

Virtualna (ne)varnost

✉ Klemen Jevnikar



Danes se ob uporabi izrazov glede svetovnega spleta hitro zapletemo in včasih niti ne vemo, o čem pravzaprav govorimo. Besedilo, ki sledi, je namenjeno vsem področjem sodobnih tehnologij, ki nam ponujajo vstop v kakršno koli virtualno resničnost – preko vseh naprav, ki omogočajo dostop do svetovnega spleta: osebni računalniki vseh vrst, telefoni (število teh naprav se nenehno povečuje).

Virtualnost

Namenoma uporabljam izraz *virtualnost* (tj. nekaj, kar naj bi obstajalo, vendar ni realno¹), saj verjamem, da se npr. uporabniki družabnih omrežij nadejajo pristnih medčloveških odnosov, čeprav jih večinoma ne vzpostavijo. Virtualno oz. navidezno resničnost sicer bolj prepoznamo kot okolje, ki ga ustvarijo različne naprave (obleke, očala ...), ki tudi preko interaktivnosti posnemajo realnost in omogočajo navidezno prisotnost. A tudi brez vsega tega je občutek prisotnosti lahko zelo močan že pri kakšni spletni igri, npr. *Second Life*².

Da se na 'bivanje' v virtualnih svetovih še zdaleč nismo navadili, ni treba razlagati. Gre za del življenja, ki nam ni dan od nekdanj; za življenje, za katerega nismo dobili nobenega nasveta preteklih generacij. Od tod vsekakor izhaja nekaj razlogov, zakaj tega življenja niti ne obvladamo.

Vsekakor je najbolj zaskrbljujoče neobvladovanje varnosti. Seveda lahko rečemo, da tudi v realnosti nismo

popolnoma varni. A v tem 'stvarnem' življenju kar veliko vemo o tveganjih. Tudi otroke poučujemo o varnosti na cesti, varovanju zdravja, zdravi prehrani, varnosti pred naravnimi nesrečami ...

Otroke torej starejši poučujemo o nevarnostih, ki prežijo v življenju. Starejše generacije so bile vedno poklicane, da mlajše poučijo o življenju. V našem primeru je to popolnoma nemogoče. Vendar izkušnja prihoda novih načinov komunikacije spremlja vse dosežanje generacije (npr. časopis, radio, televizija, telefon); vsi novi načini so bili šokantni in razburljivi. Lahko bi rekli: zgodovina se vendarle ponavlja. Ne bodimo torej neomajni nasprotniki, zvišeni kritizerji. Vse preizkušajmo, in kar je dobro, obdržimo.³

Menim pa, da obstajajo le redki starši, ki vedo o dogajanju na svetovnem spletu več od svojega sina/hčerke – starejšega osnovnošolca ali srednješolca. Kako bomo torej na tem področju poučevali in vzgajali svoje otroke?

Realnost

Vse le ni tako brezizhodno. Naša naloga sicer ni lahka, a ob zavedanju, da moramo ukrepati čim prej, bomo uspešni. Virtualnost posnema okolje, odnose, človeške lastnosti idr. iz realnega življenja. To je naše izhodišče.

Najprej se moramo poučiti o tehnologiji, o načinih komunikacije, navadah, nevarnostih. Tudi tu je prvo pravilo: pogovarjajmo se, sprašujmo, poslušajmo. Navadno to pričakujemo od otrok, a naši otroci bodo ponosni, če bomo tako pokazali zanimanje za njihovo življenje. Sodelujmo in opazujmo, kaj otroci počnejo.

Eno izmed konkretnih pravil je, da v družini (tudi v šoli, knjižnici) računalnik postavimo v skupni prostor.

Če računalnik uporabljamo v službene namene, za spletno bančništvo ali kaj drugega, pri čemer je možnost, da se povzroči večja škoda, naj otroci uporabljajo drug računalnik. Ob tem pa ne pozabimo, da ima večina otrok dostop do spleta tudi preko svojega mobilnega telefona. Tam z omejitvijo že pri samem paketu določimo ali pa sproti spremljamo promet dostopa do omrežja. Če imamo doma urejeno

“ *Nikakršno kasnejše brisanje ne bo pomagalo: kar se enkrat znajde na spletu, tam za vedno ostane.* ”

brezžično omrežje, lahko telefonski dostop do njega otroku omejimo z geslom, ki ga ne pozna. Vendar ne pozabimo, da gre lahko tu zgodba že naprej. Če ima otrok svoj telefon, lahko uporabi odprto omrežje v svoji okolici in brezplačno ter nenadzorovano dostopa do spleta.

Zgolj s prepovedjo torej ne bomo prišli daleč. Z otroki raje skupaj sestavimo pravila, ki se jih bomo držali vsi. Tako bomo pripomogli k varnosti, zaupanju ter bistveno zmanjšali možnost neprimerne uporabe in zasojenosti. Predstaviti jim moramo nevarnosti, ki prežijo na spletu.

Nevarnosti, o katerih moramo spregovoriti

Na spletu se lahko pojavimo s polnim imenom (kadar se prijavimo npr. v spletno banko), z vzdevkom (npr. na forumih) ali pa smo anonimni (npr. pri pregledovanju). Te možnosti izkoristimo sebi v prid in ne posredujmo svojih osebnih podatkov, kadar to ni potrebno. Na drugi strani pa se zavedajmo, da so na spletu prisotni tudi ljudje, ki splet izkoriščajo

v slabe namene (nelegalni zaslužek, izkoriščanje, kraja, zloraba ...). Lahko se skrivajo za lažno identiteto (nekdo se predstavlja kot direktor podjetja, drugi kot 12-letno dekle ...). Zato velja: komunicirajmo le z ljudmi, ki jih poznamo. Če torej ne poznamo identitete sogovornika(ov), vsekakor ne dajajmo osebnih podatkov in se ne spuščajmo v osebne teme. Otrokom pomagajmo pri ustvarjanju vzdevkov in varnih gesel, vendar ne vztrajajmo pri poznavanju le-teh. Navadimo jih, da bodo spoštovali zasebnost drugih, hkrati pa se zavedali možnosti zlorabe.

omrežji, celo s posameznimi spletnimi igrami). Skrajne oblike teh zasvojenosti peljejo v odtujenost, odsotnost fizičnih stikov, odsotnost gibanja v naravi, fizično izčrpanost, neprimerne prehranjevalne navade ... Skupaj postavimo pravila (dnevni red, omejitev), v primeru zasvojenosti poiščimo strokovno pomoč. Najboljše preventivno zdravilo pri tem je zgled!

Družabna omrežja (najbolj uporabljeno tako omrežje je Facebook) so za lastnike teh omrežij zbirka podatkov. Sicer obstaja t. i. politika zasebnosti, ki se ji lastniki teh podatkov zavežejo,

in poškoduje. Ozaveščenost je torej ključnega pomena.

Tehnična varnost

Tehnični varnosti pogosto posvečamo več pozornosti. Prav tako bomo o slednji na spletu našli mnogo več informacij in nasvetov kot o osebni varnosti. Seveda sta področji močno povezani, ob upoštevanju nasvetov z obeh strani pa bomo največ naredili za svojo varnost in tako bili zgled drugim.

Nasveti za tehnično varnost so mnogo bolj konkretni in operativno usmerjeni. Skoraj vsak pozna izraze, kot so: računalniški virus, črv, trojanski konj, vohunski programi ter ostala zlonamerna programska oprema. Tako tudi večina poskrbi, da ima na svojem računalniku protivirusni, protivohunski program, ter uporablja požarni zid. Treba je seveda dodati, da moramo poskrbeti, da bo tak protivirusni program redno posodobljen.

Pomisli ti je treba tudi, ali je zaščitena vsak računalnik, s katerim delamo (npr. v službi, knjižnici). Nehote se nam namreč lahko zgodi, da virus z okuženega računalnika prenesemo na svoj osebni računalnik preko prenosnih medijev (npr. USB-ključa, prenosnega trdega diska).

Če želimo zmanjšati možnost okužbe:

- se izogibamo spletnim stranem s sporno vsebino: erotika, stave, strani za izmenjavo piratske opreme in drugih datotek, družabna omrežja;
- ne sledimo pojavnim oknom, povezavam, slikam, ki nas usmerjajo na druge spletne strani (sploh na straneh, na katerih poslušamo, vedno vpisujemo naslov);
- nameščamo le programsko opremo in posodobitve, ki jih potrebujemo oz. uporabljamo, in to le z uradnih in preverjenih strani;
- uporabljamo najvišjo možno zaščito svojega računalnika.

Poleg virusov manj poznamo spletne prevare. Te srečujemo pri brskanju po spletu ter elektronski pošti. Najpogostejše in najnevarnejše so različne prevare, neposredno ali posredno povezane z denarjem (ponujen velik zaslužek ali dobiček, prošnje za po-



Foto: arhiv Socialna akademija

Tudi pri komuniciranju z ljudmi, ki jih poznamo, upoštevajmo pravila bontona ter zdrave mere. Primer neprimerne komunikacije, posebno med mladimi, je v zadnjem času t. i. 'sexting', kjer si partnerja po mobilnem telefonu pošiljata besedilo, slike ali videoposnetke s seksualno vsebino. Seveda si lahko predstavljamo, kaj se lahko zgodi, če se taka partnerja konfliktno razideta. Taka vsebina se pogosto znajde prosto na spletu. Nikakršno kasnejše brisanje ne bo pomagalo: kar se enkrat znajde na spletu, tam za vedno ostane. Če je vsebina privlačna in iskana, pa lahko v nekaj dneh obide svet.

Vsekakor se moramo posvetiti pogovoru o zasvojenosti. Tu je treba omeniti vse: od splošne zasvojenosti z digitalnimi mediji do specifičnih zasvojenosti (zasvojenost z družabnimi

a zavedati se moramo, da se ta politika spreminja. Ko se namreč številno uporabnikov (in s tem podatkov, tj. osebnih in drugih podatkov, slik, videoposnetkov) poveča, si podjetja mnogokrat povečajo pravice do pregledovanja in uporabe teh podatkov: obdelave, prodaje, nadzora. Z otroki se o tem pogovorimo, skupaj pregledamo nastavitve zasebnosti in jih postavimo pred vprašanje: »Ali bi želel, da za to izve cel svet?«

Pogovor o različnih zlorabah se dotika tako realnega kot virtualnega sveta. Na spletu bomo največkrat našli različne oblike spletnega nadlegovanja, izsiljevanje, različne oblike nasilja, krajo identitete, pornografijo, rasizem, terorizem, seksizem ... Nema lokrat zlorabe preidejo iz virtualnega v realni svet; s psihične tudi na fizično raven, kar otroka še bolj zaznamuje

moč). Škodljive pa so lahko tudi lažne spletne strani, kraja identitete, vsiljena pošta, včasih tudi navadna verižna pisma (morda so v njem podatki, ki jih ne bi smeli razkriti oz. posredovati).

Zavarujmo svoja gesla, svojega elektronskega naslova ne posredujmo vsakomur, predvsem pa preverimo vsakršen sum: neznanec nam ponuja zaslužek; nekdo bo prejel denar, če bomo posredovali sporočilo 10 prijateljem; spletna stran banke je nekoliko drugačna kot navadno; vsebina sporočila je skoraj neverjetna. Tak sum lahko najhitreje preverimo tako, da ključne besede iz sporočila ali strani vpišemo v iskalnik ali pobrskamo po straneh zanesljivih ponudnikov antivirusnih programov.

Zaključek

Članek le delno pokriva področje virtualne varnosti. Danes je veliko informacij, poiščemo pa lahko tudi strokovno pomoč pri vprašanjih, na katera ne znamo odgovoriti. Obiščemo lahko delavnico ali tečaj, kjer bomo izvedeli več ter se poučili o varnosti in zaščiti.

Pustimo se poučiti komu, ki o zaščiti in varnosti ve več od nas in mu zaupamo. Naj pregleda naš računalnik in nam svetuje. Če se znajdemo v resnih težavah, ko sumimo, da gre za kršenje zakona, se obrnimo na policijo.

V uporabo priporočam naslednje spletne strani:

- www.safe.si (osveščanje o varni rabi spleta in novih tehnologij);
- www.spletno-oko.si (prijava otroške pornografije in sovražnega govora);
- www.cert.si (center za posredovanje pri omrežnih incidentih);
- www.varninainternetu.si (problematika informacijske varnosti);
- www.varniinternet.si (izobraževanje na področju varnosti na spletu);
- saferinternet.at/chadvice (priročnik za učitelje Avstrijskega inštituta za uporabne telekomunikacije z naslovom Spolnost in nasilje v digitalnih medijih – ni v slovenskem jeziku). ■

Opombe

1. <http://sl.wikipedia.org/wiki/Virtualnost>.
2. http://sl.wikipedia.org/wiki/Second_Life.
3. Sveto pismo, 1 Tes 5,21.

En klik, tisoč posledic

Nekaj pravil varnega vedenja na internetu za otroke in starše

✍ Kristina Lepen

Internet je zanimiv, saj omogoča potovanje v neznano, usvajanje novih spoznanj, pomaga pri učenju; preko njega spoznamo nove prijatelje, lahko si brez težav dopisujemo z mnogimi ljudmi. Internet omogoča svobodo; lahko se igramo, poslušamo glasbo, pri vsem tem pa ni pomembno, koliko smo stari. Ponuja veliko izzivov, ki se jim je težko upreti.

(Ne)varnost interneta

Brskanje po spletu je v zadnjem času izpostavljeno tudi različnim nevarnostim. Za varno brskanje je pomembno, da pri tem sodelujejo otroci oz. mladostniki, starši, učitelji oz. izobraževalne ustanove in država. Varnost brskanja na spletu je predvsem svetovni problem, zato se ga je treba lotevati globalno. Zato je v zadnjem času veliko ozaveščanja in proučevanja problematike varnega brskanja preko anketiranja uporabnikov svetovnega spleta in analize rezultatov.

Internet je med slovenskimi otroki zelo razširjen. Otroci in najstniki ga najraje uporabljajo za klepetanje, dostop do filmov in glasbe ter kot vir informacij za izdelavo različnih šolskih nalog. Internet je realen del v življenju današnjih mladih. Več časa namenijo brskanju po internetu kakor gledanju televizije ali druženju s prijatelji. Moramo pa se zavedati, da 'virtualni' svet vsebuje enake nevarnosti in nevarnosti kot 'realni'. Otroci in mladostniki so najbolj ranljivi uporabniki interneta, saj tehnično sicer računalnik in internet obvladajo do popolnosti, toda zaradi mladosti in

neizkušenosti, pa tudi pretirane radovednosti, se lahko hitro ujamejo v skrivne pasti tega medija.

Nasveti za otroke in mlade

Mladostniki že ogromno vedo o internetu, otroci malo manj, vendar pa bi bilo najboljšo, da bi se še več naučili o varni uporabi interneta sami ali ob pomoči staršev. Za večjo varnost in obenem tudi zabavo z virtualnimi prijatelji je potrebno, da otroci in mladostniki upoštevajo določena pravila pri brskanju po spletu (http://www.safe.si/c/676/TOP_10_NASVETOV/?preid=671):

1. Ko klepetas na internetu, vedno uporabljalj vzdevek.
2. Ne srečuj se z neznanci s spleta (tudi če se ti zdijo v virtualnem svetu tvoji prijatelji).
3. Gesla so skrivnost. Pogosto jih spreminjaj.
4. Spoštuj spletno etiko oz. bonton. Cesar ne želiš, da drugi storijo tebi, tudi ti ne naredi drugim.
5. Nadlegovanje preko interneta ali mobilnega telefona je nedopustno. Staršem povej, če te kdo nadleguje prek spleta ali če naletiš na neprijetno vsebino.
6. Ne odpiraj pošte in priponk od neznancev.
7. Uporabljalj antivirusni program in požarni zid, ko brskaš po spletu.
8. Na spletu ne izdajaj svojih osebnih podatkov, niti podatkov svojih staršev. Ne objavljaj svojih zasebnih fotografij, niti fotografij svojih prijateljev.
9. Z uporabo interneta ne pretiravaj.
10. Z interneta ne prepisuj, vedno navedi vir in avtorja. Preveri tudi druge vire (knjige ...) in ne verjemi, da je vse, kar piše na internetu, tudi res.