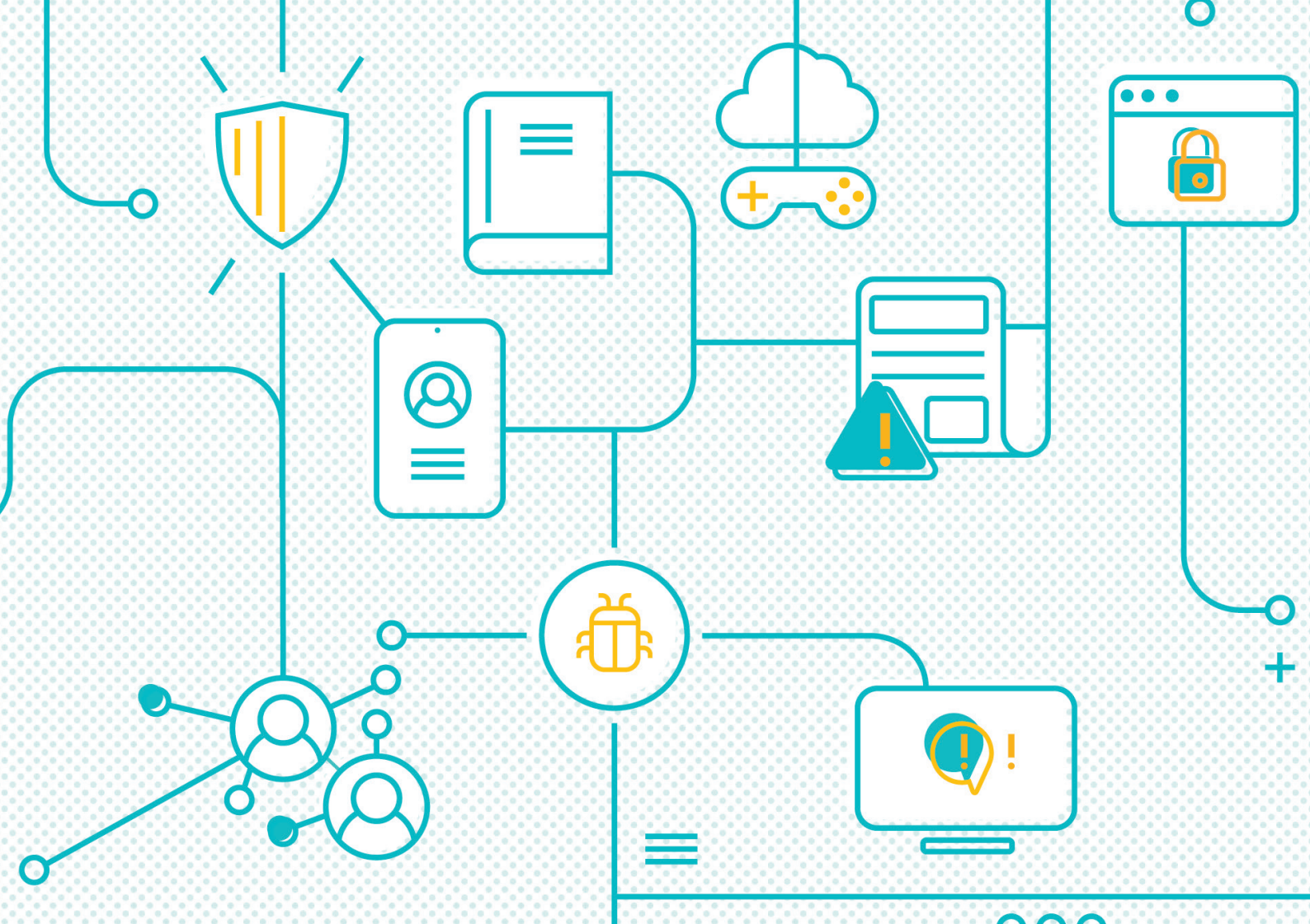


PRIROČNIK O DIGITALNI VARNOSTI

ZA UČITELJE

saferkidsonline by ESET

PRIROČNIK O DIGITALNI VARNOSTI ZA UČITELJE

saferkidsonline by eset

Izvirni naslov dela
DIGITAL SECURITY HANDBOOK FOR TEACHERS

Prevedla: Anja Jug
Prelom in oblikovanje: Žiga Vuk, zzigc.net
Izdal in založil: SI SPLET d.o.o.
Ljubljana, 2021

Tisk: Demago d.o.o., Maribor
Prva izdaja, prvi natis
Tisk na zahtevo.

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

004.738.5.056(035)
077.5(035)

PRIROČNIK o digitalni varnosti : za učitelje / [prevedla Anja Jug]. - 1. izd., 1. natis. - Ljubljana : SI splet, 2021

Prevod dela: Digital security handbook

ISBN 978-961-95405-0-3
COBISS.SI-ID 65827843

Vsebina

Zahvala

Zahvaljujemo se vsem zaposlenim podjetja **ESET**, ki so s svojimi strokovnimi nasveti, predlogi in organizacijskimi sposobnostmi pomagali ustvariti ta priročnik.

Zahvaljujemo se tudi psihologinji **Jarmili Tomkovi**, ki je prispevala več ključnih poglavij, ki odražajo njeno strokovno in praktično znanje.

In nenazadnje se zahvaljujemo **vsem učiteljem**, ki kljub neugodnim razmeram novo generacijo vzgajajo in pripravljajo na življenje v digitalni dobi. Posebna zahvala gre **Petru Kučeri**, ki si je uspel vzeti čas iz svojega natrpanega urnika in nam poslal zelo koristne povratne informacije.

Predstavitev

Internet in digitalizacija sta spremenila svet. Pametni telefoni, aplikacije in socialna omrežja so prinesli globoke spremembe v način odraščanja otrok in mladih. Te tehnologije odpirajo nova, prej nepredvidena obzorja, hkrati pa predstavljajo tveganja in grožnje, ki jih prejšnje generacije niso poznale.

V tej situaciji se osnovnošolski učitelji znajdejo v prvi vrsti, vendar pogosto ostanejo brez koristnega gradiva ali informacij. Kljub temu ostaja njihova naloga posredovati znanje o digitalnem in resničnem svetu ter pripraviti učence na življenje v obeh.

ESET je tu, da pomaga.

Kot globalni vodja na področju digitalne varnosti z več kot 30-letnimi izkušnjami in več kot 110 milijoni zaščitenih uporabnikov po vsem svetu verjamemo, da lahko starši uživajo v digitalnem življenju, ne da bi se bali za varnost svojih otrok. Da pa bi to dosegli, je najpomembnejše ozaveščanje otrok o pomembnosti spletne varnosti.

S tem v naših mislih smo ustvarili platformo SaferKidsOnline[1], polno izobraževalnih in privlačnih vsebin za otroke, starše in učitelje. Pomemben del tega dolgoročnega in obsežnega prizadevanja je ta priročnik, ki temelji na znanju, izkušnjah in spoznanjih naših priznanih, nagrajenih strokovnjakov. Osnovnošolskim učiteljem nudi osnovno teoretično razumevanje spletne varnosti in varne uporabe interneta. Vsebuje tudi praktične vaje, s katerimi lahko na zanimiv in interaktiven način predstavijo teme, zajete v priročniku, s poudarkom na sodobnih didaktičnih metodah.

Ta priročnik digitalno varnost obravnava z dveh različnih stališč:

- Tehnično stališče, ki temelji na ESET-ovem 30-letnem strokovnem znanju pri razvoju varnostnih rešitev za digitalno opremo.
- Psihološko stališče s poudarkom na različnih digitalnih grožnjah, kot je spletno ustrahovanje, ki jih ni mogoče rešiti samo s tehnologijo, saj se pogosto prelivajo s spleta v realni svet.

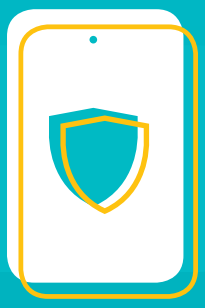
Ena od ovir pri izobraževanju je lahko tako imenovana generacijska vrzel. Današnji otroci in mladostniki so nenehno v neposrednem stiku z najnovejšimi tehnologijami, kar jim daje veliko podrobnejša znanja in spretnosti na tem področju. To pa ne pomeni, da jim učitelji ne morejo slediti in premostiti generacijske vrzeli:

- Naloga učitelja ni, da se ujema z otrokovim znanjem v vseh pogledih. Vendar se lahko smiselno dopolnjujejo in usklajujejo medsebojne učne izkušnje.
- Učitelji bi morali poleg posredovanja znanja izkoristiti tudi najnovejše izkušnje učnih metod, projektnega učenja, vzajemnega učenja in še več.
- Učitelji lahko predstavijo težke teme, sprožijo razprave in zanetijo zanimanje za vprašanja. Ni jim treba vedno predstavljati rešitev - lahko samo moderirajo razpravo, v kateri skupina učencev najde ustrezne rešitve, ali vsaj začne razmišljati o obstoju problemov.

Verjamemo, da bo ta priročnik koristen pripomoček za učitelje pri pripravi in oblikovanju pouka.

1 https://saferkidsonline.eset.com

Nekatera teoretska poglavja so podprta s predlaganimi praktičnimi dejavnostmi, ki jih najdete v Priročniku o digitalni varnosti (v nadaljnjem besedilu: “Dejavnosti”). Gre za vrsto dejavnosti, ki so jih oblikovali ESET-ovi strokovnjaki, učitelji računalništva in otroški psihologi, ki v zanimivi in praktični obliki predstavljajo teme digitalne varnosti in varne uporabe interneta s strani otrok. Če najdete to ikono v priročniku, poiščite dejavnost zanjo v ustrezni temi.



Varnost mobilnih naprav

aplikacija | oblak | mobilni antivirus | mobilna varnostna rešitev | mobilna naprava | tovarniška ponastavitev | operacijski sitem | PIN koda | sledilec | razvijalec | pametni telefon | tablica

Teme zajete v tem poglavju:

Katera so osnovna pravila varnosti mobilnih naprav?
Zakaj bi morali zakleniti zaslon in kateri način je najbolj varen?
Zakaj posodabljati aplikacije in operacijski sistem?
Zakaj prenašati aplikacije samo iz uradne trgovine z aplikacijami za Android / Apple?
Kako lahko varno prenašate aplikacije in na kaj morate biti pozorni?
Ali mobilni telefon / tablični računalnik potrebuje antivirusno zaščito?
Zakaj je priporočljivo varnostno kopirati podatke in kako jih varno shraniti?

Katera so osnovna pravila varnosti mobilnih naprav?

Ena izmed prvih stvari, ki jo lahko vsak uporabnik / učenec / študent stori za povečanje svoje varnosti, je izbira kakovostne mobilne naprave uglednega proizvajalca.

Številna naslednja priporočila veljajo za dva najpogosteje uporabljena operacijska sistema - Android in iOS. V sistemu Android lahko uporabniki izkoristijo tako vgrajeno varnostno kot tudi varnostno programsko opremo drugih proizvajalcev. Mobilne naprave imajo več plasti zaščite (zlasti tablični računalnik in pametni telefon):

1. **Dostop do naprave:** Napravo morate vedno zakleniti, če se izgubi ali ukrade, hkrati pa tudi zaščititi shranjene podatke pred nepooblaščenim dostopom tretjih oseb. Trenutno dostopni mehanizmi za zaklepanje vključujejo vzorec odklepanja[2], PIN kodo, prepoznavo obraza in prstnega odtisa. Prepoznava prstnega odtisa v kombinaciji s štirimestno do šestmestno kodo PIN trenutno velja za najbolj varno obliko zaščite. Če naprava nima optičnega bralnika prstnih odtisov, mora biti v razdelku "Nastavitve" na voljo vsaj ena od drugih možnosti.

2. **Fizična zaščita naprave:** Sodobne mobilne naprave shranjujejo veliko občutljivih podatkov, ki lahko v primeru izgube ali kraje naprave končajo v napačnih rokah. Uporabniki bi tako morali izkoristiti storitve, ki jim omogočajo oddaljeno iskanje, zaklepanje ali brisanje naprave. To vrsto storitve lahko aktivirate tako:

    a. Android naprave[3]
    b. Apple naprave[4]

3. **Varnostne kopije:** Nekateri zlonamerni napadi lahko vplivajo na delovanje mobilne naprave do te mere, da zahteva ponastavitev na tovarniške nastavitve. S tem bodo samodejno izbrisani **vsi uporabniški podatki**, vključno s stiki, slikami, videoposnetki in shranjenimi nastavitvami. To je eden od razlogov, zakaj bi morali uporabniki redno (npr. enkrat mesečno) kopirati vse svoje dragocene podatke iz mobilne naprave na drugo lokacijo in ustvarjati varnostne kopije.

    To lahko storite na več načinov:

    a. Eden izmed uporabnikom najbolj prijaznih načinov je uporaba varnostne kopije v oblaku, ki jo proizvajalci, kot sta Google in Apple ponujajo za skromno mesečno naročnino, ali uporaba druge aplikacije, ki je na voljo v Google Play ali App Store.

    b. Kot alternativo lahko uporabniki varnostno kopirajo podatke na trdi disk, ki ni povezan z internetom in tako ni dostopen nobenemu napadalcu, ki bi ponavadi zlorabil ranljivosti ali šibko varnost za dostop do povezanega pomnilnika. Primer tega je zunanji trdi disk, ki ga uporabnik takoj po izdelavi varnostne kopije odklopi od računalnika.

4. **Zaščita občutljive aplikacije:** Kombinacijo prstnih odtisov in kode PIN lahko uporabite tudi za zaščito dostopa do nekaterih aplikacij, kot so internetno bančništvo ali kripto denarnice[5]. To naj bo ločena koda PIN, ki se razlikuje od tiste, ki se uporablja za dostop do naprave.

2 Uporabnik mora povezati nekaj od devetih pik, ki jih prikaže naprava, v pravilnem vrstnem redu.
3 https://support.google.com/accounts/answer/6160491
4 https://support.apple.com/en-us/HT201472
5 Aplikacija, ki lahko shranjuje kriptovalute, kot so bitcoin, Monero, Ethereum in druge.

5. **Bodite previdni pri nalaganju iz neuradnih trgovin z aplikacijami:** Za največjo varnost naprave priporočamo uporabo samo aplikacij iz uradne trgovine z aplikacijami za določeno platformo (Google Play za Android in App Store za iOS). Uporabniki naj se izogibajo neuradnim trgovinam z aplikacijami in forumom, ki so najpogostejši kanali za širjenje zlonamerne programske opreme.

6. **Uporabniške ocene aplikacije:** Pred namestitvijo aplikacije iz uradne trgovine z aplikacijami vedno preberite mnenja, ki so jih objavili drugi uporabniki. Če aplikacijo označujejo za ponarejeno, zlonamerno programsko opremo ali virus (str. 73), namestitev preložite in jo preprosto poiščite v spletu, da preverite, ali aplikacija ni označena kot nevarna. Posebno pozornost je treba nameniti vsem negativnim kritikam. Pozitivne odzive napadalci pogosto ustvarijo sami, da si izboljšajo možnosti za uspeh. Lažne aplikacije pogosto obljubljajo tudi tisto, česar ne morejo dostaviti, na primer hitro in brezplačno povečanje števila prijateljev / sledilcev na družbenem omrežju ali denar v zameno za namestitev aplikacije v napravo.

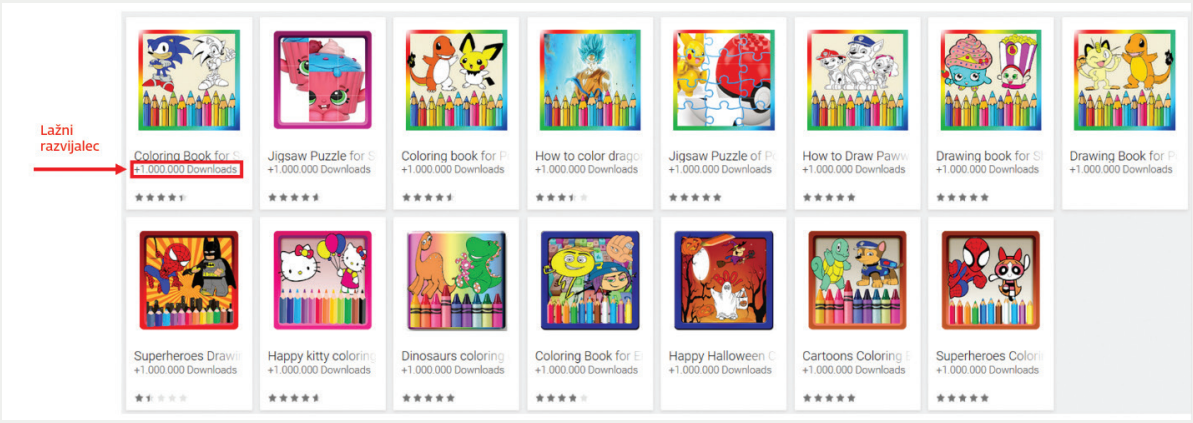
7. **Dovoljenja za aplikacije:** Pred začetkom namestitve vsaka aplikacija obvesti uporabnika, do katerih podatkov in funkcij potrebuje dostop, da lahko popolnoma deluje. Sumljive aplikacije pogosto zahtevajo dostop do funkcij, ki niso popolnoma povezane z njihovim namenom. Če na primer aplikacija za pregledovanje slik zahteva dostop do mikrofona, lahko to nakazuje poskus zalezovanja uporabnika.

8. **Posodobitve operacijskega sistema in aplikacij:** Razvijalci v aplikacijah nenehno odkrivajo nove slabosti in ranljivosti ter redno izdajajo posodobitve, da jih odpravijo. Uporabniki naj tako redno posodabljajo operacijski sistem in aplikacije, nameščene v njihovi napravi. Uporabniki lahko nastavijo samodejne posodobitve naprav ali pa nastavijo napravo, da avtomatsko ponudi posodobitve, ki jih nato uporabnik ročno namesti (vse možnosti so na voljo v razdelku "Nastavitve"). Za več informacij o temi glejte poglavje Posodobitve (str. 91).

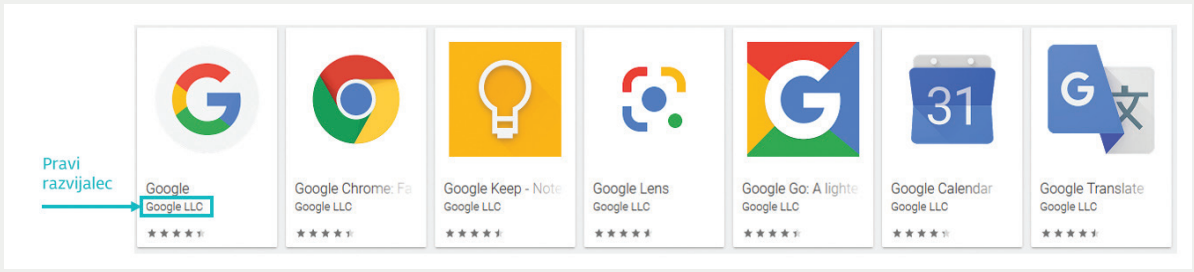
9. **Mobilna varnostna rešitev (antivirus):** Za nadaljnjo izboljšanje varnosti naprav Android priporočamo uporabo varnostne aplikacije, ki jo običajno imenujemo mobilni antivirusni program. Zanesljiva varnostna aplikacija lahko uporabnika obvesti o škodljivi naravi ali vedenju aplikacij in ga zaščiti pred zlonamernimi povezavami ali krajo podatkov. To velja tudi, če se škodljiva narava aplikacije razkrije šele po namestitvi v napravo. Nekatere varnostne aplikacije uporabnika obvestijo tudi o šibkih ali nepravilnih varnostnih nastavitvah ali mu lahko pomagajo pri iskanju izgubljene ali ukradene naprave. Za več informacij o temi glejte poglavje Varnostna rešitev (antivirus) (str. 79).

NAMIG: Na kaj še naj bodo pozorni uporabniki mobilnih naprav?

Celo v uradne trgovine z aplikacijami lahko vdrejo zlonamerni igralci ali zlonamerna programska oprema, ki jo je težko opaziti. Eden od znakov, ki lahko odda lažno različico priljubljene aplikacije, je ime razvijalca. To se lahko od pravega imena razvijalca razlikuje le z enim samim znakom (npr. Velik „I" (kot v imenu Ivan) lahko nadomestimo z majhnim „l" (kot v besedni črki)). Drug pristop, ki ga uporabljajo napadalci, je imenovanje njihovega računa razvijalca na način, ki poveča njihovo zaupanje. Primer tega so imena, ki so videti kot število prenosov uporabnikov (glej sliko 1 in sliko 2).



SLIKA 1: *"+1,000,000 prenosov" je lažno ime razvijalca. Ustvari vtis, da je to aplikacijo preneslo na milijone uporabnikov, v resnici pa jo je preneslo le nekaj sto uporabnikov. Vir: Trgovina Google Play*



SLIKA 2: *Običajno je tukaj prikazano ime razvijalca (kot pri teh Googlovih aplikacijah) in ne število prenosov. Vir: Trgovina Google Play*

Pravila za otroke, ki uporabljajo mobilno napravo

Učitelji naj učencem / študentom svetujejo o tveganjih, povezanih z uporabo mobilnega telefona ali zlorabo klicne linije v sili:

- Otroci naj nikoli ne uporabljajo klicev za nujne primere, če to res ni nujno. V nasprotnem primeru ovirajo tiste, ki resnično potrebujejo pomoč in tvegajo globo ali strožjo kazen.
- Ko otroka pokliče neznana oseba, naj nikoli ne deli osebnih ali drugače občutljivih podatkov. Banka, tehnična podpora in drugi strokovnjaki nikoli ne pokličejo svojih strank in ne zahtevajo takšnih informacij.
- Oseba, ki kliče otroka, se mora najprej predstaviti.

- Otroci v svojem sporočilu v odzivniku naj ne navajajo svojih ali kontaktnih podatkov drugih.
- Otroci bi morali vedno razmisliti, komu dajo svojo telefonsko številko.
- Če otrok prejme neželena sporočila prek Bluetootha, naj onemogoči Bluetooth in izbere, da naprava v "Nastavitvah" ni vidna.
- Če otrok ne pozna pošiljatelja sporočila SMS, v takem sporočilu ne bi smel klikniti nobene povezave ali nanj odgovoriti.

Selfiji

sebek | selfi | palica za selfije | viralna slika

Teme zajete v tem poglavju:

Kaj je sebek (ang. selfie) in kakšna tveganja predstavlja? Katerih pravil se morate držati, ko snemate sebek?

Kaj je sebek in kakšna tveganja predstavlja?

Sebek je avtoportretna fotografija, ki je običajno posneta s pametnim telefonom, ki ga lahko držite v roki ali podprete s palico za selfi. Kljub sodobnemu imenu selfiji obstajajo že kar nekaj časa. Stotine let pred izumom prvega mobilnega telefona ali družbenega omrežja so številni ugledni umetniki, kot so Leonardo da Vinci, Rembrandt in Vincent van Gogh, naredili "selfije" ali avtoportrete.

V nasprotju z velikimi slikarji v preteklosti številni današnji uporabniki (ne glede na njihovo starost) pri fotografiranju sebkov niso preveč pozorni na to, kaj je vidno na posnetku, in preden sliko preverijo, jo že objavijo na svojih profilih na družbenih omrežjih. S tem se izpostavijo različnim tveganjem. Slika lahko vsebuje predvsem stvari, ki jih uporabnik ni nameraval objaviti, ali pa jih lahko prikaže v neprijetni pozi.

Oglejmo si recept za dober (in še posebej varen) selfi Da Vincija, Rembrandta in van Gogha. Ko so slikali svoje avtoportrete in ustvarjali druge umetnine, so dneve in dneve vlagali v premišljevanje, kaj naj bo v ospredju in kaj v ozadju. Uporabnikom o tem ni treba razmišljati več dni, ampak bi morali premisliti, preden posnamejo samoportrete, in vedno natančno pregledati končno sliko, tako kot bi to naredil preiskovalni policist ali detektiv.

Neupoštevanje preprostega sklopa pravil lahko privede do številnih težav, kot so posmeh vrstnikov, spletno ustrahovanje ali objava in prodaja intimnih slik na spletnih forumih.

Katerih pravil se držati, ko snemate selfie?

1. Najprej bi se morali zavedati svoje okolice in njenega izgleda. Kot se je marsikdo naučil na težek način, je lahko selfie usoden. Statistika kaže[6], da vsako leto več ljudi umre zaradi fotografiranja sebkov kot zaradi napadov morskih psov.
2. Pri sebku se osredotočite tudi na podrobnosti, na primer: kaj je na mizi, na okenski polici ali na tleh v ozadju? Ali slika zajema mojo osebno izkaznico, zavarovalno izkaznico, potni list ali vstopnico za koncert s kodo QR? Ali slika razkrije mojo lokacijo nekomu, ki je ne bi smel vedeti?
3. Pred objavo se morate zavedati, da bo slika za vedno ostala na internetu in da je ne bo mogoče popolnoma odstraniti. Za ponazoritev tega lahko učitelji uporabijo dejstvo, da so številne fotografije navadnih ljudi nehote postale viralne[7] in jih njihovi avtorji / lastniki ne morejo več nadzorovati. Dobro pravilo je, da si najprej odgovorite na vprašanje: "Ali bi rad, da si to fotografijo / selfi ogledajo moja babica, starši, znanci ali moj bodoči delodajalec?"
4. Uporabniki vseh starosti bi morali svojo zasebnost zaščititi tudi s prilagajanjem nastavitev profila. Za več informacij o tej temi glejte poglavje o socialnih omrežjih (str. 25).
5. Ko je govora o sebkih, naj učitelji delujejo kot vzor in upoštevajo pravila, ki jih zagovarjajo.

NAMIG:

Če želite narediti selfi z drugo osebo (slavno osebo), jo najprej vprašajte za dovoljenje. Vsi smo upravičeni do zasebnosti, enako velja za znane YouTuberje, glasbenike, filmske zvezde in druge znane osebnosti, ki jih lahko srečate na ulici. Obstaja celo videoposnetek, posvečen tej temi, ki ga je posnela Kirsten Dunst[8].

6 https://www.bbc.com/news/newsbeat-45745982
7 https://www.google.com/search?q=meme+kid&tbm=isch
8 https://www.youtube.com/watch?v=rwDbOmPQNx0

Spletno ustrahovanje

pomanjkanje zadržkov na spletu (dezinhibicijski učinek) | spletno ustrahovanje | razkritje | spletno zalezovanje | veselo klofutanje | trol | trolanje | spletno sovraštvo

Teme zajete v tem poglavju:

Kako se pomanjkanje zadržkov kaže v spletnem okolju?
Kaj je spletno ustrahovanje in kateri so njegovi osnovni znaki?
Kaj delajo spletni ustrahovalci?
V čem se spletno ustrahovanje razlikuje od osebnega ustrahovanja?
Zakaj poznati spletno ustrahovanje in narediti kaj glede tega?
Je več ustrahovalcev moških ali žensk?
Kako lahko učitelji ugotovijo, da je otrok ustrahovan?
Kaj lahko učitelji storijo proti spletnemu ustrahovanju?
Kako naj se odzovejo učitelji, ko jim otrok pove, da je nadlegovan?
Katera okolja predstavljajo večje tveganje za (spletno) ustrahovanje?
Na kaj morate biti pozorni pri poučevanju o preprečevanju (spletnega) ustrahovanja?

Kako se pomanjkanje zadržkov kaže v spletnem okolju?

Elektronska komunikacija je specifična na več načinov:

- **Ljudje ne komunicirajo sproti v točno določenem času.** To velja tako za klepete kot tudi za komentarje o vsebini na družbenih omrežjih in odgovore na e-pošto. Izjema pri tem so video igre.
- **Elektronska komunikacija je pogosto anonimna** in ljudje se lahko počutijo nad zakonom.
- **Težko je čutiti empatijo**. Razen, če sta osebi v video klicu, otrok ne vidi obraza, telesa, gibanja ali reakcij sogovornika in ne razume v celoti posledic svojih dejanj in komunikacije.
- **Ko nihče ne vidi otroka (ali uporabnika), se sprostijo, počutijo se manj zadržane, bolj pogumne in manj omejene s socialnimi normami.** To je lahko koristno za sramežljive med nami, lahko pa povzroči preveč "sprostitve" z drugimi in povzroči izražanje agresije. Brez običajnih zadržkov in slabe vesti ljudje pogosto pustijo svoja čustva, želje in vedenje na prosto.

To "pomanjkanje spletne omejitve" imenujemo tudi **dezinhibicijski učinek**. Ljudje na internetu pogosto kažejo premalo zadržanosti in previdnosti zaradi zaznane anonimnosti. Zaradi tega popuščanja ljudje v spletni komunikaciji pogosto delujejo bolj pogumno ali celo agresivno. Pogosto se soočijo z ljudmi, ki jih nikoli ne bi upali izzivati iz oči v oči. To lahko povzroči izražanje agresije in neprimerno komunikacijo:

- To se lahko kaže v obliki posameznih incidentov, na primer spletno žaljenje in sovraštvo,
- ali sistematično ustrahovanje ali spletno zalezovanje.

Kaj je spletno ustrahovanje in kateri so njegovi osnovni znaki?

Dandanes lahko ustrahovanje poteka tako na spletu kot tudi zunaj njega. Ko se uporabljajo elektronska sredstva, temu rečemo **spletno ustrahovanje, elektronsko ustrahovanje, ustrahovanje prek mobilnih naprav in interneta ali elektronska agresija.**

Raziskave pa kažejo, da so pri spletnem ustrahovanju žrtve pogosto ustrahovane tudi v resničnem svetu, njihovi odnosi z vrstniki so moteni in manj zadovoljivi. Spletno ustrahovanje tako ni popolnoma ločeno od realnosti brez povezave. Digitalna orodja samo dajo napadalcem še eno možnost, da škodujejo žrtvi.[1]

Ustrahovanje, bodisi v spletnem prostoru bodisi iz oči v oči, ima naslednje osnovne značilnosti:

- **Obstaja nesorazmerje moči med napadalcem in žrtvijo**. Dominantnost napadalca in nemoč žrtve sta lahko resnična ali očitna, in izhajata iz fizične moči, samozavesti, občutka manjvrednosti ali nadrejenosti skupine. Prevlada je lahko resnična ali subjektivna. Kar zadeva spletno ustrahovanje, se lahko superiornost kaže tudi v obliki tehničnih veščin in odzivov občinstva na škodljiva dejanja.
- **Vključuje namerno škodo**, povzročeno eni ali več osebam.
- Napadalec je lahko **en sam otrok ali skupina otrok**.
- **Ponavljajoče se slabo ravnanje**.

- Enkratno agresivno dejanje v neposrednem okolju se običajno ne šteje za ustrahovanje. Pri spletnem ustrahovanju je stvar bolj zapletena. Ustrahovalec lahko doda en posmehljiv prispevek, ki ga lahko drugi všečkajo, komentirajo in delijo z drugimi uporabniki. Objavljena je bila samo ena objava, vse ostale reakcije in interakcije pa lahko štejemo tudi za škodljive, kar se še pomnoži z velikostjo občinstva. **Je pod vplivom skupinske dinamike**. Ne gre samo za napadalca in žrtev, ampak tudi za občinstvo — **mimoidoči**, ki so vir povratnih informacij za napadalca (občudovanje, spodbujanje, zavrnitev, ignoriranje) in priča ponižanju žrtve na družbenih omrežjih. Pasivnost ali dejavnost prič določa, ali se žrtev izolira ali jo prijatelji podprejo. Stališča ali dejanja opazovalcev / njihovo pomanjkanje lahko ublažijo ali popolnoma ustavijo ustrahovanje ali, nasprotno, ga legitimirajo in prispevajo k njemu.
- Spletno ustrahovanje, tako kot katera koli druga oblika fizične ali psihološke zlorabe, pomeni **kršitev otrokovih pravic**.

Spletno ustrahovanje vključuje zlorabo interneta in digitalnih tehnologij, torej pametnih telefonov, mobilnih naprav, interneta, spletnih mest, aplikacij in spletnih dejavnosti, da bi namerno škodovali drugim.

Kibernetsko ustrahovanje ima lahko naslednje oblike:

- **neposredna sporočila, SMS in e-poštna sporočila,**
- **blogi**, objavljena mnenja in opažanja, ki škodujejo žrtvi,
- **fotografije, slike in video posnetki**, ki škodujejo žrtvi,
- **(spletne) ankete, kvizi ali pozivi**, ki napadajo žrtev,
- **všečki na družbenih omrežjih** predstavljajo odobravanje škodljive vsebine, tako se postavijo na stran napadalca,
- **žaljivi komentarji,**
- **vesela klofuta**, znana tudi kot "klofutanje za zabavo". To je nova oblika slabega ravnanja, ki združuje ustrahovanje iz oči v oči s spletnim ustrahovanjem. Ustrahovalec med snemanjem dogodka na mobilni telefon fizično napade žrtev. Posneti video se nato naloži na internet ali v sporočilih razširi med vrstnike. Za veselim klofutanjem pogosto stoji skupina, ne le posameznik. Člani skupine se "zabavajo" in spodbujajo medsebojno škodovanje žrtvi. Ta oblika agresije ima uničujoč učinek na psiho žrtve.

Spletno ustrahovanje se najpogosteje zgodi:

- na družbenih omrežjih,
- v klepetalnih skupinah,
- prek sporočil, poslanih na mobilno napravo žrtve,
- prek e-poštnih sporočil.

Kaj delajo spletni ustrahovalci?

Cilj spletnega ustrahovanja je, da ustrahovalec (večkrat) uveljavi svojo prevlado nad žrtvijo. Za to lahko uporabi različne oblike slabega ravnanja, ki:

- **Žrtev izzove s sporočili in objavami**, ki vsebujejo žaljivo, lažno, nesprejemljivo in / ali vulgarno besedilo. Narava in vsebina takšnih sporočil pritegne žrtvino pozornost. Žrtev tega ne odobrava, ustrahovalec pa jo s tem vključi v dialog in dokazuje svojo prevlado.
- **Žrtev ogroža in izsiljuje**, npr. z vdorom v njen profil na družbenem omrežju, spreminjanjem gesla in zlorabo profila. Lahko na primer spremenijo izvirna sporočila, v njihovem imenu komunicirajo s stiki žrtve ali objavijo neprimerne objave, ki škodujejo žrtvi in njenim prijateljem. Ustrahovalec lahko ugrabljeni profil uporabi tudi za manipulacijo in izsiljevanje žrtve.
- **Žrtev ponižuje in zasmehuje** pred drugimi, npr. na družbenih omrežjih in v klepetalnih skupinah.
- **Žrtev obrekuje**, npr. s širjenjem govoric in laži s ciljem škodovati ugledu in odnosom žrtve.
- **Pretvarja se, da je druga oseba / žrtev (ukrade njihovo identiteto)** in škoduje drugim ali žrtvi.
- **Objavlja žrtvine zasebne ali intimne podatke** brez njihovega soglasja. Razkrite informacije so lahko slike ali intimni videoposnetki, ki žrtev javno diskreditirajo.
- **Žrtev namerno izključuje iz spletne skupnosti** bodisi na družbenih omrežjih, v klepetalnicah ali na forumih za razprave. Takšna izključitev iz skupine ni postopna, temveč hitra in razločna, zato jo bo žrtev zagotovo opazila in se počutila osamljeno.
- **Žrtev nadleguje in zalezuje**, kar ogroža njen občutek varnosti. Ustrahovalec žrtvi povzroča nelagodje z neželeno pošto, pošiljanjem fotografij, pošiljanjem sporočil v klepetih, puščanjem všečkov in komentarjev ali zvonjenjem telefona. Tovrstna pozornost je lahko pozitivna, vendar je zaradi svoje intenzivnosti običajno vsiljiva. V nekaterih primerih lahko komunikacija postane negativna in škodljiva in lahko vključuje celo grožnje fizične škode, lažne obtožbe, poškodovanje podatkov ali krajo identitete, zalezovanje zunaj spleta, spremljanje računalnika žrtve itd. Intenzivnost nadlegovanja se običajno poveča in se ne ustavi, tudi če se napadalca pozove, naj se ustavi ali potem, ko ga žrtev blokira. Iz spletnega okolja se pogosto širi v realen svet.

V čem se spletno ustrahovanje razlikuje od osebnega ustrahovanja?

Občutek anonimnosti odpravlja ovire in povečuje stopnjo okrutnosti.
Ljudje se na internetu počutijo anonimne, zato se lahko pretvarjajo, da so nekdo drug, in se počutijo imune na kazen. To odpravlja ovire, zato so napadalci pogosto ljudje, ki v resničnem svetu ne bi mogli prevladati.

Spletno ustrahovanje lahko žrtev doseže kjer koli.
Medtem ko je ustrahovanje iz oči v oči bolj ali manj vezano na določene lokacije in je torej bolj predvidljivo, lahko spletno ustrahovanje žrtev doseže kjer koli, kadar koli in večkrat. Ta vseprisotnost ustrahovanja odvzame žrtvi vse varne prostore in občutek nevarnosti se širi po številnih področjih, ki se sicer štejejo za varna.

Več napadalcev lahko ustrahuje samo eno žrtev.
Medtem ko so pri ustrahovanju na štiri oči ustrahovalci tam, kjer fizično srečajo žrtev, se lahko na internetu aktivno pridruži vsakdo.

Število in narava članov občinstva (“priče ustrahovanja”) se spreminjata.
Pri ustrahovanju iz oči v oči je občinstvo običajno jasno: žrtev ve, kdo jih je pretepel ali osramotil, kdo je to videl in kako daleč lahko potujejo informacije o teh dogodkih, npr. sošolci in dijaki. V bistvu je nemogoče predvideti velikost občinstva spletnega ustrahovanja, saj vsebina postane del digitalnega sveta in se lahko vedno znova širi. Žrtev ne more biti prepričana, kdo je videl njihovo ponižanje, ki ima lahko duševno uničujoče posledice in je veliko bolj škodljivo.

Možnost, da ostanemo anonimni za monitorjem ali zaslonom, krepi “**pojav socialnega bahanja”**. Občinstvo čuti malo odgovornosti za ukrepanje proti krivicam. Priče imajo občutek, da niso osebno vpleteni v situacijo in le zelo malo jih bo branilo žrtev.

Pri spletnem ustrahovanju je veliko težje prepoznati ustrahovalca in ga kaznovati za njegova dejanja.

Ker je razkritje resnične identitete ustrahovalca zapleteno, spletno ustrahovanje pogosto ostane nerazrešeno, kar še dodatno pripomore, da se vpleteni ne zavedajo posledic ali svojega dela krivde. To velja tako za ustrahovalce kot za morebitne navzoče, ne glede na to, ali gre za vrstnike ali avtoriteto. Poleg tega se spletno ustrahovanje pogosto dogaja zunaj šolskih površin. Učitelji in šolski psihologi tako čutijo manjši pritisk za reševanje teh incidentov.

Zakaj moramo vedeti o spletnem ustrahovanju in kaj storiti glede tega?

Glede na več mednarodnih raziskav (HBSC, EUKO, TIMSS, GSHS in PISA) lahko trdimo, da je imel približno **vsak tretji otrok** nekakšne izkušnje s spletnim ustrahovanjem. In postaja še bolj razširjeno. Kadar ustrahovanje ostane nerešeno ali je le delno razrešeno, trajno negativno spremeni identiteto žrtev, ustrahovalcev in navzočih.

Ko doživite moč ali nemoč, ko vidite, da se nasilje in pasivnost v medosebnih odnosih legitimizirata, se vam te izkušnje vtisnejo v spomin, dokler jih ne prepiše pozitivnejša izkušnja. Takšne pozitivne izkušnje so lahko, ko prenehamo z grdim ravnanjem, ko so napadalci izpostavljeni, ko se odnosi med vrstniki popravijo, ko se ljudje popravijo, ko vidijo prijateljstva in pogum, da se zavzamejo za šibke itd. To je nekaj, kar naj odrasli delajo skupaj z otroki.

Spletno ustrahovanje je, tako kot vsaka fizična ali psihološka zloraba, kršitev otrokovih pravic in zato nesprejemljivo.

Ali je več ustrahovalcev moških ali žensk?

Raziskave kažejo[9] da je med napadalci več fantov kot deklet in te razlike med spoloma lahko zaznamo v vseh starostnih skupinah otrok in mladostnikov. To velja za ustrahovanje na spletu in zunaj njega. Ko gre za število napadalcev, postanejo te razlike na podlagi spola manj izrazite pri 11 do 13 letih, ko dekleta v puberteti težje nadzorujejo lastne impulze in tudi same lahko znatno škodijo svojim vrstnikom; to je tudi čas, ko začnejo uporabljati socialna omrežja, ki ponujajo več možnosti za spletno ustrahovanje.

Kljub temu pa na splošno fantje vedenje ustrahovanja kažejo pogosteje kot dekleta. Tako kot med napadalci je tudi med žrtvami več fantov kot deklet.

Večina deklet postane žrtev spletnega ustrahovanja med 12. in 17. letom, ko je najbolj dejavna na družbenih omrežjih. Verjetno zato, ker socialni standardi nasilje nad ženskami in dekleti bolj natančno presojajo, so mlade ženske žrtve in napadi na druge v spletu (kjer izgubijo ovire in dojemanje socialnih standardov je šibkejše) pogosteje kot v realnem svetu.

Kako lahko ugotovite, da je otrok ustrahovan?

Učitelji bi morali otrokom razložiti, kako naj opazijo, kdaj je nekdo ustrahovan. Tako se lahko otroci naučijo videti zgodnje znake in preprečijo obsežne psihološke poškodbe žrtve.

Otroku spletno ustrahovanje predstavlja pomemben dejavnik stresa, ki povzroča tesnobo, depresijo, strah in občutek nemoči. Ti pogoji imajo pogosto zunanje simptome, ki jih morajo opaziti starši, učitelji in vrstniki.

Njihove skrbi se lahko kažejo na naslednje načine:

- **psihosomatski simptomi** — bolečine v trebuhu, glavobol, motnje prehranjevanja in spanja,
- **negotovost, zmanjšana samozavest in samospoštovanje**, občutek ogroženosti zaradi socialnih stikov, nevrotičnega vedenja in izogibanja družbi,
- **spremembe v vedenjskih vzorcih** — manj stikov z vrstniki, manj hobijev in dejavnosti, povečana apatija, osamljenost, izguba zanimanja za šolske dejavnosti, slabše ocene in vedenje,
- **novi škodljivi vzorci v otrokovem vedenju** — tveganje, uporaba snovi, ki povzročajo zasvojenost, samopoškodovanje, prestopništvo, odsotnost,
- **stresne reakcije pri uporabi ali govoru o računalniku in pametnemu telefonu**. Prikaz stresa pri uporabi digitalnih orodij pa ni nujno vedno posledica spletnega ustrahovanja. Vzrok so lahko druge težave, ki jih preživi mlada oseba, ali spremembe, povezane s puberteto. Ne pozabite, da gre pri spletnem ustrahovanju predvsem za odnose.

Vsak otrok se na skrbi in stres odzove drugače. Pomembno je, da sošolci in odrasli v šoli **ostanejo pozorni**, da opazijo, da je nekaj narobe. V šoli so otroci in učitelji nenehno v stikih, kar povečuje možnosti, da bodo opazili spremembe v vedenju.

9 http://eprints.lse.ac.uk/87794

Kaj lahko učitelji storijo glede spletnega ustrahovanja?

Starši in učitelji lahko poudarijo naslednja dejstva:

1. **Otroke naučite, kaj je (spletno) ustrahovanje**
   - Učitelj naj otroke nauči meje med zabavo in (spletnim) ustrahovanjem.
   - Učitelj naj otroke nauči, kako zmanjšati tveganje (spletnega) ustrahovanja.

2. **Otroke naučite, kako ravnati, če občutijo (spletno) ustrahovanje**
   - Učitelj naj priporoči določene ljudi, na katere se otroci lahko obrnejo, če naletijo na težave, na primer starši, starejši brat ali sestra ali vrstnik za čustveno podporo ali učitelj računalništva za tehnično podporo.
   - Učitelj naj otroke nauči, kako naj ravnajo, ko se jim na internetu dogaja nekaj slabega.

3. **Izboljšati socialne veščine otrok, podpirati njihovo samopodobo in empatijo**
   - Učitelj lahko otrokom pomaga tako, da jih nauči razlikovati lastne občutke, zato so bolj občutljivi na lastne izkušnje in izkušnje drugih.
   - Učitelj lahko otrokom pomaga izboljšati samopodobo in socialne veščine, da lahko gradijo in vzdržujejo zdrave odnose.
   - V učilnici lahko učitelj podpira vrednote, kot so prijateljstvo, sprejemanje in pripadnost.

4. **Spodbujajte otroke, da pomagajo šibkejšim**
   - Učitelj otroku pomaga razviti sposobnost, da aktivno brani sebe in druge, če jih kdo prizadene.

5. **Razviti otrokove veščine varne uporabe interneta**
   - Učitelj razloži, kako se bolje zaščititi z uporabo razpoložljivih tehničnih sredstev.

6. **Na internetu ustvarite varna mesta in območja za žrtve**
   - Učitelj pomaga ustvariti varna območja, kjer lahko ustrahovani otroci delujejo brez strahu pred več napadi.

7. **Zagotovite otrokovo zaupanje**
   - Učitelj naj pojasni, ključni pomen, da odrasli ali vsaj nekateri zrelejši vrstniki vedo za to težavo. Če nihče ne ve za težavo, nihče ne more ponuditi roke za pomoč.

Kako naj se odzovejo učitelji, ko jim otrok reče, da ga nadlegujejo?

Kako ravnati z žrtvijo:

Otrok potrebuje pomoč nekoga, ki nudi socialno podporo in je usposobljen za reševanje incidenta. Poleg čustvene podpore, poslušanja in pomoči otroku, da izrazi svoja čustva, lahko učitelj razloži tudi, kaj storiti naprej:

1. **Shranite sporočilo o ustrahovanju**, kot so sporočila SMS, sporočila v klepetu, ponižujoče fotografije, komentarji ali posnetki zaslona spletnih aplikacij. To je pomemben korak, kajti otrok bo, razumljivo, želel izbrisati vse omalovažujoče spletne vsebine in omembe, da prepreči njihovo širjenje. Vendar je ravno ta vsebina dokaz, ki je potreben za ukrepanje proti ustrahovalcu.
2. **Ne komunicirajte z** ustrahovalcem, blokirajte ga in odstranite iz stikov. Na tej točki se ustrahovanje lahko ustavi, vendar je treba otroku pomagati razrešiti obstoječe konflikte in ohraniti delujoče odnose s sovrstniki.

Kako ravnati v zvezi s šolo, starši, strokovnjaki in oblastmi:

1. Učitelj ne sme spregledati ali prikriti informacij o slabem ravnanju med učenci, ker predstavljajo kršitev otrokovih pravic. V podobnih primerih se mora učitelj vedno obrniti na ravnatelja in otrokove zakonite zastopnike.
2. Učitelj mora takoj ukrepati in poskusiti otroku pomagati v sodelovanju z ustreznimi člani šolskega sistema, kot so starši, sošolci, ravnatelj, drugi šolski strokovnjaki, šolski psiholog ali socialni pedagog in policija.

Kako nadaljevati v učilnici, v kateri se je zgodilo (spletno) ustrahovanje:

1. Učitelj takoj prosi za **pomoč v učilnici.**
2. Pomaga spremeniti **negativno izkušnjo v razumljivo lekcijo**, ki pojasnjuje, kaj se je zgodilo, kako določeno vedenje predstalja (spletno) ustrahovanje, zakaj to ni dovoljeno in kaj lahko učenci v učilnici storijo, da popravijo svoje odnose.
3. Učitelj pomaga otrokom z uporabo skupinskih dejavnosti **obnoviti občutek varnosti in zdravih odnosov.** Pri spletnem ustrahovanju storilci niso nujno sošolci žrtve, lahko pa sošolci pomagajo žrtvi, da se počuti bolj vključeno in podprto.
4. Uspešno vključevanje učencev[10], ki so sodelovali v slabem ravnanju pri urejanju odnosov z vrstniki, je lahko način za delitev **odgovornosti** in zmanjšanje kazni za kršitev pravil učilnice / šole.
5. Učitelj lahko učencem ali njihovim družinam priporoči tudi **individualno psihološko podporo.**
6. Koristno je, če ima šola jasna pravila, kako ravnati proti (spletnemu) ustrahovanje. Ta pravila bi morala vključevati **sankcije**, saj otrokom pomagajo, da se naučijo biti odgovorni za svoja dejanja.

10 https://dulwichcentre.com.au/explorations-2010-1-michael-williams.pdf

Troli in spletno sovraštvo

trolanje | trol | spletno sovraštvo

Teme zajete v tem poglavju:

Kdo je trol? Kako se lahko uporabniki izognejo trolom? Kaj je spletno sovraštvo? Kaj naj si učitelji prizadevajo v smislu preprečevanja trolanja in spletnega sovraštva?

V digitalnem okolju uporabniki pogosto čutijo napačen občutek varnosti, saj mislijo, da jih nihče ne bo mogel povezati s svojimi dejanji. V mnogih situacijah ta občutek vodi v nadlegovanje in celo dejanja agresije. Nekateri posamezniki pa zavestno objavljajo vnetljive pripombe in v ta namen celo ustvarjajo lažne račune. S takimi računi napadajo druge in spodbujajo sovraštvo, spore in kaos. Tako motečega uporabnika v spletni razpravi imenujemo **trol**.

Kdo je trol?

Trol je oznaka za motečega uporabnika, ki:

- spodbuja spore in argumente, izziva druge na internetu,
- namerno objavlja žaljive, neprijetne, lažne ali nepomembne objave,
- poskuša izzvati močan odziv drugih uporabnikov (vir[11]),
- zavestno moti ali preprečuje razpravo in objavlja digresivna sporočila (vir[12]).

Cilj trola je pridobiti pozornost in občutek moči. Najboljši način za uporabnika je, da trolu onemogoči to priložnost.

Raziskave kažejo, da so troli ponavadi narcistični in lahko kažejo tudi nekatere lastnosti osebnostne motnje (psihopatija, sadizem, makijavelizem, shizofrenija) in so bolj impulzivni. Vendar moramo biti previdni, da ne bomo preveč posploševali. Vsak človek z osebnostno motnjo ne sme biti tudi trol in obratno - ni treba, da ima vsak trol osebnostno motnjo. Kljub temu je verjetnost, da bi jo imeli, večja.

11 https://www.pcmag.com/encyclopedia/term/68609/internet-troll
12 https://kb.iu.edu/d/afhc

Kako se lahko uporabniki izognejo trolom?

Uporabniki se najpogosteje srečujejo s troli na družbenih omrežjih, v klepetalnih skupinah in v posameznih klepetih. Obstajajo načini, kako se jim izogniti:

- Uporabite pravilne nastavitve zasebnosti v družbenih omrežjih. Če je mogoče, ne uporabljajte javnih profilov na nobenem od družbenih omrežij.
- Na družbenih omrežjih kot stike dodajte samo osebe, ki jih osebno poznate ali imate več skupnih prijateljev.
- Prepoznajte lažne profile in se nanje ne odzivajte. Včasih se lažni uporabnik računa lahko pretvarja, da je vaš prijatelj, samo da bi vstopil v skupino. Previdni bodite tudi, ko neznan profil na družbenem omrežju:
  - nima fotografije, na kateri je uporabnikov obraz prepoznaven,
  - nima skupnih prijateljev ali stikov z uporabnikom, ki ga poskuša dodati kot prijatelja,
  - vsebuje agresivno, sumljivo ali zlonamerno predhodno dejavnost ali lastnosti nestrpnosti in sovražnega govora v svojih komentarjih ali vsebini, ki jo deli,
  - ima bistveno več prijateljev kot povprečen uporabnik. Za otroka / učenca je dobra referenčna številka število prijateljev priljubljenega vrstnika,
  - ne ustvarja lastne vsebine, deli le sporočila, videoposnetke ali fotografije drugih uporabnikov in dodaja nesmiselne komentarje.

Kako naj se spopadam s troli?

V stiku s trolom obstaja eno preprosto pravilo: ne reagiraj. S trolom ni razumne razprave. Z njimi ne morete logično sklepati, ker radi delajo škodo in uživajo v pozornosti, ki jo dobijo na spletu. Ko enkrat veste, da imate opravka s trolom, je najbolje, da se ne odzovete na njihove komentarje in ne končate razprave. Vsak odziv na njihovo vsebino je zanje "nagrada".

Če je vaš odgovor pozitiven, je trol vesel, da se nekdo strinja z njimi. Če je vaš odziv negativen, je trol vesel, da jim je uspelo koga razžalovati ali razjeziti. Če jih ignorirate, pokažete, da njihova objava na vas ne vpliva pozitivno ali negativno, in jih ničete nagraditi.

Če vaše "pomanjkanje odziva" trola ne odvrne in nadaljuje z zlonamerno dejavnostjo, shranite posnetke zaslona njihovih objav in jih prijavite skrbnikom. Odgovorni uporabnik bo to storil ne glede na to, ali trol moti njega ali koga drugega v spletnem okolju. V ta namen družbena omrežja običajno ponujajo funkcijo "Prijavi". S prijavo zlonamerne dejavnosti lahko prispevate k ustvarjanju varnejšega spletnega okolja za vse.

1. Ko prijavite trola, ga blokirajte in odstranite iz stikov, če ste ga že dodali.
2. Najboljši način je, da se z nekom, ki mu zaupate, pogovorite o vsem, kar vas moti tako na spletu kot tudi zunaj njega.
3. Če se nadlegovanje nadaljuje prek drugih "kanalov", ne pozabite shraniti posnetkov zaslona in sporočil ter takoj stopiti v stik z odraslim ali starejšim vrstnikom. Nato lahko posnetke zaslona in druge dokaze zagotovite policiji.

Kaj je spletno sovraštvo?

Spletno sovraštvo izvira iz stereotipov in predsodkov do določenih skupin ljudi, ki se pogosto lahko spremenijo v sovraštvo.

Sovražna dejanja[13] — komunikacija in vrste vedenja, pri katerih napadalec diskriminira, obrekuje ali si prizadeva izključiti nekoga na podlagi rase, narodnosti, jezika, polti, vere, spola, spolne usmerjenosti, politične pripadnosti, socialno-ekonomskega statusa, starosti ali duševnega in telesnega zdravja.

Njihovo vedenje pogosto kaže lastnosti šovinizma, rasizma, ksenofobije, antisemitizma, islamofobije in homofobije. Vse šole so dolžne preprečevati **sovražna dejanja** v učnem procesu in poučevati kulturo strpnosti in spoštovanja človekovih pravic tako v spletu kot tudi zunaj njega.

Dejanja sovraštva so kršitev človekovih pravic in osnovnih svoboščin, ki veljajo za vse ljudi od njihovega rojstva so zaščitena na svetovni ravni in so jasno opisana v Splošni deklaraciji o človekovih pravicah.

Spletno sovraštvo je v primerjavi s trolanjem bolj resno, ker krši človekove pravice in svoboščine, diskriminira ljudi ali neposredno širi ekstremistična stališča in je tako lahko opredeljen kot kaznivo dejanje ali kaznivo dejanje..

Kaj naj si učitelji prizadevajo v smislu preprečevanja trolanja in spletnega sovraštva?

Učitelji lahko sistematično vodijo otroke k aktivnemu digitalnemu državljanstvu, kar lahko na kratko označimo takole: "Če se ne strinjamo z nepravičnostjo, je to le prvi korak, pomembna so naša dejanja." Sporočilo otrokom je: "Kadar koli opazite spletno sovraštvo, ga morate prijaviti z gumbom "Prijavi". Na ta način lahko pasivni navzoči postanejo aktivni ustvarjalci boljšega spletnega okolja.

Pri izobraževanju otrok / učencev se morajo šole osredotočiti na:

- vzpostavljanje odnosov okoli spoštovanja, empatije in zdrave samozavesti,
- posredovanje znanja o človekovih pravicah in svoboščinah,
- rušenje stereotipov in predsodkov,
- konstruktivno reševanje konfliktov,
- kako biti proaktiven uporabnik interneta in kako se pravilno odzvati na spletno sovraštvo.

13 https://www.adl.org/education-and-resources/resource-knowledge-base

Socialna omrežja

klepet | odkrivljivost | šifriranje med koncema | posnetek zaslona | socialno omrežje | povezava | strah pred zamujeno priložnostjo | spletno ustrahovanje | mehurčki socialnih omrežij | vplivnež | youtuber | vloger | bloger | sovražni govor | problematična raba interneta | internetna odvisnost | prenos iz iger v realni svet | selfi dismorfija

Teme zajete v tem poglavju:

Kakšna so pravila varnosti socialnih omrežij?
Kakšna psihološka tveganja predstavljajo socialna omrežja in kako jih obravnavati?
Kdo so vplivneži in kako vplivajo na življenje otrok?
Realni in spletni svet – kdaj govorimo o problematični rabi interneta in socialnih omrežij?

Socialna omrežja in digitalna varnost

klepet | odkrivljivost | šifriranje med koncema | posnetek zaslona | socialno omrežje | povezava

Teme zajete v tem poglavju:

Kateri so osnovni elementi varnosti socialnih omrežij? Kako lahko izboljšate varnost socialnih omrežij? Katere funkcije vam lahko pomagajo izboljšati varnost računa na družbenih omrežjih? Katerih podatkov in dejstev ne bi smeli deliti na družbenih omrežjih? Kaj morate upoštevati pri izbiri socialnega omrežja? Na katere lastnosti bi se morali osredotočiti pri izbiri aplikacije za klepet? Na koga se lahko obrnete, če imate težave na družbenih omrežjih? Kako napadalci zlorabljajo socialna omrežja?

Kateri so osnovni elementi varnosti socialnih omrežij?

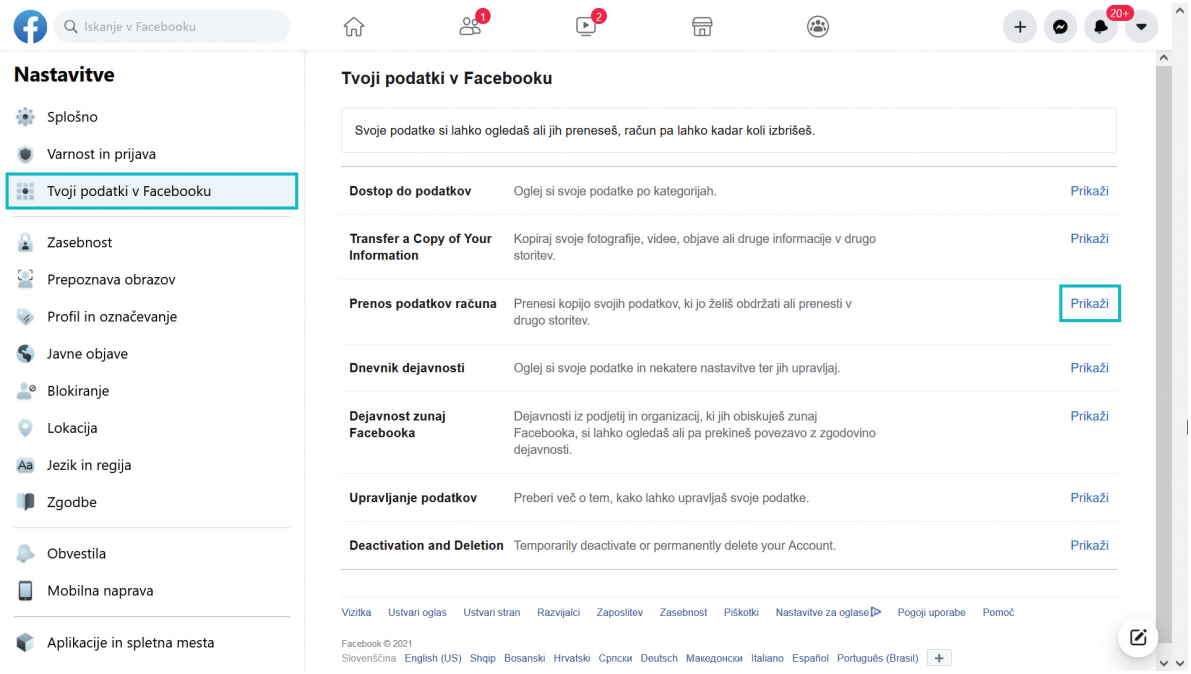
Tudi pri družabnih omrežjih, tako kot pri celotnem internetu, velja naslednje: kar gre na splet, ostane za vedno na spletu. Tudi če podatke odstranite iz profila na družabnem omrežju, se lahko pojavijo v drugačni obliki — kot posnetek zaslona, del videoposnetka ali vdelani v drugo obliko digitalne vsebine. Tudi če določenega podatka ne najdete na spletu, to še ne pomeni, da ga tam ni.

Kako lahko izboljšate varnost socialnih omrežij?

1. **Ko nastavite profil, ga nastavite kot zasebnega** in vsebino (statusi, objave, fotografije, videoposnetki) delite samo z omejeno skupino uporabnikov. Manjša kot je skupina, bolj varen je vaš profil. Možnost lahko nastavite tudi samo na "prikaži objave prijateljem". Če izberete možnost "prikaži objave prijateljem prijateljev", bo vsebina vidna tudi ljudem, ki jih neposredno ne poznate.

2. **Previdno izberite, katero vsebino želite deliti.** Vse fotografije ali objave niso primerne za internet. Vsako fotografijo, video in objavo natančno preglejte, tako kot bi to storil preiskovalni uradnik. Tako lahko preprečite razkritje občutljivih ali zasebnih podatkov. Dobro in preprosto pravilo je: *"Ne delite ničesar, česar ne bi pokazali svojim (starim) staršem."*

3. **Redno preverjajte vsebino v skupni rabi.** Na Facebooku vam možnost v nastavitvah (glej sliko 3) omogoča prenos vseh informacij, ki jih je o vas shranilo socialno omrežje. Podobno možnost ponujajo tudi druga družbena omrežja, kot sta Snapchat ali Instagram. Najboljši primer je, da v prenesenih podatkih najdete le minimalne osebne podatke. To pomeni, da neznanci ne bi smeli izvedeti vašega rojstnega datuma ali kraja bivanja, dela ali študija.



SLIKA 3: *Kako prenesti vse informacije, ki jih je Facebook zbral o uporabniku.*

4. **Redno preverjajte članstvo v skupini.** Skupine na družabnih omrežjih (Facebook strani in podobno) lahko spremenijo svojo vsebino ali fokus. S staranjem se spreminjajo tudi vaša mnenja in morda se znajdete v skupini, katere mnenja ne delite več. Nekatere skupine so celo namerno ustanovljene, da čim hitreje zberejo čim več članov in jih nato prodajo ponudniku, ki najbolje ponudi. Novi lastnik lahko nato spremeni ime skupine in se osredotoči na pošiljanje nezaželene vsebine svojim članom.

5. **Poglej, preden klikneš.** Če uporabnik socialnega omrežja prejme sporočilo ali povezavo od enega od svojih prijateljev, naj vedno najprej pomisli, ali bi ta oseba dejansko poslala takšno vsebino. Če je mogoče, naj najprej najprej preveri, na kaj kaže povezava (ne da bi jo kliknili, samo miškin kazalec premaknite nad povezavo in prikazan bo naslov, na katerega kaže). Če je poslana vsebina ali sama povezava videti sumljiva ali je katera koli od njih v jeziku, ki ga določeni prijatelj ne uporablja, se izogibajte kliku nanj in opozorite prijatelja, ki vam ga je poslal.

6. **Preverite in pravilno nastavite, kako vas lahko ljudje najdejo.** V nastavitvah družbenega omrežja lahko nastavite strožja pravila, kdo lahko najde vaš profil - v idealnem primeru bi to morala biti le vaša družina, prijatelji ali določena skupina ljudi.

7. **Prilagodite svoje vedenje na socialnih omrežjih.** Če želite biti prepričani, da ne boste razkrili preveč informacij o sebi, lahko izberete pristop, pri katerem boste svoj profil ali napravo obravnavali, kot da jo nekdo spremlja. Seveda na takšnih mestih ne bi smeli hraniti občutljivih podatkov.

Katere funkcije vam lahko pomagajo izboljšati varnost računa v družabnih omrežjih??

Poleg pravilne nastavitve in varnega vedenja je treba račun zaščititi z dodatnimi varnostnimi funkcijami. To sta zlasti **močno geslo** in **dvofaktorska avtentikacija**, ki lahko zaščitita podatke, shranjene v računu družbenega omrežja. Za več podrobnosti o temi glejte poglavje Gesla (str. 86).

Katerih podatkov in vsebin ne bi smeli deliti na družbenih omrežjih?

Ne objavljajte nobene **zasebne ali drugače občutljive vsebine**. V družabnih omrežjih, blogih ali na drugih javnih mestih ne sme biti objavljeno:

- številka in fotografija vozniškega dovoljenja, osebne izkaznice ali drugega uradnega dokumenta,
- telefonska številka,
- vaš šolski, domači ali službeni naslov ter naslovi vaših sorodnikov in znancev,
- registrska tablica vozila,
- pogodbe in drugi uradni dokumenti (šolska poročila itd.)

Prav tako ne smete javno deliti nobenih vozovnic ali vstopnic za prireditve, saj jih veliko vsebuje QR kode, ki jih napadalec lahko preprosto kopira s fotografije ali videoposnetka in jih uporabi. Enako pozornost, ki jo namenjate stvarem, ki jih fotografirate in posnamete, morate posvetiti ozadju svojih posnetkov, fotografij in video posnetkov.

Ni priporočljivo objavljati podatkov ali drugih občutljivih podatkov, povezanih z vašimi bližnjimi (vključno z družinskimi člani in sošolci) ter znanci, saj lahko s tem kršite zakone o varstvu osebnih podatkov.

Dokazano je bilo, da ni priporočljivo objaviti in deliti svoje trenutne lokacije na družbenih omrežjih, saj je to mogoče zlahka zlorabiti. Primer tega je rop, v katerem je Kim Kardashian izgubila[14] milijonski nakit, ker je na družbenih omrežjih razkrila preveč o sebi. Uporabniki lahko svojo lokacijo nevede delijo z objavo fotografij ali objav na družbenih omrežjih, vendar lahko takšne podatke zbirajo tudi številne aplikacije. Če želite omejiti zbiranje podatkov o lokaciji, lahko prilagodite nastavitve naprave ali nastavitve posameznih aplikacij.

Kaj naj uporabniki upoštevajo pri izbiri socialnega omrežja?

Učenci / študentje naj uporabljajo samo tista družbena omrežja, katerih starostna omejitev in pogoji ustrezajo. Pri izbiri omrežja ne bi smeli upoštevati le, koliko ljudi iz njihovega družbenega kroga že ima profil v tem omrežju, temveč tudi raven varnosti, ki jo storitev zagotavlja.

Če želite to preveriti, si zastavite naslednja preprosta vprašanja:

- Ali lahko profil nastavim kot zaseben in ali lahko omejim, kdo lahko vidi vsebino, ki jo dam v skupno rabo?
- Kako je moj račun zavarovan: ali gre le za uporabniško ime in geslo ali je mogoče dodati drug faktor preverjanja (številčna koda, preverjanje aplikacije ali SMS-a, prstni odtis)?

Če ste na obe vprašanji odgovorili z ne, vendar se še vedno želite povezati s socialnim omrežjem s tako slabšo varnostjo, morate ustrezno prilagoditi vsebino v skupni rabi in se izogniti občutljivim informacijam v svojih objavah.

14 https://www.vanityfair.com/style/2016/10/solving-kim-kardashian-west-paris-robbery

Na katere lastnosti bi se morali osredotočiti pri izbiri aplikacije za klepet?

Če učenci / študentje uporabljajo aplikacije za klepet, naj se osredotočijo na tiste, ki ponujajo celovito šifriranje. Ta tehnologija ščiti njihovo komunikacijo **od začetka do konca**[15] te komunikacije, vsebina je tako vidna samo obema končnima uporabnikoma. To bistveno otežuje vsakršne poskuse spremljanja sporočil "na poti". Tudi pri teh storitvah lahko vsebina v skupni rabi konča na spletu brez vaše vednosti ali soglasja (npr. če jo uporabnik na drugem koncu komunikacije objavi po uspešnem prejemu).

Ko izbirate aplikacijo za klepet, morate vedno preveriti, kako ponudnik storitev uporablja vaše podatke ter kako jih shranjuje in uporablja. Pogoji so običajno na voljo na spletnem mestu aplikacije, vendar so v nekaterih primerih dostopni neposredno v nastavitvah aplikacije ali v opisu njenih funkcij. Če nekaterih pogojev ne odobravate, jih poskusite onemogočiti ali se popolnoma izogniti uporabi storitve.

Pri nalaganju aplikacij morate vedno preveriti, ali jih prenašate z uradnega spletnega mesta ali iz zaupanja vredne trgovine, zlasti iz profila dejanskega razvijalca (za več informacij glejte poglavje Varnost mobilnih naprav, str. 8). Zlasti trgovina za platformo Android je imela prej težave z lažnimi različicami in imitacijami priljubljenih aplikacij za klepet (WhatsApp, Messenger, Snapchat, Hangouts itd.), katerih namen je bil zbiranje in kraja občutljivih uporabniških podatkov.

Na koga se lahko obrnete, če imate težave na družbenih omrežjih?

Vedno prosite za pomoč nekoga, ki mu zaupate. Za otroke so to običajno njihovi starši, starejši bratje in sestre ali učitelj. Glede na resnost vprašanja lahko poiščejo nadaljnjo pomoč ali se obrnejo na policijo.

Kako napadalci zlorabljajo socialna omrežja?

1. Prepoznajo in zalezujejo bodoče žrtve.
2. Zbirajo občutljive podatke.
3. Širijo (zlonamerne) oglase in potegavščine.
4. Širijo zlonamerno kodo (prek objav, fotografij, skupin in povezav do sporočil).

15 Podrobnosti o uporabi tehnologije v posamezni aplikaciji lahko preverite na Googlu, ali v opisu aplikacije v trgovinah Google Play oz. App Store.

Socialna omrežja in psihološka trdoživost

povezava | strah pred zamujeno priložnostjo | spletno ustrahovanje | mehurčki soacialnih omrežij

Teme zajete v tem poglavju:

Kakšna psihološka tveganja predstavljajo socialna omrežja in kako naj se otroci spopadajo z njimi? Kako negativne in nezadostne povratne informacije na socialnih omrežjih vplivajo na otroke? Kako lahko učitelji otrokom pomagajo premagati negativne ali nezadostne povratne informacije? Zakaj nekateri otroci brez težav uporabljajo socialna omrežja, nekateri pa se soočajo s težavami ali celo z zasvojenostjo? Kako na otroke vplivajo konvencije o lepoti in življenjskem slogu družbenih omrežij? Kako se lahko otrok zaščiti pred temi tveganji? Kaj je FOMO in kako je povezan z uporabo socialnih omrežij? Kako lahko učitelji pomagajo otrokom premagati FOMO?

Kakšna psihološka tveganja predstavljajo socialna omrežja in kako jih otroci lahko obvladajo?

Za njihove uporabnike, zlasti najstnike, so socialna omrežja zelo privlačna. Zanje se predstavitev prek njihovega profila zdi varna, poleg tega lahko delijo različne vrste vsebin, ostanejo v stiku z drugimi in se predstavljajo, ne da bi se morali soočiti s sovrstniki. Lahko tudi objavijo vse, na kar so ponosni - ali njihove izboljšane različice -, kar jim lahko pomaga, da se izognejo neprijetnim situacijam.

Pozitivne reakcije drugih (npr. v obliki všečkov in interakcij) jim začasno spodbudijo samozavest. Vendar se tega človek zlahka navadi in lahko celo povzroči odvisnost. Lahko je škodljivo, če povratne informacije niso pozitivne ali niso tako dobre, kot smo pričakovali. Uporabnika lahko prepričamo, da so na družbenih omrežjih vsi videti še bolj neverjetni in srečni. Otroke je treba naučiti, kako dojemati te pojave v družabnih medijih, in zgraditi psihološko odpornost proti naslednjim tveganjem:

1. Negativne ali nezadostne povratne informacije
2. Obsedeno in problematično vedenje
3. Pritisk konvencij o lepoti in življenjskem slogu
4. Strah pred zamujeno priložnostjo (FOMO)
5. Število prijateljev in priljubljenost
6. Mehurčki družabnih omrežij

Negativne ali nezadostne povratne informacije

V skrajnih primerih lahko to vključuje (spletno) ustrahovanje, trolanje ali sovražni govor na družbenih omrežjih.

Otroci, ki uporabljajo socialna omrežja, se s spletnim ustrahovanjem srečujejo pogosteje kot tisti, ki jih ne uporabljajo. V zvezi s tem so socialna omrežja pogosto platforma, na kateri otroci javno sramotijo svoje vrstnike pred veliko večjim občinstvom, kot bi se lahko "iz oči v oči". Ustrahovalec želi svojo moč pokazati v javnosti.

Učitelji bi morali voditi otroke, da oblikujejo občinstvo, ki ustrahovalca ne opolnomoči in se ne pridruži sramoti; nasprotno, žrtev mora imeti podporo tako v spletu kot zunaj njega. Otroci bi se morali tudi zavedati, da če izvedo za podobno dejanje, naj to povedo odrasli osebi. Za več informacij glejte poglavje Spletno ustrahovanje (str. 14).

Socialna omrežja (npr. Snapchat), ki omogočajo tako imenovane kratkotrajne vsebine, ki so dostopne le kratek čas (npr. fotografije in videoposnetki), predstavljajo tvegano okolje. To lahko pri uporabnikih povzroči tvegano vedenje, ker vedo, da bodo vse sledi njihovih objav kmalu izginile. Takšno tvegano vedenje na družabnih omrežjih vključuje pošiljanje intimnih fotografij, sekstanje, pa tudi neprimerno in ustrahovanje vsebine.

Otrokom je treba poudariti, da lahko tisti, ki želijo zlorabiti fotografije, objavljene na družbenih omrežjih, posnamejo posnetek zaslona, preden fotografija izgine, ali fotografijo posnamejo z drugo digitalno opremo. Vsebino je lahko zlorabljena, npr. zasmehovanje ali izsiljevanje žrtve. Otroci ne trpijo slabega ravnanja le kot stresno - nezadostne povratne informacije so lahko enako težavne.

Kako lahko učitelji otrokom pomagajo premagati negativne ali nezadostne povratne informacije?

Učitelji lahko sistematično vodijo otroke do:

- osredotočiti se na dobre odnose s sovrstniki,
- naučite se reševati konflikte in se prepirati in pobotati po prepiru,
- da ne delijo ničesar, zaradi česar ne želijo biti zasmehovani; manj digitalnih odtisov, manj materialov, ki jih je mogoče zlorabiti,
- vedeti, zakaj bi morali skrbno določiti zasebnost svojih objav,
- vedeti, kako naprej, ko se jim na družbenih omrežjih zgodi kaj neprijetnega.

Uporaba socialnih medijev - kompulzivno in problematično vedenje ter zasvojenost

Otroci lahko družabna omrežja uporabljajo prosto, tudi če z njimi preživijo veliko časa. Pomembno je, kaj točno otrok počne, ali je zadovoljen s tem, koliko časa preživi na družbenih omrežjih, ali pa z njim ni zadovoljen, a ga ne more nadzorovati.

Zakaj nekateri otroci brez težav uporabljajo socialna omrežja, nekateri pa se soočajo s težavami ali celo z zasvojenostjo?

Ali bo otrok zasvojen z družabnimi mediji, je odvisno od njegove situacije - kako zadovoljen je s sabo in s svojimi odnosi. Bolj ko je otrok v notranjosti ranljiv, manj je zadovoljen in integriran s svojimi vrstniki, bolj je njegovo počutje odvisno od tega, kaj mu pomaga izboljšati samopodobo - npr. uspeh na družbenih omrežjih. Za več informacij glejte poglavje Realni in spletni svet (str. 40).

Otroci, ki so preveč negotovi ali zaskrbljeni, lahko obsesivno preverjajo reakcije na svoje objave. Včasih se otroci obrnejo na družabna omrežja zaradi dolgočasja ali osamljenosti ali da bi se zamotili, ko jih skrbi.

PRITISK IDEALOV O LEPOTI IN ŽIVLJENJSKEM SLOGU

Kako na otroke vplivajo konvencije o lepoti in življenjskem slogu družbenih omrežij?

Profili v družabnih omrežjih so pogosto videti kot vitrine popolnih videzov in razburljivih življenj, v primerjavi s katerimi se najstnik lahko počuti neustrezno. To še posebej velja za družbena omrežja, ki temeljijo predvsem na fotografijah, kot je Instagram. Ker so otroci še posebej ranljivi in pogosto uporabljajo družabna omrežja, so bolj nagnjeni k tesnobi, slabemu videzu ali strahu pred pogrešanjem. Socialna omrežja, ki temeljijo na skupni rabi videoposnetkov, na primer YouTube, manj negativno vplivajo na dobro počutje otrok in jih lahko obogatijo v mnogih pogledih.

Če jih uporabimo preveč, je lahko pritisk socialnih medijev na dobro počutje velik. V tem primeru so najbolj ranljivi otroci, ki pred uporabo družbenih omrežij niso zadovoljni.

Kako se lahko otrok zaščiti pred pritiski lepotnih in življenjskih konvencij?

- Uporabniki naj izberejo družbena omrežja, ki ustrezajo njihovi starosti, ob upoštevanju priporočil profesionalnih razvijalcev.
- Socialne medije je treba uporabljati za interakcijo in ne samo za pasivno brskanje po objavah drugih ljudi. Tudi v Instagramu, socialnem omrežju, značilnem za pasivno gledanje, lahko ustvarjate stvari, kot so zgodbe, ki povečajo stopnjo interakcije z drugimi uporabniki.
- Uporabniki lahko navadno več izkoristijo s socialnimi mediji, ki ponujajo raznoliko in bolj realistično vsebino (na primer YouTube).
- Z manj interaktivnimi družabnimi mediji (kot je Instagram) mora biti uporabnik aktiven in preudaren pri izbiri prijateljev in naročnin. Poleg vplivnih oseb lahko spremljate objave iz različnih kategorij, kot so hobiji, potovanja, umetnost, šport itd. Izbira naročnin je v celoti odvisna od vas in bo vplivala na to, kaj boste videli in se obdali.

STRAH PRED ZAMUJENO PRILOŽNOSTJO (ANG. FOMO)

Kaj je FOMO in kako je povezan z uporabo socialnih omrežij?

Strah pred zamujeno priložnostjo (ang. fear of missing out - FOMO) je strah, da se lahko zgodi kaj zanimivega ali pomembnega in ga lahko človek zamudi. Strah pred zamudo je povezan tudi z izkušnjami brez povezave - ljudje običajno želijo biti tam, kjer se nekaj dogaja, in ostati v stiku. Na internetu se strah pred pogrešanjem lahko nanaša na marsikaj, ne le na socialna omrežja. Nekdo na primer lahko obsesivno preveri novice v strahu, da ne bi izpustil socialnih zadev. Otroke in mladostnike pa običajno bolj kot gospodarske in politične razmere zanima to, kaj se dogaja med njihovimi vrstniki ali njihov profil, in tega ne želijo zamuditi. Preprosto je čutiti strah pred zamujenimi socialnimi omrežji, saj lahko neprestano preverjamo, ali so na voljo posodobitve in interakcije s socialnimi statusi.

Uporabnike tudi redno obveščajo o dogodkih in dejanjih, ki bi jih lahko zanimali, ali tistih, ki jih zanimajo njihovi prijatelji. Nenehno preverjanje, kaj njihovi prijatelji počnejo ali nameravajo storiti, in primerjava tega s tem, kar počnejo, otroke pogosto pritiska ali se počutijo neustrezne. Če ne bi vedeli za dejavnosti svojih prijateljev, bi jim bilo morda povsem naravno, da ostanejo doma in čas preživijo umirjeno.

Kako lahko učitelji pomagajo otrokom premagati FOMO?

- Učitelj lahko pomaga otrokom, da se bolje spoznajo in odkrijejo, kakšne so njihove resnične potrebe in želje.
- Učitelj lahko razloži, kaj je FOMO, in tako zmanjša vpliv pojava. Uporabnike mladostnikov je treba tudi opozoriti, da so družabna omrežja vitrina strnjenih, ekskluzivnih trenutkov, ki ne ponujajo uravnotežene podobe posameznikovega življenja, ki vključuje tudi slabe trenutke in vsakodnevna opravila.

ŠTEVILO PRIJATELJEV IN PRILJUBLJENOST

Za mlade se zdi veliko prijateljev fantastično. Pa so to resnični prijatelji? Ali pa gre le za uporabnike, ki so jih naključno dodali, da se predstavljajo kot "prijatelji"? Ali bi morali ti "prijatelji" res vedeti vse, kar želi uporabnik deliti s svojimi najbližjimi prijatelji? Odgovor na to vprašanje je najverjetneje "ne", vendar se večina mladih uporabnikov tega ne zaveda pri pisanju posameznih objav. Skupna raba se običajno zgodi v določenem razpoloženju, ko se uporabnik ne ustavi in pomisli na možne posledice. Poleg tega lahko podzavestno mislijo: več ljudi kot to vidi, večja je možnost (dobre) povratne informacije. To pa običajno ni najboljša rešitev.

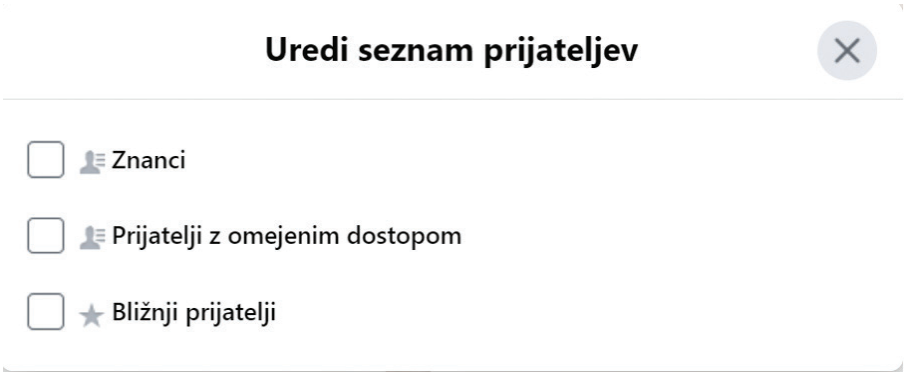
Koga bi morali dodati med svoje stike na družbenih omrežjih?

- Osnovno pravilo za vse uporabnike družabnih omrežij je, da dodajo / prijavijo samo osebe, ki jih že poznajo v resničnem življenju ali s katerimi imajo v resnici vsaj več skupnih prijateljev.
- Če vas zanimajo mnenja nekoga, ki ga osebno ne poznate, lahko njegove dejavnosti "spremljate", ne da bi se z njimi družili na družabnih omrežjih (npr. Facebook) ali če tej osebi ne dovolite, da sledi vaši vsebini (npr. Instagram). "Slediti" vam omogoča, da vas navdihujejo spoznanja drugih, hkrati pa ne delite preveč svojega zasebnega življenja.

- Podobno lahko nekdo drug brez vaše vednosti začne spremljati vaše dejavnosti na družbenih omrežjih, tudi če vam ne pošlje zahteve za prijateljstvo. Takšna oseba je lahko tudi nekdo s slabimi nameni. Da bi se temu izognili, lahko spremenite nastavitve zasebnosti, npr. na Facebooku v razdelku "Nastavitve" → "Zasebnost" → "Kdo vam lahko pošlje zahteve za prijateljstvo?" in "Kdo te lahko poišče?".

Prijatelj na družbenem omrežju ni samodejno tesen prijatelj

- Če je mogoče, si vzemite dovolj časa za ustvarjanje kategorij stikov / prijateljev v svojih družabnih omrežjih. Odnosi se naravno razvijajo in nekomu, s katerim ste se razumeli pri 13 letih, sploh ni treba, da je vaš prijatelj pri 15. Zato morate redno posodabljati seznam prijateljev in njegove podkategorije. Na Facebooku lahko vsakemu prijatelju s seznama dodelijo eno od naslednjih kategorij: "Prijatelji z omejenim dostopom", "Znanci", "Bližnji prijatelji" (glej sliko 4).



SLIKA 4: *Kategorije prijateljev na Facebooku.*

- Facebook ponuja tudi možnost "prejemanja obvestil" o objavah vaših stikov v družbenih omrežjih. Običajno se uporablja za stike, o katerih želite biti še posebej dobro obveščeni.
- Potem obstaja možnost, da "odstraniš" prijatelja iz Facebooka. Ko nekoga odstraniš, se to naredi diskretno, torej ta oseba ne bo izvedela, da si z njo prijateljeval, in to ne bo škodilo njenim občutkom. Tako vam ni treba skrbeti in lahko prilagodite nastavitve stikov, kot želite.

Pri pregledu stikov na družbenih omrežjih morate upoštevati naslednje:

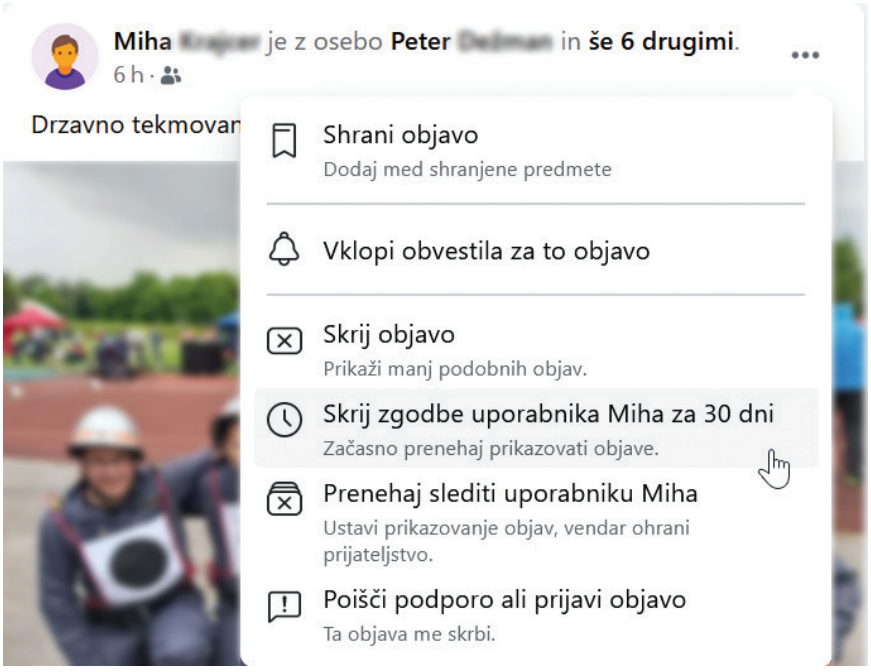
- Ali sem še vedno prijatelj s to osebo?
- Me še vedno zanima, kaj počnejo?
- Kaj mi nudi?
- Ali se želim obkrožiti z njihovimi mnenji ali jih ne maram?
- Bi morali vedeti vse, kar včasih želim deliti?

Mehurčki socialnih omrežij
Algoritem za prikaz vsebine v vašem viru novic se prilagodi glede na to, s katerimi objavami najpogosteje komunicirate in katere (in čigave) objave kliknete, ocenite in komentirate. Algoritem družabnega omrežja ovrednoti vse te interakcije in nato prikaže ujemajoče se in podobne objave v vašem viru novic, pri čemer prepreči druge vrste objav, s katerimi v preteklosti niste komunicirali.

Vendar to ustvari izbor določene vrste objav, prikazanih uporabniku. To se včasih imenuje ustvarjanje mehurčkov za družabno mreženje. To pomeni, da je uporabnik večinoma obkrožen z vsebino in mnenji, ki ga zanima. Druga mnenja ali vsebina se prikažejo manj, teme pa postanejo manj raznolike in uporabnika zaprejo v njegov oblaček. To tudi daje uporabniku občutek, da so njegova mnenja resnična in jih potrjuje okolica, kar slabi njegovo kritično razmišljanje in je uporabnik bolj dovzeten za dezinformacije in prevara.

Učinek socialnih balončkov je mogoče zmanjšati:

- Z urejanjem tega, s čim je uporabnik obkrožen na družbenih omrežjih.
- S pogostejšimi interakcijami v družabnih omrežjih in vzdrževanjem raznolikih medosebnih odnosov brez povezave.
- Z namernim iskanjem tem in prijateljev, s katerimi uporabnik v zadnjem času ni imel veliko stikov, tudi če algoritem socialnega omrežja ni vključeval njihovih objav na uporabnikovem prikazovanju objav.
- Na Facebooku z občasnim (začasnim) onemogočanjem objav določenih oseb. Če uporabnik meni, da njegov vir novic vsebuje preveč objav določene vrste, lahko bodisi blokira prijatelja, skrije vse njegove objave ali zahteva, da socialno omrežje en mesec ne prikazuje njihovih objav. Če uporabnik ve, da si želi daljše premore, lahko osebi preneha slediti ali omeji prikaz določenih vrst objav. To lahko storite tako, da nastavite možnosti za določeno objavo, ne v nastavitvah prijateljstva.



Vplivneži

vplivnež | youtuber | vlog | vloganje | blog | bloganje | bloger | sovražni govor

Teme zajete v tem poglavju:

Kdo so vplivneži in kako vplivajo na življenja otrok? Kašno moč imajo vplivneži? Kako dojemati psihološko pomoč vplivnežev? Ali vplivneži vplivajo na otrokovo samoumevnost in identiteto? Kako lahko izberete pravega vplivneža? Kako lahko opazite oglaševanje katerega soavtorji so vplivneži? Kako lahko pri opazovanju vaših najljubših vplivnežev ohranjate kritično razmišljanje? Kaj je potrebno, da postaneš vplivnež?

VIDEO ZA UČITELJE: youtu.be/8LEJovZ2Diw

Kdo so vplivneži in kako vplivajo na življenje otrok?

Vplivnež je nekdo, ki je postal priljubljen prek družbenih omrežij, ima veliko sledilcev in ima visoko stopnjo ogledov. Njihove objave lahko tako pomembno vplivajo na mnenja in vedenje drugih.

Otroci odkrivajo lastno identiteto in pogosto jim pomaga, če se lahko poistovetijo z nekom svoje starosti. Vplivnež je pogosto lahko tudi najstnik. Pogovarjajo se o tem, kar marsikaterega otroka zanima, a o tem še ne vedo veliko. To otrokom pomaga dojeti marsikaj, jih navdihuje in jim daje nasvete. Objave vplivne osebe so lahko hkrati trendovske in zabavne ter otrokom pomagajo pri sprostitvi.

Objave vplivnih oseb imajo lahko več oblik:

1. **Fotografije**, npr. na Instagramu in Snapchatu - dveh družbenih omrežjih, ki temeljita predvsem na izmenjavi in ocenjevanju fotografij in video zgodb.

2. **Blog** — spletno mesto, ki omogoča registriranim uporabnikom (blogerjem), da kronološko objavljajo svoje objave v obliki člankov, ki lahko vsebujejo dodatno večpredstavnostno vsebino, na primer fotografije in video posnetke. Vsebina in teme so lahko zelo raznolike - od razmišljanj o družbi, do znanstvenih člankov, nasvetov in trikov, dnevnika, pa vse do šolskega ali podjetniškega bloga. Blogi običajno omogočajo uporabnikom, da komentirajo, ocenjujejo in delijo posamezne objave, kar še poveča njihove stopnje ogledov in možnosti za vpliv

3. **Videi** v skupni rabi na družabnih omrežjih - včasih imenovani tudi **vlogi**. Vlog (kratica za video blog) je oblika spletnega dnevnika, pri katerem komunikacija uporabnika (vlogerja) ni pisna, temveč ustna; snemajo sebe in okolico, medtem ko se o nečem pogovarjajo. Posneti video blogi (vlogi) so najpogosteje v skupni rabi na YouTubu, zato vlogerje, ki svoje objave delijo na YouTubu, imenujejo tudi **youtuberji**.

Za nekatere uporabnike je preprostejše in bolj naravno snemanje vloga namesto pisanja besedila. Podobno je za nekatere ciljne skupine ogled videoposnetka bolj privlačen kot branje besedila. Vplivci se ukvarjajo z različnimi temami, s čimer ustvarjajo svojo specifično vsebino in oblikujejo svojo identiteto. Teme so lahko zelo raznolike, npr. navodila, vadnice za video igre, šaljivi ali poučni video posnetki, redni povzetki novic, potovanja, fitnes itd.

Sledenje vplivnežem vključuje tudi določena tveganja, zato moramo razviti otrokovo sposobnost soočanja s tveganji. Otroci morajo vedeti, s katerimi tveganji so povezani, da bodo lahko vplivali in jim ne le slepo sledili. To zahteva tudi kritično razmišljanje in medijsko pismenost, ker je koristno med seboj povezati takšne teme in dejavnosti.

Kakšno moč imajo vplivneži?

Vplivneži so za svoje oboževalce živo utelešenje vrednot, trendov, idealov lepote in življenjskega sloga. Otroci začnejo opažati stvari o sebi in okolici, ki temeljijo predvsem na tem, kaj vplivneži počnejo in o čem govorijo. To je skrita moč, ki jo vplivneži pridobijo, ko postanejo priljubljeni. Uporablja se lahko za plemenite namene, npr. za širjenje dobrega, rušenje predsodkov ali podporo zdravim ali ekološkim vzrokom, za pomoč drugim itd. Lahko pa se uporablja tudi za podporo izdelkov blagovnih znamk, s katerimi vplivne osebe sodelujejo.

Kako bi morali dojemati psihološko pomoč vplivnežev?

Lahko je koristno, kadar vplivneži pomagajo otrokom, da vidijo, da so v redu taki kot so in se spoštujejo. Vplivneži lahko to storijo tako, da govorijo o pozitivnih in negativnih izkušnjah, s katerimi so se morali spoprijeti. Nekateri vplivneži odkrito govorijo o tem, kaj je potrebno, da se soočijo s sovražnim govorom ali ustrahovanjem, psihološkimi krizami in težavami, razhodi in lastnimi strahovi ter kako so se z njimi spoprijeli. Takšne objave otrokom kažejo, da se jih ni treba sramovati, kaj preživljajo, včasih pa lahko celo najdejo nasvet, kako se spoprijeti s svojimi težavami. Kljub temu njihove objave ne predstavljajo univerzalnega nasveta.

Kako lahko še naprej kritično razmišljate, ko gledate svoje najljubše vplivneže?

Redno spremljanje vplivnežev in zvezdnikov je običajna dejavnost v prostem času, ki je bila včasih priljubljena tudi pri prejšnjih generacijah. Spremenili so se medij, oblika in pogostost, s katero jim današnji otroci lahko sledijo - zahvaljujoč pametnim telefonom to v bistvu pomeni neprekinjeno. Na družbenih omrežjih lahko pogosteje vidimo strnjeno različico stiliziranih in retuširanih objav ter prototipe neverjetnih življenj in popolnega videza drugih uporabnikov in vplivnežev.

Ko si predstavljajo življenje vplivnežev, najstniki verjetno razmišljajo o neverjetnih slikah in video posnetkih s počitnic, potovanj in sodelovanja z velikimi blagovnimi znamkami in brezplačnimi izdelki. Otroke lahko celo prepričajo, da v svetu njihovih idolov ni težav.

Tveganje za otroka je, da se takšna delovna mesta strežejo prek medija, ki lahko v odsotnosti kritičnega mišljenja ustvari videz pristnosti.

Za razliko od fotografij videoposnetki zagotavljajo več dražljajev in bolj skladno sliko kot stilizirane in urejene slike. Video posnetki vsebujejo tudi neverbalno komunikacijo in so tako bližje resničnosti. Občasno lahko vplivneži v videu naredijo kaj nepopolnega, se smejijo sebi in niso ves čas popolni.

Kako vplivneži vplivajo na otrokovo samozaznavanje in identiteto?

- **Samozavest**
  Otroci se morda ne zavedajo, da sta video ali objava le majhen delček vpliva življenja. Niso vedno popolnoma oblečeni in duhoviti, tudi njim je lahko dolgčas, so depresivni ali povsem običajni. Tega pa običajno ne zajamejo fotografije in video. Ko otroci postanejo žrtve te iluzije, ne da bi se tega zavedali, se lahko počutijo manjvredne in običajne.
  - Otroke je treba opozoriti, da objave vplivnih oseb ne kažejo celotne resnice, da so videoposnetki urejeni, da so fotografije stilizirane in da številni vplivniki kažejo le lepe stvari.
- **Imitacija**
  - V mladosti je naravno, da otroci želijo posnemati svoje idole. Vendar jih je treba nenehno opozarjati, da je vsak od njih edinstvena osebnost in škoda bi bilo, če bi se ta posebnost izgubila. Otroci se morajo tudi bolje spoznati, torej spoznati, kaj jih dela edinstvene.

Kako lahko otrok izbere pravega vplivneža?

Vplivneži imajo veliko moč in sposobnost vplivanja na javna mnenja in vrednote. Ta moč ni samooklicana, nasprotno, občinstvu je nekaj všeč na njih in to "nekaj" jim je pomagalo zbrati privržence uporabnikov. Več oboževalcev imajo, močneje vplivajo na javnost in ljudi, ki morda sploh ne vedo, kaj naredi vplivneža "tako edinstvenega in privlačnega". V bistvu jim sledijo, ker sledijo trendom in sledijo času.

Sledenje vplivnežem samo zato, ker so priljubljeni in v trendu, ni nujno najbolj razumna rešitev. Prikrito ima vplivnež različna mnenja, okus in vrednote, zato je pomembna izbira pravega vplivneža. Nekatere znane osebnosti lahko otroke navdihnejo, da se ukvarjajo s športom, sprejmejo bolj zdrav življenjski slog, pokažejo pogum ali podprejo dobrodelne organizacije, druge pa ponujajo sporen način življenja, povezan s številnimi tveganji.

Učitelj naj se s svojimi učenci pogovori o naslednjem:

- S čigavim mnenjem, jezikom in osebnostjo želijo biti redno v stiku?
- Kaj jim pomeni?
- Kaj želijo videti in slišati od izbranega vplivneža?
- Kako bi jih vplivnež lahko nepopravljivo razočaral?

Kako lahko opazite oglaševanje, katerega soavtorji so vplivneži?

Današnji vplivneži sodelujejo z nekaterimi blagovnimi znamkami in s promocijo njihovih izdelkov zaslužijo dobiček. To spremeni njihove objave v oglase. Ko gledalci na televiziji vidijo oglas, npr. za kozmetični izdelek se jasno zavedajo, da gre za oglaševanje. Če pa priljubljena influencerka v enem od svojih videoposnetkov omeni, kako ji je določena krema pomagala, je videti kot izkušnja in resničnost. Sledilec to morda ne dojema kot oglaševanje, prej dejstvo. Sledilcu je vplivnež všeč, mu zaupa in je bolj verjetno, da bo verjel, kar pravi o izdelkih. Zaradi pomanjkanja eksplicitnosti vplivneži postanejo zelo močna oglaševalska orodja. Med promovirane izdelke običajno sodijo modne znamke, pijače, zdrava prehrana, izdelki za fitnes, elektronski izdelki, igre, nakit ali potovalne agencije. In seveda lastne blagovne znamke in izdelki, če jih imajo (oblačila, glasbeni albumi itd.).

Kaj je potrebno, da postaneš vplivnež?

Otroci in najstniki pogosto zaznajo le prednosti, ki jih prinese delo vplivneža, in ne razmišljajo o trdem delu in tveganjih, s katerimi se srečujejo njihovi vzorniki. Mnogi sanjajo o tako privlačni in na videz lahki karierni poti. Anketa[16] o sanjskih zaposlitvah, izvedena med 11 in 16-letniki, kaže, da zdravnik še vedno ostaja najbolj priljubljen poklic (18%), tesno pa mu sledijo influencer (17%) in YouTuber (14%). Ta premik v priljubljenosti poklicev je povsem naraven glede na to, kaj je prinesla digitalna doba in obstoj družbenih medijev.

Vendar pa njihova mnenja izkrivljajo nenehni obiski priljubljenih vplivnežev, torej rezultat dolgoročnega prizadevanja več ljudi, ki jim je uspelo. Poleg njih je veliko tistih, ki po nekaj mesecih izčrpavajočega dela na družbenih omrežjih s slabimi rezultati niso uspeli ali so "izgubili zanimanje". Uspeh ni enostaven. Priljubljeni vplivneži v enem tednu niso postali priljubljeni in konkurenca narašča. Poleg tega, čeprav so priljubljeni, poklic vplivneža prinaša veliko **negativnosti, ki jih oboževalci ne vidijo**:

1. **Pritisk za izvedbo.** Vplivnež mora ostati nenehno aktiven in ustvarjalen. Da bi ohranili svoje sledilce, potrebujejo natančen koncept in načrt, na kaj naj se osredotočijo in kako to doseči s svojimi objavami. Svoje vizije morajo napolniti z vsebino in ne smemo pozabiti, da je priprava, snemanje in promocija njihovih objav resnično delo, ki zahteva čas in energijo. Delo, ki ga je treba opraviti, tudi če vplivnež ni razpoložen.

2. **Pritisk za povratne informacije.** Kljub velikemu trudu vplivne osebe so povratne informacije o njihovih objavah lahko šibke ali povprečne, včasih nesorazmerno slabe glede na vloženo energijo.

16 https://www.hrreview.co.uk/hr-news/1-of-5-british-children-want-a-career-as-social-media-influencers/114597

3. **Ustrahovanje in trolanje.** Verjetno vsi vplivneži na družbenih omrežjih doživljajo negativne povratne informacije, spletno ustrahovanje in trolanje.

4. **Nevarnost izgorelosti.** Po nekaj mesecih ali letih vplivne osebe pogosto doživijo sindrom izgorelosti, izgubijo energijo za nadaljevanje in se počutijo utrujene ter odvrnjene zaradi negativnih reakcij.

5. **Izguba zasebnosti.** Z vso priljubljenostjo in pretirano izmenjavo vsebin o svojem življenju tvegajo, da bodo izgubili vso zasebnost, kar ogroža njihovo počutje in varnost.

6. **Vprašanja odnosov in resničnega življenja.** Osredotočenost na delo in oboževalce jim jemlje čas, pozornost in energijo, ki bi jo lahko namenili svojim najdražjim in družini. Nekatera prijateljstva bodo na preizkušnji ali ogrožena zaradi bremena priljubljenosti in ljubosumja njihovih prijateljev. Roji oboževalcev ne pomenijo nujno, da imamo dovolj tesnih prijateljev, ki so dragoceni.

Realni in spletni svet

problematična raba interneta | internetna odvisnost | prenos iz iger v realni svet | selfi dismorfija

Teme zajete v tem poglavju:

Ali obstaja zasvojenost z internetom? Kaj se nam zdi pri uporabi interneta problematično? Kdaj postanete odvisni od spletnih dejavnosti? Kako lahko učitelj opazi, da je otrok odvisen od spletnih dejavnosti? Ali obstaja resnična grožnja, da bi se otrok s pogostimi igrami lahko izgubil v navidezni resničnosti? Kdaj govorimo o problematični uporabi družbenih omrežij? Ali se otroci predstavljajo res taki kot so na slikah objavljenih na družbenih omrežjih? Kaj povzroča strah pred zamujeno priložnostjo pri otrocih? Kako lepotne konvencije vplivajo na samozaznavanje otrok? Ali otroci dojemajo svoje dejanske izkušnje ali pa samo izbirajo ozadje za svoje "fotografiranje"? Ali otroci tvegajo komunikacijsko preobremenitev?

Ali obstaja zasvojenost z internetom?

Zasvojenost z internetom (ob upoštevanju interneta kot medija) ne obstaja. Spletni in nespletni svet sta le dve različni okolji, v katerih ljudje doživljajo različne stvari, in tako kot ni zasvojenosti z "brez povezave", ni odvisnosti od "biti na spletu". Obstajajo samo odvisnosti od določenih spletnih dejavnosti ali prekomerna / problematična uporaba takšnih dejavnosti. Pri otrocih in najstnikih to vključuje zlasti naslednje spletne dejavnosti:

- igranje digitalnih iger,
- iskanje informacij,
- uporaba socialnih omrežij in klepeta,
- pretirano gledanje videov,
- spletno nakupovanje.

Kaj se nam zdi pri uporabi interneta problematično?

V internetu lahko uživate v številnih dejavnostih, ki pa vas v določenih okoliščinah lahko prevzamejo do te mere, da jih nenehno ponavljate in se ne morete ustaviti. To je tako imenovana problematična uporaba interneta, torej tista, ki moti tako zasebno kot družbeno življenje in vodi do slabših rezultatov v službi ali v šoli.

Problematična uporaba interneta še ni odvisnost, ampak nekakšno sivo kritično območje. Z boljšim spletnim režimom se lahko izboljša brez kakršnih koli trajnih posledic. Vendar obstajajo tudi primeri, ko se problematična uporaba interneta razvije v popolno odvisnost, podobno odvisnosti od alkohola. Ko zaznamo tako problematično uporabo interneta, moramo biti previdni in poskusiti preprečiti, da bi se razvil v odvisnost. Prekomerna uporaba interneta je razširjena zlasti med najstniki in mlajšimi odraslimi (13–20 let).

Kaj priljubljeno spletno dejavnost spremeni v težavo ali zasvojenost? Vprašanje ni le intenzivnost in čas, ki ga otrok namenja takšnim dejavnostim, temveč moramo pogledati tudi njihov poseben položaj in ranljivost.

Sledijo dejavniki tveganja za problematično uporabo interneta:

- genetska ranljivost (zgodovina odvisnosti v družini),
- trenutna psihološka ranljivost (težko obdobje, veliko stresa, depresija),
- splošno zadovoljstvo z življenjem, družinskimi razmerami in kakovostjo vrstnikov ter drugimi odnosi,
- psihološka odpornost otroka, stres in strategije spopadanja s konflikti,
- situacijski dejavniki (razpad, prepiri, izguba varnosti, močne negativne izkušnje),
- pomanjkanje raznolikih dejavnosti, ki jih lahko otrok uživa v svetu brez povezave,
- naravo spletne dejavnosti.

Kdaj postanete odvisni od spletnih dejavnosti?

Čas, namenjen samo tej aktivnosti, ni nujno znak odvisnosti. Najpomembnejši kazalnik je odnos otroka do dane dejavnosti, torej ali je to razmerje relativno brezplačno ali je otrokovo "življenje od njega odvisno". Odločilni dejavnik je prednostna naloga, ki jo otrok dodeli spletni aktivnosti, in ali jim ta dejavnost odvzame druge pomembne vidike življenja.

Kot pri vseh drugih odvisnostih mora biti tudi v spletnih zasvojenostih naslednjih 6 kazalnikov:

1. **Pomen.** Dana dejavnost postane za človeka na prvem mestu, vse druge dejavnosti pa postanejo nepomembne. Oseba večino svoje energije posveti eni sami dejavnosti in njenemu razmišljanju. Če je ta oseba otrok, lahko tisti okoli njih opazijo zmanjšanje števila različnih hobijev in dejavnosti, ki so bile prej del njihovega življenja.

2. **Nihanje razpoloženja.** Če je otrokovo razpoloženje odvisno od dejavnosti, ki jo zasvoji, ali pomanjkanja le-te.

3. **Rast potrebe** po opravljanju eno določeno dejavnost. Da bi neka oseba še naprej prinašala veselje osebi, jo mora izvajati vedno pogosteje, z naraščajočo intenzivnostjo.

4. **Odtegnitveni simptomi.** To je neprijetno stanje, ki se začne, ko odvisnik ne more opravljati ali mora omejiti dejavnosti, od katere je odvisen. Neželeni učinki - tako kot pri odvisnosti od snovi - so slabo razpoloženje, razdražljivost, agresivnost, živčnost in nezmožnost osredotočanja.

5. **Konflikt.** To je eden osnovnih simptomov odvisnosti. Ponavljajoče zasvojenost povzroča težave v odnosih, v šolskih rezultatih in lahko pride tudi do notranjega konflikta (občutki krivde, gnusa do sebe).

6. **Izguba nadzora.** Po obdobju, v katerem si nekdo prizadeva omejiti spletne dejavnosti, običajno pride do situacij, ko človek popolnoma izgubi nadzor in zasvojenost postane močna.

Osnovni razlikovalec med odvisnostmi in spletnimi aktivnostmi je konflikt in izguba nadzora. To pomeni, da se oseba res zaveda, da ji določeno vedenje povzroča težave, vendar ga kljub vsem prizadevanjem ne more nadzorovati in se k njemu še naprej vrača. Simptomi zasvojenosti z internetom so pogosto znaki drugih duševnih težav, ki bi prav tako lahko bile pozorne.

Na srečo je takšna zasvojenost s spletnimi dejavnostmi, ki ne temelji na snoveh, dokaj redka in v večini primerov imamo opravka s "problematično uporabo interneta", ki prizadene precej velik del prebivalstva, zlasti mlade.

Kako lahko učitelj opazi, da je otrok odvisen od spletnih dejavnosti?

Otrok skoraj nikoli ne bo stopil v stik z učiteljem, če bo začel izgubljati nadzor nad svojimi spletnimi aktivnostmi. Prav tako ni težko opaziti te težave, ker sta internet in digitalne tehnologije postala sestavni del našega življenja. Otroci tudi o njih veliko govorijo, zato je tema v bistvu vseprisotna. Učitelj pa lahko opazi nekaj sprememb v otrokovem vedenju:

- otrok je zaspan in nemiren,
- njihove ocene se slabšajo in izgubijo zanimanje za šolo,
- otrok je pogosto slabe volje, vznemirjen, agresiven in moten,
- imajo bistveno manj prijateljev,
- ne govorijo o ničemer drugem,
- izgubijo zanimanje za vse druge hobije,
- veselijo se le svoje najljubše spletne aktivnosti.

Te spremembe v otrokovem vedenju lahko učitelju pomagajo prepoznati spletno odvisnost. Običajno je mogoče ugotoviti, s katero specifično zasvojenostjo s spletom imamo opravka iz tistega, o čemer otrok najpogosteje govori, na primer igranja iger, družbenih omrežij itd.

Ker so lahko vpletene tudi druge duševne težave, se mora učitelj o tem posvetovati z otrokovimi starši, ki običajno najbolje vedo, kaj se dogaja z njihovim otrokom. Lahko se obrnejo tudi na šolskega psihologa in priporočijo, da učenčevi starši poiščejo družinsko terapevtsko pomoč.

Kaj lahko stori učitelj?

- z otroki zgradi dober odnos, ki temelji na spoštovanju in zaupanju,
- pokaže zanimanje za njihovo počutje, kako jim gre in kaj počnejo v prostem času,
- je pozoren, da opazi morebitne spremembe v vedenju posameznih otrok,
- če sumi, da gre za težavo, se pogovri s starši o otrokovih skrbeh, starši pa doma določijo pravila glede spletnih dejavnosti in digitalnih orodij,
- med poukom vključi učence v dejavnosti, ki opozarjajo na različna tveganja,
- ozavešča o odvisnosti od spletnih dejavnosti,
- uporabi preproste načine za medvrstniško učenje in za preprečevanje medvrstniškega nasilja,
- izboljša lastno znanje in kompetence ter spremlja uporabo posameznih spletnih dejavnosti in aplikacij,
- nauči učence, kako naj dojemajo lastne uporabniške navade v širšem pomenu - npr. kako se navezujejo na njihovo razpoloženje, sodelovanje v dejavnostih zunaj spleta, dojemanje uspeha ali neuspeha, življenjskih situacij itd. Ozaveščen uporabnik interneta je bolje pripravljen prevzeti nadzor nad svojim spletnim življenjem.

Problematično igranje video iger

Danes skoraj vsi otroci igrajo nekatere videoigre, bodisi na računalnikih, tablicah, igralnih konzolah, pametnih telefonih ali kje drugje. Zdi se, da imajo dekleta in fantje približno enako zanimanje za elektronsko zabavo. Starši in učitelji bi vsekakor raje, če bi otroci igrali le poučne igre, dejstvo pa je, da otroci želijo igrati predvsem za zabavo. Ko otroci igrajo starosti primerne igre ter se zavedajo časa in vloge iger v življenju, je to le neškodljiva zabava. Vendar pa obstajajo tudi otroci, ki pretirano igrajo in nočejo početi ničesar drugega ter za katere je igranje iger postalo prednostna naloga številka ena. To so lahko znaki zasvojenosti z igrami. Le približno 3-5% otrok trpi zaradi te težave.

Odvisnosti se najpogosteje razvijejo med igralci MOBA - večigralskih spletnih borilnih aren (ang. Multiplayer Online Battle Arena). To so kratka bojna zaporedja, ki jih igrajo večinoma fantje (npr. League of Legends, World of Tanks).

Sledijo igre MMORPG - masivno-večigralsko spletno igranje domišljijskih vlog (ang. Massively Multiplayer Online Role-Playing Game), ki vključujejo nenehno izboljševanje lastnega avatarja (npr. World of Warcraft).

Med otroki so zelo priljubljene tudi kreativne gradbene igre, kot je Minecraft. Tu lahko igralec oblikuje okolje, v katerem je njegov lik. Pri igrah, kot je Minecraft, je verjetnost zasvojenosti veliko manjša, saj je igra kreativna, neagresivna in zaporedje gibov v igri počasnejše. Ta igra je zelo priljubljena tudi med mlajšimi otroki. Če starši podpirajo različne dejavnosti in hobije, so odvisnosti od spleta v mladosti precej redke.

Ali obstaja resnična grožnja, da bi se otrok s pogostimi igrami lahko izgubil v navidezni resničnosti?

Pojav prenosa iz iger v realni svet[17]

Kadar ljudje pogosto igrajo spletne ali računalniške igre, se tudi po izklopu videoigre še vedno odzivajo na dražljaje iz resničnega sveta, kot da bi bili dražljaji v igrah. Vsakodnevne situacije jih lahko opomnijo na izzive, s katerimi so se soočali v igri, in nanje reagirajo enako. To je lahko bodisi čustveni odziv (naval adrenalina, pripravljenost za akcijo) bodisi besedni / duševni odziv. Včasih se ljudje lahko dojemajo kot junaki v igri in svet vidijo skozi njihove oči. V resničnem svetu lahko vidijo rešetke, ki visijo nad glavami ljudi, ali pričakujejo, da bodo našli skrit zaklad tik za vogalom.

Kljub temu pa to ne pomeni nujno, da so razvili odvisnost. To je lahko le naravna prilagoditev uma načinu, kako možgani dojemajo svet v igri. To lahko vključuje tudi ponavljanje vsiljivih misli, povezanih z igrami - neke vrste povratne informacije. To je običajno pri dolgih igralnih sejah ali pri spremljanju TV oddaj. Ko si oddahnete od teh dejavnosti, se vaš um ponastavi nazaj v resnični svet.

Tveganje je, ko vaš um želi ostati v okolju, na katerega se je navadil. To je pogosto osnova za obsesivno igranje in v nekaterih primerih gonilo zasvojenosti. Ni vsak otrok, ki veliko časa preživi z igranjem iger, zasvojen - lahko uživa in še vedno uživa v številnih drugih dejavnostih v svojem življenju.

17 https://www.psychologytoday.com/us/blog/mental-mishaps/201405/video-games-invade-the-real-world

Kdaj govorimo o problematični uporabi družbenih omrežij?

Otroci lahko družabna omrežja uporabljajo prosto, tudi če z njimi preživijo veliko časa. Pomembno je, kaj točno otrok počne in zakaj ter ali je zadovoljen s tem, koliko časa preživi na družbenih omrežjih. Včasih z njo niso zadovoljni, vendar je ne morejo nadzorovati. Bolj ko je otrok v notranjosti ranljiv, in manj kot je zadovoljen in integriran s svojimi vrstniki, bolj sta njegovo razpoloženje in počutje lahko odvisni od njegovega uspeha na družbenih omrežjih.

Otroci, ki so zaskrbljeni in nimajo samozavesti, lahko obsesivno preverjajo reakcije na svoje objave. Včasih se otroci obrnejo na družabna omrežja zaradi dolgočasja ali osamljenosti ali da bi se zamotili, ko jih skrbi.

Kako lepotne konvencije vplivajo na otrokovo samozaznavanje?

Občinstvo pogosto ne ve, kdaj so bile fotografije urejene. To negativno vpliva na samooceno uporabnikov, ki se po ogledu urejenih fotografij počutijo grde in nepopolne. Pri najstnikih lahko pretirana uporaba družbenih omrežij povzroči nezadovoljstvo in občutek neprimernosti in osamljenosti.

Ta lepotni ideal tudi premakne k nerealnim slikam. Ko imajo otroci manj stika z resničnostjo, z naravnim, resničnim in verodostojnim, lahko spremenjeni videz postopoma začnejo dojemati kot normo in bodo naredili vse, da dosežejo enak videz.

Ali se otroci predstavljajo res taki kot so na slikah objavljenih na družbenih omrežjih?

Nekateri uporabljajo internet, da pokažejo, kaj radi počnejo, drugi pa se pretvarjajo, da so nekdo drug. Takšno pretvarjanje lahko posredno povzroči tesnobo in povzroči notranji konflikt ter zavračanje samega sebe. Če se predstavljate samo z urejenimi slikami, ste pod pritiskom in razočarani nad izkušnjami, ki se ne ujemajo s to spremenjeno sliko o sebi.

Ali otroci dojemajo svoje dejanske izkušnje ali pa samo izbirajo ozadje?

Mladim so selfiji zabavni. Vendar pogosto ne izkusijo trenutka in se raje osredotočijo na dobro fotografiranje. Na primer, med sprehodom po mestu se bo najstnik bolj osredotočil na tisto, kar bo naredilo dobro kompozicijo za njegovo fotografijo, ne pa na sam sprehod ali družbo svojih prijateljev. Bili so celo primeri zasvojenosti mladih s slikanjem in objavljanjem sebkov.

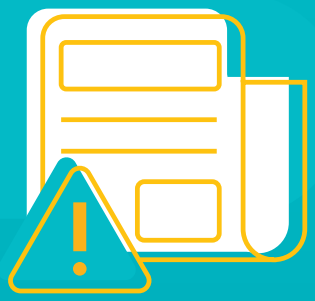
Kaj povzroča strah pred zamujeno priložnostjo (FOMO) pri otrocih?

Strah pred zamujeno priložnostjo (FOMO) je strah, da bi lahko zamudili kaj zanimivega ali pomembnega, na primer koncert, praznovanje prijatelja, potovanje, športni trening itd. To lahko povzroči tesnobo in druge negativne občutke. Podobne občutke je lahko in jih je povzročil tudi strah uporabnika / otroka, da bi zamudili najnovejše trače na družbenih omrežjih. Zaradi tega strahu je otrok živčen in prepogosto preverja svojo napravo.

Ali otroci tvegajo komunikacijsko preobremenitev?

"Biti vedno na voljo" na več različnih platformah mladostnikom pogosto daje hrepeneči občutek vključenosti v skupnost in biti na vrhu stvari, vendar je lahko zelo psihično naporno. Pogosto obsesivno preverijo svoje pametne telefone, kar jih odvrne, preobremeni z informacijami in postavi pod pritisk. Povprečen študent bo pametni telefon preverjal vsake tri minute. Raven pritiska pa je odvisna tudi od števila in narave platform, ki jim sledijo.

Odrasli lahko otrokom pomagajo doseči notranje ravnovesje, povečati samozavest in razviti svoje vrstniške sposobnosti, tako da imajo dovolj dobrih prijateljev brez povezave in lahko najdejo smiseln način preživljanja prostega časa. Če ima otrok večkrat spore in težave z družino in prijatelji, bo potreboval zaupne nasvete, po možnosti strokovno pomoč psihologa.



Dezinformacije, potegavščine in lažne novice

potegavščina | dezinformacija | lažne novice | obveščevalne vojne | potrditvena pristranskost | zarota | dezinformacijski mediji proti tradicionalnim medijem | analitične spretnosti

Teme zajete v tem poglavju:

V čem se napačne informacije razlikujejo od dezinformacij?
Kdo ustvarja dezinformacije in zakaj?
Kaj so dezinformacijski mediji?
Katere informacije se širijo hitreje in zakaj?
Kaj je pristranskost potrditve?
Kako naš um poskuša najti odgovore na neznana vprašanja?
Kaj so potegavščine?
Kakšne oblike imajo dezinformacije in potegavščine?
Kako lahko prepoznate lažne novice?
Kako se zaščitite pred potegavščinami?
Kako lahko ustavite lažne novice? Kje lahko preverite novice?
Kaj storiti s ponarejenimi novicami? Kakšno grožnjo predstavljajo potegavščine?

V čem se napačne informacije razlikujejo od dezinformacij?

Ta dva pojma se pogosto uporabljata zamenljivo, vendar nimata enakega pomena. V obeh primerih se širijo napačne ali izmišljene informacije, toda v primeru napačnih informacij je oseba, ki podatke širi, iskreno prepričana ali ne ve, ali so informacije resnične, in ne namerava povzročiti škode. Tudi dezinformacije niso pravilne, toda oseba, ki jih je ustvarila in razširja, to ve in kljub temu zavestno še naprej to počne z namenom povzročiti škodo.

Dezinformacije so lahko tudi informacije, ki so v bistvu resnične, vendar se širijo brez kakršnega koli konteksta - tako da en portal ali profil ustvari popačen pogled na zadevano težavo. Posamezne primere lahko izberemo in naberemo na enem mestu. Dezinformacije lahko vodijo do napačnih sklepov ali odločitev. Je eno od orodij, ki se uporabljajo v tako imenovani psihološki vojni.

Kdo ustvarja dezinformacije in zakaj?

Dezinformacije v nelojalni konkurenci pogosto uporabljajo politične stranke v obveščevalnih vojnah med različnimi političnimi sistemi ali sovražnimi državami. Dezinformacije so lahko tudi del vojaških spopadov. Cilj dezinformacij je prevarati nasprotnika in ga prepričati, kar avtor dezinformacij meni, da je koristno. Cilj je pogosto ustvariti vzdušje kaosa in dvoma o tem, kaj je res, ter tako zmanjšati zaupanje javnosti v državo ali druge organe. Nekateri ustvarjalci dezinformacij si bodo morda prizadevali motnje v delovanju določenega sistema.

Tudi posel je lahko eden od razlogov - trg je lačen informacij, ki niso predstavljene v tradicionalnih medijih. Vendar glavni razlog, zakaj taka vprašanja niso zajeta, ni poskus zadrževanja informacij, temveč dejstvo, da so informacije neresnične, slabe kakovosti ali jih ni mogoče preveriti. Če zapolnijo to praznino, lahko mediji za dezinformacije zberejo veliko sledilcev in ustvarijo znaten prihodek od oglaševanja.

Kaj so dezinformacijski mediji?

Mediji za dezinformacije se osredotočajo na razširjanje dezinformacij. Včasih jih imenujemo tudi zarotniški mediji. Njihov glavni cilj je širjenje teorij zarote, prevara ali nepreverjanje in manipuliranje informacij. Običajno potiskajo eno glavno temo - zlasti te trenutno vključujejo priseljence, informacije proti COVID-19 in proti EU.

Kar zadeva predstavitev, si prizadevajo posnemati tradicionalne medije, mnogi pa objavljajo tudi prave novice. Medtem ko tradicionalni mediji prikazujejo svet bolj zapleteno in celovito, se mediji za dezinformacije osredotočajo na izbrane teme, ki jih predstavljajo na način, ki jim omogoča, da negativno vplivajo na misli bralcev. Pogosto objavljajo zgodbe iz drugih virov ali jih prevajajo z bolj šokantnimi naslovi. Ko opravljajo razgovore, običajno intervjuvajo ljudi, ki imajo enaka stališča in podpirajo iste cilje. Ne zanimajo jih etika ali zaupanje. Njihov cilj ni obveščanje, temveč nadzor javnih organov ali vodenje kampanje proti demokratičnemu sistemu. Pogosto pride do namernih napak ali delnega zadrževanja informacij in predstavitve izven konteksta.

Velik del medijev za dezinformacije niso le portali z novicami ampak tudi mediji, namenjeni zdravju.

Eden najbolj priljubljenih člankov na češkem internetu je bil "Vodikov peroksid - zdravilo proti raku", na Slovaškem pa "Skrivnost je pokazala: rak ni bolezen, temveč posel. Tako se ga lahko znebite. "

Poleg običajnih medijev so mediji za dezinformacije dejavni skoraj v vseh državah sveta. Kljub tveganju, ki ga predstavljajo, bi jih morali poznati, da se jim lahko izognemo in prenehamo širiti novice, ki jih objavljajo.

Katere informacije se širijo hitreje in zakaj?

Raziskava[18], ki jo je marca 2018 objavila revija Science, je potrdila, da se laži po internetu širijo veliko hitreje kot resnica. Avtorja sta primerjala, kako se informacije širijo na Twitterju, in ugotovila, da se lažne govorice širijo šestkrat hitreje. Ljudje radi delijo in širijo informacije s kančkom občutka. To avtorju posreduje socialni status, kar kaže na to, da je "seznanjen" ali da ima dostop do edinstvenih "notranjih" informacij.

Na številna vprašanja je mogoče zlahka odgovoriti, resnica pa je pogosto manj privlačna in bolj dolgočasna kot laži. Preverjene informacije, ki pojasnjujejo ali zavračajo laži, se širijo veliko počasneje in pogosto niti ne dosežejo ljudi, ki so prebrali izvirne lažne novice. Posledično je pogosto zelo težko, če ne celo nemogoče, popraviti škodo, ki jo povzročajo tisti, ki širijo dezinformacije. Lažne informacije so pogosto populistične in se hitro širijo po internetu tudi zaradi pomanjkanja zaupanja v uradne vire.

Ljudje imajo tudi raje informacije, ki se ujemajo z njihovimi lastnimi pogledi in obstoječimi mnenji, kar ustvarja tako imenovana potrditvena pristranskost.

Kaj je potrditvena pristranskost?

Pristranskost potrditve je naraven način razmišljanja, napaka v presoji. Nagnjenost k favoriziranju, iskanju in priklicu informacij potrjuje naša obstoječa prepričanja ali hipoteze. Ljudje ponavadi posvečajo veliko manj pozornosti alternativnim pogledom.

Poskusi so pokazali, da ljudje ne iščejo informacij, temveč mnenja, ki potrjujejo, kaj verjamejo - potrditev svojih idej. Pristranskost potrditve je še močnejša pri čustveno pomembnih temah in globoko zakoreninjenih prepričanjih. Ljudje se ponavadi osredotočajo samo na eno možnost in ne upoštevajo drugih možnosti. Zaradi pristranskosti potrditve smo pogosto prepričani, da so lažne informacije resnične, in jih v dobri veri razširjamo kot resnico. Razširjamo napačne informacije. In ker smo prepričani, da so novice resnične, ne vidimo, zakaj bi jih morali preverjati. Vedeti o pristranskosti potrditve in nenehno dvomiti, ali so dejstva resnična, in jih preverjati, je zato zelo pomembno. Le z nenehnim preverjanjem in primerjanjem informacij z zanesljivimi viri se lahko izognemo širjenju lažnih novic.

18 https://science.sciencemag.org/content/359/6380/1146

Kako naš um poskuša najti odgovore na neznana vprašanja?

Pri presojanju imamo raje enostavnejše in lažje rešitve kot tiste, ki zahtevajo več razmišljanja in truda. Preleni smo, da bi brali bolj zapletene informacije.

Ko bomo postavili vprašanje, na katerega ne vemo odgovora, ga bo naš um preoblikoval v nekaj, kar je lažje oceniti. V postopku ocenjevanja se spominjamo situacij, ki si jih je najlažje zapomniti. Poskusite odgovoriti na to vprašanje: Katero delo je nevarnejše - policist ali ribič? Večina ljudi bo verjetno rekla policist, ker se bodo spomnili vseh akcijskih filmov, v katerih so policisti vpleteni v orožje. V resnici pa bi morali na vprašanje odgovoriti tako, da bi razmislili, v koliko nevarnih situacijah smo videli policista in v koliko ribičih. Po statističnih podatkih je biti ribič eno najbolj tveganih delovnih mest na svetu. Več o tem, kako deluje naš um, in napakah v presoji lahko izveste v knjigi Daniela Kahnemana Thinking, Fast and Slow.

Gordon Pennycook in David Rand, strokovnjaka, ki preučujeta človeški um, sta potrdila, da naša težnja, da verjamemo lažnim novicam, temelji na pomanjkanju analitičnih veščin.

Kaj so potegavščine?

Prevara je novica z lažno ali kako drugače nepravilno vsebino (tj. dezinformacije), katere namen je vzbuditi negativna čustva in prejemnika manipulirati pri posredovanju in razširjanju sporočila. Prevara je posebna vrsta dezinformacij, ki nas spodbujajo k širjenju. Z manipulacijo se lahko širijo prevare in prepričajo, da je to, kar širijo, resnično in v bistvu povzročajo napačne informacije. Avtor se pogosto predstavlja kot zaupanja vreden vir (podjetje, državni organ ali napačno uporablja njihovo ime, npr. "Ameriški znanstveniki so našli" ali "po Interpolu") in opozarja na katastrofalne posledice izmišljenega dogodka. Pri tem uporabljajo trditve, ki ne temeljijo na znanstvenih podatkih ali kakršnih koli preverljivih dejstvih. Cilj ustvarjalca potegavščin je razširiti strah, tesnobo in občutek nevarnosti ter prisiliti žrtev, da deluje brez razmišljanja.

Kakšne oblike imajo dezinformacije in potegavščine?

Dezinformacije in potegavščine imajo lahko več oblik - spodaj najdete primere najpogostejših.

- **Prevara, privlačna za vaše sočutje** — tovrstna potegavščina privlači prejemnikovo sočutje in obljublja namišljeno nagrado, rešena življenja ali druge koristi v zameno za širjenje.
- **Lažne novice in dezinformacije** — z uporabo spremenjenih, zvitih ali izmišljenih informacij je njihov namen manipulirati z javnim mnenjem, najpogosteje s političnimi ali ideološkimi cilji. Družbena omrežja, ki ne urejajo podobne vsebine, še povečujejo moč ponarejenih novic in dezinformacij, ker jih zaradi zelo virusne narave algoritmi omrežij še hitreje širijo.
- **Izmišljeni citati znanih ljudi** — avtor informacije širi kot citat (izjavo) nekoga, ki je v tej državi (kraju) znan in mu zaupa in ga pogosto obravnavajo kot mnenjskega voditelja. Fotografiji te osebe se pogosto doda članek ali informacija, da je videti bolj zaupanja vreden. To je lahko zvezdnica, ki je starejša in ni (zelo) aktivna na družbenih omrežjih, zaradi česar je novic težko preveriti.
- **Dezinformacije, ki jih širijo znane osebnosti** — včasih lažne novice širijo znane osebnosti s številnimi navijači, ki niso strokovnjaki za določeno temo. To je lahko pevec, politik ali znani zdravnik. Na primer, laži o COVID-19 je razširjal znani zdravnik, specializiran za medicino življenjskega sloga. Donald Trump je predlagal uporabo razkužil kot sredstva COVID-19, kar naj bi povzročilo en primer zastrupitve.

- **Tehnološke potegavščine** — večina se širi po e-pošti in opozarja na namišljen virus ali tehnološko grožnjo. Pogosto vas bodo prosili, da naredite nekaj, kar bo poškodovalo vašo napravo, npr. zahtevali bodo, da izbrišete določeno datoteko operacijskega sistema (ki je standardni del sistema) in trdijo, da je datoteka, če jo najdete v svoji napravi, že okužena z virusom.
- **Šale, potegavščine, ustvarjene ob posebnih priložnostih, ko se jim zdi družbeno sprejemljivo** — večina teh je ustvarjena kot prvoaprilske potegavščine ali praktične šale, katerih cilj je prelisičiti ljudi. Včasih pa bodo ljudje informacijam verjeli in jih še naprej širili. Ta oblika prevar je v bistvu neškodljiva.
- **Verižna pisma** — v preteklosti so bila razširjena po pošti, zdaj pa so se preselila na internet. Prosili vas bodo, da še naprej širite sporočilo in izkoriščate človeške vraževerje. Lahko denimo trdijo, da če sporočila ne pošljete vsaj petim ljudem, boste nesrečni.
- **Spremenjene ali stare fotografije (videoposnetki)** — pri ustvarjanju dezinformacij se pogosto uporabljajo stare fotografije, ki so resnične, vendar vezane na povsem drugačen dogodek. Včasih se lahko fotografija ali njeni deli spremenijo in tako ustvarijo ponaredek. Avtor lahko doda tudi besedilo, sestavljeno iz člankov, objavljenih na spornih spletnih mestih, ki redno širijo potegavščine. Tipičen primer tega je fotografija ladje z imenom Vlora. Fotografija je bila posneta leta 1991, vendar je bila uporabljena v povezavi s priseljensko krizo leta 2015.

Slike, ki jih je mogoče javno iskati preko Googla

Dodajanje zavajajočega besedila stari fotografiji je zelo preprosta in učinkovita metoda zavajanja ljudi. Podobe niti ni treba spreminjati, saj je videti sama po sebi dovolj zaupanja vredna.

Kako lahko prepoznate lažne novice?

Obstaja nekaj tipičnih znakov, ki vam lahko pomagajo prepoznati lažne novice. Pogosto izvirajo iz dvomljivih ali kontroverznih virov ali pa sploh ni naveden noben vir. Na spletnih mestih, ki širijo lažne novice, običajno ni nobenih kontaktnih podatkov za avtorja ali uredništvo, slovnica in slog pa sta pogosto slaba.

Vendar se včasih takšna besedila in spletna mesta lahko zdijo zelo profesionalna. V tem primeru je edini način, da razkrijemo lažno naravo novic, stalno preverjanje in navzkrižno preverjanje informacij z uporabo več zanesljivih virov. Zanesljivi viri so običajno osrednji mediji, ki delujejo transparentno, preverjajo svoja dejstva in upoštevajo etični kodeks. Dober vir so lahko tudi neodvisne (mednarodne) organizacije, nevladne institucije, univerze ali znanstveni inštituti demokratičnih držav.

Članke, ki ne določajo datuma in kraja dogodka, ki ga opisujejo, je treba obravnavati tudi kot sumljive. Paziti bi morali tudi glede objav na politično občutljive teme, ki spodbujajo senzacionalizem in polemike.

Bolj ko je novica pretresljiva, večja je verjetnost, da gre za dezinformacije. Ne pozabimo, da število všečkov in delitev nima nobene zveze z verodostojnostjo in zaupanjem v novico.

Kako se lahko zaščitite pred potegavščinami? Kako lahko ustavite lažne novice?

Vsakdo bi se moral naučiti razlikovati med resničnimi in lažnimi novicami. To ni samo zato, da bi lahko vedeli, kaj je res, ampak tudi zato, da bi se izognili širjenju dezinformacij. Naslednji koraki vam lahko pomagajo prepoznati ponarejene novice in preprečiti njihovo širjenje.

- **Preverite vir —** preverite namen spletnega mesta in objavljene kontaktne podatke - preverite jih z iskalnikom. Je vir osrednji medij ali ste ga našli med mediji za dezinformacije?
- **Preverite avtorja —** poiščite informacije o avtorju. Je zaupanja vreden? S katerimi temami se običajno ukvarja? Je to dejanska oseba ali izmišljena oseba?
- **Preverite datum —** je vključen datum? Ali gre za nov ali star članek? Bodite previdni pri starih novicah. Samo to, da je veljalo v preteklosti, še ne pomeni, da je še danes pomembno. Znanstveno znanje se je na tem področju morda zelo razvilo.
- **Pomislite na svojo pristranskost —** kakšna so vaša prepričanja? Ali novice podpirajo vaše stališče? Bodite previdni pri pristranskosti potrditve.
- **Preberite celotno zgodbo, ne samo naslova —** naslov je morda videti šokantno, da vas spodbudi, da kliknete nanj (vaba). Kaj je celotna zgodba? Ali vas naslov zavaja samo zato, da pritegne vašo pozornost?
- **Preverite kakovost vira —** ali članek vsebuje povezave do drugih virov? Preverite, ali navedeni viri niso v nasprotju s tem, kar piše v članku.
- **Je to le šala —** se zdi vsebina čudna? Pomislite, ali je to lahko samo satira ali ironija. Preverite spletno stran in avtorja, da se prepričate, da to ni le šala.
- **Vprašajte strokovnjaka —** preverite pri strokovnjaku, svetovalcu ali spletnem mestu za preverjanje dejstev.

Kje lahko preverite novice?

Če želite preveriti, ali je članek z novico resničen ali ne, lahko uporabite spletna mesta, specializirana za razkritje prevara. Na primer: snopes.com ali stopfake.org, FactCheck.org, hoax.cz.

Ko objava oziroma članek vsebuje sliko, lahko s pomočjo obratnega iskanje slik na Google reverse image search[19] preverite, ali je slika resnična.

Kaj storiti z lažnimim novicami?

Če ugotovite, da je članek lažen, ga ne širite. Če poznate avtorja sporočila (pogosto prihaja od ljudi, ki jih poznate), jih obvestite, da so novice ponarejene. Družbena omrežja ponujajo orodja, s katerimi lahko poročate o lažnih novicah, potegavščinah in dezinformacijah, objavljenih na družbenih omrežjih. Tik ob objavi najdete možnost "Prijavi objavo" in nato med razpoložljivimi možnostmi izberite "Lažne novice".

Kakšno grožnjo predstavljajo potegavščine?

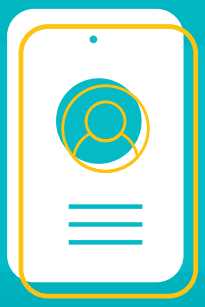
Prevara in dezinformacije niso zgolj sestavljeni podatki, ki jih lahko pošljete ali poveste komu. Ni opravičilo, če je vaša motivacija za razširjanje laži le zabava ali igranje praktičnih šal. Dezinformacije lahko povzročajo veliko škodo tako na lastnini kot na zdravju. Če menite, da nekatere bizarne informacije ali nekdo pridobi vaše občutljive podatke (npr. številko vaše kreditne kartice) na družbenem omrežju z razširjanjem potegavščine, lahko zaradi prevare izgubite denar.

Zelo nevaren pojav je tudi širjenje potegavščin, povezanih z zdravjem. Če verjamete v prevaro in zavrnete zdravila ali cepljenje, lahko to ne samo škoduje vašemu lastnemu zdravju, temveč ogroža družbo širše.

In ne pozabimo, da je lahko ustvarjanje in razširjanje prevar in dezinformacij tudi kaznivo dejanje. Morda ste v družabnih omrežjih naleteli na informacije, da policija išče avtorje potegavščin. Uporabnike družabnih omrežij lahko na primer prosijo za pomoč pri prepoznavanju glasu na posnetku.

19 https://images.google.com

VIR: https://www.ifla.org/publications/node/11174
PODROBEN PRIROČNIK: https://unesdoc.unesco.org/ark:/48223/pf0000265552



Digitalna identiteta in zasebnost

oblak | digitalno državljanstvo | digitalni odtis | e-poštni račun | lokacija

Teme zajete v tem poglavju:

Kaj je digitalna identiteta?
Kaj je digitalni odtis in kakšne vrste digitalnih odtisov obstajajo?
Ali lahko odstranite svoj digitalni odtis?
Kako lahko ugotovite, kje in katere digitalne stopinje so vam ostale?
Kaj je digitalno državljanstvo?
Kaj je digitalni podpis?
Ali bomo v prihodnosti volili po spletu?

Kaj je digitalna identiteta?

Na internetu lahko vsak ustvari v bistvu neomejeno število digitalnih identitet. Nekateri od njih se lahko v mnogih pogledih ujemajo z dejansko osebo - npr. Facebook ali Instagram profil - vendar se lahko tudi bistveno razlikujejo - igralski profil v Fortnite ali Steam, ki se skriva za izmišljenim vzdevkom. Nekatere identitete so lahko namerno drugačne, da preprečijo izsledite prvotnega lastnika - na primer ponarejeno e-poštno sporočilo za naročanje na novice.

Ključ digitalne identitete je ugled. Oseba gradi svoj ugled s svojim vedenjem in interakcijami z drugimi uporabniki na določeni platformi. Če je njihov ugled dober, so bolj zaupanja vredni in lahko sklepajo pogodbe in sporazume na spletu ali pridobijo boljše pogoje. Primer tega je uporabnik, ki ponuja svoje stanovanje za kratkoročni najem (npr. Airbnb). Če je uporabnik zanesljiv, je stanovanje vedno čisto in so kupci zadovoljni, bodo od svojih strank dobili dobro oceno. Če je teh ocen veliko, to ustvarja njihov ugled in lahko s spletno platformo pridobijo prednosti in privabijo boljše stranke. Enako velja za stranke. Če so znani po tem, da puščajo nered ali se poskušajo izogniti plačilu, se njihov ugled poslabša in skupaj s tem možnosti, da najdejo nastanitev.

Kaj je digitalni odtis in kakšne vrste digitalnih odtisov obstajajo?

Če imate e-poštni račun, če uporabljate družabno omrežje, če igrate spletne igre ali samo brskate po različnih razvedrilnih vsebinah, novicah in drugih spletnih mestih, ustvarjate lastne digitalne odtise. To ne pomeni nujno, da nekdo pozna vašo identiteto tudi v resničnem svetu. Digitalna identiteta je anonimen odraz vašega vedenja v digitalnem svetu, ki lahko v povezavi z drugimi informacijami - digitalnimi odtisi - pripelje do določene osebe.

Podatke, ki tvorijo digitalni odtis, je mogoče zagotoviti **aktivno** ali **pasivno**:

- **Pasivni digitalni odtis** sestavljajo informacije, ki jih uporabnik nevede pusti v spletnem prostoru in ki niso neposredno vidne. Primer pasivnega digitalnega odtisa je lahko vrsta brskalnika, model naprave, jezikovne nastavitve, operacijski sistem ali naslov IP, shranjeni v zbirki podatkov internetnega ponudnika ali na strežnikih ponudnika, katerega storitev uporabljate. Naslov IP pomaga prepoznati približno lokacijo ali ponudnika interneta, vendar je lahko nezanesljiv, saj ga je mogoče namenoma prikriti (z uporabo navideznega zasebnega omrežja ali VPN).
- **Aktivni digitalni odtis** vključuje vse podatke, ki so zavestno posredovani in objavljeni na internetu. Če pošljete e-poštno sporočilo, objavite spletni dnevnik, na primer fotografijo / komentar, objavite videoposnetek ali besedilo na družbeno omrežje ali pošljete sporočilo, postanejo te in podobne informacije vaš aktivni digitalni odtis. Zavedati se morate tudi, da veliki ponudniki spletnih storitev, kot sta Google in Facebook, uporabljajo svojo kodo na številnih spletnih mestih, da lastniku spletnega mesta pomagajo pri analizi njihovih obiskovalcev. Takšni podatki prav tako pomagajo tem podjetjem zbrati širok spekter digitalnih odtisov, da dobijo podrobnejšo sliko uporabnikovega spletnega vedenja.

Ali se določen odtis šteje za aktivnega ali pasivnega, je pogosto odvisno od uporabniške tehnične ravni. Bolj izkušen uporabnik se zaveda, da je njegovo vedenje v spletu mogoče spremljati, in se zavestno izogiba nekaterim spletnim mestom ali spletnim storitvam ali uporablja orodja za preprečevanje takšnega spremljanja.

Ali lahko odstranite svoj digitalni odtis?

Digitalni odtis je stalen in neizbrisen del našega spletnega obstoja. V skladu s Splošno uredbo o varstvu podatkov[20] (GDPR), ima vsak državljan EU "pravico biti pozabljen", vendar je to precej dolgotrajen postopek. Poleg tega, čeprav na koncu postopka določena storitev ali ponudnik ni lastnik nobenih uporabnikovih podatkov, se nekateri podatki lahko še vedno shranijo v drugo bazo podatkov ali so del podatkovnega paketa, ki je medtem v rokah druge organizacije. Neprimerno e-poštno sporočilo ali fotografijo uporabnika lahko shranite tudi na trdem disku nekoga, ki je posnel posnetek zaslona. Torej se lahko informacije kljub izbrisu iz primarnega vira v prihodnosti znova pojavijo na internetu in postanejo breme, npr. zapletanje uporabnikovih prihodnjih prošenj za delo ali oteževanje novih odnosov.

Kako lahko ugotovite, kje in katere digitalne stopinje so vam ostale?

Zahvaljujoč obstoječi zakonodaji je to mogoče, a precej težko. V skladu z GDPR so podjetja, ki zbirajo podatke o svojih uporabnikih (to velja samo za prebivalce EU), dolžna uporabniku zagotoviti takšne podatke, če jih ta zahteva. To je eden od razlogov, zakaj velike spletne storitve ponujajo možnost - običajno na voljo v uporabniških nastavitvah, s katero lahko posameznik zahteva vse podatke, ki jih o njih shrani kateri koli ponudnik.

Kaj je digitalno državljanstvo?

Tako kot smo državljani države v resničnem svetu, postajamo tudi državljani digitalnega sveta. Estonija, Nizozemska in Britanija so le nekateri primeri evropskih držav, ki ponujajo številne vladne storitve prek spleta. To uvaja številne prednosti, kot so neprekinjena razpoložljivost storitev, čas, ki ga prihranijo državljani, ki bi sicer morali čakati na različnih lokalnih vejah oblasti, finančni prihranek države, ki bi ga sicer morala porabiti za uradnike, kot je pa tudi manj napak in neutrudnost teh avtomatiziranih sistemov. Prednosti takšnih spletnih storitev so se jasno začutile med pandemijo koronavirusa.

Ker so storitve elektronske, ljudem ni treba večkrat posredovati svojih podatkov različnim organom, saj jih lahko državni uslužbenci iščejo v centraliziranih vladnih sistemih. Storitve digitaliziranih organov poenostavljajo tudi upravne akte, kot so sprememba lastništva vozila, sprememba naslova stalnega prebivališča ali ustanovitev podjetja. Namesto da bi morali obiskati organ, počakati na vrsto in predati dokumente na okencu, lahko zdaj ljudje izpolnjujejo obrazce doma, jih podpišejo s čipom v osebni izkaznici in jih z nekaj kliki oddajo.

Seveda imata centralizacija in avtomatizacija tudi slabosti. IT sistemi so prav tako nagnjeni k napakam, včasih so lahko preobremenjeni in razpoložljivost storitev omejena. Drugo tveganje je, da takšni sistemi morda niso dovolj zaščiteni pred zunanjimi napadi ali lahko zaradi nepravilne nastavitve puščajo občutljive podatke. Primer tega je bilo masovno uhajanje podatkov 6,5 milijona izraelskih volivcev[21], ki je bil na voljo na spletu zaradi napake v aplikaciji, ki jo uporablja politična stranka.

Če ustanavljate podjetje, razmislite tudi o tem, da bi morali obdelovati podatke o strankah - torej bi morali upoštevati stroge zakonske zahteve (npr. GDPR). Zakonodaja ne določa le, kako naj se podatki zbirajo, shranjujejo in varujejo, temveč tudi uvaja stroge kazni v primeru uhajanja ali kraje podatkov.

20 https://gdpr-info.eu
21 https://www.nytimes.com/2020/02/10/world/middleeast/israeli-voters-leak.html

Kaj je (ne) digitalni podpis?

Ko so svetu vladali kralji in plemiči, so pošto zavarovali z voščenimi plombami, na katerih je bil vtis njihovega grba ali drugega prepoznavnega znaka. Če je bilo pismo naslovniku dostavljeno s polomljenim pečatom, je bilo jasno, da je nekdo pismo odprl in prebral v tranzitu, pri čemer je morda spremenil njegovo vsebino.

Podoben sistem se uporablja tudi v digitalnem svetu, kjer sporočila, e-pošta in občutljivi dokumenti nosijo tako imenovani digitalni podpis.

Pomembno: digitalni podpis ni uporabnikovo ime, napisano ali "narisano" v digitalni obliki v enem izmed grafičnih urejevalnikov ali zapisan v urejevalniku besedil (npr. Word) ali celo optično prebran lastnoročni podpis. Če bi uporabnik samo risal / napisal / optično prebral podpis, bi ga napadalec zlahka posnemal in v njegovem imenu podpisal pogodbe ali dokumente ter ukradel njihovo identiteto.

Pravi digitalni podpis je matematična shema za preverjanje pristnosti dokumentov in sporočil. Digitalni podpis tudi zagotavlja, da podatki (dokumenti, sporočila itd.) izvirajo od določenega uporabnika in niso bili spremenjeni med prenosom (oziroma pokaže, da jih je nekdo spreminjal), podobno kot v preteklosti voščen pečat.

Digitalni podpis (njegov šifrirni mehanizem) je sestavljen iz dveh komponent:

- **zasebni ključ,** ki je skriven in znan samo uporabniku,
- **javni ključ,** ki je javno dostopen, a hkrati seznanjen z zasebnim ključem uporabnika.

Primer: Alice bi rada digitalno in varno podpisala svoje sporočilo, kar lahko stori tako, da ga šifrira s svojim zasebnim (skrivnim) ključem. Bob (ali kdorkoli drug), ki želi prebrati sporočilo, lahko z Aliceinim javnim ključem (v paru z njenim zasebnim ključem) preveri, ali sporočilo prihaja od Alice. Ker je zasebni ključ znan le Alice, nihče drug ne more podpisati dokumenta tako, kot lahko ona, zato je Bob lahko prepričan, da sporočilo izvira od Alice in da ga ni nihče spremenil med prenosom.

Seveda to deluje tudi obratno. Če Bob šifrira svoje sporočilo z Aliceinim javnim ključem, bo le Alice lahko odprla in prebrala sporočilo. To zagotavlja, da samo ta dva posameznika poznata vsebino sporočila in da nihče med prehodom ni prestregel ali spremenil njune komunikacije.

Ta matematična shema je tesno povezana s tako imenovanim asimetričnim šifriranjem — koncept je razložen v video posnetkih Kaj je asimetrično šifriranje[22] in Kaj je digitalni podpis[23].

22 https://youtu.be/AQDCe585Lnc
23 https://youtu.be/VIcBpRpiBoc

Ali bomo v prihodnosti volili na spletu?

Eno od področij, ki se digitalizaciji še vedno upira, je postopek glasovanja. Čeprav se na prvi pogled zdi jasen kandidat za spletno izvedbo, možne prednosti v obliki večje udeležbe volivcev ali "lažjega" postopka glasovanja pomenijo več resnih tveganj, zaradi katerih je papirna alternativa še vedno varnejša možnost.

Fizično glasovanje je hkrati pregledno, brezplačno in tajno. Volivec mora obiskati volišče blizu svojega doma, izpolniti glasovnico za v volilni kabini in jo spraviti v volilno skrinjico. Vsa ključna dejanja izvaja volivec pod nadzorom volilne komisije, vendar jih še vedno skriva v volilni kabini, tako da nihče ne vidi, katero stranko ali kandidata je izbral. V primeru dvoma se lahko glasovi preštejejo, da se preveri pravilnost rezultatov.

Elektronsko glasovanje bi moralo zagotoviti vse te lastnosti (brezplačno, tajno, preverljivo), kar do zdaj ostaja nerešen problem. Na primer, brez nadzora volilne komisije je težko zagotoviti, da se glas odda prosto, na skrivaj in ne pod prisilo. Če volivec odda svoj glas doma ali nekje v javnosti, lahko nekdo drug vpliva nanje.

Brez nadzora volilne komisije je tudi težko preveriti, pod kakšnimi pogoji in v kakšnem stanju je oseba glasovala. Lahko so na primer pod vplivom psihoaktivne snovi. To jih ne izključuje pri glasovanju, vendar pa je potrebna registracija pri volilnem odboru na volišču, saj gre za psihološko oviro za preprečevanje takšnega vedenja.

Spletne volitve z uporabo računalnikov, mobilnih telefonov in tabličnih računalnikov ne zagotavljajo enakega obravnavanja vseh volivcev, saj nima vsak volivec v lasti naprave z dostopom do interneta, ki bi mu omogočala uporabo sistema glasovanja.

Drugo vprašanje je lahko raven zaupanja volivcev v sistem spletnega glasovanja. Številni volivci ne razumejo digitalnih sistemov in so lahko prepričani, da lahko IT osebje z rezultati manipulira, saj je takšne sisteme ustvarjalo in upravljalo.

Prav tako se moramo zavedati, da lahko digitalni napadi ogrozijo varnost elektronskega glasovanja. Obstaja več strank, ki jih zanima manipulacija z volilnimi rezultati, na primer tuji igralci, različni domači akterji (oligarhi, mafija itd.), pa tudi navadni kriminalci. Osredotočijo se lahko na ranljivosti glasovalne opreme / strežnikov, ki se uporabljajo za zbiranje in štetje glasov, in jih bodisi poskušajo narediti neuporabne bodisi preusmerijo rezultate v korist določenega kandidata / stranke. Obstaja nevarnost manipulacije z glasovi volitev tudi na papirju, vendar je to tveganje lokalizirano. Fizično napasti eno volišče je lahko lažje kot centraliziran informacijski sistem, vendar lahko napadalec na centraliziran sistem vpliva na veliko večji del rezultatov.

	Prednosti	Slabosti
Glasovanje na papirju	• preglednost zakona glasovanja • glasovi se oddajo na skrivaj • glasovi se oddajo prosto • preprosta in razumljiva pravila • preverljivi rezultati	• visoki stroški • problematična dostopnost volivcev, ki ne morejo potovati, invalidov ali volivcev, ki živijo v tujini • dolgotrajen in fizično zahteven za ročno štetje glasov, ki so lahko nagnjeni k napakam
Glasovanje na papirju	• (verjetno) višja volilna udeležba • nižji stroški organizacije voliev • boljša dostopnost volivcev • hitro štetje glasov brez napak	• dostopnost potrebne volilne opreme in programske opreme do vseh družbenih slojev • morebitno poseganje v svobodo in tajnost glasovanja • možni kibernetski napadi na informacijske sisteme • namerno prirejanje rezultatov v informacijskih sistemih

Več držav je že uvedlo elektronsko glasovanje z vsemi njegovimi prednostmi in slabostmi. Nekateri, na primer Indija in Brazilija, uporabljajo specializirano opremo za glasovanje, priključeno na internet, kljub temu pa zahtevajo, da je volivec osebno prisoten na volišču. V več primerih so strokovnjaki potrdili, da imajo te naprave ranljivosti in varnostne težave.

Estonija je šla še korak dlje in uvedla glasovanje prek interneta na daljavo: prva država na svetu, ki je to storila. Volivec se mora registrirati z uporabo svojega elektronskega osebnega dokumenta in večkrat potrditi svojo identiteto. Več informacij o elektronskih sistemih glasovanja v izbranih državah je opisanih na Wikipedija strani[24].

Elektronsko glasovanje postaja izvedljiva alternativa, zlasti po globalni pandemiji koronavirusa, saj omogoča izvedbo volitev kljub strogim pravilom o družbeni distanciranosti. Ameriško ministrstvo za domovinsko varnost pa je odločno odsvetovalo[25] glasovanje po internetu in pozvalo države, naj se izogibajo tej obliki glasovanja ali jo omejijo samo na tiste, ki drugače ne morejo oddati svojega glasu.

24 http://en.wikipedia.org/wiki/Electronic_voting

25 https://www.theguardian.com/us-news/2020/may/08/us-government-internet-voting-department-of-homeland-security

Na spletu niso vsi takšni, kot se zdijo

spletna identiteta | preverjanje identitete | lažni račun | lažni profil

Teme zajete v tem poglavju:

Kdo je kdo na internetu? Kako lahko preverite identiteto nekoga na internetu?

Kdo je kdo na internetu?

"Na internetu nihče ne ve, da si pes." Dobro znana karikatura[26] Petra Steinerja, objavljena v ameriškem tedniku The New Yorker, zelo lepo prikazuje eno od težav, s katerimi se sooča internet - preverjanje identitete.

Če nekoga spoznate po spletu, se morate pogosto zanašati na informacije, ki jih je druga oseba navedla v enem od njihovih profilov ali med neposredno komunikacijo. Vendar je lahko zelo težko, če ne celo nemogoče, preveriti njihovo identiteto.

"Na internetu nihče ne ve, da si pes", karikatura Petra Steinerja, objavljena v reviji The New Yorker.

26 https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you're_a_dog

Oglejmo si primer: na internetu me je Olivia123 dodala za svojo prijateljico. Trdi, da je stara 18, rada bere in deska na snegu ter obožuje filme in TV oddaje. V resnici je profil ustvaril 30-letni brezposelni moški, ki ne bere knjig in večino časa preživi za računalnikom.

V resničnem svetu bi lahko osebo takoj videli in ugotovili, da so nekatere njene trditve neresnične, toda na internetu so stvari bolj zapletene. Poleg tega lahko zlonamerni posameznik zlahka ustvari nov profil z drugo fotografijo, preneseno iz interneta, in si izmisli novo ime ali hobije. To se lahko ponavlja v neskončnost. Takšne lažne račune lahko uporabljajo tudi v zlonamerne ali nezakonite namene.

Kako lahko preverite identiteto nekoga na internetu?

Če nekdo poskuša stopiti v stik z vami, lahko poskusite preveriti njegovo identiteto na več načinov:

Najprej lahko uporabite razpoložljivo ime in jih poiščete z Googlovim iskanjem. Nekateri rezultati vas lahko obvestijo, kje ta oseba živi, kam hodi v šolo ter ali dela na območju ali regiji, ki jo je navedla v svojem profilu.

Če Google na družbenem omrežju najde profile z ustreznim imenom, preverite podatke, ki jih je dala ta oseba. Nekateri zunanji znaki računa lahko nakazujejo tudi, da je račun ponarejen - npr. zelo malo prijateljev, nobenih fotografij ali selfijev, na katerih ni drugih ljudi.

Prav tako bodite previdni, če njihov profil vsebuje vsebino, ki se zdi preveč dobra, da bi bila resnična. Fotografije morate natančno preučiti in se osredotočiti na vse podrobnosti v ozadju.

Enako uporaben je uporabnikov e-poštni naslov, vezan na njegove račune v družbenih omrežjih, kot so TikTok, Snapchat, Instagram, Facebook, Twitter, Reddit in drugi. Če prevarant pri takšnih podrobnostih ni previden, lahko na posameznih spletnih mestih navede različne ali celo nasprotujoče si informacije.

Nekatere storitve pa bodo uporabniško ime razkrile šele, ko jim pošljete sporočilo ali se drugače obrnete nanje. Če ste osebo že dodali za svojega "prijatelja", natančno preglejte njen profil. Upoštevajte, kdaj je bil profil ustvarjen, ali se zagotovljeni podatki ujemajo s tem, kar oseba trdi, in s tem, kar je v preteklosti delila, kateri jezik je uporabljala in kako je komunicirala z drugimi uporabniki.

Varnost brskalnika

piškotki | temni splet | globoki splet | zgodovina brskanja | varno brskanje | način brez beleženja zgodovine | površinski splet | napad s posrednikom

Teme zajete v tem poglavju:

Kako lahko povečate varnost brskalnika?

Kaj je zgodovina brskanja?

Ali anonimno brskate v načinu brez beleženja zgodovine?

Kako lahko opazite ponarejena ali nevarna spletna mesta?

Kaj storiti, če odprete nevarno spletno mesto?

Katere so najpogostejše oblike napadov brskalnika?

Kateri del spleta lahko najdete s pomočjo iskalnika?

Kako lahko povečate varnost brskalnika?

Ena izmed prvih stvari, ki jo lahko naredite za povečanje varnosti, je uporaba prepoznanega in posodobljenega brskalnika. Upoštevajte, da je na računalnik mogoče namestiti več brskalnikov in da morate pred uporabo posodobiti vsakega od njih.

Številni priljubljeni brskalniki ponujajo možnost "varnega brskanja", ki uporabnika ščiti pred napadi z lažnim predstavljanjem (goljufivi poskusi kraje uporabniških imen, gesel in drugih občutljivih podatkov) in jih opozori, če poskušajo obiskati sumljiva ali spletna mesta, za katera je znano, da širijo zlonamerno programsko opremo (str. 73). Če je mogoče, vključite možnost varnega brskanja pod "nastavitvami".

Kaj je zgodovina brskanja?

Po namestitvi brskalniki samodejno zbirajo zgodovino brskanja. To je uporabna funkcija, če se želite vrniti na spletno mesto, ki ste ga že obiskali, vendar se ne spomnite njegovega imena. Po drugi strani pa je tudi vir informacij o uporabnikovih navadah, ki so pomembne tako za proizvajalca brskalnikov kot za digitalne velikane, kot sta Facebook in Google. Če se takšne informacije znajdejo v napačnih rokah, jih je mogoče prodati ali zlorabiti za druge podle namene (na primer izsiljevanje, če so bila obiskana neprimerna spletna mesta).

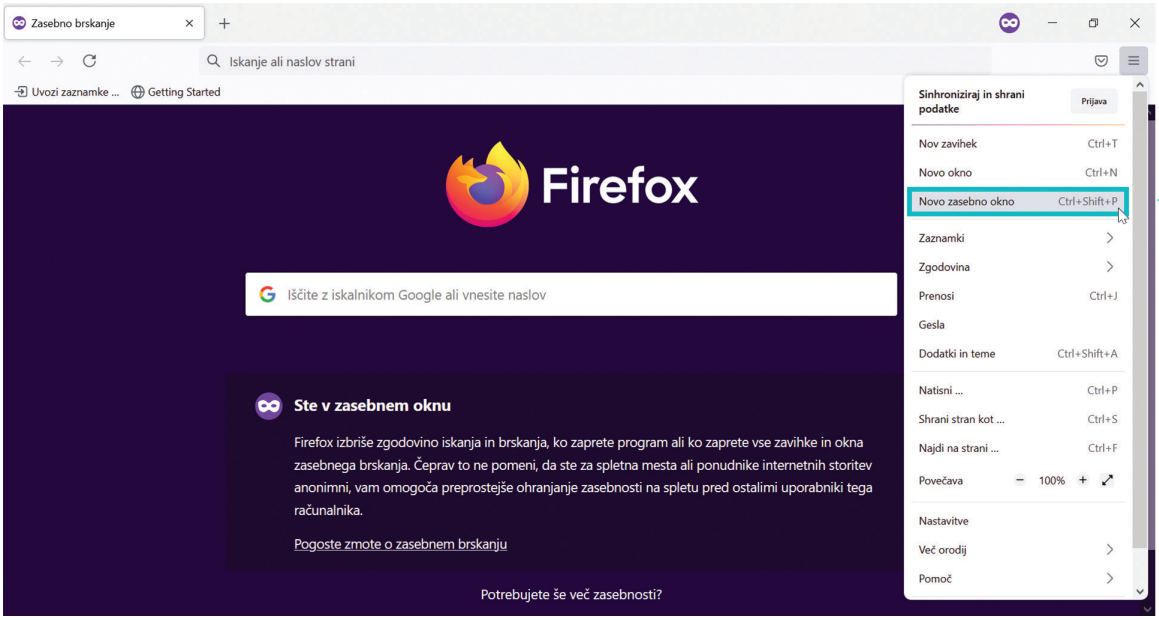
Ali način brez beleženja zgodovine pomeni, da anonimno brskate po spletu?

Če obiskujete / uporabljate spletna mesta, ki vsebujejo občutljive podatke (npr. E-pošto, socialna omrežja ali, v starejših letih, internetno bančništvo), uporabite tako imenovani "način brez beleženja zgodovine" (ang. private browsing, incognito mode). Ko je ta način omogočen, se v zgodovino brskanja prenehajo zbirati nekateri uporabniški podatki.

NAMIG:

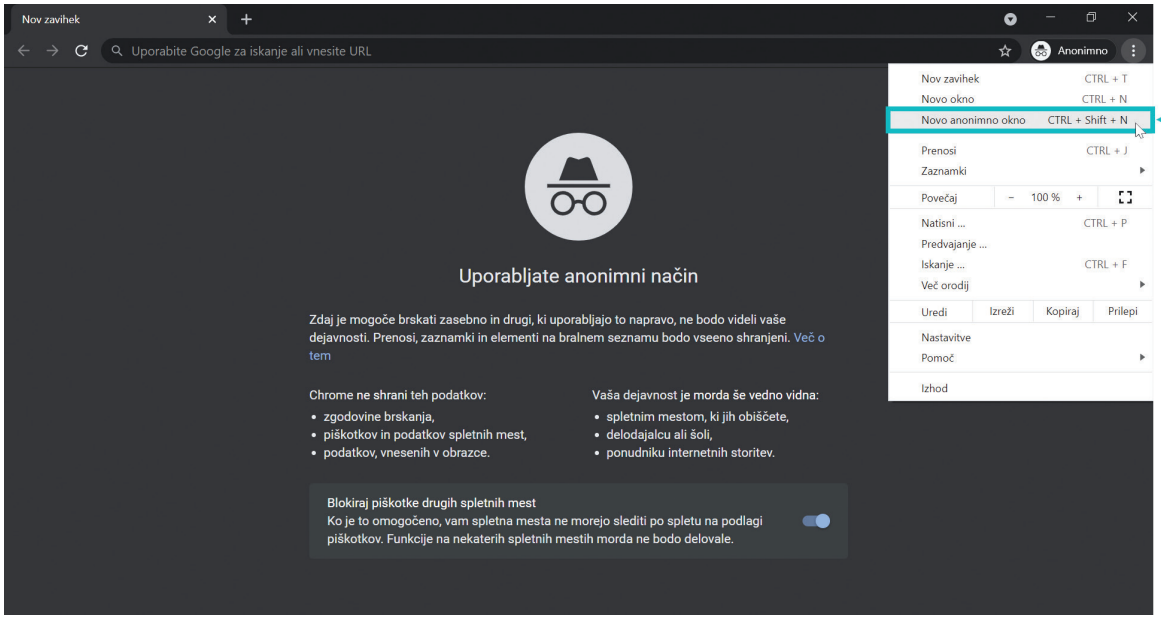
Način brez beleženja zgodovine ne pomeni, da ste popolnoma anonimni na internetu, ampak omejuje količino podatkov, ki jih zbere vaš brskalnik. Podatke o vaših obiskih posameznih spletnih mest lahko zbere proizvajalec brskalnika ali ponudnik povezave in jih uporabi za ugotavljanje vaših navad in preferenc, na podlagi katerih lahko prilagodijo oglase ali vsebino, ki vam bodo pozneje predstavljene.

Poenostavljeno bi lahko rekli, da način brez beleženja zgodovine skriva spletna mesta, ki jih obiščete, pred vsemi, ki uporabljajo isto napravo za vami. Podatki pa se še vedno digitalno beležijo in shranjujejo na drugih mestih, kot so brskalniški strežniki ali strežniki spletnih storitev (socialna omrežja, iskalniki itd.), in so tako potencialno na voljo drugim, npr. vladnim organom.



Novo zasebno okno

Mozilla Firefox



Novo anonimno okno

Google Chrome

Kako lahko prepoznate (ne) varno spletno stran?

- **https://**
  V prvi vrsti bodite pozorni na to, ali je vaša komunikacija z določeno spletno stranjo šifrirana. To lahko ugotovite tako, da pogledate naslov URL, ki naj se začne s https: //. Mala črka "s" na koncu pomeni "varno", torej varno različico protokola http. To v vrstici z naslovom URL potrjuje tudi majhen simbol ključavnice.

  Če se naslov URL začne s http: // in ni simbola ključavnice, vaša komunikacija ni varna in je nešifrirana. Vse informacije, ki jih vnesete na takšno spletno mesto, so poslane brez kakršne koli zaščite, kar potencialnemu napadalcu omogoča, da jih prestreže, prebere in ukrade.

  Za napredne uporabnike: Po kliku na zeleno ikono ključavnice si lahko ogledate dodatne informacije o spletnem mestu, na primer veljavnost njegovega digitalnega potrdila, izdajatelja potrdila ali seznam dovoljenih in blokiranih piškotkov.

  Piškotki so majhne besedilne datoteke, ki jih spletno mesto shrani v vaši napravi. S pomočjo piškotkov spletno mesto začasno shrani izbrane podatke o vaši dejavnosti in nastavitvah (npr. uporabniško ime, jezik, velikost pisave itd.) za ponovno uporabo med naslednjim obiskom. Piškotke lahko izbrišete[27] iz predpomnilnika spletnega brskalnika, vendar bo zaradi tega uporaba spletnega mesta manj priročna, saj bodo odstranjene informacije, kot so poverilnice in nastavitve, ki jih je uporabnik v preteklosti zagotavljal.

- **Jezik spletnega mesta**
  Da bi bila njihova ponarejena in / ali zlonamerna spletna mesta videti vredna zaupanja, napadalci pogosto samo kopirajo zasnovo drugega zakonitega spletnega mesta in prevedejo njegovo vsebino z brezplačnimi prevajalniki (npr. Google Translate). To pogosto vodi do izgube pomena, napak pri slovnici ali tipkarskih napak. Takšne pomanjkljivosti je na prvi pogled enostavno prepoznati in bi morale uporabnika spodbujati, da spletno mesto takoj zapusti.
- **Kontaktni podatki lastnika spletnega mesta**
  Sumljiva spletna mesta običajno ne skrbijo za stik z uporabniki. Zato običajno ni nobenih kontaktnih podatkov ali pa samo anonimni obrazec ali splošni e-poštni naslov, ki ne zagotavlja nobenega zagotovila, da vas bo nekdo dejansko poklical nazaj. Preverite tudi, kdo je registriral določeno spletno mesto, kar bi lahko opozorilo na njegovo goljufivo naravo. Takšni podatki so običajno na voljo pri storitvah, kot sta lookup.icann.org ali whois.com. Previdni bodite zlasti, če je spletno mesto pred kratkim registriral nekdo z naključnim imenom, na primer John Smith ali John Smith Industries Inc.
- **Sumljiva vsebina**
  Če spletno mesto zahteva, da vnesete veliko občutljivih podatkov, še preden sploh veste, kakšno blago ali storitve ponuja, bodite previdni. Če naletite na podoben primer, obstaja velika verjetnost, da gre za goljufijo. To velja tudi, kadar avtor spletnega mesta skuša uporabnika prestrašiti ali kako drugače prirejati, da se hitro registrira in vnese osebne podatke. Pred registracijo pri novi storitvi se morajo mlajši uporabniki (mlajši od 13 ali 16 let) posvetovati tudi s starši, ker jim Splošna uredba o varstvu podatkov ne dovoljuje, da svoje podatke posredujejo brez soglasja staršev.

27 http://www.arnes.si/pomoc-uporabnikom/brisanje-piskotkov-in-vsebine-predpomnilnika/

Kaj storiti, če odprete nevarno spletno mesto?

Če slučajno pridete do sumljivega spletnega mesta, se izogibajte kliku katerega koli predmeta na strani (gumbi, slike, povezave) in ga čim hitreje zaprite. Za dodatno varnost lahko svojo napravo - računalnik ali mobilno napravo s sistemom Android - optično preberete z ugledno varnostno programsko opremo, ki naj zazna, odpravi in odstrani vse grožnje, ki jih je uporabnik morda prenesel ob obisku takega spletnega mesta.

Katere so najpogostejše oblike napadov brskalnika?

V brskalniku lahko najpogosteje naletite na phishing napade, socialni inženiring in okužbe z zlonamerno programsko opremo.

Socialni inženiring (v primeru napadov brskalnika) je psihološka manipulacija žrtve pri odpiranju nevarnega ali ponarejenega spletnega mesta, kjer lahko napadalec iz njih pridobiva občutljive podatke, ali jih prestraši, da bodo namestili neželeno / nevarno aplikacijo ali zlonamerno kodo.

Lažno predstavljanje uporabljajo napadalci, ki se predstavljajo kot zaupanja vredno spletno mesto ali organizacija za zbiranje občutljivih podatkov. E-poštni naslov (sporočilo) ali spletno mesto napadalca je lahko videti skoraj enako sporočilom / spletnim mestom družabnega omrežja, e-poštne storitve ali spletnega mesta za spletno bančništvo ali pa se lahko pretvarja, da je ugledna e-trgovina. Za primere in teste, v katerih lahko študentje ugotovijo, ali lahko ločijo med resničnimi in lažnimi spletnimi mesti, glejte priročnik predlaganih dejavnosti.

Brskalnik lahko predstavlja pot za prenos zlonamerne programske opreme (z drugimi besedami, zlonamerne kode). Lahko se širi na različne načine, ki jih podrobneje obravnavamo v naslednjih poglavjih. Ko okužbo vnesemo prek brskalnika, se to najpogosteje zgodi prek:

1. **Zlonamerne razširitve brskalnika,** ki jih je uporabnik namestil, ne da bi vedel za njegov zlonamerni namen, zaradi pritiska napadalca ali zaradi neznanja (aplikacija se pretvarja, da ponuja zanimivo funkcionalnost ali določene funkcije ponuja brezplačno).

2. **Z obiskom zlonamernega spletnega mesta.** Na zlonamerno spletno mesto lahko pridete po kliku na povezavo, prejeto v e-poštnem sporočilu, neposrednem sporočilu, v dokumentu, na drugem spletnem mestu ali po kliku na lažni oglasni pas. Lahko se okužite, tudi na naslednje načine: zlonamerno kodo lahko samodejno prenesete, ko obiščete takšno spletno mesto in jo namestite v svojo napravo. Prav tako lahko optično prebere vašo napravo in / ali samodejno prenese drugo zlonamerno programsko opremo.

3. **Napad s posrednikom v brskalniku ang. man-in-the-browser (MITB).** Med to vrsto napada je žrtvina naprava že okužena z zlonamerno programsko opremo, ki nato omogoča napadalcu dostop do ranljivega brskalnika. Zlonamerna programska oprema lahko prestreže podatke, ki jih je uporabnik vnesel na različnih spletnih mestih, jih spremeni ali pridobi občutljive podatke (številka kreditne kartice, datum rojstva, prijavno ime, geslo itd.) in jih posreduje napadalcu. Žrtev ničesar ne sumi, ker brskalnik in spletna mesta delujeta po pričakovanjih.

Površinski, globoki, temni

temni splet | globoki splet | površinski splet

Teme zajete v tem poglavju:

Kaj je površinska mreža? Kaj je globoki splet? Kaj je temni splet? Ali se globlji deli spleta uporabljajo samo za nezakonite dejavnosti? Kako delujejo različne plasti spleta?

Površinski splet

Površinski splet sestavljajo javno dostopna spletna mesta, ki jih lahko uporabniki najdejo z uporabo internetnih iskalnikov, kot so Google, DuckDuckGo ali Bing. To je najmanjši del spleta, figurativno rečeno "vrh ledene gore".

Globoki splet

To je del interneta, "skrit pod površjem", ali če ponovno uporabimo metaforo ledene gore - del ledene gore pod vodo. Ocenjuje se, da temni splet vsebuje do 96% celotne spletne vsebine. Imenuje se globoki splet, ker gre za spletna mesta in vsebine, ki naključnim uporabnikom niso dostopne. Za njihovo iskanje ali dostop uporabnik potrebuje posebno programsko opremo, orodja ali pravice dostopa. Velik del spletnega interneta je zakonit in legitimen. To so lahko na primer elektronske knjige poročil, izobraževalne vsebine, namenjene določenemu razredu, pa tudi plačljivi odseki novičarskih portalov, interni sistemi podjetij in javnih zavodov, dostopni samo njihovim zaposlenim ali posameznim uporabnikom.

Temni splet

To predstavlja podmnožico globokega spleta in tisti del ledene gore, ki je najbolj oddaljen od površine. Iskalniki ga ne indeksirajo in deluje v temnem omrežju, torej infrastrukturi, ki operaterjem in uporabnikom temne mreže zagotavlja anonimnost. Za povezavo s temnim spletom mora uporabnik namestiti posebno programsko opremo, npr. TOR ali storitev I2P (Invisible Internet Project).

Ker je temni splet skrit in anonimen, ščiti ljudi, ki so v njihovih državah preganjani zaradi njihovega dela (npr. novinarji) ali verskih in političnih prepričanj, ter jim omogoča varno komunikacijo z drugimi skupinami ali posamezniki, ki razmišljajo enako. Žal to anonimnost zlorabljajo tudi (spletni) kriminalci, npr. prodajajo zlonamerno programsko opremo in trgujejo z nezakonitim orožjem, mamili ali storitvami.

Nezakoniti prenosi

avtorske pravice | peer-to-peer storitev | pretakanje | torrent | stran za pretakanje vsebin

Teme zajete v tem poglavju:

Kaj se šteje za nezakonito prenesene vsebine? Katere grožnje so povezane z nezakonitim prenosom vsebine?

Kaj se šteje za nezakonito prenesene vsebine?

Kot smo že omenili v poglavju o digitalni identiteti (str. 55), vsak uporabnik na internetu aktivno ali pasivno pušča sledi, ki kažejo, kaj je tam počel. To velja tudi za prenesene datoteke ali ogledane videoposnetke. Prenašanje in gledanje nezakonitih kopij TV-serij je med trenutnimi uporabniki interneta zelo priljubljena dejavnost. Najpogosteje jih uporabniki najdejo na spletnih mestih za pretakanje (ang. streaming)[28] polnih oglasov. Lahko jih prenesejo z brezplačnih strežnikov za shranjevanje ali pa jih delijo z drugimi preko enakovrednih omrežij tako imenovanih vsak-z-vsakim ang. peer-to-peer.

Večina teh dejavnosti krši avtorske pravice ustvarjalcev določenega dela in posledično tudi zakone različnih držav. Pri prenosu ali gledanju takšne vsebine je uporabnik lahko izpostavljen tudi digitalnim tveganjem, kot so napadi zlonamerne programske opreme ali škoda in izguba osebnih podatkov.

Katere grožnje so povezane z nezakonito preneseno vsebino?

1. Ko prenašate filme / TV-oddaje s pomnilniških strežnikov ali jih delite z veliko skupino neznanih ljudi (peer-to-peer storitve), je zelo enostavno prenesti nekaj, česar niste želeli. Datoteka je lahko na primer poimenovana kot ena izmed priljubljenih televizijskih oddaj, filmov ali iger, vendar namesto tega vsebuje zlonamerno programsko opremo.

2. Prav tako se lahko okužite z zlonamerno kodo (str. 73) ali pristanete na nevarni spletni strani, medtem ko gledate filme ali TV- serije in uporabljate storitev brezplačnega prenašanja. Ti so večinoma znani po ogromnem številu oglasov, med katerimi lahko nekateri vsebujejo povezave do zlonamernih spletnih mest. Za prenos zlonamerne programske opreme v napravo je potreben en napačen klik.

3. Prenos nezakonite vsebine ima tudi pravne posledice. Če uporabnika zasačijo pri prenosu ali uporabi nezakonite kopije, ga lahko čaka kazen. Kazen se od države do države razlikuje, v nekaterih primerih pa lahko zajema visoke globe[29] in včasih celo zaporno kazen.

28 Ne gre zamenjati za plačljive storitve pretakanja kot sta Netflix ali HBO GO.
29 https://www.theguardian.com/technology/2012/sep/11/minnesota-woman-songs-illegally-downloaded

Spletne igre

lažne aplikacije | odjemalec iger | omrežni bonton | spletne igre | igre za več igralcev | igralna konzola

Teme zajete v tem poglavju:

Katera so osnovna pravila digitalne varnosti pri igranju spletnih iger?
Kaj je skupnega igram za več igralcev in socialnim omrežjem?
Ali med igranjem iger potrebujete antivirusno zaščito?
Kakšna so tveganja pri prenosu in namestitvi ponarejenih iger?
Kaj storiti, če naletite na neprimerno vedenje v (spletni) igri za več igralcev?
Kaj morate storiti, preden prodate igralno konzolo / računalnik ali drugo napravo?

Katera so osnovna pravila digitalne varnosti pri igranju spletnih iger?

Pri igranju spletnih iger naj igralec upošteva osnovna pravila spletne varnosti, vključno z uporabo **zanesljivih in varnih naprav** za igranje, na primer domačega računalnika ali lastnega pametnega telefona. Naprava naj bo povezana v zanesljivo omrežje (najbolje domače omrežje) in uporablja posodobljen in podprt[30] operacijski sistem ter aplikacije. Naprava naj uporablja tudi zanesljivo in posodobljeno varnostno rešitev (antivirusni program) (str. 79).

Ko igralec za zagon iger uporablja odjemalce iger, mora zagotoviti, da so dobro zaščiteni z močnim geslom in - če je mogoče - uporabiti tudi dvofaktorsko preverjanje pristnosti[31]. Ponudnik iger je program, ki uporabnikom omogoča nakup, namestitev in zagon iger ter omogoča komunikacijo in interakcijo z več igralci. Steam[32], Origin[33] in Epic[34] so le trije primeri priljubljenih storitev. Ponudnik igre pridobi tudi podatke o plačilu (npr. kreditno kartico, s katero igralec plačuje za nove igre), kar je dragocen podatek za napadalca. Podobna pravila veljajo tudi za varnost igralne konzole (npr. Xbox, Nintendo ali PlayStation).

Kaj je skupnega igram več igralcev in socialnim omrežjem?

Zahvaljujoč hitrim internetnim povezavam in množični razširitvi iger za več igralcev so številni igralni svetovi v bistvu postali socialna omrežja. Namesto profila z lastno fotografijo igralci ustvarijo izmišljene like, ki se lotijo nalog, opravljajo različne naloge ali zbirajo redke predmete.

Če ima igra tudi način za več igralcev, se lahko igralci med izpolnjevanjem nalog povežejo z drugimi uporabniki, ki jih še niso srečali in jih v resničnem življenju ne poznajo. V takih primerih bi morali biti zlasti mlajši igralci previdni, kot je priporočeno za družabna omrežja. Igralci se morajo izogibati izmenjavi občutljivih podatkov v svojem igralnem profilu ali ustvarjanju podobnosti igralnega lika. Prav tako naj se izogibajo stikom z ljudmi v igri, ki osebno predlagajo sestanek ali zahtevajo osebne podatke.

Ali med igranjem iger potrebujete antivirusno zaščito?

Pri igranju igre bi morali igralci uporabljati varnostno programsko opremo, ki jih lahko zaščiti pred zlonamerno vsebino. Primer tega so zlonamerne povezave, ki jih je zavestno ali nevede igralcu poslal nekdo drug.

Napadalci se lahko tudi pretvarjajo, da bo povezava, ki so jo zagotovili, igralca pripeljala do dodatnega predmeta ali druge ugodnosti igre (npr. novega paketa razširitev). V mnogih primerih pa samo poskušajo žrtev pripraviti do tega, da odpre stran in z njo manipulirati tako, da se bo posredovala občutljive podatke ali onemogočila zaščito (na primer antivirusni program), da bodo nato napadlci napravo lahko okužili z zlonamerno kodo.

30 Proizvajalec nudi podporo za dano različico sistema / aplikacije in izda popravke in posodobitve zanj.
31 Za več podrobnosti o tej obliki zaščite glejte poglavje Gesla (str. 86).
32 https://store.steampowered.com
33 https://www.origin.com
34 https://www.epicgames.com

Kakšna so tveganja pri prenosu in namestitvi lažnih iger?

Igre morate vedno kupiti v uradnih in zaupanja vrednih trgovinah. Razlog za to je, da napadalci radi kopirajo priljubljene igre, da bi dosegli čim več žrtev. Najpogosteje bodo uporabili eno od naslednjih tehnik:

1. **Ustvarijo ponarejeno različico igre**, ki posnema najbolj priljubljene igre, kot sta Minecraft ali Fortnite, vendar vsebuje zlonamerno kodo. Zanesljiva antivirusna programska oprema lahko takšne grožnje blokira. Uporabniki / igralci igre se lahko srečajo s podobnimi ponarejenimi aplikacijami tudi v nekaterih uradnih trgovinah (npr. Google Play). Opazijo jih lahko po mnenjih drugih uporabnikov, ki so igro verjetno namestili in po tem, ko so videli, da je ponarejena, v svojih komentarjih na to opozorili druge uporabnike.
2. **Okužite pravo igro z zlonamerno kodo** in ustvarite tako imenovane "trojance". Takšne igre lahko najpogosteje najdemo v neuradnih trgovinah in na spletnih forumih, kjer jih lahko ponudimo kot "brezplačne prenose". Cena, ki jo plačate za to, je običajno računalniška okužba, ki ima lahko daljnosežne posledice, zlasti če ukrade vaše podatke ali poškoduje vašo napravo.

Kaj storiti, če naletite na neprimerno vedenje v (spletni) igri za več igralcev?

Tako kot v kateri koli drugi skupnosti lahko tudi med igralci srečate različne vrste vedenja. Igra daje prosto pot čustvom, ki jih še bolj poudarjajo adrenalin in zavzetost igralcev. To pogosto povzroči agresivne komentarje, žalitve, obtožbe itd. To vzbudi čustva, ki jih igralci igre pogosto pustijo prosto v klepetu med igro. Če gre le za enkratni pojav, to ni težava, vendar vam ni treba trpeti rednih žalitev.

- Najboljši način je, da se na takšne enkratne dogodke ne odzovete in jih ne jemljete preveč resno, sicer vas bodo vlekli v neprimerno komunikacijo.
- Če se takšno vedenje v skupini ponavlja, razmislite o izbiri druge skupine igralcev.
- Tako kot v drugih skupinah so tudi skupine igralcev nagnjene k ustrahovanju in spletnemu sovraštvu, s čimer se vam ni treba sprijazniti. Določeni igralec je lahko tudi ustrahovalec, ki igralno okolje zlorablja za škodovanje drugim.
- Številne igre - tako kot družbena omrežja - igralcem omogočajo, da poročajo o neprimernem vedenju, problematičnih igralcih ali prevarantih. Odgovorno poročanje izboljša varnost igralcev, ki poročajo o težavi, in vseh drugih v igri.
- Ko se v igri ali skupnosti igralcev zgodijo zaskrbljujoče stvari, o tem obvestite nekoga, ki mu zaupate.
- Za vse igralce veljajo isti standardi. Uporabniki se morajo tudi zavedati, da lahko njihovo vedenje in komentarji nekomu škodijo. Tudi pri igranju iger je treba upoštevati "omrežni bonton".

Kaj morate storiti pred prodajo igralne konzole / računalnika ali druge naprave?

Če se odločite prodati ali zamenjati igralno konzolo, računalnik ali drugo (mobilno) napravo za novo, morate najprej izbrisati vse svoje osebne podatke in igre ter jih v najboljšem primeru ponastaviti na tovarniške nastavitve. Ta možnost je običajno na voljo v igralni konzoli ali nastavitvah operacijskega sistema za osebni računalnik. S tem boste odstranili vso shranjeno vsebino ter različne spletne račune in storitve, ki ste jih uporabljali, sicer pa bi jih skupaj z napravo podarili kupcu.

Zlonamerna programska oprema in druge zlonamerne dejavnosti

oglaševalska programje | stranska vrata | bančno zlonamerno prograje | rudarji kriptovalut | napad z zavrnitvijo storitve DDoS | prenašalec | ranljivost | črv | nezaželena pošta | beležnik tipkovnice | kriptovaluta | kripto denarnica | kibernetsko orožje | orodna vrstica | spletno vohunjenje | kradljivec gesel | potencialno neželene aplikacije | vohunsko programje | izsiljevalsko programje | prevara | posnemanje | socialni inženiring | trojanci | virus | napredna vztrajna grožnja | ranljivost ničelnega dneva | lažno predstavljanje

Teme zajete v tem poglavju:

- Kaj je zlonamerna programska oprema?
- Katere kategorije zlonamerne programske opreme poznamo?
- Katere vrste zlonamerne programske opreme obstajajo?
- Kaj motivira zlonamerne dejavnosti napadalcev?
- Kako izgledajo potencialno neželene aplikacije (PUA)?
- Kako izgleda pogost napad zlonamerne programske opreme?
- Kaj lahko stori napredna zlonamerna programska oprema, na primer APT?
- Zakaj ne bi govorili še več o virusih in črvih?
- Kaj še poleg zlonamerne programske opreme uporabljajo napadalci?
- Katere druge oblike napada obstajajo?

Kaj je zlonamerna programska oprema?

Ta beseda je združitev besed zlonamerno in programska oprema ter označuje računalniško kodo, ki je bila ustvarjena za škodovanje. To je natančnejše ime za tisto, kar mnogi imenujejo (računalniški) virus, kar je le ena podkategorija zlonamerne programske opreme.

Katere kategorije zlonamerne programske opreme poznamo?

Zlonamerno programsko opremo lahko razdelimo v različne kategorije. Če zlonamerno programsko opremo razvrstimo glede na tveganje, ki jo predstavlja, dobimo naslednje kategorije:

1. **Potencialno neželene aplikacije (PUA)**
   Ti programi sicer sami po sebi niso zlonamerna programska oprema, saj imajo nekatere neželene lastnosti. Morda ne bodo neposredno škodljivi za uporabnika, lahko pa so moteči, zavajajoči ali pojedo vire naprave in predstavljajo prvi korak k resnično zlonamerni kodi ali nevarnim internetnim lokacijam. Uporabniki lahko takšne PUA-je pogosto namestijo v paketu z drugo programsko opremo ali jih naletijo na dvomljiva spletna mesta.

2. **Zlonamerna programska oprema**
   Zlonamerna programska oprema vsebuje zlonamerno kodo, ki ima jasen cilj - škodovati uporabniku. Lahko na primer ukrade podatke za prijavo ali spremlja uporabnika ali njegovo spletno aktivnost, ga izsiljuje ali mu ukrade denar. Cilj večine zlonamerne programske opreme je zaslužiti denar za njene ustvarjalce, ki širijo in upravljajo zlonamerno programsko opremo. Zlonamerna programska oprema vsebuje številne podkategorije, kot so izsiljevalska programska oprema, vohunska programska oprema, trojanci, prenašalci, beležnik tipkovnice, stranska vrata, oglaševalska programska oprema in številne druge.

3. **Napredna obstojna grožnja (znana tudi kot APT)**
   Kot že ime pove, gre za izjemno dovršene vrste zlonamerne kode, ki so jih ustvarile skupine strokovnjakov, ki so vložili veliko časa, energije in denarja v ustvarjanje svoje zlonamerne programske opreme. Običajno se osredotočajo na občutljiva področja javnih storitev, kot so oskrba z električno energijo, vladne ali mednarodne institucije ali sistemi za nadzor prometa. Skupine APT in njihova orodja lahko povzročijo resno škodo in celo ogrozijo človeško življenje. Nekatera njihova zlonamerna programska oprema je celo označena kot spletno orožje (npr. Stuxnet) ali orodje za kibernetsko vohunjenje. Običajna oseba verjetno nikoli ne bo neposredno doživela napada APT; lahko pa doživi posledice, če tak napad onemogoči oskrbo z električno energijo v njeni regiji ali onemogoči storitev državne agencije.

Kaj motivira zlonamerne dejavnosti napadalcev?

Trenutno se motivacija spletnih kriminalcev zelo razlikuje od motivacije njihovih predhodnikov v osemdesetih in devetdesetih letih, ko so se začeli prvi kibernetski napadi. V preteklosti je bil njihov glavni cilj pokazati svetu svoje sposobnosti in si zgraditi ugled znotraj "hekerske" skupnosti.

Glavna motivacija danes je denar. Zlonamerna koda je običajno narejena tako, da jo lahko drugi napadalci v zameno za znatne vsote denarja ponovno uporabijo, prodajo in ponovno uporabijo. Prodaja zlonamerne programske opreme kot storitve odpira dostop do zlonamerne programske opreme tudi neizkušenim storilcem kaznivih dejanj, ki kode ne morejo napisati sami, lahko pa jo enostavno kupijo in širijo v lastno korist.

Obstaja tudi majhna skupina zelo naprednih napadalcev, ki pišejo zlonamerno programsko opremo za ciljne napade. V tem primeru dobiček ni pomemben, ker ga financira izvajalec - ponavadi nacionalna država, ki ima dovolj virov in razlogov, na primer uporabo kode kot orožja v hibridnem vojskovanju. Čeprav lahko posledice takšnih dejavnosti vplivajo na resnični svet in lahko povzročijo škodo, na primer na industrijski opremi ali kritičnih sistemih, jih včasih imenujemo spletno orožje.

Kako izgledajo potencialno neželene aplikacije (PUA)?

Ena vrsta PUA so tako imenovani **ang. coinminers (rudarji kriptovalut)** ki porabljajo računalniške vire za pridobivanje kriptovalut, kot sta bitcoin ali Monero. Nekatere od teh neželenih aplikacij uporabljajo preobleko in vas poskušajo prepričati, da jih namestite neposredno v svojo napravo, vendar pa lahko nekateri dostopajo do virov vaše naprave prek brskalnikov, takoj ko žrtev odpre spletno mesto, ki vsebuje kodo za rudarjenje kriptovalut[35]. Programi za rudarjenje so uvrščeni med manj nevarne, saj se njihova dejavnost ustavi takoj, ko uporabnik zapre okno brskalnika ali sam brskalnik.

V preteklosti so bile najpogostejše PUA **tako imenovane orodne vrstice**, ki jih je žrtev zavestno ali nevede namestila v svoj brskalnik. Te orodne vrstice so bile običajno v kompletu z drugo programsko opremo, vendar niso zagotavljale oglaševane funkcije; namesto tega so upočasnile brskalnik in zapletle njegovo uporabo.

Drugi primeri PUA so različni **brskalniški programi in razširitve** ki obljubljajo odstranitev napak, zmanjšanje obremenitve ali "čiščenje" naprave in izboljšanje njene učinkovitosti. V večini primerov gre le za prazne obljube brez dejanskih rezultatov. Glavni cilj takšnih aplikacij je prikazovanje oglasov ali zbiranje informacij o vedenju uporabnikov.

Kako izgleda pogost napad zlonamerne programske opreme?

Zlonamerna programska oprema ima lahko različne oblike. Ta splošni izraz vključuje viruse, črve, trojanske programe in druge vrste zlonamerne kode. Spodaj bomo podrobneje obravnavali posamezne vrste zlonamerne programske opreme, s katerimi se lahko srečate.

- **Oglaševalska programska oprema**
  Če se naprava okuži z oglaševalsko programsko opremo, bo prikazala preveliko število oglasov, tudi če tega ne pričakujete - npr. ko brskalnik ni odprt. Če menite, da oglaševalska programska oprema ni tako nevarna, se motite. Poleg tega, da moti uporabnika, uporablja tudi nekatere agresivne tehnike, značilne za zlonamerno programsko opremo. Tako lahko na primer brez vednosti uporabnika spremeni nastavitve naprave ali namesti in odstrani drugo programsko opremo. Ti ukrepi lahko predstavljajo nevarnost sekundarne, veliko resnejše okužbe.
- **Stranska vrata ang. backdoor**
  Tudi to ime je zelo primerno. To je vrsta zlonamerne programske opreme, ki lahko odpre zakulisno ploščo in omogoča napadalcu, da zlorabi tak dostop do uporabnikovega sistema, ga nadzira ali namesti dodatno zlonamerno programsko opremo. Backdoor pogosto služi kot osnovno orodje in izhodišče za napredne trajne grožnje (APT), ki so podrobno opisane spodaj.

35 Dobro je upoštevati, da nekateri uporabniki zavedno in namerno nameščajo podobno kodo na njihove naprave ali na spletna mesta, da bi zaslužili denar.

- **Zlonamerna programska oprema bančništva**
  Osredotoča se predvsem na krajo finančnih informacij žrtev, kot so številke kreditnih kartic, dostop do bančnih računov, kripto denarnice in druge storitve, povezane z denarjem ali kriptovalutami. Nekatere družine bančne zlonamerne programske opreme poskušajo zbrati še več podatkov in so zato pogosto označene kot prodajalci informacij.
- **Prenos**
  Po namestitvi se ta zlonamerna koda poveže z določenim spletnim mestom ali strežnikom ter prenese in namesti dodatno zlonamerno kodo, ki so jo izbrali kriminalni operaterji.
- **Beleženje tipkanja**
  Ta koda spremlja uporabnikov vsak korak ali natančneje vsak premik tipkovnice in premikanje miške. To mu omogoča podrobno spremljanje (preslikavo) njegove dejavnosti in lahko tudi ukrade podatke, ki niso nikjer shranjeni, ampak jih uporabnik občasno vnese na zaslon za prijavo v storitev ali program.
- **Kradljivec gesel**
  Kar zadeva kategorije zlonamerne programske opreme, je kradljivec gesel zelo podoben bačni zlonamerni programski opremi in prodajalcem zlonamerne programske opreme. Vendar se osredotoča na datoteke in programe, ki lahko vsebujejo gesla. Mnogi med njimi na primer poskušajo ukrasti gesla, shranjena v brskalnikih ali ranljivih upraviteljih gesel.
- **Izsiljevalska programska oprema**
  Izsiljevalska programska oprema blokira zaslon naprave ali šifrira njene podatke. Žrtev mora plačati odkupnino za odblokiranje / dešifriranje naprave. Najbolj znana primera sta WannaCry[36] (2017) ali CryptoLocker[37] (2013). Izsiljevalec z imenom (Not)Petya[38] (2017) je bil del najbolj uničujočega kibernetskega napada v zgodovini in povzročil škodo za več kot 10 milijard dolarjev.
- **Vohunska programska oprema**
  Zlonamerna koda, ki vohuni za žrtvijo prek ogrožene naprave. Cilj je prikrito zbrati čim več podatkov, npr. gesla, dostopne kode in druge občutljive podatke ter jih naložiti na strežnike napadalcev. Zločinci bodo nato poskušali monetizirati podatke na "temnem spletu"[39] ali jih uporabiti za druge zlonamerne dejavnosti. To pomeni, da lahko uporabnikovi občutljivi podatki pridejo v roke storilcem kaznivih dejanj, ki jih lahko zlorabijo za škodo žrtvam, npr. s krajo podatkov ali s krajo njihovega denarja ali identitete.

Ta seznam seveda ni izčrpen in lastnosti zlonamerne kode se lahko razlikujejo in se osredotočajo, na primer, na omrežno komunikacijo, zbiranje občutljivih podatkov iz pomnilnika naprave ali na napad na napravo, še preden se zažene operacijski sistem. Včasih lahko pride do kombinacij različnih vrst zlonamerne programske opreme, ki je sestavljena iz več ravni ali modulov s podobno funkcionalnostjo.

Kaj lahko stori napredna zlonamerna programska oprema, na primer APT?

Kriminalci, ki stojijo za takšno zlonamerno programsko opremo, so običajno prekaljeni razvijalci programske opreme z dolgoletnimi izkušnjami pri delu z zlonamerno programsko opremo. Njihovi "izdelki" so običajno modularni - vsebujejo več delov, ki jih je mogoče dodati ali odstraniti, pri čemer izkoriščajo znane programske ranljivosti ali prefinjene manipulacijske tehnike za infiltriranje v sisteme žrtev. Velika verjetnost je, da imajo dovolj časa in sredstev za razvoj zlonamerne programske opreme, zato dobiček ni njihova glavna motivacija. Večinoma se osredotočajo na vohunjenje in uničujoče učinke svojega dela.

36 https://www.welivesecurity.com/2017/05/15/wannacryptor-key-questions-answered/
37 https://en.wikipedia.org/wiki/CryptoLocker
38 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
39 Za več informacij o temi, glejte poglavje Površinski, globoki, temni splet (str. 68).

Primer takšnega ciljanega napada je bil napad na distributerje energije v Ukrajini, kjer so napadalci ciljali na industrijska "stikala" in računalnike, ki jih nadzorujejo. Vse skupaj je bilo prizadetih le nekaj deset naprav, vendar so napadalci lahko povzročili izpad električne energije, ki je prizadel več sto tisoč uporabnikov. Operaterji, ki stojijo za napadom, so dostop dobili prek okuženih e-poštnih prilog, ki jih je odprl eden od zaposlenih v distribucijskem podjetju. Ta dostop jim je omogočil namestitev in zagon nevarne zlonamerne programske opreme, natančneje BlackEnergy[40] in kasneje Industroyer[41]. Obema je za nekaj ur uspelo izklopiti napajanje gospodinjstev. Prefinjena zlonamerna koda je bila tudi vir najbolj uničujočega napada v zgodovini, znanega pod tem imenom Petya or NotPetya[38]. Ta napad je onemogočil številna svetovna podjetja in povzročil škodo za več kot 10 milijard USD, čeprav je bil prvotno namenjen le ukrajinskim podjetjem.

Zakaj ne govorimo še več o virusih in črvih?

Obe kategoriji zlonamerne programske opreme sta bili v preteklosti zelo razširjeni, zlasti med osemdesetimi in devetdesetimi leti. Danes pa je obseg zlonamerne programske opreme veliko večji in niti virusi niti črvi se ne uvrščajo med najbolj prevladujoče, zlasti v primerjavi s trojanci, oglaševalsko ali odkupno programsko opremo.

- **Virusi** delujejo podobno kot gripa ali druge virusne bolezni. Potrebujejo gostitelja, tj. ranljive programe in programe, ki jih lahko okužijo in uporabljajo za nadaljnje širjenje.
- **Črvi**, za razliko od virusov, ne potrebujejo nobenega programa za širjenje in se lahko sami razmnožujejo (množijo) prek omrežja, e-pošte in prenosnih medijev (npr. USB-pogoni).
- **Trojanci** so danes verjetno najbolj razširjena vrsta zlonamerne programske opreme. Uporabljajo isto načelo kot bajesloven trojanski konj. Na zunaj se pretvarjajo, da imajo legitimno funkcijo (na primer video predvajalnik, igra, aplikacija za klepet) ali se predstavljajo kot neškodljiva datoteka (dokument, posodobitev), vendar je njihov resnični cilj povzročiti škodo. Zanimivo je, da nekateri trojanci nudijo del obljubljene funkcionalnosti ali storitve, da prikrijejo svoj glavni, podli cilj.

Kaj poleg zlonamerne programske opreme še uporabljajo napadalci?

Da bi napadalec kaj pridobil, potrebuje vsaj delno sodelovanje žrtve. Če večinoma ustvarijo zlonamerno kodo brez dostopa do trdega diska v katerem so dokumenti, ali do kamere, mikrofona ali drugih delov sistema, od tega napadalec ne bi imel veliko koristi.

Zato napadalci pogosto uporabljajo **socialni inženiring**, to so sofisticirane tehnike, namenjene manipulaciji z uporabnikom, ki jim nevede daje odobritev nadzora nad napravo. Več informacij o tej obliki napada najdete spodaj.

Najnaprednejši napadalci pa imajo druge načine, kako se infiltrirati v napravo. Nekateri v programski opremi iščejo doslej **neznane ranljivosti**[42] ali pa za njihovo iskanje uvedejo posebna orodja. V drugih primerih napadalci določijo zakonit del programske opreme (ali eno od njenih različic) in jo ogrozijo z zlonamerno programsko opremo. Prvotni ustvarjalci zakonite programske opreme tega ne vedo in uporabnik, ki namesti okuženo različico, nevede zažene zlonamerno programsko opremo.

40 https://www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

41 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

42 Tovrstne ranljivost so ustvarjalcu programske opreme še neznane. Napadalec zlorabi to ranljivost, ne da za to kdo vedel. Najpogosteje se napadalci osredotočajo na dobro znane in dokumentirane ranljivosti, ki so bile prej javno objavljene, saj je to cenejša in lažja alternativa.

Katere druge oblike napada obstajajo?

Kibernetski napadi se lahko pojavijo v različnih oblikah in zlonamerna programska oprema ni nujno edino / končno orodje, ki ga napadalci uporabljajo. Tu je še nekaj primerov:

- **Botnet** je mreža okuženih naprav ("botov"), ki jih napadalec s strežnika nadzoruje na daljavo ali z uporabo ukazov, ki si jih naprave izmenjujejo. Botnet lahko širi neželeno pošto ali zlonamerno programsko opremo ali se uporablja za pokrivanje sledi napadalca ali za napade DDoS (glej definicijo spodaj). Obstoječi botnet lahko napadalec celo ponudi v najem v temnem spletu drugim napadalcem. Botnet je lahko sestavljen iz milijonov naprav. Trenutno se napadalci osredotočajo na naprave, ki vključujejo internet stvari (pametne naprave ali IoT), ki so znane po slabši varnosti.
- Cilj **napada porazdeljene zavrnitve storitve (DDoS)** je odstraniti spletno mesto ali spletno storitev z uporabo omrežnega prometa, ustvarjenega z botnetom. Veliko omrežje okuženih naprav lahko ustvari ogromno zahtev za dostop, usmerjenih na določeno spletno mesto, s čimer preobremeni strežnike, ki ga gostijo. Eden največjih napadov DDoS[43] se je zgodil marca 2018 in je bil usmerjen na nerazkrito ameriško podjetje z 1,7 terabita na sekundo (Tbps) podatkov.
- **Izkoriščati, exploit** je angleška beseda, ki pomeni "uporabiti nekaj v svojo korist". Njegova negativna konotacija se uporablja na področju digitalne varnosti. To je v bistvu del kode ali postopek, ki so ga napadalci ustvarili, da bi izkoristili ranljivosti in napake v programski ali strojni opremi, da bi prevzeli nadzor nad njo.
- **Lažno predstavljanje** je goljufiv poskus pridobivanja občutljivih informacij in podatkov, pri katerem se napadalci predstavijo kot zaupanja vreden subjekt, službo ali osebo. Lažna povezava, prejeta po e-pošti, bo uporabnika usmerila na spletno mesto, ki naj bi ga zaupali zaupanja vredni strani, kot so družabno omrežje, e-poštna storitev ali banka. Uporabniki lahko naletijo na lažne povezave v neželeni pošti, pogosto pa se širijo tudi prek forumov za klepet, družbenih omrežij ali prek sporočil SMS. Številne med njimi lahko prestreže varnostna programska oprema. Kot vedno je pomembno, da dvakrat preverite, preden kar koli kliknete.
- **Socialni inženiring** opisuje vrsto netehničnih tehnik napadov, ki jih spletni kriminalci uporabljajo za manipulacijo z žrtvami, da bi kršile varnostna pravila in izvajale škodljiva dejanja ali se odrekle občutljivim informacijam.
- **Vsiljena pošta** je vsa nezaželena elektronska pošta. Lahko je v obliki e-pošte, sporočila SMS ali klepeta. Lahko vsebuje neželeno oglaševanje, lahko pa se uporablja tudi za širjenje povezav do druge zlonamerne vsebine.
- **Prevara** je vrsta socialnega inženiringa, kjer napadalec zavede žrtev ali skupino žrtev, da pridobi njihovo zaupanje, ki se nato izkoristi v korist zločinca. Takšne dovršene prevare običajno izkoristijo človeške lastnosti, kot so lahkovernost, sočutje, neodgovornost ali pohlep. Primeri prevar so ponarejene e-trgovine z očali s poceni blagovno znamko ali tekmovanja, ki obljubljajo brezplačno podelitev priljubljene naprave. Na koncu lahko žrtve izgubijo svoje podatke ali včasih celo svoj denar.
- **Posnemanje** spada v kategorijo bančnih napadov. Gre za neopazno strojna naprava, nameščena na bankomatu za skeniranje podatkov z vstavljenih kartic. Ti dragoceni podatki se nato shranijo ali pošljejo napadalcu, ki jih lahko nato proda ali izkoristi za nakupe v imenu žrtve. Podobni napadi se dogajajo tudi v digitalnem okolju, kjer lahko napadalci z zlonamerno kodo okužijo plačilni prehod zakonite e-trgovine.

43 https://www.welivesecurity.com/2018/03/08/new-ddos-attack-method-breaks-record/

Varnostna rešitev (antivirusni program)

antivirus | varnostna rešitev | zlonamerna programska oprema | lažni antivirus | strojno učenje

Teme zajete v tem poglavju:

Kaj počne antivirusni program?
Zakaj potrebujete varnostno rešitev?
Na kaj morate biti pozorni pri izbiri varnostne rešitve?
Kakšna je razlika med plačano in brezplačno varnostno rešitvijo?
Ali dve varnostni rešitvi zagotavljata boljšo zaščito kot ena?
Zakaj je ime "antivirus" netočno in zakaj bi ga bilo treba zamenjati?

Kaj počne antivirusni program?

Antivirus ali natančneje varnostna rešitev je del programske opreme, ki uporabnika ščiti pred grožnjami in tveganji, ki obstajajo v digitalnem okolju. Ko varnostna rešitev zazna zlonamerno kodo, vedenje ali dejavnost, o tem obvesti uporabnika.

Zakaj potrebujem varnostno rešitev?

Informacije v današnjem svetu so izjemno pomembne. Napadalci se tega zavedajo in zlorabljajo številna tehnološka in psihološka orodja za dostop do informacij, njihovo prodajo ali izkoriščanje za lastno korist. Mnogi uporabniki mislijo, da nimajo nobenih dragocenih informacij, vendar je ravno obratno. Poleg tega je okužena naprava lahko tudi dragocen vir za posrednika, ki še naprej širi zlonamerno programsko opremo.

Izkušeni napadalci, katerih cilj je izkoristiti žrtev in njene podatke, napišejo svojo zlonamerno kodo, jo izboljšajo, prodajo in razširijo. Manj tehnološko usposobljeni lahko takšno kodo kupijo ali se osredotočijo na ustvarjanje iznajdljivih laži, s katerimi lahko manipulirajo z žrtvami in iz njih pridobivajo občutljive podatke, na primer poverilnice na bančnih računih.

Seveda obstaja razmeroma velika siva cona, kjer se oba pristopa mešata. Za več informacij o oblikah zlonamerne kode glejte poglavje Zlonamerna programska oprema (str. 73).

Uporabniki se lahko zaščitijo pred velikim delom teh groženj z uporabo ugledne in zanesljive varnostne programske opreme (običajno imenovane tudi antivirusna programska oprema). Takšne rešitve bi morale biti sposobne zaznati grožnje z različnimi tehnikami in ponujati več ravni zaščite. Grožnje lahko zaznamo na različnih krajih, npr. na omrežni ravni, ob vstopu v napravo, ob zagonu ali pri dostavi v mapo "Prejeto", ki se pretvarja, da je neškodljiva e-pošta ali "nedolžna" priloga.

Na kaj morate biti pozorni pri izbiri varnostne rešitve?

Dobra praksa pri izbiri varnostne rešitve je pregled rezultatov neodvisnih testov. Tu je nekaj primerov organizacij, ki izvajajo takšno testiranje: VirusBulletin[44], AV Comparatives[45], AV-Test[46].

V svojih testih lahko uporabniki pregledajo različne funkcije varnostne programske opreme - npr. koliko virov uporabljajo, kolikšen odstotek zlonamerne kode lahko zaznajo in blokirajo ali koliko lažno pozitivnih rezultatov ustvarijo.

Ključni dejavnik pri izbiri rešitve bi moral biti, ali varnostna programska oprema uporablja kombinacijo tehnik, ki lahko uporabnika zaščitijo na več ravneh. Protivirusne rešitve, ki uporabljajo samo eno prevladujočo tehniko ali se osredotočijo samo na eno vrsto odkrivanja, napadalci lažje obidejo.

To bi lahko primerjali z varnostnimi funkcijami avtomobila. Vozilo, opremljeno z asistenčnimi sistemi, ki vozniku lahko pomagajo pri izgubi oprijema ali jih zaščitijo z varnostnimi pasovi in zračnimi blazinami, je zagotovo veliko varnejše od starejšega modela, ki potnike varuje z eno od teh lastnosti.

44 https://www.virusbulletin.com
45 https://www.av-comparatives.org
46 https://www.av-test.org/en

Pomembno je tudi opazovati, ali izbrana varnostna programska oprema zahteva soglasje uporabnika za obdelavo podatkov v skladu z regionalnimi zakoni, kot sta GDPR v EU ali CCPA v Kaliforniji. Uporabnika je treba pred namestitvijo obvestiti, katere podatke bo zbrala rešitev in za katere namene.

Kakšna je razlika med plačljivo in brezplačno varnostno rešitvijo?

Kakršnakoli varnostna programska oprema je boljša kot nobena. Na splošno obstajata dve glavni kategoriji varnostnih rešitev - plačljive in brezplačne.

Brezplačne varnostne rešitve zagotavljajo določeno stopnjo zaščite, vendar mora podjetje, ki jih proizvaja, zaslužiti na drugačen način. To lahko storijo z zbiranjem in prodajo podatkov o svojih uporabnikih, s prodajo plačljivih funkcij v aplikaciji ali s prikazovanjem oglasov.

Plačljiva varnostna rešitev v povprečju stane nekaj deset evrov na leto. V zameno za ta znesek lahko njeni razvijalci delajo na zagotavljanju njenega delovanja in izboljšanju tehnologije, hkrati pa uporabnika ne motijo z oglaševanjem in zbirajo samo informacije o zlonamerni programski opremi. Nekateri varnostni programi ponujajo tudi tako imenovana preizkusna obdobja, v katerih jih lahko uporabnik brezplačno namesti in uporablja več tednov ali mesecev.

Vendar bodite previdni pri programski opremi, ki spominja na varnostno rešitev in ne zagotavlja nobene zaščite - tako imenovani **ponarejeni antivirusni program**. Ta vrsta goljufije lahko žrtev stane precej denarja, hkrati pa ogrozi njeno varnost. Pri izbiri varnostne rešitve vedno preverite, ali gre za zanesljiv in zaupanja vreden izdelek.

Ali dve varnostni rešitvi zagotavljata boljšo zaščito kot ena?

Ko se na eni napravi izvajata dve ali več varnostnih rešitev, to običajno poslabša uporabniško izkušnjo in raven zaščite. Razlog za to je, da varnostne rešitve pregledajo dohodne in odhodne podatke, omrežno komunikacijo, procese, ki se izvajajo v napravi itd., da bi odkrili in odstranili morebitne zlonamerne dejavnosti. Ko več varnostnih programov dobi takšne pravice, si stopijo na pot in zmanjšajo svojo učinkovitost. Uporabnikov položaj se lahko zaplete, saj lahko trčenja med posameznimi aplikacijami privedejo do številnih lažnih pozitivnih rezultatov.

Zakaj je ime “antivirus” netočno in zakaj bi ga bilo treba zamenjati?

Trenutno se kot sinonima uporabljata “protivirusni program” in “varnostna rešitev”. Z vidika proizvajalcev pa je prišlo do pomembnih sprememb, ki jih beseda “protivirusni program” - kljub svoji priljubljenosti - ne more zajeti. Ime programska oprema za zaščito ali varnostna rešitev je zato veliko bolj primerna.

Najprej se sodobne varnostne rešitve ne osredotočajo izključno na zaščito pred virusi, temveč pred veliko širšim naborom zlonamerne kode in dejavnostmi, ki v obdobju prvotnih protivirusnih rešitev sploh niso obstajale. Da bi to lahko storili, se je moral tradicionalni protivirusni program razvijati in dodajati nove tehnologije in zaščitne sloje, vključno s strojnim učenjem - tj. sposobnost samega programa za analizo podatkov, prepoznavanje podobnosti ali nepravilnosti in učenje iz prejšnjih izkušenj. Sodobna varnostna rešitev poleg zaščite uporabnikov pred zlonamerno kodo ponuja tudi druge vrhunske funkcije, kot so šifriranje podatkov, upravljanje gesel ali lokalizacija izgubljene ali ukradene naprave.

Varnost internetne povezave

dostopna točka | internetni brskalnik | internet stvari (IoT) | pametni dom | pametna naprava | navidezno zasebno omrežje (VPN) | spletna kamera | zaščiten Wi-Fi dostop (WPA)

Teme zajete v tem poglavju:

Katere vrste omrežij ali omrežnih povezav so varnejše? Kako lahko prepoznate (ne) varno omrežje? Kako se lahko izognete nevarnim omrežjem? Kaj je navidezno zasebno omrežje (VPN)? Kaj je internet stvari (IoT)? Kako IoT vpliva na spletno varnost uporabnikov? Ali morate pokrivati svojo spletno kamero?

Katere vrste internetnih povezav (omrežij) nudijo večjo varnost?

Korporativna omrežja običajno ponujajo najvišjo raven varnosti, vendar se postopoma izboljšuje tudi varnost domačega omrežja. Najnižjo raven varnosti ponujajo javna omrežja Wi-Fi brez zaščite z geslom. Običajno so na voljo na mestnih trgih, kavarnah, javnem prevozu, hotelih in v javnih prostorih.

Glavna razlika med varnim in manj varnim omrežjem je uporaba izboljšanega varnostnega protokola (WPA2 ali idealno prihajajoči WPA3) in geslo, ki ga mora uporabnik vnesti, da se lahko poveže. Vendar nobena od teh lastnosti ne ponuja 100-odstotne garancije, da napadalec omrežja, s katerim se povežete, ni ogrozil ali celo ustvaril.

Kako lahko prepoznate (ne) varno omrežje? Kaj iskati?

- **Izberite mesto, kjer se želite povezati z internetom**
  - Če je mogoče, se povežite samo z omrežji, za katera poznate skrbnika ali varnostne nastavitve. To so običajno šolska, domača (v vašem domu ali domu prijateljev) in omrežja v podjetju. Če je mogoče, se popolnoma izogibajte javnim omrežjem.
- **Ime omrežja Wi-Fi**
  - Ko izbirate omrežje Wi-Fi, natančno preučite njegovo ime. Ena izmed najbolj razširjenih metod napada je ustvariti dostopno točko / omrežje z imenom, ki je skoraj enako legitimnemu omrežju na tej lokaciji. Z uporabo tega pristopa napadalci izboljšajo možnosti, da se žrtev poveže prek njihovega omrežja, nato pa lahko spremljajo, katere podatke žrtev pošilja.

KONKRETEN PRIMER: Kavarna ponuja brezplačno omrežje z imenom *Cafe_wifi*. Napadalec pa ustvari podobnega z imenom *Cafe_wifi_free* ali *Cafe_wifi1*. Če z osebjem ne preverite, kateri je legitimen, ne boste mogli biti prepričani.

- **Varnostni protokol/geslo**
  - Do nedavnega je najvišjo raven zaščite ponujal protokol WPA2 (Wi-Fi Protected Access 2). Podatki, poslani prek omrežja, zaščitenega s tem protokolom, so šifrirani, kar napadalcem preprečuje, da bi jih prebrali. Vendar so raziskovalci v tem protokolu našli resne ranljivosti, zato trenutno uvajajo novo različico z imenom WPA3.
  - Protokola WEP (Wired Equivalent Privacy) in WPA (Wi-Fi Protected Access version 1) sta zastarela in ne zagotavljata zadostne zaščite za vašo komunikacijo. Ko razpoložljivo omrežje Wi-Fi še vedno uporablja te protokole, se jim je bolje izogniti.
- **Poiščite https://**
  - Če se povežete prek javnega omrežja Wi-Fi, ki ga ne morete preveriti kot varnega, obiskujte samo spletna mesta, katerih URL se začne s **https: //**. To pomeni, da je komunikacija s spletnim mestom šifrirana in napadalec, prijavljen v isto omrežje, ne bo mogel prebrati podatkov, ki jih pošljete.

Kako se lahko izognete nevarnim omrežjem?

Dandanes imajo skoraj vsi v lasti mobilni telefon s podatkovnim paketom. Če je dovoljena količina podatkov, lahko ustvarijo lastno omrežje Wi-Fi (tako imenovana dostopna točka) in z imenom in geslom nastavi želeno raven varnosti (idealno WPA2 ali WPA3). Nato lahko to omrežje uporabljajo za povezovanje drugih naprav, na primer prenosnika, tabličnega računalnika ali drugih pametnih naprav. Napadalcu je težko vdreti v takšno omrežje.

Kaj je virtualno zasebno omrežje (VPN)?

Če nimate možnosti ustvariti lastnega omrežja, lahko kot alternativo uporabite storitev VPN (navidezno zasebno omrežje), ki lahko ustvari šifriran predor med uporabnikovo napravo in ciljnim spletnim mestom. Ta predor je skoraj neprehoden za napadalce. Slaba stran je, da zanesljive in kakovostne storitve VPN niso brezplačne. Vendar imajo nekateri brskalniki, na primer Opera ali EPIC, vgrajeno to funkcijo. VPN predstavlja višjo raven zaščite, kar je smiselno zlasti, kadar mora uporabnik ostati anonimen ali če mora zaobiti omejitve internetne povezave. Primeri takih situacij so novinarji in civilni aktivisti, ki jih avtoritarni režimi preganjajo ali omejujejo.

Kaj je internet stvari (IoT)?

Internet stvari označuje vse naprave, ki jih skupaj imenujemo “pametne” ali “inteligentne”. Ko je naprava imenovana “pametna”, mora biti poleg izpolnjevanja drugih pogojev povezana tudi z internetom. Medtem ko so bili v preteklosti takšne naprave večinoma računalniki, kasneje pa mobilni telefoni in tablični računalniki, pa danes vključujejo tudi številne televizorje, kamere, ure, hladilnike in celo avtomobile. Internetna povezljivost razširja funkcionalnost takšnih naprav, a hkrati odpira pot napadalcem.

Kako internet stvari (IoT) vpliva na spletno varnost uporabnikov?

Internet stvari spreminja naša gospodinjstva in ocenjuje se, da se bodo v prihodnjih desetletjih celotna gospodinjstva (tako imenovani "pametni domovi") povezala z internetom. Zbrali bodo ogromno občutljivih podatkov o prebivalcih gospodinjstva. To je dragoceno blago, zlasti za spletne kriminalce, ki lahko take podatke ukradejo in prodajo ter zlorabijo za sledenje žrtvam. Najslabši scenarij je, da dobijo nadzor nad celotnim pametnim domom.

To ni znanstvenafantastika- tovrstne ranljivosti so odkrili skoraj v vsaki napravi, ki so jo preizkusili strokovnjaki za spletno varnost. Nekatere naprave trpijo zaradi resnih težav - uporabljajo šibko geslo ali ga sploh ne uporabljajo, shranjenih podatkov ne šifrirajo - druge pa tvorijo osrednje točke pametnih domov in v primeru uhajanja podatkov ali ranljivosti lahko predstavljajo veliko tveganje zasebnosti njihovih lastnikov.

DOBER PRIKAZ, kakšne ranljivosti lahko povzročimo, je prikazan v uvodnem prizoru priljubljene televizijske oddaje Mr. Robot (2. sezona, 1. epizoda)[47].

Ali moram pokrivati svojo spletno kamero?

Prenosniki, pametni telefoni in tablični računalniki so običajno opremljeni s kamerami. Ta tehnologija dodaja video telefonskim klicem in poenostavlja dodajanje novih fotografij na družbenih omrežjih, forumih za klepet ali v vašo osebno zbirko.

Vendar ima to tudi svojo slabost. Obstaja tveganje, da bo nekdo te tehnologije zlorabil proti lastniku naprave. Napadalci so vedno znova dokazali, da je spletna kamera lahko koristno orodje za sledenje žrtvam. Ta učinek se še pomnoži z dejstvom, da mnogi uporabniki skoraj ves čas držijo svoje pametne telefone na dosegu roke.

Zdi se, da je zaščita kamer glavni poudarek številnih vodilnih tehnoloških osebnosti, med njimi tudi ustanovitelja in vodje Facebooka Marka Zuckerberga. Zuckerberg je leta 2016 objavil to fotografijo[48], kjer v ozadju vidite, da ima njegov računalnik prelepljen priključek za kamero in mikrofon.

Čeprav nimajo vsi tako dragocenih informacij, kot je direktor Facebooka, so lahko tudi zasebne ali intimne fotografije dragocene za napadalce. Uporabljajo jih lahko za izsiljevanje žrtev z grožnjo, da jih bodo objavili ali prodali na temnem spletu (str. 68).

47 https://youtu.be/aAj8zHOEfiI

48 https://www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook

Vendar ta oblika napada zahteva sodelovanje žrtve. Napadalec jih mora prepričati ali z njimi manipulirati, da v svojo napravo namestijo zlonamerno aplikacijo. Taka aplikacija lahko nato aktivira kamero ali zbere starejše slike in jih pošlje napadalcu. V večini objavljenih primerov je imel napadalec celo fizični dostop do naprave in nanjo ročno namestil vohunsko programsko opremo.

Da bi se temu scenariju izognili:

- Pokrijte kamero na napravi. Nekateri računalniki to funkcijo ponujajo privzeto, če pa je ne, je priporočljivo, da fotoaparat prelepite z neprozornim lepilnim trakom ali posebnim pokrovom.
- Uporabite zanesljivo varnostno programsko opremo, ki lahko zaščiti kamero in prepreči kakršne koli poskuse zlorabe kamere.
- Prepričajte se, da je fotoaparat izklopljen in ne beleži dogajanja okoli njega. Redno preverjajte tudi, katerim aplikacijam in programom v napravi je dovoljen za dostop do kamere in slik.
- Ko napravo z vgrajeno kamero odložite, jo postavite tako, da ne bo pokazala občutljivih predelov sobe ali stanovanja. Kamera ne sme biti usmerjena npr. na posteljo, v kopalnico ali druge prostore, kjer bi lahko nenamerno posneli intimne slike.
- Izogibajte se tudi fotografiranju z intimno vsebino, ki lahko pride v napačne roke. Najstniki bi morali imeti v mislih, da takšnih slik ni priporočljivo deliti s svojim trenutnim partnerjem, saj lahko slike, v primeru razhoda, končajo v napačnih rokah ali na internetu.

Ko gre za spletne kamere (in druge grožnje spletne varnosti), bi morali učitelji in starši biti vzor in upoštevati pravila, tako kot učenci in otroci.

Gesla

šifrirna fraza | dvofaktorska avtentikacija | geslo | upravitelj gesel | napad s surovo silo | večfaktorska avtentikacija

Teme zajete v tem poglavju:

Kaj je geslo?
Kakšno je dobro geslo?
Kaj lahko storite, če imate preveč gesel?
Kaj lahko uporabite namesto gesla?
Kaj je dvo- / večfaktorska avtentikacija?
Kako napadalci ukradejo gesla?

Kaj je geslo?

Geslo je skrivna koda, beseda, besedna zveza, stavek ali zaporedje znakov, ki je znana samo uporabniku in se uporablja skupaj z uporabniškim imenom za identifikacijo uporabnika pri prijavi v digitalne naprave, sisteme ali storitve.

Kakšno je dobro geslo?

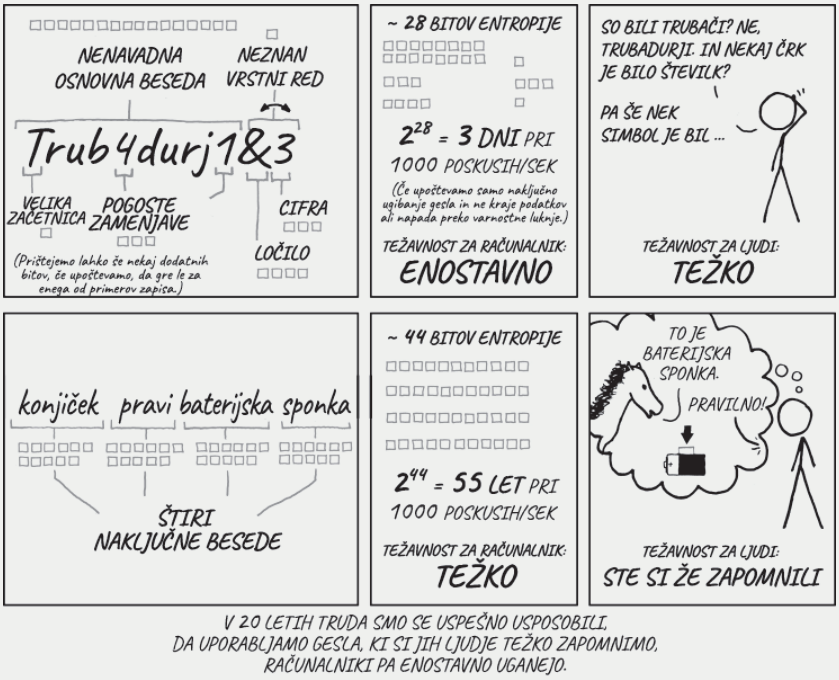
Dobro geslo mora izpolnjevati več meril. Lastnosti dobrega gesla:

- **Je skrivnost —** poznana samo uporabniku[49].
- **Je edinstven —** vsaka storitev ali naprava mora biti zaščitena z drugačnim geslom, tako da če nekdo ukrade enega od njih, ne bo imel dostopa do vseh računov / naprav.
- **Je dolgo —** sestavljen je iz najmanj 8 znakov, v idealnem primeru 16 ali več. Dobra možnost so varnostni stavki, kot je opisano spodaj.
- **Je težko za uganit —** ne sme vsebovati preprostih nizov številk, kot je „123456“, ali preprostih besed, kot je „geslo“. Napadalci lahko tudi zlahka uganejo priljubljene citate iz knjig ali filmov, besede iz slovarja ali kombinacije uporabniških podatkov, npr. „imepriimekleto“. Podatki, ki jih vsebuje takšno geslo, so pogosto na voljo na družbenih omrežjih in kadar uporabnikova varnost ni pravilno nastavljena, jih napadalci lahko zberejo in z njimi ugibajo gesla.
- **Ni del prejšnjega uhajanja ali kraje podatkov —** to je mogoče preveriti s pomočjo storitev, kot je Have I Been Pwned[50].
- **Pretirana kompleksnost ni potrebna —** prej so uporabnikom svetovali, naj gesla ustvarijo z uporabo številk, malih in velikih črk ter posebnih znakov (npr. @, #, $,%). Vendar je ta nasvet nadomestila najnovejša izdaja smernic in zahtev za gesla[51], ki jih je objavil Ameriški nacionalni inštitut za standarde in tehnologijo (NIST).
- **Sestavljen je iz varnostne fraze —** stavek ali fraza (vključno s presledki), ki si ga uporabnik zlahka zapomni in je dovolj dolg in zapleten, zato ga je nemogoče uganiti. Primer dobrega varnostnega stavka je ang. “Nobody can t8ke w#at you already ate”, saj vsebuje 36 znakov, vsebuje presledke, male in velike črke, številko, poseben znak in si ga je enostavno zapomnit.[52]

NAMIG:
Seznam sto najhujših gesel, ki so pricurljali po internetu, vsako leto objavi TeamID (2018[53], 2017[54], 2016[55], 2015[56], 2014[57]).

49 V primeru majhnih otrok je treba gesla deliti z otrokovimi starši ali jih ustvariti z njihovo pomočjo.
50 https://haveibeenpwned.com
51 https://pages.nist.gov/800-63-3/sp800-63b.html
52 Na žalost tudi objava primera v tem priročniku pomeni, da geslo ni več varno, ker ga bo marsikdo videl in z lahkoto uganil.
53 https://www.teampassword.com/blog/worst-passwords-of-2018
54 https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf
55 https://www.teamsid.com/worst-passwords-2016
56 https://www.teamsid.com/worst-passwords-2015
57 https://www.teamsid.com/worst-passwords-of-2014

Strip na xkcd.com/936 lahko uporabimo kot demonstracijo primernega postopka za ustvarjanje močnega gesla:



Kaj lahko storite, če imate preveč gesel in se jih ne morete spomniti?

Priporočamo uporabo aplikacije, imenovane upravitelj gesel. Shrani lahko ne le vsa uporabniška gesla, ampak ta seznam zaščiti z dodatnim geslom in jih tudi šifrira. Pri izbiri upravitelja gesel morate biti previdni pred goljufijami in iskati zaupanja vredne blagovne znamke z dobrim ugledom in preverjeno varnostjo — na primer Sticky Password, KeePass ali LastPass. Nekateri operacijski sistemi ponujajo vgrajen upravitelj gesel - npr. Keychain v sistemu MacOS.

Kaj lahko uporabite namesto gesla?

Gesla zdaj nadomešča biometrična identifikacija - npr. skeniranje uporabnikovega prstnega odtisa ali obraza. Če ti ne uspejo, običajno za varnostno kopijo uporabijo številčno kodo PIN.

Na splošno so gesla običajno zavarovana z dodajanjem novega preverjanja / koraka, s katerim se zagotovi, da je geslo vnesel pooblaščeni posameznik. To se imenuje **dvofaktorska** ali **večfaktorska avtentikacija**. Ta oblika preverjanja ima lahko več oblik:

- **Uporaba druge komunikacijske poti** — na uporabnikov mobilni telefon se pošlje SMS s preverjanjem.
- **Uporaba drugih, predhodno dogovorjenih kod** — npr. fizična kartica, ki vsebuje matrico kod, med katero je naključno izbrana ena, ki jo mora uporabnik nato vnesti na spletnem mestu ali v aplikaciji; ali elektronski čitalnik - strojna naprava, ki ustvari edinstveno kodo za uporabnika, ki jo lahko preveri druga stranka.

- **Uporaba posebne aplikacije, ki ustvarja kode, ki potečejo —** koda običajno velja omejeno obdobje, npr. 30 sekund. Po poteku roka se koda spremeni in original izgubi veljavnost. To bistveno skrajša čas za napad in dodatno izboljša varnost gesla. Vendar pa je te aplikacije mogoče uporabljati samo z nekaterimi spletnimi storitvami. Dva primera razmeroma univerzalne rešitve sta Google Authenticator in Microsoft Authenticator.

Tu je nekaj nespodbudnih primerov, ki jih učitelj lahko predstavi (glede na resnično življenje):

Dekle je uporabljalo Facebook račun z geslom, ki ga je enostavno uganiti. Poleg tega se je na potovanju v tujino prijavila v nezavarovano omrežje Wi-Fi, kjer je napadalec verjetno prestregel njeno geslo. S pomočjo teh informacij mu je uspel vdor v račun in ukrasti zasebne fotografije, ki jih je izmenjala s svojim fantom. Nato jo je izsiljeval in ji zagrozil, da bo objavil slike, razen če bo plačala odkupnino. Ko je zavrnila, je fotografije poslal vsem njenim skupinam Messenger.

Žrtev je imela v svojem podjetju e-poštni strežnik, zaščiten s preprostim geslom. Bil je javno dostopen sistem, napadalec pa ga je našel v internetu in izničil geslo. Nato je še naprej pošiljal zlonamerna e-poštna sporočila in neprimerne oglase vsem stikom v imeniku.

Kako napadalci kradejo gesla?

Geslo žrtve lahko napadalec pridobi na več načinov:

1. **Tako, da jih opazuje —** to se morda sliši absurdno, toda napadalci gesla pogosto dobijo tako, da pogledajo žrtev čez ramo ali jih posnamejo na video. To velja tako za prijavo v spletne storitve kot tudi za naprave.

    a. Video posnetek: https://youtu.be/e9CfWK-uN44 — koda je dolga in zapletena, a ko je objavljena na internetu, uporabnika ne more več zanesljivo zaščititi.

2. **Socialni inženiring —** napadalec manipulira ali prevara žrtev, da ji da geslo. Za to lahko uporabijo ponarejeno spletno stran, e-poštno sporočilo po meri ali sporočilo socialnega omrežja, kjer se pretvarjajo, da so zaupanja vredna oseba / institucija, ali se pretvarjajo, da zahteva izvira iz banke / družbenega omrežja / spletne storitve.

3. **Zlonamerna koda —** napadalec žrtvino napravo okuži z zlonamerno programsko opremo (npr. z uporabo ranljivosti programske opreme, socialnega inženiringa, okuženega spletnega mesta itd.), ki je bila ustvarjena posebej za prepoznavanje, nadzor in krajo gesel ter njihovo pošiljanje napadalcu.

4. **Napad omrežne komunikacije —** napadalec lahko prestreže žrtvine podatke na omrežni ravni. Če se napadalec odloči za to v javnem omrežju Wi-Fi, mora biti v večini primerov v bližini žrtve, Wi-Fi pa mora delovati po zastarelem varnostnem protokolu. Podoben napad pa lahko izvedemo tudi z zlonamerno kodo - v tem primeru napadalcu ni treba biti prisoten.

5. **Ugibanje (tako imenovani napad s surovo močjo) —** ena najpogosteje uporabljenih taktik. Napadalec ugiba pogosto uporabljena ali prednastavljena gesla in uporablja slovarje ali znane besedne zveze. V ta namen uporabljajo posebno kodo ali celotne naprave, ki lahko v nekaj sekundah uganejo na tisoče gesel. To jim omogoča enostaven in hiter vdor v račun s šibkim ali kratkim geslom. Na primer, šifro, sestavljeno iz štirih znakov in številk, lahko napadalec ugane skoraj takoj.

    a. Primera kalkulatorjev moči gesel:

    http://lastbit.com/pswcalc.asp

    https://tmedweb.tulane.edu/content_open/bfcalc.php

Posodobitve

posodobitev | strojna koda | operacijski sistem | popravek

Teme zajete v tem poglavju:

Kaj so posodobitve in kako lahko uporabnik ve, da je treba posodobiti del programske opreme?

Zakaj so posodobitve pomembne?

Zakaj ne bi smeli preložiti posodobitev?

Bi morali uporabljati avtomatske posodobitve?

Kateri programi in deli naprave morajo biti redno posodabljati?

Kaj so posodobitve in kako lahko uporabnik ve, da je treba posodobiti del programske opreme?

Posodobitve so nove različice programske opreme ali njeni deli. Posodobitve pogosto odpravijo napake programske opreme in izboljšajo varnost aplikacije.

Prej ali slej bo vsak uporabnik digitalne naprave naletel na posodobitve. Operacijski sistem ali aplikacija jih bo obvestila o potrebi po posodobitvi, običajno s pomočjo pojavnega okna / obvestila. Ko je posodobitev končana, bo morda treba napravo znova zagnati.

Nekatere posodobitve se imenujejo tudi popravki, ker popravljajo "varnostne luknje". Druge posodobitve (npr. posodobitve varnostne programske opreme) posodabljajo samo izbrane zbirke podatkov ali dodajajo nove funkcije. V slovenščini jih večinoma imenujejo "posodobitve" ali "popravki".

Zakaj so posodobitve pomembne?

Poznamo različne posodobitve. Z vidika varnosti odpravljajo ranljivosti in izboljšujejo varnost aplikacij, uporabnikov in naprav. Drug namen posodobitve je odpraviti težave, o katerih poročajo uporabniki - npr. nepravilno delovanje gumbov, manjkajoče funkcije itd. - s tem se izboljša zmogljivost in uporabniška vrednost.

Večje posodobitve aplikacij ali operacijskega sistema, ki vključujejo prehod na novejšo različico, pogosto vključujejo druge ugodnosti v obliki novih funkcij, izboljšanega vmesnika in možnosti, ki omogočajo aplikacijo ali operacijski sistem, privlačnejši za uporabnike.

Zakaj ne bi smeli odložiti posodobitev?

Pojavna okna, ki vas obvestijo o posodobitvi, običajno vključujejo možnost, da posodobitev prestavite za nekaj minut, ur ali dni. Žal se uporabniki pogosto odločijo za čim daljšo zamudo, saj v tem trenutku nočejo biti zadržani. Posodobitev pa lahko odpravi kritično varnost ali drugo težavo, povezano s programom / napravo, in je ne bi smeli odlagati.

Zaradi spletne kriminalitete je treba vso programsko opremo posodobiti čim prej. Napadalci običajno skušajo izkoristiti znane ranljivosti programske opreme, da pridobijo nadzor nad žrtvino napravo. Dlje kot odložite posodobitev, večje je tveganje, da bo kdo zlorabil ranljivost.

Bi morali uporabljati samodejne posodobitve?

Dobra možnost za posodobitev naprav in skladnost z najnovejšimi varnostnimi standardi je aktiviranje samodejnih posodobitev. Lahko jih na primer vedno namestite ob koncu dneva ali tik pred izklopom naprave. Samodejne posodobitve lahko običajno omogočite neposredno v pojavnem oknu, ki se prikaže uporabniku, ali v nastavitvah naprave.

Katere programe in dele naprave je treba redno posodabljati?

Vse operacijske sisteme je treba posodobiti. Med najbolj priljubljenimi so Windows, MacOS, Linux, iOS in Android.

Posodobitve je treba namestiti tudi za vse programe, ki se izvajajo v napravi, vključno z internetnim brskalnikom, predvajalnikom glasbe, grafičnimi urejevalniki ali igrami. V nekaterih primerih je treba posodobiti tudi tako imenovano vdelano programsko opremo - npr. nizkorazredna programska oprema, ki deluje pod operacijskim sistemom in zagotavlja pravilno delovanje vseh komponent strojne opreme.

Slovarček

Ta priročnik vsebuje nekatere specifične izraze povezane z IT varnostjo. Za lažje sklicevanje in razumevanje bralcem priporočamo, da se z njimi seznanijo pred uporabo tega priročnika. V spodnjem slovarčku boste našli tudi razlage nekaterih izrazov, ki so zaradi njihove prekomerne pojavnosti v medijih izgubili del svojega pomena, ki je po našem mnenju ključen.

Napadalec / spletni kriminalec

Ker zlonamerni hekerji tvorijo samo podskupino te skupine, so izrazi napadalec ali spletni kriminalec veliko bolj primerni in zato jih uporabljamo v celotnem priročniku.

Spletno ustrahovanje — zloraba interneta in digitalnih tehnologij za namerno in sistematično povzročanje škodo drugim.

Spletno sovraštvo — kakršnakoli uporaba elektronske komunikacije za napad na druge zaradi rase, narodnosti, jezika, polti, verskih prepričanj, spolne usmerjenosti, politične pripadnosti, starosti ali duševnega in fizičnega zdravja ter razširjanje sovražnega govora.

Spletno nadlegovanje — ponavljajoča se in dolgotrajna zloraba digitalnih tehnologij za zalezovanje in nadlegovanje drugih uporabnikov, kar je običajno zelo zastrašujoče in žrtvi odvzame občutek varnosti. Vključuje lahko grožnje z fizičnimi poškodbami, lažne obtožbe, poškodovanje podatkov ali krajo identitete, spremljanje računalnika žrtve in podobno. Intenzivnost nadlegovanja se običajno poveča in se ne ustavi, tudi če je napadalec pozvan, da se ustavi ali tudi potem, ko jih žrtev blokira. Iz spletnega okolja se pogosto širi v realni svet.

Dezinhibicijski učinek — izguba zavor in zadrževanja v spletnem okolju zaradi občutka anonimnost. Posledično so ljudje pri spletnem komuniciranju pogosto bolj pogumni, pa tudi bolj agresivni in si upajo početi stvari, ki jih z nekom nikoli ne bi naredili iz oči v oči. Ta učinek se nanaša na spletno ustrahovanje, trolanje in spletno sovraštvo.

Heker

V širši javnosti ima beseda heker negativen prizvok – IT strokovnjaki pa jih ne poimenujejo tako. Beseda opisuje posameznika, ki poskuša najti novo ali izvirno uporabo za sistem (programska / strojna oprema) ali del, ki se popolnoma razlikuje od prvotnega namena. Na splošno lahko hekerje razdelimo v tri kategorije: etični hekerji (beli klobuk), tisti, ki delujejo v sivi coni (siva kapa) in tiste z očitno zlonamernimi nameni (črna kapa).

Na splošno je heker lahko tudi oseba, ki razstavi radio in namesto da prejema signale in posluša glasbo to uporablja kot oddajnik in moti signal. Etični hekerji skušajo najti šibke točke v sistemih organizacije s ciljem obvestiti lastnika in mu pomagati odpraviti težavo. Ta postopek se imenuje tudi ***penetracijsko testiranje.***

Vdiranje ang. hacking

Spletni kriminalci v filmih pogosto potrebujejo le internetno povezavo in v nekaj minutah (ali celo sekundah) lahko dostopajo do katerega koli sistema - ne glede na to, ali gre za elektronsko ključavnico vrat, notranje omrežje tajne službe ali policije ali nadzor prometnih kamer. Zapletenost današnjega sistema je taka, da bi takšna dejanja kriminalcem vzela tedne ali morda mesece, ker se morajo najprej seznaniti z notranjim delovanjem sistema in šele nato lahko začnejo dosegati svoj cilj. Vdiranje je pogosto dolgoročna in ciljno usmerjena dejavnost, pri kateri heker (etični heker ali napadalec) poskuša najti ranljivosti v danem sistemu in poroča (etično) ali jih izkoristi (napadalec).

Veselo klofutanje – "klofutanje iz zabave" je nova oblika slabega ravnanja, ki združuje ustrahovanje iz oči v oči s spletnim ustrahovanjem. Agresor fizično napade žrtev, medtem ko incident zabeleži na mobilni telefon. Posneti video se nato naloži na internet ali v sporočilih razširi med vrstnike. V mnogih primerih napadalca predstavlja skupina, ki se zabava in spodbuja drug drugega pri škodovanju žrtvi.

Zlonamerna programska oprema / zlonamerna koda

Beseda zlonamerna programska oprema je združitev besed „zlonamerno" in „programska oprema". Dobesedno označuje računalniško kodo ali njen del, ki je bil ustvarjen za škodo. Zlonamerna programska oprema je ime za (računalniške) viruse, pa tudi številne druge kategorije zlonamerne kode.

Socialni inženiring

To je kategorija napadov, ki skoraj ne zahtevajo tehničnega znanja. Z uporaba socialnega inženiringa, napadalci poskušajo prevarati ali manipulirati z njihovimi žrtvami, da kršijo določena varnostna pravila. Njihov cilj je žrtev pretentati, da odpre nevarno ali ponarejeno spletno stran in iz nje pridobiti občutljive podatke, jih prestrašiti, da bi namestili neželeno / nevarno aplikacijo ali drugo škodljivo programsko opremo. Ta vrsta napada izkorišča človeško nevednost in / ali šibkost.

Nezaželena pošta in lažno predstavljanje (phishing)

Nezaželena ali vsiljena pošta je vsako nezaželeno elektronsko sporočilo, npr. e-pošta, SMS sporočilo, sporočilo v programu za hitro sporočanje ali klepetalniku.

Lažno predstavljanje (phishing) je goljufiv poskus pridobivanja občutljivih informacij in podatkov, v katerem se napadalci prikažejo kot zaupanja vreden subjekt, služba ali oseba, Napad z lažnim predstavljanjem je lahko tudi v obliki e-pošte, na katero naj bi žrtev odgovorila ali povezava do spletnega mesta, ki je videti kot original, npr. spletno mesto družbenega omrežja, e-poštno sporočilo ali storitev spletnega bančništva. Povezave do spletnih mest z lažnim predstavljanjem se pogosto širijo po e-pošti, klepetu in družbenih omrežjih ali sporočilih SMS. Učitelji in učenci si lahko ogledajo phishing teste, ki so na voljo na spletu.

Razkritje — objava žrtvinih zasebnih ali intimnih informacij na internetu brez njenega soglasja.

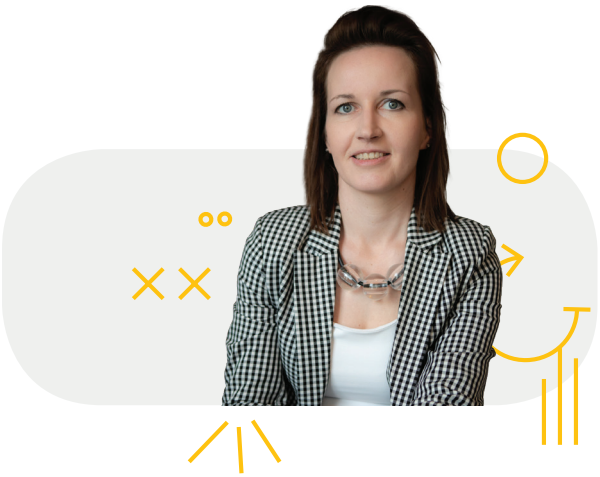
Trol — uporabnik interneta, katerega cilj je sprožiti močan odziv in namerno moti ali ovira razpravo in objavlja agresivna sporočila.

Trolanje — spletna komunikacija, katere namen je spodbujati spore in argumente, izzivati, žaliti, lagati in na splošno uvajanje kaosa v komunikacijo.

O avtorjih

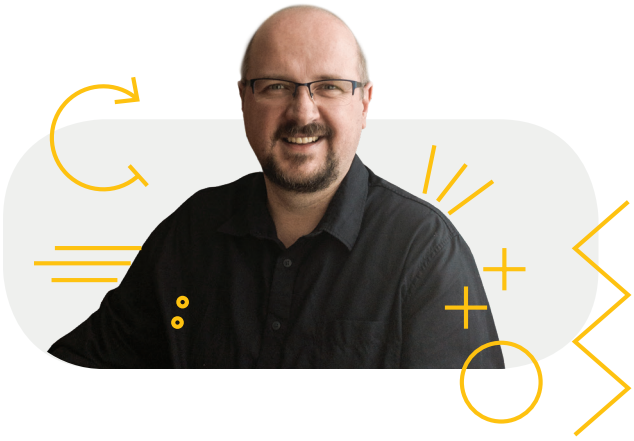
Ondrej Kubovič, strokovnjak za varnostno ozaveščanje

Ondrej je v ESET-u delal kot strokovnjak za ozaveščanje o varnosti, zato mora slediti in pisati o tem ter ozaveščati o najnovejših grožnjah spletne varnosti. Je strokovnjak za to temo, mnogo tveganj vidi tudi skozi oči svojih dveh mladih nečakinj, ki sta že del današnjega digitalnega sveta preko računov na družbenih omrežjih njunih staršev. Je član ekipe, ki je sutvarjala materiale za projekt Digital Skills, ki slovaškim šolam ponuja usposabljanje in dodatne informacije o spletni varnosti. Ondrej upa, da bomo kljub vsemu zlonamernemu delovanju, ki ga je zaznala raziskava ESET, otrokom omogočili prijetnejše in kar je najpomembnejše, varne spletne izkušnje.



dr. Jarmila Tomková, psihologinja

Jarmila je na Slovaškem izjemno cenjena psihologinja. Delala je na raziskovalnem inštitutu za otroke psihologije in patopsihologije, kjer je vodila raziskovalne skupine, ki so preučevale priložnosti in tveganja otrok ob uporabi interneta. Koordinirala je slovaško ekipo EU Kids Online, večnacionalne raziskovalne mreže. Delala je tudi kot šolska psihologinja, kjer je zasnovala in izvedla več razvojnih dosežkov in preventivne programe, kot je učenci proti ustrahovanju. Jarmila še naprej deluje kot svetovalka za organizacije in šole pri preprečevanju negativnega vedenja, kot sta ustrahovanje in sovražni govor. Prav tako je ustanovila in vodi civilno združenje ViaSua, ki je namenjeno podpori duševnega zdravja in osebnostne rasti posameznikov, družin in družbe na splošno. To dosega s svetovanjem, ozaveščanjem in destigmatizacijo o problematiki duševnega zdravja. Meni, da sta jezik in diskurz ključnega pomena.



Peter Kučera, učitelj računalništva

Peter je učitelj računalništva na gimnaziji v Bratislavi (1. Sukromne Gymnazium v Bratislave) in avtor več učbenikov. Skrbi za kakovost izobraževanja na tem področju, ne samo v šoli, kjer poučuje, ampak v vseh delih družbe. Prav tako poučuje praktiven pouk za študente s področja računalništva na Fakulteti za matematiko, fiziko in informatiko Univerze Comenius v Bratislavi.

Ustvaril je vrsto učbenikov z naslovom Ustvarjanje s Pythonom, ki vključuje učiteljske vodnike in izvaja Python tečaje za učitelje. Peter je ustanovil in vodi Klub računalništva učiteljev naravoslovja, ki deluje kot platforma za izmenjavo izkušenj in uvajanje novih tem. Skupnost učiteljev v klubu se skupaj odziva na trenutni razvoj na področju digitalne tehnologije in prinaša nove teme in predloge strokovnjakov za učitelje in študente.

Po njegovem mnenju je digitalna varnost ključna tema današnjega spletnega obdobja. S hitrim razvojem tehnologije je težko spremljati spremembe in se nanje odzivati z zadostno prilagodljivostjo. Ravno zato je učiteljem in študentom pomembno pomagati pri izobraževanju in usposabljanju na tem področju.

Jakub Daubner, vodja notranjih sistemov

Jakub je v naravoslovju užival že od otroštva, zato se je odločil za študij teoretičnega računalništva in uporabne računalniške znanosti. Vzporedno s študijem se je pridružil ESET-u, kjer je v 10 letih uspel zgraditi oddelek z 45 razvijalci. Njegova ekipa se osredotoča predvsem na razvoj notranjih orodij in avtomatskih sistemov. Delavnica je pripravila tudi detekcijski modul, ki temelji na strojnem učenju in umetni intelegenci. Poleg tega vodi programersko skupino učencev na osnovni šoll in z Ondrejem Kubovičem sodeluje pri projektu Digital Skills, v katerem izdelujejo izobraževalna gradiva in usposabljajo učitelje.

Informacije v tej publikaciji so informativne narave in se lahko spremenijo brez predhodnega obvestila, za podjetji ESET, spol. s r.o. ter SI SPLET d.o.o. pa niso zavezujoče. Podjetji tudi ne prevzemata odgovornosti za morebitne napake ali netočnosti, ki se morda pojavijo v tej publikaciji.

saferkidsonline by ESET

ISBN 978-961-95405-0-3