Nacionalni CERT 15 godina u zaštiti kibernetičkog prostora Republike Hrvatske

CARNET – Odjel za Nacionalni CERT

Marina Dimić Vugec

Dan sigurnijeg interneta 2023. // 07.02.2023.

CARNET CERT.hr

Nacionalni CERT (CERT.hr)

- Nacionalni CERT (CERT.hr) je odjel Hrvatske akademske i istraživačke mreže – CARNET
- obrada računalno-sigurnosnih incidenata,
- podizanjem svijesti i edukacijom o kibernetičkoj sigurnosti građana Republike Hrvatske.

Nacionalni CERT (CERT.hr)

- 2007. osnovan u skladu sa **Zakonom o informacijskoj sigurnosti**
- odjel unutar Hrvatske akademske i istraživačke mreže – **CARNET**
- **Glavna zadaća CERT.hr-a:**
  - obrada incidenata ako je jedna od strana u **.hr domen**i ili u **hrvatskom IP adresnom prostoru** (osim tijela državne uprave→ **ZSIS CERT**)
- **Misija CERT.hr-a:** prevencija i zaštita od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj

15 godina djelovanja Nacionalnog CERT-a

- obradio više od 71 000 računalno-sigurnosnih incidenata
- obradio više od 42 000 abuse incidenata
- proveo više od 3000 provjera ranjivosti
- izdao više od 82 000 sigurnosnih upozorenja
- izdao oko 9000 elektroničkih certifikata
- objavio više od 3000 novosti
- objavio 900 recenzija alata
- objavio više od 200 stručnih dokumenata.

Kibernetička sigurnost

„Aktivnosti i mjere kojima se postiže sigurnost podataka i sustava u kibernetičkom prostoru.”

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.”

Akteri u kibernetičkoj sigurnosti

HAKER (White hat/Grey hat/Black hat)

HAKERSKE SKUPINE

- organizirani kriminal,
- najčešće motivirane novčanom dobiti

DRŽAVNO POTPOMOGNUTE SKUPINE

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

CERT.hr


Digitalni trag
Svjesno i namjerno ponašanje, aktivnosti, akcije, objave i komunikacije putem interneta i digitalnih uređaja
(ne)zgodne fotografije (odmor, zabava, prijatelji, obitelj)
objave na društvenim mrežama
akcije koje poduzimamo unutar neke online usluge ili platforme
komentari ispod nekog video zapisa ili novosti na nekom portalu
sve promjene koje možemo napraviti na nekom dokumentu
sve javno dostupne informacije o nama
Tko prati naš digitalni trag?
marketinške kuće
poslodavci
online trgovine
prijatelji i neprijatelji
...
Kako?
Zašto nas prate?
Naši interesi
Lokacije
Hobiji
Teme
Društvo
Aktivnosti
Informacije
Stavovi
Navike...
Prvo provjeri sastojke kolačića!
Odjavi se iz svih profila!
Napravi popis svih korisničkih imena!
Guglaj brojeve telefona!
Guglaj slike!
Postoje i druge tražilice. Potraži se i putem njih!
Guglaj se! Provjeri svoj digitalni trag!
Digitalni trag - moj saveznik
Istražite sebe
Razmišljajte prilikom objavljivanja
Podesite svoje postavke privatnosti
Pažljivo upravljajte svojim korisničkim računima
Koristite više adresa elektroničke pošte
Koristite online servise za zaštitu podataka
Izgradite svoju reputaciju ponašanjem
Imate pravo na zaborav
CARNET CERT.hr

DIGITALNI TRAGOVI

- Svjesno i namjerno ponašanje, aktivnosti, akcije, objave i komunikacije putem interneta i digitalnih uređaja

ŠTO ostavljamo:

- Fotografije i video sadržaji
- Objave na društvenim mrežama
- Akcije koje poduzimamo na online uslugama
- Komentari
- Promjene na dokumentima

https://www.cert.hr/aktivnosti/certhrecsm/certhrecsm2020/

SAVJETI – DIGITALNI TRAG – MOJ SAVEZNIK

- Istražite sebe
- Dobro razmisli prije nego što nešto objaviš na mrežama
- Podesite svoje postavke privatnosti
- Pažljivo upravljajte svojim korisničkim računima
- Možda će ti nekada biti neugodno zbog nečeg što ti je danas simpatično
- Sve što objaviš svatko može kopirati i tako se informacija širi velikom brzinom
- Ako i obrišeš nešto što nije primjereno, to ne znači da je nestalo s interneta
- Analizirajući tvoje digitalne tragove svatko može steći mišljenje o tebi
- Pazi na svoj digitalni ugled
- Imate pravo na zaborav

Imate pravo na zaborav!

Phishing i kako ga prepoznati

Phishing prijevare

Smishing

Spearphishing

Vishing

Catphishing

Whaling

Istražitelj za kibernetičku sigurnost (CSI)

CARNET CERT.hr

6 SAVJETA ZA OTKRIVANJE ZLONAMJERNIH E-PORUKA

LAŽIRANO POLJE POŠILJATELJA

Usporedite prikazano ime i stvarnu adresu e-pošte. Varalice se često lažno predstavljaju.

DRAGI PRIJATELJU

Općeniti pozdravi, koji nisu upućeni izravno vama znak su za oprez.

UPLATI MI NEŠTO NOVCA

Neka vam odmah bude sumnjivo ako netko od vas traži prijenos novca.

PODACI O BANKOVNOM RAČUNU

Budite oprezni ako se e-porukom traže privatni podaci.

<pošiljatelj> <Vedran Vedrić> **<tmurnilazov@lazz.xyz>**

<primatelj> <Ja> **<moj@mymail.xyz>**

ODGOVORI | ODGOVORI SVIMA | PROSLIJEDI

DRAGI PRIJATELJU,

molim te, **uplati mi nešto novca.**
Za to su mi prvo potrebni **podaci o bankovnom računu**. Zbog sigurnosnih razloga još moraš **resetirati lozinku** svoje e-pošte. Više informacija pronaći češ **ovdje.**

Pozdrav,

Vedran.

RESETIRATI LOZINKU

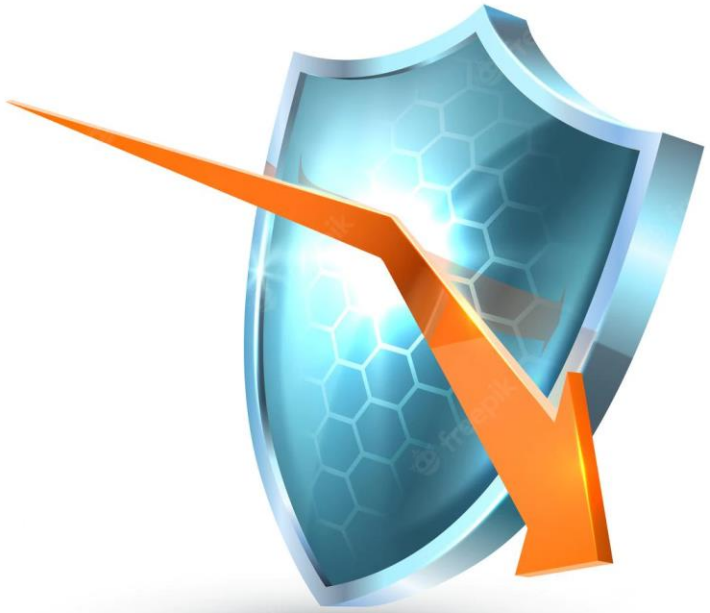
Ne nasjedajte na ničim izazvan zahtjev za resetiranje vaše lozinke.

OVDJE

Poveznicu uvijek provjerite tako da preko nje prijeđete mišem, bez klikanja.

#ThinkB4UClick

Kako se zaštititi?



Kibernetička higijena

- set pravila
- sigurnosne prakse
- smjernice
- praktični postupci

Dobra lozinka

Najmanje 16 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

*preporuka – koristite dvofaktorsku autentifikaciju

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

*preporuka – ne spremajte lozinke u pregledniku

Upravitelji za lozinke

Prednosti:

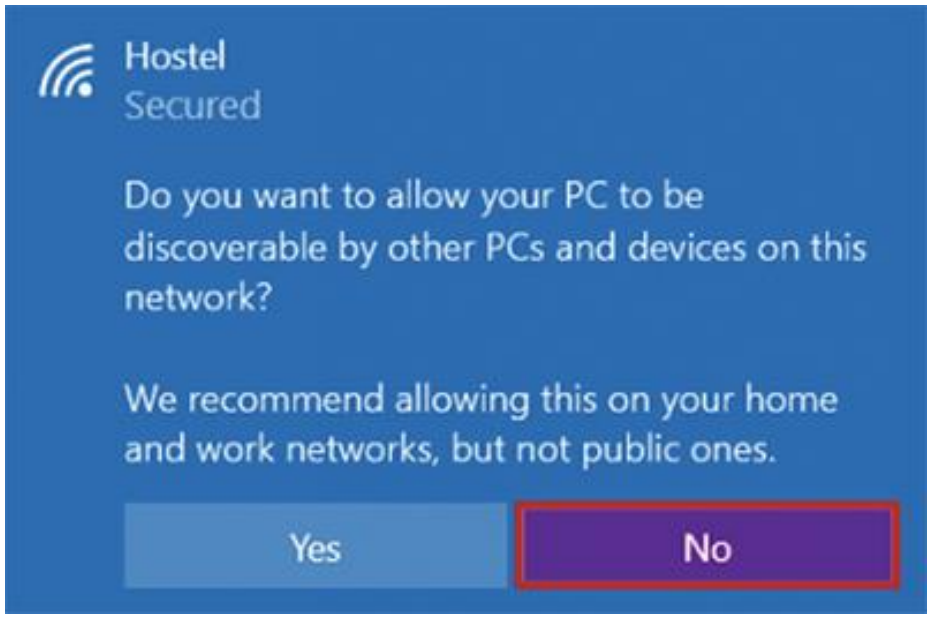
- Jedna lozinka za sve druge lozinke.
- Automatsko stvaranje snažne lozinke.
- Možete imati različite lozinke za svaki račun, a ne morate ih pamtiti.

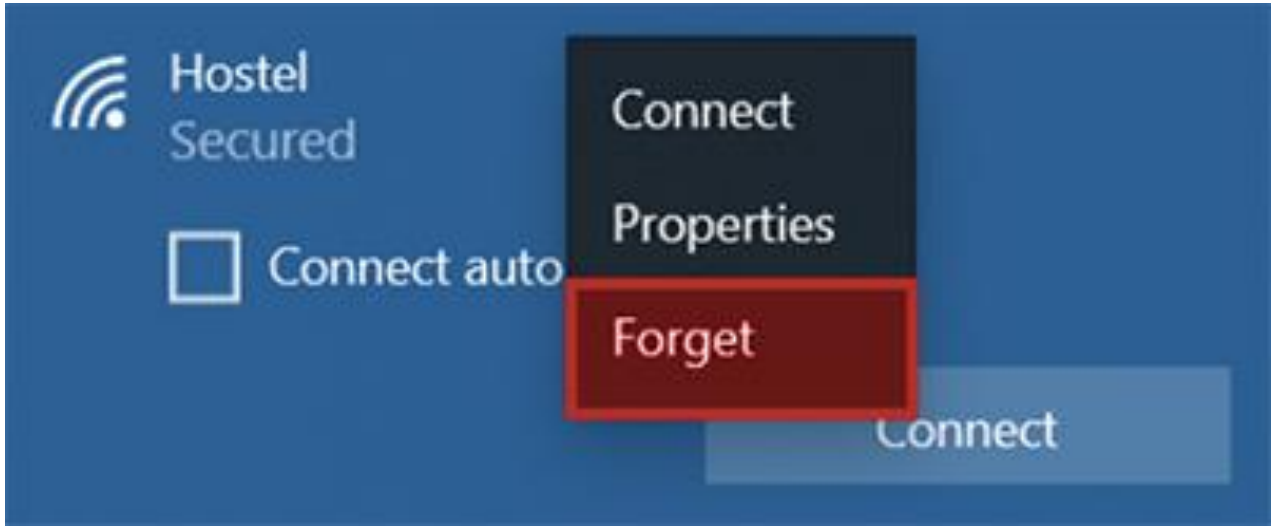
Nedostaci:

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

Spajanje na Wi-Fi

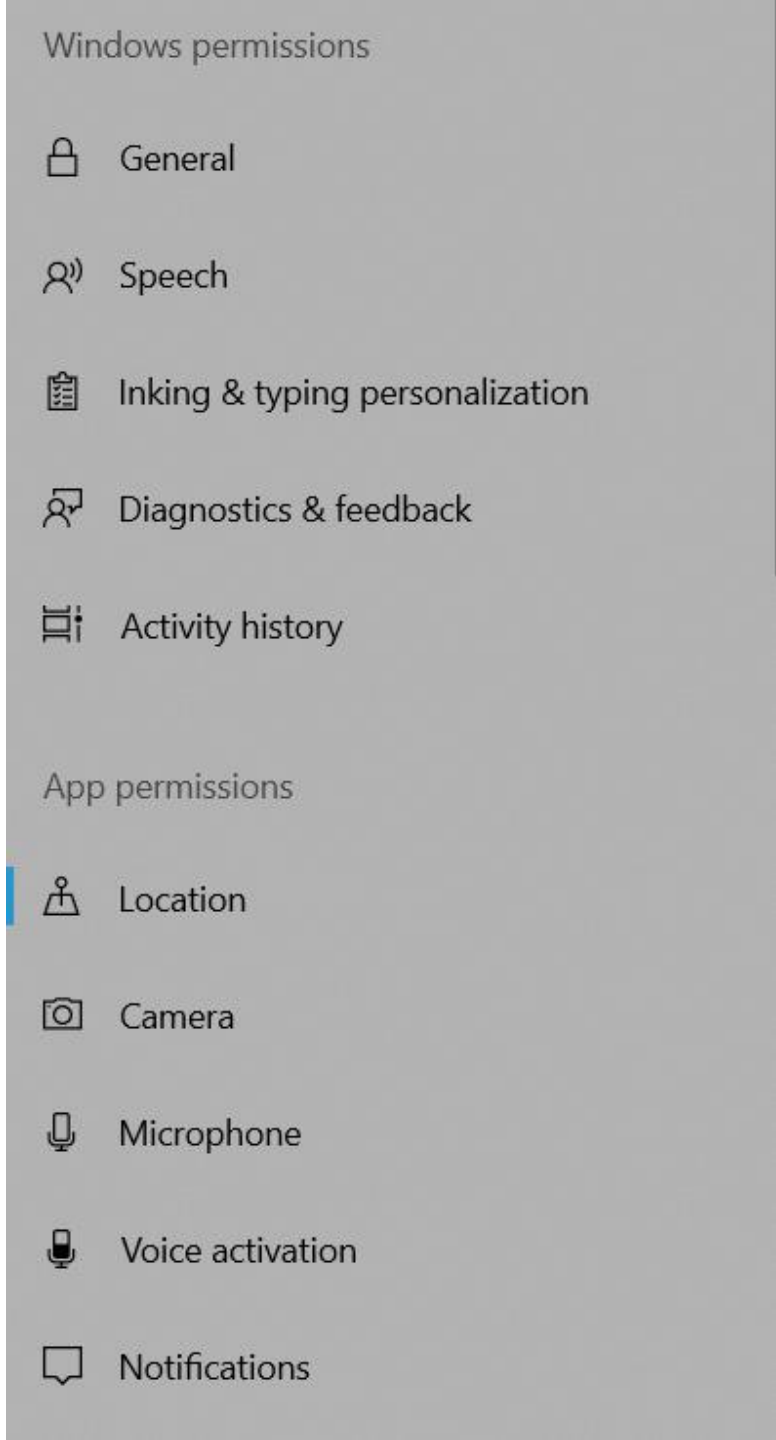
- Kućnom Wi-Fi-u promijeniti početnu lozinku.
- Ako je moguće izbjegavati spajanje na javni Wi-Fi.
- Kreiranje mobilne pristupne točke.
- Ako nema druge opcije nego spojiti se na javni Wi-Fi:
  - Označiti ga kao javni („*public*”) Wi-Fi i ne dopuštati da vas drugi uređaji mogu otkriti na toj mreži.
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

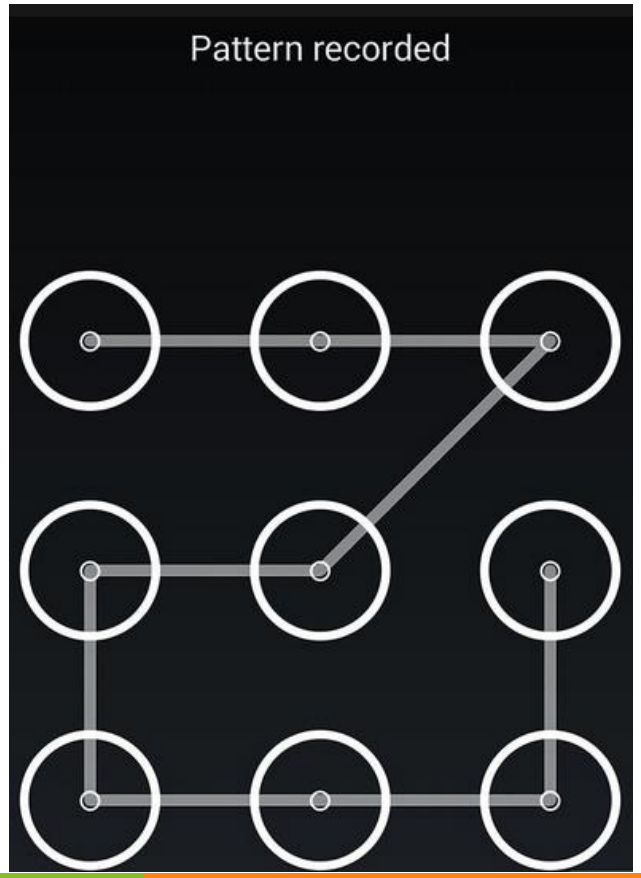
Surfanje u anonimnom prozoru preglednika?

- 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.

Zaključavanje uređaja

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



Društvene mreže

Društvene mreže su izvor

- krađe identiteta
- krađe osobnih/bankovnih podataka
- cyberbullying
- neprimjerenog sadržaja
- ovisnosti
- nepoznate osobe
- (ne)privatnosti
- phishinga i drugih prijevara
- lažnih online trgovina
- dječje pornografije
- lažnih vijesti

Dobna granica

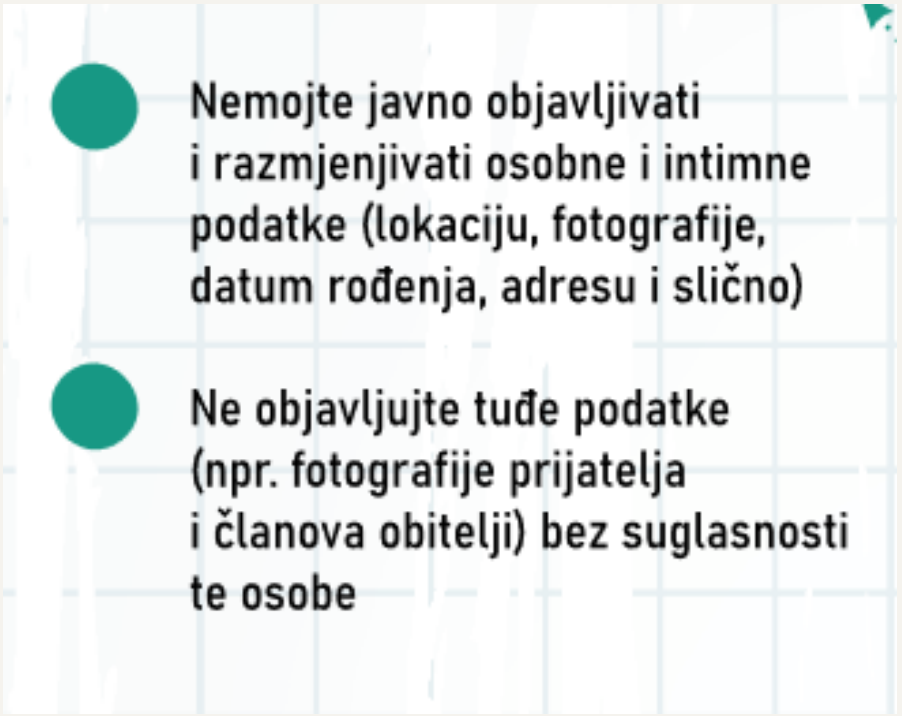
- Facebook
- Twitter
- Instagram
- Youtube
- Snapchat
- TikTok

13 godina

Kako prepoznati lažni profil

- istražite profil
- profilna slika
- datum prve objave
- prijatelji/pratitelji
- logika profila (godine/radno mjesto)
- potražite informacije o osobi drugim kanalima
- budite sumnjičavi u komunikaciji
- blokirajte/prijavite

Sigurnosne prakse



- Održavajte kibernetičku higijenu
- Provjerite postavke sigurnosti i privatnosti
- Čitajte uvjete i pravila upotrebe
- Ne prihvaćajte zahtjeve nepoznatih osoba
- Ne klikajte na sumnjive poveznice
- Prijavite sumnjive aktivnosti
- Društvene mreže izvor su podataka za socijalne inženjere

Provjerite je li vaš mail kompromitiran

https://**haveibeenpwned**.com

www.carnet.hr

www.cert.hr

Kontakt:
ncert@cert.hr

Kontakt za prijavu incidenta:
incident@cert.hr

Kontakt za upite medija:
press@carnet.hr

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

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