

Ukoliko smatrate da ste žrtva prevare molimo Vas da nas kontaktirate putem email-a

contact@capitaltransfer.me

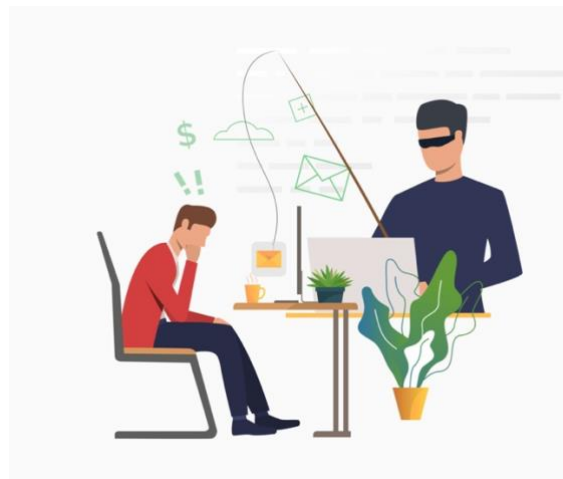
Ria Money transfer koristite samo da biste slali novac prijateljima i porodici. Nemojte da šalžete novac nekome koga ne poznajete lično.

Da izbjegnute da postanete žrtva bilo koje online prevare važno je da znate da, koliko god primamljivo zvučalo, nikad ne šalžete novac nepoznatim ljudima, za kupovinu preko interneta, za donaciju u dobrotvorne svrhe, za kupovinu auta... Čak i ako poznajete osobu koja vam se javlja, provjerite njen identitet drugim putem (pozovite je telefonom, nađite se s njom...), jer nije isključeno da je ona žrtva ukradenog identiteta, i da prevarant koristi identitet vašeg prijatelja kako bi izmamio novac od vas.

Ako obavite transfer novca, osoba kojoj ga šalžete će ga brzo dobiti. Nakon isplate novca, Ria Money Transfer neće biti u stanju da vam ga refundira, čak iako ste žrtva prevare, osim pod ograničenim okolnostima.

Šta je Internet/online prevara?

Internet ili online prevare su dio prevarantskih šema u kojima počinioci koriste razne online aplikacije ili platforme društvenih mreža za pronalaženje potencijalnih žrtava. Obično su to osobe koje se predstavljaju kao neko ko traži ljubavnu vezu, ili je u teškoj zdravstvenoj situaciji pa su njemu ili njoj potrebna sredstva/novac za oporavak, ili treba da naslijedi ogromno bogastvo pa im je novac potreban za advokata. Nerijetko se dešava da to budu i preprodavci motornih vozila.



Koji su najčešći oblici internet prevare i kako se zaštititi?

Nabrajaćemo par najčešćih oblika internet prevara koje targetiraju ljude na ovim prostorima, sa opisom toga kako ih prevaranti sprovode:



Prevaranti koji se lažno predstavljaju kao institucije (najčešće tako što prave lažne stranice banaka i trgovinskih lanaca na društvenim mrežama ili tako što šalju masovne e-mail ili SMS poruke) i raspisuju nagradnu igru u kojoj je lako učestvovati (recimo “unesite broj 76 u komentaru”). Nakon što ispuniti “kriterijum za učestvovanje”, privatnom porukom vas obavještavaju da ste dobili nagradu, i da im od vas treba “samo još nekoliko podataka”. Podaci su često broj bankovne kartice, datum isteka kartice, CVC broj, Vaše ime i prezime, matični broj, slika vaše lične karte ili računa za komunalije i slično. Ovi podaci su dovoljni da prevarant, uz manje ili više dodatnog truda, može da transferuje novac sa vašeg računa ili kupuje za sebe usluge, plaćajući ih vašom karticom.

Sa sve većim brojem ljudi koji znaju da ne smiju dijeliti osjetljive podatke, prevaranti su došli na ideju da naprave sajtove koji izgledaju identično kao oni gdje su ljudi već navikli da unose te podatke, i da sakupljaju sve što su korisnici unijeli u obrasce. Ako žrtva vidi sajt koji izgleda identično kao Facebook ili sajt njihove banke i nije mu jasno da se radi o lažnom sajtu, refleksno će unijeti svoje podatke. Ova metoda se u internet žargonu zove “fišing”. Google Chrome i ostali moderni browseri imaju relativno pouzdanu, ali ne stoprocentnu zaštitu od fišinga, i preporučljivo je da redovno apdejtujete svoj pretraživač. Dobar savjet je da nikada ne unosite svoje pristupne podatke na link koji vam je neko poslao, već da ukucate adresu sajta na koji želite da se logujete u address bar.

Online emotivna prevara ili ljubavna prevara počinje na nekoj od aplikacija za upoznavanja ili na nekoj platformi društvene mreže. Razmjenjuju se emailovi, razgovara se telefonom i razmjenjuju slike. Na kraju, naprave se planovi da se sretnu, čak i da se vjenčaju. Kako veza jača, stvari počinju da se mijenjaju. Obično jedna strana zatraži novac, potreban za autobusku kartu da posjeti bolesnog rođaka. Prva uplata novca je mala, ali često se zahtjevi nastavljaju i rastu –, potrebna im je avionska karta da dođu u posjetu i slično. Obećanja za povraćaj novca su prazna.

Prevare sa zaposlenjem obično počinju sa previše dobrom ponudom – rad od kuće i zarada od nekoliko hiljada dolara mjesečno, bez potrebnog iskustva – a koje završavaju sa klijentom koji je ostao bez „posla“ i bez novca. Obično prate jednu od tri šeme: Prevaranti se predstavljaju kao novi „poslodavci“ i šalju žrtvi ček za pokrivanje početnih troškova, kao što je potrošni materijal. Žrtve deponuju ček, kupe neophodan materijal i pošalju preostala sredstva nazad prevarantu. Nekoliko nedelja kasnije, saznaju da su čekovi lažni i da su dužni za cio iznos. Prevaranti se predstavljaju kao „specijalisti za zapošljavanje“ koji nude garantovano zaposlenje ili kao poslodavci koji proširuju poslovnu ponudu pod uslovom da žrtva plati unaprijed za kreditne čekove, za prijavu ili naknadu za zapošljavanje. Žrtve plaćaju, ali ponude za posao se nikada ne ostvare.

