Projekat finansira Evropska unija

e-business DEVELOPMENT

Republika Srbija
Ministarstvo trgovine, turizma i telekomunikacija

Republika Srbija
Ministarstvo privrede

Kako se boriti protiv visokotehnološkog kriminala?

PROJEKAT *RAZVOJ ELEKTRONSKOG POSLOVANJA*

IZDAVAČ:
Projekat *Razvoj elektronskog poslovanja*
www.eposlovanje.biz

NACIONALNI DIREKTOR PROJEKTA:
Željko Rakić, Ministarstvo trgovine, turizma i telekomunikacija

DIREKTOR PROJEKTA:
Sara Širvz (*Sarah Shreeves*), Exemplas ltd.

VOĐA PROJEKTA:
Lešek Jakubovski (*Leszek Jakubowski*), Exemplas ltd.

KORISNICI PROJEKTA:
Ministarstvo trgovine, turizma i telekomunikacija
Ministarstvo privrede

AUTOR:
Siniša Begović, ekspert projekta *Razvoj elektronskog poslovanja*

UREDNIK:
Lešek Jakubovski

SARADNICI:
Branislav Veselinović, Ministarstvo unutrašnjih poslova
Snežana Pavlović, projekat *Razvoj elektronskog poslovanja*

PRIPREMA I ŠTAMPA:
MaxNova Creative

TIRAŽ:
500 kopija

ISBN: 978-86-80388-04-5

Ova publikacija izrađena je u okviru projekta *Razvoj elektronskog poslovanja* koji finansira Evropska unija. Sadržaj publikacije apsolutno izražava stanovišta, mišljenja i stavove projekta *Razvoj elektronskog poslovanja* i ne predstavlja nužno stavove i mišljenja Evropske unije.

Projekat sprovodi konzorcijum predvođen *Exemplas ltd* u saradnji sa: *ACE Consultants, European Profiles, Imorgon, Seidor i Teamnet International.*

Sadržaj

Uvod

Ovaj vodič bavi se izazovima i zahtevima digitalnog sveta koji se neprekidno menja, a čije promene kao rezultat donose sve češće probleme u oblasti visokotehnološkog kriminala. Vodič će povećati svest među potrošačima, malim i srednjim preduzećima i preduzetnicima o zamkama i opasnostima u našoj stalno povezanoj i umreženoj sredini u kojoj brzina i anonimnost interneta dovode do rasta sajber kriminala.

Vodič ima za cilj da potrošačima, malim i srednjim preduzećima i preduzetnicima ukaže šta treba da traže na internetu i koje zaštitne mere da preduzmu. Odgovarajući nivo opreza među potrošačima i malim i srednjim preduzećima sprečiće moguće kriminalne radnje i drastično smanjiti privlačnost i efikasnost ovih kriminalnih aktivnosti. Vodič se bavi zloupotrebama debitnih i kreditnih platnih kartica, krađom identiteta i zloupotrebom ličnih podataka, računarskim prevarama, a koncipiran je tako da čitaocima na jednostavan način prenese informacije i znanja koja su im neophodna kada koriste računare, tablete i pametne telefone.

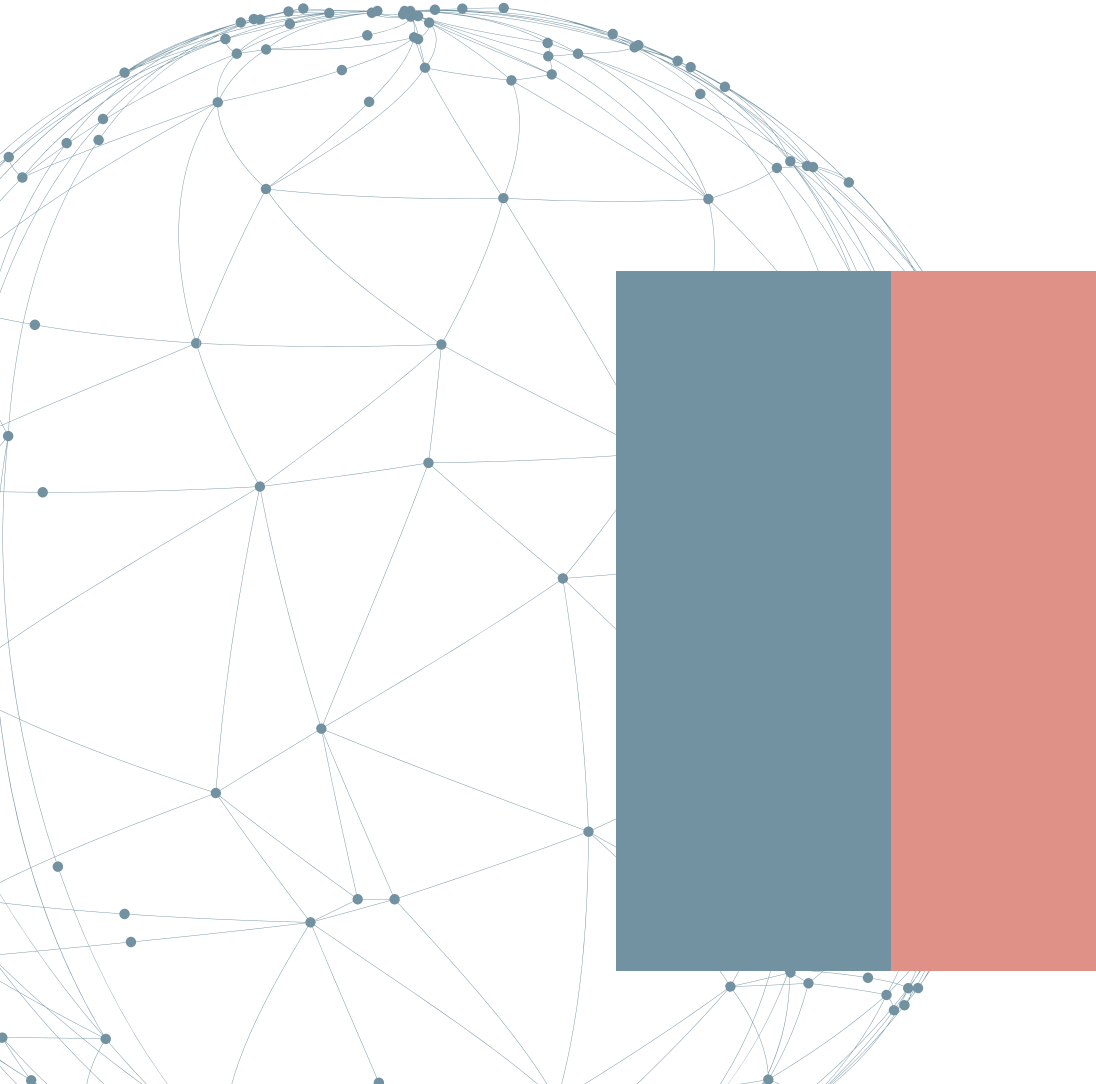
U prvom poglavlju govori se o tome šta potrošači, mala i srednja preduzeća i preduzetnici treba da znaju o visokotehnološkom kriminalu.

Objašnjeni su osnovni termini, elementi i koncepti koje korisnici interneta treba da poznaju. Na kraju svakog odeljka dat je spisak praktičnih saveta kako da se potrošači, mala i srednja preduzeća i preduzetnici zaštite na internetu.

U drugom poglavlju dati su praktični primeri sajber prevara i obmana da bi se čitaoci upoznali sa potencijalnim opasnostima od kojih se treba čuvati. U ovom poglavlju čitaocima je na praktičan način objašnjeno kako da uoče potencijalne sajber kriminalne radnje i kako da reaguju na njih. Kao i u prethodnom poglavlju, dati su praktični saveti šta treba uraditi da bi se smanjila izloženost sajber kriminalu. Na taj način, potrošači, mala i srednja preduzeća i preduzetnici zauzeće proaktivan stav u osiguravanju vlastite bezbednosti na internetu.

U trećem poglavlju govori se o tome kako prijaviti krivična dela vezana za visokotehnološki kriminal. Potrošači se upućuju na relevantne institucije Republike Srbije koje im mogu pomoći i sprečiti ponavljanje ovih krivičnih dela. U ovom poglavlju navedeni su i podaci za kontakt i linkovi ka institucijama koje mogu da pomognu.

1. Šta je potrebno da znate



1.1 Šta je visokotehnološki kriminal, e-kriminal ili sajber kriminal?

Visokotehnološki kriminal, poznat i kao e-kriminal ili sajber kriminal, obuhvata skup krivičnih dela koja podrazumevaju upotrebu interneta, računara ili nekih drugih elektronskih uređaja.

Pojedini oblici e-kriminala direktno su vezani za računare, kao što su širenje opasnih elektronskih virusa ili pokretanje DoS napada (engl. *Denial of Service Attack*) koji onesposobljavaju računarski sistem tako da on odbija da izvrši bilo koju uslugu ovlašćenog korisnika.

Ostali oblici e-kriminala obuhvataju prevare, govor mržnje, krivična dela protiv intelektualne svojine, kao i proizvodnju, posedovanje i distribuciju spornog materijala.

Kako da se zaštitite od e-kriminala?

Informišite se o osnovama bezbednosti na internetu i pažljivo pročitajte ovaj vodič.

Primenite bezbednosne savete na sve oblike elektronske komunikacije, uključujući i komunikaciju putem mobilnog telefona i slanjem SMS poruka.

Informišite članove porodice o osnovama bezbednosti na internetu.

Postavite osnovnu zaštitu na vašem računaru protiv zlonamernih softvera (engl. malware) kao što su virusi i računarski špijuni (engl. spyware).

Ako je reč o preduzeću, postarajte se da Vaše internet transakcije, kao i podaci o Vašim korisnicima/klijentima budu bezbedne.

Ako je reč o preduzeću, osmislite politiku poštene upotrebe na radnom mestu i o njoj obavestite svoje zaposlene tako što ćete je uneti u pojedinačne ugovore. Pratite upotrebu interneta da biste bili sigurni da se ova politika poštuje.

Politika poštene upotrebe predstavlja niz pravila koje primenjuje vlasnik, autor ili administrator mreže, veb-sajta ili usluge kojom se ograničava i propisuje način upotrebe mreže, veb-sajta ili sistema i daju smernice kako ih treba koristiti.

1.2 Šta je krađa identiteta?

Krađa identiteta se događa kada neko prisvoji identitet druge osobe, kao što su ime, detalji o bankovnom računu ili broj kreditne kartice, da bi počinio prevaru ili druga krivična dela.

Krađa identiteta je jedna od kriminalnih aktivnosti koja ima najbrži rast na svetskom nivou i ne poznaje geografske granice – žrtve i prestupnici mogu biti na suprotnim stranama sveta. Zbog toga je policiji teško da istraži ova krivična dela, da uhvati počinioca ili da pomogne žrtvi.

Najveći broj krivičnih dela krađe identiteta počini se uz pomoć računara i drugih elektronskih uređaja. Može da obuhvati krađu:

- *brojeva platnih i kreditnih kartica*
- *pasoša*
- *imena*
- *adrese*
- *podataka iz vozačke dozvole*
- *podataka za prijavljivanje za ostale usluge*

Kako da se zaštitite od krađe identiteta?

Nemojte da dajete svoje lične podatke preko telefona, lično ili preko računara, ukoliko niste sigurni da je reč o proverenoj osobi ili organizaciji.

Nikada ne zapisujte PIN brojeve za svoje platne ili kreditne kartice na samim karticama ili bilo kom dokumentu ili papiru u novčaniku.

Na bezbedan način se rešite ličnih podataka (iscepajte papire, obrišite/uklonite hard diskove iz računara pre prodaje ili bacanja).

Količinu dokumenata koju svakodnevno nosite sa sobom ili ostavljate u kolima svedite na minimum. To su vredni predmeti.

Proverite da li na izvodima iz banke i izvodima o stanju na kreditnoj kartici ima neodobrenih transakcija. Odmah prijavite bilo kakva neslaganja ili neovlašćene aktivnosti banci ili izdavaocu kartice.

Budite naročito oprezni kada ostavljate lične podatke na javno dostupnim veb-sajtovima. Lični podaci mogu biti zloupotrebljeni na više načina od strane kradljivaca identiteta koji pretražuju veb-sajtove.

1.3 Šta je SPAM?

Spamom se obično smatra neželjena elektronska pošta ili neželjene objave u tematskim grupama (engl. *newsgroups*). Opšte gledano, to je elektronska pošta poslata na spisak adresa ili na tematske grupe u kojoj se reklamira neki proizvod. Spameri obično šalju e-poštu na spisak od milion adresa i očekuju da će samo mali broj čitalaca reagovati na njihovu ponudu. Spamovi su postali jedan od glavnih problema za sve korisnike interneta. Termin *spam* potiče iz čuvenog skeča Monti Pajtonovaca („Pa ješćemo Spam, paradajz sa Spamom, jaja sa Spamom, jaja sa slaninom i Spamom) koji se prikazivao u vreme kada se spam pojavio na internetu. Inače, *Spam* je robna marka preduzeća *Hormel* za mesni proizvod koji je bio popularan među vojnicima SAD-a tokom Drugog svetskog rata.

Kako da se zaštitite od SPAM-a?

ŠIFRUJTE VAŠU ADRESU E-POŠTE

Umesto da objavite adresu e-pošte u standardnom formatu, možete je šifrovati i na taj način sakriti. Da bi se šifrovana adresa e-pošte vratila u funkcionalan format, potrebno je da to uradi pažljiv i inteligentan um. Šifrovana adresa e-pošte može da izgleda ovako: vašeime et nazivdomena tačka com, dok bi ista ovakva nešifrovana adresa izgledala ovako: vašeime@nazivdomena.com

SAKRIJTE VAŠU ADRESU E-POŠTE U SLICI

ŠIFRIRAJTE VAŠU ADRESU E-POŠTE

Ukoliko morate da objavite aktivan link za Vašu adresu e-pošte, npr. da biste ostalima omogućili da Vas kontaktiraju na brz i jednostavan način, možete je šifrirati tako da ne bude čitljiva spambotovima koji prikupljaju adrese sa veb-sajtova. Navedena veb usluga Vam može pomoći u tome: ***http://hivelogic.com/enkoder/***

SAKRIJTE SVOJU ADRESU E-POŠTE POMOĆU TESTA

Uz pomoć alatke koja se zove scr.im, možete zaštititi svoju adresu e-pošte pomoću jednostavnog testa. Na početnoj strani scr.im unesite svoju adresu e-pošte, a ova stranica će Vam dati veoma kratki skriveni URL, zajedno sa prilagođenim HTML linkovima tako da svoju adresu e-pošte možete deliti na Twitter-u, Facebook-u, u okviru HTML dokumenata i na forumima.

NEMOJTE DELITI VAŠU ADRESU E-POŠTE

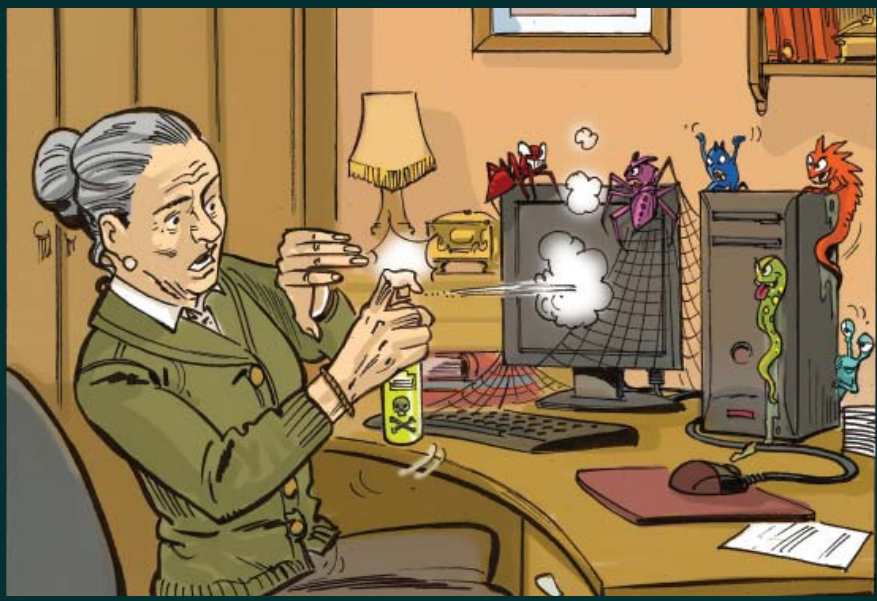
Poslednje čemu možete pribeći je da uopšte ne delite svoju adresu e-pošte. Napravite privremene prijemne sandučiće (engl. Inbox) ili obrazce preko kojih Vas mogu indirektno kontaktirati. Na primer, ***www.whspr.me*** *Vam omogućava kreiranje privremenih obrazaca preko kojih će se poruke prebacivati na Vašu adresu e-pošte. Korisnici moraju da dokažu da su ljudska bića tako što će proći CAPTCHA test.*

1.4 Šta je to *malware* ili zlonamerni softver?

Malware ili zlonamerni kod predstavlja pretnju po računare i njihovu bezbednost koju ugrožavaju računarski špijuni (engl. *spyware*), virusi, računarski crvi, trojanci i botovi. To su veoma rasprostranjeni programi koji mogu da evidentiraju sve što ukucate na računaru, da naprave snimke ekrana, ukradu dokumenta i datoteke i otvore skrivena zadnja vrata do vašeg računara. Ove informacije se zatim šalju osobi koja je instalirala neki od navedenih programa.

Malware može da instalira svako ko ima pristup računaru ili može biti skriven u „bezopasnom" prilogu poslatom putem e-pošte ili otpremljen putem sumnjivog veb-sajta.

Na primer, ukoliko koristite internet bankarstvo, *malware* može da evidentira lozinku Vašeg bankovnog računa. Ta informacija može da bude zloupotrebljena tako što će novac nestati sa Vašeg računa.



Opšta klasifikacija zlonamernih softvera

VIRUSI

Virusi su mali računarski programi koji mogu da se sami kopiraju i šire na ostale računare. Neki od njih su relativno dobroćudni, jednostavno Vam prikazuju poruku, ali ima i onih koji su izrazito zlonamerni i dovode do toga da programi ne funkcionišu kako treba, da se datoteke uništavaju, a *hard* diskovi ponovo formatiraju. Virusi se uglavnom klasifikuju prema dole navedenim kategorijama.

1. Makro virusi: inficiraju samo specifične programe za koje su i napisani.
2. Virusi koji inficiraju datoteke: inficiraju izvršne datoteke kao to su .exe i .dll datoteke.
3. Skripte: napisani jezikom za pisanje skripti kao što su Perl ili VBScript.

RAČUNARSKI CRVI

Nasuprot inficiranju relativno malog broja datoteka, crvi velikom brzinom inficiraju ceo računar. Na primer, *Slammer worm* koji je bio usmeren na poznatu ranjivost unutar baze podataka Microsoft's SQL Servera zarazio je preko 95% računara koji su bili povezani na internet u roku od deset minuta od trenutka kad je poslat, onemogućivši rad fiskalnih kasi u supermarketima i Banci Amerike.

TROJANCI

Trojanci su zlonamerni softveri koji su maskirani tako da izgledaju kao nešto što korisnik možda želi da instalira, a zatim obavljaju nepredviđene radnje - najčešće omogućavaju pristup računarskim botovima preko zadnjih vrata računara. Bot (skraćeno od robot) je zlonamerni program koji se prikriveno instalira na računare povezane na internet. Ovakve računare mogu kontrolisati treće strane, a da vlasnici računara toga nisu ni svesni.

RAČUNARSKI ŠPIJUNI

Računarski špijuni su vrsta zlonamernog softvera koji se instalira na računaru, bez znanja vlasnika da bi prikupio njegove privatne podatke. Računarski špijun je obično sakriven od vlasnika da bi prikupio podatke o internet interakcijama, pritiscima na taster (poznato kao i *keylogging*), lozinkama i drugim vrednim podacima.

Kako da se zaštitite od zlonamernih softvera?

Ne možete uvek da znate da li imate neki zlonamerni softver u svom računaru, tako da je važno da imate najnoviju verziju softvera koji detektuje viruse instaliranu u vašem računaru. Proverite da li Vas taj softver štiti i od računarskog špijuna. Možete da uradite i sledeće:

Budite svesni toga da kada god koristite računar na javnom mestu poput internet kafea ili biblioteke, on može da sadrži zlonamerni softver napravljen u svrhu prikupljanja Vaših podataka.

Ažurirajte svoj operativni sistem.

Budite pažljivi sa programima za razmenu datoteka – ukoliko nisu pravilno konfigurisani, ostali mogu imati pristup svim Vašim datotekama.

Povećajte nivo zaštite na Vašem pretraživaču tako da ne prihvatate cookies sa neproverenih veb-sajtova.

Nikad nemojte da kliknete na link u vašoj e-pošti jer Vas možda neće odvesti na dati veb-sajt.

Budite pažljivi kada otvarate priloge, jer oni mogu da zaraze Vaš računar.

Budite pažljivi kada preuzimate programe sa interneta, koristite proverene izvore i preuzete materijale skenirajte na viruse.

Budite oprezni sa veb-sajtovima koje koriste iskačuće forme (engl. pop-ups) ili deluju sumnjivo, jer mogu biti opasni.

Koristite jedinstvenu lozinku za internet bankarstvo koja se razlikuje od svih drugih lozinki.

Koristite softver za detekciju zlonamernih softvera.

Podesite svoj veb pretraživač tako da ne čuva vaše lozinke (i izbrišite one koje su već sačuvane).

1.5 Šta je to zaštitni zid (engl. *Firewall*)?

Zaštitni zid je bezbednosni hardver ili softver koji u sklopu računarske mreže kontroliše odlazni i dolazni mrežni saobraćaj na osnovu niza pravila.

Kao barijera između sigurnih i nesigurnih mreža, zaštitni zid kontroliše pristup mrežnim resursima i pomaže pri eliminaciji hakerskih upada, virusa i računarskih crva koji pokušavaju da dođu do Vašeg računara preko interneta.

Najefikasniji i prvi korak koji možete preduzeti da biste zaštitili svoj računar je da uključite zaštitni zid.

Ukoliko imate više povezanih računara u svom domu ili imate manju kancelarijsku mrežu, važno je da zaštitite svaki računar. Potrebno je da imate hardverski zaštitni zid (kao što je ruter) da biste zaštitili mrežu, ali i softverski zaštitni zid na svakom računaru, da biste sprečili širenje virusa širom mreže ukoliko se neki od računara zaraze virusom.

1.6 Šta je to SCAM?

Termin *scam* koristi se za opisivanje bilo kojih prevara ili planova za izmamljivanje novca ili drugih dobara od osoba koje ne sumnjaju da je reč o prevari. *Scam* je šema za brzo ostvarivanje profita kada neka osoba, grupa ljudi ili organizacija vara druge osobe ili grupe tako što im pruža lažne podatke prilikom davanja ponude ili nuđenja dogovora.

Ciljna grupa ovih prevara su osobe svih profesija, godišta, obrazovanja i prihoda. Ne postoje grupe ljudi koje su podložnije da postanu žrtve ovih prevara, svako od nas u nekom trenutku može da postane laka meta.

Scam prevare su uspešne zato što podsećaju na realnu stvar i zbog toga Vas mogu uhvatiti nespremne. Takođe, zloupotrebljava se i Vaša želja da budete ljubazni, učtivi, velikodušni i saosećajni.

Prevaranti postaju sve sofisticiraniji u svojim pokušajima da dođu do Vašeg novca ili poverljivih detalja. Pošto svet zahvaljujući internetu postaje sve povezaniji, broj prevara na internetu, kao i njihovih vrsta se sve više povećava.

U poglavlju „Primeri sajber prevara i obmana“, opisani su najčešći primeri prevara, tako da ih lako možete prepoznati i ispravno reagovati.

1.7 Bezbedni veb-sajtovi – Šta je to oznaka poverenja *(E-Trustmark)*?

Oznaka poverenja u elektronskoj trgovini je elektronska oznaka, slika ili logo koji je postavljen na veb-sajtu nekog preduzeća i koji pokazuje da je to preduzeće prošlo bezbednosne testove koje sprovodi organizacija koja izdaje ovu oznaku i na taj način dokazala da je vredno poverenja.

Oznaka poverenja povećava poverenje među korisnicima i pokazuje im da je sa preduzećem na čijem veb-sajtu je izložena oznaka bezbedno poslovati.

Na primer, (http://www.ecommerce-europe.eu/trustmark) oznaka poverenja koju izdaje udruženje *Ecommerce Europe (Ecommerce Europe Trustmark)* stimuliše prekograničnu elektronsku trgovinu putem bolje zaštite potrošača i trgovaca tako što je uspostavljen niz pravila na evropskom nivou i što je uspostavljena jasna komunikacija o ovim pravilima.

2. Primeri sajber prevara i obmana

Prevare na internetu postoje koliko i sam internet. Svake godine sajber kriminalci pronalaze nove tehnike i taktike osmišljene da prevare potencijalne žrtve. Potrebno je napraviti razliku između internet prevara i ostalih pretnji na internetu kao što su virusi, trojanci, računarski špijuni, SMS blokatori, itd. Kod prevara, meta sajber kriminalaca nije nužno računar čiju bezbednost je potrebno zaobići, već ljudska bića koja, kao što znamo, imaju svoje slabosti. Zbog toga nijedan program ne može obezbediti stoprocentnu zaštititu, ali sami korisnici moraju zauzeti proaktivan stav u obezbeđivanju vlastite bezbednosti na internetu.

U ovom poglavlju navedeni su brojni primeri prevara iz celog sveta sa kojima su upoznate organizacije poput Europola, UK policije, policije Republike Srbije, FBI, državne institucije za zaštitu potrošača Republike Srbije i Novog Zelanda. Opisani su različiti primeri prevara i obmana i dati saveti šta treba da preduzmete da biste se zaštitili.

2.1 Prevare sa računarskim virusima

Prevare sa računarskim virusima se obično obavljaju iz udaljenih korisničkih centara. Neko Vas pozove i kaže da je predstavnik za tehničku podršku neke kompanije. Najčešće tvrde da su predstavnici tehničkih usluga Windows ili Linux kompanija, PC Windows ili Linux podrške, Virtual PC Doctor, itd.

Sagovornik Vam saopštava da je Vaš računar zaražen virusom. Posavetovaće Vas da se prijavite na svoj računar i da preuzmete neki softver. Tako ste omogućili daljinski pristup svom računaru.

Sagovornik Vam uslužno pokazuje mesto na kome se virus nalazi na vašem računaru. Zatim će Vam ponuditi šestomesečni ili godišnji ugovor za usluge održavanja računara. Na taj način bi Vas zaštitili od novih virusa.

Ukoliko pristanete, sagovornik će Vam zatražiti podatke o kreditnoj kartici ili će tražiti da uslugu platite elektronskim transferom novca. Ono što ne shvatate je da virus u Vašem računaru ne postoji. Datoteke koje su Vam date na uvid su uobičajeni deo Vašeg uređaja.

Štaviše, prevaranti su Vas možda naveli da preuzmete računarskog špijuna. To će im omogućiti pristup svim Vašim ličnim podacima kao što je spisak adresa e-pošte ili bankovnim podacima. Ugovor koji ste zaključili pruža Vam veoma mali ili nikakav nivo zaštite od virusa. Međutim, može se ispostaviti da ga je veoma teško raskinuti.

Kako da se zaštitite?

Ako Vas neko iz čista mira pozove i kaže da je Vaš računar zaražen virusom, samo spustite slušalicu.

Ukoliko ste preuzeli neki softver, nakon ovakve prevare, odmah se isključite sa interneta.

Pokrenite antivirus programe i programe za detekciju računarskih špijuna i promenite sve svoje lozinke pomoću drugog računara.

Ukoliko niste sigurni, odnesite svoj računar kod stručnjaka „na čišćenje".

Ukoliko ste potpisali ugovor za koji verujete da je deo prevare, odmah kontaktirajte svoju banku ili izdavača kreditne kartice. Možda ćete uspeti da dobijete povraćaj novca.

Ne dozvolite da Vas zaplaše osobe koje Vas pozivaju, pošto mogu biti izuzetno napadne. Ne pokušavajte da saznate nikakve detalje od njih. Samo spustite slušalicu.

2.2 Prevare pri online kupovini

LAŽNI VEB-SAJTOVI

Iznenađujuće je kako je lako napraviti veb-sajt koji deluje kao pravi. Da bi Vas privukli, prevaranti najčešće koriste nazive i adrese veb-sajtova pravih trgovaca. Da bi bili što verodostojniji, ponekad se reklamiraju na pravim *online*

katalozima i na stranicama društvenih mreža. Ponekad čak plaćaju da njihovi oglasi budu istaknuti na pretraživačima.

Lažne stranice preduzeća na društvenim mrežama kao što je *Facebook* mogu da uvuku ljude u prevaru.

TRAŽENJE DODATNOG NOVCA

Pojedini prevaranti reklamiraju lažne proizvode, a onda traže dodatni novac nakon što ste im već platili. Obično tvrde da im je potreban dodatni novac za poštarinu, poreze i osiguranje.

Pošto je prvobitna cena bila niska, možda ćete biti u iskušenju da pošaljete dodatni novac. Nemojte. Oni će stalno iznalaziti razloge da traže još novca. Štaviše, plaćate za robu koja uopšte ne postoji.

PREVARANTI NA PRAVIM AUKCIJSKIM SAJTOVIMA

Aukcijski sajtovi koji imaju dobru reputaciju imaju sisteme za uočavanje prevara. Tako da prevaranti često pokušavaju da Vas odvuku sa tog aukcijskog sajta da biste sklopili dogovor. Budite oprezni ako Vam neko ponudi privatnu prodaju. Bez obzira da li je reč o prodaji na osnovu njihovog oglasa ili je reč o oglasu koji ste Vi postavili.

LAŽNI *ONLINE* AUKCIJSKI SAJTOVI

Može se dogoditi da budete preusmereni na lažni sajt na koji treba da se prijavite pod izgovorom da je potrebno da ponovo uspostavite Vaš nalog ili da verifikujete detalje iz naloga. Možete da dobijete poruku od nekoga ko tvrdi da je prodavac na aukciji koju propuštate. Nakon nekoliko e-poruka, tražiće Vam lične podatke i detalje o finansijama koje prevaranti mogu da iskoriste za krađu identiteta.

SLANJE PREVELIKE SUME NOVCA

Ukoliko Vam osoba koja je pobedila na aukciji koju ste Vi objavili pošalje veću sumu novca pri plaćanju, neka Vam to bude signal da nešto nije u redu. Ovo je vrsta prevare koja se zove „plaćanje unapred“(engl. *Upfront Payment scam*). Prevaranti će tvrditi da su pogrešili. Tražiće od Vas da im vratite višak uplaćenog novca ili možda da taj višak preusmerite na nekog drugog. U svakom slučaju, otkrićete da njihove transakcije menjaju pravac i završićete u minusu.

LAŽNE KARTE

Prevaranti mogu da iskoriste velike sportske događaje ili muzičke nastupe za prevaru. Zato je bezbednije karte kupovati kod ovlašćenih prodavaca karata.

Kako da se zaštitite?

Pre nego što počnete da kupujete online, bilo bi dobro da uradite domaći zadatak. Ukucajte naziv preduzeća, a zatim reč scam. Ukoliko je veb-sajt lažan, možda ćete pronaći priče onih koji su bili žrtve te iste prevare.

Ne zaboravite da komentari o preduzeću ili proizvodu koji zvuče previše dobro da bi bili istiniti, možda i nisu istiniti. Ništa lakše za prevarante nego da sami sebi napišu sjajne kritike.

Sigurnije je da platite kreditnom karticom, nego da obavljate transfer novca preko banke. Ukoliko nešto krene po zlu, možda ćete biti u mogućnosti da dobijete povraćaj novca. Naročito se pazite sajtova na kojima Vam traže da novac prebacite preko servisa koji nude usluge brzog transfera novca, kao što je Western Union. Ukoliko vodite preduzeće, nikada nemojte plaćati putem Western Union-a, niti bilo kog sličnog servisa.

Proverite da li sajtovi za plaćanje izgledaju bezbedno. Potražite simbol katanca i proverite da li adresa sajta počinje sa 'https' ('s' je oznaka za bezbedno, engl. secure).

Uvek proverite kontakt podatke trgovca. Budite oprezni ako su jedini dostupni podaci adresa e-pošte ili broj mobilnog telefona. Ukoliko imaju broj fiksnog telefona, pozovite ga. Ako ne možete nikoga da ga dobijete ili je Vaš poziv preusmeren na neki udaljeni korisnički centar, možda je reč o prevari. Takođe, budite oprezni ukoliko je jedina dostupna adresa broj poštanskog pretinca (P.P.).

Uvek pročitajte odredbe i uslove koji dolaze uz svaku ponudu. Proverite da li ima skrivenih troškova i obaveza. Ne verujte onim ponuđačima koji Vam ne omogućavaju da pročitate odredbe i uslove.

Kada trgujete na aukcijskim sajtovima, uzmite u obzir ocene koje su date kupcima i prodavcima.

Odbijte ponude da obavite kupovinu tako što ćete napustiti aukcijski proces.

Banka navedena na fakturi treba da se nalazi u zemlji u kojoj se nalazi trgovac.

2.3 Bankovne i fišing prevare

Kako funkcionišu bankovne i fišing prevare?

FIŠING (ENGL. *PHISHING*)

Prevaranti koriste fišing prevare da bi došli do Vaših poverljivih podataka. Podaci kao što su detalji o bankovnim računima, lozinke sa društvenih mreža i sl. mogu da imaju veliku vrednost za prevarante. Oni im pružaju slobodan prolaz do Vaših finansija i identiteta.

Pokušaji fišing prevara obično se obavljaju putem e-pošte. Međutim, mogu se obavljati i preko telefona ili SMS porukama.

UVERLJIVI RAZLOZI

Od Vas će tražiti lične podatke, na primer broj računa, korisničko ime, lozinku, broj kreditne kartice i PIN. Dobićete veoma uverljiv izgovor zbog čega su ovi podaci potrebni:

- *unapređenje bezbednosnog sistema*
- *održavanje sistema*
- *verifikacija računa/naloga*
- *zaštita od prevare*
- *ponuda za refundaciju takse ili računa.*

Banke i kreditna udruženja ponekad zaista kontaktiraju svoje klijente ukoliko postoje neke sumnjive aktivnosti, ali oni nikada neće tražiti Vaš PIN broj ili lozinke.

LAŽNI OBRASCI U E-POŠTI I NA VEB-SAJTOVIMA

Od Vas će tražiti da popunite obrazac u poruci e-pošte ili će Vas usmeriti na obrazac na veb-sajtu. Obrazac može da izgleda veoma uverljivo. Može da sadrži logo ili format koji koristi Vaša banka ili preduzeće, da biste poverovali da zahtev dolazi od njih.

Naziv veb-sajta, takođe, može da bude sličan, ali ne i potpuno isti kao pravi veb-sajt preduzeća.

Vrste bankovnih prevara

LIČNO BANKARSTVO

Može se desiti da dobijete e-poštu od nekoga ko tvrdi da je iz Vaše banke. Poruka može da izgleda kao prava i da sadrži logo i obrazac Vaše banke. U poruci se traži da potvrdite detalje o svom računu. Verovatno ćete dobiti i link preko kog treba da pošaljete poruku ili koji će Vas preusmeriti na veb-sajt gde će se od Vas tražiti da ostavite lozinku i PIN broj.

Nemojte to da radite. Banke Vam nikad neće tražiti lozinku ili PIN broj preko telefona, lično ili putem e-pošte.

Prevaranti šalju fišing poruke na milione adresa e-pošte u nadi da će pogoditi stvarne korisnike neke banke. Stoga se nemojte iznenaditi ukoliko dobijete poruku od banke u kojoj čak i nemate otvoren račun.

SAJTOVI ZA PRENOS NOVCA

Može se desiti da dobijete e-poruku sa sajta za prenos novca kao što je *PayPal* u kojoj se od Vas zahteva da obnovite svoj nalog. U poruci može da bude navedeno da je to bezbednosna mera, jer je Vašem nalogu pristupljeno sa nekog drugog računara. Takođe, od Vas mogu tražiti da ponovo unesete detalje sa kreditne kartice na sajt.

CARD SKIMMING

Prevaranti mogu da kopiraju elektronske podatke sa magnetne trake Vaše kreditne ili debitne kartice na bankomatu ili prilikom plaćanja karticom u prodavnici. Kada dobiju Vaše podatke, mogu da „kloniraju“ Vašu karticu i pristupe Vašim računima.

Šta treba da znate?

KADA KORISTITE INTERNET BANKARSTVO:

Postarajte se da Vaš računar ima ažuriran antivirus softver i instaliran zaštitni zid. Razmislite i o instaliranju softvera protiv računarskih špijuna. Preuzmite najnovije bezbednosne popravke (engl. *patch*) za Vaše pretraživače i operativni sistem.

Pre nego što počnete da koristite *online* bankarstvo, proverite da li se na Vašem pretraživaču pojavljuje katanac. Kada je povezivanje bezbedno, na početku internet adrese Vaše banke treba da stoji „https“ umesto „http“

Pazite se od neželjenih e-poruka, tj. fišing poruka, u kojima Vam traže poverljive finansijske podatke. Ni Vaša banka, ni policija Vas nikada neće kontaktirati da bi Vam tražili PIN broj.

Vodite računa da Vaš pretraživač bude podešen na najveći nivo zaštite za obaveštenja i praćenje. Ove bezbednosne opcije se ne aktiviraju uvek po automatizmu kada instalirate računar.

Uvek pristupajte sajtu banke tako što ćete ukucati adresu u pretraživač. Nikad nemojte ići na veb-sajt preko linka koji ste dobili u poruci e-pošte, a onda unositi Vaše lične podatke.

KADA KUPUJETE PREKO INTERNETA:

- Prijavite se na *Verified by Visa* ili *MasterCard SecureCode* kada god imate tu opciju pri kupovini na internetu. Time ćete registrovati lozinku kod preduzeća koje Vam je izdalo karticu.
- Kupujte samo na bezbednim sajtovima. Pre nego što ostavite podatke sa kartice, proverite da li se simbol katanca pojavljuje u pretraživaču. Adresa trgovca će se iz „http“ promeniti u „https“ ukoliko je povezivanje bezbedno.
- Nikada ne ostavljajte svoj PIN broj na internetu.
- Skenirajte ili odštampajte svoju porudžbinu i čuvajte kopije odredbi i uslova, politike povraćaja robe, uslova isporuke, poštanske adrese (ne poštanskog pretinca) i broja fiksnog (ne mobilnog) telefona.

Kako da se zaštitite?

Nikada ne unosite svoje lične podatke na veb-sajt, ukoliko niste sigurni da nije lažan.

Pažljivo proverite adresu veb-sajta. Ukoliko podseća na URL stvarnog preduzeća, ali nije potpuno ista, budite pažljivi. Nikad nemojte posećivati veb-sajt Vaše banke tako što ćete kliknuti na link – sami unesite adresu veb-sajta.

Nemojte davati podatke o svom računu putem telefona, osim ako Vi niste pozvali i sigurni ste da broj koji ste pozvali nije lažan. Ukoliko Vas pozovu, tražite ime i broj, tako da ih možete kasnije pozvati, kada proverite da li se broj sa koga ste primili poziv poklapa sa brojem za koji već znate da nije lažan.

Ne odgovarajte, ne klikćite na linkove i ne otvarajte nikakve datoteke u spam porukama. Ne pozivajte brojeve iz spam e-poruka.

Nemojte koristiti softvere koji za Vas popunjavaju određene obrazce na svom računaru.

Nikad nemojte slati svoje poverljive podatke, račune ili lozinke u poruci e-pošte. E-pošta je veoma nebezbedan sistem.

Proveravajte svoje bankovne izvode i izvode kreditnih kartica da biste bili sigurni da niko drugi nema pristup Vašem računu. Zatražite od banke godišnji izveštaj o korišćenju kreditne kartice da biste bili sigurni da niko ne koristi Vaše ime za podizanje novca ili gomilanje dugova.

Nikad ne ispuštajte svoju karticu iz vida u prodavnici i odbijte da provučete karticu kroz više od jedne mašine. Ukoliko Vas brine nečije ponašanje u prodavnici pri proveri kartice, obratite se glavnom nadređenom u prodavnici ili kontaktirajte svoju banku.

Nemojte koristiti bankomate koji imaju sumnjive uređaje prikačene na otvor za karticu. Tako nešto odmah prijavite banci.

2.4 „Hakovanje" računara

RAČUNARSKI ŠPIJUN

Računarski špijun (engl. *spyware*) je vrsta zlonamernog softvera. Kada kliknete na link u neželjenoj poruci e-pošte ili preuzmete neke datoteke sa interneta, možete aktivirati računarskog špijuna na svom računaru, a da toga niste ni svesni.

Prevaranti koriste računarske špijune da prikupe informacije o tome kako koristite svoj računar. Na primer, „*keystroke-logger*" je vrsta računarskog špijuna koji evidentira sve što otkucate na tastaturi. Tako da, kada otvarate svoj nalog e-pošte ili koristite internet bankarstvo i ukucate lozinku, prevaranti će moći da vide šta ste ukucali.

Računarski špijuni mogu da budu skriveni u datotekama koje se nazivaju „trojanci". Oni su naizgled bezopasni, npr. elektronska razglednica, muzički

sadržaj ili e-poruka od „prijatelja“, ali zapravo sadrže skrivene programe. Kada prevaranti dobiju pristup Vašem računaru onda mogu da:

- prikupljaju Vaše lične podatke i koriste ih za krađu identiteta
- iskoriste Vaš računar da bi pronašli nove žrtve za prevaru

Na koji način Vaš računar može biti „hakovan”

BANERI I PREUZIMANJA

Prevaranti koriste banere, iskačuće prozore ili čak cele veb-sajtove da bi instalirali računarskog špijuna u Vaš računar. Koriste besplatna preuzimanja, isprobavanje proizvoda ili slične ponude koje privlače pažnju. Da biste dobili besplatni proizvod, morate kliknuti na link. Tako se na Vašem računaru instalira računarski špijun. Ponekad od Vas zahtevaju broj kreditne kartice ili detalje o bankovnom računu, čime prevarantima dajete vredne poverljive podatke.

***SPAM* ILI NEŽELJENA E-POŠTA**

Spam podrazumeva upotrebu elektronskih sistema za nasumično slanje ogromnog broja neželjenih poruka. Preduzeća sa dobrom reputacijom ne šalju neželjene poruke. Tako da, kada dobijete neželjenu e-poštu, možete sa velikom sigurnošću pretpostaviti da je reč o prevari.

Prevaranti koriste *spam* da bi Vas:

- namamili da im date novac ili lične podatke
- namamili da instalirate zlonamerni softver na svom računaru

Spam poruke mogu da imaju sve moguće naslove u zaglavlju e-pošte. Oni se koriste kao sredstvo za mnoge druge prevare i mogu Vas navesti da uradite sledeće:

- tražite nagradu za učešće na takmičenju
- donirate novac u dobrotvorne svrhe
- kupite robu na popustu
- napravite unosnu investiciju

Spam poruke se koriste da ulove vaše bankovne lozinke. *Spam* poruka može da izgleda kao da je šalje neko sa vaše kontakt liste ili liste prijatelja.

SPAM PORUKE NA DRUŠTVENIM MEDIJIMA

Razvoj društvenih medija neizbežno je doveo do pojave *spam* poruka. Uobičajeni *spam* trikovi na društvenim mrežama su oni koji Vas navode da „lajkujete"/delite sadržaj (tzv. *like-jacking*) ili promovišete zlonamerni softver neke treće strane. *Spam* poruke na društvenim medijima je teško uočiti jer one obično dolaze od nekog od Vaših prijatelja i mogu da budu personalizovane.

PREVARE RAČUNARSKIM VIRUSIMA

Ukoliko ste bili žrtva prevare računarskim virusima i preuzeli ste softver koji prevarantima daje pristup Vašem računaru, možda bi bilo dobro da proverite da li Vaš računar ima instaliranog i računarskog špijuna.

Kako da se zaštitite?

Ukoliko Vam poruka e-pošte izgleda neobično i sumnjivo, nemojte je otvarati – čak iako dolazi od prijatelja. Nikad nemojte odgovarati ili kliknuti na linkove, nemojte pokušavati ni da se odjavite. Nemojte pozivati brojeve telefona navedene u poruci. Ukoliko sumnjate, najbolje je da odmah izbrišete e-poruku.

Isto važi i za iskačuće prozore i banere u koje nemate poverenja. Nemojte kliknuti na njih, samo ih zatvorite.

Ukoliko na internetu ugledate reklamu koja Vam nudi nešto što ne možete da odbijete, prvo istražite podatke o preduzeću, umesto da kliknete na link. Tako ćete možda otkriti da je ponuda legitimna bez rizika da kliknete na zlonamerni link.

Nemojte da unosite svoje lične podatke, uključujući informacije o kreditnoj kartici i bankovnom računu ni na jednom veb-sajtu za koji niste sigurni da je pravi.

Pre nego što iskoristite neku besplatnu ponudu, proverite je sa ostalim internet korisnicima ili istražite preduzeće koje ponudu nudi.

Budite oprezni sa veb-sajtovima koji nude besplatne igrice, muziku ili video sadržaje. Datoteke koji oni nude mogu da budu trojanci (pogledajte odeljak o trojancima). Istražite da li ti veb-sajtovi imaju dobru reputaciju pre nego što bilo šta preuzmete ili kliknete na neki link.

Instalirajte internet bezbednosni softver, koji proverava prisustvo virusa i računarskih špijuna. Kreatori ovih bezbednosnih softvera redovno objavljuju ažurirane verzije da bi se borili protiv najnovijih rizika. Postarajte se da Vaš softver bude ažuriran.

2.5 Vrste prevara pri zapošljavanju

ADMINISTRATOR ZADUŽEN ZA PLAĆANJE

Ponuđeno Vam je da obavljate plaćanja za neku prekomorsku kompaniju. Dobijate proviziju za svako obavljeno plaćanje. Ono što ne znate je da se taj novac koristi za protivzakonite aktivnosti. I ne znajući, postali ste „mazga za prenos novca“ (engl. *money mule*) i možete biti krivično gonjeni.

ZAGARANTOVANO ZAPOSLENJE/PRIHOD

Zagarantovan Vam je određeni prihod ili zaposlenje. Da biste dobili obećano morate da kupite npr. neki poslovni plan, materijale ili softver. Možda će tražiti i da uplatite novac i da se upišete u neki veb direktorijum, da bi Vam posao bio „zagarantovan“. Jedino što je zagarantovano je da ćete izgubiti novac.

MREŽNI ILI *MULTI-LEVEL* MARKETING

Osobe koje prodaju robu putem šeme mrežnog marketinga dobijaju provizije od prodaje onih koje su angažovali, kao i od prodaje koju sami izvrše. Pojedine šeme

mrežnog marketinga (ili marketinga u više nivoa), kao što je prodaja *Tupperware* posuđa su legitimni poslovni modeli.

Međutim, neki oblici mrežnog marketinga su skrivene piramidalne šeme koje u ponudu uključuju i prodaju proizvoda. Proizvodi su lošeg kvaliteta, precenjeni i teško ih je prodati.

Neke druge pirmidalne šeme, koje se prikazuju kao mrežni marketing, od svojih članova traže da plate velike sume novca za materijale za obuku.

SEMINARI

Prevaranti koji se predstavljaju kao agencije za zapošljavanje održavaju seminare za zapošljavanje. Govore Vam o „izuzetnim prilikama" obično u prekomorskim zemljama. Tokom seminara, tražiće Vam da unapred uplatite izvesnu proviziju – možda za doterivanje Vaše radne biografije, za administrativne troškove ili za radnu vizu. Kada jednom uplatite novac, „agenta" više nećete videti.

VIZE I DOZVOLE ZA RAD

Potencijalni poslodavac iz neke od prekomorskih zemalja Vam nudi da sredi dokumentaciju za vizu. Međutim, morate mu poslati novac da bi to uradio. Vaša viza nikad neće stići, a „potencijalni poslodavac" nestaće bez traga.

Kako da se zaštitite?

Posao tražite preko dobro poznatih veb-sajtova za zapošljavanje ili proverenih agencija.

Budite oprezni kada vidite oglase koji promovišu mogućnosti za rad od kuće – većina njih su prevare.

Proverite preduzeće koje Vam nudi posao ili poslovnu priliku. Ne dozvolite da Vas zavedu sjajne preporuke i tvrdnje – možda su lažne. Ukucajte naziv preduzeća i reč scam u pretraživač. Možda ćete naići na izjave osoba koje su i same bile žrtve iste prevare.

Pre nego što se uključite u bilo kakvu šemu mrežnog marketinga, zapitajte se da li se iza nje krije piramidalna šema. Da li ste impresionirani proizvodima i uslugama? Da li ćete moći da ih prodajete?

Ignorišite neželjenu e-poštu. Najbolje je da je izbrišete i uopšte ne otvarate. Ukoliko je otvorite, nemojte da kliknete na linkove, čak ni na one koji kažu „odjavite se" – oni mogu da pokrenu računarskog špijuna ili viruse u Vašem računaru.

Pažljivo proverite poslovne poruke, naročito ukoliko dolaze iz prekomorskih zemalja. Raspitajte se o troškovima vize i procedurama kod nadležnog organa za vize. Nikad nemojte slati novac na prekomorske račune ukoliko ne poznajete i u potpunosti ne verujete toj osobi ili organizaciji.

Kontaktirajte svoju banku i proverite da li ste imali uplate na Vašem računu za koje sumnjate da potiču iz nelegalnih izvora.

2.6 Vrste investicionih prevara

***COLD CALL* INVESTICIONE PREVARE**

Ova vrsta prevare ponekad se naziva i *boiler room* prevara. To je obično vrlo vešto vođena operacija. Dobijate poziv od „brokera" koji zvuči kao pravi profesionalac i koji Vam nudi ponudu koju je teško odbiti. Često je ponuda vezana za neku od prekomorskih zemalja.

Vrlo je verovatno da će svoje tvrdnje obrazložiti pozivanjem na imena proverenih preduzeća i prikazivanjem dokumentacije i veb-sajtova koji izgledaju kao pravi. Ponekad će se predstaviti kao brokeri ili portfolio menadžeri koje su ovlastila proverena preduzeća.

Na osnovu unapred pripremljenog uverljivog scenarija, prevaranti mogu ponuditi sledeće:

- akcije
- hipotekarne investicije
- investicije u nekretnine
- investicione šeme
- trgovinu opcijama
- trgovinu stranom valutom

Prevaranti mogu biti veoma uverljivi. Ponudiće Vam visok i brz povrat investicije uz mali ili nikakav rizik.

Rizik je, naravno, da je insvesticija prevara, a da Vi svoj novac više nećete videti.

PREVARE SA „SIGURNIM DOJAVAMA“ O AKCIJAMA (ENGL. SHARE ‘HOT TIP’ SCAMS)

Ove prevare obično počinju porukom e-pošte koju dobijate od „insajdera u preduzeću“. Kaže Vam da će akcije određenog preduzeća naglo skočiti. Poruka će možda biti adresirana na nekog drugog, tako da izgleda da ste je greškom primili.

Proveravate tvrdnje. Zaista, akcije preduzeća rastu. To je zbog toga što je cena akcija „napumpana“ zbog reakcija investitora na poruku prevaranata.

Kupujete. Cena akcija naglo pada zbog masovne prodaje. Gubite veliku sumu novca. Sa druge strane, osobe koje su Vam poslale poruku ostvaruju ogroman profit zato što su akcije prodali u trenutku kad su dostigle najveću vrednost na tržištu.

Bilo koja berza može da postane meta „pumpanja“ akcija. Vrlo je lako nasesti na prevaru onih koji tvrde da imaju neku „insajdersku informaciju“. Međutim, malo je verovatno da prevaranti imaju bilo kakve veze sa preduzećem čije su akcije „napumpane“. Ne zaboravite, insajderska trgovina je protivzakonita.

INVESTICIONI SEMINARI I PREVARE SA NEKRETNINAMA

Prevaranti ponekad koriste seminare na kojima potencijalnim investitorima predstavljaju načine kako da zarade veliko bogatstvo. Tokom seminara na učesnike se vrši pritisak da iskoriste šansu i odmah reaguju da bi ih što brže privukli.

Naravno da postoje i legitimni seminari. Ključno je da pažljivo proverite šta se nudi. Ne dozvolite da Vas neko pritiska da donesete odluku pre nego što dobijete savet o ponudi od poverljivog i nezavisnog stručnjaka.

Pored toga što vrše pritisak na Vas da uložite novac u lažnu investiciju, prevaranti zarađuju i od kotizacija za seminar i skupih izveštaja i konsultantskih usluga koje imaju vrlo malu ili nikakvu vrednost.

Ovi seminari mogu da budu prepuni obmanjujućih izjava – o honorarima, provizijama za prodavce, garancijama za iznajmljivanje i popustima koje dobijate ukoliko odmah pristanete na ponudu. Proverite svaku tvrdnju.

SOFTVERI ZA PREDVIĐANJE

Kompjuterizovani sistemi za kockanje obećavaju predviđanje tačnih ishoda konjskih trka, sportskih utakmica, pa čak i berzanskih rezultata.

Iako postoje legitimni softverski paketi koji prate promenljive u investicijama, prevaranti preteruju u svojim tvrdnjama da ćete zaraditi novac klađenjem.

Prevaranti naplaćuju velike novčane iznose za ove programe i često vrše pritisak na svoje kupce da šalju dodatne sume novca. Kažu Vam da ste prvobitnom investicijom izgubili novac, ali ako pošaljete još samo malo, povratićete novac.

PIRAMIDALNE PREVARE

U piramidalnim prevarama se obećava novac ili neka nagrada ukoliko uključite nove članove u piramidalnu šemu. Prevaranti Vas mogu kontaktirati na seminarima, na kućnim sastancima, telefonom, pismom ili e-poštom.

Vi šaljete proviziju osobi koja Vas je angažovala. Zatim treba da ubedite još ljudi da Vama šalju novac.

Međutim, piramidalne šeme su isplative samo onima koji su na vrhu piramide. Matematički je nemoguće da piramida nastavi da funkcioniše čim ostanete bez potencijalnih članova.

Kako da se zaštitite?

Najsigurniji način da investirate je da to obavljate preko registrovanih finansijskih savetnika, a investicioni proizvodi moraju da sadrže registrovani prospekt.

Ukoliko odlučite da investirate, a onda promenite mišljenje, ne dozvolite da Vas zavedu ponudom da zamenite investiciju za neku drugu ili uverenjima da će Vaša investicija uskoro dobiti na vrednosti.

Uvek tražite savet od nezavisnog finansijskog stručnjaka pre nego što donesete bilo kakvu odluku o investiranju. Ne oslanjajte se na savet osobe koja pokušava da Vas nagovori da investirate.

Nemojte da dozvolite da na Vas vrše pritisak da odluku donesete na brzinu. Brokeri sa dobrom reputacijom daju svojim klijentima dovoljno vremena da razmisle i provere njihovu preporuku.

2.7 Prevare sa plaćanjem unapred

Zahtev za plaćanjem unapred je jedan od uobičajenih mamaca kod mnogih prevara. Ove prevare obično funkcionišu na dva načina:

- Dobijete ponudu da „oslobodite“ veliku sumu novca tako što ćete unapred platiti proviziju.
- Pod izgovorom da su preplatili proizvod ili uslugu koju ste im pružili, od Vas će tražiti povraćaj novca ili da višak prosledite nekom drugom.

Vrste prevara sa plaćanjem unapred

NIGERIJSKA PREVARA

Iako je uobičajen naziv za ovu vrstu prevara „nigerijska“, ona može da potiče iz bilo kog dela sveta. Prevara funkcioniše na sledeći način:

Dobili ste neočekivanu poruku, e-poštu ili pismo.

Pismo je navodno od nekoga ko je povezan sa visokim državnim zvaničnicima – kao što je princ, izvršni direktor ili državni službenik – najčešće iz zapadnoafričkih zemalja poput Nigerije.

Oni žele da iskoriste Vaš bankovni račun da bi izneli novčana sredstva iz svoje zemlje – obično je reč o ogromnoj svoti novca, desetinama miliona američkih dolara.

Za prebacivanje sredstava, zauzvrat Vam obećavaju veliku sumu novca.

Ukoliko odgovorite, tražiće Vam detalje o Vašem bankovnom računu. Takođe, tražiće da platite i neku „proviziju“ unapred tako da se prenos novca može obaviti.

Iznos provizije je u početku mali, čime se stvara lažni utisak sigurnosti. Međutim, prevaranti znaju da kada jednom investirate neki novac u prevaru, manje su šanse da ćete odustati. Tražiće sve veće i veće iznose za provizije koje je potrebno platiti da biste dobili obećanu „nagradu".

Novac odjednom postaje „zarobljen" iz nekih dramatičnih razloga kao što je građanski rat, državni udar ili egzotične prirodne katastrofe. Nasleđe postaje „zarobljeno" zbog restrikcija državne vlasti ili lokalnih poreza.

U suštini, prevaranti od Vas traže da im perete novac. Čak iako je to što tvrde istinito, pranje novca je protivzakonito.

PREVARE SA NASLEĐEM/FONDOVIMA ZA NEKRETNINE

Kontaktira Vas neko ko tvrdi da radi u preduzeću koje se bavi nekretninama i obaveštava Vas da preduzeće pokušava da pronađe korisnike testamenta. Navodno se ispostavlja da ste Vi „najbliži srodnik". Možda će se pozvati na neki događaj kao što je avionska nesreća da bi zvučali što uverljivije. Može se desiti da Vi proverite tvrdnje i otkrijete da na tom letu postoji preminula osoba koja ima isto prezime kao Vi. Tražiće Vam da im unapred uplatite proviziju za pravnu pomoć koju su Vam pružili da biste dobili nasledstvo. Naravno, nasledstvo ne postoji, kao što ne postoji ni davno izgubljeni bogati rođak, a preduzeće će nestati onog trenutka kada uplatite novac.

Kako da se zaštitite?

Nemojte da odgovarate na neželjenu e-poštu ili pismo. Nikad nemojte da kliknete na „odjavi se“ u spam poruci: time ćete prevarantima samo dati do znanja da ste pročitali spam. Smesta izbrišite poruku e-pošte, a pismo bacite.

Ako ste već platili „provizije“ prevarantima, jedini način da prevara prestane je da prestanete sa plaćanjem. Kada uložite izvesnu sumu novca, uvek ste u iskušenju da nastavite i vidite šta će se desiti – za svaki slučaj. Ali znajte da Vas na kraju ne očekuje nagrada. Nikada nećete dobiti obećani novac.

Ne zaboravite da je pranje novca protivzakonita aktivnost. Nikada ne pristajte da prebacujete novac za nekoga koga ne poznajete. Kontaktirajte svoju banku ukoliko Vam je na račun uplaćen novac za koji verujete da bi mogao poticati iz nelegalnih izvora.

2.8 Prevare sa mobilnim telefonima

Kao što svi prelazimo na mobilne telefone, tako prelaze i sajber kriminalci. Pametni telefoni pružaju nove mogućnosti sajber kriminalcima i prevarantima. Pametni telefoni su mini računari – sadrže podatke o računima, nalozima e-pošte, porukama... spisak je zaista dug.

Sajber kriminalci mogu da preprodaju vredne lične podatke. Takođe, te podatke mogu da iskoriste za krađu Vašeg identiteta ili za druge prevare.

Čak iako nemate pametni telefon, možete postati žrtva neke od prevara vezanih za mobilne telefone.

Izgubili ste telefon? Ukoliko nije zaštićen lozinkom, ko god da ga pronađe imaće pristup svim Vašim podacima. Bez imalo truda.

Prevare sa mobilnim telefonima funkcionišu na sledeće načine:

- preuzimanjem kontrole nad pametnim telefonom pomoću zlonamernih aplikacija;
- navođenjem da pozovete ili pošaljete poruku na brojeve sa dodatnom tarifom i tako napravite ogromne telefonske račune.

Vrste prevara sa mobilnim telefonima

ZLONAMERNE APLIKACIJE

Danas je moguće preuzeti aplikaciju za gotovo sve – od toga kako da najbrže dođete do nekog kafića, kako da izmerite puls, pa do toga kako da uredite kuću. Ali nisu sve aplikacije proizvedene na isti način. Sajber kriminalci koriste aplikacije koje sadrže

zlonamerni softver, tako da kada ih preuzmete, dobiju potpunu kontrolu nad Vašim telefonom. U većini slučajeva, Vi to nećete ni primetiti.

TAKMIČENJA I KVIZOVI

Bez obzira da li imate pametni telefon ili ne, možete da postanete žrtva ove prevare. Dobijete poruku u kojoj Vas pozivaju da učestvujete u takmičenju ili *trivia* igri. Pomislite: „Što da ne?"

Ono što Vam nisu rekli je da se svaka poruka koju pošaljete naplaćuje po dodatnoj tarifi. Čak je vrlo moguće da ćete platiti i za poruke koje ste primili.

Postoje prave igre i takmičenja. Ali nagrada je bezvredna u odnosu na cenu koju ćete možda platiti ukoliko pristanete da učestvujete.

Nekada i ne dobijete zahtev za učešće u igri ili takmičenju. Prevaranti jednostavno počnu da Vam uzimaju novac tako što zadužuju Vaš telefonski račun. Vrlo je verovatno da ćete to shvatiti tek kada dobijete račun za telefon ili ostanete bez kredita.

PREVARE SA PROPUŠTENIM POZIVIMA I SMS PORUKAMA

Dobijete poruku da imate propušten poziv. Uzvraćate poziv, a da prethodno niste proverili broj. Ispostavlja se da je u pitanju broj sa dodatnom tarifom. Poziv koji ste uzvratili može mnogo da Vas košta. Slična tehnika se primenjuje i sa SMS porukama.

Kako da se zaštitite?

Zaključajte telefon pomoću lozinke.

Razmislite o investiranju u softver za bezbednost i upravljanje mobilnim uređajima.

Držite se zvaničnih kanala za distribuciju kao što je iTunes, kada birate aplikacije. Proverite reputaciju izdavača svake aplikacije koju preuzimate. Takođe, proverite koje im sve dozvole dajete pre nego što preuzmete aplikaciju.

Proverite brojeve sa kojih imate propušten poziv ili SMS poruku. Proverite da li broj ima standardni format. Ukoliko Vam se broj čini neobičnim, nemojte da ogovarate.

Pre nego što pristanete na bilo koju ponudu iz poruke, proverite ceo spisak odredbi i uslova. Morate da znate koliki su troškovi ukoliko treba nešto da platite. Tu treba da budu uključeni troškovi i za otkazivanje pretplate.

Proverite da li se radi o prevari tako što ćete pozvati svoju telefonsku kompaniju. Pitajte ih koliko će Vas koštati da pozovete taj broj.

Nikad nemojte prihvatati neku ponudu navedenu u poruci, niti poziv za učešće u takmičenju, ukoliko Vam nije ponuđena opcija kako da odustanete kada god poželite.

Nikad nemojte slati svoje lične podatke i podatke o finansijama porukom. Vaša banka, niti bilo koja druga uvažena institucija sa kojom komunicirate, nikad od Vas neće tražiti informacije na takav način.

2.9 Prevare usmerene na mala preduzeća

Kada imate svoju firmu, vrlo lako možete postati meta za sve vrste prevara – od plaćanja za oglase koje niste postavili pa do zahteva da prosledite uplatu nepostojećem dobavljaču.

Onda kada Vam je svaki dinar bitan, ne možete dozvoliti da bilo šta dajete prevarantima. Ovo su neke od uobičajenih prevara usmerenih na mala preduzeća kojih se treba paziti.

LAŽNE FAKTURE

Ove vrste prevara su obično povezane sa lažnim reklamama ili obnavljanjem dozvole za upotrebu naziva domena. Prevare funkcionišu na sledeća dva načina:

- dobijete lažnu fakturu za nešto što ste zaista naručili.
- Ispostavljen Vam je račun za proizvod ili uslugu koju niste naručili, ali Vam je rečeno da jeste.

Vrlo lako se može desiti da platite račun bez pogovora, naročito ako se radi o nečemu što redovno poručujete.

Kada je reč o reklamama ili nazivu domena, prevaranti Vas mogu pozvati da potvrde detalje – iako Vaša kompanija ili organizacija nikada nije poručila tu reklamu ili domen.

Prevaranti će čak pokušati i da zbune Vas ili Vaše osoblje, tako što će se pozivati na pravu reklamu ili oglas koji ste objavili na stvarnom veb-sajtu.

LAŽNI KATALOZI I PUBLIKACIJE

Pojedini prevaranti idu tako daleko da štampaju časopise manjeg tiraža ili prave lažne *online* kataloge da bi lakše prodali svoje marketinške usluge „klijentima".

Preduzeća poveruju da su postavila pravi oglas, a zapravo su pomenutu publikaciju videle samo druge žrtve.

Možda će Vam neko ponuditi besplatno oglašavanje. Pomislite kako je to sjajno. Ono što nije tako sjajno je tekst ispisan sitnim slovima gde se navodi da postoje troškovi za obradu i objavu Vašeg oglasa. Prihvatanjem ponude, prihvatili ste i taj trošak.

Ukoliko odbijete da platite, prevaranti će pokušati da Vas zaplaše tužbom. Najčešće su te pretnje samo prazna priča. Međutim, brojna preduzeća plate dugovanje pre nego što shvate da bi prevaranti odustali da su im se suprotstavili.

IZMENJENI PODACI O BANKOVNOM RAČUNU

Pozove Vas neko za koga mislite da je jedan od Vaših dobavljača. Obaveštavaju Vas da su promenili neke podatke u svom bankovnom računu.

Vi unosite datu ispravku u svoj računovodstveni sistem. Pre nego što shvatite šta se dešava, novac koji dugujete svom dobavljaču prema pravim fakturama uplaćujete na bankovni račun prevaranata. Shvatićete šta se dešava tek kada Vas dobavljač pozove i obavesti da kasnite sa plaćanjem.

LAŽNI KLIJENTI/UPITI

Pojedini prevaranti se predstavljaju kao klijenti koji su zainteresovani za Vaše usluge.

Na primer, ukoliko ste fotograf, neko Vas pita da li biste mogli da fotografišete venčanje njegovog sina.

Prevarant će poslati nekoliko upita, uglavnom preko e-pošte. Postavljaće pitanja o raznim detaljima. Kada Vam stigne druga ili treća poruka, već ćete biti uvereni da je veoma zainteresovan za Vaše usluge. Stoga ćete dati sve od sebe da udovoljite potencijalnom klijentu.

U jednom trenutku prevarant će izvršiti plaćanje – uplatiće ceo iznos ili depozit. Kada proverite izvod, videćete da je uplaćen veći iznos.

Zatim stiže detaljno obrazložen zahtev da deo uplaćenog novca prosledite trećoj strani – turističkom agentu, preduzeću koje iznajmljuje automobile i slično. Vi ispunjavate zahtev, a nakon toga otkrivate da je njihova prvobitna uplata povučena.

Ostali ste bez novca i gubili vreme zbog klijenta koji nikad nije ni postojao. Da stvar bude još gora, iskoristili su Vas za pranje novca, što je protivzakonito.

OPTIMIZACIJA VEB-SAJTA PREMA ZAHTEVIMA PRETRAŽIVAČA (SEO)

U eri interneta, prevaranti su našli mesto i u SEO aktivnostima.

Mogu da Vam obećaju da će dešifrovati komplikovane algoritme, da će napraviti linkove ili da imaju „svog čoveka“ u kompaniji Google.

Ukoliko niste dovoljno upoznati sa tehnologijom i svim žargonima koji su u upotrebi, vrlo lako možete postati žrtva.

Obratite pažnju na neželjenu e-poštu, kao i na druge iznenadne pokušaje ponude u kojima Vam nude mogućnost za unapređenje pozicioniranja veb-sajta vašeg preduzeća.

U najvećem broju slučajeva, to što Vam obećavaju je nemoguće izvesti ili ćete platiti velike svote novca za jednostavne stvari koje ste mogli i sami da uradite.

Kako da zaštitite sebe i svoje preduzeće?

Ograničite broj ljudi u preduzeću koji imaju dozvolu da kupuju i poručuju robu i usluge.

Skenirajte originalne račune i dokumente i arhivirajte ih na sigurnom mestu.

Uporedite sve fakture sa porudžbenicama. Tražite dokaz o kupovini i proverite sa kolegama da biste bili sigurni da ste dobili ono za šta ste platili.

Ukoliko faktura sadrži referencu za oglas ili za ulistavanje u katalog koje ste zaista poručili, proverite da li se svi detalji slažu sa Vašom porudžbinom. Prevaranti mogu da iskoriste stvarni oglas kao osnovu za pripremu lažnih faktura, na primer, naziv preduzeća, adresu, podatke o banci i slično.

Poslujte samo sa ljudima i preduzećima koja poznajete i kojima verujete.

Ukoliko pristanete da kupujete od novog dobavljača, postarajte se da precizno saznate šta nudi, po kojoj ceni, kakav je kvalitet i koje su odredbe i uslovi poslovanja.

Ne prihvatajte poslovne ponude koje dobijate preko telefona. Zatražite da Vam pošalju pisanu ponudu pre nego što prihvatite.
Potražite savet kada obavljate značajnu

kupovinu. Nemojte se oslanjati samo na to što Vam je prodavac rekao o konkurentskim proizvodima i uslugama.

Pažljivo pročitajte ono što je ispisano sitnim slovima u svakoj ponudi koju dobijete. Ukoliko ste dobili ponudu faksom, a tekst nije čitak, zatražite bolju kopiju... ali zahtev pošaljite samo ako nije reč o broju sa dodatnom tarifom.

Proverite da li je broj telefona koji pozivate ili broj faksa na koji šaljete dokument broj sa dodatnom tarifom. Ukoliko niste sigurni, pozovite svog telefonskog operatera.

Budite oprezni ukoliko dobijete pismo, e-poštu ili telefonski poziv od „dobavljača" koji od Vas traži da ažurirate njegove podatke o bankovnom računu. Možda je u pitanju prevara. Pozovite svog dobavljača i proverite s njim. Ukoliko nemate broj telefona, potražite broj u nekom od poverljivih izvora kao što su Žute strane ili Bele strane.

Ukoliko planirate da optimizujte svoj veb-sajt, potražite savet od prijatelja koji se razume u veb-sajtove, od saradnika ili od proverenih stručnjaka.

2.10 Vrste prevara na društvenim medijima

ZLONAMERNI LINKOVI

Društveni mediji nude izvrsne mogućnosti za razmenu smešnih snimaka, omiljenih pesama i drugih trivijalnih sadržaja. Ipak, morate biti oprezni. Ono što izgleda kao bezazlena zabava, na kraju može da izazove brojne probleme.

Prevaranti koriste upadljive naslove da Vam privuku pažnju i navedu da kliknete i delite link ili aplikaciju. Aplikacije kao što su „Šta tvoji prijatelji misle o tebi" ili „Ko posećuje tvoju *Facebook* stranicu" su tipični primeri.

Pre nego što preuzmete aplikaciju, zatražiće Vam podatke o nalogu. Vi popunjavate i... bingo! Preveranti mogu suvereno da upravljaju Vašim nalogom.

Neki drugi linkovi mogu da pokrenu računarske špijune na Vašem računaru. Računarski špijuni omogućavaju prevarantima pristup do Vaših ličnih podataka, kao što su lozinke za razne naloge i adresari. Kada prikupe podatke iz Vašeg računara, onda meta za slanje zlonamernih linkova postaju Vaši prijatelji.

FIŠING E-POŠTA

Slanje fišing e-pošte je još jedan metod za krađu identiteta na društvenim medijima. Dobijete e-poštu koja izgleda kao da je poslata sa veb-sajta nekog društvenog medija. U poruci Vam traže podatke o nalogu, koji su navodno potrebni da bi se „unapredila bezbednost". U pojedinim porukama Vam mogu tražiti i podatke o kreditnoj kartici. Bićete preusmereni na lažnu stranicu za prijavu koja može da izgleda veoma uverljivo.

Veb-sajtovi društvenih medija Vam nikada neće tražiti finansijske podatke da bi unapredili bezbednost, niti će Vam u poruci e-pošte slati priloge i linkove.

LAŽNO OGLAŠAVANJE

Kao što treba da budete oprezni kad je reč o reklamiranju na veb-sajtovima, isti oprez treba da postoji i sa oglasima na društvenim medijima. Ne sadrže svi oglasi na društvenim medijima istinite ponude. Štaviše, ukoliko kliknete na neki od njih, možete pokrenuti računarskog špijuna koji će prevarantima dati direktan pristup do Vašeg računara.

PLJAČKA

Pretražujete sadržaje na Facebook-u i jedan od prijatelja Vam iznenada šalje poruku. Saopštava Vam da se nalazi u nekoj drugoj državi, da je opljačkan i da je ostao bez pasoša i novčanika. Pita Vas da li biste mu poslali nešto novca preko servisa za transfer novca.

Naravno da želite da pomognete svom prijatelju, ali nemojte dozvoliti da Vas prevare. U najvećem broju slučajeva, reč je o prevarantu koji je ukrao podatke o nalogu Vašeg prijatelja i koji sistematično kontaktira svakog od prijatelja na spisku pokušavajući da izvuče novac.

LAŽNI POSLOVNI PROFILI

Svako može da otvori stranicu na društvenim medijima – uključujući i „preduzeća". Proverena preduzeća koriste društvene medije da bi se povezali sa svojim klijentima i obaveštavali ih o novinama u svom radu. Nikada ne bi koristili društvene medije da bi od Vas tražili novac.

PORUKA OD PRIJATELJA

Dobijete poruku od jednog od svojih prijatelja sa društvenih medija u kojoj Vam kaže da pogledate neki smešni video zapis ili link. Kada kliknete na link, dolazite do, kako se čini, prave stranice neke društvene mreže gde treba da se prijavite. Unošenjem podataka prevarantima dajete pristup ka svim Vašim prijateljima na društvenim medijima. Da i ne pominjemo mogućnost da ste preuzeli zlonamerni softver.

Kako da se zaštitite?

Dobro razmislite pre nego što preuzmete aplikaciju ili kliknete na linkove sa „smešnim" ili „privlačnim" sadržajem, čak iako je reč o nečemu što je Vaš prijatelj podelio. Ponekad je teško doneti tu odluku, jer društveni mediji su prepuni čudnog i novog. Ali ako Vam nešto deluje sumnjivo i neobično, bolje je da ne rizikujete.

Budite oprezni kada je reč o porukama u kojima Vam traže lozinku, podatke o nalogu i druge podatke – čak i kada stranica na koju je potrebno da se prijavite izgleda kao prava.

Ukoliko dobijete poruku od prijatelja u kojoj Vam traži novac, zamolite ga da Vas pozove – ili da Vam pošalje broj na koji možete da ga dobijete.

Podesite privatnost na svom nalogu tako da samo Vaši prijatelji mogu da vide Vaš sadržaj na društvenim mrežama. Postarajte se da to isto urade i Vaši prijatelji.

Dobro razmislite pre nego što prihvatite zahtev za prijateljstvo – koliko zaista poznajete tu osobu i štaviše, da li joj možete verovati?

Budite oprezni sa preduzećima i fizičkim licima koja koriste društvene medije kao mesto trgovine.

3. Prijavljivanje kriminalnih radnji na internetu

U današnjem digitalnom svetu postojanje e-kriminala je činjenica koja se ne može zanemariti. E-kriminal ima negativan uticaj na celokupnu privredu. Štaviše, e-kriminal ima negativne uticaje na konkurentnost preduzeća i spremnost potrošača da koriste digitalne aplikacije za kupovinu roba i usluga. Zbog toga je nužno da preduzeća, potrošači i država rade zajedno na suzbijanju e-kriminala, a jedan od načina je prijavljivanje sajber kriminalnih radnji nadležnim organima koji će preduzeti odgovarajuće korake da zaštite celu zajednicu.

Zakon o informacionoj bezbednosti omogućava osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima. Ovaj centar, koji je u fazi osnivanja, pružiće dragocenu podršku fizičkim licima, državnim organima, privatnom sektoru, agencijama i drugima koje je potrebno zaštititi od prevara i drugih zloupotreba kada su na internetu.

Strategija za razvoj informacionog društva u Republici Srbiji do 2020. godine definiše informacionu bezbednost kao jednu od šest prioritetnih oblasti razvoja. Štaviše, Narodna skupština Republike Srbije usvojila je *Zakon o informacionoj bezbednosti* koji ima za cilj povećanje nivoa zaštite i bezbednosti informacionih sistema. Ovim zakonom se definišu mere zaštite protiv bezbednosnih izazova i pretnji koje su, između ostalog, usmerene direktno na mala i srednja preduzeća i preduzetnike. *Zakon o informacionoj bezbednosti* definiše parametre i uloge u borbi protiv sajber kriminala, što je dovelo do predloga za osnivanje Nacionalnog centra za prevenciju bezbednosnih rizika (engl. CERT – Computer Emergency Resonse Team) koji će pružiti podršku kod IKT incidenata i raditi na podizanju svesti u javnosti o potrebi za zaštitom IKT sistema i mogućim rizicima.

Nažalost, nije moguće da svaka žrtva internet prevara bude obeštećena, bez obzira da li se radi o preduzeću ili potrošaču, ali prijavljivanje ovih krivičnih dela pomaže na više načina. Pre svega, omogućava nadležnim organima da drže korak sa sajber prevarama i služi kao mehanizam kojim se drugima šalje upozorenje od čega je potrebno da se zaštite. Često se ta upozorenja saopštavaju u vestima, što za rezultat ima veći broj prijava ovih krivičnih dela u celini.

Na osnovu *Zakona o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala* obrazovano je posebno odeljenje u Višem javnom tužilaštvu u Beogradu koje se bavi slučajevima sajber kriminala.

Ovo posebno tužilaštvo procesuira počinioce krivičnih dela čija su meta računari (tj. „svaki elektronski uređaj koji je zasnovan na automatskoj obradi i razmeni podataka“), računarski sistemi, računarske mreže, računarski programi i radovi zaštićeni autorskim pravom koji se mogu koristiti u elektronskom obliku.

U daljem tekstu navedene su dve institucije koje možete kontaktirati ukoliko želite da prijavite krivično delo visokotehnološkog kriminala, kao i podaci koje je potrebno dostaviti.

PRIJAVITE KRIVIČNO DELO VISOKOTEHNOLOŠKOG KRIMINALA NA SLEDEĆE ADRESE:

Možete prijaviti krivično delo visokotehnološkog kriminala lično policiji ili e-poštom na:

- vtk@beograd.vtk.jt.rs (Posebno tužilaštvo za visokotehnološki kriminal) ili
- ukp@mup.gov.rs (Policija – Služba za borbu protiv organizovanog kriminala)

DOSTAVITE SLEDEĆE INFORMACIJE:

1. Lični podaci:
   a. Ime i prezime
   b. JMBG (nije obavezno)
   c. Adresa
   d. Adresa e-pošte
   e. Broj mobilnog ili fiksnog telefona

2. Informacije o fizičkom licu/preduzeću koje Vam je nanelo štetu
   a. Pošaljite sve poznate i/ili raspoložive podatke.

3. Novčani gubitak
   a. Navedite ukupan iznos koji ste izgubili.
   b. Da li ste koristili usluge treće strane pri plaćanju kao što su *PayPal* ili *Escrow*?

4. Opis incidenta i dokazi
   a. Svojim rečima opišite na koji način ste postali žrtva.
   b. Podnesite sve dokaze koje imate.

5. Kontakt za svedoke i druge žrtve
   a. Ukoliko postoje svedoci i druge žrtve tog krivičnog dela, dostavite njihove kontakt podatke.

CIP - Каталогизација у публикацији - Народна библиотека Србије, Београд

343.85:[343.533::004(035)

БЕГОВИЋ, Синиша, 1974-
Kako se boriti protiv visokotehnološkog kriminala? / [autor Siniša Begović]. - Beograd : Projekat Razvoj elektronskog poslovanja, 2016 (Beograd : MaxNova Creative). - 46 str. : ilustr. ; 21 cm

Tiraž 500.

ISBN 978-86-80388-04-5

a) Високотехнолошки криминал - Сузбијање - Приручници
COBISS.SR-ID 222921996

e-business
DEVELOPMENT

www.eposlovanje.biz