Damir Dizdarević

05.11.2025. 13:35
Pogledano: 54 puta

PREVARE U DIGITALNOM SVIJETU I KAKO IH IZBJEĆI (2.dio) – KRAĐA DIGITALNIH IDENTITETA

U prošlom nastavku, bavili smo se temom prevara u digitalnom svijetu koje za cilj imaju materijalnu odnosno finansijsku korist. Pomenuli smo tada da su te vrste prevara najčešće jednokratne, stresne, ponekad i otrežnjujuće ali uglavnom nemaju dugoročne niti šire efekte osim u nekim ekstremnim slučajevima.

No pored ove vrste prevara, u digitalnom svijetu možemo sresti i još jednu široko rasprostranjenu kategoriju zlonamjernih aktivnosti a to je ugrožavanje odnosno krađa digitalnog identiteta žrtve. I dok prevare iz prethodnog teksta imaju za krajnji i jedini cilj novac, krađe identiteta su vrlo često višefazne, novac im može ali i ne mora biti krajnji cilj, a posljedice su obično mnogo teže za sanaciju. Ova vrsta prevara je zato vrlo podmukla, često jedno vrijeme i nevidljiva pa samim tim i teža za otkrivanje. Zato je potrebno posvetiti posebnu pažnju upravo ovoj vrsti prevara kako bi se smanjila mogućnost da postanete žrtva.

U jednom od ranijih tekstova iz ovog ciklusa govorili smo o digitalnom identitetu i njegovoj važnosti. Rekli smo tada da je digitalni identitet reprezent fizičke osobe u digitalnom svijetu, te da nas vrlo često opisuje mnogo bolje i detaljnije nego par suhoparnih atributa kojima smo formalno definisani kroz lične dokumente koje sam izdaje država. Želite li danas da saznate nešto o nekome koga ne poznajete lično, vaš prvi izbor će sasvim sigurno biti da ga potražite na društvenim mrežama. Nekada bismo možda pokušali da se raspitamo kod zajedničkih poznanika, ali danas je mnogo jednostavnije i brže pregledati Instagram, Facebook i LinkedIn, te za par minuta saznati dosta toga o osobi koja nas interesuje. Vjerovatno čak i više nego što bi nam ta osoba sama rekla u prvom razgovoru. Digitalni identitet još uvijek nije jedinstven kao ovaj analogni. Za razliku od fizičkog identiteta koji je samo jedan za svaku osobu (osim ako niste kriminalac), u digitalnom svijetu je sasvim normalno da imamo više od jednog identiteta – za posao, za LinkedIn, za Facebook, za Twitter, Instagram, TikTok i tako dalje. Već dosta dugo se u naučnim krugovima, koji se bave digitalnim svijetom, traga za rješenjem koje bi omogućilo da svako ima samo jedan digitalni identitet, a koji bi na neki način sublimirao sve atribute sa danas različitih digitalnih identiteta koje ima svaka osoba. Takav identitet bi bio jedinstven za svaku osobu i mogao bi da se koristi na svim ili bar većini servisa koji danas zahtijevaju posjedovanje zasebnog digitalnog identiteta (koji često nazivamo i korisnički nalog ili account). Ipak, do globalno prihvatljivog rješenja se još uvijek nije došlo. Za one koje zanima više o ovome konceptu preporučujem da pretražite sadržaje na temu „decentralized identity“.

Značaj digitalnog identiteta direktno je proporcionalan učešću i aktivnošću njegovog vlasnika u digitalnom svijetu. Ovo je potpuno suprotnom onome kako se ponaša naš analogni identitet – čija se vrijednost ili značaj uglavnom ne mijenja. Razlika se najbolje vidi na sljedećem primjeru. Ukrade li neko ličnu kartu ili čak kreditnu karticu neke poznate osobe poput Elona Muska ili Billa Gatesa, vjerovatno se neće mnogo okoristiti, a sanacija štete će biti vrlo jednostavna. S druge strane, ako bi neko kojim slučajem uspio samo na par sati da preuzme kontrolu nad digitalnim identitetom neke od ovih osoba recimo na Twitteru, šteta bi mogla biti ogromna i teško sagledliva. Samo jedan tweet ovih osoba može uticati na značajan pad ili rast vrijednosti dionica kompanija, što lančano može izazvati pogrešne reakcije hiljada ili miliona njihovih pratilaca. Kontroverzni i ekscentrični Musk je tako, bukvalno putem tweet-ova već par puta rušio i dizao vrijednost BitCoin-a ali i vrijednost dionica kako svoje tako i drugih kompanija. Šta bi mogao uraditi neko zlonamjeran, preuzimanjem digitalnog identiteta neke uticajne osobe, može se samo naslućivati.

Međutim nisu samo poznate, bogate i uticajne osobe ugrožene od krađe digitalnog identiteta. Oni možda jesu pod najvećim rizikom, ali ugroženi su praktično svi. Krađa ili kompromitacija digitalnog identiteta žrtve može da se radi iz različitih razloga – da bi se neovlašteno pristupilo nečijim podacima, da bi se sama žrtva kompromitovala, da bi se došlo do novca ili jednostavno iz zabave. Šta god da je motiv, rezultat je to da žrtva više nema kontrolu nad jednim ili više svojih digitalnih identiteta. Većina kompanija koje su vlasnici popularnih servisa poput Google-a, Meta, Microsofta i sl. imaju procedure koje se aktiviraju kada prijavite da vam je neko ugrozio ili preuzeo nalog (identitet) na nekoj od mreža, ali te procedure često nisu jednostavne niti brze, jer sada vi morate da dokažete da ste onaj ili ona za koju se predstavljate, te da je ukradeni identitet zaista bio vaš. Za to vrijeme, napadač može da radi ono što je naumio, predstavljajući se kao vi, kako prema drugim korisnicima tako i prema digitalnim servisima na koje ste imali pristup. Međusobne interkonekcije različitih servisa cijelu priču čine još složenijom.

Kako se krade digitalni identitet?

Kada formirate svoj digitalni identitet na nekom Internet baziranom servisu obično prolazite kroz manje-više uobičajenu proceduru. Ostavljate nešto od svojih ličnih podataka, i u jednom od koraka definišete svoje korisničko ime i lozinku. Ta dva podatka, korištena zajedno, su način kako vi „otključavate“ svoj digitalni identitet, te zatim pristupate resursima servisa na kojem ste ga kreirali (recimo Gmail, Facebook, Instagram, Office365 itd.). Kako smo ranije govorili, izrazito je preporučljivo uz lozinku definisati i metoda više faktorske provjere (obično putem mobilnog telefona) ali veliki broj korisnika to još uvijek ne radi. Prema tome, napadaču je obično dovoljno da na neki način sazna vaše korisničko ime i lozinku i time sebi omogući pristup svemu čemu vi inače imate pristup. Nekad ranije, lozinke su mogle i da se pogode (kroz tzv. bruteforce napade) jer su korisnici težili ka tome da postavljaju lako pamtljive i jednostavne lozinke, ali danas se taj metod krađe sve manje koristi. Umjesto toga, pribjegava se metodima socijalnog inžinjeringa putem kojeg se korisnik navodi da sam otkrije odnosno upiše svoje podatke (korisničko ime i lozinku) na mjesto koje mu napadač podmetne. U metodima socijalnog inžinjeringa napadači su izrazito maštoviti i

vješti, pa je zato potrebno biti posebno oprezan. Neki od najčešćih načina su:

· Lažna obavijest putem emaila da vam je istekla lozinka na nekom od servisa koje upotrebljavate, te da je potrebno da je odmah promijenite. U mailu se obično podmetne link na stranicu napadača (koja izgleda slično ili isto kao prava) i gdje se od korisnika traži da upiše postojeću i novu šifru. Nasjednete li, napadač dobija vaše podatke vrlo brzo, pristupa vašem nalogu, mijenja šifru na onu koja je samo njemu poznata i vi više nemate pristup.

· Lažna obavijest da vam je neko pokušao provaliti u korisnički nalog te da je hitno potrebno da potvrdite vlasništvo nad istim da biste ga zadržali. Dalji scenario je isti kao u prethodnom slučaju.

· Lažna obavijest od banke da je potrebno da upišete svoje podatke za e-banking radi održavanja sistema.

· Lažna obavijest od policije (ovo je dosta često u zadnje vrijeme kod nas) da ste počinili prekršaj, te da je potrebno da se logirate na stranicu policije (naravno lažnu) kako biste napisali izjašnjenje.

· Lažna obavijest telekom operatera da je vaš račun zadužen za neki veliki iznos pri čemu se navodite na logiranje na lažnu stranicu

· Lažne obavijesti o nagradama koje daju velike kompanije poput Microsofta, gdje se traži upisivanje korisničkog imena i lozinke da bi se nagrada „preuzela“.

· Lažna obavijest da vam je prostor u mailboxu popunjen i da je potrebno logiranje da biste isti proširili inače će vam nalog biti suspendovan.

· Telefonski poziv, navodno novog uposlenika u IT-u kompanije u kojoj radite, u kojem se traži da kažete svoje lozinku kako bi se izvršile neke navodne „popravke“ na sistemu.

Ovo su samo neke, najčešće primijećene, tehnike koje napadači koriste ne bi li žrtvu naveli da upiše svoje podatke za pristup digitalnom identitetu na stranicu koju napadač podmetne, a koja najčešće izgleda vrlo slično onim pravim. Nemoguće je pobrojati sve načine koji se danas koriste jer se gotovo svakodnevno iznalaze novi metodi. Dok su ranije ove lažne obavijesti dolazile uglavnom na engleskom jeziku, danas je gotovo redovna pojava da se iste lokaliziraju na jezik žrtve što ih čini dodatno uvjerljivim. Tehnologije napreduju, pa tako i metodi za napade. Napadači posvećuju dosta vremena pripremi, posebno ako napadaju neku tačno određenu žrtvu. Na dark web-u je moguće (naravno ilegalno) platiti i naručiti napad na digitalni identitet određene osobe. Napadač je tada motivisan novcem koji dobija od naručitelja napada, često i ne znajući koga i zašto napada.

Kako se zaštititi od krađe digitalnog identiteta?

Svijest o važnosti digitalnog identiteta i potrebi njegove zaštite ključna je za odbranu od ove vrste napada. Ta svijest je danas, u prosjeku, na dosta niskom nivou pa je i broj uspješnih napada ove

vrste dosta visok. Naprosto, ljudi još uvijek nemaju stvarnu predstavu o tome koliko su duboko u digitalnom svijetu i koliko je važno da svoje bivanje u istom obezbijede. Nešto poput pješaka koji bi se šetali autoputem nesvjesni da tuda prolaze automobili i to velikom brzinom.

Kada svijest postoji, na nju se onda mora nadograditi znanje o tome kako prepoznati i izbjeći napade ove vrste. Neke ključne preporuke, savjeti i činjenice su:

· Prije upisivanja korisničkog imena i lozinke na neku web stranicu uvijek provjeriti da li je ista autentična, pogotovo ako ste na nju došli putem linka iz emaila. Autentičnost se može provjeriti pregledom web adrese na kojoj se stranica nalazi (kako smo ranije pisali), posjedovanjem validnog certifikata na web stranici (na to će vas upozoriti Internet pretraživač) kao i pregledom sadržaja stranice.

· Nikada ne vjerovati porukama u kojima se od vas traži upisivanje korisničkog imena i lozinke, posebno ako izgleda da te poruke (navodno) stižu od velikih i dobro poznatih kompanija (Google, Microsoft, Facebook,..). Niti jedna ozbiljna kompanija neće od korisnika tražiti lozinku putem emaila.

· Nikada ne vjerovati porukama od telekoma ili banke u kojem dobijate poziv da izvršite određenu akciju koja zahtijeva upisivanje lozinke. Ako ipak mislite da je poruka autentična, provjerite radije prvo telefonom pozivanjem call centra.

· Niti jedna policija ne obavještava prekršioce zakona putem emaila o počinjenom prekršaju a pogotovo ne traži izjašnjenje putem emaila. Koliko god te poruke djelovale uvjerljivo (a djeluju uvjerljivo, čak i za naše lokalne policije) nemojte nasjedati.

· Ako se nađete u situaciju da neko putem telefona traži vašu lozinku, nemojte to raditi. Niko dobronamjeran to neće tražiti.

· Nikada nemojte dijeliti svoje korisničke podatke za bilo koji servis sa drugim ljudima. Koliko god da nekome vjerujete, to predstavlja dodatni rizik.

· Nemojte postavljati iste lozinke na različite digitalne identitete. Ako to uradite, ugrožavanje jednog identiteta olakšava napadaču i ugrožavanje drugih sa istom loznikom.

· Uključite višefaktorsku provjeru autentikacije gdje god je to moguće. Vrijedi potrošiti tih par sekundi više prilikom logiranja, a sigurnost se značajno podiže.

U svakom slučaju, opreza nikada nije previše. Ako sumnjate, pitajte ili provjerite. Razmišljajte o svom digitalnom identitetu i onome što znači za vas. U budućnosti koja je pred nama, bez svake sumnje, to će biti sve važnije i važnije. Dosta skoro, morat ćemo početi razmišljati i o grobljima digitalnih identiteta. Koliko god da ta tema danas zvuči morbidno ili uvrnuto, „sahrana“ digitalnog identiteta je jednako realna kao i njegovo „rođenje“. Ali to je već neka druga tema.

Tags

Digitalna kompetencija

Collections

Autorski tekstovi

AI u nastavi