



PREVARE U DIGITALNOM SVIJETU I KAKO IH IZBJEĆI (1.dio)

Čega sve treba da se čuvamo u digitalnom svijetu

Današnji digitalni svijet može biti i lijepo i opasno mjesto. Balans između ta dva pola digitalnog svijeta za svakog je individualan i uglavnom zavisi od toga koliko je „stanovnik“ digitalnog svijeta iskusan u tome da nađe lijepe ili naleti na opasne stvari.

Prevare su stare koliko i ljudska civilizacija. U manjoj ili većoj mjeri, uvijek su postojali ljudi koji su pokušavali da iskoriste nečije neznanje, neiskustvo ili nepažnju kako bi prisvojili nešto tuđe, oteli novac ili neku drugu vrijednost te se generalno okoristili na neki nelegalan, nemoralan ili nezakonit način. Prevara ima i danas, kako u analognom tako i u digitalnom svijetu, ali je broj pokušaja prevara u digitalnom svijetu danas mnogo veći nego u fizičkom (odnosno analognom) svijetu. Naravno, old-school prevaranata na ulici ima i danas – pokušat će vam prodati lažni Chanel 5, Rayban naočale, ukradenu robu ali djelovanje iz digitalnog svijeta mnogo je udobnije, pa se i prevaranti sele tamo. Prevara u analognom svijetu uglavnom uključuje neki vid fizičkog kontakta sa žrtvom, što pretpostavlja i vizuelnu identifikaciju, a to se kasnije može pokazati kao veliki rizik odluči li se žrtva na prijavu policiji. S druge strane, digitalni svijet garantuje mnogo veći stepen anonimnosti, a i prevaranti imaju mogućnosti da budu mnogo kreativniji i ubjedljiviji, te im fizička lokacija ne predstavlja više nikakav limit. Ukratko, zašto bi se neki prevarant ograničio samo na područje jednog naselja ili dijela grada, kad uz nešto truda može iz svog skrovišta da vara čitav svijet (ili bar njegov dobar dio)?

Prevare u digitalnom svijetu danas imaju i mnogo veći procent uspjehnosti nego one koje se dešavaju na „starinski“ način. Razloga tome ima više. Prvo, mogućnosti ima daleko više pa i kreativnost i ubjedljivost prevaranata može doći do izražaja. Drugo, još uvijek ima jako puno potencijalnih žrtava koje se ne snalaze dovoljno dobro u digitalnom svijetu, pa relativno lako nasjednu. Treće, prevaranti imaju mnogo više vremena na raspolaganju i prevare mogu da se pripremaju i izvršavaju u fazama, što je u fizičkom svijetu dosta teško izvodivo (uglavnom se preferira hit-and-run opcija). Na kraju, današnje tehnologije dozvoljavaju da se radi na više žrtava odjednom, što povećava mogućnost uspjeha.

Prevare u digitalnom svijetu ili prevare na Internetu, možemo dosta oštro podijeliti na dvije glavne kategorije:

- Prevare koje za cilj imaju jednokratnu ili višekratnu krađu novca

- Prevare koje za cilj imaju krađu identiteta, a putem toga dalje krađu novca, podataka, ličnih foto i video materijala itd.

Vrlo je važno znati raspoznati ove dvije vrste prevara i naravno, po mogućnosti, nikada ne nasjesti ni na jednu od njih. Treba odmah reći da su prevare koje ciljaju na krađu identiteta složenije i opasnije, sa dugoročnijim posljedicama koje ne moraju biti samo materijalne, pa ih se zato treba posebno dobro čuvati.

PREVARE U CILJU KRAĐE NOVCA

Najčešće, ovaj vid prevara oblikovan je na način da se žrtvu ubijedi (a nekada i prinudi) da kupi ili plati nešto što nije adekvatno onome što očekuje. Ovaj vid prevara se najčešće (mada ne isključivo) bazira na jednoj od dosta čestih ljudskih osobina – pohlepi, odnosno želi da se do nečeg vrijednog dođe za malo ili ništa novca odnosno truda. Moglo bi se reći da i napadača i žrtvu kod ove vrste digitalnih prevara pokreće gotovo isti motiv. I zato i idu u istom smjeru, te ova vrsta prevara još uvijek dosta često uspijeva.

Možda najšire poznat „uzorak“ ove vrste prevara je tzv. nigerijski princ, koji ima bezbroj svojih podvarijanti. Ukratko, sve se svode na manje-više isti obrazac – čovjek ili žena iz obično neke daleke zemlje, imaju ili su dobili veliki novac, nemaju nasljednike i žele taj novac da poklone u humanitarne svrhe. Žrtva se obično kontaktira putem e-maila, traži se pomoć da se novac, najčešće su to milioni USD, pokloni nekoj humanitarnoj organizaciji, a posrednik (žrtva) može 10% zadržati za sebe. Kako se obično radi o velikim iznosima u USD, i ovih 10% predstavlja puno, pa se jedan broj ljudi još uvijek na ovo upeca. Priča dalje ide tako da se obično od žrtve traži uplata nekog iznosa radi pokrivanja „administrativnih troškova“ slanja tog velikog iznosa. Nakon što žrtva uplati novac, prevarantu se obično gubi svaki trag. Slična prevara se često dešava i kod navodnih nagradnih igara koje „organizuju“ velike kompanije tipa Microsofta, Amazona, Facebooka itd. Žrtva se sa lažnog naloga (koji izgleda kao pravi) obavještava da je dobitnik nagrade od recimo 500.000 USD, a nakon što se komunikacija uspostavi, traži se uplata unaprijed za „porez na nagradu“, „troškove transfera novca“ i sl. U posljednje vrijeme ovakve prevare su lokalizirane i za naše „tržište“ pa se tako počesto sretnu mailovi obavještenja o „nagradama“ koje daju poznate BH kompanije. Ti mailovi obično sadrže link do lažne web stranice na kojoj žrtva onda upisuje lične podatke a najčešće i broj kartice za „uplatu nagrade“.

Vrlo su česti takođe i tipovi prevara koji se dešavaju kod online kupovine. U ovom kontekstu, prevara može da se desi i kada je žrtva kupac ili kada je prodavac. Kod slučaja kada je žrtva prevare kupac, scenario obično izgleda tako da se nudi neka atraktivna roba po neobično niskoj cijeni. Recimo, neko prodaje najnoviji iPhone za 500 KM, Prada cipele za par stotina EUR ili KM itd. Sajтови na kojima se ova „roba“ prodaje dosta često i liče na legitimne sajtove poznatih online prodavnica. Vrlo često imaju i slično ime, da bi se dodatno zavarali lakovjerni. Nakon takve kupovine žrtva najčešće ne dobije ništa ili u najboljem slučaju dobije neki lažni proizvod koji imitira ono što je trebalo da se dobije. Ove prevare i nije tako teško razotkriti prije nego se dese, ako

slijedite jedno prilično jednostavno pravilo – ako vam se ponudi nešto što izgleda suviše dobro da bi bilo stvarno, najčešće i nije stvarno i nemojte nasjedati. Ako niste sigurni u sajt gdje želite nešto kupiti, provjerite isti proizvod na pouzdanim sajtovima, tipa Amazona. Ako je razlika u cijeni značajna, nešto nije ok. Nije loše ni pogledati Trust Pilot, to je platforma koja je upravo namijenjena razmjeni iskustava sa online kupovinama. Tu veliki broj ljudi iznosi svoja iskustva online kupovine, što može pomoći, ali naravno ne treba svemu bezuslovno vjerovati.

Kupovine putem društvenih mreža su generalno dosta loša ideja iako dosta ljudi koristi ovaj način. Tu se roba obično prodaje na crno, prodavci nisu registrovani, vrlo lako mogu koristiti lažne profile, pa je i mogućnost da budete prevareni veća. Neki istina rade i sasvim pošteno, ali mnogo više je onih iz druge kategorije.

Ako treba nešto da platite putem žiro-računa, dobro provjerite da li je na računu ili ponudi koju ste dobili upisan pravi broj za uplatu. Prevaranti ponekad generišu lažne ponude ili račune, na ime poznatih kompanija, ali sa svojim brojem računa. Ovakve prevare su uglavnom usmjerene na firme, ali ni pojedinci nisu isključeni.

Kada je žrtva prevare prodavac, priča ima nešto drugačiji karakter. Prevarant se predstavlja kao kupac, te od žrtve obično traži broj kartice (sa svim ostalim podacima) da bi „uplatio novac“ za robu koju želi kupiti. Veliki broj ljudi i danas na ovo nasjeda, zato ću ponoviti ono o čemu se već pisalo u ovom serijalu – broj kartice se koristi isključivo za plaćanje, nikada za prijem novca. Ako vam neko traži broj kartice da bi vam nešto uplatio, znajte da se radi o pokušaju prevare. No i ova prevara ima svoje varijacije, pa se u zadnje vrijeme javljaju i slučajevi kada prodavca kontaktira navodna kurirska služba koja treba preuzeti robu, a prodavcu ostaviti (lažnu) potvrdu o uplati i slično.

Jedan poseban i možda i najperfidniji tip prevara koji se dešava u digitalnom svijetu su emotivne prevare koje imaju za cilj krađu novca. Za razliku od realnog života, gdje takve prevare nije baš lako izvesti (mada nije nemoguće), moderne komunikacijske tehnologije, kao i mogućnosti za lažiranje identiteta u digitalnom svijetu ih čine znatno uspješnijima. Ova vrsta prevare se najčešće realizuje putem društvenih mreža i to najčešće putem Facebooka ili neke od platformi za upoznavanje. Cilj su obično sredovječni ljudi, srednjeg ili boljeg imovnog stanja, najčešće oni koji su sami i/ili usamljeni i željni društva ili partnera. Žrtva se pažljivo bira, najčešće na osnovu podataka koje sama o sebi ostavlja na društvenim mrežama. Prevara se priprema i izvodi dosta dugo, ali je i ciljani iznos za krađu obično veći nego kod druge vrste prevara.

Scenario ide tako da se prevarant javlja žrtvi, nudi neobavezni kontakt i razgovor pod izgovorom da traži društvo odnosno prijatelja. Ako je žrtva muškarac, obično se javlja žena i obrnuto, mada ni istopolni kontakti nisu isključeni ako se utvrdi da je žrtva iz homoseksualne populacije. Nakon početnih kontakata i razgovora, počinje se graditi emotivna veza a time i povjerenje. Žrtva i prevarant nakon nekog vremena online kontaktiranja (chat) počinju pričati telefonom ili preko video poziva, planiraju prvi susret (što je obično komplikovano jer tobože ne žive u istoj zemlji, mada ima

slučajeva i kada je dolazilo do susreta), otvaraju se razne teme i to tako traje obično par sedmica, nekada i mjeseci. Nakon što prevarant procijeni da mu žrtva dovoljno vjeruje počinje druga faza. U toj fazi, prevarant i žrtva su već u emotivnoj vezi i počinje razgovor i o nekim teškim životnim temama. Prevarant obično počne govori o nekoj svojoj navodnoj bolesti, skupom liječenju ili lijekovima, bolesnom roditelju ili djetetu, hipoteci na kuću ili stan koji ne može da vraća i sl. Teme koje se biraju su obično vrlo osjetljive tako da je vjerovatnoća da žrtva reaguje na željeni način što veća. Dalje se priča obično razvija tako da žrtva, sada već zaljubljena u svog navodnog partnera, nudi pomoć. Prevarant se prvo nećka, navodno mu/joj je nezgodno, ne voli da pozajmljuje novac, ali na kraju zbog situacije u kojoj jeste, prihvata. Naravno, slijedi beskrajna zahvalnost, izjave ljubavi, opsjedanje žrtve koja samo dodatno propada u živi pijesak prevare. Ako se odmah u prvom pokušaju uspije izvući željeni novac, najčešće se nakon uplate svaki kontakt prekida, nalozi na mrežama se brišu, identitet je ionako bio lažan i prevarant nestaje. Žrtva ostaje devastirana i emotivno i finansijski. Ako se pak desi da žrtva ne da odmah dovoljno novca, priča se nastavlja, na različite načine dok se ne dođe do cilja. Ishod je obično isti samo je pitanje koliko traje. Ovu vrstu prevara je gotovo nemoguće dokazati, pa je i stoga posebno opasna. Naime, žrtva je svojevolumeno dala novac prevarantu, na osnovu povjerenja i emotivne veze. Čak i u rijetkim slučajevima kada se otkrije identitet prevaranta, krivicu je teško dokazati jer se ne može osporiti emotivna veza i želja da se pomogne koja je postojala (bar sa jedne strane). Zato je izrazito važno da se u ove situacije ne dođe. Naravno, postoje slučajevi da su se nepoznati ljudi i potpuno legitimno povezali putem društvenih mreža, izgradili vezu koja ponekad završi i brakom, ali na žalost, broj pokušaja prevare je daleko veći. Savjet je i ovdje dosta sličan kao i kod kupovine – dobro razmislite da li stvari izgledaju previše dobro da bi bile istinite. Konkretno, imate li recimo 50+ godina a kontaktira vas nepoznata osoba, najčešće suprotnog pola, od nekih 25-30 godina, atraktivnog izgleda, sa prijedlogom za druženje jer je usamljen(a), gotovo sigurno je riječ o pokušaju prevare. Da biste bili ipak sigurni, istražite malo – pogledajte kada su kreirani profili osobe koja vas kontaktira, da li ima drugih prijatelja, imate li zajedničkih prijatelja, tražite vizuelni kontakt i sl. Prevaranti obično uvijek kreiraju novi profil na društvenim mrežama za svaku novu žrtvu, pa i to može biti koristan signal. Toplo preporučujem, posebno ako ste u rizičnoj kategoriji za ovu vrstu prevara, da pogledate dokumentarni film *Tinder Swindler*. Baziran je na istinitim događajima i bavi se upravo ovom vrstom prevara u njenim ekstremnim slučajevima.

Na kraju, vrijedi još jednom pomenuti i prevare, koje se u zadnje vrijeme ponovo dosta često javljaju, a mogu se svrstati u kategoriju iznude. Radi se o mailovima u kojima se žrtva obavještava da je potajno snimana tokom posjete web sajtovima sa porno sadržajem, te se traži uplata određenog novca u kripto valuti, kako bi snimci bili obrisani. Nemojte nasjedati, čak i ako jeste posjećivali sajtove koji se navode u takvim mailovima. Ovi napadači šalju veliki broj ovakvih poruka, u nadi da će neke ljude dovoljno preplašiti te da će pristati na plaćanje naknade za brisanje snimaka.

Da sumiramo za kraj, nekoliko korisnih preporuka i savjeta za izbjegavanje prevara čiji je cilj krađa novca:

1. Niti jedna kompanija na svijetu ne dijeli nasumice novac putem email-a. Svi emailovi kojima se obavještavate o dobijenoj nagradi su lažni.
2. Niko ko se ozbiljno bavi nekim poslom ne traži unaprijed uplaćivanje novca za troškove nečega što treba biti vaš benefit. Ako naiđete na takav zahtjev, u pitanju je prevara.
3. Skupe i vrijedne stvari su skupe i u digitalnom svijetu. Sve što izgleda predobro (prejeftino) da bi bilo istinito, najčešće i nije istinito.
4. Nikada ne upisujte ili ne šaljite broj svoje kartice da biste dobili novac. Za to se koristi broj računa a ne broj kartice.
5. Ako treba nešto da platite putem žiro računa, provjerite da li koristite ispravan broj prije nego napravite uplatu. Najbolje kontaktirajte onoga kome uplaćujete.
6. Budite veoma oprezni u kontaktima sa nepoznatim osobama koje vam se jave putem društvenih mreža.

Ako se dovoljno dobro brinete o svom računar, vrlo je teško izvodivo da vas neko potajno sa njega snima. Ne nasjedajte na prevare niti pokušaje iznude tog tipa.

Tags

Digitalna kompetencija

Collections

Autorski tekstovi

AI u nastavi