SVEUČILIŠTE U SPLITU
PRIRODOSLOVNO – MATEMATIČKI FAKULTET

Završni preddiplomski rad

SIGURNOST RADA NA RAČUNALU

Mentor :
dr.sc. Ani Grubišić

Student:
Marija Prolić
st. gr. Informatika

Split, listopad 2012.

Sadržaj

1 UVOD

Pojam računalne sigurnosti posljednjih se godina sve više prepoznaje i izvan stručnih krugova. Polako uviđamo kako korištenje računala na globalnoj mreži sa sobom nosi niz odgovornosti i sigurnosnih pravila. Zašto je uopće globalna mreža u tolikoj mjeri preplavljena opasnim i neželjenim sadržajem? Kome je i zašto zanimljivo naše kućno računalo? Naše je računalo, kada ga spojimo na Internet, dostupno svim drugim računalima spojenim na Internet, komunicirali mi s njima ili ne. Internet je mreža u kojoj su svi međusobno povezani. Naše računalo samo po sebi i nije posebno zanimljivo, no tisuće takvih kao što je naše predstavljaju velike resurse s kojima se štošta može napraviti. Ljudi kojima je zanimljivo naše računalo nazivaju se i računalni kriminalci (često nazivani hakerima ili provalnicima) koji napadaju tuđa računala. Oni mogu napasti izravno, provalom u vaše računalo putem Interneta i krađom vaših osobnih podataka, ili neizravno, stvaranjem zlonamjerne programske podrške (eng. *malware*) s ciljem oštećivanja ili krađe vaših podataka. Iako je do vašeg računala ponekad moguće doći i bez vašeg odobrenja, većinom su vaše odluke prva i posljednja linija obrane. Vaša svijest o informacijskoj sigurnosti najbolji je sigurnosni alat. Na tehničkoj razini, računalo je potrebno zaštititi odgovarajućom sigurnosnom programskom podrškom, te ispravnim podešenjima operativnog sustava i aplikacija. Srećom, danas postoji mnoštvo kvalitetnih besplatnih rješenja na ovom području.

Uz do sada spomenute prijetnje, Internet je postao i velika opasnost za djecu. Djeca u sve ranijoj dobi upoznaju računalo i sam Internet. Internet je djeci savršeno mjesto za istraživanje. Kao i u stvarnome svijetu, u njemu se ponekad zlo blisko susreće s dobrim. Izloženost neprimjerenim sadržajima i opasni susreti opasnosti su koje ne treba podcjenjivati.Velika količina informacija koja je dostupna na Internetu nije prikladna za djecu, bilo da su informacije koje promiču nasilje ili pornografski materijal. Kroz ovaj rad upoznati ćemo se malo detaljnije o dobrim i lošim stranama koje Internet pruža djeci te kako ih zaštiti od potencijalnih problema.

Zbog ne mogućnosti prijevoda određenih engleskih termina u radu, koristila sam izvorne engleske nazive.

2 SIGURNOST NA INTERNETU

Problemi privatnosti i sigurnosti na Internetu svakako su najveći problemi pri upotrebi Interneta. Povećanjem broja korisnika i primjene Interneta povećava se i mogućnost zlouporabe na Internetu. One su doista raznovrsne: od slanja velikog broja reklamnih poruka na adrese elektroničke pošte korisnika, preko provale računala i krađe informacija, pa do slanja virusa koji korisniku mogu nanijeti veliku štetu [Franjić, 1999].

2.1 ŠTO JE INTERNET?

Internet je javno dostupna globalna paketna podatkovna mreža koja zajedno povezuje računala i računalne mreže korištenjem istoimenog protokola [Wiki1]. Osnovna jedinica Internet komunikacije naziva se paket. Svaka Web stranica koju vidite, elektronička pošta (eng. *e-mail*) koju primite ili datoteka koju preuzimate najprije se dijeli na male pakete od kojih se svaki pojedinačno isporučuje na vaše računalo. Ono zatim ponovno sastavlja te pakete u suvislu cjelinu koja vam se prikazuje.
Načinima na koje se paketi konstruiraju, adresiraju i usmjeravaju preko Interneta rukovodi skup pravila koja osiguravaju zajednički radni okvir koji svako računalo slijedi. Ta se pravila nazivaju protokoli. Svaki protokol ili aplikacija koristi priključke za spajanje na pojedinačna računala. Portovi su pristupna vrata kroz koja informacije dolaze u računalo i odlaze od njega.
Temelj protokola za Internet jesu IP (eng. *Internet Protocol*) i TCP (eng. *Transmission Internet Protocol*). IP opisuje način na koji se šalju paketi s jednog na drugo računalo. Svako računalo na Internetu ima neku IP adresu [Conry-Murray,2005].

Za povezivanje se koriste telefonske mreže, ISDN (eng. *Integrated Services Digital Network*), ADSL (eng. *Asymmetric Digital Subscriber Line* = asimetrična digitalna pretplatnička linija) , optički kabel , satelitske veze i drugi načini.
Najpoznatije usluge na internetu su:

- svjetska mreža (eng. *World Wide Web ili WWW*) - koristi HTTP (eng. *HyperText Transfer Protocol*) za prijenos Web stranica napisanih u HTML-u (eng. HyperText Markup Language)
- razgovor ili čavrljanje (eng. *chat*)
- elektronička pošta (eng. *e-mail*)
- prijenos datoteka
- usenet - mreža namijenjena razmjeni poruka u interesnim grupama [Wiki1].

Internet je zbog svoje raširenosti najveći izvor zlonamjerne programske podrške (eng. *software*). Najveći dio zlonamjerne programske podrške dolazi s pornografskih stranica, te većine internetskih stranica s torrentima, krekovima, generatorima ključeva (eng. *keygeni*),

serijskim brojevima i slično. Korisnik može dobiti neku vrstu zlonamjerne programske podrške pokretanjem zaražene datoteke skinute s Interneta a ponekad i jednostavnim posjećivanjem zlonamjerne internetske stranice. Osim zlonamjernih programskih podrški, postoje i zlonamjerni ljudi [Franjić, 1999].

2.2 TKO SU NAPADAČI?

Napadi na korisnike spadaju u dvije osnovne klase: prijevaru i otmicu. Računalna prijevara je pokušaj izmamljivanja novca nuđenjem sumnjivih proizvoda elektroničkom poštom i iskočnim oglasima, ili pak navođenje na otkrivanje osobnih informacija ili podataka o bankovnim računima.
Otmičari pokušavaju preuzeti kontrolu nad računalom kako bi proveli svoje zle namjere. Kriminalci se pri otimanju računala snažno oslanjaju na malware. U nekim slučajevima kriminalci kombiniraju prijevare i otmice kako bi ostvarili svoje ciljeve. Upoznajmo se sada sa konkretnim nazivima ljudi koji izravno imaju doticaja sa samim napadima na računalo [Conry-Murray,2005].

2.2.1 Hacker

Hakeri (eng. *hacker*) su osobe koje odlično poznaju računala, programsku podršku i sklopovsku podršku (eng. *hardware*) [Wiki2]. Osoba koja je vješta u programiranju, osobito u strojnom jeziku i koja potanko poznaje sve tajne računalnog sustava, ali za razliku od profesionalaca, obično ne radi u tvrtki koja se bavi proizvodnjom programske ili sklopovske opreme i svoje znanje koristi i izvan profesionalne djelatnosti. Osoba koja se bavi računalima više zbog zabave i skupljanja znanja nego zbog materijalne dobiti. Osoba koja istražuje pojedinosti u programima ili računalnim sustavima i pronalazi načine proširivanja njihovih mogućnosti uz minimalna proširenja programskog koda te se bavi programiranjem s mnogo entuzijazma, pa i opsesije [Kiš, 2002]. Često ih se zamjenjuje s piscima virusa i uljezima koji upadaju u informacijske sustave, tzv. Krekerima.

Hakerska etika također nalaže da hakeri dijele svoja dostignuća s drugim korisnicima. Neovlašteno upadanje u tuđe računalne sustave, samo po sebi, nije neetično, ako namjera iza takva čina nije krađa ili uništavanje informacija i podataka ili povreda privatnosti. Nakon neovlaštenog upada u računalni sustav hakerska etika nalaže obavještavanje voditelja sustava o tome kako je upad izveden i kako se može popraviti propust u sigurnosnom sustavu [Kiš, 2002]. To je bitno obilježje koje ih razlikuje od krekera i lamera čiji je cilj uglavnom krađa ili uništavanje podataka ili povreda privatnosti drugih korisnika.
Pravi početak hakerstva seže u 1969 godinu u kojoj su hakeri, Ken Thompson i Dennis Ritchie, napisali prvu verziju Unixa [Wiki2].

SAMURAI - haker čije su provale zakonski opravdane ili ne krše zakonske odredbe (npr. elektroničko dobavljanje informacija pri borbi frakcija u nekoj tvrtki ili dobavljanje informacija potrebnih za sudsko gonjenje) [Kiš,2002].

2.2.2 Kreker (eng. Cracker)

Razbijač, provalnik lopov- osoba koja neovlašteno pristupa nekom računalnom sustavu i sa zlom namjerom razbija sigurnosne sustave te pokušava ukrasti vrijedne informacije. Prema nekim mišljenjima, a suprotno prihvaćenom mitu, za razbijanje sigurnosnih sustava često ne treba veliko znanje, već najprije upornost, dugotrajno ponavljanje unaprijed poznatih i definiranih radnji te upotreba inače dobro poznatih trikova kojima se mogu iskoristit slabosti sigurnosnih sustava. Pojam je nastao s namjerom razlikovanja pojma haker. Krekeri se najčešće okupljaju u malim i donekle tajnim skupinama i nisu u izravnoj vezi s javnom i otvorenom zajednicom hakera. U svijetu kompjuterskih znalaca krekeri se najčešće karakteriziraju kao nedorasle i neodgovorne osobe koje ne mogu zamisliti ili odabrati bolji način upotrebe računala nego što je neovlašteno upadanje u tuđe računalne sustave i krađa podataka [Kiš,2002].

Općenito, krekere možemo podijeliti u tri skupine:

1) bijele - osobe koje svoje znanje koriste kako bi testirale i poboljšale programe te surađuju s proizvođačima programske podrške (eng. *white hats*)
2) crne - kriminalci koji namjerno uništavaju sustave (eng. *black hats*)
3) sive - kombinacija bijelih i crnih, npr. špijuni (eng. *grey hats*) [Wiki2].

Krekerima su prethodili tzv. *frikeri* (eng. *Phreaking = Phone+breaking*) koji su tijekom šezdesetih godina pronašli način kako besplatno koristiti telefonske usluge. John Draper, znan pod nadimkom ” *Captain Crunch*”, jedan je od prvih frikera koji je 1971. godine otkrio da pomoću zviždaljke iz zobenih pahuljica koja proizvodi zvuk frekvencije 2.600 Hz može prevariti telefonsku centralu i telefonirati besplatno. Kad je uhvaćen, odlužio je 5 godina uvjetne kazne [Wiki2].

2.2.3 Lamer

Lameri su uglavnom maloljetnici, koji ništa nisu otkrili i koji nanose štetu drugima, obično da bi ukrali neku šifru za Internet ili uništili nekome disk koristeći trojance i viruse koje su krekeri napisali [Conry-Murray,2005].

Premda se čini da najveći broj hakerskih napada dolazi iz smjera raznih političkih skupina i industrijske špijunaže, prema istraživanju tvrtke IDC, više od 70% hakerskih napada omogućili su zaposlenici unutar tvrtke, koji se ne pridržavaju osnovnih sigurnosnih pravila.

Druga je teškoća u tome što zaposlenici često surfaju na stranice koje nisu vezane uz njihov posao. Nielsen Media Research studija napravljena za Penthouse otkrila je da su radnici IBM-a, Applea, AT&T-a, NASA-e i HP-a bili među najčešćim posjetiteljima Penthouseve stranice [Conry-Murray,2005].

2.3 PRIJETNJE NA INTERNETU

Internetski napadi postaju sve više sofisticirani i sprecijalizirani budući da kriminalci u potrazi za zaradom stalno usavršavaju različite vrste prijetnji na Interetu. Najčešće prijetnje na Internetu su krađa identiteta, društveni inženjering, spam, hoaxing, spoofing, phishing i malware. Upoznajmo ih redom malo detaljnije.

2.3.1 Krađa identiteta

Krađa identiteta oblik je kriminalne radnje lažnog predstavljanja radi stjecanja materijalne ili druge koristi [Wiki3]. Jedna od danas najvećih i najbrže rastućih prijetnji s Interneta je krađa identiteta tj. kopiranje informacija poput brojeva kreditnih računa, zaporki i osobnih matičnih brojeva. Te se informacije mogu koristiti za online ili offline prijevare [Franjić, 1999]. Postoje dva načina krađe identiteta. Jedan način je krađa informacija iz baza podataka banaka, e-trgovina, obračunskih ustanova i drugih koje pohranjuju takve informacije. Drugi način je da napadač izravno od nas ukrade informacije ili ih dobije na prijevaru. Kad je u pitanju prvi način, treba nadzirati svoje bankovne izvode i izvode kreditnih kartica ne bi li uočili čudne transakcije i paziti s kim ćemo poslovati. Kad je u pitanju drugi način možemo više poduzeti, ali prvo nešto o različitim načinima prijevare [Conry-Murray,2005].
Prema podacima Federalne trgovinske komisije SAD-a (eng. *Federal Trade Comission*), gotovo je 10 milijuna Amerikanaca bilo žrtvama krađa identiteta 2003. godine. U ekstremnim slučajevima, financijski gubici kreću se i do nekoliko desetaka tisuća američkih dolara [Franjić,1999].
Vaša sposobnost da dokažete svoj identitet, odnosno moć uvjeravanja da ste stvarno osoba za koju se predstavljate osnovni je način na koji se danas u svijetu provodi trgovina. Dokaze identiteta koristite da biste dokazali vlastitu autentičnost organizacijama s kojima poslujete ili da biste ovlastili isporuku usluga ili transakcija.
Na Internetu se vaš identitet sastoji od niza elemenata poput korisničkih imena, zaporki, osobnih identifikacijskih brojeva (PIN-ova), jedinstvenih matičnih brojeva, raznih brojeva računa i drugih osobnih podataka. Ti digitalni identiteti rade pod pretpostavkom da ste vi jedina osoba koja zna svoje podatke. To je loša pretpostavka i olakšava kriminalcima da počine zločin.

U ranim danima Interneta najgore što vam se moglo dogoditi, što se tiče krađe identiteta, bila je krađa korisničkog imena i zaporke koje ste koristili za svojeg davatelja Internet usluga ISP-a (Internet service provider), a to je značilo da je netko drugi mogao za vaš novac surfati Internetom. Danas koristimo Internet za sve oblike financijskih transakcija, što bitno podiže ulog za krađu identiteta. Kriminalci mogu upotrijebiti vaš digitalni identitet za otvaranje računa kreditnih kartica (Slika 1), mijenjanje vaše adrese, dizanje nenamjenskih i hipotekarnih kredita i provođenje financijskih transakcija, sve u vaše ime. Prijevara s kreditnim karticama najčešći je oblik krađe identiteta [Conry-Murray,2005].

Slika 1 Krađa identiteta [athome.allentate.com]

2.3.2 Društveni inženjering

Društveni inženjering maštovit je način upućivanja na varanje ljudi. Društveni inženjering oslanja se na vaše prirođeno povjerenje u ljude naročito u ljude koji imaju određene društvene uloge, poput onih u uniformama, sa iskaznicama ili u poslovnim odijelima. Kriminalci i stručnjaci za sigurnost (koji se zovu i testeri za provale) koriste društveni inženjering kada pokušavaju provaliti na neku sigurnu lokaciju. Mnoge prijevare s namjerom krađe identiteta oslanjaju se do određenog stupnja na društveni inženjering. Najkorištenija sredstva su lažne poruke elektroničke pošte koje ukazuju da dolaze iz zakonite organizacije ili bezazlene Internet lokacije koje nude besplatne sitnice poput programske podrške za razmjenjivanje datoteka, igrica ili pomoćnih programa koji sadrže i zlonamjerne programe za krađu povjerljivih informacija [Conry-Murray,2005].

2.3.3 Spam

Spam su razne poruke, najčešće reklamne, koje dobijete kao elektroničku poštu, a da ih niste tražili niti očekivali. Često se radi o porukama u kojima se nudi brza i jednostavna zarada, članstvo na nekoj pornografskoj stranici, proizvod raznih tvrtki i slično. Spam poruke šalju se na stotine tisuća ili milijuna adresa. Spameri pokušavaju sve: manipuliranje sustavima za elektroničku poštu, tehnološki sofisticirane napade koji poražavaju spam filtre i brutalnu silu poplavljivanja lošim porukama elektroničke pošte koja nastoji poraziti obranu samom količinom [Franjić,1999].

Pod spamom obično podrazumijevamo poruke marketinškog karaktera, gdje nepoznati pošiljatelj nudi svoje usluge. Nažalost, velik broj takvih poruka nije samo "gnjavaža" za primateljev sandučić nego je i potencijalna opasnost, jer poruka može biti zaražena virusom, spyware-om ili nekim drugim zlonamjernim kodom, te je najbolje takve poruke pokušati spriječiti programima koji štite od spama [Wiki7]. Ako ipak uspiju pronaći put do računala, preporuka je da ih se trajno obriše bez otvaranja. Ponekad je promjena adrese elektroničke pošte jedini učinkovit način rješavanja spam poruka [Franjić,1999].

2.3.4 Spoofing

Pojam spoofinga u domeni računalne sigurnosti označava bilo kakvu pojavu u kojoj se korisnika pokušava prevariti, u prvom redu stvaranjem dojma da je netko pouzdana osoba koja time može dobiti pristup osobnim, financijskim i drugim zaštićenim i povjerljivim informacijama. Spoofing je toliko širok pojam da se pod spoofing aktivnostima smatraju phishing, hoaxing i čitav niz drugih pojmova ovisno o kontekstu.

S obzirom na načine izvedbe, spoofing možemo podijeliti u tri glavne kategorije:

- E-mail spoofing
- IP spoofing
- URL spoofing

2.3.4.1 E-mail spoofing

U većini slučajeva e-mail spoofing je okarakteriziran u sljedećem scenariju: korisnik prima poruku elektroničke pošte za koju se čini kako je stigla od jednog pošiljatelja (kojem korisnik možda vjeruje), premda je u biti poslana s neke druge adrese elektroničke pošte. Zlonamjerni korisnici ovime žele prevariti nevinog korisnika, koji u uvjerenju da je dobio elektroničku poruku s adrese kojoj vjeruje, može odgovarajući na takvu poruku proslijediti i svoje osobne ili financijske informacije (npr. broj kreditne kartice) [sigurnost.tzv.hr].

2.3.4.2 IP spoofing

IP Spoofing (eng. *Internet Protocol Spoofing*) se ubraja u jedan od najraširenijih oblika „online kamuflaže“. Cijela se ideja sastoji u stvaranju IP paketa (eng. *IP packets*) s lažnom izvorišnom IP adresom. Naime, u zaglavlju svakog IP paketa se nalazi njegova izvorišna adresa i obično je riječ o adresi s koje je IP paket i poslan. Zlonamjerni korisnik može krivotoriti zaglavlje i time stvoriti dojam da je paket poslan s drugog računala. Ovom se metodom učestalo koriste napadači koji žele steći neovlašteni pristup nad mrežnom infrastrukturom pokušavajući zavarati sustave za autentifikaciju koji se temelje na IP adresama [sigurnost.tzv.hr].

2.3.4.3 URL spoofing

URL spoofing se sastoji u pokušaju da se URL (eng. *Universal Resource Locator*) neke zlonamjerne stranice prikaže kao URL pouzdane stranice. Napadači koji se služe ovom tehnikom često iskorištavaju sigurnosne propuste u Web preglednicima. Zbog ovih razloga je uvijek dobro koristiti najnovije inačice Web preglednika koje u pravilu donose poboljšanja i ispravke sigurnosnih i drugih propusta. Korisnik obično dobije poveznicu (link) ili poruku elektroničke pošte u kojoj se nalazi poveznica koja djeluje poznato, te korisnik klikne na nju vjerujući da odlazi na ispravno i valjano Web sjedište. Ukoliko se na toj stranici od korisnika pokušavaju prikupiti osobne ili financijske informacije tada je riječ o pokušaju phishinga [sigurnost.tzv.hr].

2.3.5 Hoax

Hoax je bilo kakva prijevara koja ima za cilj lažno predstavljanje i obmanu ljudi, a čiji se sadržaj najčešće nalazi u poruci ili spamu [Wiki9]. Hoax je poruka u obliku elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja. Želja osobe koja je poslala hoax je njegovo prosljeđivanje na što veći broj adresa. Pri tome ih primatelji doista i prosljeđuju Internetom jer su uvjereni da time pomažu drugima. Hoaxi ne mogu uzrokovati oštećenja računalnih programa i operacijskih sustava, ali zabilježeni su brojni slučajevi gdje su hoaxi svojim sadržajem i vještom psihologijom naveli korisnike da sami oštete svoje programe i sustave. Drugi oblik štete koji hoaxi nanose korisnicima je zavaravanje korisnika te narušavanje njihovog ugleda, kao i ugleda određenih organizacija, tvrtki i poznatih osoba. Scam je ozbiljniji oblik hoaxa, često s ozbiljnim financijskim, pravnim ili drugim posljedicama za žrtvu. Velika se šteta ne može izazvati širenjem hoaxa. Ipak, hoaxi često zavaravaju korisnike, narušavaju ugled određenih organizacija ili osoba, a pri tome bespotrebno opterećuju mrežu, povećavaju troškove korištenja Interneta te zatrpavaju dolazne poruke osoba koje dobivaju hoaxe [Cert].

Primjer hoaxa je:

"Ovu poruku Vam šalje osnivač Microsofta želeći vas upozoriti: svijetom vreba novi virus (zove se Miaxao) koji briše 99% datoteka s diska te onesposobljuje antivirusne programe. Miaxao je podrijetlom iz Kine, autor mu je nepoznat, kao i datum nastanka. Do sada je, prema novijim podacima, napao 38 mil. računala u cijelom svijetu, i to uglavnom u Europi, SAD-u i Kanadi. Molimo Vas, proslijedite poruku svojim prijateljima i poznanicima koji vjerojatno ne znaju za virus" [Wiki9].

2.3.6 Phishing

Pecački (eng. *phishing*) napadi su najprominentniji i najštetniji napadi današnjih prevaranata s Interneta. Mnogi phishing napadi počinju elektroničkom porukom. Na primjer, organizacija

kriminalaca pošalje tisuće spam poruka koje ukazuju na to da ih je poslala banka, kompanija za izdavanje kreditnih kartica, ISP ili kompanija za e-trgovinu (eBay i PayPal su najpopularnije mete). Neke pecačke poruke očigledne su prijevare, ali druge su prava remek djela, s logotipom kompanije i napisane jezikom korporativnog marketinga [Conry-Murray,2005].

2.3.7 Malware

Malware (kratica od MALicious softWARE, zlonamjerna programska podrška). Općeniti pojam koji opisuje programski kod kreiran s namjerom da našteti računalnom sustavu. Malware obuhvaća brojnu zlonamjernu programsku podršku, uključujući viruse, crve, trojanske konje i neki spyware i adware visokog rizika. U starim danima (kasne 1980.-te), malware je putovao na disketama. Da biste uhvatili virus trebali ste zaraženu disketu umetnuti u svoje računalo. Danas se malware širi elektroničkom poštom, sustavima za dopisivanje u realnom vremenu, raznim Internet protokolima i World Wide Webom. Automatizirani malware može otkriti, provaliti ili preuzeti kontrolu nad tisućama računala i od njih napraviti vojsku strojeva-robova kojima se može upravljati na daljinu. Kućna računala s DSL ili kabelskim modemima su popularne mete jer su često nezaštićena, a njihove širokopojasne internetske veze znače da mogu slati tisuće elektroničkih poruka ili zatrpati tisuće Web lokacija u sekundi [Conry-Murray,2005].

2.3.7.1 Virusi

Virus je zlonamjeran program ili kod koji se sam umnožava u drugim datotekama s kojima dolazi u kontakt. Većina virusa samo se razmnožava, ali mnogi mogu oštetiti vaš računalni sustav ili korisničke podatke. Ponekad virus zahtjeva interakciju čovjeka da bi se umnožio, poput klika programa koji sadrži virus ili otvaranjem neke zaražene datoteke. Kada se jednom aktivira, virus može kreirati i distribuirati svoje kopije inicirajući druge programe ili se širiti komunikacijskim mehanizmima poput elektroničke pošte.
Računalnim virusima se često nazivaju i drugi štetni programi, npr. trojanski konji i crvi, iako oni zapravo ne inficiraju datoteke, već imaju druge funkcije, na primjer širenje mrežom (crvi) te krađa korisničkih zaporki i brojeva kreditnih kartica i/ili omogućavanje pristupa neovlaštene osobe zaraženom računalu (karakteristično za trojanske konje) [Conry-Murray,2005].

2.3.7.2 Crvi

Crvi su računalni programi koji omogućuju distribuciju vlastitih kopija, često bez interakcije čovjeka. Oni su izgrađeni kao samodostatni programi koji rade nezavisno od drugih programa na računalu. Crvi otežavaju rad mreže, a mogu oštetiti podatke i kompromitirati sigurnost računala. Današnji se crvi sve više kreiraju za traženje i iskorištavanje specifičnih pukotina u popularnim operativnim sustavima ili aplikacijama. Te pukotine koje nazivamo i

ranjivosti dopuštaju crvima da dobiju pristup računalu, provedu bilo koji zadatak koji im je dodijeljen i repliciraju se da bi pronašli druga ranjiva računala. Crvi koji se nazivaju mass maileri šire se sami elektroničkom poštom, dok drugi crvi koriste razne mehanizme širenja [Conry-Murray,2005].

2.3.7.3 Spyware

Špijunski software (eng. *Spyware*) je pojam za neke tehnologije uhođenja koje se provode na vašem računalu bez primjerenog upozorenja, vaše suglasnosti ili kontrole [Conry-Murray,2005]. Za razliku od virusa i crva on se ne može sam umnožavati. Spyware može nadzirati vaše online aktivnosti i/ili provoditi funkcije bez vašeg znanja ili pristanka. Ovisno o programu, spyware može pratiti i izvještavati o svakoj Web lokaciji koju posjetite, generirati iskočne oglase, promijeniti polaznu stranicu i postavke pretraživača ili bilježiti svaku tipku koju pritisnete. Kao mnogi novi virusi, spyware je dizajniran da iskorištava zaražena računala za komercijalnu dobit. Tipične taktike su prikazivanje ne zahtjevnih pop-up reklama, krađa osobnih informacija (uključujući i financijske informacije kao što su brojevi kreditnih kartica i zaporke), preusmjeravanje HTTP zahtjeva na reklamne stranice. Zaraza se u najvećem broju slučajeva događa prilikom posjete stranica sa ilegalnim ili pornografskim sadržajem. Distributeri spywarea obično predstavljaju program kao koristan uslužni program ili agent programske podrške [sigurnost.tzv.hr].

2.3.7.4 Adware

Oglašivački software (eng. *Adware*) je podskup šire kategorije spywarea, koji je dizajniran da isporučuje ciljano oglašavanje na vaš web pretraživač, naročito preko skočnih prozora (eng. *Pop-up*) (Slika2). Adware, oglašivački software (eng. *advertising-supported software*) je program koji automatski prikazuje ili skida (preuzima) oglase na računalu nakon što je instalirana neka programska podrška ili nakon korištenja neke aplikacije. Pojedini oglašivački programi pripadaju i špijunskj programskoj podršci te se stoga mogu svrstati u programe koji narušavaju privatnost korisnika. Obično se nalazi u besplatnim programima (eng. *freeware*) kako bi njihovi autori pokrili troškove koji su bili potrebni za izradu tih programa, no nalazi se i u nekim ograničeno djeljivim programima (eng. *shareware*), programima koje je potrebno platiti nakon određenog roka korištenja [Wiki4]. Adware zna koje vam vrste oglasa treba isporučiti jer prati koja mjesta na Internetu posjećujete. Osim praćenja korisnikovog surfanja i dosađivanja s oglasima, adware može i otvoriti vezu s Internetom da bi na središnji poslužitelj slao izvještaje o vašim navikama surfanja. Te informacije, koje mogu obuhvaćati korisnikovu dob, spol, navike kupovanja pa čak i korisnikovu lokaciju, mogu se koristiti za „istraživanje tržišta“ za privlačenje novih klijenata [Conry-Murray,2005].

Slika 2 Skočni prozori (pop-up) [wikipedia.org/wiki/Pop-up]

2.3.7.5 Trojanski konj

Trojanski konj je zlonamjeran računalni program koji se predstavlja da je netko drugi s korisnim ili poželjnim funkcijama. Za razliku od virusa i crva, trojanski konj ne može sam sebe umnožavati, no korisnik ga može kopirati na drugo računalo. Naziv trojanski konj nastao je po poznatoj priči o osvajanju grada Troje zlouporabom povjerenja. Na sličan se način virtualni trojanski konj može predstaviti kao igra ili zanimljiv sadržaj koji se šalje u elektroničkoj poruci. Kada se pokrene, na računalo se na primjer instalira aplikacija za udaljenu kontrolu. Može izvoditi razne aktivnosti poput krađe korisničkih zaporki, brojeva kreditne kartice, PIN-a i drugih osjetljivih informacija koje potom šalje nekoj drugoj osobi ili može nepotrebno zauzimati resurse računala usporavajući ga na taj način [Conry-Murray,2005].

2.3.8 Keystroke logger

Keylogger (dolazi od engleskih riječi key i logger) je program koji bilježi sve vaše pritiske na tipke tipkovnice. Keystroke loggeri tipično pohranjuju zabilježene pritiske na tipke za kasnije učitavanje ili informacije šalju udaljenom napadaču, koji skenira informacije da bi pronašao korisne dijelove podataka poput zaporki i brojeva računa. Neki keystroke loggeri dolaze s popisom Web lokacija poput bankovnih kompanija za izdavanje kreditnih kartica i kompanija za e-trgovinu, te krenu bilježenje pritisaka na tipke kada u svoj pretraživač unesete URL s tog popisa. Keystroke loggeri se koriste za krađu zaporki i druge informacije o identitetu [Conry-Murray,2005].

2.3.9 Rootkits

Rootkiti su posebna grupa zlonamjernih programa ili, preciznije rečeno, to su programi čija je namjena skrivanje drugih zlonamjernih programa (npr. virusa, spyware-a, trojanskih konja) od korisnika. Cilj rootkita najčešće je preuzimanje kontrole nad računalom uz istovremeno skrivanje datoteka, procesa, zapisa u registrima pomoću kojih se navedeno preuzimanje

kontrole ostvaruje. Spomenutim tehnikama „skrivanja“ od korisnika, zlonamjerni programi na taj način ostaju nevidljivi i neuklonjivi antivirusnim programima, blokatorima spyware-a i sl.
Napadači najčešće uočavaju i iskorištavaju trenutne ranjivosti operativnog sistema (npr. otvorene pristupe, računala bez sigurnosnih nadogradnji ili sa slabim administratorskim zaporkama) kako bi dobili pristup računalu. Jednom kada je pristup osiguran, napadač ručno instalira rootkit. Takvu vrstu „skrivenog“ napada vrlo često teško otkrivaju firewall-i te antivirusni i antispyware programi za zaštitu računala [sigurnost.tzv.hr].

2.3.10 Browser hijacker (otimači pretraživača)

Otimači pretraživača nanovo postavljaju polaznu stranicu (Slika 3) i preusmjeravaju vaš pretraživač na neželjene ili nepoznate tražilice ili druge Web lokacije. Neki otimači pretraživača mogu vas spriječiti prilikom objavljivanja polazne stranice. Neki rade tako da brišu unos za polaznu stranicu koju ste odabrali i umeću vlastitu u posebnu datoteku koju konzultira vaše računalo (eng. *hosts datoteka*). Oni također mogu presresti unose za pretraživanje upisane u legitimnu tražilicu i prikazati vlastite rezultate.

Slika 3 Otimači pretraživača [outside.thebikinibottom.com]

2.3.11 Dialer

Dialeri su programi koji koriste modem računala za povezivanje ili pristupanje uslugama. Korisnici žele ukloniti dialere jer biraju neočekivane telefonske brojeve i nabijaju velike telefonske račune. Dialer je kolokvijalan izraz za tehnologije biranja telefonskih brojeva. Nekoliko je načina da se dialer instalira na računalo korisnika. Najčešće se dialerom može zaraziti pretraživanjem raznih Web sadržaja namjenjenima zabavi, pogotovo onih za odrasle. Na takvim Web stranicama obećavaju se razni besplatni sadržaji pod uvjetom da instalirate „poseban program“ kojim ćete taj sadržaj moći pregledati. Taj „poseban program“ ustvari je dialer, a korisnik ga iz neznanja i nepažnje potpuno svjesno i dobrovoljno instalira na svoje računalo, nakon čega dialer prekida trenutnu te pokreće novu, štetnu vezu na Internet.

Pored ovog najočitijeg načina, dialeri se mogu instalirati zajedno sa drugim besplatnim sadržajima koji su korisniku dostupni za preuzimanje na Internetu (mp3 glazba, melodije za mobitele, igre, filmovi) [sigurnost.tzv.hr].

2.4 KAKO ZAŠTITI RAČUNALO OD INTERNETSKIH NAPADA

Postoji nekoliko načina za sprječavanje online krađe identiteta i sličnih prijetnji s Interneta. Neki uključuju tehnologiju, ali se većina oslanja na zdrav razum. Alati koji mogu pomoći su antivirusni programi i ani-spyware programi. Potrebno je redovito skenirati svoje računalo [Conry-Murray,2005].

2.4.1 Antivirusni programi

Antivirusni program ili antivirus je računalna programska podrška koja se koristi za zaštitu, identifikaciju i uklanjanje računalnih virusa, kao i drugih programa koji mogu oštetiti programsku podršku, a jednim imenom se naziva malware. Prvi antivirusni programi pojavili su se 1983 godine [Wiki5]. Antivirusni program je najbolja zaštita od virusa i crva. On može spriječiti instaliranje virusa, a može i otkriti, izolirati i ukloniti viruse i crve s korisnikovog računala. Antivirusni program radi stvaranjem potpisa svakog virusa ili komada malwarea. Potpis identificira sekciju koda koje se pojavljuje samo u malwareu. Svaki put kada antivirusni program skenira neki prilog u elektroničkoj pošti ili ispituje datoteke na tvrdom disku (eng. *hard disk*), on traži potpise poznatih virusa i crva. Antivirusni program vas može zaštiti od poznatih virusa koji se pojavljuju na nekoliko mjesta: u dolaznim i odlaznim porukama elektroničke pošte, porukama u sustavu za dopisivanje u realnom vremenu (chat, MSN, Skype…) i na tvrdom disku vašeg računala. Većina antivirusnih proizvoda isporučuje se sa skenerom u realnom vremenu koji provjerava vaše datoteke svaki put kada im pristupate. Potrebno je redovito skenirati tvrdi disk [Conry-Murray,2005].

Heuristička metoda se može koristiti kod novih i nepoznatih virusa. Može se koristiti na dva načina: analiza datoteka i emulacija datoteka. Analiza datoteka je proces traganja za sumnjivim programskim zapovijedima u datotekama. Slabost ove metode je to što ona može znatno usporiti računalni sustav provjeravajući veliki broj datoteka. Emulacija datoteke je metoda koja izvršava program u virtualnom okruženju i bilježi sve akcije koje on izvrši. Lažni antivirusni programi (neki od engleskih naziva su rogue security software i fake antiviruses) se korisniku lažno predstavljaju kao oni pravi. Ova vrsta zlonamjerne programske podrške pokušava navesti korisnika na kupnju tako što će simulirati pregledavanje njegovog računala i pokušati ga zastrašiti porukom da je pronađen ogroman broj nepostojeće zlonamjerne programske podrške te da će ih biti moguće ukloniti tek ako korisnik kupi program. Lažni antivirusni programi najčešće instaliraju zlonamjerne internetske stranice [Wiki5].

2.4.2 Anti-spyware programi

Specijalizirani programi za uklanjanje špijunske programske podrške se zovu antišpijunski (eng. *antispyware*) programi. Oni često bolje prepoznaju većinu špijunskih programa od antivirusnih programa, dobro prepoznaju i adware, a neki od poznatijih su Spybot Search & Destroy, Lavasoftov Ad-Aware, SUPERantispyware, CA Antispyware, Windows Defender i Sunbelt CounterSpy [Wiki6]. Anti-spyware programi mogu skenirati tvrdi disk i pronaći nepoželjnu programsku podršku. Kada otkriju nepoželjni program pitaju da li ga korisnik želi izbrisati, izlorati ili ga ostaviti gdje je. Izoliranjem ga ostavljate na svom računalu ali spriječavate njegovo funkcioniranje. Anti-spyware software ne nudi potpunu zaštitu od svih malwarea. Anti-spyware i antivirusni proizvodi počeli su se poklapati, a samo anti-spyware program nije dovoljan za zaštitu od virusa, crva i trojanskih konja. Anti-spyware proizvodi ne mogu skenirati elektroničku poštu koja postaje popularan put širenja zaraze za spyware [Conor-Murray,2005]. Postoje i programi koji mogu vršiti i imunizaciju internetskih preglednika. Imunizacija internetskih preglednika sprječava instalaciju određenih špijunskih programa na računalo te blokiraju opasne ActiveX skripte [Wiki6]. Za potpunu zaštitu potrebno je koristiti antivirusni i anti-spyware program [Conor-Murray,2005].

2.4.3 Sigurnosni tokeni

Sigurnosni tokeni su usko povezani sa problemima e-trgovine te provjere autentičnosti. Autentikacija s dva faktora je autentikacija kod koje nešto imamo (pametna kartica ili token) i znamo nešto čime dokazujemo da je to što imamo uistinu naše (PIN ili upravo generirani broj na tokenu). Drugim riječima, kod autentikatora „nešto što imaš“ korisnik mora dokazati da je autentikator njegov. To će dokazati dodatnim upisivanjem PIN-a (engl. *Personal identification number*) kod pametnih kartica ili broja koji je u tom trenutku generirao token, ako je kao autentikator korišten token.
Token je poseban uređaj koji generira jednokratne zaporke (Slika 4), no kad je u pitanju autentikacija, token može biti bilo što. Tako se npr. pametna kartica često naziva token. Postoje različiti tipovi tokena. Osnovna podjela je na:

1) tokene koji generiraju statičke zaporke
2) tokene koji generiraju sinkrone dinamičke zaporke
3) tokene koji generiraju asinkrone zaporke
4) tokene koji rade na načelu izazova/odgovora.

Na primjeru tokena većine banaka u Hrvatskoj proces je sljedeći:

1) Korisnik upiše PIN.
2) Token izbaci zaporku za jednokratno korištenje.
3) Korisnik se prijavljuje na sustav upisujući broj tokena i zaporku koju je token generirao.
4) Poslužitelj na osnovu broja tokena uzme odgovarajući ključ i generira jednokratnu zaporku.

5) Ako su zaporke identične, autentikacija je uspješna.

Kod potvrde transakcije koristi se izazov/odgovor za autorizaciju :

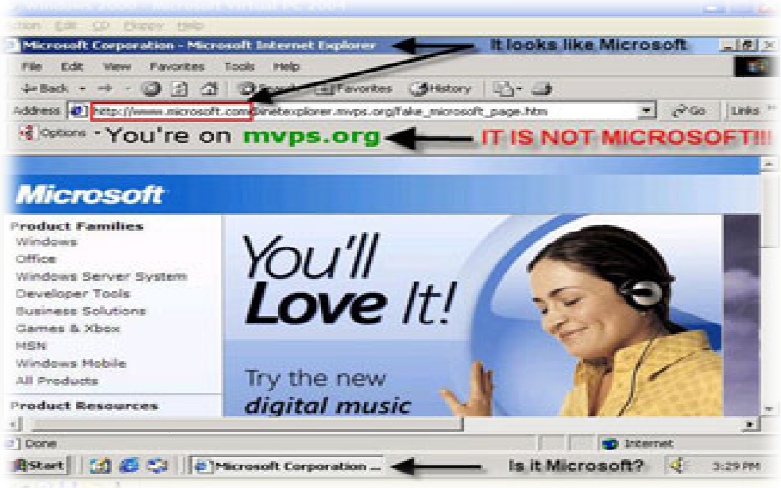
1) Poslužitelj generira neki broj i pošalje ga klijentu.
2) Klijent unosi taj broj u token i dobiva odgovor.
3) Klijent unosi odgovor i šalje ga poslužitelju.
4) Poslužitelj propusti izazov broj koji je poslao klijentu kroz istu funkciju kao i klijent i autorizacija je, ako je dobio isti rezultat, uspješna.

Prijavljivanje na sustav korištenjem tokena, pametne kartice i sl. znatno je sigurniji način autentikacije od zaporke [Čavar,2010].

Slika 4 Sigurnosni token [otpbanka.hr]

2.4.4 SpoofStick

SpoofStick je mali program, takozvana ekstenzija pretraživača, koji vam može pomoći da otkrijete lažne Web lokacije. Program kreira novu alatnu traku (Slika 5) u vašem pretraživaču koja prikazuje po kojoj Web lokaciji trenutno surfate [Conry-Murray, 2005].



Slika 5 SpoofStick [www.certtechs.com]

2.4.5 Protokoli za zaštitu

Nekoliko je načina zaštite podataka i provjere njihove autentičnosti. Uz do sada već neke spomenute koristimo i protokole za sigurno trgovanje na Internetu. U našim Web preglednicima koristimo Secure Sockets Layer (SSL), korporacije u svijetu već odavno koriste Electronic Dana Interchange (EDI), najpoznatiji od novih rješenja je The Secure Electronic Transactions protokol (SET), a ima i drugih protokola [Franjić, 1999].

2.4.5.1 SSL

Security Socket Layer je protokol koji omogućuje šifrirani prijenos informacija putem HTTP-a. SSL omogućuje korištenje digitalnih certifikata tako da Web pretraživač može provjeriti autentičnost neke Web lokacije. Digitalni certifikat oblik je elektroničke provjere vjerodostojnosti koji potvrđuje da je treća strana povjerila vjerodostojnost nositelja certifikata. Svi se Web pretraživači isporučuju s već učitanim sposobnostima za korištenje SSL-a i nije potrebno dodatno uključivanje ili isključivanje. Postoje dva načina da provjerite koristi li se SSL. Adresa na traci za adrese Web pretraživača napisana je kao **https://** a ne kao http://. (HTTPS je zaštićena verzija Hypertext Transfer Protocola.) Vidjet ćete i ikonu lokota u donjem desnom kutu pretraživača (Slika 6) [Conry-Murray, 2005].

Slika 6 SSL protokol [plus.hr]

2.4.5.2 EDI

EDI je protokol koji se koristi za razmjenu informacija, dokumenata, te raznih drugih poslovnih transakcija poput narudžbi, plaćanja i sličnog. To je standard za elektroničko poslovanje i prije svega je sigurno i pouzdano riješenje [Franjić, 1999].

2.4.5.3 SET

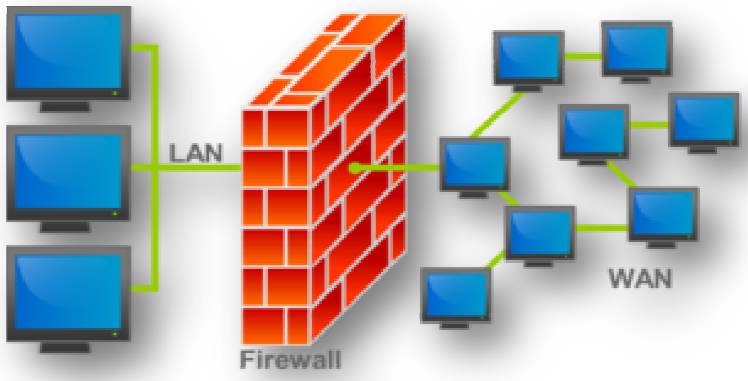
SET ili Protokol za sigurne elektroničke transakcije. SET treba sačuvati privatnost i integritet online plaćanja kreditnim karticama u realnom vremenu. Temelji se na stvaranju digitalnih „certifikata“ ili potvrda koje provjeravaju identitet kupca i prodavača prije ego što se pokrene mrežna transakcija plaćanja. Sadržaj transakcije zatim se zaštićuje zaporkom, zbog daljnjeg poboljšanja sigurnosti [Franjić, 1999].

2.5 FIREWALL (VATROZID)

Vatrozid (eng. *firewall*) je sigurnosni element (mrežni uređaj ili program) smješten između neke lokalne mreže i javne mreže (Interneta) (Slika 7), a koji je dizajniran kako bi zaštitio povjerljive, korporativne i korisničke podatke od neautoriziranih korisnika (blokiranjem i zabranom prometa po pravilima koje definira usvojena sigurnosna politika). Služi spriječavanju neželjenog upada uljeza u lokalnu mrežu (računalo). Osnova rada vatrozida zasniva se u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i priključku u oba smjera.
Vatrozid postavlja ograničenja na dolazni, ali i odlazni promet te prikriva identitet korisničkog računala što onemogućava, odnosno otežava, dobivanje informacija o računalu koje bi olakšale upad. Vatrozid možete shvatiti kao vrstu polupropusne barijere koja zaustavlja promet informacija prema vašem računalu te prema definiranim parametrima određuje što će propustiti, a što blokirati.
Budući da aplikacije koriste priključke za pristup računalima, jedan od poslova vatrozida je da nadzire koji portovi smiju komunicirati s računalom.
Vatrozid može biti programski ili sklopovski:

1. Programski vatrozid omogućava zaštitu jednog računala, osim u slučaju kada je isto računalo postavljeno na zaštitu čitave mreže
2. Sklopovski vatrozid omogućuje zaštitu čitave mreže ili određenog broja računala

Za ispravan rad vatrozida potrebno je precizno odrediti niz pravila koje definiraju kakav mrežni promet je dopušten u pojedinom mrežnom segmentu. Takvom sigurnosnom politikom se određuje nivo zaštite koji se želi postići primjenom vatrozida [Conry-Murray, 2005].



Slika 7 Firewall (vatrozid) [wikipedia.org]

2.5.1 Na kojem principu i što radi vatrozid?

Postupak u kojem se netko na Internetu ili mreži pokušava spojiti na vaše računalo se naziva „netraženi zahtjev“ (eng. *unsolicited request*). Svaki put kada vaše računalo zaprimi netraženi zahtjev, vatrozid blokira spajanje. Međutim, ako koristite program kao što je klijent za komunikaciju u realnom vremenu gdje je potrebno primati informacije s Interneta ili mreže, vatrozid će vas pitati treba li blokirati ili dopustiti spajanje. Ako odaberete opciju dopuštanja, vatrozid će ulazne informacije te vrste promatrati kao tzv. iznimke. Kada jednom dopustite ulaz informacija putem klijenta za komunikaciju u realnom vremenu, vatrozid će zapamtiti tu postavku i neće vas svaki put pitati isto pitanje [Belošević,2011].

Vatrozid ne pronalazi računalne viruse i crve koji su već na vašem računalu. Protiv ovakvog oblika opasnosti se bore antivirusni programi. Nadalje, vatrozid neće spriječiti otvaranje opasnih privitaka primljenih elektroničkom poštom. Vatrozid neće blokirati ni spam i ostale neželjene poruke poslane elektroničkom poštom [Conry-Murray,2005].

2.5.2 Povijest vatrozida

Vatrozid tehnologija nastala je u kasnim 1980-im, kada je Internet bio relativno nova tehnologija u pogledu globalnog povezivanja i uporabe.

Vatrozid prve generacije pojavio se u AT&T Bell Labs. Cheswick Bill i Steve Bellovin su nastavili istraživanja o filtriranju paketa, te su razvili model zaštite za svoju vlastitu kompaniju na temelju njihove izvorne arhitekture prve generacije.

Od 1980-1990 troje kolega iz AT&T razvili su drugu generaciju vatrozidova, sklop na razini vatrozida (eng. *Circuit level firewalls*). Prednost tog vatrozida je da omogućava ispitivanje stanja paketa i može odrediti je li paket početak nove veze, dio postojeće veze ili je nevažeći paket.

Cheswick Bill na AT&T Laboratories i Marko Ranum opisali su treću generaciju vatrozida, poznatu kao aplikacijski sloj vatrozida. Ključna riječ od primjene vatrozida trećeg sloja je razumijevanje određenog programa i protokola.
1992.godine Bob Braden i Annette DeSchon su poboljšali pojam vatrozida. Proizvod poznat kao „Vize“ bio je prvi sustav sa vizualnim sučeljem i sa integracijom boja i ikona, koji bi se mogao lako implementirati, te kojem bi se moglo lako pristupiti na računalu. U 1993. godini, tvrtka Check Point prati trend s Firewall – 1 proizvodom. Vatrozidovi prije Firewall – 1 zahtijevali su editiranje ASCII datoteka s ASCII editorom. Ranim ASCII vatrozidovima bilo je lako pružati podršku, jer su bili vrlo ograničeni Internet servisima u to vrijeme. Tipično za organizaciju je potreba sigurnog spajanja preko interneta na udaljene terminale usluga, prijenos datoteka (FTP), elektronička pošta (SMTP) i Usenet (NNTP). U današnje vrijeme ti servisi su dodani na listu zahtjeva za pristup, ali kako se razvija Internet i dalje se razvija potreba za više servisa, pa se tako i napadi mijenjaju, kako bi vatrozidovi mogli pratiti trendove, nova pravila se moraju kontinuirano nadodavati [Belošević,2011].

2.6 KRIPTOGRAFIJA

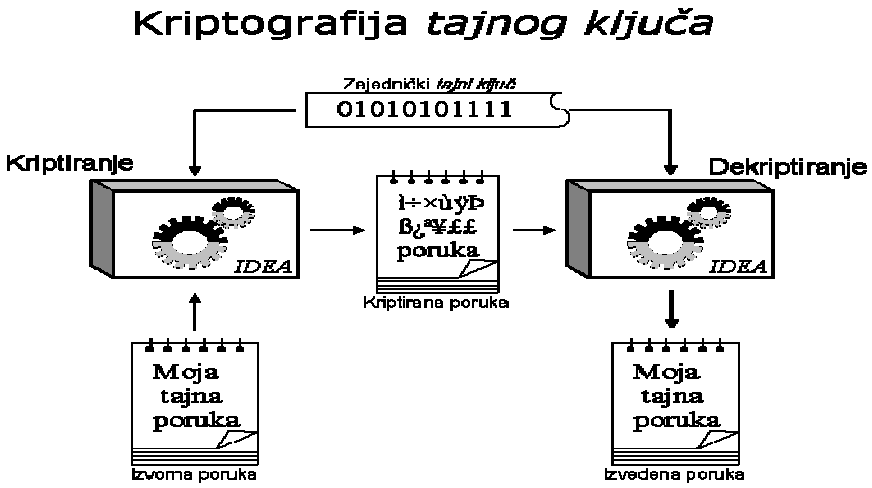
Kriptografija (eng. *Cryptography*), tajno pismo. Sustavno zamjenjivanje i razmještanje grafičkih znakova nekog teksta koje ima svrhu da sakrije informaciju koja je u njemu sadržana te da se na taj način očuva tajnost poruke, tj. da značenje ostane skriveno onima kojima informacija nije namjenjena [Kiš,2002]. Za bolje razumijevanje kriptografije potrebno je poznavati pojmove šifriranje, dešifriranje i ključ. Šifriranje znači skrivanje podataka i njihovo transformiranje u obično neprepoznatljiv sadržaj. Dešifriranje predstavlja obrnuti proces iz neprepoznatljivog šifriranog oblika natrag u "čitljiv" oblik. Ključ kao pojam vezan uz kriptografiju predstavlja podatak koji omogućava šifriranje i/ili dešifriranje. Ključ dakle predstavlja jedan ili više podataka koji uz poznati algoritam vode do početnih podataka i obratno [Wiki8].

Moguće je postići određenu dozu privatnosti kada govorimo o korištenju Interneta programskom podrškom koja može šifrirati elektroničku poštu i istovremene poruke koje šaljete, te datoteke i mape koje spremate na svoje računalo. Šifriranje je proces u kojem se informacije provlače kroz matematički algoritam da bi se proizveo nečitki tekst. Jedini način za pretvaranje nečitkog u čitki tekst je nekim ključem. Postoje dvije vrste digitalnog šifriranja: simetrično i asimetrično.

2.6.1 Simetrično šifriranje

Kod simetričnog šifriranja isti se ključ koristi za šifriranje običnog teksta i dešifriranje nečitkog teksta kao što je prikazano na Slici 8. Sigurnost šifriranja ovisi dijelom o algoritmu koji se koristi i o duljini ključa. Duljina ključa mjeri se u bitovima. Snaga duljine ključa

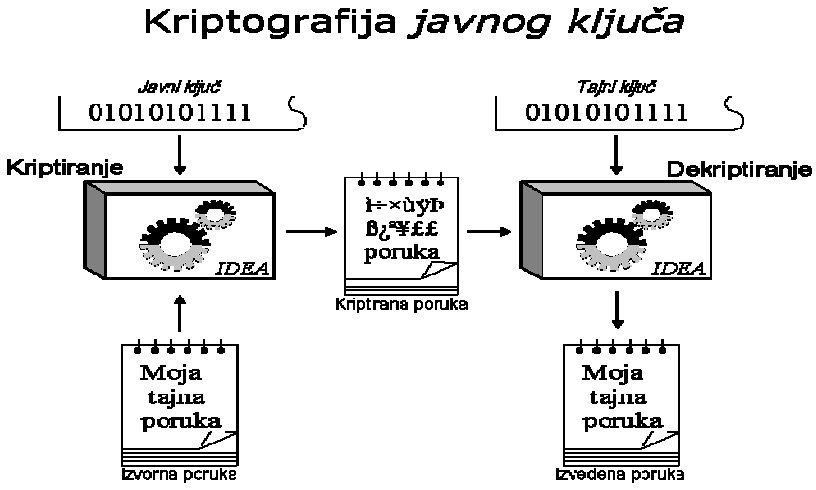
procjenjuje se po tome koliko bi komercijalno dostupnom računalu trebalo vremena da dešifrira šifriranu poruku isprobavanjem svih mogućih kombinacija brojki i slova. To se naziva napad golom silom (eng. *brute-force*). Simetrično šifriranje dobro je opremljeno za šifriranje podataka kao što su datoteke, mape i dokumenti. Kod njega je problem u tome što je manje korisno za slanje šifriranih poruka. U poruku ne možete staviti ključ jer bi je svatko tko ju presreće mogao lako dešifrirati. Ključ možete staviti na disk i poslati ga običnom poštom ali time riskirate da se disk izgubi ili presretne.



Slika 8 Simetrično šifriranje [fly.cc.fer.hr]

2.6.2 Asimetrično šifriranje

Rješenje gore navedenog problema je asimetrično šifriranje, koje se naziva i šifriranje s javnim ključem. Pri asimetričnom šifriranju jedna matematička funkcija generira dva ključa (Slika 9), jedan se ključ koristi za šifriranje običnog teksta, a drugi za njegovo dešifriranje. Ključ po kojem se šifrira običan tekst ne može se koristiti za dešifriranje tog teksta i obratno [Conry-Murray,2005].



Slika 9 Asimetrično šifriranje [fly.cc.fer.hr]

2.7 BACKUP

Koristimo li računalo za ozbiljnije stvari od povremenog igranja i pregledavanja sadržaja na Internetu, podaci koje na njega pohranjujemo važni su nam i postanu li nedostupni to može predstavljati veliku štetu. Srećom, ovaj je problem danas znatno lakše rješiv nego što je bio još nedavno [Cert.hr]. Backup je jedna od najvažnijih stvari u svijetu računala. Backup je izrada rezervne, sigurnosne kopije datoteka ili programa. Svrha je izbjegavanje gubitka podataka u slučaju nestanka struje, kvara računala te arhiviranje, tj.trajno bilježenje podataka koji se odnose na jedno razdoblje a mijenjaju se u drugom [Kiš,2002]. Backup se može pohraniti na magnetnim trakama, tvrdim diskovima, CD, DVD i ostalim medijima za pohranu podataka. Pri izradi Backup-a često se koristi sažimanje tj.komprimitiranje podataka zbog uštede prostora. Pričuvni (backup) podaci se obično trebaju držati na više mjesta radi bolje sigurnosti, također moguće je držati podatke na nekom udaljenom Internet serveru [Wiki10]. Zaštitnu kopiju također treba izraditi pomoću specijaliziranih programa a može se koristiti i Windows backup i Restore programska potpora [Buzdo.hr].

2.8 BEŽIČNE MREŽE

Bežična tehnologija nudi nevjerojatnu mobilnost i praktičnost kod kuće i olakšava spajanje na Internet izvan kuće. Danas mnogi koriste u kućanstvu nekoliko računala i nekoliko osoba želi istodobno pristupiti Internetu. Bežične su mreže popularne jer vam nisu potrebni kabeli do svakog računala. Osnovna bežična mreža zahtijeva dvije komponente: bežičnu karticu ili čip u računalu i pristupnu točku, koja se još naziva i bežični usmjerivač. Pristupna točka povezuje svaki mehanizam koji koristi za spajanje na Internet: telefonsku utičnicu, DSL modem ili kabelski modem. Nedostatci u slučaju bežične tehnologije su veliki. Problemi idu u rasponu od bežičnih „nametnika“ koji se spoje na vašu vezu s Internetom i besplatno surfaju do lopova i drugih kriminalaca koji kradu osjetljive informacije. Današnje bežične mreže temelje se na skupu standarda koji se zajednički nazivaju Wi-Fi što znači bežična odanost (eng. *Wireless fidelity*) [Conry-Murrax,2005].

Praktičnost Wi-Fi mreža koje se nazivaju i bežične lokalne mreže (eng. *Wireless Local Area Networks ili WLAN-ovi*) ima svoju cijenu: ozbiljno narušavanje privatnosti i sigurnosti. Bežična kartica ili čip u računalu i pristupna točka su zapravo radio prijemnici. Signale koje šalju bežični uređaji može uhvatiti bilo koji uređaj unutar dometa, a ne samo korisnikova pristupna točka. Napadači to znaju pa koriste programe koji se nazivaju sniferi i koji im omogućuju „prisluškivanje“ nešifrirane bežične veze. Bežične mreže nisu samo za dom. Mnoga javna mjesta, uključujući kafiće, restorane, hotele… nude bežične mrežne veze. Ti javni WLAN-ovi nazivaju se vruće točke (eng. *hotspots*) i održavaju nevjerojatnu praktičnost i potražnju za bežičnim povezivanjem. Ako koristite javne vruće točke, trebali biste poduzeti

korake za osiguravanje veze uz postavljanje vlastite zaporke prilikom priključivanja na vašu mrežu [Conry-Murray,2005].
Trenutno postoje tri metode šifriranja za bežične mreže: Wi-Fi zaštićeni pristup (WPA i WPA2), Wired Equivalent Privacy (WEP) i 802.1x.

2.8.1 Zaštićeni bežični pristup (WPA)

Zaštićeni bežični pristup (eng. *Wi-Fi Protected Access, WPA*) Za WPA i WPA2 korisnik mora navesti sigurnosni ključ da bi se omogućilo povezivanje. Nakon provjere ključa svi podaci koji se šalju između računala ili uređaja i pristupne točke šifriraju se.

Dvije su vrste WPA provjere autentičnosti: WPA i WPA2. Ako je moguće, koristite WPA2 jer je najsigurniji. Gotovo sve nove mrežne kartice podržavaju WPA i WPA2, ali neke starije ne. Kada se koristi osobni WPA i osobni WPA2, svi korisnici dobivaju isti pristupni izraz. To je preporučena konfiguracija za kućne mreže. Korporacijski WPA i korporacijski WPA2 osmišljeni su za kompatibilnost s poslužiteljima za provjeru autentičnosti koji koriste standard 802.1X, a svakom korisniku distribuiraju različite ključeve. Taj način obično se koristi u poslovnim mrežama [Microsoft].

2.8.2 Wired Equivalent Privacy (WPE)

WEP je starija metoda zaštite mreže koja je još uvijek dostupna za zaštitu starijih uređaja, ali se više ne preporučuje. Kada omogućite WEP, morate postaviti mrežni sigurnosni ključ. Taj ključ šifrira informacije koje jedno računalo šalje drugom putem mreže. No zaštitu WEP relativno je lako razbiti. Postoje dvije vrste WEP zaštite: provjera autentičnosti otvorenog sustava i provjera autentičnosti zajedničkim ključem. Nijedna od te dvije metode nije u potpunosti sigurna, ali provjera autentičnosti zajedničkim ključem je nesigurnija. Za većinu bežičnih računala i bežičnih pristupnih točki zajednički ključ za provjeru autentičnosti isti je kao statički ključ za WEP šifriranje (ključ koji koristite da biste osigurali mrežu). Zlonamjeran korisnik koji uhvati poruke prilikom uspješne provjere autentičnosti zajedničkim ključem može pomoću alata za analizu odrediti zajednički ključ za provjeru autentičnosti i tako saznati statički ključ za WEP šifriranje. Kada sazna ključ za WEP šifriranje, zlonamjeran korisnik ima potpun pristup mreži. Zbog toga ova verzija sustava Windows ne omogućuje automatsko postavljanje mreže pomoću ključa za WEP šifriranje [Microsoft].

3 SIGURNOST DJECE NA INTERNETU

Djeca danas u sve ranijim godinama dobivaju pristup Internetu. S jedne strane to je vrlo pozitivna činjenica jer im Internet može poslužiti kao izvanredan alat za prikupljanje novih znanja i informacija, širenje vidika i spoznaja te naravno , zabavu. Negativna strana priče su brojne opasnosti kojima je dijete danas izloženo i koje, isključivo za dobrobit djeteta, nužno zahtijevaju povećan oprez roditelja i ostalih odgovornih osoba (nastavnika, skrbnika i sl.) [sigurnost.tzv.hr]. Nasilja na Internetu sve je više, a u okruženju virtualne komunikacije na prvi se pogled čini da zakon, tehnologija, škole i roditelji mogu učiniti vrlo malo kako bi ga zaustavili. Djeci je dostupnije sve više moćnih tehničkih sredstava, a odrasli, nažalost, najčešće nisu svjesni opasnosti koje tehnologija nosi sa sobom. Često ne kontroliraju što djeca rade različitim tehničkim pomagalima zato što ili nemaju vremena ili ih je strah da ne naruše privatnost vlastite djece. Mnogi roditelji se i zbog vlastitog neznanja i neiskustva u elektroničkom području osjećaju nesigurnima i nemoćnima da uopće pokrenu pitanje pravilna korištenja. Često se osjećaju prilično bespomoćnima, jer ne znaju što učiniti [Buljan Flander,2007].

3.1 CYBERBULLYING

Nasilje preko Interneta, u svijetu poznato kao cyberbullying, opći je pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opće dobro. Tim oblikom nasilja među vršnjacima obuhvaćene su mogućnosti kad je dijete ili tinejdžer izloženo napadu drugog djeteta, tinejdžera ili grupe djece, putem Interneta ili mobilnog telefona. Odnosno i počinitelj i žrtva su maloljetnici. Postoje dvije vrste nasilja preko Interneta: izravan napad i napad preko posrednika.

Izravan napad događa se kada maloljetnik:

1) Šalje uznemirujuće poruke mobitelom, elektroničkom poštom ili na chatu
2) Ukrade ili promijeni zaporku za elektroničku poštu ili nadimak na chatu
3) Objavljuje privatne podatke ili neistine na chatu, blogu ili internetskoj stranici
4) Šalje uznemirujuće slike putem elektroničke pošte ili MMS poruka na mobitelu
5) Postavlja internetske ankete o žrtvi
6) Šalje viruse elektroničkom poštom ili mobitelom
7) Šalje pornografiju i neželjenu poštu
8) Lažno se predstavlja kao drugo dijete

Nasilje preko posrednika događa se kad počinitelj napada žrtvu preko treće osobe, koja toga najčešće nije svjesna. Napad preko posrednika najopasnija je vrsta nasilja preko Interneta jer

često uključuje odrasle, među kojima ima mnogo ljudi s lošim namjerama [Buljan Flander,2007].

Stručnjaci ističu da Internet briše društvene kočnice. Dopušta djeci da govore i čine stvari koje ne bi mogli napraviti u interakciji "licem u lice", i ona imaju osjećaj da neće morati odgovarati za takva ponašanja na način na koji bi inače odgovarali za, primjerice, javno izrečene riječi. To im daje lažan osjećaj sigurnosti i moći [Buljan Flander, 2007].

3.2 SEKSUALNI GRABEŽLJIVCI I INTERNET

Činjenica modernog života je ta da seksualni grabežljivci koriste Internet, naročito online sobe za čavrljanje (eng. *chat*), da bi pronašli potencijalne žrtve [Conry-Murray, 2005]. Prema rezultatima istraživanja Poliklinike za zaštitu djece grada Zagreba, više od 50% djece svakodnevno se koristi Internetom, a 27 % ih je izloženo porukama seksualnog sadržaja ili nekom drugom obliku internetskih prijetnji [os-brodarica.hr]. Uglavnom mladi korisnici Interneta primaju nepoželjne seksualne ponude. Otvorena priroda ovih soba olakšava započinjanje online konverzacije koja obično počinje bezazlenim razgovorima. S vremenom kada grabežljivci zadobiju povjerenje djeteta , mogu započeti dodatni razgovor na privatnom mediju kao što su elektronička pošta, istovremene poruke (eng. *Instant messaging*) ili čak telefon. Ovaj se problem pogoršava iz dana u dan jer su djeca manje oprezna na Internetu nego što su u realnom svijetu, djelomice zato što Internet pruža lažan osjećaj anonimnosti i sigurnosti. Mlađa djeca podložna su manipulacijama i mogu razviti pogrešno povjerenje u online „prijatelje". S obzirom da djeca imaju veliki pristup Internetu nije idealno rješenje zabraniti pristup sobama za čavrljanje. Potrebno je razgovarati sa djecom o potencijalnim opasnostima na Internetu, uputiti ih da ne otkrivaju svoja imena, dob, adresu ili telefonske brojeve, te da ne šalju svoje fotografije online. Potrebno je nadzirati online aktivnosti svoje djece [Conry-Murray, 2005].

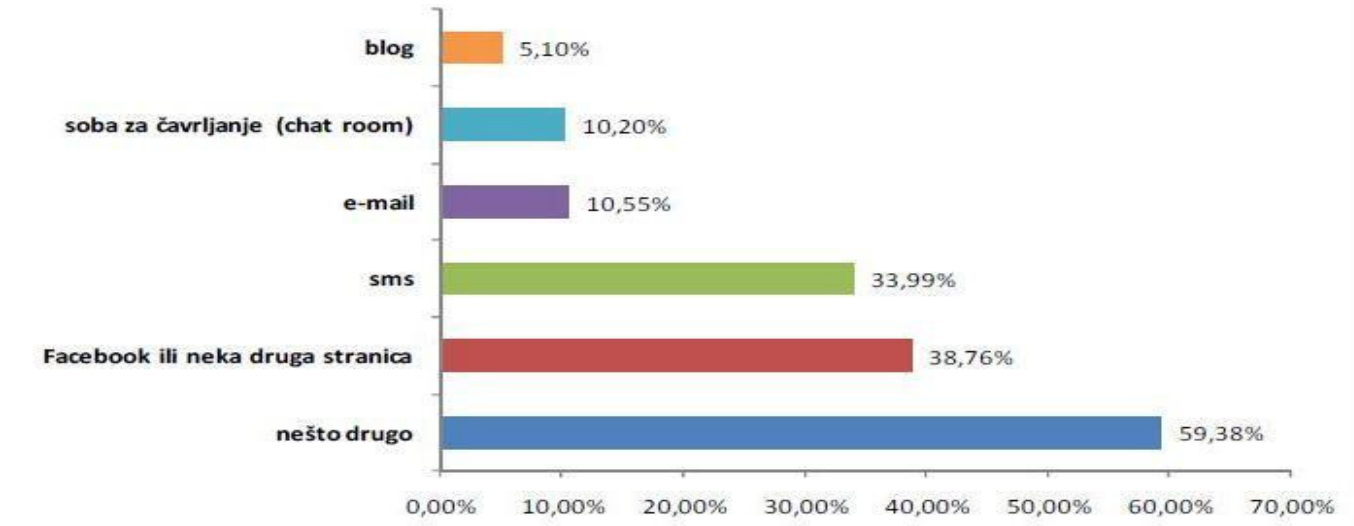
3.3 ISTRAŽIVANJA U SKLOPU PROGRAMA PREVENCIJE ELEKTRONIČKOG NASILJA

Ured UNICEF-a je proveo istraživanje na uzorku 23 osnovne škole iz cijele Hrvatske koje su uspješno završile osnovni program prevencije vršnjačkog zlostavljanja. Uzorak čini 8 škola iz velikih gradova, 7 škola iz manjih gradskih sredina te 8 manjih seoskih škola. U Istraživanju je sudjelovalo 5215 učenika u dobi od 10 do 15 godina 2484 roditelja i 759 učitelja. Većina roditelja je između 31 i 40 godina starosti. Istraživanje je provedeno 2010. godine.
Već iz prvih upitnika rezultati su pokazali da većina učenika ima vlastiti mobitel (96%), računalo je prisutno u većini domova (95%), pristup Internetu od kuće ima 85% učenika i roditelja te 91% učitelja. Gotovo polovica učenika i nešto manje učitelja navodi da

svakodnevno pristupa Internetu, kao i trećina roditelja. Zabrinjavajuća je gotovo petina od ukupnog broja roditelja (17,55%) koja nikada ne pristupa Internetu, što je i statistički značajno u odnosu na broj djece (6,71%) koja se ne koriste Internetom .
Osim učestalosti korištenja, upitnikom je ispitana i svrha korištenja Internetom. Omiljene aktivnosti učenika na Internetu su traženje zabavnih sadržaja (glazba, filmovi, igre), dopisivanje s prijateljima te korištenje specijaliziranim stranicama za druženje (Facebook, MySpace i sl.). Iz školskih iskustava znamo da se djeca, a i roditelji, susreću s poteškoćama ograničavanja i kontrole djetetovog vremena provedenog na Internetu. Dječaci, u skladu s očekivanjima, više istražuju sadržaje na Internetu te su skloniji avanturizmu i rizičnom ponašanju. Pokazalo se da dječaci češće u odnosu na djevojčice vrijeme na Internetu provode na forumima i sobama za čavrljanje. Kako je razvojno prirodno, djeca se u pubertetu i adolescenciji više okreću vršnjacima, pa im je zato i potrebno da na više načina i svakodnevno budu u kontaktu s njima.
Rezultati nam pokazuju i kako su učitelji vičniji korištenju Internetom od roditelja, što osnažuje našu strategiju prevencije nasilja i rizičnih ponašanja u virtualnom svijetu putem škole, jer učitelji koristeći se više ovim medijem mogu bolje i utemeljenije raspravljati s učenicima o njihovim iskustvima, doživljajima i kretanjima u tom svijetu te im mogu biti bolji vodiči.
U percepciji prednosti i opasnosti elektroničkih medija razlikuju se djeca koja doživljavaju nasilje kroz navedene tehnologije od one koja ga ne doživljavaju. Rezultati pokazuju kako djeca koja ne trpe elektroničko nasilje percipiraju statistički značajno pozitivnijima prednosti elektroničkih medija i značajno manjima opasnosti elektroničkih medija od djece koja to nasilje trpe. Djeca koja čine elektroničko nasilje doživljavaju elektroničke medije više pozitivnima i manje opasnima, dok djeca koja trpe to nasilje doživljavaju ih manje pozitivnima i opasnijima od prosjeka. Internet je prostor u kojem djeca sklona nasilju mogu zadovoljiti svoju potrebu za kontrolom i moći, pritom je zbog prostorne distance i odsustva svjedočenja neposredne reakcije povrijeđenog djeteta još manja mogućnost za suosjećanje, a nema niti vidljive opasnosti ili rizika od reakcije drugih, osobito odraslih. Djeci sklonoj nasilju elektronički mediji čine izbjegavanje odgovornosti za vlastito ponašanje još lakšim i emocionalno distanciranijim. To posebno vrijedi za djecu sklonu zlostavljanju jer ona (kao, uostalom, i odrasli) to čine s namjerom da ponize (uspostave odnos nadmoći) i pritom su relativno hladna, proračunata i kontrolirana. Online komunikacija ohrabruje ljude/djecu da djeluju agresivnije i motivira ih na radnje koje u realnom životu možda ne bi bili u stanju izvršiti.
Ukupno gledajući prema Olweusovom kriteriju (2-3 puta mjesečno i češće) 4,90% učenika doživljava neki oblik vršnjačkog nasilja putem elektroničkih medija, 29% ih to doživi 1-2 puta mjesečno, a 66,20% nikada nije doživjelo elektroničko nasilje.

Među učenicima koji trpe elektroničko nasilje (2-3 puta mjesečno i češće), dakle koju zlostavljaju, gotovo 40% djece to doživi putem Facebooka ili neke druge specijalizirane stranice za druženje, a više od 30% putem SMS-poruka (Slika 9). Udio djece koja su zlostavljana kroz ova dva vodeća elektronička oblika statistički se značajno razlikuje u korist

Facebooka. Uvjerljivo vodstvo Facebooka očekivano je s obzirom na njegovu popularnost i učestalost korištenja među učenicima, ali i višestruke načine virtualne komunikacije koje takve stranice omogućavaju – komentiranje statusa na profilu, postavljanje i označavanje („tagiranje“) fotografija, dopisivanje porukama, igranje online igrica, čavrljanje (eng. *chat*) i sl., ali i osnivanje različitih grupa koje su „za“ ili „protiv“ nekoga ili nečega.



Slika 10 Učestalost pojedinih oblika elektroničćkog nasilja među djecom koja ga trpe 2-3 puta mjesečno i češće [unicef.hr]

Gledajući ukupan rezultat, pet najčešćih odgovora na elektroničko nasilje su povjeravanje u prvom redu roditeljima, zatim prijatelju, nekoj odrasloj osobi, bratu/sestri te prestanak posjećivanja problematične stranice ili blokiranje osobe koja ih vrijeđa.

Roditelji i učitelji imaju dobar uvid u svrhe za koje se djeca koriste Internetom, s tim da učitelji smatraju da djeca više vremena provode na stranicama za odrasle, na forumima i tražeći sadržaje vezane za školu nego što iskazuju djeca sama. Što se tiče stavova o prednostima i opasnostima elektroničkih medija (računala, interneta i mobitela), pokazuje se da djeca uočavaju prednosti više nego roditelji i učitelji, dok su roditelji najviše svjesni opasnosti. Učitelji se i u odnosu na prednosti i opasnosti nalaze negdje između roditelja i učenika [Unicef,2010].

3.4 KRATKI SAVJETI ZA DJECU

1) Nikad ne daj osobne informacije na Internetu, bilo na chatu, blogovima ili osobnim Web stranicama.
2) Nikad nikome, osim roditeljima, ne reci svoju zaporku, čak ni prijateljima.

3) Ako ti netko pošalje zlonamjernu ili prijeteću poruku, nemoj odgovoriti. Pokaži je odrasloj osobi kojoj vjeruješ.
4) Nikad ne otvaraj poruke elektroničke pošte koje ti pošalje netko koga ne poznaješ ili netko za koga već znaš da je zlostavljač.
5) Ne stavljaj na Internet ništa što ne želiš da vide tvoji prijatelji iz razreda
6) Ne šalji poruke kad si ljut. Prije nego što klikneš "Pošalji" zapitaj se kako bi se ti osjećao da primiš tu poruku.
7) Pomogni djeci koju na taj način zlostavljaju tako da ne prikrivaš nasilje i da odmah obavijestiš odrasle.
8) I na internetu poštuj pravila ponašanja kao i u svakodnevnom životu [Buljan Flander, 2007].

4 ZAKLJUČAK

Za pisanje završnog rada o sigurnosti rada na Internetu potaknulo me gubljenje vlastitog Facebook profila. Osim vlastitog iskustva sa krađom identiteta medije svakim danom sve više pune naslovi o hakerskim napadima. Navedimo samo neke od njih: "Palestinski hakeri napali najveće američke banke i financijske institucije", "Hakeri napali GoDaddy, srušili su milijune stranica na par sati", "Hakeri napali web stranice Europskog parlamenta" itd. Ovo su samo neki od primjera i to u zadnjih par mjeseci. Sve ovo me potaklo da malo detaljnije upoznam tko se sve bavi računalnim napadima, na koji način mogu napasti te kako se zaštiti od napada. Problem napada na računalne sustave u svijetu intezivno je prisutan već nekoliko godina, a posebno je došao do izražaja pojavom Interneta, kao otvorene mreže arhitekture. Napadi na računalne sustave postali su omiljenim sportom milijuna maloljetnika diljem svijeta. Anonimnost je jedna od temeljnih karakteristika kompjutorskog kriminaliteta. Nedostatkom zakonske regulative kompjuterski kriminal se sve više širi. Udruge kriminalaca i poslovne organizacije bez reputacije stječu profite pisanjem programa koje ne biste željeli na svojem računalu. Upravo radi takvih programa potrebno je imati antivirusne programe na svom računalu te se educirati na koje još načine zaštititi vlastito računalo. Svakim danom ljudi sve više stvari obavljau preko Interneta. Danas najpopularniji su online kupovina, internet bankarstvo, razna preuzimanja s Interneta i sl. Prilikom bilo koje od tih radnji potrebna je registracija, tj davanje osobnih podataka. Potrebno je biti vrlo oprezan kod davanja osobnih informacija na Internetu, bez obzira kako profesionalno i „ozbiljno“ izgledaju Web stranice. Nikada ne smijemo davati podatke o broju kreditne kartice, o adresi, telefonskom broju i sl. ukoliko nismo na „sigurnim“ tj. zaštićenim Web stranicama.

Internet je postao i velika opasnost za djecu. Danas sve mlađa djeca, ne samo učenici nižih razreda, već i djeca predškolskog uzrasta, kreću u avanturu kako upotrebe računala, tako i istraživanja milijuna mrežnih mjesta koja su im dostupna u svega nekoliko klikova mišem. Ovo nije nimalo čudno jer su djeca praktično od rođenja okružena raznim digitalnim i elektroničkim uređajima koji, uz njihovu znatiželju, vrlo brzo i vrlo lako postaju njihovi svakodnevni „nerazdvojni prijatelji“ u odrastanju. Za snalaženje djece na Internetu nužno je znanje korištenja računala, vještina procjene vrijednosti informacija te ostale vještine najčešće obuhvaćene terminom informacijska pismenost. Isto tako za korištenje Interneta potreban je i dobar odgoj. Baš kao što se djeca za život u stvarnom svijetu u svojim obiteljima pripremaju dobrim odgojem, te ukazivanjem na loše i dobre postupke, tako se i za korištenje računala i Interneta trebaju pripremiti ponajprije u školama, s naglaskom na osvješćivanje vidljivosti i javnosti osobnih informacija na Internetu.

5 LITERATURA

[Kiš, 2002] Miroslav Kiš ,2002 „*Informatički rječnik*“, drugo izdanje, naklada Ljevak Zagreb

[Conry-Murray, 2005] Andrew Conry-Murray i Vincent Weafer , 2005 „*Sigurni na Internetu*“, Tiskara Zelina

[Franjić, 1999] Franjić Marko, 1999 „*Digitalna ekonomija*“ Internet -budućnost poslovanja , Digimark d.o.o, Zagreb

[Čavar, 2010] grupa autora,Ivan Čavar…, 2010 „*Sigurnost računalnih mreža*“

[Buljan Flander, 2007] Gordana Buljan Flander , 2007 „*Nasilje preko interneta*“,Grad Zagreb

[Wiki1] „*Internet*“
URL: http://hr.wikipedia.org/wiki/Internet

[Wiki2] „*Hakeri*“
URL: http://hr.wikipedia.org/wiki/Hakeri

[Wiki3] „*Krađa identiteta*“
URL: http://hr.wikipedia.org/wiki/Kra%C4%91a_identiteta

[Wiki4] „*Adware*“
URL: http://hr.wikipedia.org/wiki/Adware

[Wiki5] „*Antivirusni program*“
URL: http://hr.wikipedia.org/wiki/Antivirusni_program

[Wiki6] „*Zločudni software*“
URL: http://hr.wikipedia.org/wiki/Zlo%C4%87udni_softver

[Wiki7] „*Spam*“
URL: http://hr.wikipedia.org/wiki/Spam

[Wiki8] „*Kriptografija*“
URL: http://hr.wikipedia.org/wiki/Kriptografija

[Wiki9] „*Hoax*“
URL: http://hr.wikipedia.org/wiki/Hoax

[Wiki10] „*Backup*“
URL: http://bs.wikipedia.org/wiki/Backup

[sigurnost.tzv.hr] „*Sigurnost i zaštita na internetu*“
URL: http://sigurnost.tvz.hr/

[Belošević,2011] „*Zaštita računalnih sustava vatrozidom*“, Anđelko Belošević
URL:http://www.scribd.com/doc/76941838/3/Povijest-vatrozida#page=6

[unicef] URL:http://www.unicef.hr/upload/file/353/176706/FILENAME/Izvjesta j_-_Iskustva_i_stavovi_djece_roditelja_i_ucitelja_prema_elektronickim_medijima.pdf

[os-brodarica.hr] URL: http://www.os-brodarica.skole.hr/sigurnost-djece-na-internetu.pdf

[Cert.hr] „*O hoaxima*“
URL:http://www.cert.hr/hoax

[Buzdo.com] „*Backup*“
URL: http://www.informatika.buzdo.com/s722.htm

[Microsoft.com] URL: http://windows.microsoft.com/hr-HR/windows7/Set-up-a-security-key-for-a-wireless-network

[Slika1] http://tektype.wordpress.com/2010/06/18/small-business-owners-are-a-hackers-favorite-target/
[Slika2] http://athome.allentate.com/2010/08/protect-against-identity-theft/
[Slika3] https://elementa.otpbanka.hr/gradjani/upute/token.htm
[Slika4] http://www.plus.hr/hosting/ssl
[Slika5] http://www.certtechs.com/escuela/windows%20xp%20learning/windows%20xp%20english/internet/Internet%20Explorer%20Add-ons%20Toys%20and%20Tools.html
[Slika6] http://en.wikipedia.org/wiki/Firewall_(computing)
[Slika7] http://fly.cc.fer.hr/~zox/diplomski/Java_i_PGP.html
[Slika8] http://fly.cc.fer.hr/~zox/diplomski/Java_i_PGP.html

[Slika9] http://www.unicef.hr/upload/file/353/176706/FILENAME/Izvjestaj_-_Iskustva_i_stavovi_djece_roditelja_i_ucitelja_prema_elektronickim_medijima.pdf