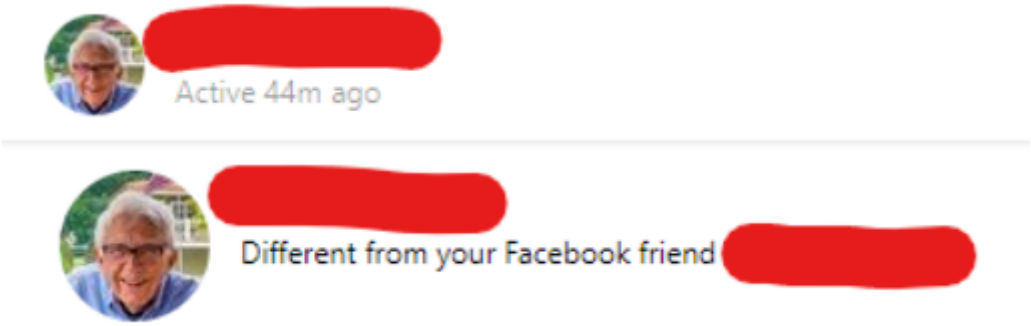
Kuidas end netipetturite eest kaitsta

6 aastat tagasi - 30.03.2020 Autor: Kristjan Karmo

Juba aastaid on erinevad küberturbe spetsialistid rääkinud, et rünnete puhul ei saa enam rääkida üksikjuhtumitest, vaid tegu on ühtlase fooniga. Järjest rohkem tundub sama kehtivat ka sotsiaalsete rünnete kohta. Ehk siis varem või hiljem on meil kõigil oht mõne küber-kurikaela ohvriks langeda. Praegusel keerulisel ajal, kus väga paljud meist on enneolematus olukorras ja ettevõtted, sh sotsiaalvõrgustikud, teevad oma töös paratamatuid ümberkorraldusi, on tõusmas ka nende hulk, kes kaosest kasu üritavad lõigata. Ma ei pea silmas mitte WC-paberi-spekulante, vaid eelkõige küberruumis varitsevaid petiseid. Mis, paraku, on terve tööstusharu.

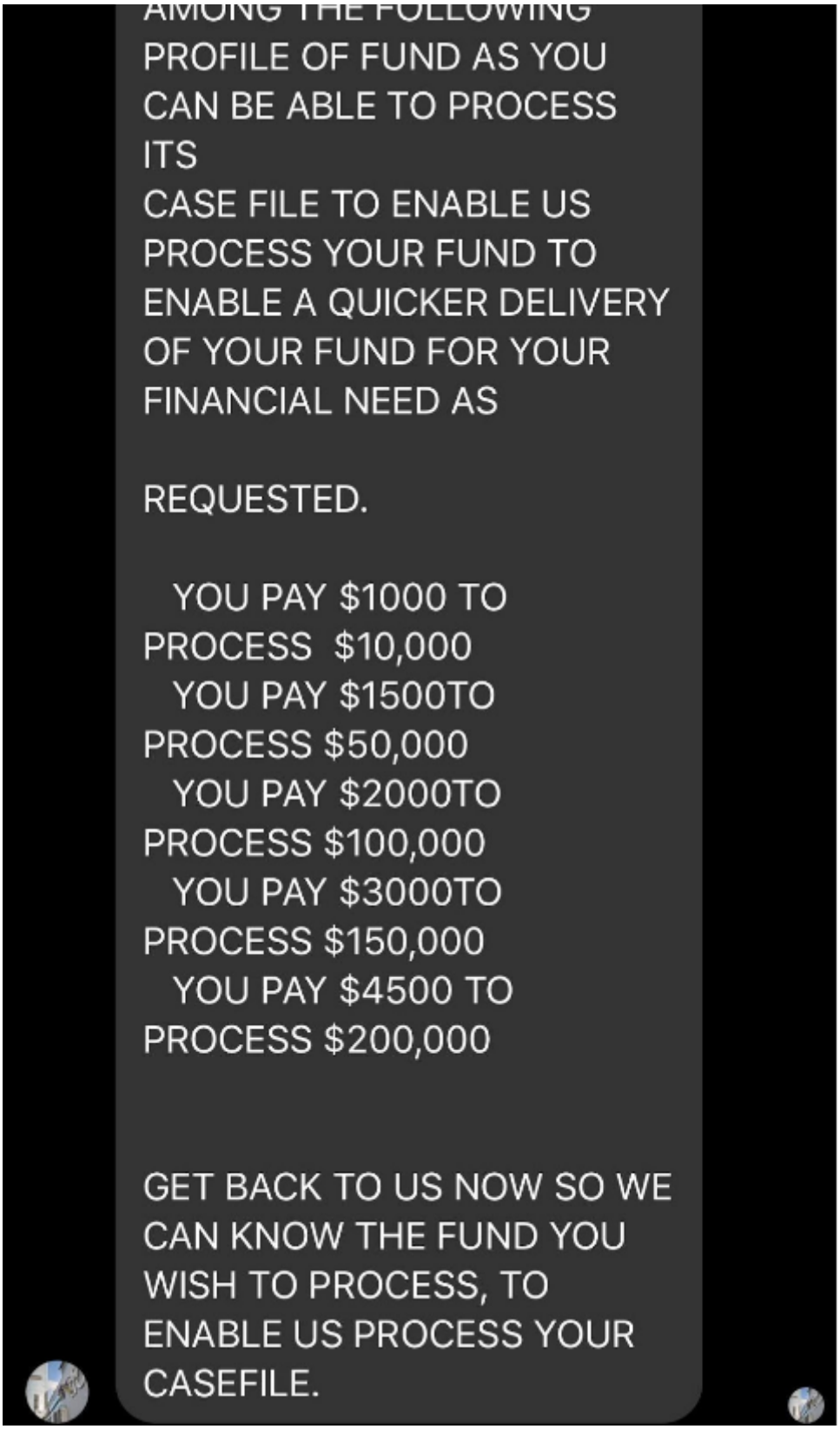
Minuga võttis paar päeva tagasi Facebook Messengeris ühendust Ameerika sugulane, kes pealtnäha oli päris õige inimene: pilt ja nimi läksid kokku ja tegu oli — veelkord, PEALTNÄHA — vana tuttavaga. Ometi torkas kohe silma, et asi ei ole õige.



Esiteks oli sama inimene mul juba varem Messengeris kontakt, aga nüüd lisas uuesti. Noh, ikka juhtub, äkki lukustas end vanalt kontolt välja ja tegi uue. Samas, vana konto oli alles hiljuti aktiivne olnud. Teiseks hakkas ta minuga suhtlema inglise keeles, kuigi me olime varem alati ilma probleemideta eesti keeles hakkama saanud. Tagatipuks hakkas ta mulle veel ühte rahvusvahelist rahastamisskeemi soovitama, kus stipendiumi kättesaamiseks tuli kõigepealt fondile sümboolne summa maksta.

Kuidas lugu edasi läks, võid lugeda artikli lõpus olevalt lingilt. Lühidalt oli tegu pisikese edasiarendusega nii-öelda “nigeeria kirjast.” Ehk siis sulle pakutakse suuremat hunnikut raha, mille kättesaamiseks pead kõigepealt pakkujale omajagu väiksema, aga siiski olulise summa läkitama. Edasiarendus seisnes

selles, et nüüd oli mu oma “tuttav” kõrva ääres skeemile takka kiitmas. Loogika seisneb siis selles, et kuna tema sai raha kätte, võiks mina antud organisatsiooni oluliselt rohkem usaldada.



Mängisin nendega mõnda aega, aga lõpuks saatsin teavituse koos kõigi sinna juurde käivate oluliste andmetega CERT-EE meiliaadressile. Lisaks raporteerisin

võltskontod ka Facebookis ja andsin ookeanitagusele sugulasele märku, kuidas tema nime ja pilti kuritarvitatakse.

Järgnevalt mõned head näpunäited, mis mind korduvalt pettuse ohvriks langemisest päästnud on. Loodetavasti aitavad ka sind.

1. **Ära ole ahne**. Kui miski tundub liiga hea, et tõsi olla, on ilmselt tegu pettusega. Ja petturid tunduvad ikkagi eelkõige inimlikku ahnust sihtivat.

2. **Jälgi hoolikalt, kellega sa e-kanalites suhtled**. Kui ise ei tea, millele tähelepanu pöörata, küsi mõne IT-teadlikuma sõbra abi. Kui keegi võõras sind ootamatult sõbraks lisab, uuri ühistelt tuttavatelt, kellega on tegu. Tuttav? Uuri mõnes teises suhtluskanalis üle, kas see on ikka tema. Näiteks helista või saada sõnum.

3. **Kaitse oma andmeid**. Kui sinult küsitakse digitaalsetes kanalites andmeid nagu isikukood, telefoninumber või esimese koera nimi, võib keegi neid sinu vastu kurjalt ära kasutada. Näiteks väita mõnele teenusepakkujale, et tema on sina ja tahab nüüd oma kontole ligi pääseda, aga unustas parooli ära. Jälgi väga hoolega, kellele ja miks sa oma andmeid jagad.

4. **Kaitse oma kontosid**. Isegi kui sa arvad, et sul midagi varjata ei ole, võib pätt su konto vallutada hoopis selleks, et sinu sõprade usaldust kuritarvitada. Ära tee seda neile liiga lihtsaks. Järgmised kaks nippi aitavad seda teha.

5. **Ära kasuta liiga lihtsat salasõna**. Kõige lihtsam on su kontole sisse murda juhul, kui parool on kergesti äraarvatav. Sinu nimi, sünnikuupäev, 123456, jms. Ohtlik on ka parool, mida sa meeles EI suuda pidada — selle pead sa tõenäoliselt kuhugi kirja panema ja see võib lekkida.

6. **Ära kasuta mitmes kohas sama parooli**. Sinu salasõna võib igalt poolt lekkida. Mida rohkemates kohtades sa sama võtit kasutad, seda lihtsam on ühe lekkega igale poole sisse murda. Kui vaja, võta appi paroolihaldur, näiteks KeePass, 1Password, DashLane või kasvõi veebilehitseja sisseehitatud funktsionaalsus. NB! Arvesta riskiga, et nii on sul “kõik munad ühes korvis” — ka paroolihaldur võib rünnaku ohvriks langeda.

7. **Lülita sisse mitmeastmeline autentimine (MFA, 2FA, vms)**. Sellisel juhul on kurikaeltel raskem su kontot üle võtta, sest sisselogimisel toimub topeltkontroll. Näiteks saadetakse sulle SMS kontrollkoodiga.

NB! Kui sind rünnatakse, teavita CERT-EE-d. Selleks saada ründe oluline info aadressile cert@cert.ee.

Täispikk “mäng” petistega on loetav Kristjan Karmo isiklikus veebipäevikus:

https://garf.juhe.ee/wp/2020/03/26/ara-mine-onge-libakontod-ifc-ja-klassikaline-petuskeem-pisut-uues-kuues/

KRISTJAN KARMO

Kristjan Karmo on Arvutimaailma pikaajaline kaasautor, kes on IT-s tegev olnud üle 20 aasta. Küberkuritegevust on ta üldiselt jälginud turvalisest kaugusest, aga kui asi isiklikuks läheb, on raske tagasi hoida.

Kristjan on ka Arvutimaailma YouTube kanalit haldava Must Post OÜ osanik.

- Tegijad
- Lahendused

- Turvalisus

Pilt