VISOKOTEHNOLOŠKI KRIMINAL – ŠTA JE TO?

Visokotehnološki kriminal obuhvata skup krivičnih djela gdje se kao objekat izvršenja i kao sredstvo za izvršenje krivičnog djela javljaju računari, računarske mreže, računarski podaci, kao i njihovi produkti u materijalnom i elektronskom obliku.

Ova definicija uključuje veliki broj zloupotreba informacionih tehnologija, kao i oblast zloupotreba u radio-difuznim tehnologijama. Tako se razlikuju krivična djela gdje se računari pojavljuju kao sredstvo izvršenja (Computer Related Crime) i kao objekat izvršenja (Computer Crime), kao i krivična djela u čijem se načinu izvršenja pojavljuju elementi nezakonitog korištenja Interneta.

Broj i vrste krivičnih djela iz oblasti visokotehnološkog kriminala, kao i ekonomska šteta koja nastaje izvršenjem ovih krivičnih djela, veoma je teško procijeniti. Međutim, broj izvršenja krivičnih djela i ekonomska šteta koja je do sada registrovana iz godine u godinu u stalnom je porastu. Načini izvršenja krivičnih djela, zbog same prirode savremenih informacionih tehnologija, veoma su raznoliki i sve sofisticiraniji.

KORISNI SAVJETI ZA ZAŠTITU RAČUNARA

1. Uvijek držite Vaš zaštitni program na računaru uključen:

Ova vrsta računarskog programa štiti Vaš računar od pokušaja izvršilaca krivičnih djela da pristupe Vašem računarskom sistemu, da oštete ili izbrišu Vaše podatke, otuđe korisnička imena i lozinke, ili druge osjetljive informacije.

2. Instalirajte i uvijek vršite ažuriranje antivirus programa na Vašem računaru

Funkcija antivirus programa je da spriječi ubacivanje računarskih virusa u računarske sisteme korisnika. Ukoliko otkriju njihovo prisustvo, oni upozoravaju korisnika o tome, ili ih automatski brišu. Računarski virusi mogu da zaraze računar i bez znanja njegovog korisnika. Veliki broj antivirus programa može da se podesi tako da se njihovo ažuriranje vrši automatski.

3. Ažurirajte operativni sistem na Vašem računaru

Operativne sisteme instalirane na računaru potrebno je ažurirati kako bi se ispratio razvoj tehnologije i kako bi se sigurnosni propusti na vrijeme otkrili i uklonili. Postarajte se da Vaš računar ima najnoviju zaštitu.

4. Pazite kada vršite „download“, tj. kada preuzimate različite sadržaje sa Interneta na svoj računar

Neki sadržaji na Internetu osmišljeni su i napravljeni, od strane izvršilaca krivičnih djela, tako da mogu da zaobiđu i najsavremeniju antivirusnu zaštitu. Nikada ne otvarajte priloge elektronskih poruka koje su Vam stigle od osoba koje ne poznajete i pazite kada vam stižu poruke u čijim se prilozima i od poznatog pošiljaoca. Moguće je da pošiljalac koga poznajete ni sam nije svjestan šta se nalazi u prilogu poruke koju vam je proslijedio.

5. Ugasite Vaš računar kada pored njega niste prisutni:

Sa porastom velikog broja Internet konekcija sa velikom brzinom protoka mnogi korisnici su stekli naviku da računare ostavljaju uključene i spremne za rad u bilo kom trenutku. Gašenjem računara izvršiocima krivičnih djela se onemogućava da preuzmu kontrolu nad njegovim radom ukoliko je isti zaražen računarskim virusom. Na taj način izbjegavate da postanete žrtva zloupotrebe (kao npr. da postanete dio botnet mreže bez vašeg znanja i pristanka).

Krađa identiteta

Krađa identiteta zloupotrebom informacionih tehnologija je, sa ekspanzijom upotrebe Interneta, postala jedna od najčešćih aktivnosti izvršilaca krivičnih djela. Korištenje informacionih tehnologija, od strane korisnika koji nisu dovoljno upućeni u opasnosti koje ih očekuju pri

upotrebi ličnih podataka koji čine njihov identitet na Internetu, dovelo je do stvaranja velike količine ličnih podataka koji su lako dostupni izvršiocima krivičnih djela, koji ih kasnije u pravilu zloupotrebljavaju.

VEOMA JE VAŽNO DA ZNATE:

Sadržaji tipa keygene, crack i mnogi drugi koji se mogu besplatno skinuti sa Interneta, vrlo često su zaraženi nekim tipom zlonamjernog programa, a ponekad se iza njihove instalacije u stvari krije i sam zlonamjerni program, koji korisnik koji ga je „skinuo“ sa Interneta pokreće, ne znajući o čemu se zapravo radi, na taj način nesvjesno kompromitujući svoj računar.

KORISNA UPUTSTVA ZA ZAŠTITU VAŠIH LIČNIH PODATAKA

1. Prije nego što bilo kome proslijedite informacije o sebi saznajte kako će se koristiti i da li će i kome, od strane primaoca, dalje biti prosljeđivane.
2. Ukoliko vršite plaćanje preko Interneta redovno vršite kontrolu stanja na vašem računu, vodite računa o tome na koju Internet stranicu se logujete, na njen izgled i sigurnosne protokole koji se na tim stranicama koriste.
3. Vodite računa o Vašoj elektronskoj pošti koju ste proslijedili, kao i o onoj koju primate. Nemojte odgovarati na poruke sa oznakom SPAM ukoliko niste sigurni da poznajete pošiljaoca, pošto se ,uglavnom, zapravo radi o rizičnim porukama namijenjenim da se vaš računar kompromituje ili da se metodama socijanog inžinjeringa dođe do Vaših ličnih i drugih podataka od značaja za izvršioce krivičnih djela.
4. Čuvajte podatke sa Vaših platnih kartica, podatke o Vašim bankovnim i drugim računima i izbjegavajte korištenje ličnih podataka na Internetu kao što su, npr. datum rođenja, broj telefona i sl.
5. Nemojte davati informacije o sebi putem telefona, preko elektronskih poruka ili na Internet servisima ukoliko niste sigurni ili ne znate sa kim komunicirate.
6. Čuvajte informacije u elektronskom obliku na sigurnom mjestu i ukoliko postoji mogućnost, na uređajima bez Internet konekcije ili na prenosivim nosačima memorije (USB, prenosivi hard disk i dr.).
7. Lozinke za elektronske naloge za poštu i dr., nikada nemojte da čuvate automatski u poljima za unos.
8. Kada vršite download sa Interneta vodite računa o tome koje podatke ostavljate prilikom registracije, pošto se ti podaci od strane izvršilaca krivičnog djela vrlo često na ovaj način prikupljaju radi njihove dalje zloupotrebe (vrlo čest slučaj je da se podaci prikupljaju na Internet sajtovima sa pornografskom sadržinom koji su pod kontrolom izvršilaca krivičnih djela, sa Internet sajtovima preko kojih se mogu preuzeti različiti zabavni multimedijalni sadržaji kao što su računarske igrice i dr).
9. Kada god je moguće izbjegavajte postavljanje Vaših fotografija na Internetu koje mogu biti javno dostupne drugim korisnicima, bez mogućnosti kontrole.

SAVJETI RODITELJIMA

Bez obzira na Vaša iskustva i stavove, djeca i mladi neizbježno dolaze u kontakt sa računarima i komunikacionim tehnologijama. Informatika je i dio školskog programa. Važno je znati da će Vaša djeca koristiti računarsku tehnologiju i da je teško, pa i štetno za njihov razvoj zabraniti im korištenje mobilnih telefona, računara i Interneta.

Iskustva pokazuju da nadzor roditelja i nadgledanje dječijih aktivnosti na Internetu predstavljaju važan korak u zaštiti djece i mladih, ali i da samo taj vid zaštite nije i dovoljan.

Roditelji nisu u prilici da stalno nadgledaju aktivnost svoje djece na Internetu. Djecu treba naučiti da računare koriste na siguran način, a ne „da ih vode za ruku". Kao što djecu učimo kako da rješavaju probleme sa uznemirujućim i neugodnim događajima u svakodnevnom životu i kako da prepoznaju i izbjegnu opasnost na ulici i u svojoj okolini, važno je naučiti ih kako da bezbjedno koriste Internet i kako da prepoznaju moguću opasnost i izbjegnu rizična ponašanja. Takođe, važno je naučiti djecu i mlade o preuzimanju odgovornosti za svoje ponašanje i o posljedicama određenih postupaka, koje pogađaju njih same, ali i druge s kojima su u kontaktu.

Potrebno je poštovati njihovu nezavisnost, interese i aktivnosti u skladu s njihovim uzrastom, kao i koristiti poruke prilagođene njihovom uzrastu. Chat, blog, forum i slična mjesta na Internetu, gdje djeca i mladi mogu razmjenjivati mišljenja i komunicirati, vrlo su popularna, pa su stoga i privlačna osobama koje žele da zloupotrijebe njihovo povjerenje na Internetu. Zloupotreba vršnjaka najčešće uključuje prijeteće poruke, vrijeđanje i širenje glasina, ucjene koje jedno dijete, ili više njih, upućuju drugom djetetu.

Zlopotrebe odraslih najčešće uključuju lažno predstavljanje i manipulisanje sa ciljem pridobijanja djece i mladih, da bi se ona navela na nepoželjna ponašanja (najčešće seksualna).

Ako saznate da je Vaše dijete bilo izloženo nasilju putem Interneta, potrebno je da preduzmete sledeće korake:

- naučite dijete da ne odgovara na nasilne, prijeteće ili bilo koje druge sumnjive poruke i pozive;
- ne brišite poruke ili slike jer mogu poslužiti kao dokaz;
- kontaktirajte Vašeg Internet provajdera i prijavite da ste primili takvu poruku;
- kontaktirajte školu i obavijestite ih o ponašanju/zlostavljanju ili eventualnim promjenama raspoloženja i ponašanja kod djeteta;
- kontaktirajte policiju ako poruke sadrže prijetnje nasiljem, uhođenje, napastvovanje, dječiju pornografiju i sl., ili kada prethodni koraci nisu dali rezultate;
- ako Vam je poznat identitet izvršioca, broj ili elektronska adresa sa koje su uznemirujuće i zlonamjerne poruke upućene, svakako obavijestite o tome policiju, mobilne operatere, Internet provajdera, školu...

Trebalo bi da razgovarate sa svojom djecom o računarskoj etici, da dogovorite pravila ponašanja na Internetu, a kao najvažnije, definišete posljedice kršenja tih pravila.

Posmatrajući internet kao savremenu pojavu koja je posljednjih godina zaživjela u velikoj mjeri, moramo istaknuti posljedice koje njegova neograničenost ima kada je u pitanju širenje govora mržnje.

Prema podacima navedenim u istraživanju američke agencije Gallup, u Bosni i Hercegovini 49% domaćinstava ima direktan pristup internet mreži. Takođe, u istraživanju je navedeno da su internet u najvećoj mjeri prihvatili mladi, posebno dobi 15-24, među kojima se njih gotovo tri četvrtine služi internetom. Studenti i učenici su grupa koja se najviše od svih služi internetom (84%), a slijede ih stalno zaposleni (50%), dok se među penzionerima nalazi samo oko 4% korisnika.

Ovi podaci govore da su mladi u najvećoj mjeri izloženi govoru mržnje u online prostoru, ali i najveći kreatori istog. Uticaj interneta utoliko raste, budući da nove generacije odrastaju uz korišćenje socijalnih mreža i drugih komunikacionih alata kao osnovnog vida komunikacije, zbog čega granica između virtuelnog i realnog postaje sve teža za razlikovati. Također, u velikom broju slučajeva, mladi se osjećaju sigurnije u virtuelnom svijetu gdje grade svoj identitet, što često

može dovesti do ozbiljnih posljedica po njihovo mentalno zdravlje, ukoliko isti bude žrtva govora mržnje usmjerenog ka pojedincu.

Anonimnost na internetu

Mnogi korisnici imaju utisak da su na internetu anonimni, naročito ako koriste usluge internet provajdera koji garantuju anonimnost. Međutim, potpuna anonimnost na internetu je ograničena zbog upotrebe IP adresa koje, u principu, omogućavaju da se identifikuje kompjuter sa kojeg je pristupljeno internetu, mada ne i sam korisnik.

Postoji mnogo načina da se uđe u trag vašem identitetu kada koristite internet. Stoga budite oprezni kada svoje lične podatke ostavljate na mreži, i ne preduzimajte nikakve radnje za koje niste spremni da preuzmete odgovornost. Ukoliko koristite bežičnu lokalnu mrežu (WLAN) budite svjesni da postoje razni alati koji omogućavaju napade na ovu mrežu. Rizici mogu biti umanjeni ukoliko aktivirate sve sigurnosne mjere na mreži. Takođe, obratite pažnju na to da promijenite lozinke jer standardne lozinke proizvođača su javno dostupne i poznate svima.

Rizici upotrebe interneta za djecu

Najčešći rizici upotrebe interneta za djecu i mlade su:

- Izlaganje seksualnim ili nasilnim sadržajima, kao i dostupnost neprimjerenim informacijama koje uključuju pornografiju, materijale i stranice koje potiču mržnju, nesnošljivost ili diskriminaciju, krvave i nasilne prizore, dezinformacije,preuvaličavanje vijesti.
- Direktna komunikacija sa odraslom osobom koja traži neprimjerene odnose, gdje djeca i mladi mogu postati žrtve pedofila ili odraslih osoba sa seksualnim namjerama koji će ih pokušati nagovoriti na susret ili na neki drugi način izigrati njihovo povjerenje (npr. objavljivanja slika maloljetnihlica).
- Izloženost uznemirujućim, neprijateljskim ili nepristojnim e-mail porukama.
- Pretjerana izolovanost djece i mladih koja proizilazi iz prečestog ili dugotrajnog korištenja računaraiinterneta.
- Djeca i mladi putem interneta mogu doći do informacija, kupovati proizvode i učestvovati u aktivnostima koje su za njih opasne. Postoji rizik da kupovinom putem interneta, popunjavanjem obrazaca ili učestvovanjem u raznim online takmičenjima daju važne, lične i finansijske podatke, te tako mogu postati meta različitih prevara.

Internet omogućava anonimnost koju je nemoguće postići u bilo kojoj drugoj vrsti komunikacije. Ova anonimnost omogućava ljudima da komuniciraju intimnije nego što bi to inače radili prilikom ličnih susreta, a takođe im daje priliku da se lažno predstave. Upravo zbog toga, potrebno je edukovati djecu i mlade kako da na siguran način koriste internet, upoznati ih sa načinima (samo)zaštite, ali i obezbjediti i nadzor roditelja u trenucima kada koriste internet.

Nasilje preko interneta u svijetu poznato kako „cyberbullying“, opšti pojam za svaku komunikaciju cyber tehnologijom koja se može smatrati štetnom kako za pojedinca, tako i za opšte dobro.Ovim oblikom nasilja među vršnjacima smatraju se situacije kad je dijete izloženo napadu drugog djeteta ili grupe njih putem interneta ili mobilnog telefona.

Postoje dvije vrste nasilja preko itnerneta:

- direktan napad

- napad preko posrednika.

Direktan napad događa se kada maloljetnik:

- šalje uznemirujuće poruke mobitelom, mail-om ili na chat-u
- ukrade ili promjeni lozinku za e-mail ili nadimak na chat-u
- objavljuje privatne podatke ili neistine na chat-u, blogu ili internetskoj stranici
- šalje uznemirujuće slike putem mail-a ili MMS poruka na mobilni
- postavlja internetske ankete o žrtvi
- šalje viruse na e-mail ili mobilni
- šalje pornografiju ili neželjenu poštu na e-mail ili mobilni
- lažno se predstavlja kao drugo dijete.

Nasilje preko posrednika događa se kad počinitelj napada žrtvu preko treće osobe, koja toga nije svjesna.

Primjera radi, neko djete dozna lozinku drugog djeteta za njegovu e-mail adresu ili nadimak na chat-u, pa sa njegove e-mail adrese može slati uznemirujuće poruke njegovim prijateljima, ostavljati neprimjerne poruke na blogu, chat-u ili forumu. Svima se zapravo čini da je žrtva zapravo ta koja čini loše stvari i prijatelji će se posvađati s njim, administrator će isključiti njegov nadimak ili e-mail adresu, rodtelji će se naljutiti na njega i biće kažnjen.
Takođe, počinitelj može staviti oglas seksualnog ili provokativnog sadržaja u ime žrtve s njenim brojem telefona ili adresom. Na taj način dijete može doživjeti mnoge neugodnosti i naći se u opasnosti.
Napad preko posrednika najopasnija je vrsta nasilja preko interneta, jer često uključuje odrasle, među kojima ima mnogo ljudi s lošim namjerama. Bez fizičkog kontakta s publikom, djeca teže vide i razumiju štetu koju njihove riječi mogu nanijeti.

Nasilje na chat-u

Chat je vrlo popularan kod mladih, pa je zbog toga i privlačan osobama koji ga žele zloupotrebiti. Zloupotreba vršnjaka najčešće uključuje prijeteće ili ucjenjujuće poruke koje jedino dijete ili više njih upućuje drugom djetetu. U takvih slučajevima treba biti oprezan, jer nasilnik može biti opasna osoba.

Kako se na chatu zaštiti od nasilja:

- Nadimci kojima se predstavljate pri korištenju ove usluge, može u velikoj mjeri uticati na druge – bilo bilo bi dobro izabrati nadimak koji će vas zaštiti od mogućeg nasilja i koji ga neće poticati.
- Većina chatova sadrži mogućnost blokiranja ili ignorisanja, kojima se zaustavljaju daljnje poruke od neželjenih korisnika. Ako je riječ o nekome ko je jednostavno dosadan, blokiranje poruka je najčešće dovoljno da se problem zaustavi. Ali, ako se radi o osobi koja iznosi stvarne prijetnje, važno je da o tome obavijestite odraslu osobu u koju imate povjerenja.
- Kontaktirajte administratora koji potom moje onemogućiti dolazak poruka određenih nadimaka, od kojih su prije dolazile neugodne ili nasilne poruke.
- Nikad ne dajte svoje pravo ime ili podatke o sebi na chatu, jer je nemoguće znati govori li druga osoba istinu ili ima loše namjere.

Nasilje na forumu

Od svih oblika komunikacije na internetu, forumi su najčešće najbolje organizovani. Na njima se nalaze administrator (jedan ili više njih) i moderatori, zaduženi za posebne dijelove foruma. Oni čitaju sve teme i diskusije, te paze da ne bude vrijeđanja, prijetnji, objavljivanja privatnih podataka i kršenja prava. Na većini foruma postoji mogućnost „obavijestiti moderatora“ ispod nečijeg zapisa, tako da jednim klikom možete obavijesiti moderatora o nekome ko zloupotrebljava forum. Moderator ili administrator će izbrisati taj zapis, upozoriti korisnika ili mu zabraniti pristup ako se to ponovi.

Nasilje putem bloga

Nasilje putem blogova odnosi se najprije na „otimanje“ blogova drugim ljudima (žrtvama), te nadopunjavanje ličnim uvredama ili seksualnim sadržajima. Takvim oblikom nasilja narušava se ugled i ugrožava privatnost druge osobe. Toj vrsti međuvršnjačkog nasilja posebno su podložna djeca koja šalju fotografije i svoje lične podatke s ciljem da pronađu prijatelje na internetu. Takvu djecu nasilnici zlostavljaju preko njihove lične internetske stranice. Naime, komentari koji se nadopisuju u blogove kod žrtve uzrokuju stres i nemir, a ovisno o jačini, mogu dosegnuti i stepen zlostavljanja.Šteta učinjena nasiljem preko interneta može zaista biti velika. Tinejdžeri ponekad zaboravljaju, posebno kad je riječ o blogovima, da bilo šta objavljeno na internetu ima i neželjenu publiku, a samim tim i neželjene posljedice, koje u ekstremnim slučajevima mogu dovesti i do destruktivnog i autodestruktivnog ponašanja.

Kako sigurno koristiti blog?

Ako koristite blog, uvijek postoji šansa da neko pronađe vaš blog, a to mogu upravo ljudi za koje najmanje želite i očekujete da vas pronađu. Činjenica je da svako može pronaći vaš blog, ako je u njemu u bilo kojem obliku naveden vaš identitet.

Kako održavati privatnost bloga?

- zaštitite blog lozinkom. Ako je neko zna, neka to budu vaši roditelji
- ne navodite u blogu lične i detaljne informacije. Kad pišete o sebi, pišite što uopštenije. Nemojte navoditi gdje živite, gdje izlazite i slično, jer svaka lična informacija može otkriti vaš identitet
- ne spominjite u blogu nikakva imena, adrese, brojeve telfona, školu, e-mail adrese i slične informacije. To su upravo informacije koje traže pedofili, zato ih izbjegavajte. U zamjenu, možete upotrebljavati nadimak. Nastojte da on ne podsjeća na vaše ime
- ne navodi u blogu ni informacije o bilo kome koga poznajete, kako ne biste mogućeg pedofila informisali da, iako vi niste zainteresovani za „čavrljanje“ s njim, vaša prijateljica Maja jeste
- ne stavljajte fotografije vas i vaših prijatelja na blog
- ne ostavljajte blog otvorenim, a računar bez nadozra, jer bi neko mogao napisati nešto nepoželjno
- ne ogovarajte i ne širite tračeve o svojim prijateljima iz razreda
- nemojte biti u rezultatima pretraživanjima. Ako ne želite da se vaš blog pojavljuje u rezultatima pretrajivanja, možete kreirati poseban fajl u kojem će te od pretrajivačkih službi zatražiti da ignorišu vaš domen. Takav fajl imaće naziv robots.txt

Zloupotreba slika

Oprezno sa slikama!

- Lijepo je ukrasiti svoj blog ili web-stranicu fotografijama, ali ako se na njima može prepoznati vaše lice, lica članova vaše porodice ili prijatelja, onda možete biti u opasnosti kao da piše vaše puno ime i prezime, te adresa stanovanja. Pokušajte ne stavljati svoje i fotografije svojih prijatelja i porodice, a ako ipak želite, mogu se jednostavno prilagoditi tako da lica nisu prepoznatljiva.

Maliciozni softver

Maliciozni softver, ili skraćeno malver (malware), je softver koji je dizajniran da se infiltrira u kompjuterski sistem, bez informisanja i pristanka njegovog vlasnika. Ovo je opšti termin koji koriste stručnjaci da opišu različite oblike neprijateljskog, nametljivog, ili dosadnog softvera ili programskog koda. Izraz "kompjuterski virus" je izraz koji obuhvata sve tipove malicioznog softvera.

Odluka da li će se softver smatrati malicioznim, tj. zlonamjernim, se zasniva na namjeri njegovog tvorca prije nego na njegovim funkcijama. U ovu grupu spadaju:

- kompjuterski virusi
- crvi (worms)
- trojanci
- softver koji tajno prati korisnika (spyware)
- izmjenjeni reklamni softver (dishonest adware)
- softver napravljen za potrebe visokotehnološkog kriminala, kao npr. za pristup online računima (crimeware)
- softver kreiran za dobijanje administratorskog pristupa sistemu (rootkit), kao i drugi zlonamjerni i neželjeni softver.

Najjednostavniji i najefikasniji način da se zaštitite od ove vrste opasnosti jeste da koristite odgovarajući antivirusni softver. Antivirusni softver mora biti redovno održavan u skladu sa uputstvima koja se nalaze u samom programu. Ovo je neophodno jer se svakodnevno pojavljuju novi virusi i drugi maliciozni softver zbog čega proizvođači antivirus softvera svakodnevno proširuju svoje baze podataka kako bi omogućili korisnicima da uspješno zaštite svoj računar. Ukoliko je vaš sistem zaražen malicioznim softverom potrebno je da se diskonektujete sa interneta i uz pomoć antivirus softvera skenirate računar i otklonite maliciozni softver. Takođe, redovno pravite kopije svih podataka koji su vam bitni zato što ne postoji apsolutna zaštita od virusa i drugog neželjenog softvera.

Softverska piraterija

Zakoni kojima se štiti autorsko pravo, u većini zemalja odnose se i na softver.

Koristite samo softver za koji posedujete odgovarajuću licencu. Pored licenciranog i zaštićenog softvera, postoje i programi koje možete koristiti besplatno, tzv. freeware programi koji su kao takvi jasno obilježeni. Ukoliko imate nedoumice u vezi softvera koji koristite na vašem radnom mestu konsultujte stručno lice u vašem preduzeću zato što licence za pojedine programe omoguavaju korištenje i na vašim privatnim računarima.

Zaštita podataka

Kako bi zaštitili podatke od neovlašćenog pristupa preporučljivo je da koristite tzv. BIOS lozinku i screensaver lozinku. Ukoliko posjedujete povjerljive podatke na računaru postoji i metod enkripcije cjelokupnog hard diska u realnom vremenu (ovi podaci će uvek biti skladišteni na disk kao enkriptovani).

Najsigurniji način zaštite podataka od neovlašćenih lica jeste da obezbedite da ova lica nemaju pristup vašem računaru. Međutim, ukoliko šaljete podatke putem elektronske pošte ne možete biti apsolutno sigurni da će ovim podacima imati pristup samo ono lice kojem su upućeni. U ovim slučajevima preporučuje se upotreba enkripcije. Jedan od najpoznatijih programa za kriptografiju je Pretty Good Privacu, poznatiji kao PGP, ali postoje i mnogobrojni slični programi koje možete pronaći na internetu. Uz pomoć navedenih programa moguće je obezbijediti elektronsku poštu, hard disk, folder sa podacima pa čak i pojedinačni Word dokument.

Zloupotreba internet naloga

Nažalost, prilično su popularni i učestali pokušaji da se na internet pristupi preko tuđeg naloga (tzv. ATO - Acconut Takeovers). Osnovna ideja je da se izbjegne plaćanje ili da se, iz određenog razloga, preuzme nečiji identitet.

Mijenjajte svoju lozinku za pristup internetu sa vremena na vrijeme i ne koristite kratke ili proste lozinke. Ne koristite istu lozinku za različite namjene, npr. za obezbjeđenje vašeg računara, pristup elektronskoj pošti i pristupanje drugim nalozima. Ne otkrivajte svoju lozinku čak ni članovima svoje porodice a naročito djeci. Ovo je naročito važno ukoliko koristite usluge vaše banke za plaćanja preko interneta. Ukoliko neko zloupotrebi lozinku za pristup vašem računu preko interneta banka vam neće nadoknaditi gubitak zato što ste svoju lozinku otkrili drugom licu čak i ako se radi o članu porodice. Ukoliko pristupate svojoj elektronskoj pošti sa računara koji nije vaš, po povratku kući promijenite svoju lozinku.

Elektronska trgovina

Kako se, u današnje vrijeme, sve više ljudi odlučuje da koristi internet za kupovinu otvorene su mogućnosti krađe podataka o računima.

Preporučljivo je da kupovinu preko interneta vršite samo preko sajtova koji nude odgovarajuću zaštitu i bezbjednost. Nikada ne kupujte robu preko interneta ostavljajući broj svoje kreditne kartice i datum njenog isteka bez enkripcije (prilikom kupovine trebalo bi da jasno vidite oznaku tzv. (padlock image) koja ukazuje da se radi u sigurnoj konekciji i da vaši podaci neće biti dostupni neovlaštenim licima. Ukoliko kupujete preko interneta, redovno provjeravajte stanje na svojim računima.

Nedozvoljeni sadržaj

Pojedini sadržaji i baze podataka smatraju se nelegalnim (npr. dječija pornografija, pretnje upućene drugim ljudima, rasistički materijali i sl.)

Ukoliko dođete u posjed navedenih sadržaja o tome odmah obavijestite lokalnu policiju.

PRAVNA REGULATIVA

Upoznavanje djeteta sa pornografijom/Proizvodnja i prikazivanje dječije pornografije
(Članovi 212.KZ FBiH, čl.209.KZ BD, čl.200.KZ RS)

Pored različitih naziva, kod ovog krivičnog djela, razlike se ogledaju i u tome što u st. 1. KZ FBiH i KZ BD propisuju kažnjavanje novčanom kaznom ili kaznom zatvora do jedne godine, "ko djetetu18 proda, prikaže ilijavnim izlaganjem ili na drugi način učini pristupačnim spise, slike, audiovizuelne i druge predmete pornografskog sadržaja ili mu prikaže pornografsku predstavu," dok KZ RS-e, (st.1., čl.200.), propisuje kažnjavanje istom kaznom kao u KZ FBiH, i KZBD, ali radnju izvršenja nešto šire određuje i propisuje; "ko nudi, distribuira, prikaže ili javnim izlaganjem ili na drugi način učini dostupnim spise, slike, audiovizuelne I druge predmete koji predstavljaju dječiju pornografiju ili ko takve materijale radi toga proizvodi, nabavlja ili drži ili ko prikaže dječiju pornografsku predstavu'', ne navodeći da se kažnjavanje za navedene radnje odnosi na počinioca koji ih čini prema dijetetu, već u st. 2., predviđa kažnjavanje kaznom zatvora od 3 godine "ako je djelo izvršeno prema licu mlađem od 16 godina," koju odredbu ne sadrže KZ FBiH i KZ BD.

Iskorišćavanje djeteta ili maloljetnika radi pornografije
(Član 211. KZ F BiH)

(1) Ko dijete ili maloljetnika snimi radi izradbe fotografija, audiovizuelnog materijala ili drugih predmeta pornografskog sadržaja, ili posjeduje ili uvozi ili prodaje ili raspačava ili prikazuje takav materijal, ili te osobe navede na u čestvovanje u pornografskoj predstavi, kaznit će se kaznom zatvora od jedne do pet godina.

(2) Predmeti koji su bili namijenjeni ili upotrijebljeni za u činjenje krivičnog djela iz stava 1. ovog člana oduzet će se, a predmeti koji su nastali učinjenjem krivičnog djela iz stava 1. ovog člana oduzet će se i uništiti.

Izvod iz Krivičnog zakona F BiH koji se odnosi na krivična djela iz oblasti kompjuterskog kriminala – PDF

Konvencija o kibernetičkom kriminalu – PDF