Stručni rad
UDK:37.013:371
DOI:10.7251/ZCMZ0123667D

IZZIVI INFORMACIJSKE VARNOSTI V ŠOLSKEM OKOLJU

Lina Dečman Molan, spec., dipl. inž.[489]

Šolski center Kranj, Strokovna gimnazija

Povzetek: *Dijaki in učitelji so vse bolj in bolj izpostavljeni grožnjam informacijske varnosti, saj vse več uporabljajo mobilno tehnologijo. Do tega prihaja tudi zato, ker so vedno bolj tehnično opremljeni. Žal se večina uporabnikov ne zaveda groženj, ki so jim so dnevno izpostavljeni. Dijaki in učitelji imajo na voljo mnogo izobraževanj ter delavnic na temo informacijske varnosti. Mnogi od dijakov tudi namerno kršijo pravila informacijske varnosti – kar si bomo ogledali na primerih. Ob primerih bomo podali tudi kritično mišljenje o možnih posledicah ter o prepotrebnih preventivnih ukrepih. Na Strokovni tehniški gimnaziji z zunanjimi strokovno usposobljenimi izvajalci izvajamo različne delavnice za informacijsko varnost. Ne glede na vse aktivnosti ne moremo preprečiti različnih incidentov s področja varnosti informacijske tehnologije. Tako ugotavljamo, da moramo še povečati število izobraževanj in delavnic. V primeru incidentov izvajamo tudi sankcije, ki morajo biti dovolj stroge, da kot opozorilo delujejo tudi preventivno. V prispevku bomo predstavili, kako v sodelovanju s ponudniki rešitev in strokovnjaki s področja informacijske varnosti izvajamo delavnice, kako delujemo v manjših skupinah in kako predstavljamo rezultate in ugotovitve na teh delavnicah.*

Ključne besede: *dijaki, informacijska varnost, preventiva, izobraževanje, delavnice*

UVOD

V današnjem času je razvoj na vseh področjih zelo hiter, množična uporaba računalnikov in pametnih naprav, ki so povezani z internetom, pa je vse večja oziroma nujna. Uporabniki so vse bolj vešči in hkrati tudi zahtevnejši. Uporaba moderne tehnologije nam omogoča veliko koristi. Poleg teh pa vse pogosteje naletimo tudi na slabe strani – dostikrat tudi nezavedno. Zaradi epidemije SARS-Cov-2 je bilo v veliki meri omejeno socialno življenje. Šolanje in tudi delo sta se preselila na dom oziroma se je oboje izvajalo na daljavo. To nas je nekako prisililo v še večjo povezanost oziroma odvisnost od informacijske tehnologije na vseh področjih življenja. Slaba stvar tega je, da so mladi postali asocialni, nekomunikativni, čustveno otopeli, skrivajo se pod anonimnimi zapisi, težave rešujejo na drugačne načine. Lahko rečemo, da velika večina komunikacije poteka preko socialnih omrežij in klepetalnic. Tam pa takšna sporočila puščajo sledi ali, rečeno drugače, ostajajo trajna in dosegljiva tudi tistim, ki jim niso namenjena. Naša šola pri pouku informatike in v različnih delavnicah ozavešča dijake o pasteh interneta oziroma o informacijski varnosti. Menimo, da je kontinuirano izobraževanje in ozaveščanje pomembno, zato z delavnicami nadaljujemo tudi v višjih letnikih. Mislimo, da je potrebno dijake čim prej in čim bolje informirati. Poleg informiranja v šoli bi se morali starši doma ukvarjati s svojimi otroki in vedeti, kaj počnejo na internetu. Predpogoj za to pa je, da so tudi starši ozaveščeni o pasteh in nevarnostih, ki jih prinaša uporaba sodobne tehnologije.

INFORMACIJSKA VARNOST

Kako pojmujemo varnost, se skozi leta razvoja spreminja. Včasih je veljalo, da je varnost potrebna samo takrat, ko je nekaj povezano z obrambo države in varovanjem njene neodvisnosti. Danes se pojem varnost uporablja na skoraj vseh področjih življenja in prinaša izzive, s katerimi se je potrebno spopasti. Veliko novih izzivov nam prinaša tudi vse večja globalizacija. Odličen primer hitrega razvoja

[489] lina.decman.molan@sckr.si

je informacijska tehnologija, ki je s sabo prinesla ne le veliko novosti in pozitivnih dosežkov, ampak tudi veliko varnostnih izzivov, s katerimi se ni lahko spopadati. Veja varnosti, ki poskuša nevtralizirati ali vsaj zmanjšati te grožnje in tveganja, je informacijska varnost (Bratuša, 2006).

Skorajda vse aplikacije oziroma storitve za dostop potrebujejo geslo. Počasi prehajamo na biometrično prijavljanje, a še vedno prevladujejo gesla. Zavedamo se, da vedno obstaja možnost, da nam geslo ukradejo. V naši šoli pri prvi uri informatike dijake poučimo o varni uporabi gesel. Vsak dijak dobi AAI račun in avtomatsko generirano geslo. Naučimo se tudi, da moramo vsako geslo, ki nam je bilo dodeljeno, ob prvi prijavi spremeniti.

VARNA GESLA

Geslo je varnostni mehanizem, ki je sestavljen iz kombinacije numeričnih, abecednih, simbolnih in alfa numeričnih znakov oziroma posebnih znakov. Obstajajo priporočila, kako naj bo geslo sestavljeno. Dolžina gesla naj vsebuje 10 ali več znakov, med njimi naj bo vsaj ena mala ali velika črka, vsaj ena številka (0–9) in poseben znak. Pri geslih ne uporabljamo šumnikov, saj niso del angleškega nabora znakov. Lahko se zgodi, da nekateri sistemi ne podpirajo uporabe teh znakov. Geslo naj ne vsebuje uporabniškega imena ali njegovega dela. Geslo, ki ga generirate, naj bo naključno, raznoliko in kreativno. Veliko aplikacij in storitev že samo dodeljuje minimalne zahteve za sestavo gesla.

Geslo je potrebno redno menjati. V primeru incidenta je potrebno geslo zamenjati takoj. Priporočena menjava gesel je na devetdeset dni. Gesel ne delimo z drugimi. V primeru, da s kom delimo geslo, ga je potrebno takoj zamenjati. V šolah in ostalih okoljih je zelo pomembno, da se vedno odjavimo iz aplikacije oziroma storitve, saj računalnik uporablja več oseb. Prav tako imajo dostop do teh računalnikov tudi dijaki. Učitelji morajo biti zelo previdni ob prijavi v aplikacijo oziroma v storitev, saj jih dijaki, ki sedijo v prvih vrstah, opazujejo pri vnašanju gesel. Ravno tako je potrebno biti previden pri vnosu gesel na javnih mestih, saj lahko kdo opazuje naš vnos gesla.

Kjer je možno in so na računalnikih nastavljena gesla, je potrebno računalnik ob koncu šolske ure zakleniti.

Za uspešno preprečevanje zlorab, je potrebno pravilno ravnanje z gesli. Navajamo splošna navodila za varno rabo gesel.

- Gesla morajo biti vedno zaupna.
- Gesla nikoli ne zapišemo in ga nikoli ne povemo nikomur.
- Gesla, ki se uporabljajo v službene/šolske namene, se ne uporabljajo v drugih informacijskih sistemih (npr. v sistemu elektronskega bančništva, drugih sistemih za e-pošto, kot je npr. Gmail, sistemih socialnega mreženja, kot sta npr. Facebook, Instagram).
- V spletnih brskalnikih se ne uporablja funkcija »zapomni si geslo«.

Pri kakršnem koli vpisovanju gesla preverite, ali svoje uporabniško ime in geslo vpisujete na varni, pravilni in zaupanja vredni povezavi (HTTPS). V spletnih brskalnikih je takšna povezava vidna v naslovni vrstici, v katero vpišemo željen spletni naslov. V naslovni vrstici se pojavi tudi simbol zaprte ključavnice. (https://it.um.si/varnostna-politika/Strani/priporocila-za-izbiro-in-rokovanje-z-gesli.aspx)
Kadar spremenimo geslo, preverimo, ali smo ga zamenjali povsod, kjer ga uporabljamo (primer: AAI račun – uporaba omrežja EDUROAM in uporaba e-pošte na mobilnem telefonu).

Večina uporabnikov še vedno uporablja slaba gesla. Med najslabšimi gesli so zaporedje številk (npr. 12345678), zaporedje črk na tipkovnici (npr: qwertzu ali fghjklčć ali yxcvbnm) in enostavna enobesedna gesla (marjan, nogomet, fido). Tudi uporaba imen in priimkov družinskih članov, imena hišnih ljubljenčkov in datumov ali letnic rojstev ne zagotavlja dobre zaščite. Če uporabljamo takšna gesla, nam lahko nekdo, ki pozna nekaj osnovnih podatkov o nas, na precej preprost način ugotovi geslo. Prav tako pa je enostavna gesla zelo lahko ugotoviti, če gledamo na tipkovnico ali zaslon telefona, ko uporabnik tipka geslo. (https://safe.si/nasveti/moja-identiteta-in-zasebnost/varna-gesla)

DVOFAKTORSKA AVTENTIKACIJA

Dvonivojska avtentikacija oziroma dvofaktorska avtentikacija (kratica 2FA) pomeni, da ne glede na aplikacijo ali storitev, v katero se prijavimo, dvojno preverimo, ali zahteva res prihaja od nas. To dosežemo recimo z dodatnim preverjanjem vnosa določenega zaporedja v našo osebno mobilno napravo. Ponuja večjo varnost, kot če za dostop potrebujemo standardno uporabniško ime in geslo. V primeru, da jim je uspelo ugotoviti naše geslo, nas dvofaktorska avtentikacija ščiti pred tem, da nimajo dostopa do računa, do katerega bi poskušali dostopati. Najvarnejša metoda dvofaktorske avtentikacije je biometrični faktor, zaradi katerega moramo za dostop do računa uporabiti prstni odtis, ali prepoznavanje obrazov.

Zakaj je uporaba dvofaktorske avtentikacije pomembna?
Vsi uporabljamo več računov in zelo verjetno je, da uporabljamo ista uporabniška imena in gesla, saj si zelo težko zapomnimo veliko količino naključnih močnih gesel za vse storitve, ki jih uporabljamo. V primeru uporabe dvofaktorske avtentikacije dodamo še eno raven varnosti in na ta način otežimo dostop brez našega dovoljenja. S tem je naš račun bolj zaščiten (Dečman Molan, 2022).

PRAKTIČNI PRIMER KRAJE GESEL – E-ASISTENT IN LOPOLIS

Platformi eAsistent in Lopolis sta sistema elektronske pedagoške evidence. Sta orodji, ki šolam pomagata načrtovati in voditi evidence. Oba vsebujeta eDnevnik in eRedovalnico. Elektronski dnevnik služi dodajanju učnih ur, dodajanju učne snovi v opis k posamezni učni uri, popis izostankov manjkajočih dijakov na določeno uro, dodajanje domačih nalog, dodajanje pohval in izboljšav, medtem ko eRedovalnica služi vpisovanju ocen. Ločimo lahko ustne in pisne ocene, ocene iz laboratorijskih vaj … Prav tako dodajamo tudi ocenjevanje znanja. Komunikacija služi komuniciranju med strokovnimi sodelavci, starši in dijaki. V obeh sistemih se nahajajo občutljivi podatki, ki so varovani skladno s pravili o varstvu osebnih podatkov (Dečman Molan, 2022).

Oba incidenta sta se zgodila v letu 2021 in 2022.

- Januarja 2022 smo bili na šoli obveščeni o vdoru v eAsistent, kjer naj bi si dijaki popravljali ocene. Neznanci so po socialnih omrežjih učencem in dijakom ponujali spremembo ocen. Pogoj za to je bil, da so jim pisali zasebna sporočila. Preko zasebnih sporočil so dobili navodila, kako naj na šolskih računalnikih nastavijo easistent.xyz, da se bodo učitelji prijavili in bodo tako pridobili njihova gesla. Učitelji razlike niso opazili, saj so uporabili klik na bližnjici, ki je bila identična pravi. Ob vpisu uporabniškega imena in gesla je učitelj izbral prijavo in se je stran z vidika uporabnika samo še enkrat »naložila«. Učitelj je mislil, da je vpisal napačno geslo in prijavo še enkrat ponovil, da se je prijavil v eAsistenta. (https://infocenter.si/zloraba-sistema-easistent/) V času prve prijave se je v ozadju pred preusmeritvijo uporabniško ime in geslo poslalo na skriti kanal Discordovega omrežja. Kar nekaj učiteljev, ki uporabljajo šolske računalnike v učilnicah, ne uporablja zaklepanja računalnikov. Prav tako se ne odjavljajo iz prijavljenih aplikacij, ki jih uporabijo pri uri, npr. Teams, elektronska pošta, eAsistent, spletne učilnice itd. (Dečman Molan, 2022).

- Aprila 2022 se je v medijih pojavila novica, da na Srednji šoli Slovenska Bistrica obstaja sum vdora v šolski sistem elektronske pedagoške evidence Lopolis. Vdrli naj bi dijaki četrtega letnika in si v sistemu opravičevali izostanke od pouka, prav tako pa naj bi si en dijak popravil oceno v e-redovalnici. (https://www.sta.si/3022712/na-bistriski-srednji-soli-sum-vdora-v-sistem-e-redovalnice)

SPLETNO MEDVRSTNIŠKO NASILJE

Spletno medvrstniško nasilje je novejša oblika nasilja. Medvrstniško nasilje se je z vse širšo uporabo mobilnih tehnologij preselilo tudi na svetovni splet. Definicij spletnega nasilja je veliko, ena izmed njih pojav opiše kot namerno in ponavljajočo se škodo, ki jo povzročamo z uporabo računalnikov, mobitelov (prenosnih telefonov) in drugih elektronskih naprav. To agresivno dejanje povzroča skupina

ali posameznik, škoda pa je usmerjena na žrtev, ki se sama ne more braniti. Veliko število elektronskih naprav zagotavlja priložnost za pojav spletnega nasilja preko sporočil, slik, videoposnetkov, elektronske pošte, instant sporočil in klepetalnic (http://pefprints.pef.uni-lj.si/5016/1/Ines_Stajan.pdf).

Pri medvrstniškem nasilju gre za ponavljajočo se in namerno uporabo nasilja med otroci/mladostniki. Močnejši ustrahujejo šibkejše, kar pomeni, da je razmerje med udeleženci neenakovredno. Velikokrat gre tudi za primer, ko neka skupina izvaja nasilje nad posameznikom ali manjšo skupino. Nasilje je lahko psihično ali fizično ali celo kombinacija obojega. Angleška beseda »bullying« je nova beseda in označuje agresivno vedenje močnejšega posameznika proti šibkejši osebi. Zajema žaljenje, trpinčenje in socialno izključitev. »Bullying« se kot proces stopnjuje in je pogosto vezan na šolsko okolje (https://svetovalnicakameleon.si/2019/11/bullying-informacije-za-starse/).

»BULLYING« – PRIMER SPLETNEGA MEDVRSTNIŠKEGA NASILJA

Vseh primerov tega pojava učitelji ne moremo oziroma težko zaznamo. Vsekakor jih obstaja več, kot smo jih sposobni zaznati. Najlažje bi nasilje zaznali starši zaradi spremenjenega vedenja svojih otrok oziroma drugi, če bi se jim dijaki zaupali. Zaznava takšnega nasilja je velikokrat mogoča med samimi vrstniki oziroma znotraj družbe. V začetku oktobra 2022 smo v dveh razredih izvedli delavnico Pasti in nevarnosti interneta, saj dijake redno izobražujemo na področju informacijske varnosti. Tako vedo, kaj lahko počnejo in česa ne smejo. Teme delavnice so bile: izdelava varnih internetnih profilov, varovanje zasebnosti in uporaba družbenih omrežij, varovanje pred krajo identitete, spletni in mobilni bonton, spletno nasilje in mobilno trpinčenje, internetne prevare, zasvojenost s tehnologijo.

Kljub vsemu se primerom nasilja nismo izognili. Jeseni 2022 smo se na šoli srečali s spletnim medvrstniškim nasiljem, ki se je stopnjevalo do te mere, da je v šoli prišlo do fizičnega pretepa med dvema dijakoma. O pretepu je bila podana prijava na policijo. V času preiskave se je razkrilo tudi spletno medvrstniško nasilje, ki se je že nekaj časa izvajalo nad dijakom.

Pri dotični preiskavi se je ugotovilo, da je skupina dijakov nadlegovala sošolca. Med poukom so ga fotografirali, njegove slike so nato prirejali in opremljali z različnimi besedili ter si jih delili na socialnih omrežjih v zaprtih skupinah ali preko zasebnih sporočil. Incident s pretepom so udeleženi dijaki snemali in posnetek delili v zaprti skupini socialnega omrežja. Tako so izvajali še dodaten pritisk na dijaka.

V šoli je težko oziroma je skoraj nemogoče zaznati, kaj se dogaja izven šolskih sten, če o tem nismo direktno obveščeni. V takih primerih bi bilo dobro, da bi se starši, ki sumijo, da je otrok podvržen ustrahovanju, čim prej obrnili na šolo, kjer bi se pogovorili z dijakom in nato ukrepali dalje pri pristojnih institucijah, saj šola razen vzgojnih ukrepov nima drugih pooblastil. Dijak, ki se mu je to zgodilo, si je pisal dnevnik o vseh dogodkih ustrahovanja. Konkretni primer se je končal s kazensko ovadbo dijaka, ki je izvajal spletno medvrstniško nasilje in se je stepel z žrtvijo nasilja. Po pogovorih s kriminalistom, policijo in ravnateljico sta se družini obeh dijakov sestali doma pri enem od njiju. Tam so se pogovorili in razrešili konflikt.

Prav tako bi lahko dijaki še bolje zaznali nepravilno dogajanje. Obstaja velika verjetnost, da so ga, vendar pa je vprašanje, kako sami dijaki dojemajo takšna dejanja. Ali se jih zavedajo? Ali vedo, kako odreagirati? Ne nazadnje tudi, ali imajo pogum za reakcijo? Vsa ta vprašanja sprožajo teme, ki jih je potrebno analizirati ter vključiti v dodatna izobraževanja in ozaveščanja tako dijakov, staršev in učiteljev.

VAROVANJE ZASEBNOSTI IN UPORABA DRUŽBENIH OMREŽIJ

Skoraj vsak srednješolec uporablja družabna omrežja. Na socialnih omrežjih je potencial na področju učenja. Socialna omrežja uporabljajo z namenom, da na njih objavljajo podatke o sebi, kaj počnejo, kje se nahajajo. Na družabnih omrežjih dijaki niso previdni pri objavi svojih podatkov. Učimo jih, da njihov profil ne sme biti javen, da ga ne vidijo in delijo dalje ostali uporabniki interneta. Ostali

uporabniki interneta so tudi bodoči delodajalci, starši, učitelji itd. Težava socialnih omrežij je tudi, komu bodo podatki, ki jih posredujejo, na voljo. Večina podatkov, ki se pojavi na socialnih omrežjih, se težko trajno izbriše. Zelo pomembno je, da si dijaki (uporabniki družabnih omrežij) profil nastavijo kot zasebni profil. V zasebnem profilu določijo, kdo lahko vidi njihove podatke in objave. Kljub temu, da je profil zaseben, še vedno ni priporočljivo objaviti domačega naslova, telefonske številke, elektronskega naslova … Dostop do osebnih podatkov je velika priložnost za izvedbo zlorabe. Večina družabnih omrežij ima možnost deljenja lokacije. Pri objavi stanja, fotografije ali videoposnetka lahko označijo, kje in kdaj je bilo posneto. Objavo lokacije lahko v času vaše odsotnosti izkoristijo roparji, saj jim sporočajo, da vas ni doma. V izogib deljenju lokacije, izklopite lokacijo. Pri objavah na družbenih omrežjih naj spoštujejo zasebnost drugih. Brez njihovega dovoljenja ne objavljajo njihovih osebnih podatkov, fotografij ali posnetkov. V primeru, da objavijo brez njihove privolitve, jih lahko kazensko preganjajo. Med prijatelje ne smejo sprejemati neznane kontakte. Na spletu se lahko določeni ljudje pretvarjajo, kdo so.

IZVEDBA DELAVNIC

Na šoli poizkušamo redno izvajati dodatna izobraževanja na področju varne rabe interneta, splošne informacijske varnosti ter tudi na temo spletnega medvrstniškega nasilja. Teme, ki smo jih predelali na delavnicah, so bile:

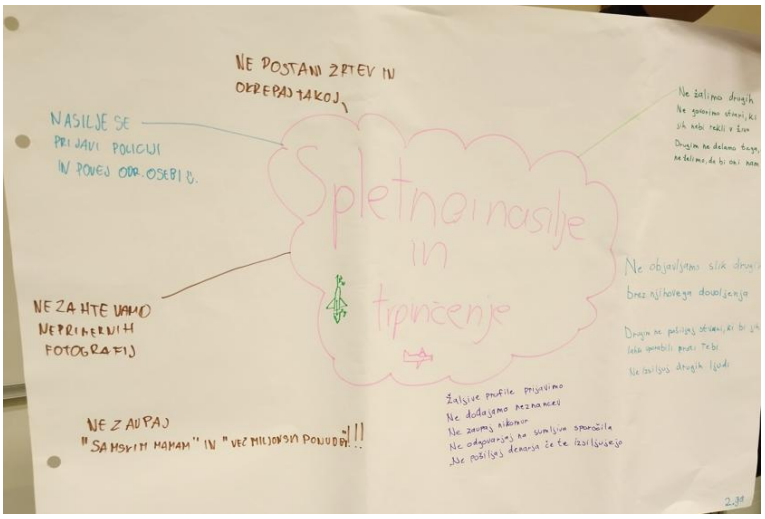
- pasti in nevarnosti interneta,
- varovanje zasebnosti in uporaba družbenih omrežij,
- varovanje pred krajo identitete,
- spletni in mobilni bonton,
- spletno nasilje in mobilno trpinčenje,
- internetne prevare,
- zasvojenost z mobilno tehnologijo.

Delavnice so se nanašale tudi na medsebojne odnose v šoli/razredu/med prijatelji. Cilji delavnic so bili, da se dijaki ozavestijo in kot rezultat delavnice izdelajo plakat.

Pri odločanju, kako te teme približati dijakom in jih zanje narediti zanimive, smo se odločili za izvedbo delavnic. Na delavnice povabimo različne strokovnjake iz obravnavanega področja. Seveda si želimo aktivnega sodelovanja vseh udeležencev delavnice. To poizkušamo doseči z interaktivnim pristopom in spodbujanjem k aktivnemu sodelovanju. K temu pripomorejo tudi vabljeni gosti ter sproščeno okolje, ki udeležence spodbuja k debati in sodelovanju. Ravno tako sprejemamo vsa različna mnenja in jih predelamo, saj tako zagotavljamo občutek varnosti v skupini, ki potem še pripomore k večji aktivnosti ter boljšim rezultatom delavnice.

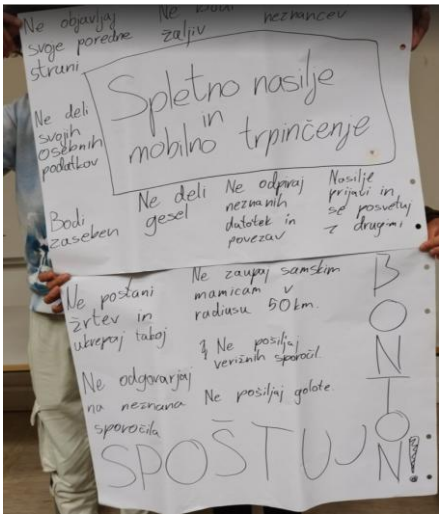
Na delavnicah v nekem trenutku formiramo manjše ekipe, ki jih spodbudimo k aktivnemu razmišljanju in izdelavi miselnih vzorcev na obravnavano temo. Z manjšimi skupinami lažje dosežemo vključevanje tudi tistih udeležencev, ki so manj aktivni v večjih skupinah. Na zaključku pregledamo, komentiramo in predebatiramo izdelke ter ugotovitve oziroma misli posameznih skupin.

V primeru delavnice »Spletno nasilje in mobilno trpinčenje« smo obdelali več tem in našli veliko primerov.

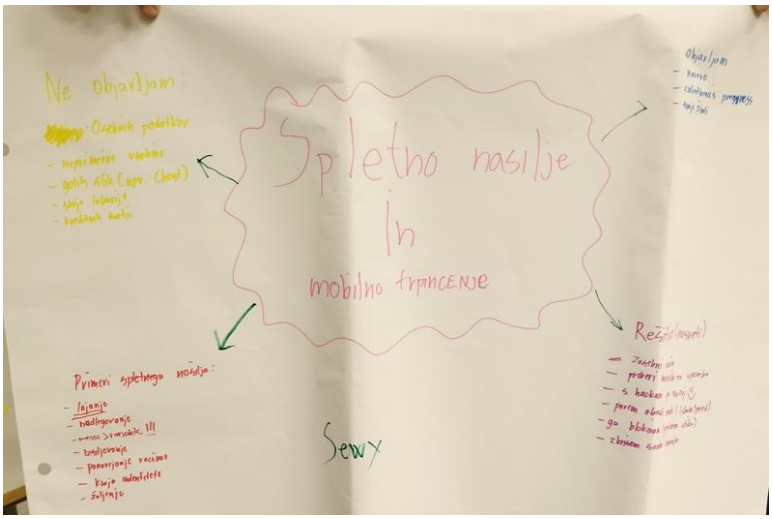


Slika1: Prikaz plakata o spletnem nasilju in trpinčenju

Največji poudarek smo dali temam, kakšni so preventivni ukrepi oziroma kaj lahko dijaki v prvi vrsti storijo sami, da se nasilju izognejo, ga preprečijo oziroma v čim večji meri omejijo.



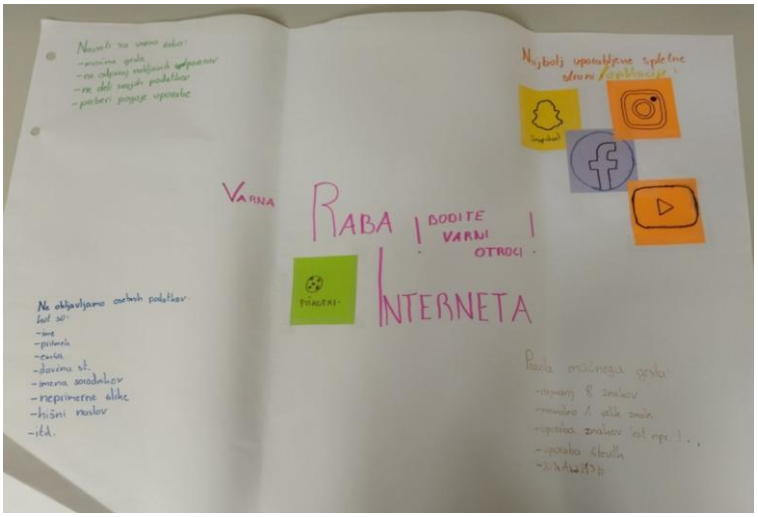
Slika 2: Prikaz plakata o spletnem nasilju in mobilnem trpinčenju



Slika 3: Prikaz plakata o spletnem nasilju in mobilnem trpinčenju

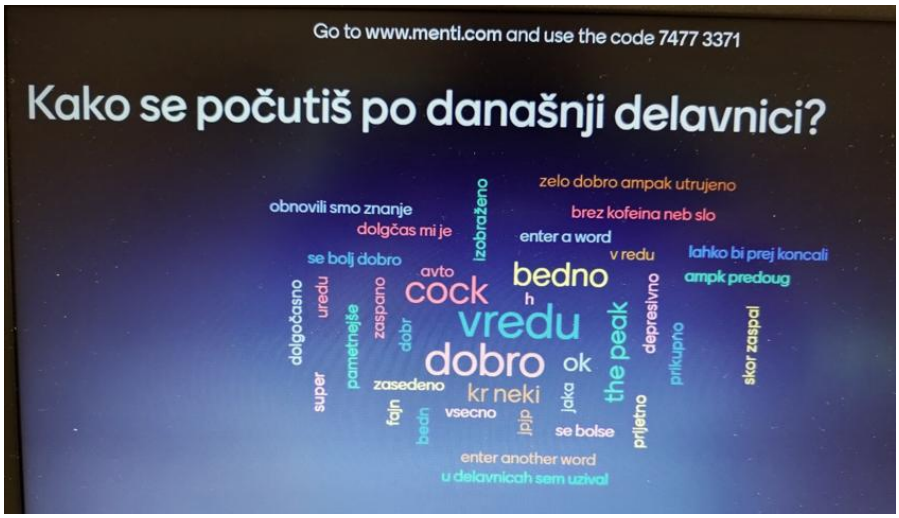
Podali smo tudi ukrepe in korake, kaj storiti, če smo sami žrtve spletnega nasilja in trpinčenja, ter tudi, kaj in kako ukrepati, če le tega zaznavamo v svoji okolici. Na koncu vsake delavnice je pomembno strniti misli, podati povzetke ter od udeležencev delavnice pridobiti povratno informacijo, kakšna se jim je zdela izvedba delavnice, ali jim je bila zanimiva ter kako se počutijo.

Vse to je pomembno predvsem za izvajalca delavnice, saj tako dobi povraten odziv, ki ga uporabi pri izvedbi ponovnih delavnic.



Slika 4: Prikaz plakata o varni rabi interneta

V vsaki izvedbi delavnice se pojavljajo udeleženci, ki jim zadeva ni zanimiva, hkrati pa preizkušajo meje oziroma želijo vzbujati pozornost z različnimi provokacijami. Na delavnicah smo take primere lahko prikazali tudi kot primere spletnega nasilja in trpinčenja. Vsekakor jih ne smemo ignorirati, pač pa takšne provokacije na pravilen način uporabiti kot primere.



Slika 5: Vprašalnik izveden po delavnici

ZAKLJUČEK

V šoli ugotavljamo, da dijaki preživijo preveč časa na mobilnih napravah in doma za računalniki. Zasvojeni so s spletom, raznimi socialnimi omrežji in spletnimi igricami. Hkrati ugotavljamo, da se premalo zavedajo vseh nevarnosti. Menimo, da je potrebno več dodatnega izobraževanja na področju informacijske varnosti. Ker so zaposleni eni od ranljivejših dejavnikov pri zagotavljanju varovanja

informacij, mora organizacija zagotoviti, da vsi zaposleni razumejo svoje odgovornosti in obveznost v zvezi z varovanjem informacij (Dreven, Markelj, 2020).

Šola lahko to izvede z vključevanjem primerov pri osnovnem izobraževanju iz informatike ali pri podobnih predmetih. Dodatno lahko izvaja delavnice ali dogodke na temo informacijske varnosti tako za dijake kot za učitelje. Na te delavnice je smiselno povabiti tudi zunanje strokovnjake. Ravno tako je smiselno obdelovati aktualne primere zlorab ter primere uspešnih razrešitev. Na ta način pridobimo aktivne udeležence, hkrati pa vsi lažje prepoznajo podobne primere v svojem okolju in ustrezno ukrepajo oziroma pridobljeno znanje in izkušnje uporabijo za večjo lastno varnost v svetu informacijske tehnologije.

Pri podajanju primerov je potrebno osvestiti udeležence, da gre pri zlorabah za kaznivo dejanje, za katero storilec nosi odgovornost in morebitne posledice. Oba primera, omenjena v članku, sta primera kršenja kazenskega zakonika. Gre za 143. člen, zlorabo osebnih podatkov, ki zajema kazniva dejanja zoper človekove pravice in svoboščine. Med drugim dotični člen ureja kazensko odgovornost oseb, ki zlorabijo osebne podatke na svetovnem medmrežju, prevzemajo identiteto drugih oseb, javno objavljajo občutljive podatke, javno objavo posnetkov brez privolitve … (https://zakonodaja.com/zakon/kz-1/143-clen-zloraba-osebnih-podatkov)

Socialna omrežja imajo veliko prednosti, a tudi kar nekaj slabosti. Zlorabe, ki se dogajajo na socialnih omrežjih, so zelo pogoste. Uporabniki socialnih omrežij se v veliki meri zavedajo le prednosti, na nevarnosti pa pozabijo. Zavedati se morajo, da potrebujejo močna gesla, ki naj jih občasno zamenjajo, in da potrjujejo prijatelje, ki jih res poznajo. Skušajo naj ne deliti svojih osebnih podatkov oziroma naj jih delijo čim manj. Kljub poplavi raznih informacij mora biti vsak posameznik dovolj ozaveščen in izobražen, da dokaj uspešno filtrira določene impulze. Hkrati se mora zavedati svojih dejanj, ki lahko vplivajo na njegovo informacijsko varnost, kot tudi dejanj, ki lahko povzročijo nasilje ali škodo drugim uporabnikom digitalnih vsebin.

LITERATURA IN VIRI

1. Bratuša, T. 2006. Hekerski vdori in zaščita. Ljubljana: Založba Pasadena.
2. Dečman Molan, L. 2022. Zbornik prispevkov: Izzivi globalizacije in družbeno-ekonomsko okolje EU: Informacijska varnost v šolskem okolju. Novo mesto: Univerza v Novem mestu. Spletno mesto: https://www.zalozba-unm.si/index.php/press/catalog/book/34 [Citirano 6. 4. 2022 ob 22.15 uri]
3. Dreven M, Markelj B. [et al] 2020. Informacijska varnost: Izzivi sodobne tehnologije. Ljubljana: Lexpera, GV Založba.
4. Infocenter: Zloraba sistema eAsistent. Spletna stran: https://infocenter.si/zloraba-sistema-easistent/ [Citirano 1. 4. 2022 ob 20.30 uri]
5. Kameleon: Bullying – informacije za starše. Spletna stran: https://svetovalnicakameleon.si/2019/11/bullying-informacije-za-starse/ [Citirano 7. 4. 2023 ob 23.35 uri]
6. Kazenski zakonik (KZ-1-NPB4). Spletna stran: https://zakonodaja.com/zakon/kz-1/143-clen-zloraba-osebnih-podatkov [Citirano 13. 4. 2023 ob 17.50 uri]
7. Safe.si: Varna gesla. Spletna stran: https://safe.si/nasveti/moja-identiteta-in-zasebnost/varna-gesla [Citirano 5. 4. 2023 ob 21.22 uri]
8. Slovenska tiskovna agencija: Na bistriški srednji šoli sum vdora v sistem e-redovalnice Spletna stran: https://www.sta.si/3022712/na-bistriski-srednji-soli-sum-vdora-v-sistem-e-redovalnice [Citirano 1. 4. 2023 ob 23.05 uri]
9. Stojan, I. 2018. Magistrsko delo: Spletno nasilje – nova oblika medvrstniškega nasilja. Ljubljana. Spletna stran: http://pefprints.pef.uni-lj.si/5016/1/Ines_Stajan.pdf [Citirano 2. 4. 2023 ob 15.40 uri]
10. Univerza v Mariboru: Priporočila za izbiro in rokovanje z gesli. Spletna stran: https://it.um.si/varnostna-politika/Strani/priporocila-za-izbiro-in-rokovanje-z-gesli.aspx [Citirano 5. 4. 2023 ob 21.02 uri]

CHALANGES OF INFORMATION SECURITY IN SCHOOL ENVIORMENT

Abstract: *Nowadays teachers and students are highly technically equipped in fields of mobile technology. This led to fact that they are exposed to threats in information security of every step. Many of them are not even aware of those threats and especially of the possible consequences. There are a lot of workshops and study materials in fields of information security to which students and teachers do have an easy access. We will take a closer look on the examples of how rules of information security are being abused. We will also provide critical points, preventive actions, and possible consequences of those abuses. In our organization we offer different workshops in the fields of information security where experts in those fields take part as guest speakers and role models. But even with all the effort we put into this topic, we still face many incidents, and that is main reason for additional education in fields of information security. Incidents are also a good case studies from which bot students and teachers can learn.*

Keywords: *preventive actions, information security, workshops, education, students*