

telemach



VARNA RABA INTERNETA

VAREN NA SPLETU, VAREN V SVETU

VARNO IN ZABAVNO



DRAGI UPORABNIK SPLETA!

Živimo v svetu, kjer je internet naš zvesti sopotnik. Od njegove uporabe pa je odvisno, ali bo ta naš najboljši pomočnik ali največji sovražnik. Pri prebiranju vsebine se boš naučil ali obnovil svoje znanje o varni rabi interneta. Vedi, da varna raba interneta ni tako enostavna, kot se morda zdi na prvi pogled. Pazljivo preuči nasvete in se jih redno poslužuj. Z usvojenim znanjem pa svetuj tudi ostalim. Toliko kot si varen na spletu, si varen tudi v svetu!

Želimo ti veliko premišljenih odločitev!

Tvoj Telemach



KAKO DOBRO JE TVOJE GESLO?



Geslo ima na internetu enako vlogo kot ključ, s katerim zakleneš stanovanje ali hišo. S tem preprečiš tatovom in drugim nepovabljenim gostom, da bi imeli dostop do tvojih osebnih stvari.

DOBRO geslo imaš, če:

- ✓ vsebuje najmanj deset znakov;
- ✓ ga sestavljajo male in velike črke, številke ter posebni znaki, kot so #?!-, %&@β;
- ✓ si ga je težko zapomniti;
- ✓ za vsako spletno mesto oblikuješ svojega.

SLABO geslo imaš, če:

- ✗ vsebuje zaporedje števil ali črk (npr. 12345678 oz. qwertz);
- ✗ je to enostavna beseda (Marjan, nogomet ...);
- ✗ uporabiš imena družinskih članov, hišnih ljubljencev, datum rojstva itd.



ZELO POMEMBNO JE, DA JE GESLO MOČNO IN ZNANO SAMO TEBI. ČE SUMIŠ, DA TI JE NEKDO VDRL V PROFIL, MORAŠ GESLO NEMUDOMA ZAMENJATI.





KAKO DOBRO JE TVOJE GESLO?

Z odgovori na spodnja vprašanja preveri, kako dobro je tvoje geslo. Točke najdeš na zadnji strani brošure.

1. Koliko znakov vsebuje tvoje geslo?

- a) manj kot pet
- b) med pet in devet
- c) deset ali več

2. Kaj sestavlja tvoje geslo?

- a) male in velike črke, številka ter znak
- b) male in velike črke ter številka
- c) male in velike črke

3. V mojem geslu se skriva ... (možen en odgovor)

- a) enostavna beseda in številke
- b) enostavna/zahtevna beseda
- c) enostavna beseda, številke in znak
- d) zaporedje števil/črk/znakov
- e) zahtevna beseda, številka in znak
- f) zahtevna beseda in številka



LESTVICA MOČI GESLA

3 do 5 točk: Tvoje geslo je **ŠIBKO**. Svetujemo, da ga nemudoma spremeniš z upoštevanjem naših napotkov ter tako nepridipravom onemogočiš, da vdrejo v tvojo zasebnost.

6 do 10 točk: Tvoje geslo je **SREDNJE MOČNO**. To ne pomeni nujno, da je slabo, priporočamo pa, da ga podkrepiš z elementi, ki ti v geslu primanjkujejo.

11 do 15 točk: Bravo, tvoje geslo je **MOČNO!** Očitno že nekaj veš o varnosti na internetu, vseeno pa ti svetujemo, da svoje geslo občasno posodabljaš ter na ta način še bolj otežiš morebitne vdore.

Na zadnji strani preveri, koliko točk si zbral in spoznaj kakovost svojega gesla.



VDOR V ZASEBNOST

Dva najpogostejša načina vdora sta:

- slab varnostni sistem/zaščita naprave in
- slabo geslo.

Nobena spletna aktivnost ne omogoča popolne zasebnosti. Splet deluje tako, da te spodbuja k temu, da o sebi razkriješ čim več. Ob tem se tvoji osebni podatki zbirajo tudi s pomočjo piškotkov (»cookies«). Zato bodi previden, katere piškotke sprejemaš.

SPLETNI KRIMINAL

Hakerji ali spletni prevaranti na nas prežijo v vsakem spletnem kotičku. Poznamo klasične programerske in takšne, ki poleg tehnologije uporabljajo tudi psihološke pristope. Tako imenovani »phishing« je spletna prevara, pri kateri goljuf pridobiva občutljive podatke spletnih uporabnikov. V slovenščini za tovrstno početje uporabljamo tudi izraz »spletno ribarjenje«.

KRAJA IDENTITETE

Kraja identitete (kamor sodi tudi ustvarjanje lažnih spletnih profilov) je kaznivo dejanje, ki se preganja na podlagi 143. člena Kazenskega zakonika. O njej govorimo, ko se druga oseba predstavlja z našim imenom. S tem lahko zavaja naše prijatelje ter si pridobi naše strogo zaupne informacije. Najpogostejši način za prevzem tuje identitete je kraja gesla, s katerim nepridiprav pridobi dostop do naših družbenih omrežij.





NEŽELENA E-POŠTA

»**SPAM**« je s tujko poimenovana **neželena oz. vsiljena pošta, ki jo najpogosteje dobivamo na elektronski naslov**. Slednja največkrat vsebuje oglasna sporočila in je poslana na najrazličnejše poštne naslove.

Neželena elektronska pošta najpogosteje vsebuje sporočila, ki nas spodbujajo k nakupu ali nas vodijo k dejanjem, zaradi katerih se lahko znajdemo v težavah. Pogosto vsebuje tudi prevare in viruse, zato priponk in povezav neželene e-pošte ne odpiramo.

Neželena pošta se ne pojavlja samo v elektronskem poštnem nabiralniku, temveč tudi v SMS sporočilih in na družbenih omrežjih.



ZANIMIVOST

Več kot **90 % najstnikov** uporablja eno ali več **družbenih omrežij**. Na njih z uporabo mobilnega telefona prebijejo kar **80 % svojega prostega časa**.

DRUŽBENA OMREŽJA

DOBRA STRAN

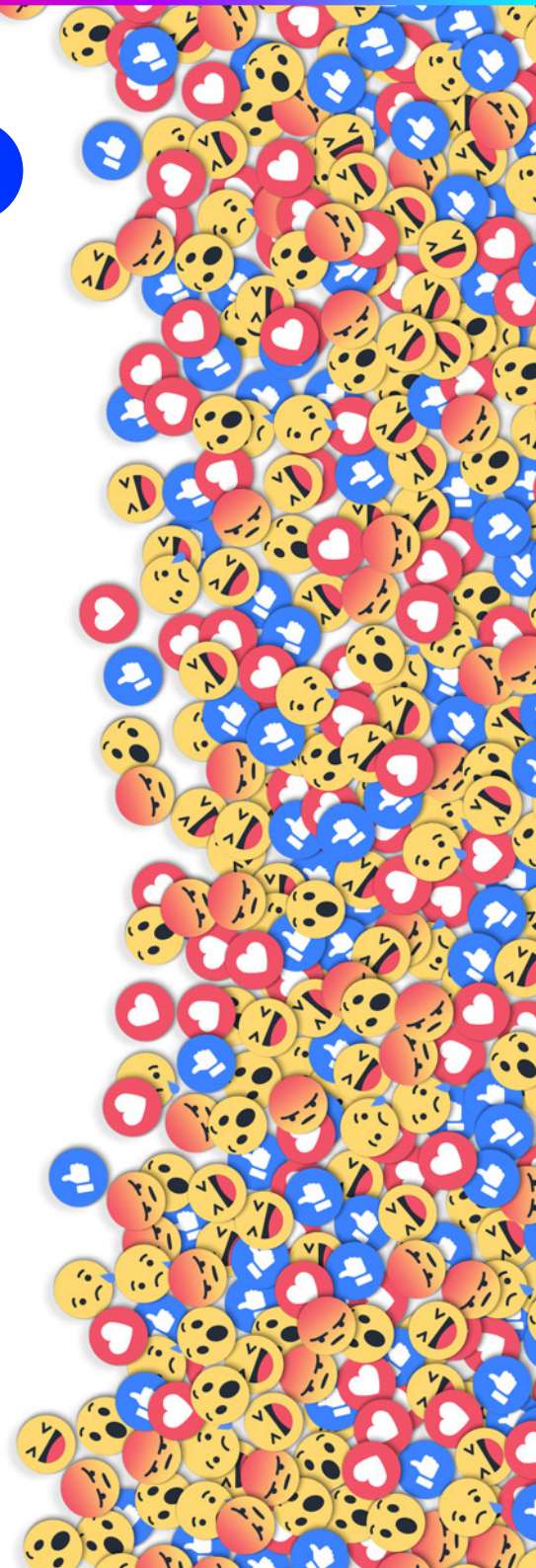
uporabe družbenih omrežij:

- ✓ Ohranjanje stikov z družinskimi člani in prijatelji.
- ✓ Pridobivanje novih znanj in idej.
- ✓ Spoznavanje novih ljudi s podobnimi interesi.
- ✓ Sledenje aktualnim dogodkom.

SLABA STRAN

uporabe družbenih omrežij:

- ✗ Zlahka postanemo tarče spletnih zlorab. Več kot delimo z javnostjo, bolj smo na udaru.
- ✗ Spremljanje prirejenih »idealnih« objav lahko negativno vpliva na našo samopodobo.
- ✗ Če nismo dovolj previdni, lahko hitro postanemo žrtev spletnega nasilja.
- ✗ Na njih smo lahko izpostavljeni lažnim in zavajajočim informacijam (t. i. »fake news«).



DRUŽBENA OMREŽJA

KAKO ZELO NEVARNA SO DRUŽBENA OMREŽJA, KAŽEJO NASLEDNJE STATISTIKE:

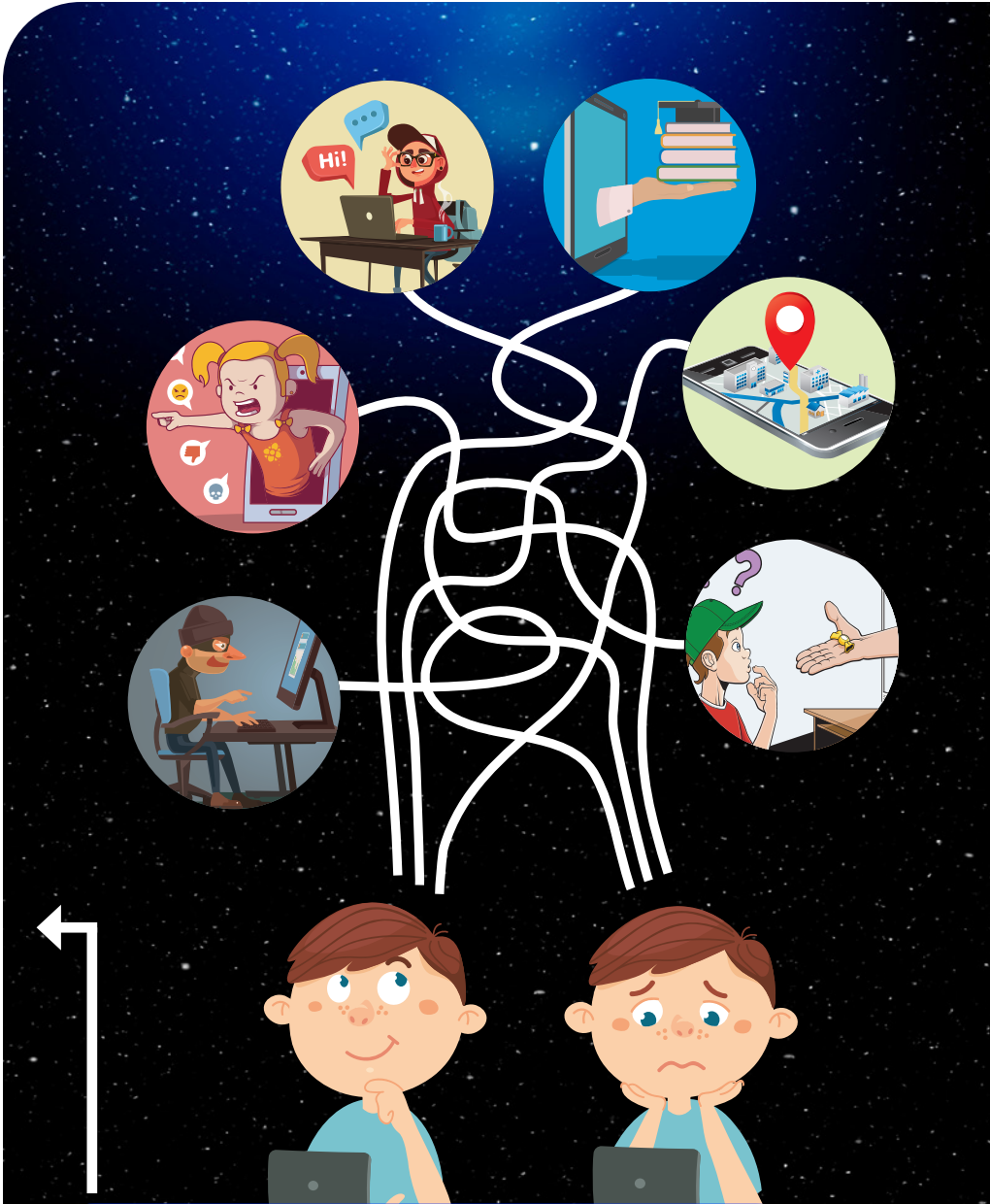
- **vsakega petega najstnika** je že kontaktirala neznana oseba;
- **vsak tretji najstnik** je že prejel neprimerne vsebine;
- **skoraj polovica najstnikov** je z izmišljeno identiteto poskušalo priti do nepreverjenih ali spornih vsebin.

DRUŽBENA OMREŽJA UPORALJAŠ VARNO, KO:

- vpisuješ čim manj osebnih podatkov (telefonska številka, datum rojstva, naslov ...);
- svoj profil zapreš za javnost;
- ne objavljaš golih ali razgaljenih fotografij;
- med prijatelje/sledilce sprejemaš le osebe, ki jih resnično poznaš;
- ne odgovarjaš neznancem.

POZITIVNE LASTNOSTI

NEGATIVNE LASTNOSTI



V prepletenki sličicam poišči pravo pot ter ugotovi, katere so pozitivne in katere negativne plati uporabe interneta. Nato te plati zapiši v ustrezen stolpec.

SPLETNI »GROOMING« = SPLETNO PRIJATELJSTVO S SLABIMI NAMENI

Pri tem odrasla oseba naveže stik z mladostnikom, mlajšim od 15 let, v pogovoru jasno namiguje na spolnost in se želi z njim srečati v živo. Neznanec izbrano žrtev nagovori tudi k pošiljanju golih fotografij.

»SEKSTING« = IZMENJEVANJE INTIMNIH FOTOGRAFIJ ALI POSNETKOV

Nevarnost, ki ob tem preti, je zloraba zaupanja, saj lahko prejemnik fotografijo deli z drugimi, jo javno objavi ali pa z njo celo izsiljuje. Nepooblaščen deljenje fotografij po spletu ali z drugimi ter grožnje in izsiljevanje je treba nemudoma prijaviti policiji.



POMEMBNO

**Kar 80 % intimnih
fotografij in posnetkov,
ki si jih izmenjajo
mladostniki,
pozneje uide
izpod nadzora
in pristane
na spletu.**



KAJ NAREDITION, ČE TE NEKDO PRIČNE IZSILJEVATI S TVOJIMI SPORNIMI FOTOGRAFIJAMI ALI POSNETKI?

1. Takoj na začetku izsiljevanja izsiljevalca opozori, da preneha s svojim početjem.
2. Ko pošleš opozorilo, TAKOJ prekini stike.
3. Shrani dokaze groženj in izsiljevanja.
4. Shrani vse znane podatke o izsiljevalcu.
5. Če obstaja grožnja fizičnega nasilja, poišči nasvet odrasle osebe.
6. Povej družini in prijateljem.
7. Obišči šolsko svetovalno službo ali pokliči **TOM Telefon (116 111)**.
8. Izsiljevanje prijavi policiji.
9. Poskušaj se izogniti samooboževanju.
10. Situacijo imej pod nadzorom.
11. Poišči informacije, kako se zaščititi v prihodnje.





Spodnje povedi dopolni z ustreznimi besedami!

1. Nikoli ne brskaj po internetu, če računalnik ni _____.
2. Svoje kontaktne podatke vedno zaupaj samo tistim, ki jih dobro _____.
3. Če na spletu naletiš na vsebino, zaradi katere ti je neprijetno, to nemudoma povej _____.
4. Bodi pozoren na elektronsko pošto, ki ti jo pošljejo _____ osebe in ti veliko obljublja. V tem primeru gre najverjetneje za _____ elektronsko pošto.
5. Ne srečuj se z _____ ljudmi, tudi če ste prijatelji na spletu. V kolikor te ta oseba povabi na srečanje, to vedno _____ staršem/učitelju/svetovalni delavki.
6. Neželene pošiljatelje lahko odstraniš s seznama stikov ali pa jih popolnoma _____.
7. Na sporočila nadlegovalca NIKOLI ne _____!

STATISTIKA SPLETNIH ZLORAB

- Vsak dan je **blokiranih približno 24.000 zlonamernih mobilnih aplikacij**.
- Vsaka peta spletna datoteka ni varnostno zaščitena.
- **Hekerski napad se zgodi vsakih 39 sekund.**
- **95 % vdorov se zgodi zaradi šibkih gesel in človeških napak.**
- V letu 2022 je kar 93,5 % prebivalcev Evrope uporabljalo internet.
- Eden od štirih uporabnikov spleta je svoje osebne podatke posredoval v spletno mrežo.
- Na spletu nakupuje že vsak četrti Slovenec.
- Ena od desetih oseb prenaša programsko opremo, glasbo, videoposnetke in igre s spleta.



»V PRIMERU IZSILJEVANJA ...«

Napiši, kateri so štirje najbolj pomembni koraki, ki jih moraš narediti v primeru izsiljevanja s fotografijami ali posnetki.

1. _____
2. _____
3. _____
4. _____

BELEŽKA



Z informacijami so nam pomagali:

www.safe.si

www.nijz.si

www.varninainternetu.si

gradiva.txt.si

REŠITVE

»KAKO DOBRO JE TVOJE GESLO?«

Vprašanje 1: a = 1; b = 3; c = 5

Vprašanje 2: a = 5; b = 3; c = 1

Vprašanje 3: a = 2; b = 1; c = 3; d = 1; e = 5; f = 3

»DOPOLNI POVEDI«

a) zaščiten; b) poznaš; c) staršem/učitelju/svetovalni službi;
d) neznane, vsiljeno; e) neznanimi, povej; f) blokiraš; g) odpisuj

»V PRIMERU IZSILJEVANJA ...«

1. Shrani dokaze groženj in izsiljevanja.
2. Povej družini in prijateljem.
3. Poskušaj se izogniti samoobtoževanju.
4. Poišči informacije, kako se zaščititi v prihodnje.



VARNA RABA INTERNETA

070 700 700
www.telemach.si

telemach