Norwegian Embassy
Sarajevo

EGG
Economic Governance for Growth

UNDP

INTERNET SIGURNOST

SADRŽAJ

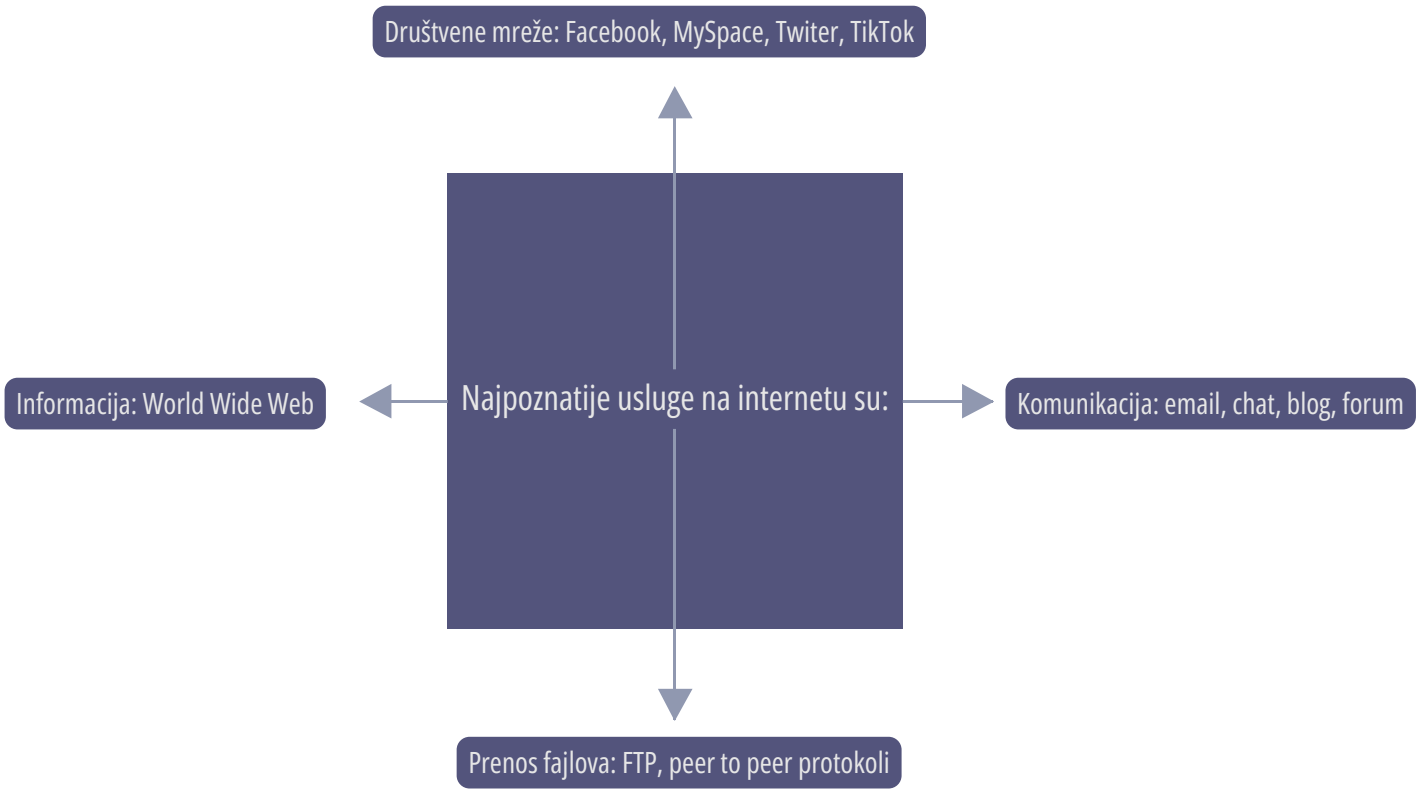
1 INTERNET - UVOD

Internet je javno je dostupna globalna mreža podataka koja povezuje računare i računarske mreže služeći se internetskim protokolima za njihovu komunikaciju. To je mreža svih mreža koja se sastoji od miliona kućnih, akademskih, poslovnih i vladinih mreža koje međusobno razmjenjuju informacije i usluge kao što su elektronička pošta, chat i prijenos fajlova te povezane stranice i dokumente World Wide Weba.

Internet je 1969. godine osnovalo Američko Ministarstvo odbrane. Zvao se ARPANET (prva četiri slova su kratica za Advanced Research Project Agency – Agencija za napredne istraživačke projekte, dok net označava računarsku mrežu). Cilj te mreže je bio da se poveže određeni broj računara u SAD-u.Radilo se o skupoj ideji, no Ministarstvu odbrane SAD-a novac nije nedostajao.Tokom šezdesetih godina vladao je hladni rat, zbog čega je Ministarstvo odbrane SAD-a strahovalo da bi se mogao dogoditi nuklearni napad. Inženjeri su morali projektovati Arpanet tako da on radi čak i ako se baci bomba na dio uspostavljene mreže te se uništi, dakle, čak i ako dio komunikacijskog dijela bude uništen, ostatak mreže treba nastaviti funkcionirati bez problema.

Servis World Wide Web izmišljen je u CERN-u u Švicarskoj 1989. godine, a izmislio ga je Britanac Tim Berners-Lee.

2 DOSTUPNE USLUGE NA INTERNETU



2.1 Informacija

World Wide Web (također WWW ili samo Web) je najpopularniji i najveći internet servis, a zbog njegove popularnosti mnogi ljudi smatraju da je on sinonim za internet, iako to nije točno. Na tom su servisu smještene internetske stranice, blogovi i wikiji. Te stranice može vidjeti svako, osim ako su zaštićene lozinkom ili su zbog nekog razloga blokirane (npr. vlade neke države blokiraju određene web stranice čiji stanovnici tokom razdoblja zabrane više ne mogu pristupati dotičnoj stranici).

Slika 1: WWW

WWW posjeduje tri vrlo važne osobine koje su ga popularizirale. To su:

Osobina WWW da jednostavno spoji sve oblike digitalnog sadržaja: tekstove, grafičke prikaze, audio i video sadržaje, koji su je određivali kao multimedij.

Multimedijalni sadržaji na WWW bili su relativno jeftini i brzi, što predstavlja dva važna zahtjeva koja su presudila u njenu korisnost na globalnom nivou.

WWW uspješno razvija i osobinu hipermedijalnosti, sposobnost istovremenog prikazivanja informacija uz pomoć više medija u više povezanih prozora i panela poznatih s računarskih operativnih sistema.

2.2 Komunikacija

Elektronska pošta (e-mail) i IM (instant messaging) se koristi za komunikaciju među korisnicima. E-mail poruke drugoj osobi stižu unutar nekoliko sekundi, a za njihovo slanje i primanje poruka i odgovora od drugih ljudi korisnik treba imati adresu elektronske pošte. Za slanje i primanje elektronske pošte postoje internetske stranice kao što su Hotmail, Gmail i Yahoo! Mail, ali i uslužni programi poput Outlook Expressa, Microsoft Outlooka (dio Microsoft Officea), Windows Live Maila, Thunderbirda, Eudore i Pegasusa. IM se često koristi za komunikaciju s prijateljima i poznanicima, te je sličan chatu zbog toga što se korisnik dopisuje s drugom osobom u realnom vremenu. Popularni IM programi su Teams, Trilian, Google Talk, Skype (osnovna namjena mu je internetska telefonija ali može poslužiti i za dopisivanje) i ICQ (prvi program za IM).

Slika 2: e-mail

Blog (anglizam, duži naziv weblog) je publikacija na Internetu (web-u) koja sadrži prvenstveno periodične članke u obrnutom vremenskom slijedu - najnoviji članci nalaze se na vrhu stranice. Blogovi mogu biti individualni i kolaborativni. Terminološki za sada nema dinstinkcije kao u engleskom jeziku gdje se termin weblog češće koristi za kolaborativne, a blog za individualne projekte. Mogu biti u obliku časopisa, tematski, osobni. Mogu biti povezani u grupe, tematski ili vezano uz domenu koju se nalaze - blogosfera.

Slika 3: Blog

Internetski forum je usluga na Internetu koja omogućava razmjenu mišljenja među učesnicima upotrebom web preglednika. Sve poruke koje korisnik napiše i pošalje na forum vidljive su svim ostalim učesnicima foruma. To nalikuje na oglasnu ploču (engl. message board) na kojoj učesnici ostavljaju poruke. U načelu poruke na forumu mogu ostavljati i čitati učesnici interneta bez ograničenja. Učesnici su najčešće anonimni jer se pri slanju poruke na forum ne mora navesti pravi identitet. Zbog lakšeg snalaženja forum je obično podijeljen u nekoliko skupina prema temama razgovora. Jednostavnost upotrebe i mogućnost anonimne rasprave o različitim temama jedan je od glavnih razloga popularnosti foruma. Za internetski forum se dovoljno služiti web preglednikom. Poruka poslana na jedan forum vidljiva je samo na tom forumu. Forum se uglavnom sastoji od mnogobrojnih kategorija unutar kojih se nalaze teme koje otvaraju i započinju korisnici. Svaka tema ima svoju diskusiju u kojoj se učestvuje pisanjem, odnosno objavljivanjem postova. Svi razgovori/diskusije ostaju sačuvani na forumu dok ih ne obriše moderator (stvarna osoba).

Slika 4: Forum

2.3 Prenos fajlova

Prenos fajlova putem interneta (na engleskom download i upload) označava prenos digitalnih podataka sa središnjih sisitema kao što su FTP server ili Mail server, na privatni kompjuter i obrnuto.

U svakodnevnom govoru skidanje s interneta, označava preuzimanje fajla s web servera na privatni kopjuter ili neki drugi medij za pohranu podataka. U nastavku navodim primjer skidanja fajlova putem torrent aplikacija.

Postavljanje fajla (upload) je prijenos digitalnih podataka s računara na središnji sistem. U nastavku ću navesti prenos podataka na Cloud i objasniti značenje.

Primjer softvera za skidanje fajlova sa interneta je torrent. Naziv torrent je nastao od ekstenzije .torrent, a to su jednostavno fajlovi koji sadrže informacije o drugim fajlovima i folderima koje treba prenijeti. Kada npr. skinete torrent za film, ovaj torrent fajl sadrži informacije koje će vam omogućiti da dođete do tog filma.

Uobičajeni način za prenos fajlova putem interneta radi tako što postoji centralni server na kome se nalaze svi fajlovi i koji komanduje kuda oni idu.

Torenti ne zavisi od centralnog servera za čuvanje podataka. Umesto toga, podaci se čuvaju na računarima korisnika koji učestvuju u mreži. Uspostavlja se peer-to-peer (P2P) komunikacijski protokol između korisnika, koji rastavlja fajlove na komade i premešta ih od onih koji na svom računaru imaju željeni fajl (seeders) do onih koji žele da downloaduju taj fajl (leechers).

Drugim riječima kada download-ujete fajl uz pomoć torrenta vi taj fajl kopirate direktno sa računara nekog od korisnika torrent mreže. Za ostvarivanje ove veze koristi se klijent za torrent-e, program koji čita sve informacije u .torrent fajlu i povezuje korisnike da bi omogućio razmenu podataka. Zbog mogućnosti ilegalnog dijeljenja podataka torrent-i su na lošem glasu i mnogi misle da je bilo kakvo korišćenje torrent-a nelegalno, ali to nije tako. Mnoge kompanije koriste torrent mrežu za dijeljenje podataka, a mnogo sadržaja na torrent sajtovima nije ilegalna.

Torrent-i su kao servis izuzetno praktični i korisni, a to što se zloupotrebljavaju za skidanje piraterije, to je već nešto drugo. Prilikom korištenja torrent-a treba biti odgovoran/na i preko torrent-a skidaie i dijeliti samo legalne fajlove.

Cloud se odnosi na servere kojima se pristupa putem interneta, te softver i baze podataka koji se izvode na tim serverima. Cloud serveri se nalaze u podatkovnim centrima širom svijeta.
Koristeći cloud computing, korisnici i kompanije ne moraju sami upravljati fizičkim serverima niti pokretati softverske aplikacije na svojim mašinama.

Umjesto toga, cloud korisnicima omogućuje pristup istim fajlovima i aplikacijama s gotovo bilo kojeg uređaja, jer se pohrana odvija na serveru u data centru, umjesto lokalno na korisničkom uređaju.

Ovo je razlog zašto se korisnik može prijaviti na svoj npr. facebook račun na novom mobitelu nakon što prestane koristiti stari uređaj, i još uvijek pronaći svoj stari račun sa svim svojim fotografijama, video zapisima i razgovorima.

Slika 5: Cloud

Cloud servisi nešto su što je danas jednostavno potrebno. Kompanije su vrlo brzo prepoznale njihovu korist, te gotovo svaka danas koristi Google Drive ili OneDrive koji su bez premca kad je u pitanju poslovno korištenje.

2.4 Društvene mreže

Društvena mreža je vrsta internetske usluge, koji se najčešće javlja u obliku platforme ili web-stranice. To je internetski prostor, koji služi za međusobno povezivanje korisnika. Danas postoje stotine ovakvih servisa.

Slika 6: Društvene mreže

Prvi oblici društvenih mreža javljaju se 90.-ih godina 20. vijeka. Kod nekih je razgovor dozvoljen samo preko registracije, dok je kod drugih potreban samo nadimak (eng. nickname). U takvim sobama, obično postoji lista sa strane, gdje korisnik može vidjeti sve druge aktivne korisnike u tom trenutku. Na donjem dijelu ekrana, nalazi se mjesto, gdje korisnik piše poruke. Servisi društvenih mreža stalno se poboljšavaju, dajući nove mogućnosti korisnicima. Pojavljuju se nove društvene mreže s novim mogućnostima. Ovakve mreže, pored prvobitne uloge komunikacije, imaju i ulogu marketinga, promovirajući druge web-stranice i niz različitih usluga. Korisnici ne mogu komunicirati sa svim članovima koji se nalaze na mreži, već mogu isključivo s kontaktima (engl. contacts). Osim standarnog načina, korisnici mogu komunicirati preko video snimki, što olakšava komunikaciju. Takav tip komunikacije može biti između dva ili više korisnika. Među najpopularnijim modernim sistemima za komunikaciju na internetu su: Facebook, Twitter, YouTube, Instagram, Skype i dr.

3 NEŽELJENE POSLJEDICE KORIŠTENJA INTERNETA

Kao što u svakodnevnom okruženju na različite načine pazimo na svoju sigurnost npr. u saobraćaju gdje se pridržavamo propisanih saobraćajnih pravila, isto tako i u online okruženju moramo voditi računa o sigurnosti na Internetu. Kada govorimo o sigurnosti u online okruženju na Internetu mislimo prije svega na sigurnost podataka i sigurnost korisnika tih podataka.

Korištenjem Interneta nailazimo na različite potencijalne opasnosti koje mogu ugroziti sigurnost naših računara i podataka na njima. Sav neželjeni i zlonamjerni sadržaj na Internetu može se podijeliti u nekoliko skupina.

Slika 7: Opasnosti na internetu

Svaka pojedina vrsta na određeni način uništava naš računar i pri tome naši podaci koje imamo u računaru postaju izloženi zloupotrebi. Čitajući dalje sadržaj, saznati ćete ponešto o svakoj vrsti, kako je prepoznati te kako se zaštititi.

3.1 Elektroničke bolesti

Od svih elektroničkih bolesti računarski virusi su daleko najpoznatiji. Vjerojatno je razlog tome, što se često pod pojmom računarskog virusa u svakodnevnom govoru podrazumijevaju različite vrste štetnih, zlonamjernih programa koji se zove malver (malware je skraćeno od malicious software). Računarski virusi su samo jedan od štetnih malver programa (osim virusa postoje i crvi, „trojanci"..).

Računarski virusi

Računarski virus je zlonamjerni program koji svojim pokretanjem može zaraziti računar na način da se bez znanja korisnika računara, kopira u programe i fajlove na računaru. Tim postupkom virus postaje dio zaraženog „zdravog" programa ili dokumenta i prilikom pokretanja tog programa, virus se aktivira. Virusi se šire s jednog računara na drugi preko zlonamjernog programskog koda putem Interneta, attachmenta u e-mail porukama ili putem medija npr. USB, CD, DVD. Jednostavno možemo reći da virus u računaru djeluje na sličan način kao i virus u organizmu čovjeka koji napada zdrave stanice i postepeno ih čini zaraženim i bolesnim. Jedino što računarski virus razlikuje od biološkog virusa je činjenica da računarski virus uvijek napiše čovjek - ne može nastati spontano.

Slika 8: Računarski virus

Može se zaštititi od virusa instaliranjem antivirusnih programa, međutim, treba opreznosti prilikom odabira antivirusa, jer postoje i lažni antivirusni programi.

Koristeći internet mogu se javiti lažna antivirusna upozorenja. Kako možete odrediti da li je upozorenje o virusu stvarno ili lažno? Dok pretražujete web, pripazite na ove znakove upozorenja:

Neprepoznatljiv antivirusni softver: Ako vidite upozorenje o virusu, zapitajte se da li izgleda kao antivirusni softver koji inače koristite. Ako ne, ovo je glavna crvena zastava. Ako primijetite da upozorenje dolazi od antivirusnog softvera koji nikada niste instalirali, vjerovatno imate posla s lažnom virusnom prevarom i ne biste trebali reagirati na upozorenje.

Neoperativni antivirusni programi: Za razliku od pouzdanog antivirusnog softvera, većina lažnih upozorenja o virusima su lažne aplikacije koje stvaraju iskačući prozor s vezom na lažno preuzimanje antivirusa ili vezu za plaćanje.

Česta antivirusna upozorenja i iskačući prozori: Da bi podstakli vašu prirodnu reakciju straha i anksioznosti, lažni antivirusni softver će uključivati česte iskačuće prozore. Prevaranti primjenjuju ovu taktiku kako bi vas požurili da im platite, slučajno preuzmu još zlonamjernog softvera ili oboje.

Sumnjivi linkovi i prilozi: Kao i kod bilo kojeg iskačućeg prozora ili web stranice, trebali biste biti oprezni sa sumnjivim vezama i prilozima. Iako se može činiti prirodnim brzo kliknuti na nešto što tvrdi da pomaže u zaštiti vašeg računara, ali bolje vam je izbjegavati bilo kakve veza sa iskačućim prozorima.

Zahtjevi za novac: Ako upozorenje o virusu uključuje zahtjev za plaćanje, vjerovatno je da imate posla s lažnim antivirusnim softverom. Da biste bili sigurni, nikada ne dajte svoje podatke o plaćanju nepoznatim web stranicama.

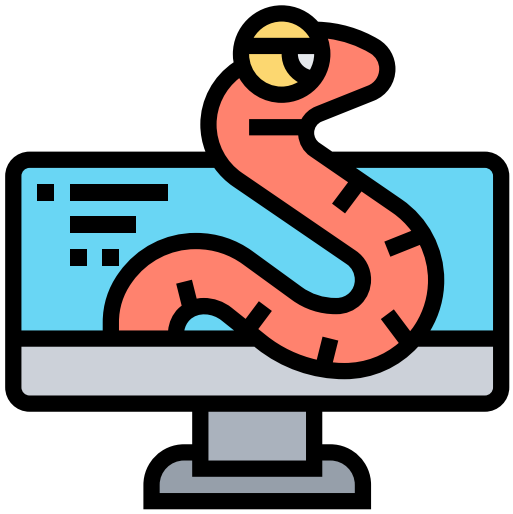
Sistem se zamrzava i sporije radi: Ako lažni antivirusni softver prati male brzine ili se sistem zamrzava, možda imate posla s prevarom. Ovi lažni virusi mogu uključivati i animacije zbog kojih izgleda kao da se vaš računar ruši. Ovo je još jedna taktika koja se koristi da mislite da vaš računar ima virus.

“Otmica” pretraživača: Kada imate posla s lažnim antivirusnim softverom, možete primijetiti nasumične promjene koje se dešavaju u vašem web pregledniku. Uobičajeni primjeri uključuju promjene na vašoj početnoj stranici ili novoinstaliranim alatnim trakama. Ako doživite ovo, vjerovatno je da je upozorenje o virusu rezultat lažne antivirusne prevare.

Imajući na umu ove “crvene zastavice” kada ste na internetu, uvelike ćete smanjiti rizik da lažnu antivirusnu prevaru zamijenite za stvarni problem s vašim računarom.

Računarski crvi

Računarski crvi su programi koji sami sebe umnožavaju i šire se putem računarske mreže. Za razliku od računarskih virusa, crvi ne zahtjevaju postojanje fajla za kojeg bi se „prikačili“ da bi djelovali .



Slika 9: Računarski crv

Trojanski konj

Trojanski konj je oblik štetnog programa koji se korisniku lažno predstavlja kao neki korisni program kako bi mu korisnik dozvolio instalaciju. Kada se instalira, trojanac preuzima nadzor nad vašim računarom radeći štetu na njemu. Termin je, zbog analogije, preuzet iz grčke mitologije (da bi trojanac „ušao“ u vaš računar vi ga morate propustiti).Uobičajeni način na koji se moguće zaraziti trojancem je:

- preuzimanjem zaraženog softvera (ključevi za ilegalno korištenje komercijalnih programa (crackovi) su često zaraženi trojacem)
- otvarajući e-mail attachment sumnjivog sadržaja
- posjećujući „ zloćudne“ web stranice sa video sadržajima
- preko ranjivosti softvera (ukoliko ne ažuriramo softver na našim računarima)

Antivirusni i drugi anti-malver programi pružaju zaštitu od trojanskih konja. Postoje i alati koji su specijalizirani isključivo za trojanske konje.

Kako se zašititi od elektroničkih bolesti?

Općenito, da bi se odbranili od zaraze „elektroničkih bolesti“ koristimo antivirusne programe. Antivirus je program koji se koristi za zašititu, identifikaciju i uklanjanje računarskih virusa i ostalih malver programa. Moderni antivirusni programi se dizajniraju tako da štite računarski sistem od što većeg broja različitih mogućih malicioznih programa (virusa, crva, trojanskih konja, spywarea, adwarea..).

Jednom instalirani antivirusni program potrebno je neprestano obnavljati odnosno ažurirati. Kako svakodnevno nastaju novi virusi i ostali štetni programi, a antivirusi uklanjaju samo poznate prijetnje, ažuriranjem antivirusnog programa vrši se obnavljanje tog antivirusa odnosno "upoznavanje" antivirusa sa novim mogućim prijetnjama da bi ih mogao prepoznati ukoliko dospiju u vaš računar.

Neki od najpoznatijih antivirusnih programa su: Bitdefender Antivirus Plus,Norton AntiVirus Plus, ESET NOD32 Antivirus,G Data Antivirus,Malwarebytes Premium,McAfee AntiVirus itd.

4 ŠTETNA PRIMJENA INTERNETA

Današnji učenici odrastaju u sve složenijem svijetu, živeći svoje živote na internetu i van njega. Ovo predstavlja mnoge uzbudljive mogućnosti – ali i izazove.

Postoji niz potencijalnih štetnih primjena interneta koje možemo grupisati u sljedeće kategorije:

- Sadržaj
- Kontakt
- Ponašanje
- Način korištenja

U ovisnosti od toga u koju potencijalnu grupu svrstamo sadržaj interneta biramo i način kako zaštiti djecu.
U nastavku navodim detaljnija objašnjenja kategorizacije kao i načine zaštite.

Sadržaj

U ovu kategoriju možemo svrstati sve štetne posljedice koje se dese kada smo izloženi nezakonitom, neprikladnom ili štetnom sadržaju. Na primjer: pornografija, lažne vijesti, rasizam, samopovređivanje, samoubistvo, ekstremizam...

Na primjeru lažnih vijesti možemo pokazati zašto je sadržaj štetan.

U medijskom svijetu i na društvenim mrežama sve se češće susrećemo s raznim dezinformacijama i lažnim vijestima. Savremene informacijske i komunikacijske tehnologije samo su olakšale i ubrzale dijeljenje takvih informacija, pa su i posljedice dalekosežnije. Stoga je Svjetska zdravstvena organizacija pojavu masovnog širenja lažnih vijesti nazvala infodemijom. Infodemija je, dakle, prekomjerna količina informacija o nekom problemu, koja otežava pronalaženje rješenja.

Uzmimo za primjer pandemiju Corona virusa koja je iza nas. Tokom zdravstvene krize, infodemija može ugušiti vjerodostojne informacije i omogućiti lakše širenje glasina, otežavajući učinkovitu javnozdravstvenu reakciju. Informacije se mogu širiti brže od virusa, a kao jedna od stvari koja tome ide u prilog navodi se rast korištenja digitalnih komunikacija i društvenih mreža. Informacije s interneta mogu negativno utjecati na našu psihu, svakodnevni život i ponašanja, te dodatno otežavajući krizu.

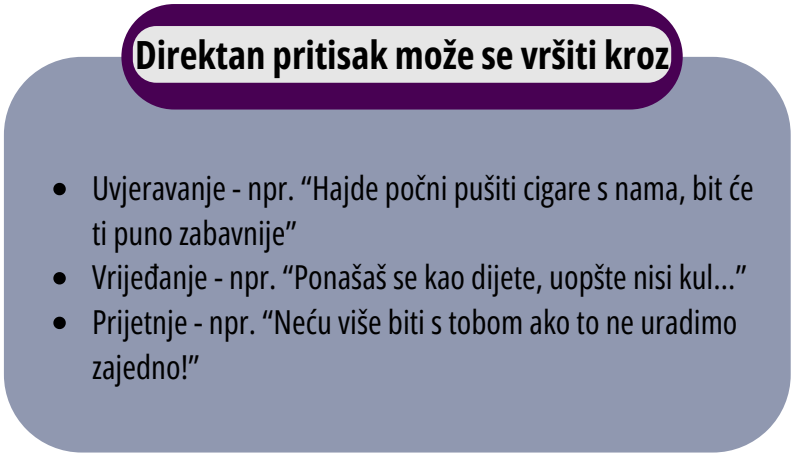
Kontakt

Kontakt podrazumijeva biti podvrgnut štetnoj onlajn interakciji sa drugim korisnicima. Na primjer: pritisak vršnjaka, komercijalno oglašavanje i odrasli koji se predstavljaju kao djeca ili mladi s namjerom da ih iskoriste.
Na primjeru pritiska vršnjaka navešću kako kontakt ostvaren putem interneta može biti štetan. Na narednoj slici vide se i pozitivne i negativne strane vršnjačkog „pritiska“

Slika 10: Vršnjački pritisak

Vršnjački pritisak može bit oblikovan na više načina:

- direktan – kada ti netko govori što bi „trebao/la“ raditi
- indirektan – kada cijelo društvo ili bliska osoba radi nešto što inače ne bi sam/a radio/la



Slika 11: Direktan vršnjački pritisak

Ponašanje

Ponašanje na internetu koje povećava vjerovatnoću za nastanak štete ili je direktno uzrokuje. Na primjer, pravljenje, slanje i primanje eksplicitnih slika, dijeljenje drugih eksplicitnih slika i nasilje.

Kao primjer za ovu kategoriju,, navodim dijeljenje ekspicitnih fotografija.

Kada netko šalje provokativne ili seksualne fotografije, slike i video uratke to se naziva sextingom. Primanje ili slanje poruka se najčešće odvija putem mobitela, ali i putem društvenih mreža i aplikacija. Mogu se izmjenjivati s prijateljima, curom ili dečkom ili nekim koga upoznaš online. Iako ponekad dijeljenje takvih fotografija i poruka djeluje kao nevini flert, šala ili igra, važno je znati da njihovo slanje može imati ozbiljne posljedice. Materijali se mogu naći posvuda i mogu ih vidjeti svi, a mogu i poslužiti kao sredstvo ucjenjivanja. Jednom kada ovi sadržaji postanu dostupni svima, nemoguće ih je kontrolirati. Stoga je važno imati uvid u moguće posljedice sextinga i ponašati se tako da do njih ne dođe. Do sextinga može doći iz više razloga, a neki od njih su:

- mišljenje da svi to rade
- dokazivanje vlastite seksualnosti
- pritisak vršnjaka, dečka/cure ili simpatije
- uznemiravanje, prijetnje i ucjene od poznate ili nepoznate osobe
- želja za nečijim odobravanjem
- potpuno povjerenje u osobu u koju smo zaljubljeni
- veza na daljinu
- ponos na svoje tijelo i želja da se podijeli s drugima
- osjećaj da to dugujemo osobi s kojom smo u vezi

Finansijska korist

Rizici kao što su kockanje na internetu, neprikladno oglašavanje i finansijske prevare.
Kao primjer lošeg načina korištenja interneta navodim online kockanje.
Online kockanje je oblik hazardnih igara i ovisnosti o njima. Putem interneta, ušlo je u naše domove i osvojilo simpatije djece i adolescenata, nudeći im lažnu nadu u veliki dobitak u igrama na sreću kao što su rulet, poker, klađenje i druge vrste kockarskih igara.

Slika 12: Internet kao ovisnost

Uzevši u obzir da onlajn kockanjem izostaje stvarni osećaj trošenja novca, veća je verovatnoća gubljenja kontrole u trenutku kockanja, u smislu češćeg kockanja sa značajnim većim ulogom, bez percepcije da se radi o stvarnom novcu. Svojstva internetskog kockanja mogu predstavljati posebnu opasnost po mentalno zdravlje.

Tipični razlozi za online kockanje uključuju lakoću i dostupnost, ali i dosadu te potiskivanje negativnih emocija. Stres i financijska kriza mogu biti dodatni okidači za kockanje.

Kockanje se na prvu može činiti kao idealno rješenje u obliku lake zarade, uz malo sreće kroz nekoliko klikova. Kao dva važna prediktora kockanja navode se aleksitimija (nedostatak prepoznavanja i odsutnost senzibilnosti za vlastite i tuđe emocije) i impulsivnost. S vremenom oblik kockanja prestaje biti važan, dovoljna je činjenica da je novac uložen te da postoje neizvjesnost i uzbuđenje oko ishoda, što je zapravo i smisao kockanja.

Istraživanja potvrđuju da su simptomi anksioznosti i depresivnosti prisutni kod gotovo 50 % ispitanika koji su se suzdržavali od kockanja, što jasno ukazuje na zaključak da je riječ o ovisnosti.

U nastavku slijedi najvažnija statistika o internet sigurnosti za 2023 godinu preuzeta sa sajta: https://zipdo.co/statistics/online-safety/

- 27% djece od 7 do 17 godina susrelo se sa štetnim sadržajem na internetu
- Oko 41% ljudi doživjelo je barem jedan negativan ishod zbog prisustva na internetu
- 95% 3-4-godišnjaka pristupa internetu u prosjeku 8 sati sedmično
- 1 od 25 mladih primio je online seksualni poziv u kojem je postojao pokušaj uspostavljanja kontakta van interneta
- Oko 50% žrtava onlajn uznemiravanja nije u stanju da identifikuje svog uznemiravača
- Otprilike 143 miliona Amerikanaca otkrilo je svoje lične podatke prilikom kršenja podataka 2017
- Oko 75% djece je spremno dijeliti lične podatke na internetu u zamjenu za robu ili usluge
- 211 miliona Amerikanaca iskusilo je online krađu identiteta ili prevaru
- Preko 60% slučajeva seksualnog zlostavljanja na internetu uključuje počinitelja koji je žrtvu upoznao na društvenim mrežama
- 15% tinejdžera iskusilo je uznemiravanje na internetu
- Svako treće dijete primilo je link do zlonamjerne stranice
- Više od dvije trećine djece mlađe od 12 godina koristi društvene mreže
- 90% tinejdžera se osjeća samopouzdano u upravljanju svojom privatnošću na internetu
- Otprilike 20% web stranica namijenjenih djeci ima barem jednu funkciju za ćaskanje
- Seksting (slanje seksualno eksplicitnih poruka ili slika putem mobilnog telefona) je porastao za 183% u posljednje 4 godine
- Do 2025. godine oko 3 milijarde ljudi će koristiti stranice društvenih mreža
- 62% djece koja doživljavaju zlostavljanje na internetu ne prijavi incident svojim roditeljima
- Gotovo 50% ljudi ne zna kako zaštititi svoje podatke na internetu

5 NAČINI ZAŠTITE

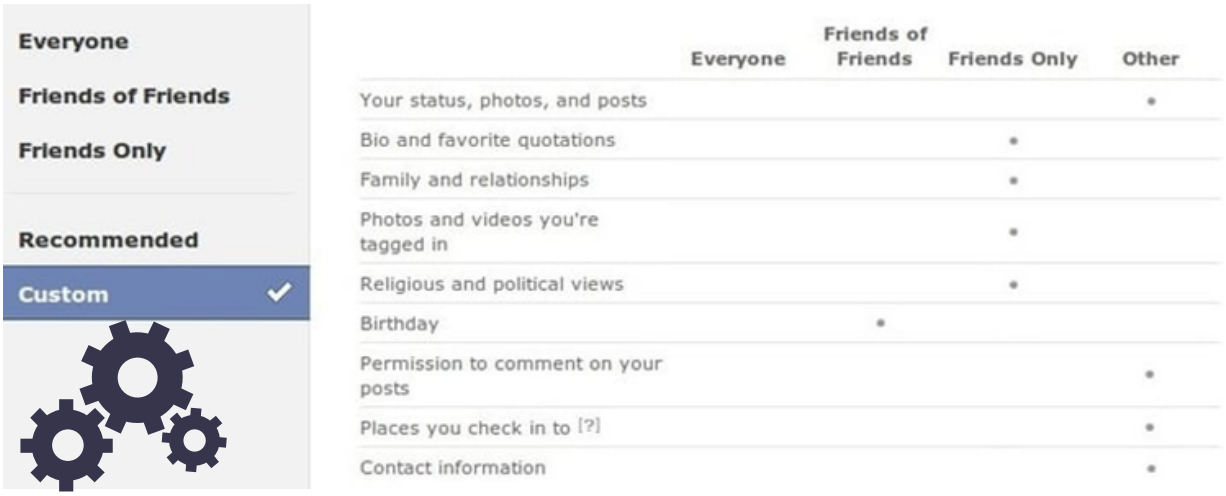
Danas su učenici stalno povezani sa svijetom oko sebe putem interneta – i u dobru i u zlu. S jedne strane, ovo učenicima daje nevjerovatan pristup najvećoj svjetskoj bazi znanja. Ali to je i zastrašujuće jer možda ne razumiju principe sigurnosti na internetu. Na kraju krajeva, internet je mač sa dvije oštrice. Omogućava nam da vidimo, istražujemo i razumijemo svijet - ali svijet nas može vidjeti. To je zastrašujuća pomisao, posebno kada se odnosi na djecu. Kako onda osigurati da vaši učenici znaju kako da ostanu sigurni na internetu? Morate naučiti sigurnost na internetu.Najbolji način da to učinite je da postavite temelje za razumijevanje bezbjednog ponašanja na internetu od strane vaših učenika.

5.1 ZAŠTITA PRIVATNIH PODATAKA

U eri pametnih telefona i društvenih medija, nikada nije bilo više načina da s nekim kontaktirate. Također nikada nije bilo toliko načina da se nađe neko. Iako mnoge društvene mreže ne dozvoljavaju nikome mlađem od 13 godina da se prijavi, ne čine ništa da spriječe ljude da lažu o svojim godinama.Dakle, svi vaši učenici mogu biti na društvenim mrežama, čak i ako nisu dovoljno stari sa stajališta politike. Niko ih zaista ne može zaustaviti jer im je potrebno samo 30 sekundi da dobiju nalog, a (što je još gore) niko neće ukloniti njihove profile.Kako možete pomoći svojim učenicima da ostanu zaštićeni kada se mogu prijaviti na ove društvene mreže, a da niko drugi to ni ne zna?

Društvene mreže imaju postavke privatnosti

Zbog negodovanja protiv načina na koji društvene mreže prikupljaju korisničke podatke, sada imaju opcije privatnosti koje vam (i vašim učenicima) omogućavaju da ograničite ono što drugi vide na mreži. Neke društvene mreže to nazivaju "postavkama privatnosti", a druge ih mogu nazvati "sigurnosnim postavkama".



Slika 13: Sigurnosne postavke

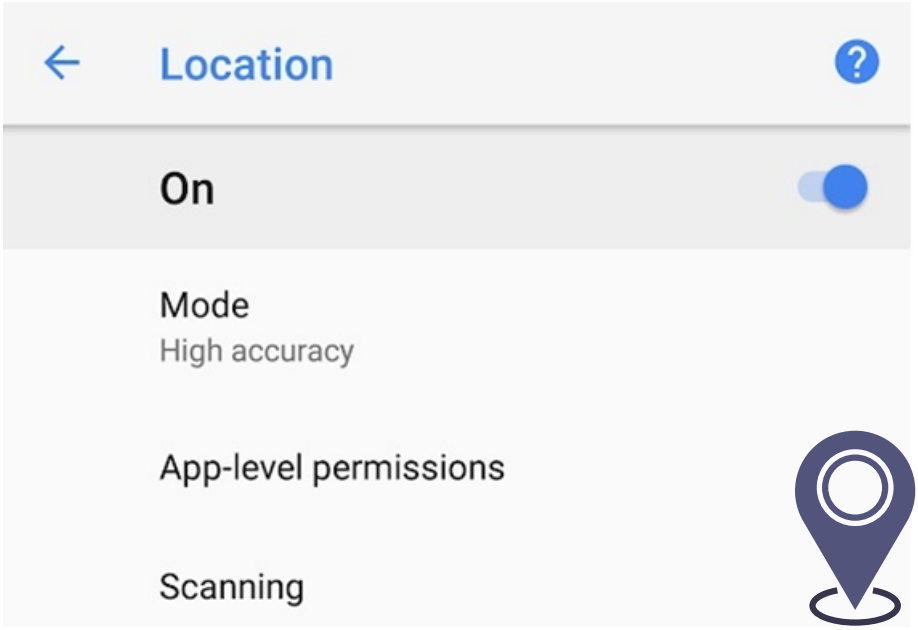
Ove postavke vam omogućavaju da blokirate druge korisnike da vide vašu adresu e-pošte, kućnu adresu, broj telefona, datum rođenja i još mnogo toga. Ako vaši učenici već koriste društvene mreže, sljedeća stvar koju trebaju učiniti je postaviti postavke privatnosti. Ovo je važno jer većina mreža nema podrazumevano omogućene postavke privatnosti. Morate ih sami promijeniti, i to odmah.

Prijava za društvene mreže pomoću lažnih naloga e-pošte

Porast besplatnih usluga e-pošte omogućio je učenicima da se prijave za više naloga e-pošte istovremeno. Ovi računi e-pošte mogu imati korisnička imena i informacije koje su potpuna besmislica. Većina platformi za e-poštu omogućit će im da kreiraju račun e-pošte bez ikakvog pitanja zašto ili koliko često će ga koristiti. Ako se učenici prijave za račun e-pošte s lažnim imenom, a zatim se registriraju za društvenu mrežu koristeći taj račun e-pošte, dodaju još jedan zid između sebe i stranaca na društvenim mrežama. Najbolje od svega, taj nalog e-pošte je efektivno beskoristan u slučaju da je društvena mreža hakovana ili proda podatke svojih korisnika drugoj kompaniji.

Odbij i isključi postavke lokacije

Jedna od najvećih opasnosti društvenih medija je da svima govore gdje ste kad god nešto objavite. Tvoji roditelji znaju. Tvoji prijatelji znaju. I internet progonitelj za kojeg niste znali da ga imate također zna. Ovo je izuzetno opasna karakteristika za učenike. Omogućuje svima da znaju gdje se nalaze dodirom na ekran ili klikom na link. Gotovo svaka društvena mreža nudi ove opcije. Ako učenici zaista žele da budu sigurni, moraju isključiti usluge lokacije i modificirati svoje objave tako da ne prikazuju njihovu lokaciju. Ako to ne urade, ključno je da naglasite učenicima koliko su ove karakteristike opasne.U pravilu bi također trebali isključiti postavke lokacije na svojim pametnim telefonima, ako ih imaju.



Slika 14: Usluge lokacije

Ponekad će društvene mreže automatski povući podatke o lokaciji pametnog telefona kako bi ih dodale u objavu. Nije baš etički, ali studenti moraju znati o tome kako ne bi emitovali svoju lokaciju svaki trenutak svakog dana.

Valjanost lozinke

Lozinke su metoda potvrde izbora za svakoga ko ima nalog u bilo kojoj kompaniji ili aplikaciji. Prednost lozinki je to što se lako pamte. Na kraju krajeva, oni su samo nekoliko slova i brojeva na tastaturi. Loša strana lozinki je to što je lako napraviti onu koju haker može pogoditi ili shvatiti! Kao rezultat toga, bitno je da vaši učenici nauče kako da kreiraju i efikasno koriste lozinke. Stoga kreiranje sigurnih lozinki može biti jedna od najvažnijih aktivnosti za sigurnost na internetu za učenike. Sve u svemu, lozinke su prilično jak način da se računi zaštite od vanjskih korisnika. Zato prevaranti moraju smisliti pametne načine za poništavanje vaše lozinke ili zaobići vaše trenutne sigurnosne postavke na računu. Ali da bi ih zaista dobro koristili, učenici moraju znati najbolje načine da svoje račune čuvaju na internetu.

Ovo je suštinski "trik" za kreiranje lozinke. To mora biti nešto čega se možete sjetiti, ali ne može biti nešto što neko može pogoditi. Najbolji način da to učinite je da razmislite o nečemu što je potpuno čudno ili jedinstveno - čak i ako je besmisleno brbljanje - i zapamtite šta je to. Općenito, učenici bi se trebali držati podalje od korištenja imena ili ideja koje im se sviđaju. Najjače lozinke neće imati apsolutno nikakve veze s njima lično, što će hakerima učiniti gotovo nemogućim da ih pogode. Nizovi nepovezanih riječi u kombinaciji sa nasumičnim znakovima, brojevima i velikim slovima imaju tendenciju da rade odlično. Uzmimo primjer da vidimo kako vi i učenici možete napraviti moćne lozinke.

Niz nepovezanih riječi: anvilmobysaunaduck
Sa nasumičnim znakovima: @nvilm()bysaunaduck
Sa slučajnim brojevima: @nvi1m()bysaun4duck
Sa nasumičnom upotrebom velikih slova: @nvI1m()bYSaun4duCK

Po svemu sudeći, ovu su jake lozinke! Ali stvaranje jake lozinke je samo pola bitke!

- **Kreiranje nove lozinke za svaki nalog**

Jedna lozinka može nekome omogućiti pristup višestrukim dijelovima vašeg života, što je posebno loše za djecu. Ovo olakšava nekome da vas lažno predstavlja, uhodi ili opljačka – a dok shvatite šta se dogodilo, skoro uvijek je prekasno. Da biste zaista ostali sigurni, koristite drugu lozinku za svaki račun koji otvorite! Tako ste sigurni da ako neko sazna jednu lozinku, neće znati sve.

- **Nikada ne pričajte o lozinkama**

Ako će lozinka obaviti svoj posao, može je znati samo jedna osoba. To znači da učenici nikada ne bi trebali dati svoje lozinke, čak ni svojim prijateljima! Ovo je ključna tačka koju učenici moraju zapamtiti. Možda žele da dijele račun za nešto, ali na taj način bi mogli ugroziti druge račune koje posjeduju. Da bi zaista bio siguran, samo učenik može znati svoje lozinke za bilo šta - čak i za školske račune.

- **Kako Google Password Manager može poboljšati vašu sigurnost na internetu**

Ukradene lozinke su jedan od najčešćih načina kompromitovanja naloga. Kako biste zaštitili svoje račune, možete koristiti Google Password Manager za:

- Predlaganje jake, jedinstvene lozinke kako biste izbjegli višestruko kompromitovanje računa iz jedne ukradene lozinke
- Obavještenje o nesigurnim lozinkama. Ako neko objavi vaše sačuvane lozinke na internetu, Google Password Manager vam može pomoći da promijenite sve nesigurne lozinke.
- Pomoć u blokiranju neovlaštenog pristupa. Vaše lozinke se pohranjuju iza Googleove ugrađene sigurnosti korištenjem enkripcije. Kako biste vidjeli lozinke, potrebna je ponovna prijava

5.2 ODGOVORNO BIRATI KONTAKTE PREKO INTERNETA

Društveni mediji su svuda na internetu. Nove društvene mreže se pojavljuju iz mjeseca u mjesec, a neke od njih mogu proći ispod radara odraslih dok privlače pažnju djece. Na primjer, svi su čuli za Facebook, Twitter i TikTok. Ali jeste li čuli za Minds, Ello, Stage 32, Spring.me, Cucumbertown, Diaspora, Wooxie ili Yookos? Ako jeste, u manjini ste odraslih koji znaju koliko je opcija društvenog umrežavanja dostupno na internetu. Vjerovatno ste također svjesni koliko je lako nekome lagati o tome ko je na internetu. Ova praksa se zove "catfishing" i uključuje jednu osobu koja kreira složeni lažni identitet kako bi prevarila ili manipulisala nekim drugim. U najboljem slučaju, catfishing je sramotna šala koju prijatelji igraju jedni drugima. U najgorem slučaju, to je pokušaj krađe nečijeg identiteta, ucjene, nasilja putem interneta, uhoda ili čak fizičkog ozljeđivanja. Dakle, šta bi djeca trebala učiniti ako dobiju prijatelja ili slijede zahtjev nekoga koga ne poznaju na društvenim mrežama? A šta da rade ako misle da je jedan od njihovih onlajn prijatelja zapravo varalica? To je prilično lako i brzo učiniti - samo trebate znati kako!

Pretražite puno ime osobe na Googleu

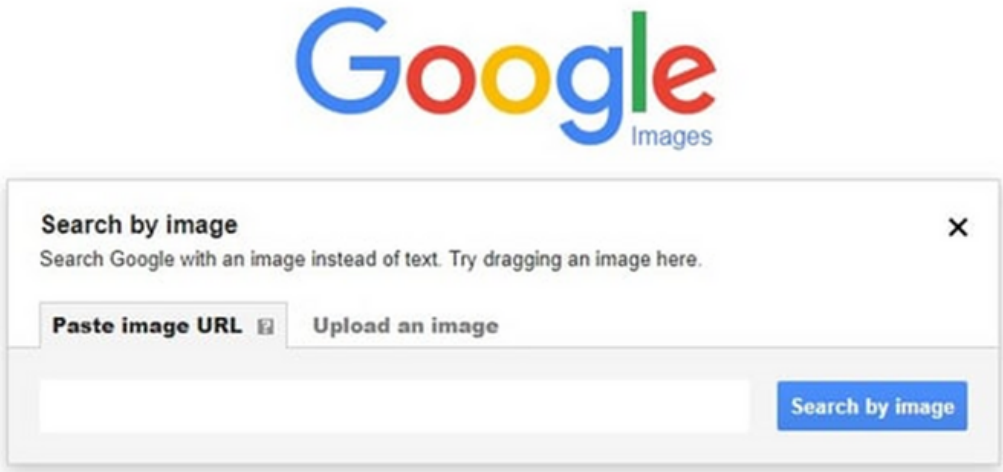
Ako se pojavljuju na više mjesta sa više profila na društvenim mrežama, to je dobar pokazatelj da je neko ono za koga se predstavljaju.Također možete kliknuti na pouzdane web stranice da vidite da li neko izgleda isto na fotografijama na jednoj društvenoj mreži kao na drugoj.

Obrnuto pretraživanje preko fotografije

Google ima funkciju pretraživanja obrnutih slika koja vam omogućava da upload-ate sliku za pretraživanje na internetu. Korištenje pretraživanja obrnutih slika može biti jedan od zabavnijih načina podučavanja sigurnosti na internetu u školi. Morate otići na images.google.com i kliknuti na ikonu kamere u traci za pretraživanje.

Slika 15: Ikonica kamere na google-u

Zatim ćete dobiti dvije opcije za pretraživanje slike - zalijepite URL ili upload-ajte sliku.



Slika 16: Kopiranje URL ili upload slike

Da biste pretraživali, morate sačuvati nečiju fotografiju na svom računaru i upload-ati je u Google-ovu obrnutu pretragu slika. Također možete kopirati URL slike desnim klikom na sliku i klikom na opciju "Kopiraj adresu slike". Ako se slika vrati s puno kopija sa mnogo različitih web stranica, to je loša vijest.

Blokiraj ih

Kada ste u nedoumici, dajte učenicima jedan veliki savjet o internet sigurnosti koji nikada neće zaboraviti - blokirajte stranca. Zapravo, oni to mogu učiniti odmah kako bi smanjili rizik da ih neko zapravo prevari. Kada je neko blokiran na društvenim mrežama, to često znači da više ne može vidjeti objave vaših učenika, prijatelje ili druga udruženja. To zaustavlja online prevaranta i sprečava vaše učenike da otkriju bilo koju drugu informaciju strancu.

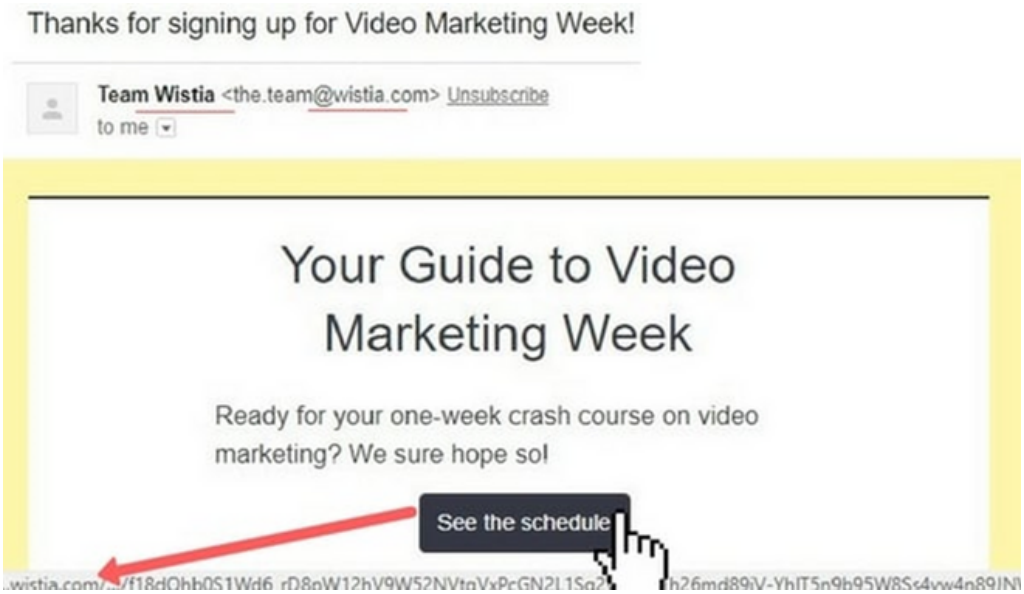
5.3 ODGOVORNO BIRATI SADRŽAJE KOJE SE NUDE PREKO INTERNETA

Slika 17: Sigurni linkovi

Ako učenik ima pristup računaru ili pametnom telefonu, velika je vjerovatnoća da ima nalog e-pošte.
Taj račun e-pošte trebao bi biti siguran – to je cilj svakog provajdera e-pošte – ali svaki učenik je i dalje ranjiv na neželjenu poštu i prevare. Ponekad ove neželjene poruke jednostavno traže novac. Postoji jednostavan način da odgovorite na njih - izbrišite e-poruke. Ali hakeri i zlonamjerni korisnici interneta svake godine postaju lukaviji. Njihovi pokušaji hakovanja zavarali su sve, od penzionera do vrhunskih IT profesionalaca i svakog između njih. Glavni način na koji hakeri to rade je falsifikovanje linkova, što se ponekad naziva i lažiranje. Ovo je čin stvaranja hiperveze koja kaže da će nekoga poslati na jednu web stranicu, ali zapravo ga šalje na drugu.Ta web stranica može biti programirana da automatski instalira zlonamjerni softver na nečiji računar ili telefon. Također može instalirati nešto što se zove "keylogger" koji prati vaše pritiske tipki i prijavljuje ih nepoznatoj osobi koja može naučiti vaša korisnička imena i lozinke. Može čak učiniti nešto tako nevino kao što je traženje sigurnosnog pitanja za određeni račun koji posjedujete. Bez obzira na oblik koji ima, sve su to opasne karike. Pa kako studenti mogu biti sigurni od njih?

Zadržite pokazivač iznad veze prije klika

Ovo je najjednostavniji način da provjerite je li veza legitimna ili ne. Zadržite pokazivač miša preko veze (ili slike, u nekim slučajevima) i pogledajte URL koji se pojavljuje. Važno je da kursor ostane nepomičan u ovom trenutku, inače će URL nestati.



Slika 18: Zadržavanje pokazivača na linku/slici

Ako prepoznajete URL, to je odličan znak! Ako ne, nemojte kliknuti!

Pažljivo pročitajte URL

Online prevaranti znaju koliko je lako učiniti da „r“ i „n“ izgledaju kao „m“. To možda ne zvuči mnogo – ali čini ogromnu razliku kada gledate URL-ove kao što su:

www.bankofamerica.com

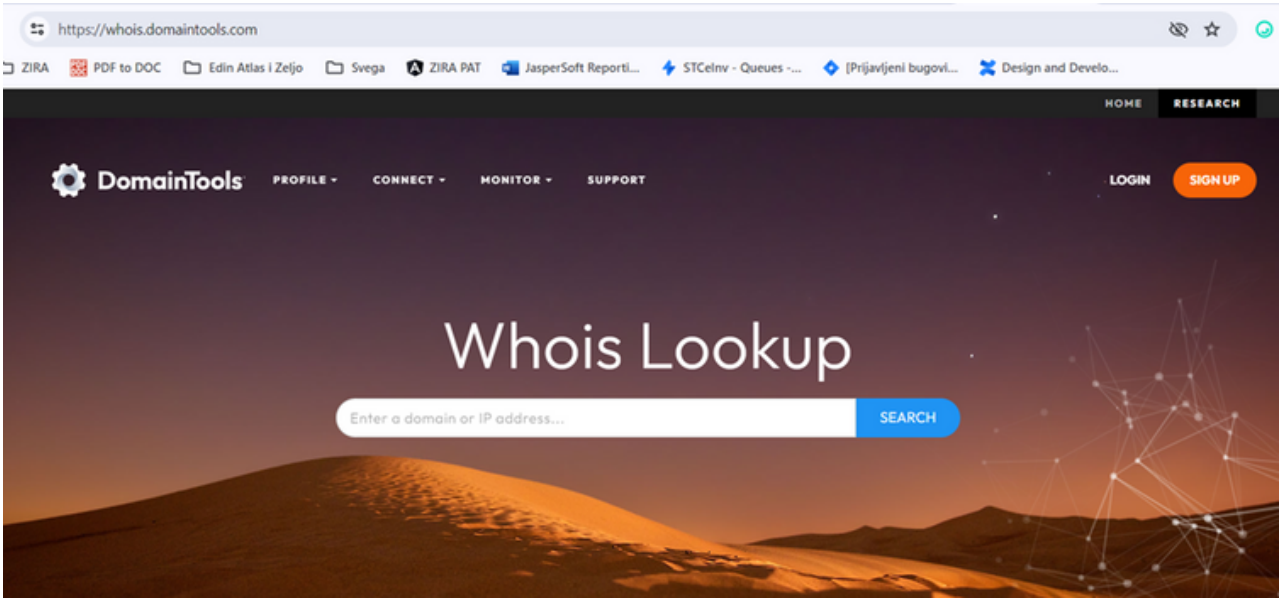
www.bankofarnerica.com

Slika 19: Sličnost linkova

Jedan od tih URL-ova ide dobro poznatoj i dugo uspostavljenoj banci u Sjedinjenim Državama. Drugi je lažna web stranica koja može učiniti bilo šta, od instaliranja ransomware-a na vaš računar do preuzimanja historije vašeg pretraživača. Srećom, postoji način da pomognete svojim učenicima da u potpunosti izbjegnu ovu opasnost. Možete ih naučiti kako prepoznati online prevaru.

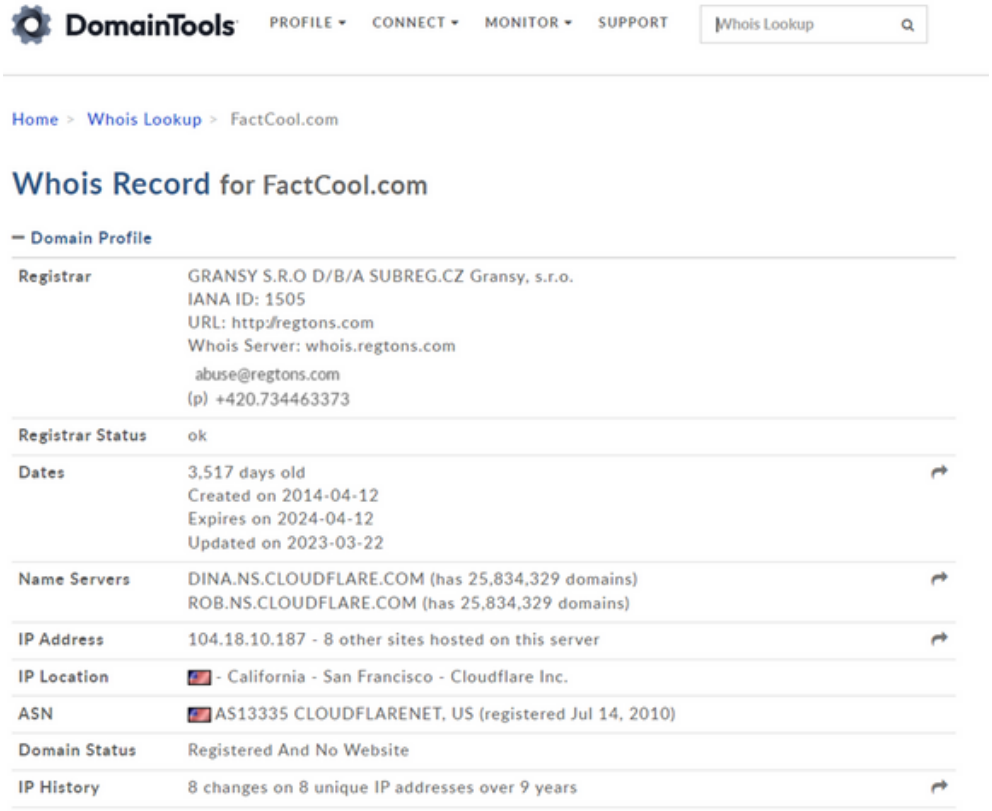
Postoji još jedan način kako detaljnije istražiti url koji koristite. Pretraživanje Whois domena omogućava vam da uđete u trag vlasništvu i trajanju naziva domene. Slično kao što su sve kuće registrovane kod organa uprave, svi registri imena domena vode evidenciju o svakom nazivu domena kupljenom preko njih, kao i o tome ko je vlasnik i datumu do kada je kupljen.
Korištenje je jednostavno:

- Ukucajte na googl https://whois.domaintools.com/



Slika 20: Whois domena

- U polje „Who is LookUp“ unesite url koji želite istražiti npr https://ba.factcool.com/
- Dobićete osnovne podatke o sajtu



Slika 21: Whois za sajt factcool

5.4 ODGOVORNO BIRATI KOJE PORUKE I SADRŽAJE OTVARATE NA SVOM RAČUNARU

Najbolji način na koji djeca mogu izbjeći prevaru je da idu sa onim što osjećaju. Ako web stranica za koju nikada nisu čuli traži njihove informacije, onda moraju biti sigurni i napustiti web stranicu. To vrijedi i za pojedince koji mogu kontaktirati učenike putem društvenih mreža ili e-pošte. Ako učenici ne prepoznaju nečije ime – ili ako nisu potvrdili nečiji identitet – onda se moraju kloniti. Nevjerovatno je šta mali dio ličnih podataka može učiniti u rukama pogrešne osobe. Evo šta možete naučiti svoje učenike da im daju pravi „osećaj“ kada naiđu na nezgodnu situaciju na internetu.

Novac je uključen

Svaki put kada se u neželjenoj poruci iz bilo kojeg izvora spominje novac, najbolje je zanemariti poruku.Po pravilu, institucije koje imaju pristup vašim ličnim podacima rijetko će o tome razgovarati putem e-pošte. Ovo važi i za zahtjeve za novcem i za zahtjeve da vam se da novac. Oba zahtijevaju da date lične podatke, poput brojeva bankovnih računa, koje prevaranti mogu koristiti da isprazne vaš račun bez traga. Često prevaranti vole da kombinuju zahtjeve za novcem sa nekim osećajem hitnosti tako da reagujete pre nego što imate priliku da razmislite o samoj poruci. Nemojte da vas zavara – ako vi ili vaši učenici ne prepoznajete nečije ime, kompaniju, adresu e-pošte ili bilo šta drugo, izbrišite e-poštu. Nemojte ga ni otvarati!

Strah i prijetnje

Strah je nevjerovatan motivirajući faktor u svakom kontekstu. Ovo nažalost važi i za prevare. Prevaranti će pokušati da koriste grubi jezik i prijetnje kaznama kako bi vas natjerali da kliknete na linkove, odgovorite s informacijama i još mnogo toga. Ako vam neko prijeti - čak i ako je napisano "službenim" jezikom - vjerovatno laže.

“Potrebne su nam vaše informacije da bismo nastavili”

Ako neko od vas traži lične podatke putem e-pošte ili društvenih mreža, to je prevara. Nijedna kompanija to ne radi. Ipak, to je jedna od najefikasnijih taktika prevare. Kako biste zaštitili svoje učenike, pobrinite se da prepoznaju da su njihovi lični podaci njihovi lični podaci.

E-mail od nepoznate osobe

Postoji nekoliko razloga zašto ste možda primili e-mail od nekoga koga ne poznajete. Obično je to samo greška. Ostali uobičajeni razlozi uključuju:

- Neko je pogrešno napisao adresu e-maila i slučajno ukucao vašu umjesto nje prilikom slanja poruke ili prijavljivanja na mailing listu.
- Neko šalje mejlove na uobičajena imena. To obično rade pošiljaoci neželjene pošte, pokušavajući pronaći nove adrese koje će dodati na svoje mailing liste. Iako je neugodno, to ne znači da je vaš račun manje siguran. Molimo prijavite ove poruke kao neželjenu poštu.
- Neko šalje e-mail negdje drugdje, ali krivotvori e-mail da izgleda kao da je došla od vas. Ako adresa na koju pokušavaju da pošalju zapravo ne postoji, dobit ćete e-mail o neuspjehu isporuke, iako toj osobi nikada niste poslali e-mail. Opet, ovo često rade pošiljaoci neželjene pošte kako bi sakrili izvorni izvor poruke.
- Neko koga poznajete ima virus koji šalje e-mail svima na njihovoj listi kontakata.

Većinu vremena dobijanje poruke od nekoga koga ne poznajete je samo greška ili neželjena pošta. Ako mislite da je poruka možda neželjena pošta, najbolje što možete učiniti je da kliknete Prijavi neželjenu poštu.

5.5 OPHODITI SE PREMA KONTAKTIMA NA ODGOVORAN NAČIN

Cyberbullying je proces napada, vrijeđanja, omalovažavanja, ponižavanja, ucjenjivanja ili na drugi način nanošenja štete nekome na internetu. Internet nasilje ima milione različitih oblika. Moglo bi biti jednostavno kao podli tvit, a može biti i složeno poput istraživanja nečijeg ličnog života i objavljivanja niza dokumenata na internetu za svako preuzimanje. Ipak, agresivno ponašanje nije uvijek okarakterisano kao internet nasilje. To može biti pasivno agresivno ili nešto sasvim drugo. Vi to znate jer možete vidjeti utjecaj na akademski i lični život učenika. Mogu da izgube prijatelje, da se naljute ili da se loše ponašaju na času. Možda imate strategije za rješavanje ovoga, ovisno o zahtjevima vaše škole. Ali najbolji način da se pomogne učenicima u cyberbullyingu je da ih naučite kako da ga prepoznaju, odupru se i zaustave ga.

Cyberbullying koristi tehnologiju, kao što su e-pošta, tekstovi, društvene mreže, online igre ili slike kako bi se povrijedilo ili naudilo nekom drugom neželjenim, agresivnim i ponavljanim ponašanjem što uključuje:

- Slanje loših tekstualnih poruka
- Objavljivanje neljubaznih izjava na internetu
- Dijeljenje slika koje nisu vaše za dijeljenje
- Lajkanje ili dijeljenje objava o nečemu štetnom
- Širenje glasina ili tračeva na internetu
- Slažem se sa nekim ko objavi nešto štetno

Maltretiranje nikada nije u redu, cool ili prihvatljivo.

Niko NIKAD ne zaslužuje da bude maltretiran.

Ko je zlostavljan?

Prvo, znajte da se maltretiranje ne bi trebalo NIKOME dogoditi.

Ne postoji "tip" osobe koja postaje meta maltretiranja. Maltretiranje može biti usmjereno na svakoga, od stidljivog, tihog učenika do tvrdog momka iz razreda. Djevojčice, dječaci, prvaci, učenici petog razreda, djeca koja vole umjetnost, djeca koja se bave sportom i svi između njih mogu biti meta maltretiranja. Maltretiranje se odnosi na to kako se ophodimo jedni prema drugima. Maltretiranje nikada nije opravdano i niko ne zaslužuje da bude njegova meta.

Ali samo zato što mnoga djeca doživljavaju maltretiranje ne znači da je to u redu ili „nešto što se jednostavno događa“. Jedina sigurna stvar je da niko NIKAD ne zaslužuje da bude maltretiran.

Najvažnija stvar koju treba zapamtiti je da maltretiranje NIKAD nije u redu, da niko NIKAD ne zaslužuje da bude zlostavljan.

Kako bi djeca shvatila da li su meta maltretiranja, dovoljno je da im se postave naredna pitanja:

- Zovu li vas druga djeca zlim imenima?
- Da li vas druga djeca ikada udaraju ili guraju?
- Da li vas djeca namjerno izostavljaju iz grupa?
- Da li vam je neko nekada slao zle poruke?
- Da li je neko nekada pokrenuo ružne glasine o vama?
- Da li je neko nekada uništio vaše stvari?
- Da li se druga djeca rugaju vašem izgledu ili ponašanju?
- Da li vam je teško sklapati prijateljstva?
- Da li se ponekad plašite da idete u školu?
- Da li vas je iko ikada natjerao da učinite nešto što niste htjeli?
- Da li se često osjećate nervozno, anksiozno ili zabrinuto zbog toga kako se druga djeca ponašaju prema vama?
- Da li su se druga deca ikada smijala kada vas je neko povredio?
- Da li ste nekada hteli da ne idete u školu jer ste se plašili drugog deteta?
- Jeste li ikada pokušali spriječiti nekoga da vas povrijedi, ali se maltretiranje nastavilo?
- Da li te je neko nekada ismijavao zbog nečega što ne radiš tako dobro kao druga deca?
- Da li te je neko nekada ismevao jer si zaista dobar u nečemu?
- Da li se druga djeca ikada rugaju ili oponašaju način na koji govorite, ponašate se ili izgledate?
- Da li vam druga djeca često govore da ne žele da se igraju s vama?

Što je više polja označeno, veća je vjerovatnoća da su djeca predmet maltretiranja ili će postati. U nastavku slijede kratki savjeti koji se mogu pružiti djeci:

- Potrebno je da djeca znaju da nisu sami i da postoje ljudi kojima je stalo i koji će im pomoći.
- Neophodno je uključiti roditelje, učitelja, nastavnika ili druge odrasle osobe kojima dijete vjeruje. Ne treba šutiti ili misliti da djeca mogu sama da rješavaju probleme. Pričanje je važno...
- Potrebno je staviti maltretiranje na njegovo mjesto! Sva djeca imaju jednaka prava; pravo da se nekome kaže, pravo da se osjećaju sigurno i pravo da se prekine nasilje.

Ukoliko djete prepozna da je meta zlostavljanja – šta može učiniti?

- Treba znati da ne zaslužujete ovo što se dešava.
- Treba recći nekome: roditeljima, učitelju, nastavniku ili odrasloj osobi od povjerenja.
- Treba pripremiti plan, uz pomoć odrasle osobe, o tome kako možete odgovoriti na situaciju.
- Treba odlučiti – uz pomoć odrasle osobe – kako bi drugi učenici mogli pomoći.
- Treba upoznati svoja prava: većina država ima zakone protiv maltretiranja.

Ako je dijete maltretirano, prva stvar koju treba znati jeste:

„Nije tvoja krivica. Ne. Ni malo. Niko ne zaslužuje da bude maltretiran...NIKAD! NIKAD nije vaš posao da popravite ono što se dešava, postoji mnogo toga što VI možete učiniti da preduzmete akciju!!“

Prepoznavanje internet nasilja

Internet nasilje se najbolje definiše tako što mora postojati negativan uticaj na učenika.Ako vršnjaci tog učenika vide da se internet nasilje dešava - čak i ako izgleda "nevino" kao zadirkivanje - važno je da znaju šta zaista vide. To nije samo šala koju neko igra. I nije "lažna" samo zato što se dešava preko interneta. To je zapravo štetno.

Neučestvovanje u internet nasilju

Internet nasilje je mnogo lakše prepoznati na daljinu nego izbliza. Učenik može biti dio grupe koja želi da igra "šalu" sa drugim učenikom na internetu. Na ovaj ili onaj način, to se brzo može pretvoriti u internet nasilje. Počinioci mogu čak misliti da je to bezopasno jer svoje postupke vide samo iz svoje perspektive. Ali iz perspektive žrtve, to bi mogao biti razarajući događaj koji će promijeniti život. Dakle, učenici mogu znati kako izgleda nasilje putem interneta, ali možda ne znaju kakav je osjećaj. U stvari, neka dobra djeca mogu na kraju nekoga povrijediti samo zato što ne shvate implikacije svojih postupaka! Učenici moraju znati empatiju da bi zaista razumjeli kako to funkcionira. Ovo nije lako – pogotovo zato što internet komunikacija ima tendenciju da dehumanizira ljude jer ne možete čuti nečiji glas ili ga pogledati u oči. Ipak, bitno je postojanje internet nasilja kako učenici ne bi postali internet nasilnici.

Zaustavljanje internet nasilju

Zaustavljanje internet nasilja je jednostavno na papiru. Zaustavljanje internet nasilja u praksi zahtijeva hrabrost. To je zato što to zahtijeva od učenika da se zauzmu za nekoga ili nešto što se ne smatra popularnim. A u školi popularnost je sve. Podučavanje učenika kako da zauzmu stav ili razumiju zašto bi trebali braniti nekoga ko je viktimiziran može uvelike pomoći u pretvaranju njih u zagovornike nenasilja. Kao što nam vijesti stalno pokazuju, može čak i spasiti nečiji život.

6 ZAKLJUČAK

Internet je nezamjenjiv medij za razmjenu informacija i komunikaciju, a sve njegove zamke možemo izbjeći svojim odgovornim ponašanjem.

Digitalna pismenost se fokusira na to kako učenici razumiju i tumače informacije na internetu. To znači razumijevanje zašto ljudi objavljuju informacije na internetu, kako prepoznati dezinformacije i još mnogo toga. To je vrijedna vještina 21. stoljeća koju učenici trebaju znati u današnjoj eri usmjerenoj na tehnologiju. Na kraju krajeva, napredak tehnologije ne usporava. Sa takvom tehnologijom koja ostaje ovdje, učenici moraju razumjeti šta vide na internetu.

Ključ da budete dobar digitalni građanin je empatija. Ovo se svodi na jedno veliko pitanje koje bi svaki učenik trebao postaviti sebi prije nego što bilo šta objavi na internetu:

"Šta bih mislio o nekome ko je ovo objavio?"

Samo ovo pitanje može promijeniti nečije postupke i, samim tim, nečiji život.

7 LITERATURA

- https://www.carnet.hr/wp-content/uploads/2019/09/Sigurnost-na-Internetu-1.pdf
- https://hr.wikipedia.org/wiki/Internet
- https://tesla.carnet.hr/mod/book/tool/print/index.php?id=6701
- https://zimo.dnevnik.hr/clanak/kako-prepoznati-lazne-vijesti-u-medijima-i-zastititi-svoj-uredjaj---604428.html
- https://www.icevonline.com/blog/how-to-teach-internet-safety-to-middle-school-students
- https://educationhub.blog.gov.uk/2023/02/01/how-we-promote-and-teach-online-safety-in-schools/
- https://www.pcmag.com/picks/the-best-antivirus-protection
- https://blogs.microsoft.com/on-the-issues/2023/02/06/safer-internet-day-global-online-safety-survey-2023/
- https://zipdo.co/statistics/online-safety/
- https://www.pacerkidsagainstbullying.org/

Priručnik je izrađen u saradnji sa Pedagoškim zavodom Zeničko-dobojskog kantona, a u okviru projekta "Boljom upravom do bržeg ekonomskog rasta" (EGG2) kojeg podržava i finansira Vlada Kraljevine Norveške, a provodi Razvojni program Ujedinjenih nacija (UNDP) u BiH. Sadržaj priručnika ne odražava nužno stavove Vlade Kraljevine Norveške, niti UNDP-a.