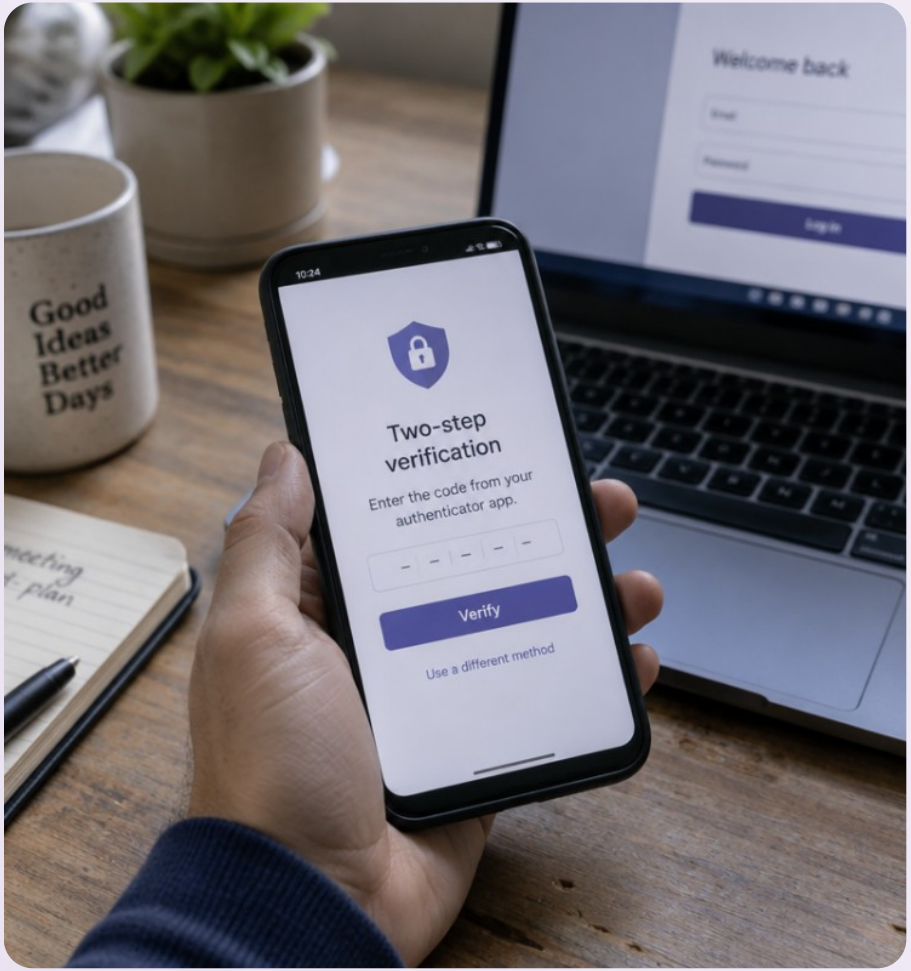
Zaštita elektroničkog identiteta

Kako sigurno čuvati svoje podatke i profile na internetu



Tko sve koristi tvoje ime?

Zamislite da netko uđe u vaš profil na društvenoj mreži i pošalje uvredljive poruke prijateljima ili nastavnicima u vaše ime.

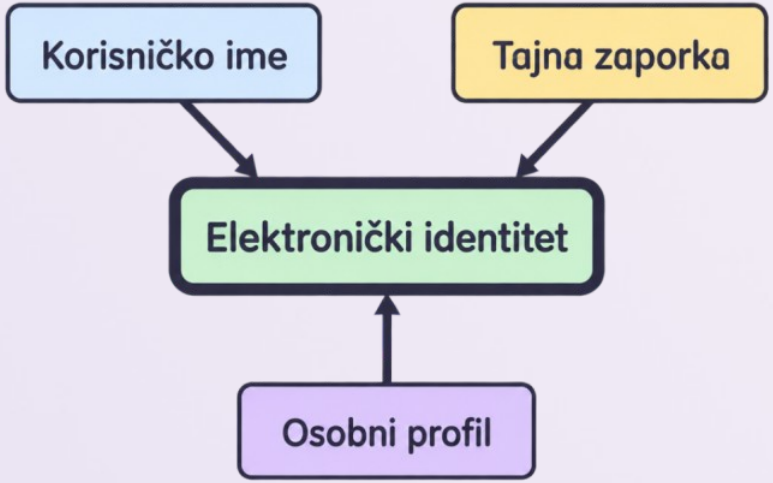
U digitalnom svijetu računalo prepoznaje samo **korisničke podatke**, a ne vaše lice. Ako netko sazna vaše podatke za prijavu, preuzima vaš cjelokupni elektronički identitet!



Što je elektronički identitet?

Elektronički identitet skup je podataka kojima dokazujemo tko smo na mreži

- **Korisničko ime**: javni naziv računa (npr. u školi AAI@EduHr).
- **Lozinka / zaporka**: tajni niz znakova poznat samo vama.
- **Digitalni tragovi**: povijest prijava, e-pošta i aktivnosti.



Opasnost: Krađa identiteta

Krađa identiteta događa se kada neovlaštena osoba dođe u posjed vaših pristupnih podataka i koristi ih bez vašeg znanja.

⚠ **Posljedice preuzimanja profila**

Napadač u vaše ime može slati zlonamjerne poruke, trošiti novac ili trajno izbrisati vaše školske radove.



Pravila za stvaranje jake zaporke

Duljina i raznolikost

Zaporka mora sadržavati najmanje 10 znakova uz kombinaciju velikih i malih slova, brojeva i posebnih znakova poput `#` ili `!`.

Izbjegavanje rječnika

Nikada ne koristite uobičajene riječi, imena članova obitelji, ljubimaca, datume rođenja ili nizove poput "123456".

Metoda rečenice

Osmislite rečenicu: *"Moj pas ima tri mjeseca i zove se Beni!"* te uzmite prva slova: **Mpi3mizsB!**

🧠 **Pravilo čuvanja**

Zaporke nikada ne dijelite s prijateljima – jedine osobe koje ih smiju znati su vaši roditelji ili skrbnici.

Dvostruka autentifikacija (2FA)

Dvostruka autentifikacija postupak je kojim se uz lozinku provjerava vaš identitet putem još jednog sigurnosnog koraka.

1. **Prvi faktor**: Unosite svoje korisničko ime i zaporku.
1. **Drugi faktor**: Unosite jednokratni kod poslan SMS-om ili stvoren u aplikaciji na mobitelu.

Čak i ako netko ukrade vašu zaporku, bez vašeg mobitela ne može ući u račun!



Provjera znanja o zaporkama

Koji je od navedenih primjera najsigurnija zaporka prema pravilima zaštite?

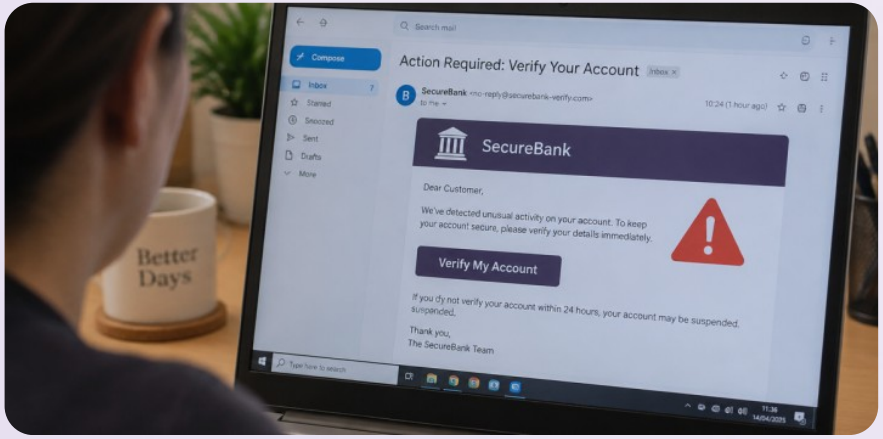
1. zagrebcroatia
2. marko2011
3. Vl#89kM!p2
4. lozinka123

Provjera znanja o zaporkama

Koji je od navedenih primjera najsigurnija zaporka prema pravilima zaštite?

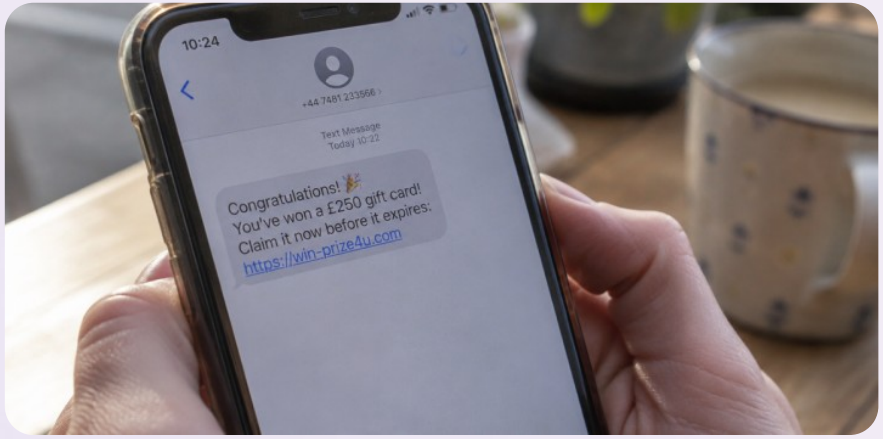
1. zagrebcroatia
2. marko2011
3. Vl#89kM!p2 ✓
4. lozinka123

Socijalni inženjering i krađa podataka



Lažno predstavljanje (Phishing)

Poruke e-pošte ili SMS-ovi koji oponašaju banke, škole ili društvene mreže kako bi vas naveli na unos podataka.



Manipulacija ljudima

Napadač ne probija zaštitu silom, već iskorištava lakovjernost, strah ili radoznalost korisnika nudeći lažne nagrade.

Prepoznavanje lažnih mrežnih stranica



HTTPS protokol i lokot

Sigurne stranice započinju oznakom *https://* i imaju ikonu lokota koja potvrđuje šifrirani prijenos podataka.



Provjera vršne domene

Prevaranti mijenjaju slova domene (npr. umjesto službene adrese *snapchat.com* upotrijebe *snapchat.net*).



Gramatičke pogreške

Lažne stranice često sadrže loš automatski prijevod, neobičan red riječi i gramatičke greške u tekstu.



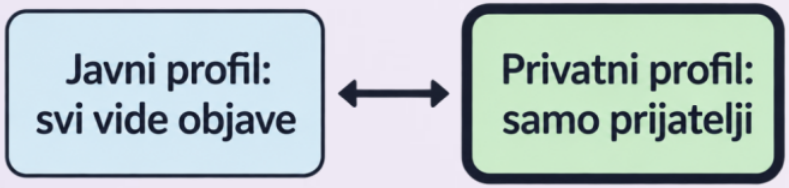
Lažne humanitarne akcije

Prevare koje traže hitne uplate za bolesne ili nagrade iziskuju uplatu na nepoznati privatni račun.

Postavke privatnosti profila

Pri registraciji na društvene mreže profil je često automatski postavljen kao **javan**. Svatko na internetu može vidjeti vaše objave i slike!

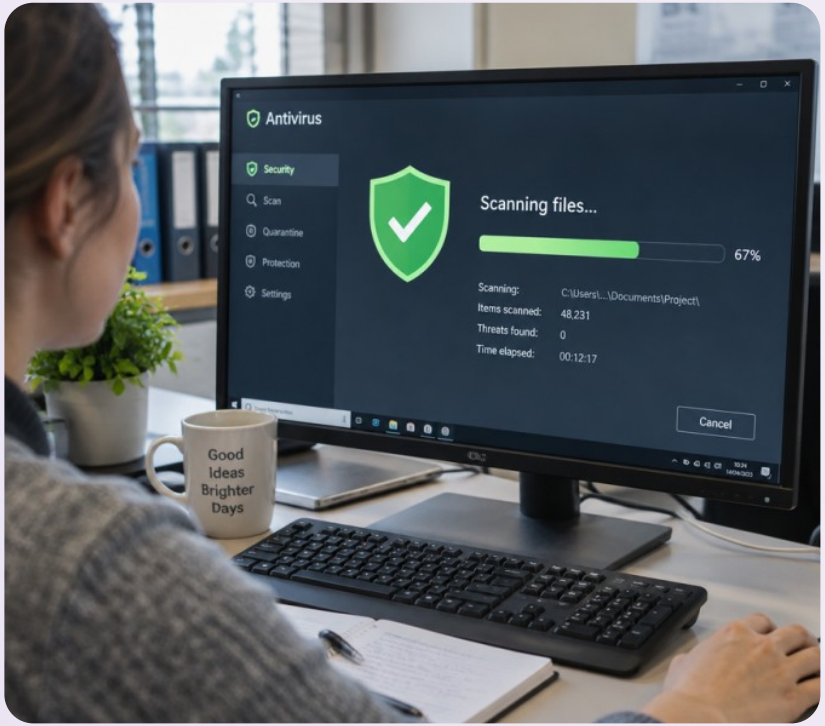
- Postavite profil na **privatno** kako bi vas pratili samo odobreni prijatelji.
- Isključite označavanje lokacije na fotografijama.
- Ne prihvaćajte zahtjeve za prijateljstvo od nepoznatih osoba.



Uloga antivirusnih programa

Antivirusni programi služe za zaštitu računala od štetnog djelovanja zlonamjernih programa koji pokušavaju otuđiti podatke.

- **Ugrađena zaštita**: Operacijski sustav Windows sadrži Windows Defender.
- **Vanjski alati**: Programi poput Norton, Kaspersky, AVG ili Avast nude dodatne provjere.
- **Redovito ažuriranje**: Antivirus je učinkovit samo ako redovito preuzima nove baze prijetnji.



Četiri zlatna pravila zaštite

1. **Stvaraj jake zaporke** i nikada ih ne dijeli s prijateljima.
2. **Uključi dvostruku autentifikaciju** za sve važne račune i profile.
3. **Provjeravaj mrežnu adresu (URL)** i traži oznaku lokota (HTTPS).
4. **Ne otvaraj sumnjive poveznice** pristigle u porukama ili e-pošti.

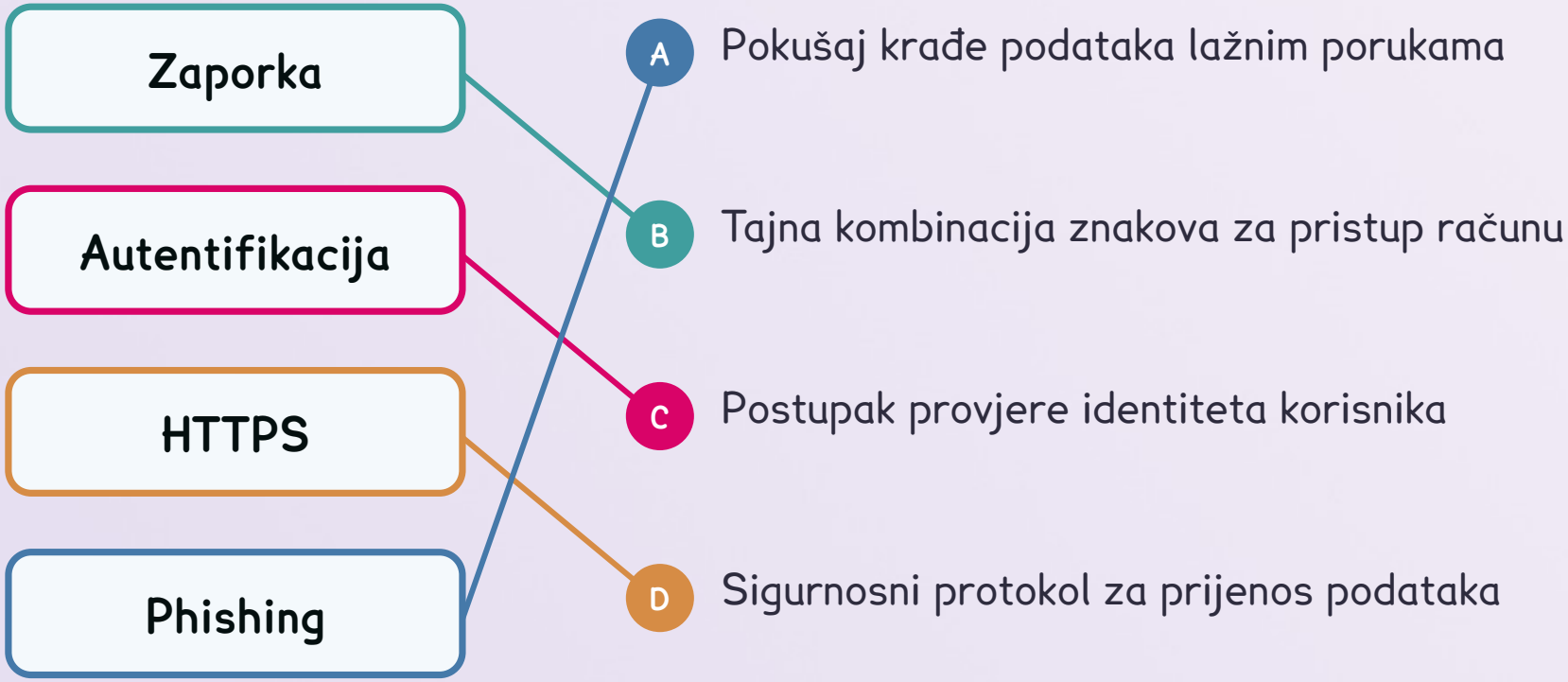
Povezivanje ključnih pojmova

Poveži riječi s definicijama

Zaporka	Pokušaj krađe podataka lažnim porukama
Autentifikacija	Tajna kombinacija znakova za pristup računu
HTTPS	Postupak provjere identiteta korisnika
Phishing	Sigurnosni protokol za prijenos podataka

Povezivanje ključnih pojmova

Poveži riječi s definicijama



Rasprava o stvarnim situacijama



Dobili ste poruku na društvenoj mreži od poznanika koji piše: 'Pogledaj tko je osvojio novu igraću konzolu na ovom linku! Hitno klikni!' Kako ćete postupiti i zašto?

Rasprava o stvarnim situacijama

Možda si rekao/la...

1.Ne otvaram poveznicu jer može voditi na lažnu phishing stranicu.

1.Provjerit ću s prijateljem drugim putem je li on poslao poruku.

1.Ako prijatelj nije poslao poruku, upozorit ću ga na hakiran račun.