

# Ustvarjaj, povezuaj in širi spoštovanje

Nekaj utrinkov predstavitev tehniškega dne

Avtorji: učenci 7. razreda

5. in 6. februar 2018

# 10 ZLATIH PRAVIL ZA VARNO UPORABO SPLETA



**1** NA SPLETU NE IZDAJAJ SVOJIH OSEBNIH PODATKOV, NITI PODATKOV SVOJIH STARŠEV.

**2** NE OBJAVLJAJ SVOJIH ZASEBNIH FOTOGRAFIJ, NITI FOTOGRAFIJ SVOJIH PRIJATELJEV.

**3** GESLA SO SKRIVNOST! NE ZAUPAJ JIH NITI NAJBOLJŠEMU PRIJATELJU.

**4** SPOŠTUJ PRAVILA LEPEGA VEDENJA NA SPLETU.

NADLEGOVANJE IN ŽALJIVI GOVOR PREKO META ALI TELEFONA STA NEDOPUSTNA!

**5** NE SREČUJ SE Z NEZNANCI S SPLETA.



**6** STARŠEM POVEJ, ČE TE KDO NADLEGUJE ALI ČE NALETIŠ NA NEPRIMERNO VSEBINO NA SPLETU.



**7** Z UPORABO INTERNETA IN MOBILNIH NAPRAV NE PRETIRAVAJ.

**8** Z INTERNETA NE PREPISUJ, NE DA BI NAVEDEL VIR.

**9** NI VSE RES, KAR PIŠE NA INTERNETU! OBVEZNO PREVERI ŠE DRUGE VIRE.



**10** ZA DODATNE INFORMACIJE, NASVETE, IGRE IN ZABAVO VEČKRAT OBIŠČI

[WWW.SAFE.SI](http://WWW.SAFE.SI)

# SEKSTING

je beseda, ki označuje pošiljanje svojih golih fotografij prek SMS sporočil ali mobilnih aplikacij, spleta. To početje je pogosto pri najstnikih, ki se fotografirajo goli ali napol goli nato pa si fotografije najpogosteje s pomočjo mobilnega telefona izmenjujejo z vrstniki, simpatijami.



# Vzrok za seksting?

Vzrok za seksting je lahko iskanje pozornosti med vrstniki ali znotraj skupin. Najstniki si izmenjujejo fotografije in se pri tem preizkušajo, koliko se upajo razgaliti. Pri deljenju fotografij obstaja tveganje, kaj bodo prejemniki fotografij z njimi naredili. Jih bodo izbrisali ali delili naprej v krogu svojih prijateljev, ali jih morda celo javno objavili na internetu? Nekateri najstniki zaradi želje po vzbujanju pozornosti ali sprejetju v skupino vrstnikov intimne slike javno objavljajo na družabnih omrežjih.



# Kako poteka seksting?

Seksting poteka po internetnih omrežjih. S pomočjo pametnega telefona. Seksting je slika **akta** določene osebe ki se največkrat slika v ogledalu.





# Kaj pa tveganje?

Skoraj 90 odstotkov aktov, ki so jih amaterji sami naložili na internet, je prej ali slej ukradenih in uporabljenih na katerih od pornografskih strani. Strokovnjaki opozarjajo, da vam v takem primeru pretita obup in depresija, saj ste lahko, če izgubite nadzor nad distribucijo fotografij, tarča javnega linča.



Uporabljaljaj dolga in zapletna gesla, različna za različne strani, pogosto jih menjaj in jih v nobenem primeru ne povej nikomur. **Gesla so tvoja skrivnost!**

Poskrbi, da imaš pametno nastavljene nastavitve zasebnosti v socialnih omrežjih.

**Zaklepaj zaslon svojega pametnega telefona!** Če ima kdo dostop do podatkov, slik, profilov prek njega, ti jo lahko pošteno zagode oz. ti naredi veliko škodo.

**Previdno z uporabo spletne kamere**

: naj bo izključena, ko je ne uporabljaš. Zavedaj se, da je kot okno, skozi katerega lahko tudi nepovabljeni pokukajo v našo zasebnost, stanovanje in življenje.

**Spoštuj in ščiti tudi zasebnost drugih.** Objavljanje slik brez dovoljenja/označevanje oseb na slikah je groba kršitev.

**Na spletu ne objavljaj svojih kontaktnih podatkov**, imena, priimka, telefonske številke, naslova bivanja, naslova elektronske pošte, messengerja **in tudi drugih osebnih podatkov**, kot so datum rojstva, davčna številka, številka kreditne kartice, ipd.

**Ne odgovarjaj na elektronska pisma, ki od tebe zahtevajo osebne in finančne podatke.**



Na družabnih omrežjih je potrebna tudi previdnost pri objavi podatkov in informacij o sebi. Če je tvoj profil popolnoma javen, ga lahko vidi in deli naprej čisto vsak uporabnik interneta: tudi tvoji starši, učitelji, profesorji, delodajalci, popolni neznanci in še kdo nepovabljen.

Pri izbiri ponudnika spletne strani za mreženje se je treba pozanimati, kako skrbijo za zasebnost in varnost svojih uporabnikov. Dobro je prebrati pravila uporabe in njihovo politiko varovanja zasebnosti. V drobnem tisku se pogosto »skrivajo« pomembne informacije, komu bodo posredovali tvoje podatke, komu bodo na voljo v vpogled in ali jih boš lahko trajno izbrisal.





# PREKOMERNA RABA MOBILNEGA TELEFONA

**-POSLABŠANJE VIDA**

**-ZARADI TEGA SE NAREDIJO NESREČE**

**-SLABŠE UČENJE**

**-PREMALO GIBANJA.**



## KOLIKO JE TO PREKOMERNA UPORABA

*Strokovnjaki so ugotovili, da je preživeti vsak dan 2 uri na računalniku samo za zabavo preveč in lahko vodi v težave.*

# Prekomerna uporaba mobilnih telefonov

Je nova zasvojenost 21. stoletja in pomeni prekomerno uporabo mobilnih telefonov bodisi za pogovarjanje, slikanje, snemanje, pošiljanje SMS-sporočil ali brskanje, klepetanje, deljenje vsebin, slik in svoje lokacije po internetu.

Mladostniki postajajo vse bolj **navezani na svoje mobilne naprave**, saj le-te omogočajo dosegljivost in povezljivost **24 ur na dan, 7 dni v tednu**. Še posebej pametne telefone s svojo izjemno **multifunkcionalnostjo** in neskončnimi možnostmi uporabe je **vse težje sploh kdaj odložiti**. **Mladi imajo potrebo, da so stalno dosegljivi in na voljo svojim prijateljem**, in v strahu, da ne bi česa pomembnega zamudili, **stalno preverjajo objave prijateljev** na družabnih omrežjih, z njimi komunicirajo, poleg tega pa še igrajo igre in/ali poslušajo glasbo. Zaradi tega mladi zasvojenci **izostajajo od pouka, v ekstremnih primerih pa celo opustijo šolanje**. Ponavadi je pretirana navezanost mladih na mobilni telefon posledica drugih težav v tem razvojnem obdobju.

# Praktični nasveti


## (kako preprečiti zasvojenost s telefonom)

- **Ne zamenjaj pravih prijateljev in druženja v živo za mobilnik.** Nikomur ni všeč, da se nekdo med pogovorom z njim poleg ukvarja še s svojim mobilnikom in je hkrati priklopljen še na množico drugih komunikacij in informacij, to so potrdile tudi raziskave med mladimi.
- **Ne ukvarjaj se z mobilnikom med jedjo, družinskim kosilom, med poukom, v kinu, gledališču ...** Posvečaj se temu, kar delaš, kaj gledaš, kaj ješ, s kom si. Mobilnik lahko počaka!
- **Ponoči imej mobitel izklopljen (sevanje).** Trdnih dokazov o vplivu sevanja ni, a pazljivost vseeno ni odveč. Kar zadeva otroke, obstajajo hipoteze, da so otroci med 3. in 15. leta občutljivejši na elektromagnetna sevanja, zato je bolje, da čim manj uporabljajo mobilnike. V smislu časovne omejitve ni znanih točnih vrednosti. V smislu upoštevanja načela previdnosti pa se omenja 30 minut na dan. (doc.dr. Peter Gajšek, direktor Inštituta za neonizirana sevanja - [www.inis.si](http://www.inis.si)). **Telefoniraj na območjih, kjer je dobra pokritost s signalom, saj je tam sevanje manjše, priporočamo tudi uporabo vrvičnih slušalk.**
- **Ne zamujaj pomembnih dogodkov v življenju samo zato, ker moraš biti non-stop priklopljen na svoj telefon.** Postajamo odvisni od informacij, ki nam, ko presežejo določeno količino ne koristijo več (dokazano), ampak pravzaprav ustvarjajo stres, pojavlja se fragmentacija koncentracije, nismo več sposobni osredotočiti se poglobljeno na eno stvar, ampak spremljamo vse, a zelo površno.





- Mobilni telefon je dobro zaščititi z ANTIVIRUSNIM programom.
- Tvoja številka mobilnega telefona je osebni podatek, zato ga NE OBJAVLJAJ kar tako na spletu in je ne dajaj komurkoli.
- Zaslona pametnega telefona zaklepaj z geslom ali vzorcem in tako ONEMOGOČI DRUGIM, da bi dostopali do tvojih podatkov in ti zagodli kakšno nevšečnost (npr. spremenijo Facebook profil, objavijo slike na splet, pišejo komu v tvojem imenu).

- 
- Pri komuniciranju prek mobilnega telefona in spleta UPOŠTEVAJ BONTON, bodi strpen in prijazen. Obnašaj se tako, kot želiš, da se drugi do tebe.
  - Zvonjenje telefona in/ali pogovarjanje v kinu, gledališu, med poukom, v bolnišnici, na avtobusu...JE NEDOPUSTNO.
  - Če nekoga slikaš in posnetek nato objaviš na spletu, ga moraš prej VPRAŠATI za dovoljenje.
  - PAZLJIVO z deljenjem informacij o svoji lokaciji prek mobilnega telefona!!!

# Zasebnost na družbenih omrežjih

- 1. Bodi previden pri objavljanju svojih osebnih podatkov**
- 2. Bodi previden s podatki, ki povedo veliko o tem, kaj počneš in kje se pogosto zadržuješ v svojem off-line življenju.**
- 3. Spoštuj zasebnost drugih**
- 4. Omeji dostop do informacij**
- 5. Previdno tudi s sprejemanjem neznanih kontaktov**
- 6. Zaupaj svojemu občutku!**
- 7. Kjer se da, namesto svojega pravega imena raje uporabi vzdevek.**
- 8. Pozanimaj se!**



# 10 naj nasvetov

1. Raje ne sinhroniziraj
2. Upoštevaj starostno omejitev
3. Nastavitve zasebnosti svojega profila v družabnih omrežjih nastavi tako, da [lahko tvoje objave in profil vidijo le prijatelji](#) in ne splošna javnost
4. Nauči se prijaviti zlorabo, [nadlegovanje](#), sovražno skupino, sliko, posnetek in [blokirati osebo](#) v družabnem omrežju, ki ga uporabljaš
5. Spoštuj zasebnost drugih
6. Nikomur ne zaupaj svojega gesla



Instagram





# DANGER

## NEVARNOST

### Kako lahko neznanec prevzame našo spletno identiteto?

1. Najlažje takrat, kadar smo sami nepazljivi in po nesreči ali celo namerno razkrijemo geslo za elektronsko pošto ali Facebook.
2. Naslednji način je phishing oziroma kraja podatkov, ko nas elektronsko sporočilo pripravi do tega, da razkrijemo svoje uporabniške podatke.
3. Storilec lahko pridobil naše geslo prek okužbe računalnika z zlonamerno kodo, ki beleži pritiske tipk (t.i. keylogger). Gre za vrsto virusa, ki napadalcu pošilja shranjena in prestrežena gesla z računalnika. Med goljufi so priljubljena mesta za krajo osebnih podatko tudi javno dostopni računalniki, ki jih uporabljamo na potovanjih, da bi pogledali elektronsko pošto ali objavili fotografije na Facebooku.

# KAKO NEZNANEC PRIDOBI NAŠO OSEBNO IDENTITETO???

-takrat kadar sami ponesreči objavimo oz. napisemo svoje geslo pred vsemi.

-kadar nas nekdo pripravi da izdamo svoje geslo.

-z okužbo računalnika, ki zabeleži tipk tipke.



# varnostno kopiranje

varnostna kopija ali rezervna kopija je dvojniki podatkov v računalniku, ki jih uporabnik ne želi izgubiti. Ti podatki so pomembni uporabniku, ali pa so pomembni za pravilno delovanje in funkcioniranje računalnika in programov. namen izdelave varnostne kopije je obnova podatkov v primeru okvare ali poškodbe nosilca podatkov diska ali računalnika. Prav tako lahko obnovimo podatke na nove sisteme (npr. zamenjava računalnika) Obstaja več varnostnih kopij npr. varnostna kopija podatkov (na trdem disku), varnostna kopija celotnega sistema ali varnostna kopija mobilne naprave. Uporabnik računalnika se mora zavedati dejstva, da so podatki na računalniku izredno ranljivi oziroma se lahko 'izgubijo' (npr. okvara diska, napaka operacijskega sistema, nenamerni izbris.





# Bonton



- **Česar ne bi rekel v živo, ne natipkaj online!** Ne skrivaj se za anonimnostjo, za zaslonom. Na spletu smo pogosto lažje nesramni do drugih, saj svoji žrtvi ne gledamo v obraz, to pa ne pomeni, da je tako kaj lažje žrtvi! Poleg tega pa na anonimnost pri takih stvareh ne gre računati, saj puščamo elektronske sledi.
- Tudi če kdo pusti svoj telefon dostopen in nezaklenjen, to ne pomeni, da lahko po njem brskaš in ga uporabljaš. V telefonu imamo tudi zasebne fotografije, sporočila in podatke, **vsak pa ima pravico do zasebnosti!**
- **Osebo, ki jo želiš fotografirati** s svojim mobilnim telefonom, prej **vprašaj za dovoljenje**. Mogoče ji ni do tega oz. se počuti neprijetno.
- Pri komuniciranju prek mobilnega telefona in spleta **upoštevaj bonton, bodi strpen in prijazen. Obnašaj se tako, kot želiš, da se drugi do tebe.**
- Tudi s fantom/punco se ne konča s spremembo statusa na FB ;) **Za resne stvari**, prekinitev zveze, izražanje sožalja ipd. **je še vedno najprimernejši način komunikacija iz oči v oči** (pa to ne pomeni prek spletne kamere).
- **Ko si z nekom v družbi**, se posvečaj tej osebi in **ne preverjaj neprestano, kaj se dogaja na tvojem mobilnem telefonu**, Facebooku ... Pogovarjanje po telefonu, pošiljanje sporočil, preverjanje telefona, ko si z nekom v družbi, je nevljudno in gre tudi večini ljudi zelo na živce.
- **Zvonjenje telefona in/ali pogovarjanje** v kinu, gledališču, med poukom, v bolnišnici, tudi na busu ... je **nedopustno**.



# Pravila bontona

- uporaba, brskanje po tujem telefonu brez dovoljenja lastnika;
- kraja identitete (pisanje, objavljanje v tujem imenu);
- obdelava fotografij na žaljiv način;
- izsiljevanje prek spletne kamere;
- snemanje pretefov, učiteljice, sošolcev;
- objavljanje fotografij, posnetkov drugih brez njihovega dovoljenja;
- zvonjenje telefona ali pogovarjanje v kinu, gledališču, med poukom, v bolnišnici, na busu ...;
- tudi slikanje in snemanje med poukom, predstav v kinu, gledališču, na razstavah pogosto ni dovoljeno;
- telefoniranje, ko vozimo kolo/avto (zelo nevarno!).





**Zvonjenje telefona in/ali  
pogovarjanje v kinu, gledališču,  
med poukom, v bolnišnici, tudi na  
busu ... je nedopustno.**

Poglejmo pa še, katerim vedenjem na spletu se vsakem primeru raje izogibaj:

- ustrahovanje, nadlegovanje, žaljenje, širjenje govoric, razpošiljanje žaljivih fotk prek spleta ali mobilne naprave;
- spamanje, verižna pisma;
- izmenjava nasilnih in pornografskih vsebin;
- uporaba, brskanje po tujem telefonu brez dovoljenja lastnika;



## PREVARE IN VARNOST NA SOCIALNIH OMREŽJIH

Lažna obvestila so ponavadi panični alarmi ,sprva poslani s strani zlonamernih ljudi ,nato pa jih pošiljajo in namnožijo nedolži uporabniki ,ki mislijo ,da pomagajo skupnosti s pošiljenjem obvestil.Ne posredujte lažnih sporočil.S pošiljenjem namreč po nepotrebnem obremenjujete poštne strežnike in povzročajo panike med ljudmi.

## ZAŠČITITE SVOJO SPLETNO KAMERO

Spletne kamere so vsekakor priročne ,če želimo imeti nadzor nad svojim domom ali delovnimi prostori. Zelo enostavno in hitro lahko prek brskalnika dostopamo do spletnega vmesnika naše kamere .Kaj ko pa gre za varnost” tovrstne spletne kamere so namreč velikokrat prosto dostopne neposredno prek IP naslova kar pomeni do-lete lahko vstopa vsiljivcev



# NADLEGOVANJE

Nadlegovanje je vsako neželjeno vedenje, povezano s katero koli osebno okoliščino, z učinkom ali namenom prizadeti dostojanstvo osebe ali ustvariti zastraševalno, sovražno, ponižujoče, sramotilno ali žaljivo okolje.



# TRPIČENJE

Trpinčenje na delovnem mestu je vsako ponavljajoče se ali sistematično, graje vredno ali očitno negativno in žaljivo ravnanje ali vedenje, usmerjeno proti posameznim delavcem na delovnem mestu ali v zvezi z delom.



# KAKO LAHKO SAM PREPREČIŠ SPLETNO NADLEGOVANJE ?

- a) Svoje telefonske številke, e-maila, naslova ne objavljaš na spletu
- b) vsak ne more biti tvoj spletni prijatelj
- c) svojega gesla ne zaupaj nikomur
- d) ne puščaj odklenjenega telefona ali odprtih profilov na javnih računalnikih
- e) skrbi za svoj SPLETNI UGLED
- f) upoštevaj SPLETNI BONTON



# KAKO UKREPATI V PRIMERU SPLETNEGA NASILJA ?

- a) Zavedaj se, da nisi ti kriv, če te nadlegujejo
- b) ne odgovarjaj na sporočila, ki so sovražna ali te žalijo
- c) shrani sporočilo, naredi zaslonsko sliko
- d) povej odrasli osebi, ki ji zaupaš ! Pokliči Tom telefon 116 111
- e) ne bodi nema priča: ne toleriraj nadlegovanja drugih

