VISOKA ŠKOLA STRUKOVNIH STUDIJA ZA INFORMACIONE TEHNOLOGIJE

Socijalni i pravni kontekst računarstva

Seminarski rad

KRIMINAL NA INTERNETU

Beograd
24.01.2011

Predmetni nastavnik:
mr. Vladimir Simović

Student:
Čedomir Novaković 37/08

Sadržaj

Rezime

Razvojem internet tehnologija i web servisa dolazi I do sve veće zloupotrebe kako interneta tako i računara radi sticanja protiv pravne imovinske koristi ili čak da bi se nekom napakostilo bez ikakvog posebno razloga. U ovom seminarskom radu upoznaćemo se sa nekim napadima hakera, vrstama kriminala na internetu i mogućnostima zaštite.

Ključne reči

Internet kriminal, kriminal na internetu, cyber kriminal, hakerski napadi

Uvod

Razvojem Internet prodavnica na mreži javila se još jedna bolest koja zahvata sve više maha –cyber kriminal. Pod ovim pojmom podrazumevaju se sve protivzakonite aktivnosti koje pojedinac ili grupa koristi za pribavljanje dobra i uvećanje sopstvene koristi. Postoji više oblika kriminala preko Weba. Najeksponiranije i najrašireniје su prevare lažnim kreditnim karticama, postavljanje lažnih web prodavnica i obaranje sajtova poznatih firmi uz istovremeno korišćenje njihovog domena.

Kriminal na internetu

Internet je jedan veliki virtuelni prostor, na njemu se može naći veliki broj podataka, velika količina informacija, sve u svemu veoma mnogo sadržaja raznih oblika. Posljednjih godina se to sve više i više povećava, i Internet još više raste, što je veoma pohvalno, jer se društvu stvarno mnogo nudi, i može se sve naći. Ali zna se da ništa nije savršeno, tako i Internet nije savršen. Javlja se problem, kakav se sadržaj nalazi na Internetu, u kojoj količini se to pojavljuje, i najviše u kojoj meri to utiče na društvo. Ali nije samo u pitanju sadržaj, već u poslednje vreme jedan od najvećih problema je i kriminal, tj. cyber kriminal. Na Internetu se javljaju razni oblici cyber kriminala, kao što je to navela profesorka Mirjana Drakulić u svom tekstu „Cyber kriminal". Najčešći oblici kriminala su haking, cracking, krađa identiteta, vremena, lozinki, i raznih drugih podataka. A u poslednje vreme se češće pojavljuju i upadi u razne firme, banke, preduzeća, što ostavlja za posledicu, krađu velikih suma novca, vrednih informacija, podataka i sličnog. Mnogo toga se dešava na Internetu, a da mi to sami ne znamo, i nemamo predstavu šta se uopšte dešava na Internetu. To je zaista jedan veliki problem, na koji se mora što prije rešiti, da bi Internet barem koliko toliko postao sigurno mesto na kome ljudi mogu da uče, da traže informacije i slično.

Zaista mnogo sadržaja se može naći na Internetu, a na povećanje količine sadržaja na Internetu utiču ljudi. Od njih samih zavisi koliko će se sadržaja pojaviti na svetskoj mreži. Ovde se javlja isto tako jedan veliki problem, verujem da pretpostavljate šta je to, u pitanju je kvalitet sadržaja. Da li je taj sadržaj štetan, kako on utiče na društvo, kakve posledice ima, mnogo se tu problema može javiti. Zadnjih godina se mnogo štetnog sadržaja pojavilo na Internetu, i veoma se malo radi da se to otkloni. Postavlja se pitanje ko je odgovoran za to. Odgovor se može naći gore u tekstu. To su ljudi koji su odgovorni za postavljanje takvog sadržaja, ljudi koji prave takav sadržaj, koji ga postavljaju na Internet. Najviše oni trebaju da snose odgvornost za to. Ali nisu samo oni u pitanju, odgovornost treba da snose ljudi koji podržavaju taj sadržaj, jer i oni na neki način utiču na širenje štetnog i nedozvoljenog sadržaja na Internetu. Ti ljudi koji im daju podršku, koji im obezbeđuju prostor gde će smestiti taj sadržaj. Svi oni od toga imaju koristi, zato se broj ljudi koji to radi povećava, jer smatraju da će imati koristi od toga. I zbog toga što ne postoji adekvatna kontrola sadržaja na Internetu, ti ljudi imaju uspeha. Štetan sadržaj na Internetu je samo jedan mali dio cyber kriminala. Mnogo toga se dešava na Internetu, mnogo veće stvari nego što je nedozvoljen sadržaj.

Da bi se to sprečilo treba uvesti neke kazne za odgovorne ljude. Te kazne treba da budu zaista stroge, bilo da je to finansijska kazna, ili zatvorska kazna. Mislim da je to jedan od boljih načina suzbijanja kriminala, jer smatram da bi to najviše uticalo na svest ljudi, i da bi počeli da drugačije razmišljaju pre nego što se odluče na bilo koji oblik kriminala. Mogu vam navesti nekoliko primera gde se to pokazalo kao jedno od dobrih rešenje za poboljšanje situacije: Povećanje kazni za prekršaje u saobraćaju (Srbiji); povećanje kazni za veliku količinu alkohola u saobraćaju (Hrvatska); povećanje kazni za ugrožavanje zelenila i okoline (Republika Srpska); i slično. Posledice toga su bile zaista zapažene, kriminal je u nekim slučajevima čak bio smanjen za 50 %, što je zaisat veliki rezultat. Zato mislim da bi kazne za svaku osobu koja je odgovorna za bilo koji oblik cyber kriminala, trebala zaista da budu velike, jer po mom mišljenju to je jedan od rešavanja problema kriminala na Internetu.

Stručnjaci za internet upozoravaju da je globalna mreža postala utočište organizovanog kriminala i dodaju da je opasnost od onlajn terorizma naša stvarnost. Na nedavnom kongresu u Londonu o elektronskim zločinima, zvaničnici NATO-a su skrenuli pažnju da onlajn špijunaža i terorizam na internetu predstavljaju neke od najopasnijih pretnji globalnoj bezbednosti.
Dok ljudi vredno rade na svojim kompjuterima – rade i stotine hiljada virusa i programa koji kruže internetom i napadaju kompjutere iz dana u dan. Pored toga što su iritantni, ti bagovi prete modernom životu. Britanski opozicioni zakonodavac Dejvid Dejvis je na konferenciji u Londonu upozorio da su rizici koje predstavlja sajber terorizam vrlo realni.

Predstavnici NATO alijanse opominju da će sa otkrivanjem potencijala koje pruža internet, pretnje postajati sve ozbiljnije i kažu da sajber terorizam predstavlja veću opasnost od udara projektila. Stručnjak za pitanja bezbednosti na internetu, Majko Hipen kaže da su zaraženi kompjuterski programi veoma zabrinjavajući.

Nikada nismo videli ovako lošu situaciju. Dobijamo sve više zaraženih programa i mnogi ljudi su zaprepašćeni, jer ne vide to na svojim kompjuterima. Međutim, virusi se i dalje prave, a hakeri koji su to ranije radili iz zabave, su sada profesionalci koji se time bave za novac.

Današnji kriminal može biti toliko ležeran, a rezultati za kriminalca i više nego uspešni, sve iz razloga što živimo u dobu Internet komunikacija. Onaj ko je Internet stvorio

samo u nastojanju da služi kao sredstvo komuniciranja grdno se prevario jer kriminal na Internetu buja poput gljiva nakon kiše. Postojeća činjenica jest da su računari postali sastavnim dijelom modernog života, ali neki ljudi u tom životu nalaze idealan način da razornim putem dođu do novca. Osobe koje se bave takvim radnjama mediji su nazvali 'hackeri', ali u daljnjem tekstu mi nećemo koristiti taj naziv već ćemo ih isključivo nazivati kriminalcima. Pritom ne mislimo na bubuljičave tinejdžere koji elektroničkom poštom šalju BackOriffice ili provaljuju u Pentagon, već o pravim kriminalcima kojima sve to nije puko istraživanje i otkrivanje rupa nego lak način zarade. Na Internetu česta meta kriminalca nisu samo bankovni sistemi i sistemi firmi već i informacije čija je vriednost financijski neprocenjiva. 'Informacija je moć' rekao je jedan drevni filozof, a kriminalci koji su se sjatili na Internetu to su i više nego dobro prihvatili.

Kriminal na Internetu vrlo često ne mora biti direktan već i indirektan u obliku neke prevare. Elektronska prodaja putem Interneta danas je vrlo popularna i njen razvoj rapidno raste, no kako bi mogli nešto kupovati potrebno je unesti svoje lične podatke i broj kreditne kartice. Mnoge brošure o Internet sigurnosti vrlo često navode kako je putem Internet najsigurnije kupovati od poznatih tvrtki. Oni koji nisu slušali često su se opekli jer su kupovali sa nepoznatih Internet stranica na kojima su cijene bile za čak 50 % manje nego na drugima, a primamljiva ponuda bila je mamac za neiskusne. Par dana nakon kupovine željenog proizvoda stranice su jednostavno nestale sa Interneta, a za tvrtke koje su prodavale proizvodne otkrilo se da su zapravo izmišljene. Vi niste dobili naručenu robu, a kriminalci su dobili broj vaše kreditne kartice koja je do trenutka kada ste saznali da ste zapravo opljačkani mogla biti opterećena do maksimuma. Internet je nepredvidljiv, a kriminal na njemu najbrže rastući dosada.

Kriminal ne znači samo krađa već i nezakonita zarada kao npr. prodaja pornografskih i pedofilskih materijala na Internetu. Ovakav oblik kriminala zadire daleko od bilo kojih moralnih granica i normalne ljudske svesti. Nažalost ljudi se bave svakakvim radnjama i upravo navedena moglo bi se reći da je jedna od težih ljudskih zlodjela.

Rastom kriminala na Internetu raste i rizik takvog poslovanja, no kako bi se rizik smanjio firme u SAD-u su otvorile nove polise osiguranja koje pokrivaju poslovanje novim digitalnim komunikacijama.

E-osiguranje ili E-surance kako je popularno nazvana ova polisa osiguranja pobudila je veliki interes tvrtki koje posluju Online. Osiguravajuće firme koje su već uvele taj oblik osiguranja plaćaju svojim klijentima financijsku nadoknadu uprkos krađi podataka sa sistema ili onesposobljavanja stranica i sistema. Ovakav novi oblik osiguranja nadasve nije jeftin: za manje firme standardna polisa e-osiguranja u SAD-u košta između 30 000 do 50 000 američkih dolara do čak milionskih iznosa. Razlog visoke cene osiguranja leži u velikoj verovatnostii da će upravo vaš računarski sistem ili vaša Internet stranica sutra biti srušena, da li iz zadovoljstva nekog hackera ili pravog kriminalca to treba ostaviti sudu, no svi su svesni kako Internet stvarno može biti opasan, te je važno kako bi opasnosti uočili na vrijeme.

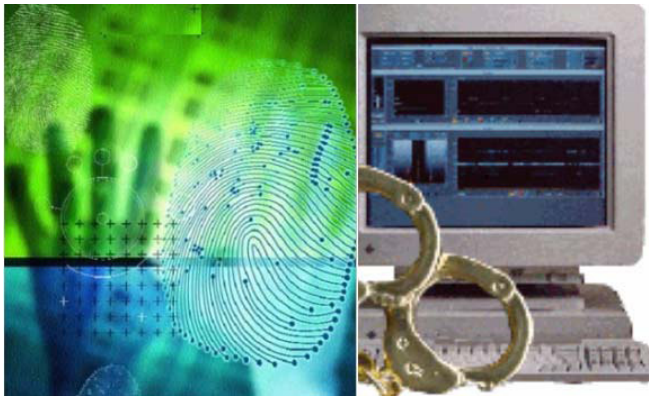
Kompjuteri i kompjuterska tehnologija se mogu zloupotrebljavati na razne nacine, a sam kriminalitet koji se realizuje pomocu kompjutera moze imati obliko bilo kog od tradicionalnih vidova kriminaliteta, ako sto su kradje, utaje, pronevere, dok se podaci koji se neovlasceno pribavljaju zloupotrebom informacionih sistema mogu na razne nacine koristiti za sticanje protivpravne koristi. Pojavni oblici kompjuterskog kriminaliteta su: protivpravno koriscenje usluga i neovlasceno pribavljanje informacija, kompjuterske kradje, kompjuterske prevare, kompjuterske sabotaze i kompjuterski terorizam i kriminal vezan za kompjuterske mreze.

Protivpravno korišćenje usluga i neovlašćeno pribavljanje informacija

Protivpravno korišćenje usluga se sastoji u neovlašćenoj upotrebi kompjutera ili njegovoj ovlašćenoj upotrebi ali za ostvarivanje potreba nekog neovlašćenog korisnika.
Primer neovlašćene upotrebe kompjutera je kada se kompjuter koristi u bilo koje druge svrhe, osim onih koje predstavljaju deo njegove namene u informatičkom sistemu. Primeri ovlašćene upotreba kompjutera, ali za potrebe neovlašćenoh korisnika, ili radi ostvarenja drugih nedopustenih ciljeva su npr., u slučaju kad zaposleni u jednoj firmi pribavi podatke za budućeg poslodavca ili kad raspoloživo kompjutersko vreme koristi za obavljanje nekih svojih poslova. Jedan od najčešćih oblika neovlašćene upotrebe kompjutera sa kojim se susreću poslodavci širom sveta jeste zloupotreba Interneta od strane zaposlenih.

Neovlašćeno pribavljanje informacija predstavlja svojevrsnu krađu podataka sadržanih u kompjuterskim sistemima, najcešće u cilju ostvarivanja protivpravne imovinske koristi. Tehničke i tehnološke mogućnosti za neovlašćeno pribavljanje informacija su sa pojavom Interneta postale mnogostruko veće tako da mete mogu biti i vas lični PC ali i bilo koji povezani ili izolovani kompjuterski sistem.

Krađa na internetu



Slika 1. Kradja na internetu

Kradja zauzima visoko mesto u oblasti kompjuterskog kriminaliteta a u razmatranom kontekstu od posebnog je značaja krađa ideniteta. Ova vrsta krađa predstavlja posebno

društveno-opasnu radnju, jer pored ostalog, znaćajno podriva poverenje u integritet komercijalnih transakcija i ugrožava individualnu privatnost. Procena stručnjaka su da ce ova vrsta krađa rasti sa povećanjem elektronske trgovine. Snabdeveni individualnim personalnim informacijama, kradljivci identiteta mogu da otvore račune u bankama, obavljaju kupovinu, a u u zemljama u kojima su automatizovane servisne usluge za građne, kogu da dobiju certifikate o rođenju, pasos, kredit i sl., a sve to u ime osobe o cijim podacima se radi. Lažnim identitetom kriminalac moze da dobije pozajmicu u banci, kupi auto, stan, ode na putovanje i sl., i na taj način žrtvu moze da optereti finansijsk,i a u nekim slučajevima da joj napravi i kriminalni dosije. Žrtva u većini slučajeva i ne zna da se njen identitet "koristi" sve dok ne dođu računi za naplatu. Dakle i finansijska i "humana" cena krađe za individualnu žrtvu mogu biti veoma visoke, mada jedina krivica za mnoge žrtve moze biti to sto su njihovi presonalni podaci bili na nekom fajlu koji je ukraden ili su naivno davali informacije pogrešnim ljudima.

Iako većina stručnjaka tvrdi da su potrošaci izloženi mnogo većem riziku korišćenjem kreditnih kartica u robnim kućama, restoranima ili benzinskim pumpama nego preko zaštićenih Web sajtova, jer kriptografska tehnologija i autentikacione procedure na Web sajtovima štite on-line transakcije većine kupaca, pitanje privatnosti i strah od malverzacija sa kreditnim karticama u određenoj meri ipak dekuražira on-line nabavke.

Kompjuterske sabotaže i kompjuterski terorizam

Kompjuterske sabotaže se sastoje u uništenju ili oštećenju kompjutera i drugih uređaja za obradu podataka u okviru kompjuterskih sistema, ili brisanju menjanju, odnosno sprečavanju korišćenja informacija sadržanih u memoriji informatičkih uređaja. Najčesci vidovi kompjuterske sabotaže su oni koji deluju destruktivno na operativno-informativne mehanizeme i korisničke programe, pre svega, one koji imaju funkciju čuvanja podataka.

Kako teroristi postaju savremeniji oni sve više ostavljaju puške i granate, a u korist ciljeva visoke tehnologije. Kad je reč o kompjuterskom terorizmu danas postoji realna opasnost da informatički resursi a posebno globalne informatičke mreze postanu i veoma efikasno sredstvo u rukama terorista, omogućavajuci im načine delovanja o kojima ranije nisu mogli ni da sanjaju.

Generalni zaključak kad se radi o kompjuterskom terorizmu bi bi da će u vremenu koje dolazi teroristi sve više koristiti visoku tehnologiju kako za špijunažu i sabotažu tako i za propagiranje svojih ideja. Njihovi ciljevi mogle bi biti banke podataka, računarski resursi, vladini komunikacioni sistemi, elktrocentrale kojima upravljaju računari, rafinerije nafte, aerodromska postrojenja...

Provaljivanje u kompjuterski sistem

Mada izraz "**provaljivanje**" asocira na primenu izvesne mehničke sile, radi ulaska u zatvorene prostore, poput vršenja klasičnih provalnih krađa, on kada je reč o kompjuterskom kriminalitetu označava jedno vrlo suptilno, elektronskim putem, izvedeno, narušavanje tajnosti, pojedinog kompjuterskog sistema, odnosno neovlašćeni elektronski upad u centralni kompjuterski sistem i njegovu bazu podataka. Ovakva dela pretežno vrše hakeri, koji se preko svojih personalnih računara uključuju u druge informativne sisteme, pri čemu prvenstveno koriste Internet. Ovi učinioci spretno zaobilaze zaštitne mehanizme, a dela ne vrše iz zlonamernih pobuda, vec nastoje da javno demonstriraju informatičku veštinu kojom raspolažu ili da ukažu na postojeće slabosti u mehanizmu zaštite kompjuterskih sistema. Zato su na meti ovakvih učinilaca često bas one kompjuterske mreže, za koje se s pravom očekuje da su maksimalno zaštićene od elektronskih provala kao sto su: vojne kompjuterske komunikacije, informatički sistemi obaveštajnih službi, državnih institucija...

Mada se nezlonamerno provaljivanje u kompjuterski sistem, uobicajeno tretira kao najbezazleniji vid kompjuterske delikvencije, ono ni u kom slučaju nije bezopasno. Nime, ovakvi upadi proizvode potencijalnu opasnost prouzrokovanja nepopravljivih šteta na vitalnim kompjuterskim mrežama. Pored toga, u krivičnopravnom smislu ovakvim se delima, ukoliko njima nisu proizvedene određene konkretne štetne posledice, obično vrsi povređivanje službene ili vojne tajne, kroz uvid u zaštićene kompjuterske banke informacija.

Kriminal vezan za komjuterske mreže

Kriminal vezan za kompjuterske mreže je oblik kriminalnog ponašanja kod koga je cybespace okruženje u kome su kompjuterske mreže pojavljuju u trostrukoj ulozi: kao sredstvo ili alat, cilj ili okruženje izvršenja krivicnog dela.

- **Kompjuterske mreže kao cilj napada** – napadaju se servisi, funkcije i sadržaji koji se na mreži nalaze. Kradu se usluge i podaci, oštećuju se ili uništavaju delovi ili celam mreža i kompjuterski sistemi, ili se ometaju funkcije njihovog rada. U svakom slucaju cilj počinilaca je mreža u koju se ubacuju malware, vrše DOS napadi...
- **Kompjuterske mreže kao sredstvo ili alat** - Danas moderni kriminalci koriste sve više kompjuterske mreže kao oruđa za realizaciju svojih namera. Korišćenje ovog novog orudja naročito je popularno kod dečje pornografije, zloupotrebe intelektualne svojine ili online prodaje nedozvoljene robe (droga, ljudskih organa, nevesta..)
- **Kompjuterske mreže kao okruženje u kome se napadi realizuju**. Najčešće to okruženje služi za prikrivanje kriminalnih radnji, kao sto to veoma vešto uspevaju da urade pedofili, a ni drugi kriminlci nisu nista manje uspešni. Naravno postoje i druge uloge, kao sto je npr., korišćenje mreže kao simbola zastrašivanja, uplitanja, koje su nekad više izražene kod kompjuterskog nego kod cyber kriminala. Bitno je da je cyber kriminalu neosporno priznato "svojstvo" kriminala kao "obliku ponašanja koji je protiv zakonit ili ce biti kriminaliozovan za kratko vreme".

Kompjuterske prevare

Kompjuterske prevare se vrše u nameri pribavljanja za sebe ili drugog protivpravne imovinske koristi, s tim što se kod njih u zabludu ne dovodi ili održava neko lice, kao u slučaju običnih prevara, kao imovinskih krivičnih dela, vec se ta zabluda odnosi na kompjuter u koji se unose netačni podaci, ili se propušta unošenje tačnih podataka, ili se na bilo koji drugi način, računar koristi, za ostvarenje prevare u krivično-pravnom smislu. Kompjuterske prevare predstavljaju najrašireniji oblik kompjuterskog kriminaliteta.

Broj oblika prevara, kao i način njihove realizacije je praktično neograničen i u praksi se susreću kako one vrlo primitivne i grube, tako i one prevare kod kojih učinioci ispoljavaju veliki stepen veštine i rafiniranost. Ali u šemama prevare uvek se otkriva neki raniji oblik. Jer skoro sve šeme prevare registrovane na Internetu su ustvari prerađene i prilagođene verzije šema kojima su, nekad i vekovima, obmanjivane neoprezne, lakoverne i pohlepne žrtve.

Ono sto karakteriše kompjuterske prevare ja da one daleko dopiru zbog veličine Interneta kao tržista, da se brzo šire jer sa Internetom kao medijem sve se dešava mnogo brže, i niski troškovi izvođenja ovakvih vrsta prevara .

Prevare sa robom neverovatnih svojstava

Na vrhu liste "svemogućih" proizvoda koji se prodaju na Internetu nalaze se pilule koje omogućavaju svojim korisnicima da piju piva koliko žele, a da se ne ugoje (cena 71 dolar za 60 tableta) i pojas, koji kad se nisi u fotelji izaziva isti efekat kao 600 sklekova urađenih u 10 min (cena 146 dolara), ljuske od jajeta ptice emu koje navodno povećavaju libido, tečnost koja masnoću iz tkiva tokom spavanja pretvara u mišiće, hormoni koji vraćaju veru u sopstvene snage, magneti protiv nesanice, voda koja leči artritis, lekovi za lečenje SIDE , koja dolazi iz Afrike kao rešenje zagonetke zašto neke Afirčke žene imaju imunitet na ovu bolest...

Najčešći način prevare na internetu

- Najčešći način prevara je putem zloupotrbe e-mail poruka. Slanjem velikog broja e-mail poruka pronalazi se zainteresovana osoba. Posle uspostavljanja prvog kontakta, zainteresovanog lica i prevaranta, odnosno prevarant-potencijalna žrtva, prevarant sa razlicitih e-maila šalje "poverljive poruke" koje treba da uvere potencijalnu žrtvu u opravdanost investicije.

- Drugi najčešći način prevara je preko online oglasnih tabli. To se obično čini tako što se u grupe koje komuniciraju na ovaj način ubacuje neko ko "**ima informacije" ili salje** "**poverljive poruke**" i na taj nacin pokušava da podigne cenu

akcija. Pošto se za komunikacije u ovim diskusionim grupama koriste pseudonimi, to je pitanje veoma problemtično.

- Treći najčešći način prevare da sam posrednik koji vam nudi hartije od vrednosti ni sam nije svestan da je žrtva manipulacije. Naime manje firme angažuju posrednike da u njihovo ime kontakriraju potencijalne investitore i da im ponude hartije od vrednosti. To se čini preko Web sajtova, "**chat room**", diskusionih grupa, e-mail poruka i online oglasnih tabli. Tako se može desiti Firma moze biti lazna! Tako vam se može desiti da vam neko nudi (a da ni sam toga nije svestan) hartije od vrednosti lažne firme ili da vi budete angažovani (povedeni obećanom provizijom) da to radite za lažnu firmu.

- Fakcifikovani čekovi - Plaćanje preko interneta sa falsifikovanim čekovima. Često ovi čekovi imaju mnogo veću vrednost od robe koja se kupuje. Kupac-prevarnt šalje falsifikovani ček, i traži od prodavca da mu vrati suvišnu sumu, na račun u stranoj državi. Banke mogu da unovče ček pre nego što je ček zaista "prošao", i žrtva misleći da je sve u redu pošalje novac kupcu-prevarantu.
  Česta je prevara sa kupovinom kola. Kupac šalje ček sa nekoliko hiljada dolara preko cene. Kada ček pristigne, kupac otkaže kupovinu uz izvinjenje i molbu da mu se vrati novac.

- Prijava za posao - Prevarnt ponudi posao, na popularnim sajtovima za pronalaženje posla, i traži da se popuni aplikacija zajedno sa brojem socijalnog osiguranja. Prevarnt poručuje neku robu na kredit sa podacima od prijavljenog. Robu potom šalje drugom prijavljenom kojeg je prevarant zaposlio kao čoveka zaduženog za transport. Roba se potom šalje van države. Potom prevarant koji se predstavio kao strana kompanija, plaća prevoz sa čekom koji značajno prelazi potrebnu sumu. Novac se vraća prevarantu pre nego što prevara bude otkrivena.

- Spoofing - Spoofing je tehika, kojom se služe prevaranti koji se predstavljaju preko e-maila ili web sajta koji pripada nekom drugom. Oni najčešće preko e-maila šalju lik do lažnog web sajta. Lažni web sajt izgleda isto kao i orginalni, na kojem je žrtva prijavljena. Prevaranti preko lažnog web sajta skupljaju šifre za nalog na orginalnom web sajtu ili brojeve kreditnih kartica.

- Roba koja nije isporučena - esto se dešava, da sajtovi, čiji su vlasnici prevaranti, pošto im uplatite novac na račun kako bi vam poslali neku robu, ta roba vama nikada ne bude isporučena.

- Lažno predstavljanje - Prevarant prisvaja lične podatke neke osobe bez njenog znanja. Prevarene osobe često misle da svoje lične podatke npr. broj kreditne kartice prosleđuju legitimnom servisu. U nekim slučajevima odgovaraju na e-mail u kojem su im zatraženi lični podaci radi nastavljanja neke pretplete i slično. Ovo se može izbeći tako što nikada, ne upisujete lične podatke ukoliko adresa ne počinje sa https://, i ukoliko sajt ne uliva poverenje. I naravno nikada ne slati lične podatke preko e-maila.

- Prevare sa kreditnim karticama - Neovlašćeno korišćene kreditne ili debitne kartice, od strane prevaranta. Do broja kartice je moguće doći preko nesigurnih web sajtova na kojim se čuvaju brojevi kreditnih kartica od kupaca. Poznat je i Card-Skimming, a to je kopiranje podata sa kreditne kartice na lažnu kreditnu karticu. Posle ovoga e-krimosi, mogu da koriste karticu kao orginal. Metod je sledeći, na

bankomat ili pos terminal, e-kriminalci ugrade svoj čitač koji će podatke sa vaše kartice zajedno sa PIN brojem da sačuva, da bi isti podaci bili prebačeni na kopiju kartice radi zloupotrebe.

Valentino prevare

Valentino prevare predstavljaju oblik internet prevara sa najvećom stopom rasta. Sama prevara povezana je sa „uslugama" koje se pružaju usamljenim osobama i imaju za predmet sklapanje brakova ili drugi vid druženja.Budući da savremeni način života neretko dovodi do otuđenja nezanemarljiv broj ljudi spreman je da izdvoji abnormalne svote novca i pristaju na praktično sve uslove kako bi rešili svoj problem.

"Srodne duše" nikada ne žive u istoj zemlji kao i žrtva, već naprotiv u zemlji koja je izuzetno udaljena, i koju karakterišu socijalna previranja. Osoba je obično veoma atraktivna, komunikativna i slabog je ili veoma lošeg imovnog stanja.Komunikacija se najčešće odvija putem e-maila i razmenom fotografija.U poslednje vreme neretko dolazi i do angažovanja školovanih osoba privlačnog izgleda kako bi se kontakt odvijao i putem web kamera - to celokupnom odnosu daje viši stepen realnosti, i "žrtve" brže pristaju na ispunjenje zahteva.Nakon proteka određenog vremena, i uspostavljanja bliže veze, prevarant iskazuje želju da upozna svoju "žrtvu", a kako bi došlo do njihovog susreta, neophodno je da "žrtva" pošalje određenu količinu novca da bi njena "srodna duša" mogla da doputuje u udaljenu zemlju.Istog momenta kada dođe do transfera sredstava, kontakt prestaje.Prema podac ima centa za istraživanje kompjuterskog kriminala, žrtve često pristaju da isplate i sume u iznosu od 5000 $US.Valentino prevare nisu jedini tip prevara čiji mehanizam se bazira na zloupotrebi emocija, ali svakako imaju zapaženo učešće u ukupnom broju izvršenih prevara.

Lančana pisma

Lančana pisma predstavljaju takvu vrstu e- mailova u kojima se od vas traži da dobijeni mail prosledite određenom broju u vaših prijatelja.
Neka od ovih pisama funkcionišu zahvaljujući činjenici da se u istima navodi da će osobu koja ne prosledi pismo pratiti nesreća, dok se u drugima navodi da će se određenoj osobi (najčešće detetu sa odredenim telesnim deformitetom) isplatiti izvesna
suma donacije za svaki e - mail koji prosledite.
Nipošto nemojte prosleđivati lančano pismo, a najbolje bi bilo i da ih ne pročitate, odnosno da ih obrišete , budući da takva pisma sadrže kriptovane informacije koje će licu koje je poslalo lančano pismo omogućiti da zloupotrebi vaše lične podatke, ali i podatke vaših prijatelja, kao i svake osobe koja primi i pročita lančano pismo.

Lutrijske prevare

Ovaj vid prevara na internetu ne predstavlja retkost. Sam mehanizam najčešće funkcioniše na sledeići način: mada se verovatno nikada niste prijavili za učešće u nekoj nagradnoj igri ovog tipa, vama stiže obaveštenje u kome se saopštava da ste dobitnik premije.Nakon toga, od vas se ili zahteva da pošaljete izvesnu sumu novca u cilju slanja dobijene nagrade, ili se traži da predate broj vašeg bankovnog računa, kao i da date određene lične podatke. Često se od "žrtve" zahteva da u cilju potvrđivanja prava na

nagradu pozove broj telefona, pri čemu takav poziv karakteriše abnormalno visoka tarifa. Lutrijske prevare omogućavaju sticanje ogromnih količina novca, i iza takvih tipova prevara stoje visokoorganizovane grupe.

Osnovni saveti za sprečavanje prevara

Savet za pocetnike: "Držite se proverenih brokerskih kuća i pouzdanih investicija sve do trenutka kad osetite da vam je znanje toliko da vam omogućava izvesna eksperimentisanja"!

Ne dozvolite da vas "primamljiva" investicija zavede. Koristite zdravu logiku, postavite sebi jednostavno pitanje: " da li investicija zvuči suviše dobro da bi bila istinita"? Ni jedan normalan pošten posao ne može doneti enormne prihode niti je bez rizika. Svako ko nudi "enormne prihode" je sumnjiv. Jednostavno razmišljajte, ne dozvolite da vas želja za profitom sputa, i da samo vidite sebe kako se posle uspešno obavljene investicije odmarate na nekom egzoticnom ostrvu, a da pritom zaboravite sva pravila kako bi ste sprečili eventualnu pravaru.

Osnovna pravila

Morate znati šta i od koga kupujete. Ovo zvuči prilicno jednostavno ali u praksi predstavlja problem. Potrebno je pribaviti sve relevantne informacije, kao što su: koliko dugo dotična firma postoji, kakvi su joj finansijski rezultati, šta proizvodi, ko upravlja investicijama, kada, kako i za koliko se mogu očekivati prvi prihodi i isl...

Morate znati osnovna pravila i uslove pod kojima se obavlja kupovina ili prodaja.

Takođe morate znati i nivo rizika koji se mora podneti pri svakoj obavljenoj transakciji.

Proverite da li je firma u koju se investira (čije se akcije kupuju) registrovana. U SAD ovo se relativno lako moze proveriti u SEC-ovoj bazi **EDGAR**. Ukoliko nije ovde registrovana onda je u **North American Securites Administrators Association (NASAA)**, što može da se proveri na njihovom Web sajtu.

Proverite da li je osoba koja obavlja prodaju ili kupovinu registrovana za taj posao. Ovu proveru je moguće izvesti na Web sajtu **NASD Regulations**, Inc.

Nikad ne zaboravite ove savete i pravila! Svaki put kad ste u situaciji da investirate, setite ih se i vratiće vam se osećaj za opreznost. Razvijajte saopstvena pravila za sprečavanje prevara.

I na kraju moj cilj ce biti ostvaren ako ovaj tekst pomogne da se bar jedna prevara spreči, a vama želimo mnogo uspešnih investicija.

Internet kriminal u Srbiji

Poznata je jedna ovdašnja organizovana grupa koja je uspela da „nasanka" prodavce skupih instrumenata, pa su svakojaka svirala počela da stižu u Srbiju. Ovi prevaranti su otkriveni kada je stigao e-mejl jednog Amerikanca čijoj skupocenoj gitari se gubi svaki trag u Srbiji. Prevaranti su najpre uhapšeni, pa oslobođeni, a kada su sa slobode ponovili prevaru, opet su zatvoreni. A onda - pušteni.

Iako nema tačnih podataka, veruje se da srpski hakeri godišnje u svetu izazovu direktnu štetu od nekoliko desetina miliona evra. Na to treba dodati poprilične milione od masovnog kršenja autorskih prava kroz falsifikovanje kompakt diskova. Indirektno, trpi i ovdašnja privreda jer se u ambijentu sveopšte piraterije ne otvaraju radna mesta, recimo u obećavajućoj industriji softvera.

Razni oblici sajber-kriminala u Srbiji su uzeli maha iz nekoliko razloga. Najpre, prevare omogućavaju hakerima da dođu do tuđeg novca ili do vrednih materijalnih dobara uz malu verovatnoću da će biti otkriveni i kažnjeni. Istovremeno, piraterija kompakt-diskova donosi profit i do 500 odsto, što je daleko više nego kod trgovine narkoticima, a rizik od hapšenja i tužbe je i dalje mali.

Zašto je to tako? Iako je Srbija kao članica Inicijative za elektronsku juoistočnu Evropu u okviru Pakta za stabilnost JIE 2002. potpisala Agendu za razvoj informacionog društva i na taj način se obavezala da će brzo usvojiti Strategiju za razvoj informacionog društva, to je učinjeno tek prošle godine. Ovaj dokument Srbija je usvojila među poslednjima u Evropi.

U Srbiji toga još nema, iako suzbijanje ovakvog kriminala zahteva specijalno obučene pojedince, dobro opremljene službe koje rade 24 časa sedam dana u nedelji. Jer, verzirani inspektori za sajber-kriminal kažu, ukoliko se u toku 12 časova od početka istrage ne prikupe ključni dokazi, slučaj kao da nije ni postojao. Za sada, srpski hakeri lepo prolaze jer posao cveta, a država se još rasanjuje

Zaključak

Videli smo sta znači internet po današnji svet. Kako se pojavom interneta, pojavili i prvi internet kriminalci. Koliko oni mogu da budu loši po društvo, ekonomiju, drzavu, kompanije, firme….itd. Pokušao sam vam objasniti da se širenjem interneta kao prostora, kao nečega bez koga današnji savremen čovek ne može da opstane, stvara mogućnost lake dobiti od strane kriminalaca. Dobija se prostor u kome kriminalci mogu nesmetano da rade razne prevare, krađe, terorizam. Danjašnje društvo je u velikoj opasnosti, i preti mu rat na nekim drugim poljima. Postoje zakoni koji su usvojeni, da bi se kriminal na internetu uništio.

Malo je toga urađeno i samo je nekolicina sitnih prevaranata osuđeno na robiju. Obično oni veći i jači, su nedodirljivi za zakon. Ali za normalnog čoveka postoji niz mera koje mora da uradi i koj se mora striktno pridržavati, da me bi bio prevaren i oštećen. Velike sume novca nestaju sa bankovinih racuna, obaraju se veliki informacioni sistemi, kradu se poverljivi dokumenti, u cilju da se dobije rat protiv države.

U svom radu sam objasnio kakve su to prevare aktuelne, i koje se najčešće upotrebljavaju na internetu. Pokazao sam par mera, kojih se svi moramo prodržavati. Pisao sam o pojavi internet kriminala u Srbiji. Dao sam jedna intervju sa prvim tužiocem na temu Interent kriminal.

Kompanija Sophos objavila je rezultate najnovijeg istraživanja o kriminalu na internetu u prvom polugodištu 2007. godine. Tokom ovoga razdoblja zabeležena je prava eksplozija novih prijetnji i malicioznih programa koji pogađaju web stranice. Reč je o pretnjama koje po broju i rizičnosti prevazilaze i donedavno najraširenije oblike napada putem elektronske pošte, pogotovo kada su u pitanju kriminalci koji putem interneta ciljaju na finansijske resurse kompanija i pojedinaca.

Samo tokom juna Sophosova globalna mreža za praćenje događaja na internetu zabeležila je rekordan broj od 29.700 inficiranih web stranica - dnevno! Za poređenje, početkom 2007. godine dnevno se otkrivalo "samo" 5.000 malicioznih stranica.
Većina web stranica koje sadrže maliciozni kod nalazi se u Kini (53,9%), a zatim slede Sjedinjene Države (27,2%), Rusija (4,5%) i Nemačka (3,5%). Kada su u pitanju kompromitovani sistemi, Apache je prestigao Microsoft IIS.

Literatura

1. http://www.apisgroup.org/sec.html 24.01.2011
2. http://www.sk.co.yu/2004/12/skin01.html 24.01.2011
3. http://megatrender.blog.co.yu/blog/megatrender/megatrender-19/2008/03/06/internet-prevare 24.01.2011
4. http://www.voanews.com/Serbian/archive/2001-10/a-2001-10-10-13-1.cfm 24.01.2011
5. http://www.voanews.com/Serbian/archive/2007-03/2007-03-26-voa3.cfm 24.01.2011