# Evropská síť pro předcházení trestné činnosti

# Série souborů nástrojů EUCPN

# č. 13

# Předcházení podvodům na jednotlivcích

## Shrnutí

Třináctý soubor nástrojů v sérii zveřejněném sekretariátem EUCPN se zaměřuje na předcházení *jednotlivým podvodům.* Bulharské předsednictví (první polovina roku 2018) se rozhodlo zaměřit se na:

„[…] *problémy související s podvody, zejména telefonické podvody. Tento druh trestné činnosti se v posledních letech stal výdělečnou trestnou činností, která se rozvíjí na vnitrostátní i přeshraniční úrovni. Zločinecké skupiny, které se na tuto činnost specializují, se dynamicky rozvíjejí a zasahují širší spektrum obětí. Vzhledem k aktivní účasti obětí a jejich zapojení do trestních scénářů a traumatizujícím účinkům na psychiku obětí je třeba vyvinout značné preventivní úsilí, přičemž je třeba zohlednit specifika na místní, vnitrostátní a přeshraniční úrovni.“*

Podvody na jednotlivcích jsou druhem podvodu, kde jsou terčem zločinců jednotlivci z řad běžných občanů. Oběť je přemluvena ke spolupráci a poté podvedena. Naše současné chápání tohoto typu podvodu je spojeno především s jeho současnými formami, přičemž nejpravděpodobnějším příkladem je phishing. Je však důležité uvědomit si, že podvody na jednotlivcích jsou zde již celé věky. Technologický vývoj posledních desetiletí umožnil, aby se tyto podvody industrializovaly ve větším měřítku, než se kdy považovalo za možné. Kdo ve svém životě neobdržel phishingový e-mail?

Jak je jasně uvedeno v *odůvodnění* bulharského předsednictví, oběti se aktivně podílejí na své viktimizaci. Pachatel cílí na peníze dané oběti, má k nim ale přístup pouze tím, že oběť přesvědčí, aby mu ho umožnila. Základní taktika, jak postrčit oběť do tohoto vyhovujícího

vztahu, se nazývá **sociální inženýrství**. To pachateli umožňuje získat od oběti důvěru, která je zásadní pro úspěch podvodu. Lepší pochopení tohoto jevu nám nabízí sociální psychologie. Tím, že pachatel apeluje na běžné sociální principy a využívá této „lidské slabosti", je schopen aktivovat to, čemu se říká „periferní cesta přesvědčování". Naopak cesta centrální vyžaduje mnoho myšlenkového a kognitivního úsilí. U druhé není nutná žádná velká propracovanost a reaguje se u ní téměř nevědomě. Například předstíráním, že je osobou s pravomocemi, např. policista, může pachatel od svých obětí snadno získat poslušnost. Tato sociální a kognitivní pravidla mají své každodenní využití, pachateli ale umožňují využít je ve svůj vlastní prospěch.

Tyto klamavé taktiky se používají v široké **škále podvodů**. *419 podvody, granny podvody, romantika podvody, podvody CEO, ...* možnosti jsou stejně nekonečné jako kreativita podvodníků. Tato škála podvodných schémat umožňuje podvodníkům zaměřit se na velmi širokou skupinu veřejnosti najednou nebo zaujmout lépe přizpůsobený přístup. Zdá se, že těchto druhých typů je stále více. Podvodníci si uvědomili, že chytrým zacílením na své oběti jejich „výnos z investic" stoupá. Phishingové e-maily jsou stále sofistikovanější a jsou adresovány vybranému cíli (skupině). Poslední překvapivý krok tohoto vývoje spočívá v kombinaci nových a starších technologií: v telefonu. Tzv. „vishing" neboli hlasový phishing nabízí příležitost kombinovat výhody internetu i telefonu. Uskutečnění telefonního hovoru on-line s sebou nenese téměř žádné náklady, je obtížnější jej sledovat a lze jej automatizovat. Využití telefonu má ještě další výhody: lidé mu důvěřují více a díky intimnějšímu prostředí lze oběť přesvědčit ještě účinněji. Pro ilustraci rostoucí míry sofistikovanosti: pachatelé si dokonce najímají rodilé mluvčí, aby telefonát vypadal co nejpřirozeněji.

Naše současné chápání podvodů na jednotlivcích je však omezené. Tento zločin je obklopen obrovským **temným počtem**, protože většina z něj je nehlášená. Oběti nevědí, že byly viktimizovány, nevnímají to jako dostatečně závažné, nemyslí si, že by nahlášení k něčemu vedlo, nebo prostě nevědí, na koho se obrátit nejprve. Kromě toho aktivní role, kterou oběť ve své vlastní viktimizaci hraje, pocit sebeobviňování a rozpaky oběti brání povědět svůj příběh. Některé podvody mají dokonce takzvaně „vestavěné" mechanismy bránící nahlášení, protože oběť musí v rámci podvodu podniknout nezákonné kroky a sama se tak v rámci procesu inkriminuje. Nahlášením podvodu tak pro ni vlastně znamená udat sama sebe.

Toto tmavé číslo také vyvolalo **mýtus**, že hlavními oběťmi tohoto zločinu jsou starší lidé, protože jsou snadnou kořistí. Některé studie tento mýtus vyvrátily, i když bychom měli zůstat

opatrní kvůli omezenému výzkumu, který je k dispozici. Mladší populace a skupina středního věku jsou však k podvodům údajně náchylnější. Dalším ze stávajících mýtů je, že oběti jsou obvykle vykreslovány jako nevzdělané nebo finančně negramotné, zdá se ale, že opak je pravdou. Jedno možné vysvětlení se nazývá „vědět, ale neumět jednat“, kdy lidé signály podvodu úspěšně rozpoznají, tyto znalosti však neuplatní na svou vlastní situaci.

Existence tzv. „**seznamů zelenáčů**“ bohužel není mýtem. Telefonní podvodníci mohou své oběti kontaktovat náhodně nebo nahlédnout do veřejných rejstříků, ale také si mezi sebou sdílejí seznamy s cíli, které již byly oklamány. Používání těchto seznamů svědčí o vysoké úrovni opakované viktimizace. Někteří podvodníci se například pokusí „pomoci“ obnovit ztracený majetek…

Vzhledem k tomu, že je dohled nad tímto zločinem mimořádně obtížný, je potřeba prevence vysoká. V otázce podvodů na jednotlivcích však bylo provedeno jen málo akademického a hodnotícího výzkumu. Nicméně můžeme sdělit několik obecných zjištění. Nejběžnější preventivní taktikou je vzdělávání veřejnosti. To lze provést v rámci obecné osvětové kampaně, ale pozitivní účinky lze zaznamenat zejména u určitého formátu školení. Tato školení se v podstatě snaží překlenout nedostatek typu„vědět, ale neumět jednat“, o němž jsme se již zmínili. Další klíčovou taktikou je práce s oběťmi. Vzhledem k jejich aktivní úloze a již existujícímu riziku několikanásobného podlehnutí by oběti měly mít podporu a měly by být informovány o svém konkrétním postavení.

Během bulharského předsednictví shromáždil sekretariát řadu **osvědčených postupů** v této oblasti. Ty lze rozdělit podle jejich cílových skupin. První kategorie se zaměřuje na celou populaci. Jsou to osvětové kampaně s příklady z Bulharska, Švédska, Belgie nebo Europolu. Jedná se o rozhlasové spoty, plakáty, letáky, mini aplikace aj., které poskytují veřejnosti užitečné informace a ukazují, jak se chránit před poškozením. Druhý soubor činností je zaměřen na starší osoby. Zde se používají interaktivnější metody, jako je tomu například v České republice. Starší lidé se účastní názorných a interaktivních předvádění, kde se učí o nejběžnějších podvodných schématech a o tom, jak na ně reagovat. Tato „zkušenost naživo“ by jim měla umožnit, aby odpovídajícím způsobem reagovali ve scénářích reálného života. Hodnocení tohoto projektu prokázalo, že tento předpoklad je pravdivý, protože tato skupina odmítla falešné obchody dvakrát a půl krát častěji než kontrolní skupina, která hru nesledovala. Poslední kategorie preventivních činností se soustředila na oběti. Příklady z

Austrálie, Spojeného království a Kanady ukázaly potřebu tohoto typu prevence. Pro oběti podvodů na jednotlivcích však existuje jen málo podpůrných služeb, a to i celosvětově.

Na závěr sekretariát EUCPN zorganizoval seminář s různými odborníky na vypracování některých **doporučení**, jak předcházet podvodům s telefonními hovory. Jsou strukturovány podle pěti strategií prevence situačního zločinu. První možnou strategií je zvýšit úsilí, které musí pachatel vynaložit, aby podvod uspěl. K tomu stačí již pouhé omezení zveřejňování telefonních čísel a přístupu k nim. Další technikou by mohlo být omezení počtu telefonních čísel, které může mít jedna osoba legálně nebo alespoň provázaní s bankovním účtem nebo číslem průkazu totožnosti.

Druhou strategií je zvýšit rizika. V této souvislosti je velmi důležité sdílení informací. Toto sdílení by se nemělo zastavit na hranicích veřejného nebo soukromého sektoru nebo na vnitrostátní úrovni. Na skládání informačního puzzle mají důležitý podíl všichni partneři. Když víte, s čím se potýkáme, zvyšuje se tím v první řadě šance, že se tomu zabrání. Není třeba říkat, že jednodušší a přístupnější by mělo být i ohlašování. Než lze informace sdílet, je třeba je nejprve shromáždit. Dalším doporučením, jak snížit anonymitu volajícího, je, že téměř nebude možná mystifikace co se týká jeho polohy. Zajímavý by zde mohl být i software pro rozpoznávání hlasu.

Snížení odměn, kterých lze dosáhnout spácháním tohoto trestného činu, je třetí strategií prevence podvodů s telefonními hovory. Hlavním doporučením je zde zabavení nezákonně získaného majetku. K tomu je nezbytné sledovat peněžní tok, aby bylo možné odhalit podezřelé transakce. Naši odborníci doporučili pro usnadnění tohoto celoevropskou iniciativu se zapojením bankovního sektoru.

Další strategií je omezit provokace. V tomto ohledu je třeba nesdílet příliš mnoho informací o tom, jak byl podvod skutečně proveden, protože to zabrání těm, kdo se budou "opičit". Kromě toho by toto mohlo pomoci zabránit některým formám opakované viktimizace. Poslední strategií bylo odstranit výmluvy. Zaměřuje se především na zvyšování povědomí o podvodech přes telefon a na to, jak se chránit. Jako klíčové příklady jsou zde uvedeny osvědčené postupy z předchozích období. Stejné sdělení by měly šířit i osvětové kampaně. Pro co největší důslednost je proto třeba vytvářet partnerství veřejného a soukromého sektoru a sítě mezinárodní spolupráce: *stačí říci ne.*