FAKTOGRAF

MALDITA.ES
PERIODISMO PARA QUE NO TE LA CUELEN

TIPOLOGIJA DIGITALNIH PRIJEVARA: OKVIR ZA OTKRIVANJE, KLASIFIKACIJU I PREVENCIJU

Projekt “Razotkrivanje prevara: odgovor poslovnog sektora i građana” provodi se zahvaljujući Fondu za građanske inovacije (CIF), jedinstvenom europskom zajedničkom fondu organizacije THE CIVICS Innovation Hub. Zaklada ERSTE podržava CIF.

UVOD

Budući da je gotovo svaki aspekt naših života postao digitalno povezan, posljednjih smo godina svjedočili kako je dostupan prostor napada za kibernetičke kriminalce eksponencijalno rasla i kako je, s današnjom tehnologijom, samo nekoliko pritisaka tipki dovoljno za otimanje mreža, paraliziranje vodoopskrbnih sustava ili čak krađu iz virtualnih razmjena. Slučaj koji to dobro ilustrira može se naći u podacima koje je prikupio FBI-jev Centar za pritužbe na internetski kriminal (IC3), primarno središte za

javno izvješćivanje o prijevarama i kibernetičkim prijetnjama u Sjedinjenim Američkim Državama. Prema *Izvješću o internetskom kriminalu za 2024. godinu*, dok je IC3 u početku primao oko 2.000 pritužbi mjesečno, u posljednjih pet godina taj je broj prosječno iznosio više od 2.000 pritužbi dnevno **[1]**. Samo u prošloj godini centar je zabilježio 859.532 pritužbe na kibernetički kriminal, s prijavljenim gubicima većim od 16,6 milijardi EUR (14,225 milijuna EUR), što predstavlja povećanje od 33 % u odnosu na 2023. godinu **[1]**.

Na međunarodnoj razini, u *Izvješću o globalnom stanju prijevara 2024.* Globalnog saveza za borbu protiv prijevara (GASA), koje se temelji na istraživanju provedenom na 58.329 osoba diljem svijeta, procijenjeno je da su prijevare preusmjerile više od 1,03 bilijuna dolara (882.000 milijuna eura) u samo protekloj godini - iznos koji konkurira bruto domaćem proizvodu (BDP) nekih zemalja **[2]**. Za neke zemlje to je predstavljalo gubitak od više od 3 % njihovog BDP-a, kao što je 4,2 % u Pakistanu i 3,6 % u Keniji. Isto izvješće također je naglasilo sveprisutnost problema, ističući da se gotovo polovica globalne populacije susreće s prijevarom barem jednom tjedno, dok samo 4 % žrtava uspijeva u potpunosti vratiti svoj novac **[2]**.

Štoviše, Svjetski gospodarski forum je u svojem izvješću Globalni izgledi za kibernetičku sigurnost 2025. prepoznao kibernetički kriminal omogućen tehnologijom - uključujući krađu identiteta, kompromitiranje poslovne e-pošte (eng. *business email compromise*, BEC) i *vishing* - kao drugi najveći organizacijski kibernetički rizik za 2025. godinu **[3]**. Štoviše, 42 % organizacija prijavilo je da su u proteklih 12 mjeseci doživjele *phishing* (krađu identiteta) ili napade socijalnog inženjeringa. Ove kampanje postale su sve sofisticiranije i skalabilnije, na primjer, zbog alata generativne umjetne inteligencije (GenAI), koji smanjuju troškove

napada i omogućuju kibernetičkim kriminalcima da automatiziraju i personaliziraju varljive komunikacije **[3]**.

Osim neposrednih financijskih gubitaka, širenje kibernetičkih prijevara narušava povjerenje građana u digitalni ekosustav i ugrožava ugled tvrtki čija se imena i robne marke iskorištavaju u prijevarnim shemama. U kontekstu ove stvarnosti, neophodno je razviti alate koji omogućuju rano prepoznavanje ponavljajućih obrazaca, analizu trendova u nastajanju i predviđanje nove dinamike prijevara. Na temelju te potrebe, ovaj rad vođen je dvostrukim ciljem: **(1) podići svijest među tvrtkama i nadzornim agencijama** o društvenom i ekonomskom utjecaju zlouporabe robne marke, s naglaskom na transparentnost i etičku odgovornost prema građanima oštećenim ovim kibernetičkim prijevarama; i (**2) opremiti stručnjake i građane** znanjem potrebnim za otkrivanje i analizu načina na koji se robne marke iskorištavaju u prijevarama osmišljenim za obmanjivanje korisnika, izvlačenje osobnih podataka i manipuliranje financijskim ponašanjem. U tu svrhu predlažemo razvoj **klasifikacijske tipologije temeljene na stvarnim slučajevima**, zamišljene kao alat za podršku **široj javnosti, agencijama za praćenje medija i njihovim klijentima** u prepoznavanju obrazaca prijevara i jačanju financijske svijesti među građanima. Razlozi za usvajanje ove klasifikacije su sljedeći:

(I) PROŠIRUJE ZNANJE O PROBLEMU I UČINKOVITIJE RAZLIKUJE FORMATE I VRSTE PODATAKA

Kibernetičke prijevare prikazuju ponavljajuće obrasce i formate koji omogućuju stručnjacima da identificiraju njihove ključne elemente. To uključuje, na primjer, strukture poruka, prijevarne metode kontaktiranja i specifična ponašanja URL-a ili tehnike socijalnog inženjeringa. Takva diferencijacija olakšava klasifikaciju, poboljšava

točnost u identifikaciji incidenata i produbljuje razumijevanje načina djelovanja prevaranata u različitim kontekstima. Štoviše, dokumentiranje tih modaliteta funkcionira kao povijesni zapis kibernetičkog kriminala, koristan za predviđanje promjena u okruženju digitalnog kriminala.

(2) POBOLJŠAVA SPOSOBNOST ODZIVA TVRTKI

Poduzeća i organizacije trebaju praktične alate kako bi utvrdili kada se njihov brend zloupotrebljava u prijevari i brzo reagirali. Praćenje incidenata podržano standardiziranom tipologijom omogućit će im: bržu identifikaciju povezanih incidenata, izradu specifičnijih internih protokola odgovora i kampanja prevencije, razvoj sustava ranog upozoravanja i učinkovitiju suradnju s drugim akterima u sektoru.

(3) SMANJUJE FINANCIJSKE GUBITKE I ŠTETU UGLEDU

Jasna tipologija omogućuje ranije otkrivanje i bolju klasifikaciju, tako da poboljšanjem identifikacije i sprječavanja kibernetičkih prijevara pomaže u izbjegavanju financijskih gubitaka i za potrošače i za tvrtke, uz očuvanje vrijednosti marke i povjerenja kupaca (npr. putem proaktivnih obavijesti i prilagođene komunikacije kada prevaranti zloupotrebljavaju marku). Naime, kada prevaranti upotrebljavaju marku za obmanu, mogu povećati negativne asocijacije s markom.

(4) POTICANJE INFORMACIJSKE I MEDIJSKE PISMENOSTI

Uspostavljanjem jasne i specifične klasifikacije kibernetičkih prijevara, ovaj okvir otvara vrata programima informacijske

i medijske pismenosti - kako vanjskim tako i unutarnjim - usmjerenima na kibernetičku sigurnost i utemeljenima na praćenju prijevara prema tipologiji. Za građane to znači razumijevanje načina na koji prijevare funkcioniraju i prepoznavanje njihovih znakova upozorenja, čime se razvijaju kritične vještine kako bi se spriječila obmana. Za tvrtke to podrazumijeva internu obuku i mogućnost boljeg informiranja i upozoravanja svojih klijenata o prijevarama koje iskorištavaju njihov brend, čime se jača povjerenje i zaštita potrošača.

(5) OSIGURAVA TERMINOLOŠKU DOSLJEDNOST U ORGANIZACIJAMA

Fragmentacija u načinu na koji se internetske prevare imenuju i kategoriziraju ometa suradnju između tvrtki, regulatora i organizacija civilnog društva. Ova tipologija temelji se na pažljivo definiranom vokabularu koji podliježe terminološkoj kontroli, osiguravajući da se pojmovi upotrebljavaju dosljedno i u skladu s drugim organizacijama. To zauzvrat olakšava buduću razmjenu informacija i usporednu analizu trendova.

(6) PREDNOSTI UČINKOVITIH JAVNIH POLITIKA ZA ZAŠTITU POTROŠAČA

Osim svoje vrijednosti za tvrtke i organizacije, detaljna klasifikacija i dubinska analiza kibernetičkih prijevara pružaju neprocjenjiv resurs za akademska istraživanja i razvoj javnih politika. U znanstvenom kontekstu nudi solidnu empirijsku osnovu za istraživanja u području kibernetičke sigurnosti, digitalne kriminologije i srodnih područja. Nadalje, omogućuje longitudinalne analize trendova koje mogu pratiti razvoj taktike prevaranata i predvidjeti nove modalitete prijevare - podatke koji su ključni za osmišljavanje učinkovitih javnih politika o kibernetičkoj sigurnosti i zaštiti potrošača.

KONTEKST I POZADINA

Internetska prijevara oblik je namjerne obmane osmišljene za stjecanje nezakonite dobiti na štetu žrtve. Karakterizira ju uporaba prijevarnih metoda koje iskorištavaju povjerenje, neznanje, pohlepu ili emocije pogođene osobe, kako bi ju potaknule na poduzimanje radnji koje koriste prevarantu. Australska savezna policija pruža sveobuhvatniju definiciju internetske prijevare definirajući pojam kao **„bilo koju vrstu sheme prijevare koja upotrebljava e-poštu, internetske stranice, sobe za čavrljanje ili internetske forume za predstavljanje lažnih poziva potencijalnim žrtvama, za provođenje lažnih transakcija ili za prijenos prihoda od prijevare financijskim institucijama ili drugima povezanim sa shemom.“ [10]**

Prijevare često upotrebljavaju tehnike uvjeravanja ili psihološke manipulacije kako bi obmanuli žrtve, iskorištavajući njihovu dobru volju ili njihove strahove i želje. Te radnje mogu uključivati upotrebu uvjerljivih narativa, lažnih obećanja, naizgled atraktivnih ponuda ili krađu identiteta.

Posljedice internetske prijevare mogu se kretati od financijskih gubitaka do gubitka osobnih podataka (financijskih podataka, osobnih dokumenata i drugih relevantnih osobnih podataka), koje kibernetički kriminalci čak mogu upotrijebiti za lažno predstavljanje kao žrtva u kriminalne svrhe. **[3]**

Kibernetički kriminalci i prevaranti neprestano usavršavaju svoje metode, koristeći napredne tehnologije kako bi povećali učinkovitost i doseg svojih napada.

- **Upotreba umjetne inteligencije (AI) i velikih jezičnih modela (LLM):** Generativna umjetna inteligencija (GenAI) i LLM-ovi povećavaju učinkovitost tehnika socijalnog inženjeringa omogućavanjem personalizirane komunikacije i automatizacijom kriminalnih postupaka **([3]**, **[6]**, **[9])**.

Omogućuju napadačima da smanje troškove kampanja krađe identiteta i socijalnog inženjeringa; uvjerljivo oponašaju komunikacijske stilove viših rukovoditelja i organizacija iskorištavanjem kontekstualnih podataka s društvenih mreža, javnih izjava ili dokumenata koji su procurili; i istovremeno izrađuju vjerodostojne napade na više jezika - ciljajući više ljudi u više zemalja uz niže troškove **[3]**. Nedavna istraživanja pokazuju da poruke o krađi identiteta koje generiraju LLM-ovi postižu znatno veće stope klikova od onih koje su napisali ljudi **[7]**. Osim toga, GenAI omogućuje zlonamjernim akterima stvaranje uvjerljivih *deepfake* snimki glasa, videozapisa i slika te imitiranje stilova korporativne komunikacije **[6]**, koji se mogu upotrijebiti za prijevaru i organizacija (npr. kada se takve dubinske prijevare održavaju tijekom dugotrajnih interakcija s osobljem, mogu pomoći napadačima da dobiju pristup korporativnim sustavima) i potrošača. U tom kontekstu, 47 % organizacija koje je anketirao WEF **[3]** izrazilo je zabrinutost zbog neprijateljskih sposobnosti koje pokreće GenAI, a 55 % CISO-a izjavilo je da dubinske prijevare predstavljaju umjerenu do značajnu kibernetsku prijetnju njihovoj organizaciji **[3]**. Također je vrijedno napomenuti da, iako je porast umjetne inteligencije u taktici prijevare sve veći razlog za zabrinutost, 31 % ispitanika u istraživanju GASA-e iz 2024. godine nije bilo sigurno jesu li kibernetičke prevare koje su pretrpjeli uključivale umjetnu inteligenciju **[2]**.

- **Zajednički kanali i platforme:** Telefonski pozivi i tekstualne poruke (SMS) ostaju primarni načini inicijalnog kontakta, a prevaranti također često upotrebljavaju platforme kao što su WhatsApp, Instagram i Gmail **[2]**.

• **Porast napada ucjenjivačkim softverom:** Ucjenjivački softver (eng. *ransomware*) ostaje jedan od glavnih rizika za organizacije i trajna, rastuća prijetnja organizacijama svih veličina **[1, 8]**. Prema Verizonovom izvješću o istragama povrede podataka za 2025. godinu, ucjenjivački softver je bio prisutan u 44 % svih analiziranih povreda, što je povećanje od 37 % u odnosu na prethodnu godinu **[8]**. Međutim, dobra je vijest da je srednji iznos isplaćen skupinama s ucjenjivačkim softverom pao na 115.000 dolara (sa 150.000 dolara prošle godine), a 64 % organizacija žrtava nije platilo otkupninu, što je više za 50 % u odnosu na prije dvije godine **[8]**.

• **Socijalni inženjering:** Kibernetička prijevara (uključujući *phishing*, BEC, *vishing* itd.) još je jedan od najvećih rizika **[11]**, što ilustrira činjenica da je 42 % organizacija koje je anketirao WEF doživjelo uspješan napad socijalnog inženjeringa 2024. godine **[3]**. Napadi socijalnog inženjeringa uključuju psihološki napad na osobu koji mijenja njihovo ponašanje na način da poduzimaju radnje ili krše povjerljivost **[8, 9]**. Unutar ove skupine, *phishing* i *pretexting* (prijetvarni izgovori) ostaju primarne taktike koje se upotrebljavaju za obmanjivanje zaposlenika **[8, 11]**. *Phishing* je utvrđen u 15 % svih kršenja, a stopa izvješćivanja za simulirane poruke e-pošte s *phishingom* znatno se povećala nakon nedavne obuke zaposlenika **[8]**. Značajno je i bombardiranje zahtjevima za višefaktorskom autentifikacijom (eng. *MFA prompt bombing*) - taktika koja preplavljuje korisnike zahtjevima za višefaktorskom autentifikacijom u nadi da će popustiti samo kako bi se upiti zaustavili. Uspješno je upotrebljena u više od 20 % napada socijalnog inženjeringa u javnom sektoru ove godine **[8]**. Na osobnoj razini, krađa identiteta ističe se kao vodeći percipirani kibernetički rizik

(37 %), nakon čega slijedi gubitak pristupa komunalnim uslugama (24 %), kompromitirani osobni podaci (20 %) i kibernetička iznuda (20 %) **[3]**.

• **Povećanje broja dobrotvornih prijevara koje iskorištavaju hitne situacije:** To je bilo vidljivo tijekom pandemije bolesti COVID-19, ruske invazije na Ukrajinu, potresa u Turskoj i Siriji te poplava „DANA" u Španjolskoj 2024. godine **[11, 12]**. Prevaranti pokazuju veliku svestranost u modeliranju svojih narativa oko trenutnih kriza.

• **Investicijske prijevare:** posebno one koje uključuju kriptovalute (poznate i kao „klanje svinja"), one su u kojima su prijavljeni najveći gubitci, s rekordnih 6,5 milijardi USD u 2024. i 66 % porasta gubitaka povezanih s kriptovalutama, prema podacima IC3 **[1]**.

• ***Crime-as-a-service* (CaaS):** Ovaj model ostaje dominantan i brzorastući jer akterima bez tehničke stručnosti omogućuje kupovinu kompleta, infrastrukture i podrške za počinjenje kaznenih djela - na primjer, za pokretanje kampanja za ucjenjivački softver ili krađu identiteta pojačanu umjetnom inteligencijom - čime se dramatično smanjuje prepreka ulasku **[3, 4]**. Kako bi se to omogućilo, ekosustav CaaS na forumima na mračnoj mreži (eng. *dark-web*) nudi širok pristup alatima za omogućavanje i vodičima o metodama prijevare, kompletima za *phishing*, alatima za daljinsku administraciju (eng. *remote administration tools*, RAT), odlagalištima kartica i bazama osobnih podataka **[11]**.

• **Konvergencija s organiziranim kriminalom i „farmama prijevara":** Porast i profitabilnost internetskih prijevara privukli su „tradicionalno" nasilne skupine organiziranog

kriminala na kibernetičko tržište. U jugoistočnoj Aziji dokumentirano je da je više od 220.000 osoba podvrgnuto prisilnom radu na „farmama za prijevare” koje kombiniraju prikupljanje podataka, dezinformacije i socijalni inženjering te djeluju kao pružatelji kaznenih usluga za treće strane **[5]**. Ova kultura niže odbojnosti prema nanošenju štete - uključujući utjecaj na kritične usluge - zajedno s razmjerom koju omogućuju CaaS platforme proširuje raspon organizacija izloženih napadima kao što je ucjenjivački softver **[3]**.

- **Izazovi u kibernetičkoj otpornosti i nedostatak vještina:** Kibernetička nejednakost se pogoršala, stvarajući sve veći jaz između velikih i malih organizacija te između razvijenih gospodarstava i gospodarstava u nastajanju **[3]**. Samo 15% ispitanika u Europi i Sjevernoj Americi nema povjerenja u sposobnost svoje zemlje da odgovori na velike kibernetičke incidente protiv kritične infrastrukture, dok se taj udio povećava na 36 % u Africi i 42 % u Latinskoj Americi **[3]**. Proširio se i jaz u kibernetičkim vještinama, pri čemu su dvije od tri organizacije prijavile umjerene do kritične nedostatke u ovom području, a samo 14 % organizacija izjavilo je da ima potrebno osoblje i vještine **[3]**.

METODA

KRITERIJI KLASIFIKACIJE

Kako bi se osigurala koherentnost i praktična primjenjivost, uspostavljen je primarni kriterij klasifikacije koji se temelji na najčešćim narativnim strategijama i tehnikama socijalnog inženjeringa utvrđenima u podacima prikupljenima putem sustava za upravljanje dezinformacijama (DMS) Maldita.es - koji obrađuje podatke iz korisničkih izvješća koja opisuju, različitim razinama detaljnosti, poruke, formate i kontekste u kojima se dogodio pokušaj obmane - i uspoređuje se sa slučajevima koje je otkrio Faktograf. Ovaj kriterij dopunjen je sekundarnim dimenzijama koje se odnose na upotrebljeni kanal ili tehniku te svrhu ili temu prijevare. To je spriječilo stvaranje pretjerano fragmentiranog ili nepraktičnog klasifikacijskog sustava, istodobno osiguravajući koherentnost i učinkovitost kontroliranog vokabulara.

PRELIMINARNI POPIS POJMOVA I PRIKUPLJANJA IZVORA

Nadovezujući se na prethodnu stručnost i reference tima Maldita.es dostupne u području kibernetičke sigurnosti, izrađen je preliminarni popis kandidata za pojmove, djelomično inspiriran *Vodičem za kibernetičke napade* španjolskog Nacionalnog instituta za kibernetičku sigurnost (INCIBE) **[13]**, koji je poslužio kao polazna točka za tipologiju.

Taj je popis zatim proširen i rafiniran upotrebom specijaliziranih izvora kako bi se osigurala čvrsta i sveobuhvatna klasifikacija i smanjio rizik od izostavljanja relevantnih koncepata. Pregledani izvori uključivali su izvješća o kibernetičkoj sigurnosti **[4-6, 9, 14-17]**, akademske i visokokvalitetne informativne članke **[7, 9, 10, 18]**,

vodiče za prevenciju od priznatih institucija (npr. INCIBE **[13, 19]**, Europol **[11]**, Guardia Civil **[20]**), industrijsku sivu literaturu **[21, 22, 24]**, kao i bibliografske baze podataka, postojeće klasifikacije, taksonomije, pojmovnike ili kontrolirane rječnike dostupne u specijaliziranim bazama podataka i repozitorijima **[25-32]**.

Proces se sastojao od sastavljanja najšireg mogućeg skupa relevantnih pojmova, koji su zatim privremeno grupirani prema tematskoj sličnosti i srodstvu. Ovaj je pristup pomogao konsolidirati robustan skup pojmova, osiguravajući da nijedan ključni element nije izostavljen iz konačne klasifikacije.

DEFINICIJE I TERMINOLOŠKA KONTROLA

Nakon što su odabrani kandidati za pojmove, definirani su i podvrgnuti terminološkoj kontroli, s ciljem osiguranja preciznog, koherentnog vokabulara prilagođenog području digitalne prijevare. Definiranje pojmova omogućilo je razgraničenje njihovog značenja i istovremeno olakšalo otklanjanje nedosljednosti unutar skupa. S obzirom na to da klasifikacije moraju funkcionirati kao kontrolirani vokabular, u ovom su procesu provjerena tri svojstva:

- **Homonimija:** pojmovi koji su se podudarali u obliku, ali su se odnosili na značenja izvan domene digitalne prijevare, odbačeni su.

- **Sinonimija:** kada se ista tehnika pojavila pod različitim imenima, odabran je najprecizniji i najrašireniji izraz u specijaliziranim izvorima. U slučajevima kada pojmovi nisu bili strogo sinonimi, već su se koristili naizmjenično, razvijene su sveobuhvatne definicije kako bi se utvrdilo je li objedinjavanje prikladno ili treba li koncepte zadržati kao zasebne.

- **Polisemija:** u slučajevima kada su pojmovi imali više značenja, primijenjen je jedan kriterij, ograničavajući svaki pojam na njegov smisao vezan za digitalne prijevare.

STRUKTURNA RAZMATRANJA

Nakon što su definirani kandidati za pojmove i odbačeni oni koji nisu relevantni, njihovi odnosi analizirani su kako bi se uspostavila koherentna klasifikacijska struktura. Mogu se identificirati sljedeće vrste odnosa između pojmova:

- Hijerarhijski odnosi (npr. između tehnika oponašanja i njihovih podtipova: *phishing*, *smishing*, *vishing*).

- Istodobno pojavljivanje pojmova (npr. ista prijevara koja kombinira socijalni inženjering i zlonamjerni softver (eng. *malware*)).

- Snažno povezani pojmovi (npr. *catfishing* i „lažno predstavljanje obitelji ili poznanika“ - odbačeni pojam).

- Međusobno isključivi pojmovi [1].

[1] Nismo identificirali zaista isključive kategorije. U praksi, napadi često obuhvaćaju više dimenzija - na primjer, napad *phishingom* također može isporučiti zlonamjerni softver. U skladu s tim, taksonomija je višestruka: analitičari mogu odabrati nekoliko opcija unutar klasifikacije kako bi kategorizirali jedan incident.

Rezultat je bila fleksibilna i skalabilna tipologija, organizirana u dvije komplementarne dimenzije, koje su razvijene u sljedećem odjeljku.

PREDLOŽENE KATEGORIJE PRIJEVARA

Pregled **specijaliziranih izvora** - vodiča INCIBE-a, akademskih članaka, izvješća o kibernetičkoj sigurnosti i terminoloških baza podataka - zajedno s analizom podataka prikupljenih putem DMS-a Maldita.es - koji obrađuje podatke korisničkih izvješća koja opisuju, različitim razinama detaljnosti, poruke, formate i kontekste u kojima se dogodio pokušaj obmane - i iskustva koja je Faktograf podijelio u vezi sa svojim radom na otkrivanju i razotkrivanju prijevara, omogućio je razvoj tipologije za strukturiranu klasifikaciju digitalnih prijevara i prijevara usmjerenih na poslovno okruženje.

Iako smo svjesni da digitalne prijevare mogu ciljati lozinku, vezu ili podatke i da se zlonamjerni softver može koristiti kao alat, ovdje predložena tipologija posebno se usredotočuje na one sheme prijevara koje se oslanjaju na **tehnike socijalnog inženjeringa.** Ovaj fokus odražava prirodu slučajeva prijavljenih na Maldita.es, koji uglavnom uključuju strategije obmane usmjerene na manipuliranje povjerenjem, strahom ili nedostatkom svijesti korisnika kako bi se postigla nezakonita dobit, i za koje smo prikupili najviše podataka i iskustva. Međutim, također je prepoznato da je važno uključiti određene pojmove koji odražavaju specifični cilj ili temu napada, kao što su financijske prijevare, pokušaji krađe osobnih podataka ili emocionalne prijevare, kako bi se osigurala sveobuhvatnija i kontekstualnija pokrivenost podataka.

Na temelju toga i kako bi se izbjegla pretjerano fragmentirana ili neupravljiva klasifikacija, tipologija je organizirana oko dvije glavne, neekskluzivne dimenzije: (1) **dimenzija temeljena na tehnici ili kanalu**, koja grupira prijevare prema tehnikama socijalnog inženjeringa, kanalima ili metodama koje se upotrebljavaju za izvođenje napada (npr. *phishing*, *smishing*, *QRshing* ili *vishing*); i (2) **tematska dimenzija**, koja klasificira prijevare na temelju narativa ili izgovora koji se upotrebljava za privlačenje pažnje žrtve (kao što su investicijska obećanja, lažne lutrije, nasljeđe, romantične

veze ili lažne ponude za posao). Ovaj pristup naglašava tematske i diskurzivne aspekte sadržaja, a ne njegove tehničke ili strukturne karakteristike, što podatke čini podložnijima identifikaciji i kategorizaciji unutar ove tipologije.

Osim toga, također omogućuje otkrivanje ponavljajućih obrazaca, kao i identifikaciju novih trendova, što je posebno korisno za generiranje upozorenja, osmišljavanje preventivnih kampanja ili poboljšanje internih protokola tvrtke. Štoviše, zamišljen je kao fleksibilna i skalabilna tipologija koja se može prilagoditi razvoju kriminalnih taktika i uključiti nove kategorije kako se pojavljuju.

U sljedećim odjeljcima prikazana je detaljna klasifikacija, zajedno s definicijama, dok se reprezentativni primjeri koji ilustriraju svaku kategoriju mogu naći u **Dodatku**.

TIPOLOGIJA I DEFINICIJE

DIMENZIJA TEMELJENA NA TEHNICI ILI KANALU

1. Napadi socijalnog inženjeringa: Oni se oslanjaju na skup tehnika usmjerenih na korisnike s ciljem da ih navedu da otkriju osobne podatke ili dopuste napadaču da preuzme kontrolu nad njihovim uređajima. Postoje različite vrste napada koje su temeljene na obmani i manipulaciji:

> **1.1. *Phishing*:** Slanje poruke putem e-pošte, društvenih mreža ili izravnih poruka uz lažno predstavljanje legitimnog subjekta - kao što je banka, društvena mreža, tehnička podrška ili javna institucija - kojem korisnik vjeruje, kako bi se postigao cilj napadača (Slika 1 i više primjera u Dodatku: **A1, A2, A3, A4, A17, A18**).

Slika 1: Prijevara *phishingom* u kojoj se osoba lažno predstavlja kao dostavljačka služba GLS

Izvor: ***Maldita.es***

Napomena: Lažne poruke e-pošte koje oponašaju GLS obavještavaju korisnike o „isporuci na čekanju“ i potiču ih da kliknu na poveznice koje vode do internetskih stranica koje od njih traže osobne i bankovne podatke, zahtijevajući plaćanje malih iznosa kao naknade za dostavu. Identitet brenda iskorištava se za krađu osjetljivih informacija i novca.

09/14/2021 06:39:27 am

Hrvatska pošta

VAŠA DOSTAVA JE NA PUTU

Dragi Gospodine / Gospođo

Plaćanje naknade za dostavu (6,37 kuna) i adresu za dostavu paketa potvrdite klikom na donju poveznicu:

Pošaljite moj paket

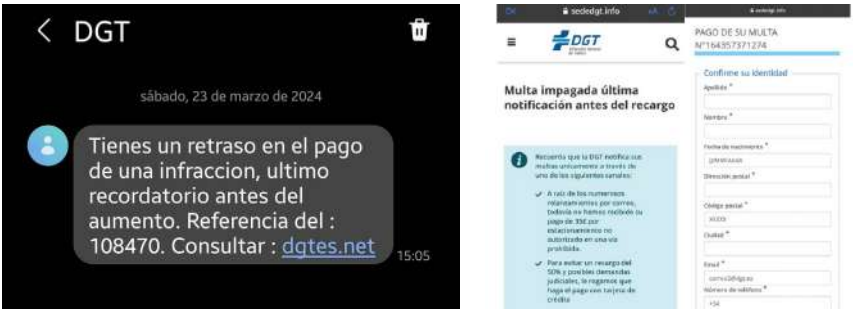
Traži se SMS potvrda. Da biste osigurali svoj identitet.

INFORMACIJE O ISPORUCI
PRIJAMNI BROJ POŠILJKE
MA221236010HR
E-pošta
urednik@t-com.hr

Izvor: Hrvatska Pošta

b. *Smishing*: Slanje prijevarnog SMS-a uz lažno predstavljanje kao pouzdani subjekt - kao što je banka, platforma društvenih mreža, tehnička podrška ili javna institucija - kako bi se postigao cilj napadača (slika 2).

Slika 2: *Smishing* i lažne obavijesti od službe ili ustanove



Izvor: ***Maldita.es***

Napomena: Za više informacija pogledajte sliku **A5** u Dodatku.

Izvor: Screenshot/Hrvatska pošta

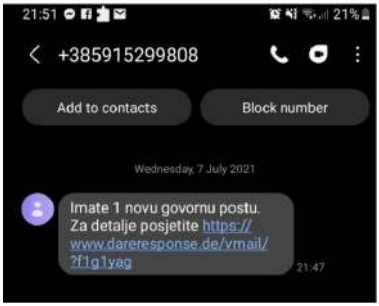
Napomena: Korisnicima se šalju lažne SMS poruke da nedostaju podaci o kućnom broju pa ih je potrebno ažurirati.

> **c. *Vishing:*** Telefonski poziv (ili video poziv) uz lažno predstavljanje kao legitimni subjekt - kao što je banka, društvena mreža, tehnička služba ili javni subjekt - kojem korisnik vjeruje, radi postizanja cilja napadača (slika 3.).

Slika 3: Vishing i lažne obavijesti od službe ili ustanove

Izvor: ***Maldita.es***

Napomena: Za više informacija pogledajte sliku **A6** u Dodatku.



Izvor: Screenshot/Telemach.hr

Napomena: Iza ove poveznice krije se zlonamjeran softver, a ne stranica na kojoj možete preslušati poruku govorne pošte.

> **d. *Baiting*:** Napadači upotrebljavaju oglase ili internetske stranice koje promiču natjecanja ili nagrade kako bi namamili korisnike da podijele dodatke ili preuzmu zlonamjerni softver. To može dovesti do krađe osobnih podataka, preuzimanja sustava, zaraze mreže ili oštećenja uređaja (slike 4, 5 i 6).

Slika 4: Prijetvorni oglasi na Twitteru koji promiču lažna ulaganja u kriptovalute

Izvor: ***Maldita.es***

Napomena: Lažni oglasi na Twitteru promoviraju izmišljene intervjue sa španjolskim glumcima kao što su Martiño Rivas i Antonio Resines. Tweetovi preusmjeravaju na internetske stranice koje se lažno predstavljaju kao medijske kuće, gdje glumci navodno tvrde da zarađuju „128.000 EUR mjesečno“ kroz ulaganja u kriptovalute. Ti oglasi krše pravila za oglase na Twitteru.

Izvor: Screenshot/Facebook

Izvor: Screenshot/Instagram

Slika 5: Baiting i promocije ili ponude

Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A7** u Dodatku.

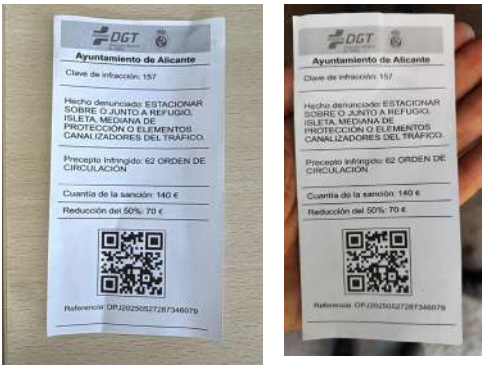
Slika 6: Baiting i promocije ili ponude

Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A8** u Dodatku.

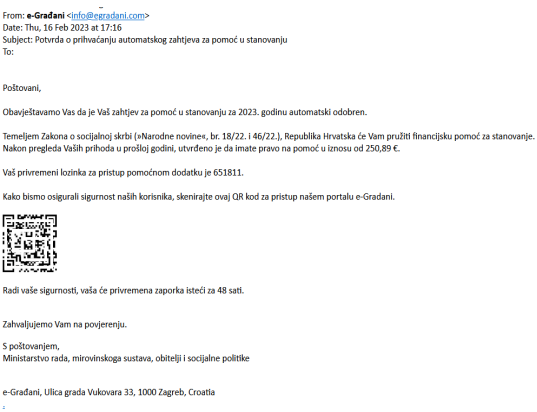
e. *QRshing*: krađa podataka ili novca, odnosno instalacija zlonamjernog softvera, putem skeniranja zlonamjernog QR koda (slika 7)..

Slika 7: QRshing i obavijesti od službe ili ustanove



Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A9** u Dodatku.



From: **e-Građani** <info@egradani.com>
Date: Thu, 16 Feb 2023 at 17:16
Subject: Potvrda o prihvaćanju automatskog zahtjeva za pomoć u stanovanju
To:

Poštovani,

Obavještavamo Vas da je Vaš zahtjev za pomoć u stanovanju za 2023. godinu automatski odobren.

Temeljem Zakona o socijalnoj skrbi («Narodne novine», br. 18/22. i 46/22.), Republika Hrvatska će Vam pružiti financijsku pomoć za stanovanje. Nakon pregleda Vaših prihoda u prošloj godini, utvrđeno je da imate pravo na pomoć u iznosu od 250,89 €.

Vaš privremeni lozinka za pristup pomoćnom dodatku je 651811.

Kako bismo osigurali sigurnost naših korisnika, skenirajte ovaj QR kod za pristup našem portalu e-Građani.

Radi vaše sigurnosti, vaša će privremena zaporka isteći za 48 sati.

Zahvaljujemo Vam na povjerenju.

S poštovanjem,
Ministarstvo rada, mirovinskoga sustava, obitelji i socijalne politike

e-Građani, Ulica grada Vukovara 33, 1000 Zagreb, Croatia

Izvor: Nacionalni CERT

> **f. *Catfishing*:** Napadači se lažno predstavljaju kao netko drugi - kao rođak, poznanik ili slavna osoba - ili upotrebljavaju lažni profil kako bi prevarili žrtvu i dobili osobne podatke ili novac (Slika 8 i više primjera u Dodatku: **A10**).

Slika 8: Catfishing, investicije i romantične veze

Izvor: Maldita.es

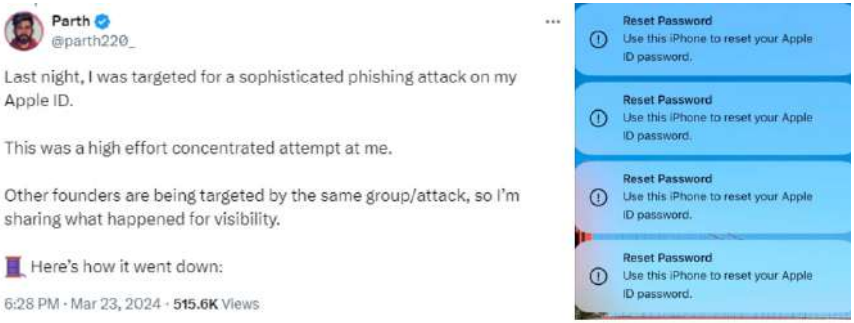
Napomena: Za više informacija pogledajte sliku **A11** u Dodatku.

Izvor: Screenshot

g. Ostali napadi socijalnog inženjeringa.

2. Napadi na lozinke: Pokušaji krađe korisničkih vjerodajnica. Kibernetički kriminalci upotrebljavaju tehnike i alate pomoću kojih pokušavaju dobiti naše korisničko ime i lozinku. Na primjer, mogu upotrebljavati specijalizirani softver ili ih pokušati pogoditi metodom pokušaja i pogrešaka na temelju informacija koje su prethodno prikupili. Jedan tip takvih napada, bombardiranje zahtjevima za višefaktorskom autentifikacijom (eng. *MFA bombing*), kombinira tehnike socijalnog inženjeringa i hakiranja lozinke kako bi pokušao ukrasti naše vjerodajnice (Slika 9).

Slika 9: Bombardiranje zahtjevima za višefaktorskom autentifikacijom protiv Apple ID-a: preplavljivanje obavijestima + lažni poziv Appleove korisničke podrške



Izvor: Maldita.es

Napomena: Napad zloupotrebljava tijek resetiranja lozinke za Apple ID kako bi preplavio iPhone uputama, što otežava uporabu uređaja (zamor zahtjevima za višefaktorskom autentifikacijom, eng. MFA fatigue). Nakon nekoliko minuta prevaranti zovu korisnika s lažnim ID-om pozivatelja, oponašaju Appleovu korisničku podršku i traže kod za potvrdu „kako bi zaustavili napad". Ako ga žrtva podijeli, napadači preuzimaju račun, mijenjaju lozinku i pristupaju osjetljivim podacima.

3. Mrežni napadi: Presretanje podataka razmijenjenih između korisnika i internetskog servisa radi praćenja i krađe informacija.

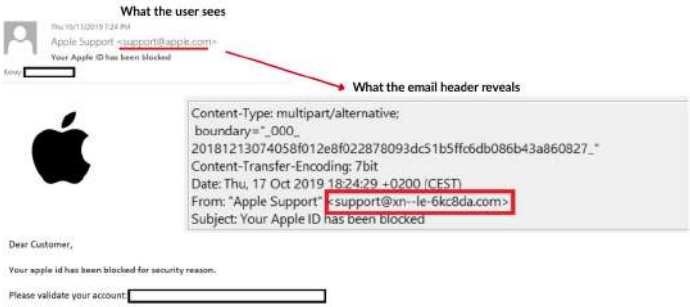
> **a. *Spoofing*:** Napad koji uključuje zlonamjernu upotrebu hakerskih tehnika za lažno predstavljanje identiteta korisnika.
>
> **I. *Spoofing* IP-a:** Falsificiranje IP adrese kako bi se prikazala kao drugačija.
> **II. *Spoofing* internetske stranice:** Izrada lažne internetske stranice koja oponaša legitimnu stranicu (Slika 10).
> **III. *Spoofing* e-pošte:** Lažiranje pouzdane adrese e-pošte radi obmanjivanja primatelja (Slike 10 i 11).

Slika 10: *Spoofing* internetske stranice i iznajmljivanje nekretnina ili rezervacije

Izvor: Maldita.es

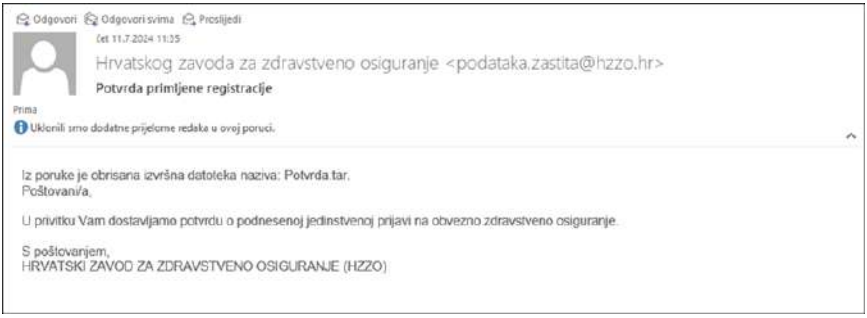
Napomena: Za više informacija pogledajte sliku **A12** u Dodatku.

Slika 11: Primjer spoofinga e-pošte. Lažna poruka Appleove korisničke podrške



Izvor: ***Kaspersky***

Napomena: Pošiljatelj se predstavlja kao „Appleova podrška" s uvjerljivim izgledom i identitetom robne marke, ali stvarna je adresa e-pošte lažna, osmišljena kako bi obmanula primatelje i potaknula nesigurne radnje. Dok klijent e-pošte prikazuje adresu *support@apple.com*, tehničko zaglavlje otkriva stvarno podrijetlo poruke: *support@xn--le-6kc8da.com*.



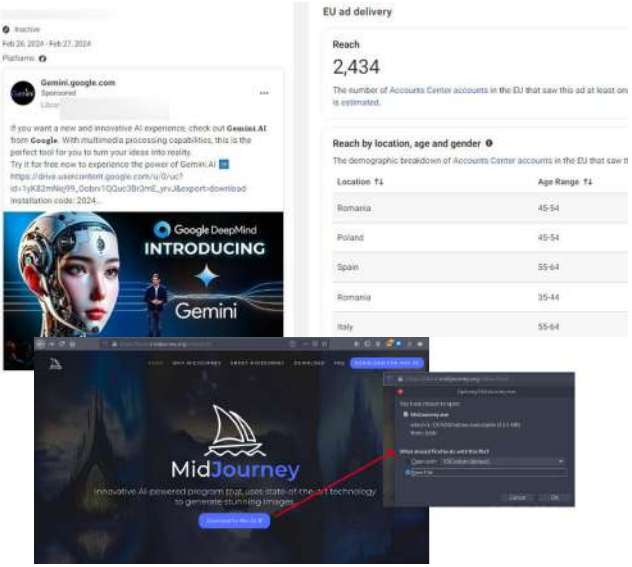
Izvor: Screenshot/HZZO

IV. DNS *Spoofing*: Manipuliranje legitimnom domenom (URL-om) kako bi se korisnika preusmjerilo na lažnu internetsku stranicu.

V. *Spoofing* SMS-om (vidi Dodatak: **A13**)
VI. *Spoofing* ID-a pozivatelja (vidi Dodatak: **A14**)

4. Napadi zlonamjernog softvera: Upotreba zlonamjernog softvera za izvođenje štetnih radnji, kao što su krađa podataka, preuzimanje kontrole nad sustavom ili nanošenje štete (Slika 12).

Slika 12: Lažni alat generativne umjetne inteligencije koji se upotrebljava za isporuku zlonamjernog softvera



Izvor: ***Maldita.es***

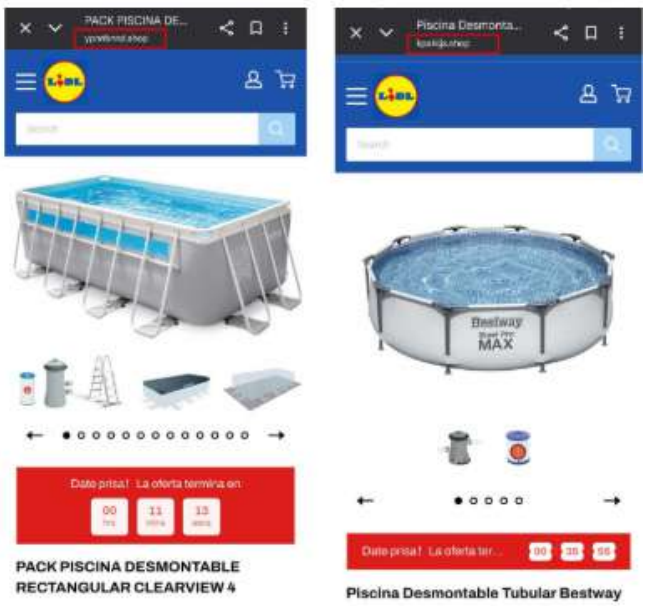
Napomena: Kibernetički kriminalci promiču besplatne alate generativne umjetne inteligencije na društvenim mrežama kako bi preusmjerili korisnike na lažne internetske stranice. Umjesto programa umjetne inteligencije, žrtve na svoja računala preuzimaju zlonamjerni softver koji napadačima omogućuje pristup povjerljivim informacijama kao što su lozinke ili bankovni podaci.

5. Ostali napadi.

TEMATSKA DIMENZIJA

1. Promocije ili ponude. Prevaranti predstavljaju vrlo atraktivnu lažnu ponudu, obično uz dodatak vremenskog roka unutar kojeg je se treba iskoristiti, tako pokušavajući nagnati primatelja da djeluje što je brže moguće (Slika 13).

Slika 13: *Phishing* i promocije ili ponude



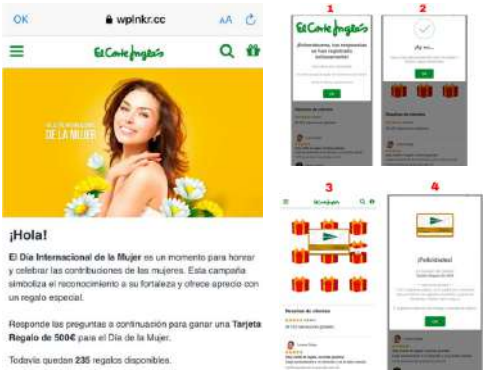
Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A1** u Dodatku.

Izvor: Screenshot/Facebook

2. Natjecanja, lutrije ili nagrade. Predstavljena je nagrada ili prilika za lutriju, a od ljudi se traži da daju svoje osobne podatke kako bi sudjelovali (Slika 14 i više primjera u Dodatku: **A7**).

Slika 14: *Phishing* i lažna natjecanja, lutrije ili nagrade



Izvor: Maldita.es

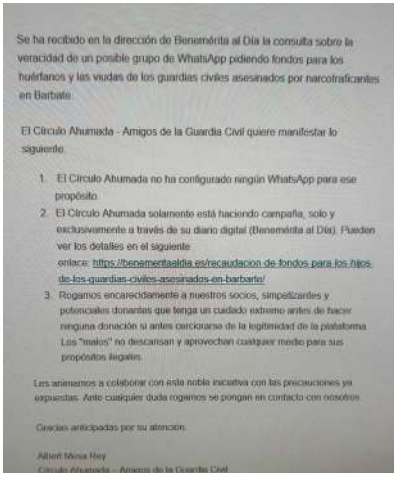
Napomena: Za više informacija pogledajte sliku **A3** u Dodatku.

Izvor: Screenshot

Izvor: Screenshot

3. Nasljedstvo, donacije ili lutrija. Prevaranti stupaju u kontakt s osobom kako bi ju obavijestili da ima pravo na veliku svotu novca i da je za isporuku potrebno samo ispuniti nekoliko dokumenata (Slika 15.)

Slika 15: *Phishing* i nasljedstvo, donacije ili lutrija



Se ha recibido en la dirección de Benemérita al Día la consulta sobre la veracidad de un posible grupo de WhatsApp pidiendo fondos para los huérfanos y las viudas de los guardias civiles asesinados por narcotraficantes en Barbate.

El Círculo Ahumada - Amigos de la Guardia Civil quiere manifestar lo siguiente:

1. El Círculo Ahumada no ha configurado ningún WhatsApp para ese propósito.
2. El Círculo Ahumada solamente está haciendo campaña, solo y exclusivamente a través de su diario digital (Benemérita al Día). Pueden ver los detalles en el siguiente enlace: https://benemeritaaldia.es/recaudacion-de-fondos-para-los-hijos-de-los-guardias-civiles-asesinados-en-barbate/
3. Rogamos encarecidamente a nuestros socios, simpatizantes y potenciales donantes que tenga un cuidado extremo antes de hacer ninguna donación si antes cerciorarse de la legitimidad de la plataforma. Los "malos" no descansan y aprovechan cualquier medio para sus propósitos ilegales.

Les animamos a colaborar con esta noble iniciativa con las precauciones ya expuestas. Ante cualquier duda rogamos se pongan en contacto con nosotros.

Gracias anticipadas por su atención.

Albert Mosa Rey
Círculo Ahumada - Amigos de la Guardia Civil

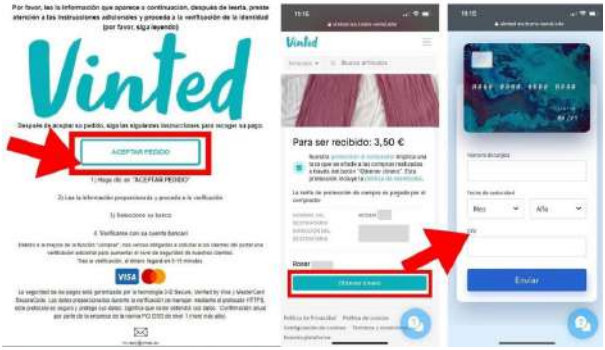
Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A2** u Dodatku.

4. Kupnja ili prodaja proizvoda i usluga (Slika 12). Prevaranti predstavljaju lažnu platformu za prodaju raznih proizvoda ili pružanje neke vrste usluga. Najčešći formati su:

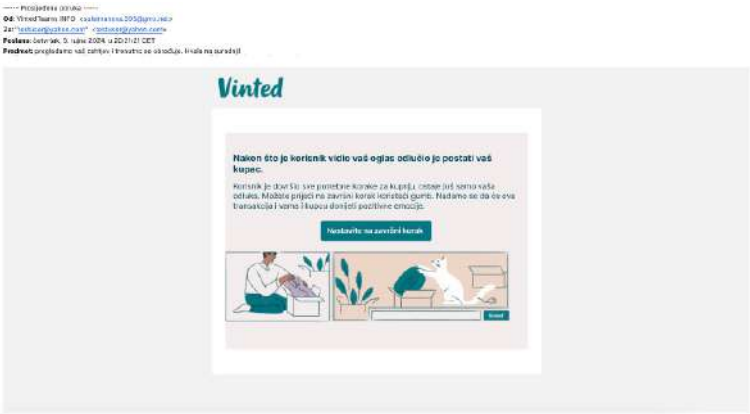
a. medicinski ili zdravstveni proizvodi
b. online trgovina
c. platforma za kupnju i prodaju (Slika 16)

Slika 16: Lažna internetska stranica Vinted koje se upotrebljava za krađu bankovnih podataka



Izvor: ***Maldita.es***

Napomena: Prevaranti su prodavačima poslali obmanjujuću e-poruku „Prihvati narudžbu" koja preusmjerava na lažnu internetsku stranicu „Vinted" koje oponaša njezin dizajn, ali se nalazi na lažnoj domeni.



Izvor: Screenshot/Vinted Hrvatska

Napomena: Primjer lažne Vinted e-mail poruke kako bi se došlo do podataka o kreditnim karticama kupca/korisnika.

5. Iznajmljivanje ili rezervacije. Simulacijom ponuda nekretnina prevaranti mogu ne samo prikupljati osobne podatke već i tražiti novac u obliku predujmova ili naknada za rezervaciju kuće ili stana (Slika 17).

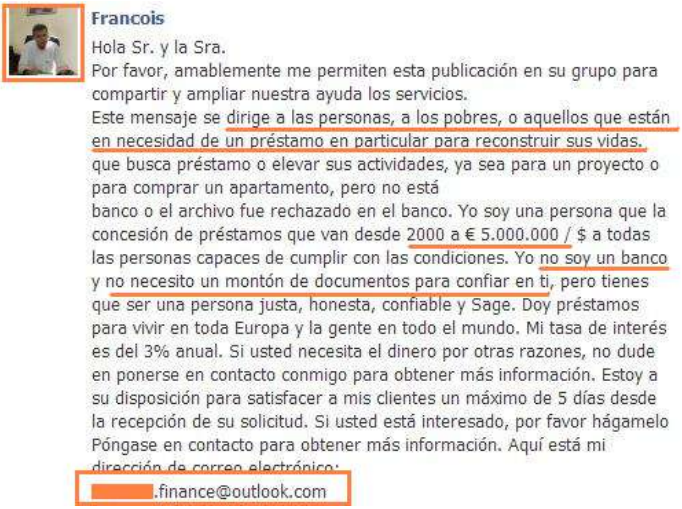
Slika 17: *Spoofing* internetske stranice i iznajmljivanje nekretnina ili rezervacije

Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A12** u Dodatku.

6. Zajmovi. Prevarant nudi navodne kredite pod vrlo povoljnim uvjetima, boljim od onoga što bi se moglo dobiti od banke (Slika 18).

Slika 18: *Catfishing* i zajmovi



Francois

Hola Sr. y la Sra.
Por favor, amablemente me permiten esta publicación en su grupo para compartir y ampliar nuestra ayuda los servicios.
Este mensaje se dirige a las personas, a los pobres, o aquellos que están en necesidad de un préstamo en particular para reconstruir sus vidas.
que busca préstamo o elevar sus actividades, ya sea para un proyecto o para comprar un apartamento, pero no está
banco o el archivo fue rechazado en el banco. Yo soy una persona que la concesión de préstamos que van desde 2000 a € 5.000.000 / $ a todas las personas capaces de cumplir con las condiciones. Yo no soy un banco y no necesito un montón de documentos para confiar en ti, pero tienes que ser una persona justa, honesta, confiable y Sage. Doy préstamos para vivir en toda Europa y la gente en todo el mundo. Mi tasa de interés es del 3% anual. Si usted necesita el dinero por otras razones, no dude en ponerse en contacto conmigo para obtener más información. Estoy a su disposición para satisfacer a mis clientes un máximo de 5 días desde la recepción de su solicitud. Si usted está interesado, por favor hágamelo Póngase en contacto para obtener más información. Aquí está mi dirección de correo electrónico:
[redacted].finance@outlook.com

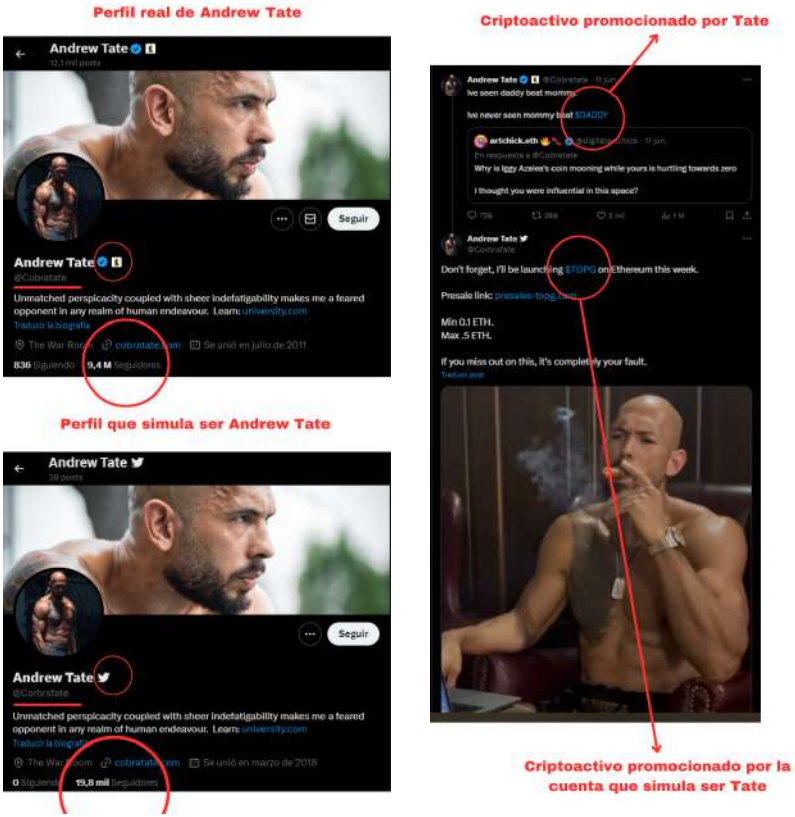
Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A15** u Dodatku.

Izvor: Screenshot/Facebook

7. Ulaganja. Predstavlja se investicija koja obećava vrlo visok povrat u kratkom vremenskom razdoblju. Česta je upotreba kriptovaluta kao mamca. (Slike 4, 6 i 19)

Slika 19: *Catfishing* i ulaganja



Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A10** u Dodatku.

Izvor: Screenshot/Facebook

8. Kockanje. Popularizacija *online* igara olakšava prevarantima da se predstavljaju kao kladioničarske tvrtke ili specijalizirane internetske stranice. (Slika 20)

Slika 20: *Catfishing* i kockanje

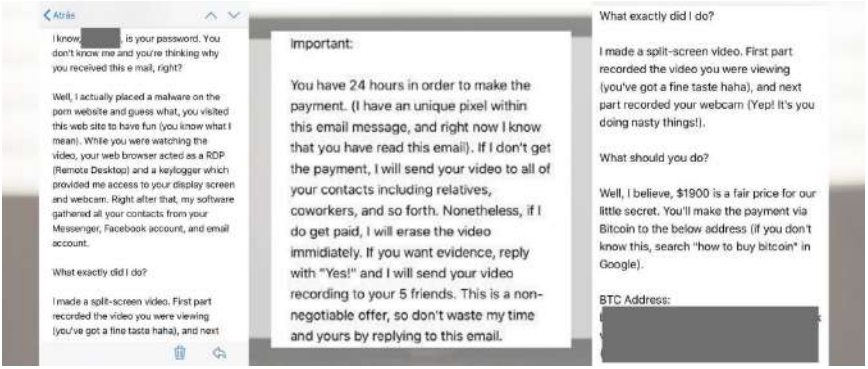
Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A16** u Dodatku.

Izvor: Screenshot/Facebook

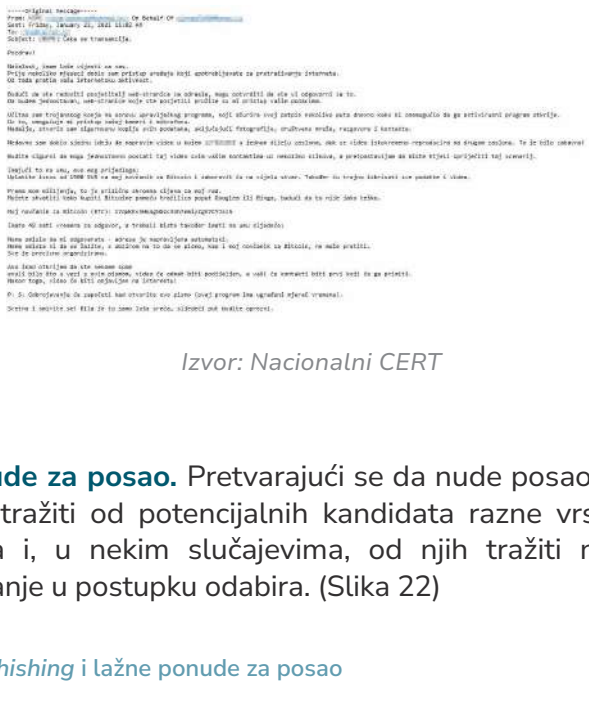
9. Prijetnje i iznude. Prevarant izravno prijeti žrtvi kako bi iznudio novac. Jedan od načina za to je prijetnja objavljivanjem kompromitirajućih seksualnih videozapisa ili slika. To je poznato kao *sextortion* (od engl. *extortion*, tj. iznuda) (Slika 21).

Slika 21: *Sextortion* prijevara putem e-pošte u kojoj se zahtijevaju plaćanja Bitcoinom.



Izvor: ***Maldita.es***

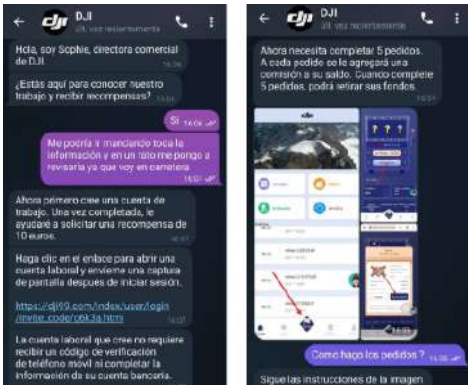
Napomena: Prevaranti putem e-pošte prijete korisnicima objavljivanjem navodnih intimnih videozapisa (koji zapravo ne postoje) osim ako se ne izvrši plaćanje Bitcoinom.



Izvor: Nacionalni CERT

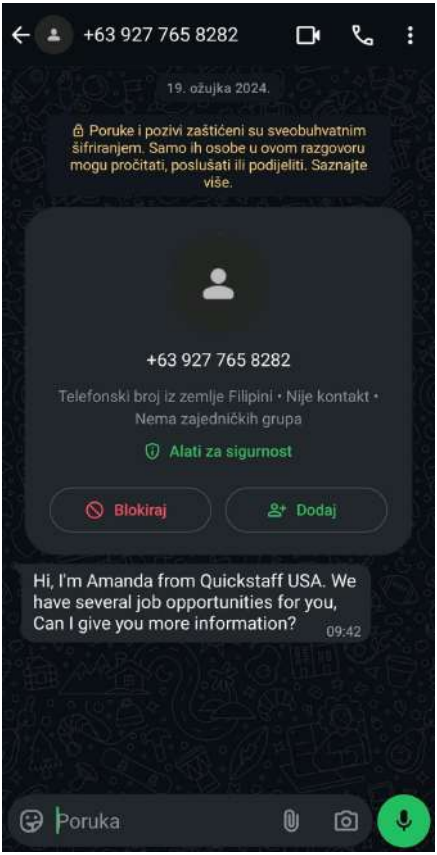
10. Ponude za posao. Pretvarajući se da nude posao, prevaranti mogu zatražiti od potencijalnih kandidata razne vrste osobnih podataka i, u nekim slučajevima, od njih tražiti naknadu za sudjelovanje u postupku odabira. (Slika 22)

Slika 22: *Phishing* i lažne ponude za posao



Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A4** u Dodatku.

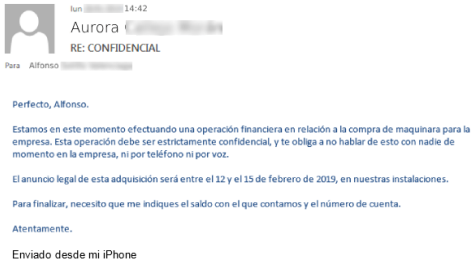


Izvor: Screenshot/Faktograf

11. Romantične veze. Prevaranti se predstavljaju kao netko tko se zaljubio u osobu koju pokušavaju prevariti. Upotrebljavaju lažne slike i pretvaraju se da im hitno treba novac (Slika 8)

12. Radno okruženje. Prevarant se predstavlja kao suradnik ili šef i iskorištava povjerenje ili hijerarhiju kako bi tražio informacije ili nešto drugo (Slika 23 i više primjera u Dodatku: **A18**)

Slika 23: *Phishing* i radno okruženje: Prijevara izvršnog direktora



lun [illegible] 14:42

Aurora [illegible]

RE: CONFIDENCIAL

Para Alfonso [illegible]

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinara para la empresa. Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

Enviado desde mi iPhone

Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A17** u Dodatku.

REPUBLIKA HRVATSKA
Ministarstvo pravosuđa i uprave

POLICIJA MUP

INTERPOL

OSOBA SAZVANA DOBROVOLJNO	IDENTITET KRIVCA	TIJEK POSTUPKA

Ja sam gospodin Nikola Milina, glavni ravnatelj policije i voditelj Cyber sigurnosti

U sklopu računalne krade u suradnji s Nacionalnim centrom za analizu dječje pornografije i kibernetičkih slika Republike Hrvatske (CNAIP) i Službom za analizu Međunarodne organizacije kriminalističke policije (INTERPOL) javit ću Vam se , da se protiv vas posebno vodi nekoliko valjanih pravnih postupaka:

_ Dječja pornografija
_ pedofilija
_ Egzibicionist
_ Cyber pornografija
_ Seks trgovina

Obavijestite nas tako što ćete nam poslati svoje popratne dokumente kako bismo ih mogli pregledati i provjeriti ima li kazni: unutar strogih 72 sata..

Po isteku ovog roka, dužni smo poslati svoje izvješće tužiteljici Republike Hrvatske koja vodi Vaš predmet, tužiteljici Branki Merzić, radi raspisivanja tjeralice za njim.

Na kraju ovog postupka bit ćete upisani u registar počinitelja seksualnih prijestupnika.
Vaš će slučaj također biti prosljeđen medijima u svrhe promidžbe kako bi se spriječilo ponavljanje prekršaja i kako bi se drugi odvratili od toga.

Bili ste upozoreni.

g. Nikola Milina
glavni policajac
Peakorter: Policija, Heinzelova ulica, Zagreb, Hrvatska

Izvor: Ravnateljstvo policije

13. Obavijesti od službe ili ustanove. Potencijalnoj žrtvi obraća se netko tko se pretvara da je pouzdana organizacija ili institucija, u pokušaju da od osobe dobije osobne podatke i novac (slike 1, 2, 7, 24 i više primjera u Prilogu: **A13**)

Slika 24: *Spoofing* ID-a pozivatelja i obavijesti od službe ili ustanove

Izvor: Maldita.es

Napomena: Za više informacija pogledajte sliku **A14** u Dodatku.

13. Ostale teme. Prevaranti prilagođavaju svoje poruke promjenjivim navikama i običajima vremena, kao i kulturnim karakteristikama svake regije, tako da se različite vrste tema mogu pojaviti u određeno vrijeme i na određenom mjestu.

Kategorije se međusobno ne isključuju; drugim riječima, neke prijevare mogu spadati u više od jedne kategorije temeljene na

tehnici i temi. Na primjer, telefonski poziv u kojem se prevaranti lažno predstavljaju kao banka, a istovremeno krivotvore njezin broj, treba kategorizirati i kao *vishing* i kao mrežni napad. Još je jedan dobar primjer **prijevara lažnom Microsoftovom tehničkom podrškom**, u kojoj kibernetički kriminalci zovu žrtve, tvrde da je njihovo računalo zaraženo (*vishing*) i na kraju pokušavaju instalirati zlonamjerni program za daljinsko upravljanje (zlonamjerni softver).

PRIMJENE

KORPORATIVNA I ORGANIZACIJSKA UPORABA

Tipologija se može integrirati u strategije zaštite robne marke i upravljanja rizicima. Primjerice:

- **Integracija u alate za praćenje:** Agencije za praćenje medija ili pružatelji usluga kibernetičke sigurnosti mogu mapirati izvješća o prijevarama prema tipologiji, omogućujući tvrtkama da vizualiziraju pomoću kojih se kategorija prijevara najčešće iskorištava njihova robna marka. To olakšava određivanje prioriteta (na primjer, ako prevladavaju *phishing* i lažne nagradne igre, resursi se mogu dodijeliti tim područjima).

- **Interna obuka:** Tipologija se može prevesti u module obuke za osoblje, omogućujući, na primjer, timovima za korisničku podršku da prepoznaju obrasce prijevare i usmjeravaju kupce koji prijavljuju sumnjive kontakte.

- **Odgovor na krizu:** Kada se pojavi nova prijevara, tvrtke je mogu brzo klasificirati prema tipologiji, povezati s prethodnim slučajevima i generirati unaprijed izrađena upozorenja za korisnike. Time se skraćuje vrijeme reakcije i osigurava dosljednost u komunikaciji.

JAVNI SEKTOR I REGULATORNA UPORABA

Ovom se tipologijom standardizira jezik izvještavanja i analize za regulatorna i nadzorna tijela. Među mogućim primjenama možemo izdvojiti:

- **Baze podataka o incidentima:** Izvješća o prijevarama mogu se sustavno kodirati pomoću tipologije, omogućujući usporedbu podataka među agencijama i tijekom vremena.

- **Međusektorska i transnacionalna suradnja:** Zajednička tipologija omogućuje institucijama iz različitih zemalja usklađivanje terminologije i razmjenu korisnih informacija koje se mogu lako usporediti.

- **Praćenje trendova:** Regulatorna tijela mogu pratiti koje kategorije prijevara postaju sve raširenije i koristiti ove informacije za izdavanje javnih upozorenja ili poduzimanje prisilnih/inhibicijskih mjera.

PRIMJENA U EDUKACIJI I ZA GRAĐANSTVO

Tipologija ima snažan pedagoški potencijal:

- **Pismenost za stručnjake:** Novinari, nastavnici i drugi dionici mogu se koristiti tipologijom kao referencom za točno izvješćivanje i podučavanje o dinamici prijevara.

- **Kampanje podizanja svijesti:** Javne institucije i organizacije civilnog društva mogu osmisliti kampanje oko određenih kategorija prijevara („romantične prijevare", „lutrijske prijevare"), pokazujući građanima stvarne primjere iz tipologije.

- **Tijek provjere za građane** Tipologija se može prilagoditi tijeku provjere koji vodi korisnike kroz proces utvrđivanja jesu li suočeni s prijevarom: Uključuje li poruka hitne zahtjeve? Traži li predujam? Predstavlja li se kontakt kao javna ustanova? Svako kritičko pitanje moglo bi izravno odgovarati kategoriji prijevare, služeći kao referentni okvir za pomoć korisnicima u donošenju informiranih odluka.

PREPORUKE

Preporuke su strateški prilagođene karakteristikama i potrebama ciljne publike, osiguravajući da aplikacije budu lakše za implementaciju, jednostavnije za upotrebu i u konačnici učinkovitije.

ZA TVRTKE

• **Interna obuka.** Razvijte kontinuirane programe obuke o kibernetičkoj sigurnosti za zaposlenike koje vode organizacije stručne u temama prijevara i financijske pismenosti, ojačane redovitim vježbama za prepoznavanje *phishinga* i socijalnog inženjeringa. Preporučljivo je upotrebljavati javno dostupne nacionalne i europske resurse (smjernice, programe obuke i digitalne alate) za poticanje kulture kibernetičke sigurnosti unutar organizacije.

• **Protokoli zaštite i sigurnosti.** Provedite napredne tehničke mjere (višefaktorska autentifikacija, filtriranje e-pošte, praćenje pristupa, šifriranje osjetljivih podataka) i uspostavite službene kanale komunikacije s klijentima i dobavljačima kako bi se smanjio rizik od lažnog predstavljanja.

• **Usklađenost s propisima i kibernetička otpornost.** Osigurajte usklađenost s europskim propisima o kibernetičkoj sigurnosti (NIS2, DORA, Akt o kibernetičkoj otpornosti, između ostalog) kao dio korporativne strategije. Osim toga, promičite kibernetičku otpornost, definiranu kao sposobnost jamčenja operativnog kontinuiteta u slučaju incidenata.

• **Suradnja i rano upozoravanje.** Održavajte izravni kontakt sa specijaliziranim organizacijama radi primanja ažuriranih informacija o pokušajima prijevare i predviđanja novih obrazaca i prijetnji.

• **Društvena odgovornost i transparentnost.** Preuzmite korporativnu odgovornost za zaštitu građana od kibernetičkih

rizika osiguravanjem transparentnog izvješćivanja o incidentima i širenjem preventivnih upozorenja. Ova praksa doprinosi suzbijanju širenja kibernetičkih prijevara i jačanju povjerenja u robnu marku. Može se uključiti kao dio odgovorne komunikacije tvrtke sa svojim klijentima, jačajući povjerenje i pokazujući predanost transparentnosti i odgovornosti.

ZA GRAĐANE

• **Kritički stav i provjera.** Budite oprezni s porukama koje pozivaju na hitno djelovanje ili koje obećavaju značajne popuste ili pogodnosti i uvijek provjeravajte autentičnost adresa e-pošte, URL-ova i profila na društvenim mrežama. Naučite prepoznati situacije kada poruka pokrene snažnu emocionalnu reakciju -bilo da je riječ o uznemirenosti ili uzbuđenju. Razvijanje svijesti o tome pomaže u sprječavanju impulzivnih reakcija i potiče poduzimanje potrebnih koraka za provjeru informacija prije djelovanja. Važno je uključiti praksu provođenja vlastitog istraživanja kao standardnu naviku i osigurati da ona postane integrirani i prirodni dio procesa.

• **Obratite se specijaliziranim organizacijama.** Ako sumnjate da bi nešto moglo biti pokušaj prijevare, obratite se organizacijama specijaliziranim za otkrivanje prijevara. Ne samo da će vam njihovi stručnjaci pomoći da razjasnite svoje sumnje, već će, ako se doista radi o pokušaju prijevare, vaše upozorenje pomoći da se upozore drugi građani. Slijedite savjete tih organizacija kako biste poboljšali svoju sposobnost otkrivanja mogućih prijevara.

• **Prijavljivanje i suradnja.** Prijavite pokušaje prijevare pogođenim platformama putem njihovih namjenskih kanala za označavanje nezakonitog sadržaja. Također podijelite takve informacije s obitelji i kontaktima jer ćete tako pomoći razbiti lanac obmane. Vođenje otvorenih razgovora o tim pitanjima može pomoći u sprečavanju potencijalnih rizika i osigurati uspostavu jasnih komunikacijskih kanala, omogućujući pravovremeno prijavljivanje problema i učinkovit odgovor na njih.

• **Osobna zaštita i prevencija.** Upotrebljavajte snažne lozinke, omogućite višefaktorsku autentifikaciju, ažurirajte softver i pratite pouzdane izvore kako biste bili informirani o novim vrstama prijevara.

ZA NADLEŽNA TIJELA

• **Edukativne kampanje.** Dijelite jasne i redovite poruke o novim vrstama kibernetičkih prijevara putem tradicionalnih i digitalnih medija. Osigurajte da kampanje budu ažurirane i da budu u toku s novim trendovima i tehnikama.

• **Provođenje zakona.** Primjenjujte postojeće propise (tj. Akt EU-a o digitalnim uslugama) o nezakonitom internetskom sadržaju, što uključuje prijevare, kako bi se osiguralo da platforme ispunjavaju svoje obveze u pogledu uklanjanja i ublažavanja tog rizika.

• **Učinkoviti kanali za prijavljivanje.** Građanima i tvrtkama pojednostavnite postupke za prijavu internetskih prijevara. Osigurajte učinkovite komunikacijske kanale koji su prilagođeni korisniku i koji građane mogu usmjeriti na odgovarajuće usluge. Ovaj pristup povećava pristupačnost, poboljšava pružanje usluga i jača povjerenje između organizacije i njezinih dionika.

• **Međunarodna suradnja.** Ojačajte mreže za razmjenu policijskih i pravosudnih informacija, s obzirom na to da mnoge internetske prijevare nisu ograničene na određenu državu.

• **Transparentnost podataka.** Objavljujte redovita izvješća sa statističkim podacima i primjerima otkrivenih prijevara. U izvješća uključite specifične praktične i preventivne preporuke. Osim toga, uvedite strategiju usmjerenu na učinke kako bi se osiguralo da su nalazi i zaključci praktični, što će učinkovito usmjeravati donošenje odluka i poboljšati ukupnu učinkovitost izvješća.

ZA INTERNETSKE USLUGE

• **Usklađenost sa zakonom.** Djelujte u skladu s postojećim zakonom (tj. Aktom o digitalnim uslugama) kako biste suzbili nezakoniti sadržaj na internetu, što uključuje uspostavljanje kanala za prijavu i reagiranje na prijave, kao i, za vrlo velike usluge, procjenu i ublažavanje rizika od iskorištavanja platformi za nezakonite kampanje prijevare.

• **Bolja detekcija.** Kontinuirano ažurirajte metode detekcije kako biste spriječili širenje ove vrste sadržaja na internetskim uslugama, vodeći računa o ograničenjima automatiziranog skeniranja.

• **Suradnja.** Njegujte blisku suradnju sa specijaliziranim organizacijama i vlastima u svrhu razmjene znanja o novim obrascima i taktikama radi bolje zaštite korisnika.

ZA ORGANIZACIJE ZA PROVJERU ČINJENICA

• **Sustavno praćenje.** Pratite ponavljajuće narative i taktike koje se upotrebljavaju u internetskim kampanjama prijevara kako biste prepoznali njihove varijacije. Deaktivacija narativa traje duže, ali nam omogućuje da razumijemo logiku i strategiju koja stoji iza prijevare i spriječimo moguće varijacije istog obrasca ponašanja.

• **Partnerstva s platformama.** Uspostavite održive sustave suradnje koji omogućuju brže otkrivanje i uklanjanje lažnih oglasa ili objava te upotrijebite postojeće kanale za uklanjanje. Imajte protokole za aktivno prijavljivanje lažnog sadržaja na platformi i jasno komunicirajte o njemu putem sigurnih kanala, proširujući postojeći sadržaj za prepoznavanje lažnih informacija.

• **Pristupačan jezik.** Izradite jasne, vizualne i lako dijeljive materijale za razotkrivanje prijevara, prilagođene različitim razinama digitalne pismenosti. Osigurajte da ti materijali budu dostupni na kanalima koje upotrebljavaju ciljani primatelji prijevara.

• **Procjena učinka.** Izmjerite doseg izdanih upozorenja kako biste poboljšali učinkovitost preventivne komunikacije.

• **Komunikacija s ključnim dionicima.** Uspostavite otvorene komunikacijske kanale za upozoravanje pogođenih tvrtki i nadležnih tijela o otkrivenim kampanjama prijevare.

ZAKLJUČCI

Brz razvoj digitalnih prijevara, potaknut izumima poput generativne umjetne inteligencije, zahtijeva uspostavu okvira koji pružaju jasnoću i dosljednost u klasifikaciji. Ovdje predstavljena tipologija služi kao odgovor na tu potrebu, nudeći pomno odabran vokabular i praktičnu kategorizaciju koji mogu podržati prevenciju, podizanje svijesti i koordinirane reakcije u svim sektorima.

Koordinacija među različitim akterima koji se bore protiv digitalnih prijevara ključna je za minimiziranje njihovih učinaka. Učinkovita kategorizacija različitih vrsta prijevara osnovni je korak za poboljšanje učinkovitosti mjera koje se poduzimaju protiv njih. Ovdje predložena tipologija obuhvaća gotovo sve obmane i prijevare koje trenutačno kruže društvenim mrežama.

Iako je nedavna pojava alata umjetne inteligencije potaknula daljnji razvoj ove vrste prijevarnih praksi, ta nova tehnologija do sada nije donijela nikakve inovacije u smislu tehnika ili tema obmane. Prevaranti su počeli upotrebljavati umjetnu inteligenciju kako bi poboljšali, sistematizirali i proširili utjecaj prijevara koje su već upotrebljavali, ali se nisu pojavile prijevare temeljene na umjetnoj inteligenciji nove generacije. Stoga, iako se krajolik digitalnih prijevara mijenja, smatramo da je tipologija koju predlažemo potpuno aktualna i korisna za praćenje i analizu pokušaja internetskih prijevara.

Pojava umjetne inteligencije primjer je prilagođavanja prevaranata tehnološkom napretku kako bi ažurirali svoje pokušaje prijevare. Zato je važno da nadležna tijela i tvrtke preuzmu odgovornost za ostajanje na oprezu od takvih pojava i za implementaciju potrebnih alata kako bi zaštitili građane i spriječili ih da postanu žrtve prijevara.

No, također je važno usredotočiti se na građane koji postaju

žrtve prijevara. Medijska i financijska pismenost nezaobilazan je alat uz koji ljudi postaju otporniji na obmane i sposobniji otkriti potencijalne pokušaje prijevare. Ove programe obuke također treba redovito obnavljati i ažurirati kako bi bili što učinkovitiji u okruženju toliko obilježenom brzim promjenama kao što je područje internetskih prijevara.

Suradnja između organizacija specijaliziranih za otkrivanje prijevara još je jedno područje koje treba aktivno jačati. Zajednički napori pružaju šire razumijevanje aktivnosti prevaranata, olakšavaju otkrivanje međunarodnih prijevara i omogućuju razmjenu iskustava u borbi protiv tih kriminalnih praksi. Značajan je primjer prednosti suradnje **istraga koju vodi *Maldita.es*** o mreži Facebook stranica koje se lažno predstavljaju kao usluge javnog prijevoza. Više od deset organizacija za provjeru činjenica iz različitih zemalja, uključujući *Faktograf*, sudjelovalo je u istrazi koja je otkrila više od 1000 lažnih stranica koje su pokušavale prevariti građane u 60 zemalja.

Bitno je održavati i jačati ovu vrstu kolektivnog i suradničkog rada kako bi različite organizacije u ovom području mogle dijeliti svoja područja stručnosti. Na primjer, postojeće strukture kao što je Europska mreža organizacija za provjeravanje činjenica (EFCSN) mogle bi se upotrebljavati za provođenje ankete o najzastupljenijim vrstama prijevara u svakoj zemlji, čime bi se omogućili učinkovitiji i ciljani odgovori.

Istovremeno, moraju se prepoznati određena ograničenja. Složene sheme prijevara koje kombiniraju napredne tehničke komponente sa socijalnim inženjeringom možda nisu u potpunosti obuhvaćene jednom kategorijom. Nadalje, činjenica da je klasifikacija prvenstveno usredotočena na tehnike socijalnog inženjeringa mogla bi podrazumijevati izostavljanje široko korištenih pojmova

kibernetičke sigurnosti. Međutim, dizajn s više oznaka na kojem se tipologija temelji osigurava fleksibilnost, omogućujući analitičarima da klasificiraju prijevare u više dimenzija kada je to potrebno. I dok davanje prioriteta napadima socijalnog inženjeringa predstavlja ograničenje u smislu pokrivenosti, njegova je dobra strana povećanje operativnosti i koherentnosti.

Tipologiju stoga ne treba smatrati statičkim ili iscrpnim modelom, već fleksibilnim, prilagodljivim i praktičnim alatom. Njezino usvajanje može poboljšati rano otkrivanje obrazaca prijevara, poboljšati strategije odgovora na krize i prevencije, pomoći u izbjegavanju financijskih gubitaka i narušavanja ugleda, može se upotrebljavati za promicanje pismenosti na terenu i izvana i iznutra te olakšati usvajanje odabranog vokabulara.

REFERENCE

[1] FBI's Internet Crime Complaint Center. (2025.). *Internet Crime Report 2024.* **https://tinyurl.com/bjx965ab**

[2] Global Anti-Scam Alliance (GASA). (2024.). *Global State of Scams Report 2024.* **https://tinyurl.com/5yefneky**

[3] World Economic Forum (WEF). (2025., siječanj). *Global Cybersecurity Outlook 2025. Insight Report.* **https://tinyurl.com/ycyjwk7b**

[4] Europol. (18. travnja 2024.). International investigation disrupts phishing-as-a-service platform LabHost. **https://tinyurl.com/5fmmwhx4**

[5] United Nations Office on Drugs and Crime. (2023., rujan). Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. **https://tinyurl.com/y6fjvw3d**

[6] Internet Organised Crime Threat Assessment (IOCTA). (2025.). *Steal, deal and repeat: How cybercriminals trade and exploit your data.* **https://tinyurl.com/48nfcc48**

[7] Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024.). Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects. arXiv preprint arXiv:2412.00586. **https://doi.org/10.48550/arXiv.2412.00586**

[8] Verizon. (2025.). *2025 Data Breach Investigations Report.* **https://www.verizon.com/business/resources/Tbf6/reports/2025-dbir-data-breach-investigations-report.pdf**

[9] Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025.). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, 62(1), 103928.
https://doi.org/10.1016/j.ipm.2024.103928

[10] Kävrestad, J., & Nohlberg, M. (2018., rujan). Defining and Modelling the Online Fraud Process. U HAISA-i (str. 203-213).

[11] Europol. (2023.). E*uropol Spotlight - Online Fraud Schemes: A Web Of Deceit.* **https://tinyurl.com/mea6ux7h**

[12] **Maldita.es**. (1. studenog 2024.). Cuidado con los supuestos voluntarios de la Cruz Roja que piden dinero por la DANA: el Ayuntamiento de Sueca dice que es una "estafa".
https://tinyurl.com/2xh9r3u5

[13] Instituto Nacional de Ciberseguridad (INCIBE). (2020.). *Guía de ciberataques: Todo lo que debes saber a nivel usuario.*
https://tinyurl.com/3877ryme

[14] Instituto Nacional de Ciberseguridad (INCIBE). (2024.). Balance de ciberseguridad 2022. **https://tinyurl.com/4fmrbwc9**

[15] Instituto Nacional de Ciberseguridad (INCIBE). (2022.). Balance de ciberseguridad 2022. **https://tinyurl.com/bdfdvd7n**

[16] Ministerio del Interior. (2023.). *Informe sobre la cibercriminalidad en España 2023.* Dirección General de Coordinación y Estudios, Secretaría de Estado de Seguridad.
https://tinyurl.com/42fv3h3a

[17] Ministerio del Interior. (2022.). *Informe sobre la cibercriminalidad en España 2022.* Dirección General de Coordinación y Estudios, Secretaría de Estado de Seguridad. **https://tinyurl.com/mtturvn7**

[18] Arroyo, D., Gayoso, V., and Hernández, L. (2020). *¿Qué sabemos de? Ciberseguridad.* Editorial CSIC.

[19] INCIBE-CERT. (2020.). *Guía nacional de notificación y gestión de ciberincidentes.* **https://tinyurl.com/yfxu9def**

[20] Guardia Civil. (n.d.). *Consejos de seguridad para no ser víctima de estafa.* **https://web.guardiacivil.es/es/colaboracion/consejos/estafa/index.html**

[21] Kaspersky. (n.d). *¿Qué es el cibercrimen? Cómo protegerte.* **https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime**

[22] Panda Mediacenter. (22. ožujka 2023.). *Tipos de cibercrimen.* **https://www.pandasecurity.com/es/mediacenter/tipos-de-cibercrimen/**

[23] Cano Teruel, Q. (4. prosinca 2020.). *Ciberdelincuencia en el Código Penal.* Cibercrim. **https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/**

[24] e-Legales. (n.d.). *Clasificación de los ciberdelitos según la víctima.* e-Legales. **https://tinyurl.com/33hv59nv**

[25] European Union Agency for Network and Information Security (ENISA). (2018.). *Reference Incident Classification Taxonomy.* Task Force Status and Way Forward. **https://tinyurl.com/4fsp2uk3**

[26] Feature Space. (2023.). SCAMS. L*a guía completa. Identificación y prevención de fraude autorizado de tarjetas y pagos.* **https://tinyurl.com/4fp6k48f**

[27] F-Secure. (s.f.). *Scam Taxonomy.* **https://www.f-secure.com/en/partners/scam-protection/scam-taxonomy**

[28] Instituto Nacional de Ciberseguridad (INCIBE). (2021.). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario.* **https://tinyurl.com/mrrfp4wv**

[29] Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). *Taxonomía*. INCIBE-CERT. **https://tinyurl.com/ynuprzvh**

[30] Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). *Ciudadanía*. **https://www.incibe.es/ciudadania**

[31] Mestre Delgado, E. (16. lipnja 2023.). *Delitos en internet: ciberestafas*. Abogacía Española. **https://tinyurl.com/yfyah5cp**

[32] Observatorio Español de Delitos Informáticos (OEDI). (n.d.). *Ciberdelitos*. **https://oedi.es/ciberdelitos/**

www.faktograf.hr

Projekt “Razotkrivanje prevara: odgovor poslovnog sektora i građana” provodi se zahvaljujući Fondu za građanske inovacije (CIF), jedinstvenom europskom zajedničkom fondu organizacije THE CIVICS Innovation Hub. Zaklada ERSTE podržava CIF.