# Európska sieť na predchádzanie trestnej činnosti

# Súbor nástrojov EUCPN, séria

# č. 13

# Prevencia podvodov na osobách

## Zhrnutie

Trinásty súbor nástrojov v sérii publikovanej sekretariátom Európskej siete na predchádzanie trestnej činnosti (EUCPN) sa zameriava na prevenciu *podvodov na osobách*. Bulharské predsedníctvo (v prvom polroku 2018) sa rozhodlo zamerať na:

„[…] *problémy súvisiace s podvodmi, najmä telefonické podvody. Tento druh trestného činu sa v posledných rokoch stal výnosnou trestnou činnosťou, ktorá sa vyvíja na vnútroštátnej aj cezhraničnej úrovni. Zločinecké skupiny, ktoré sa špecializujú na túto činnosť, sa vyvíjajú dynamicky a napádajú širší okruh obetí. Vzhľadom na aktívnu účasť obetí, ich zapojenie do zločineckých scenárov a traumatizujúci vplyv na ich mysle je potrebné vynaložiť intenzívne úsilie na prevenciu tejto činnosti a zároveň zohľadniť osobitosti na miestnej, vnútroštátnej a cezhraničnej úrovni.“*

Podvody na osobách sú typ podvodov, pri ktorých sa zločinci zameriavajú na jednotlivých bežných občanov. Obete presvedčia, aby s nimi spolupracovali a následne ich podvedú. Naše súčasné chápanie tohto typu podvodu je späté najmä s jeho súčasnými podobami, kde je najpravdepodobnejším príkladom phishing. Je však dôležité uvedomiť si, že podvody na osobách existujú od nepamäti. Technologický vývoj v posledných desaťročiach sa zaslúžil o industrializáciu týchto podvodov vo väčšom rozsahu, než sa vôbec považovalo za možné. Kto ešte nedostal phishingový e-mail?

Ako je zrejmé z *odôvodnenia* bulharského predsedníctva, obete sa aktívne podieľajú na svojej viktimizácii. Páchateľ sa zameria na peniaze obete, avšak dostať sa k nim môže len presvedčením obete, aby mu prístup udelila. Nevyhnutnou taktikou, ktorá má obeť dotlačiť do

tohto poddajnému vzťahu, sa nazýva **sociálne inžinierstvo**. Páchateľovi umožňuje získať si dôveru obete, ktorá je rozhodujúca pre úspešnosť podvodu. Sociálna psychológia nám umožňuje lepšie porozumieť tomuto fenoménu. Odvolávaním sa na každodenné sociálne zásady a využívaním „ľudskej slabosti“ sú páchatelia schopní aktivovať takzvaný druhý spôsob presviedčania. Prvý spôsob si vyžaduje veľa premýšľania a kognitívneho úsilia. Druhý si však nevyžaduje skutočnú prípravu a reakcia je takmer podvedomá. Páchatelia napríklad dokážu ľahko primäť svoje obete, aby ich poslúchali tým, že predstierajú, že sú osobou v zodpovednom postavení, napríklad policajtom. Tieto sociálne a kognitívne pravidlá sa každodenne používajú, no páchateľom umožňujú využívať ich vo svoj prospech.

Tieto podvodné taktiky sa používajú v širokej **škále podvodov**, *ako sú nigérijské podvody, podvody na seniorov, romantické podvody, CEO podvody a mnohé ďalšie,* možnosti sú nekonečné, rovnako ako kreativita podvodníkov. Táto škála podvodných schém umožňuje podvodníkom zamerať sa na rozsiahlu verejnosť naraz alebo sa naopak sústrediť na jednotlivca. Zdá sa, že druhá možnosť sa vyskytuje čoraz častejšie. Podvodníci si uvedomili, že šikovné zacielenie obetí povedie k vyššej „návratnosti investícií“. Phishingové e-maily sa stávajú čoraz sofistikovanejšie a odosielajú sa konkrétnemu cieľu (skupine). Prekvapujúcim posledným krokom v tomto vývoji je kombinácia novej a staršej technológie: použitie telefónu. Vishing (telefonická obdoba phishingu) poskytuje podvodníkom príležitosť kombinovať výhody internetu aj telefónu. Uskutočnenie online telefonického hovoru je takmer bez nákladov, je ťažšie ho vystopovať a dá sa automatizovať. Používanie telefónu má ďalšie výhody: ľudia telefonátom viac dôverujú a vďaka intímnejšiemu prostrediu je možné obete efektívnejšie presvedčiť. Príkladom rastúcej úrovne sofistikovanosti je situácia, kedy si páchatelia dokonca najímajú rodených hovorcov, aby telefonáty zneli čo najprirodzenejšie.

Naše súčasné chápanie podvodov na osobách je však obmedzené. Tento zločin sprevádza vysoké **temné číslo kriminality**, keďže veľký počet prípadov ostáva nenahlásených. Obete si neuvedomujú, že sa stali obeťami, nepovažujú skutok za dostatočne závažný, myslia si, že nahlásenie trestného činu k ničomu nepovedie alebo jednoducho nevedia, kde majú trestný čin nahlásiť. Okrem toho obetiam bráni v rozpovedaní ich príbehu pocit sebaobviňovania a rozpaky, nakoľko pri ich viktimizácii zohrávali aktívnu úlohu aj ony samy. Niektoré podvody majú dokonca „zabudované“ mechanizmy na zabránenie nahlasovaniu trestného činu, pretože obete museli v rámci schémy podniknúť nezákonné kroky, čím by v procese nahlásenia trestného činu usvedčili aj samy seba. Ak by podvod nahlásili, cítili by sa, akoby sa k skutku samy priznali.

Toto temné číslo tiež vyvolalo **fámu,** že seniori sú hlavnými obeťami tohto trestného činu, pretože sú ľahkou korisťou. Niektoré štúdie tento mýtus vyvrátili, aj keď by sme mali zachovať obozretnosť z dôvodu obmedzeného dostupného výskumu. Napriek tomu sa uvádza, že mladšia generácia a stredná veková skupina sú náchylnejšie na podvody. Ďalší mýtus hovorí, že obete sú zvyčajne vykreslené ako nevzdelané či finančne negramotné, opak sa však zdá byť pravdou. Jedno možné vysvetlenie sa nazýva „bariéra medzi teóriou a praxou“, kde ľudia dokážu rozoznať znaky podvodov, no tieto znalosti nedokážu uplatniť vo svojej vlastnej situácii.

Bohužiaľ, existencia takzvaných „**zoznamov podvedených osôb**“ nie je mýtus. Telefónni podvodníci môžu svoje obete kontaktovať náhodne alebo ich vyhľadať vo verejných registroch, no medzi sebou zdieľajú aj zoznamy s osobami, ktoré už boli podvedené. Používanie takýchto zoznamov svedčí o vysokej úrovni opakovanej viktimizácie. Niektorí podvodníci sa napríklad pokúsia obetiam „pomôcť“ získať späť stratený majetok.

Keďže sankcionovanie tohto trestného činu je nesmierne zložité, je nevyhnutná jeho prevencia. V súvislosti s podvodmi na osobách sa však uskutočnilo málo akademických a hodnotiacich výskumov. Môžeme však konštatovať niektoré všeobecné zistenia. Najbežnejšou preventívnou metódou je vzdelávanie verejnosti. Môže sa uskutočniť v rámci kampane na všeobecné zvyšovania povedomia, no pozitívny vplyv sa zaznamenal najmä v prípadoch, kedy sa zvyšovanie povedomia realizovalo v určitom školiacom formáte. V podstate sa tieto školenia snažia odstrániť spomenutú bariéru medzi „teóriou a praxou“. Ďalšou kľúčovou metódou je práca s obeťami. Z dôvodu ich aktívnej roly a rizika, že sa stanú obeťami viackrát, je potrebné, aby boli obete podporované a informované o ich konkrétnej situácii.

Počas bulharského predsedníctva zhromaždil sekretariát niekoľko **osvedčených postupov** v tejto problematike. Možno ich kategorizovať podľa ich cieľovej skupiny. Prvá kategória sa zameriava na celú populáciu. Sú to kampane na zvyšovanie povedomia, ako napríklad kampane Bulharska, Švédska, Belgicka alebo Europolu. Ide o rozhlasové spoty, plagáty, letáky, informačné predmety atď., ktoré poskytujú verejnosti užitočné informácie a ukazujú, ako sa chrániť pred podvodmi. Druhý súbor aktivít je zameraný na seniorov. Pre nich sa zavádzajú interaktívnejšie metódy, ako je to v Českej republike. Seniori sa zúčastňujú interaktívnej vzdelávacej divadelnej hry, kde sa dozvedia o najbežnejších podvodných schémach a spôsoboch, ako na ne reagovať. Táto „prežitá skúsenosť“ by im mala umožniť

primerane reagovať v skutočnom živote. Vyhodnotenie tohto projektu ukázalo, že tento predpoklad je pravdivý, pretože táto skupina odmietla podvodné návrhy dvaapolkrát viac než kontrolná skupina, ktorá sa hry nezúčastnila. Posledná kategória preventívnych aktivít sa zamerala na obete. Príklady z Austrálie, Spojeného kráľovstva a Kanady ukázali, že tento typ prevencie je potrebný. Aj na celosvetovej úrovni však existuje málo podporných služieb pre obete podvodov na osobách.

Nakoniec sekretariát EUCPN zorganizoval seminár s rôznymi odborníkmi s cieľom vypracovať niekoľko **odporúčaní** o spôsoboch prevencie telefonických podvodov. Sú štruktúrované podľa piatich stratégií prevencie situačnej trestnej činnosti. Prvou možnou stratégiou je zvýšenie úsilia, ktoré musí páchateľ vynaložiť, aby bol jeho podvod úspešný. V súčasnosti sa to už dá docieliť obmedzením uverejňovania a prístupu k telefónnym číslam. Ďalšou metódou môže byť obmedzenie počtu telefónnych čísiel, ktorými môže jedna osoba disponovať, alebo aspoň prepojenie telefónneho čísla s bankovým účtom alebo identifikačným číslom.

Druhou stratégiou je zvýšenie rizika. Pri tejto stratégii hrá zdieľanie informácií kľúčovú rolu. Toto zdieľanie by sa nemalo zastaviť na hranici verejného či súkromného sektora ani na vnútroštátnej úrovni. Jednotliví partneri disponujú dôležitým kusom potrebným na zloženie informačnej skladačky. Disponovanie informáciami o tom, čomu čelíte, zvyšuje šance, že tomu dokážete predísť. Netreba ani dodávať, že podávanie správ by malo byť jednoduchšie a prístupnejšie. Informácie je najprv potrebné zhromaždiť a až potom sa môžu zdieľať. Boli formulované ďalšie odporúčania na zníženie anonymity volajúceho tak, aby bolo sfalšovanie polohy takmer nemožné. V tejto súvislosti by mohol byť tiež zaujímavý softvér na rozpoznávanie hlasu.

Tretia stratégia, ktorá by mohla zabrániť telefonickým podvodom, je zníženie zisku zo spáchania tohto trestného činu. Hlavným odporúčaním je zaistenie nezákonne nadobudnutého majetku. Na odhalenie podozrivých transakcií je preto nevyhnutné monitorovať peňažné toky. Naši odborníci odporučili zriadenie celoeurópskej iniciatívy v oblasti bankovníctva.

Ďalšou stratégiou je obmedzenie provokácií. V tomto ohľade je dôležité nezdieľať príliš veľa informácií o tom, ako bol podvod vykonaný, a zabrániť tak jeho napodobeniu. Okrem toho by to mohlo pomôcť zabrániť niektorým formám opakovanej viktimizácie. Konečnou stratégiou bolo odstránenie ospravedlnení. Zámerom je hlavne zvyšovanie povedomia o telefonických

podvodoch a o tom, ako sa pred nimi chrániť. Zmienené osvedčené postupy sú tu uvedené ako kľúčové príklady. Kampane na zvyšovanie povedomia by mali šíriť to isté posolstvo, Preto je potrebné nadviazať partnerstvá medzi verejným a súkromným sektorom a medzinárodnú spoluprácu tak, aby boli čo najkonzistentnejšie: *jednoducho povedzte nie.*