

»Osamljena srca« so priljubljeno lovišče spletnih prevarantov

Zakaj ljudje nasedejo na spletne prevare? Katere družbene in psihološke vzorce izrabljajo prevarant? Zakaj pomislimo, da smo pametnejši od njih?

Lenart J. Kučič, Sobotna priloga

sobotnaPRILOGA

ned, 13.01.2013, 18:00

Spletne prevare vsako leto v povprečju zahtevajo po dve smrtni žrtvi. Ti posamezniki so odpotovali v Nigerijo ali na Nizozemsko po obljubljeni denar, ki ga sicer ni bilo. Tam so jih pričakali prevaranti, jih ugrabili in zahtevali odkupnino. Če žrtve niso imele več denarja, so postale pogrešljive.

Soproga pokojnega afriškega poslovneža želi dvigniti veliko možovo premoženje, ki je varno shranjeno na švicarski banki. Ker zaradi krutega političnega režima ne more iz države, potrebuje vašo pomoč. Le poslati boste morali osebne podatke za odprtje bančnega računa, plačati nekaj odvetniških pristojbin in podpisati kopico dokumentov. V zahvalo boste lahko obdržali tretjino vsega denarja – na milijone dolarjev.

Poznavalci spletnih prevar ocenjujejo, da je bilo lani poslanih na desetine milijard podobnih elektronskih sporočil. Veliko so jih prestregli spletni filtri za preprečevanje neželene pošte (spama), še več jih je končalo v elektronskih koših za smeti, nekateri pa so kljub oviram pritegnili pozornost prejemnikov.

Čeprav je takšna ponudba manj verjetna kot zadetek sedmice na loteriji, ji vsako leto nasede veliko žrtev. Britanski novinar Misha Glenny v knjigi o elektronski mafiji Dark Market ugotavlja, da je globalni trg elektronskih prestopkov vreden že več kot tisoč milijard dolarjev. Na nedavni svetovni konferenci o elektronskih komunikacijah v Dubaju so udeleženci razpravljali o različnih tehničnih in zakonskih rešitvah, s katerimi bi zamejili internetne prevarante, vse več zahtevajo tudi policija in tajne službe, ki svarijo pred razmahom organiziranega elektronskega kriminala in kiberterorizma.

Vendar zmogljivejši internetni filtri in strožji policisti niso edina rešitev, meni ekonomski psiholog in psihoterapevt David Modic, ki zadnjih dvanajst let raziskuje virtualne skupnosti, kiberkriminal in odklonskost, nedavno pa je na temo psihologije spletnih prevar doktoriral na britanski univerzi v Exetru. Bolj koristno bi bilo razumeti, zakaj uporabniki nasedajo na spletne prevare, katere družbene in psihološke vzorce izrabljajo prevaranti in kako ta spoznanja uporabiti za hitrejše zaznavanje vzorcev prevar in učinkovitejše izobraževanje uporabnikov.

Na slovenskih televizijah so lani predvajali [oglas](#), v katerem je bila postavljena lesena kulisa z napisom banka. Blagajnik poskuša prepričati stranko, da so čisto prava banka, in ji izvabiti osebne podatke, številko računa, kodo pin ... Sporočilo kampanje je bilo zelo jasno: če bi sredi polja zagledali takšno kuliso, ne bi nikoli verjeli, da je to prava banka. Če zagledamo spletno kuliso, pa nismo tako previdni. Zakaj?

Najbolj samoumeven odgovor bi bil: ker ne pomislimo, da gre morda za prevaro. Če bi vedeli, potem ne bi

nasedli. Takšna je ponavadi logika ozaveščevalnih kampanj. A ni tako preprosto. Velika večina spletnih potegavščin je zelo starih. Zne nigerijske prevare, v katerih vas nagovarjajo bogate vdove diktatorjev, politični zaporniki in drugi liki, imajo zametke vsaj že v šestnajstem stoletju, ko se je pojavilo prvo pismo španskega zapornika – izmišljene osebe, ki je žrtvi ponudila vabljev delež, če ji bo pomagala do denarja, plačala odkupnino in jo osvobodila. Prevaranti so najprej uporabljali pisma, nato telefone, fakse in danes internet. Tehnologija se je spremenila, psihološki mehanizmi pa ostajajo enaki, zato ljudje še naprej nasedajo internetnim različicam španskih pisem. Pri raziskovanju spletnih prevar so me najbolj zanimali prav ti mehanizmi.

Katere mehanizme in čustva nagovarjajo prevaranti? Pohlep?

Ne nujno. Marsikdo je lahko zelo pohlepen, a ne bo nasedel prevari.

Občutek pomembnosti? Da so ravno mene izbrali za tako nalogo, ponudbo ali poslovno priložnost?

To je že bliže. Prevare so oblika kriminala, pri kateri mora žrtev aktivno sodelovati, zato so prevaranti odlični poznavalci ljudi in njihovega obnašanja, ki vas znajo nagovoriti na pravi način – izrabiti vaše slabosti in oslabiti vašo možnost treznega razmišljanja. Veliko metod je enakih kot pri marketingu in prodaji. Dober trgovec vam bo mimogrede povedal, da tudi sam vozi enak avto, počitnikuje na istem hrvaškem otoku kot vi in doma z družino gleda prav takšno plazemsko televizijo, ki si jo ravno ogledujete. S takimi potezami pridobiva vaše zaupanje, saj nehote pomislite, da vam je podoben, in pozabite, da vam v resnici samo prodaja svoj izdelek. Hkrati začnete do njega čutiti tudi obveznost, saj se toliko ukvarja z vami, da bi ga bilo že neprimerno zavrniti. Spletni prevaranti znajo zelo dobro izrabiti ta mehanizem. Če se jim odzovete, se vam najprej približajo, nato vas začnejo prositi ali izsiljevati za najrazličnejše usluge in plačila, vi pa ne znate ali zmorete več izstopiti, ker želite pomagati sočloveku. Podobnih mehanizmov je veliko: vpliv skupine, podvrženost avtoriteti, želja po adrenalinu ...

Adrenalinu? Da sodelovanje v prevari vidimo kot razburljivo nevarno igro?

Znan je primer nekega ameriškega poslovneža, psihoterapevta in doktorja psihologije, ki so ga nigerijski prevaranti pošteno obrali, pa še v zaporu je pristal za dve leti. Natanko je vedel, da gre za prevaro, a je hotel dokazati, da je pametnejši od nasprotnikov. Do zadnjega je verjel, da on vodi igro, a se je precenil. To so zelo nevarne zmote, saj se prevaranti ne igrajo, ampak od tega živijo. Prav tako se na drugi strani elektronskega zaslona ne skrivajo le koristoljubni posamezniki, ampak organizirane kriminalne skupine, zato spletne prevare vsako leto v povprečju zahtevajo po dve smrtni žrtvi. Ti posamezniki so odpotovali v Nigerijo ali na Nizozemsko po obljubljeni denar, ki ga sicer ni bilo. Tam so jih pričakali prevaranti, jih ugrabili in zahtevali odkupnino. Če žrtve niso imele več denarja, so postale pogrešljive.

Včasih pa v prevare zavestno vstopajo tudi osamljeni posamezniki, je pokazala profesorica na univerzi v Leicesteru, Monica Whitty. Raziskovala je skupnosti »osamljenih src«, ki veljajo za priljubljeno lovišče spletnih prevarantov. Ti iščejo primerne posameznike in z njimi več mesecev ali celo let gradijo razmerje, preden jih prvič prosijo za denar. Whittyjeva je med drugim ugotovila, da nekatere žrtve zelo dobro vedo, da je njihov elektronski prijatelj sumljiv, da jim preveč piha na dušo in je nenaravno prijazen, a vzdržujejo komunikacijo, ker so preprosto osamljeni. Zato prevare vedno odražajo tudi širše družbene pojave – v tem primeru osamljenost in odtujenost kot spremljajoča pojava moderne družbe, ki so lahko dobra poslovna

priložnost za spletne kriminalce.

Omenili ste podvrženost avtoriteti. Ali nas zato v elektronskih pismih tako radi nagovarjajo profesorji, doktorji in podobni ugledneži?

Seveda. Socialni psihologi so v zadnjih petdesetih letih izvedli veliko poskusov, v katerih so pokazali, da posamezniki pod vplivom skupine počnemo tudi stvari, s katerimi se ne strinjamo, saj nočemo izstopati ali postati črne ovce. Enako predvidljivo se obnašamo pod vplivom avtoritete, kar je med drugim pokazal znani poskus ameriškega socialnega psihologa Stanleyja Milgrama, ki je čisto običajne državljane prepričal, da so v laboratoriju stresali »žrtve« z močnimi elektrošoki, tudi čez točko, ko bi lahko »žrtev« umrla, če bi jih v resnici streslo – ker so to pač zahtevali ljudje v belih haljah. Spletni prevaranti uporabljajo zelo podobne metode kot oglaševalci, kadar v reklamah za zobne paste ali shujševalne izdelke uporabijo resne sivobrade gospode z doktorskim nazivom. Če vas v elektronskem pismu nagovori bogati poslovnež, odvetnik, doktor ali profesor, se zdi ponudba bolj verodostojna.

Čeprav sociologi ugotavljajo, da avtoritetam ne zaupamo več?

Spletni prevaranti imajo pred raziskovalci veliko prednost. Za vsako znano človeško slabost lahko pošljejo na milijone elektronskih pisem in ugotovijo, kaj deluje – na kakšne ponudbe in nagovore se uporabniki najbolj odzivajo. Če lahko sklepam po besedilih spletnih prevar, ljudje očitno še vedno podlegamo formalnim avtoritetam, ki pa se razlikujejo glede na izobrazbo, starost in kulturo. Vendar odnosa do avtoritet nisem natančneje raziskoval. Upošteval sem ga le kot enega izmed dejavnikov, ki povečujejo dovzetnost za spletne prevare.

Vam je uspelo določiti kake splošne značilnosti žrtev? So pomembnejši demografski ali psihološki dejavniki?

Strokovna literatura ne daje dokončnega odgovora. Na splošno so za spletne prevare dovzetnejši manj izobraženi in starejši uporabniki spleta, več žrtev pa je med mlajšimi in bolj izobraženimi, ker na spletu preživijo veliko več časa in uporabljajo naprednejše elektronske storitve, nakupujejo, nakazujejo denar ... Ti rezultati me niso zadovoljili, zato sem pomislil, da so morda osebne lastnosti boljši pokazatelj dovzetnosti za spletne prevare. Pomagal sem si s kriminološkimi raziskavami, ki so poskušale določiti profil storilca, saj sem postavil hipotezo, da je podobno mogoče opredeliti tudi profil žrtve.

Verjetno ne z merjenjem lobanje in drugimi podobnimi pristopi, s katerimi so v 19. stoletju poskušali določiti fizionomijo kriminalca?

Nikakor ne! (smeh) Raziskovanje bioloških dejavnikov kriminalnega obnašanja se sicer počasi vrača – merjenje oblike lobanje je zamenjalo beleženje možganske dejavnosti v napravah za magnetno resonanco –, a sem se omejil na analizo osebnostnih lastnosti. Psihologi so sicer do ideje, da obstaja tipična osebnost protostorilca, zelo zadržani, ker poznamo preveč različnih vrst kriminala in razlogov, zakaj nekdo prekrši zakone. Ne bi bilo logično, da bi imel serijski morilec skoraj enake poudarjene osebnostne lastnosti kot tat koles. Vseeno obstajajo raziskave, ki nakazujejo, da je pri storilcih pogosto močneje izražena tako imenovana temna triada osebnostnih lastnosti: psihopatija, narcizem in makjavelizem. Če lahko storilec na določenem področju kriminalitete določimo poudarjene osebnostne lastnosti, jih morda lahko tudi žrtvam

prevar.

Ste jih določili?

Prva pomembna ugotovitev je bila, da se ljudje na internetu ne obnašajo bistveno drugače kot v fizičnem svetu. Na to sem postal pozoren že pri svoji magistrski raziskavi, saj sem pokazal, da lahko za elektronskimi identitetami sicer spremenimo obnašanje, vendar kljub anonimnosti, možnosti spreminjanja identitet in igranja vlog ostanemo enake osebe, čeprav se morda določene lastnosti močneje izrazijo. To je pomenilo, da sem lahko pri poznejših raziskavah spletnih prevar uporabil podobno metodologijo kot pred mano kriminologi, ki so raziskovali storilce v konkretnem svetu, in socialni psihologi, ki so proučevali potrošniško obnašanje. Ko sem za doktorat analiziral podatke, so največje statistične odklone pokazali dovzetnost za družbene vplive in avtoriteto ter samoobvladovanje. Osebnostni lastnosti, ki sta bili močno poudarjeni, sta bili ekstravertnost in odprtost za nova doživetja. Šibko samoobvladovanje pa velja po eni od kriminoloških teorij za najpomembnejši dejavnik, ki iz zglednih državljanov naredi prestopnike in žrtve.

Torej je za prevarante in njihove žrtve značilno, da se težje obvladujejo?

Tako so pokazali rezultati več eksperimentov, mojih in tujih.

Kakšna bi morala biti učinkovita preventiva pred spletnimi prevarami, če je največ odvisno od samoobvladovanja?

Če samoobvladovanje razumemo kot značajsko lastnost, torej neko vrednost, ki se skozi čas ne spreminja, potem ljudi, ki se težje samoobvladajo, tudi težje obvarujemo pred spletnimi prevarami. Vendar mi je bližji pogled, ki samoobvladovanje vidi kot stanje, ki se s časom spreminja. Takšno pojmovanje samoobvladovanja so drugi opisali, kot da je podobno mišici. Z redno vadbo jo razvijamo in izboljšujemo kondicijo, s prehudo obremenitvijo pa izčrpamo.

Kako torej »utrudimo« samoobvladovanje?

Primerov iz vsakdanjega življenja je veliko. Vzemimo, da ima vaš šef zelo slab dan. Ker veste, da se mu ne smete zameriti, nekako požirate njegovo slabo voljo, vendar ste po koncu službe čisto izčrpali svojo »samoobvladovalno mišico«. Takrat ste dovzetni za nepremišljene nakupe, škodljive razvade ali nepremišljene besede, ko pridete domov. Prav tako ste takrat precej manj pozorni na spletne prevare in boste spregledali tudi opozorilne znake, ki bi jih sicer opazili. Zato se je v takem stanju dobro izogibati spletnim in drugim nakupom, podpisovanju pogodb, pogovorom in drugim pomembnim opravkom. Ena izmed pogostih tehnik spletnih prevarantov je zasuvanje žrtev z goro formularjev, ki jih mora podpisati, med njimi pa se lahko znajde tudi pooblastilo za razpolaganje z vašim celotnim premoženjem. Znani so primeri, ko so prevaranti prodali hišo in so se žrtvi pred vrati pojavili novi lastniki z veljavno kupoprodajno pogodbo.

Ali spletni trgovci, izdajatelji kreditnih kartic, ponudniki spletnih storitev in državni spodbujevalci spletne ekonomije sploh hočejo potrošnika, ki se zna obvladovati?

Raziskovalci lahko proučimo in pokažemo psihološke mehanizme, ki vplivajo na dovzetnost za spletne prevare. Drugo vprašanje je, kdo in kako bo uporabil to znanje. Strinjam se, da od trgovcev in finančnih

ustanov težko pričakujem ukrepe, s katerimi bi zavirali potrošniško obnašanje, čeprav spletni trgovci velikokrat plačajo račun uspešne prevare in bi jim moralo biti v interesu, da to škodo zmanjšajo. Podjetjem, ki izdajajo kreditne kartice, bi lahko denimo pomagali sestaviti preprost spletni izpit, ki bi ga moral pred prvo uporabo opraviti vsak novi lastnik kreditne kartice. Poleg tega lahko s poznavanjem psiholoških mehanizmov spletnih prevar izboljšamo internetne elektronske filtre in ozaveščevalne kampanje, določimo najpomembnejše poudarke in opozorimo na najpogostejše trike. Problem običajno ni v kakovosti teh kampanj, temveč bolj v doseganju populacije, ki jo kampanje nagovarjajo. Hkrati ne smemo pozabiti, da nobena tovrstna kampanja ne more odpraviti družbenih okoliščin, ki jih izrabljajo prevaranti: osamljenosti, nezaupanja v institucije in nenehnega stresa.

Kaj pa lahko storimo uporabniki sami?

Predvsem ne smemo pomisliti, da smo prepametni in zato ne moremo postati žrtev spletne prevare. Z raziskovanjem spletnih skupnosti in kiberkriminalom se ukvarjam že več kot deset let, a še vedno nasledem na kako novo inovativno pogruntavščino. Nazadnje je le malo manjkalo, da se nisem opekel pri spletnem nakupu očal, ko sem hotel pametno prihraniti dobrih sto funtov, a sem skoraj ostal brez denarja. Prav tako bi se skoraj zapletel v sporen sistem spletnih akademskih recenzij, ki je bil namenjen pridobivanju osebnih podatkov recenzentov in verjetno poznejši kraji identitete. Mehanizem je običajno podoben. Racionalno sem vedel, da je nekaj predobro, da bi bilo resnično. Obnašal pa sem se čisto narobe (nasmešek).