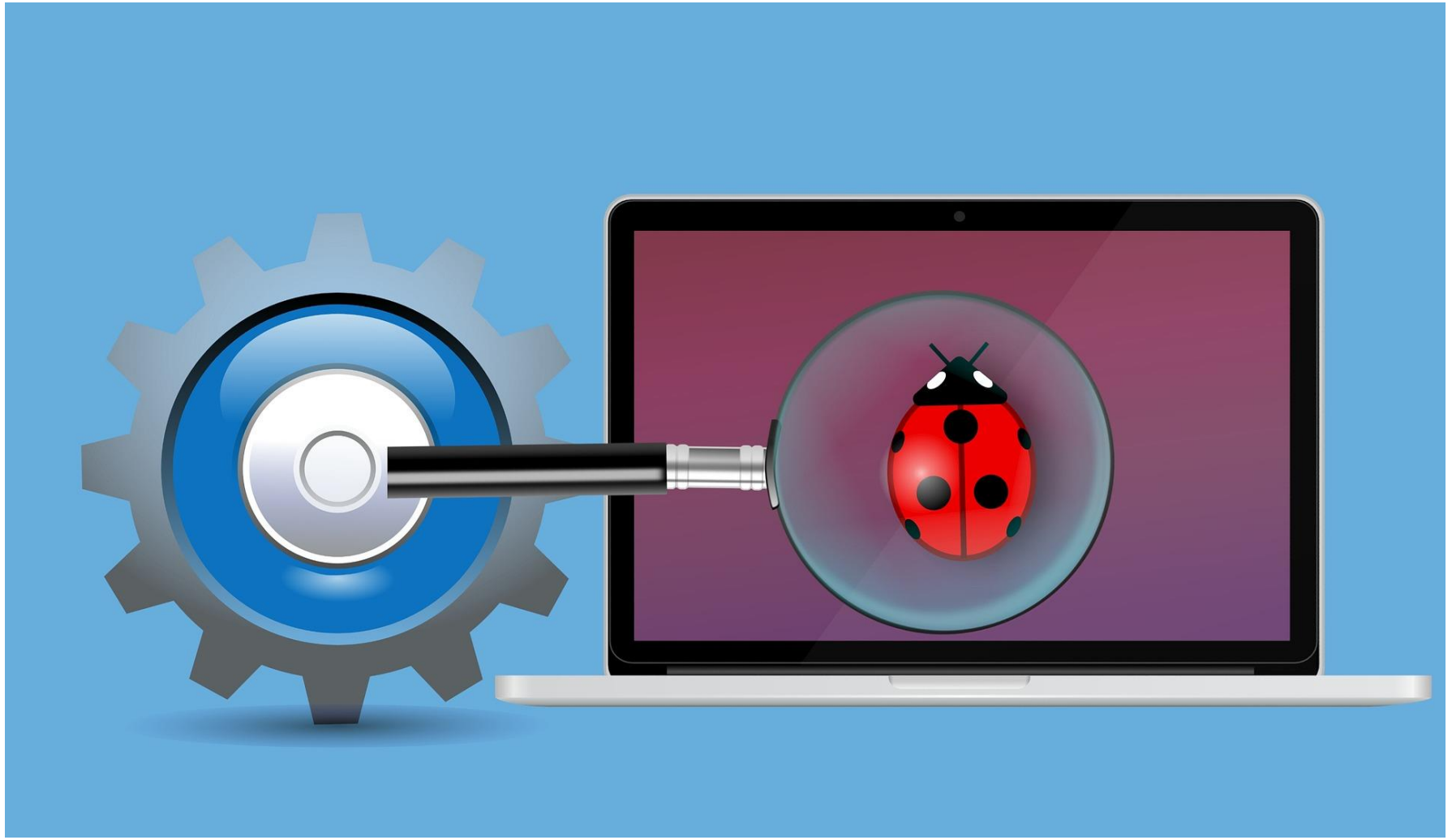
Digitalni potpis



Zaštita komprimiranih datoteka (*zip*)



Antivirusni programi



Najpopularniji u 2022. godini:

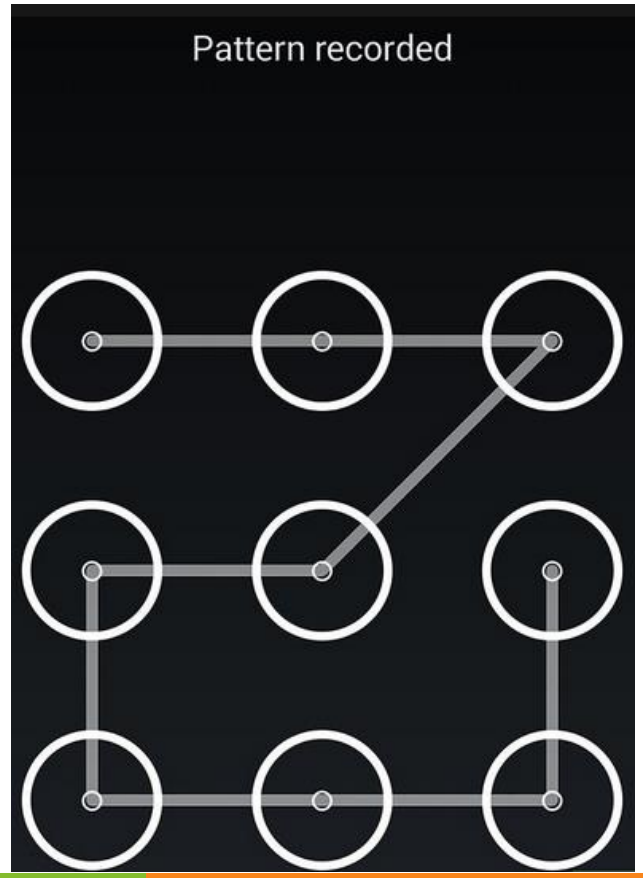
- Norton
- Bitdefender
- Intego
- TotalAV
- McAfee

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

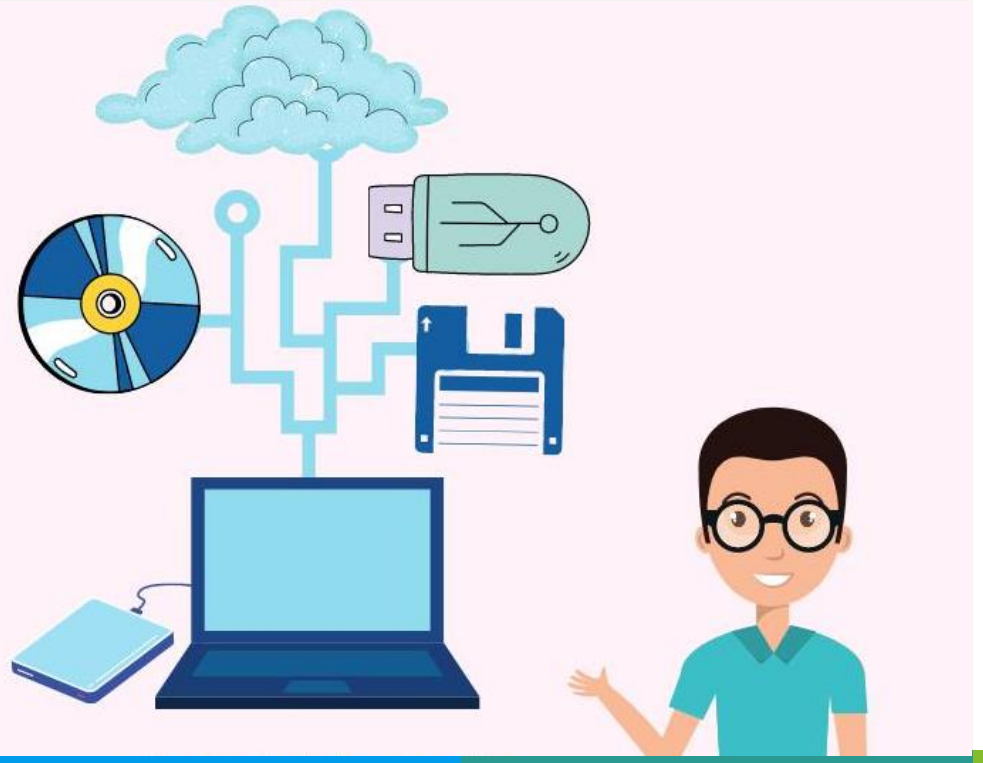
Zaključavanje uređaja

- 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.

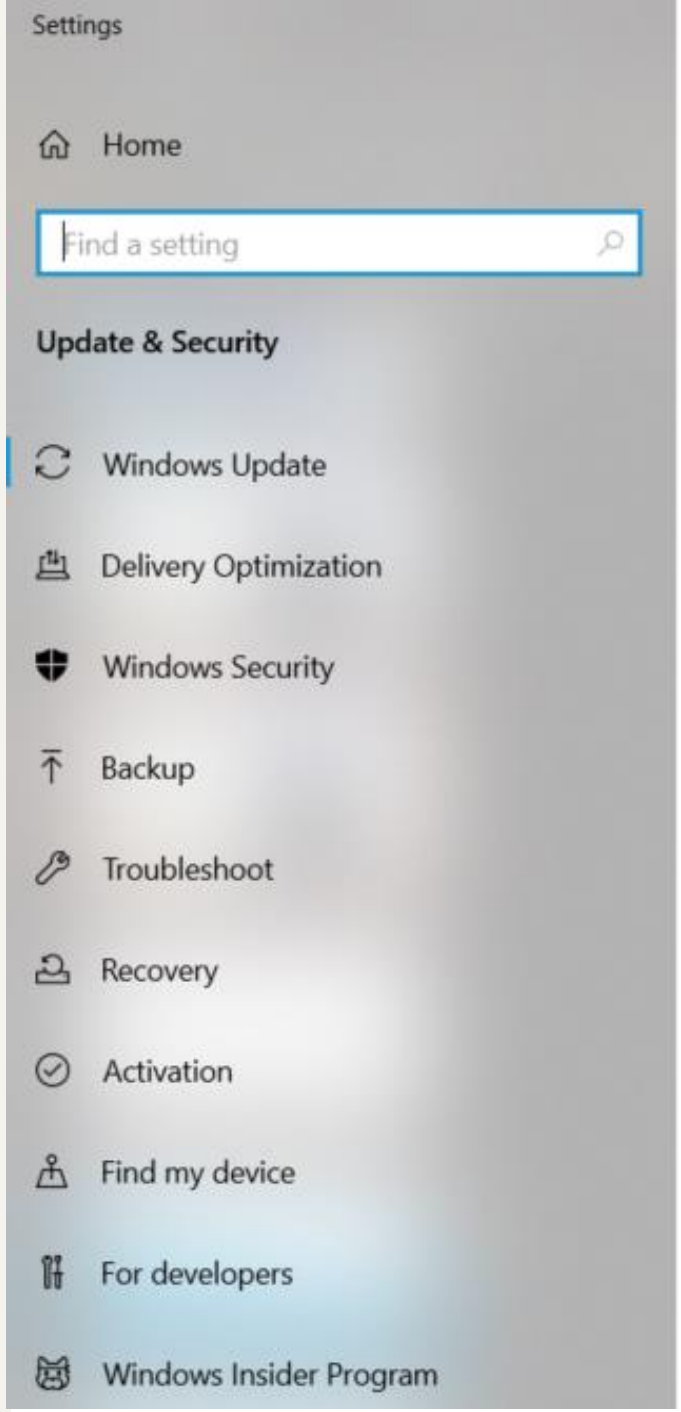
Pravilo 3-2-1:

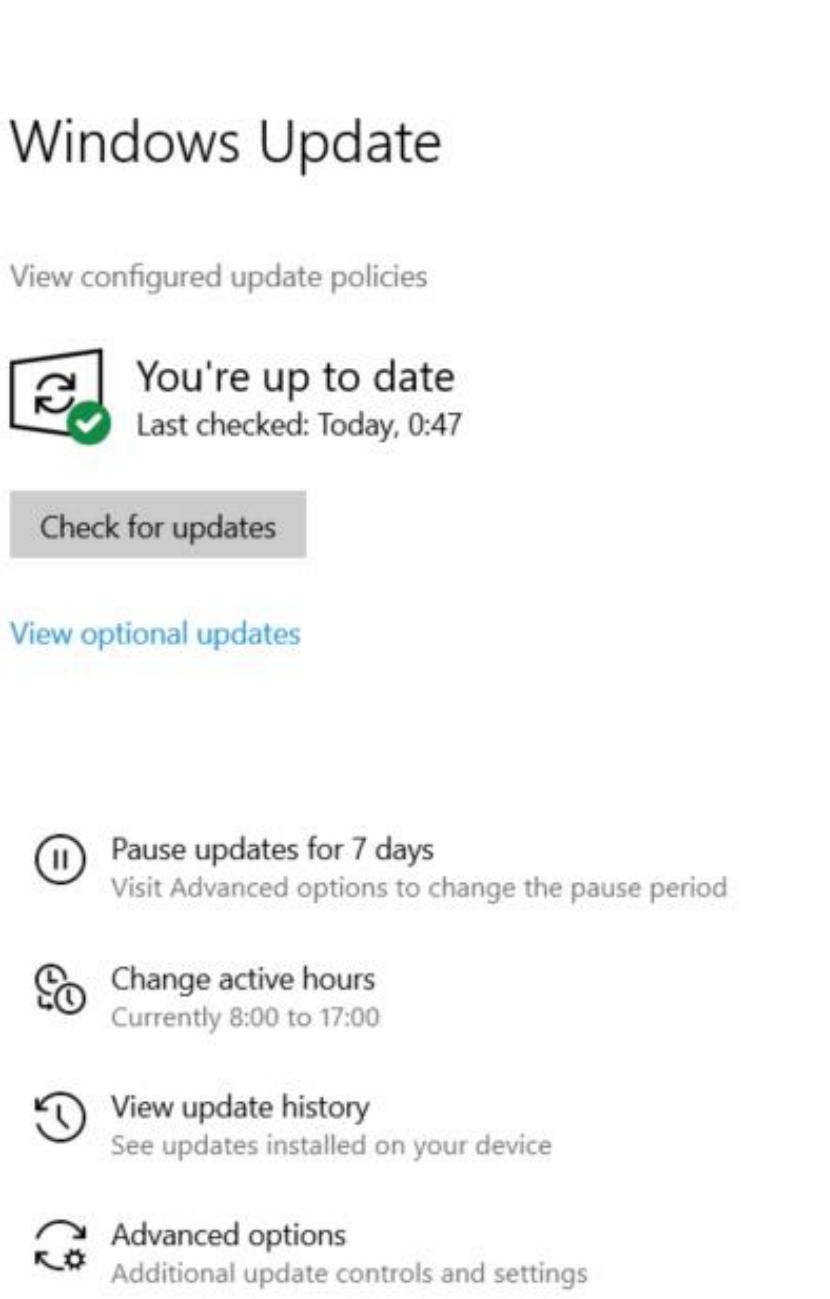
- 3 kopije
- 2 pohranjene na istoj lokaciji
- 1 pohranjena na drugoj lokaciji

Podaci vrijede više od uređaja na kojem su pohranjeni!

Ažuriranje softvera

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





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