Reţeaua europeana de prevenire a criminalităţii

Seria de instrumente metodologice EUCPN

nr. 13

Prevenirea fraudei individuale

Raport sumar din partea conducerii executive

Cel de-al 13-lea set de instrumente din seria publicată de către secretariatul EUCPN se concentrează pe prevenirea *fraudei individuale*. Preşedinţia bulgară (prima jumătate a anului 2018) a decis să se concentreze pe:

„[…] *problemele asociate fraudelor, în special pe escrocheriile telefonice. Acest tip de infracţiune a devenit o activitate infracţională profitabilă în ultimii ani, care se dezvoltă atât la nivel naţional, cât şi la nivel transfrontalier. Grupurile infracţionale specializate în această activitate se dezvoltă în mod dinamic şi lovesc o gamă mai largă de victime. Având în vedere participarea activă a victimelor şi implicarea acestora în scenarii infracţionale şi efectul traumatizant asupra minţii victimelor, trebuie depuse eforturi serioase de prevenire, ţinând cont de specificul la nivel local, naţional şi transfrontalier”*

Frauda individuală este un tip de fraudă în care cetăţenii individuali şi obişnuiţi sunt vizaţi de infractori. Victimele sunt convinse pentru a fi cooperante şi sunt fraudate ulterior. Înţelegerea noastră actuală a acestui tip de fraudă este legată în principal de formele sale contemporane, phishingul (un tip de înşelătorie utilizată pentru ca utilizatorii de computer să îşi dezvălui informaţii personale sau financiare) fiind cel mai probabil exemplu. Cu toate acestea, este important să recunoaştem că frauda individuală există de secole. Evoluţiile tehnologice din ultimele decenii doar au permis ca aceste escrocherii să fie industrializate la o scară mai mare decât s-a considerat vreodată posibil. Cine nu a primit vreodată un e-mail de tip phishing?

După cum s-a clarificat în *raţionamentul* Preşedinţiei bulgare, victimele participă în mod activ la victimizarea acestora. Infractorul a pus ochii pe banii victimei, dar nu poate avea acces la

aceştia decât prin convingerea victimei în acest sens. Tactica esenţială pentru a atrage victima în această relaţie conformă se numeşte **inginerie socială**. Acest lucru permite infractorului să obţină încrederea victimei care este crucială pentru succesul escrocheriei. Psihologia socială ne oferă o mai bună înţelegere a acestui fenomen. Prin apelarea la principiile sociale cotidiene şi exploatarea acestei „slăbiciuni umane", infractorii sunt capabili să activeze ceea ce se numeşte a doua cale de convingere. Prima cale necesită foarte multă gândire şi efort cognitiv. Cea de-a doua nu are însă nevoie de o elaborare reală şi se desfăşoară aproape în mod inconştient. De exemplu, pretinzând că sunt o persoană în autoritate, cum ar fi un ofiţer de poliţie, infractorii pot obţine cu uşurinţă un anumit nivel de supunere de la victimele acestora. Aceste reguli sociale şi cognitive, general valabile, au utilizările lor zilnice, dar permit infractorilor să le exploateze în propriile beneficii.

Aceste tactici înşelătoare sunt folosite într-o mare **varietate de escrocherii**. *Escrocherii de tip taxă în avans, escrocherii aplicate bunicuţelor, escrocherii romantice, fraude ale directorilor executivi, ...* posibilităţile sunt la fel de nesfârşite ca şi creativitatea escrocilor. Această gamă de scheme înşelătoare le permite escrocilor să vizeze un public foarte mare simultan sau să adopte o abordare mai personalizată. Cea din urmă pare să se întâmple din ce în ce mai mult. Escrocii au realizat că, vizând în mod inteligent victimele acestora, „profitabilitatea" este mai mare. E-mailurile de tip phishing devin din ce în ce mai sofisticate şi se adresează unei ţinte izolate (de grup). Ultimul pas surprinzător în această evoluţie implică asocierea de tehnologie nouă şi mai veche: telefonul. Vishingul sau phishingul vocal oferă posibilitatea de a combina atât avantajele internetului, cât şi ale telefonului. Efectuarea unui apel telefonic online are aproape zero costuri, este mai greu de urmărit şi poate fi făcută în mod automat. Folosirea telefonului are avantaje suplimentare: oamenii au încredere în acesta şi, datorită cadrului mai intim, victimele sunt convinse într-un mod mai eficient. Caracterul informativ al nivelului tot mai mare de sofisticare: infractorii angajează chiar şi vorbitori nativi pentru ca apelurile telefonice să pară cât mai adevărate.

Înţelegerea noastră actuală cu privire la frauda individuală este limitată. În spatele acestui tip de infracţiune este un **număr întunecat şi uriaş**, întrucât o mare parte din acestea nu sunt raportate. Victimele nu ştiu că au fost victimizate, nu percep victimizarea ca fiind suficient de gravă, nu cred că raportarea va duce la ceva anume sau pur şi simplu nu ştiu unde să raporteze. În plus, din cauza rolului activ pe care victima îl joacă în propria victimizare, sentimentele de auto-învinovăţire şi jenă împiedică victimele să-şi spună povestea. Unele înşelătorii au chiar mecanisme anti-raportare „încorporate", deoarece victimele trebuie să

întreprindă acţiuni ilegale în cadrul schemei, incriminându-se în proces. Raportarea escrocheriei ar fi ca şi cum persoanele s-ar preda singure.

Acest număr întunecat a dat naştere şi **mitului** că vârstnicii sunt principalele victime ale acestei infracţiuni, întrucât sunt o pradă uşoară. Unele studii au respins acest mit, deşi ar trebui să rămânem precauţi din cauza cercetărilor limitate disponibile. Cu toate acestea, populaţia mai tânără şi grupul de vârstă mijlocie sunt raportate a fi mai susceptibile la escrocherii. Un alt mit care există este faptul că victimele sunt de obicei înfăţişate ca needucate sau analfabete din punct de vedere financiar, dar pare să fie adevărat exact contrariul. O posibilă explicaţie este numită „decalajul dintre cunoaştere şi punere în aplicare", în care oamenii au succes în a recunoaşte semnalele unei escrocherii, dar nu reuşesc să pună în aplicare aceste cunoştinţe în propria lor situaţie.

Din păcate, existenţa aşa-numitelor „**liste de fraieri**" nu este un mit. Escrocii care folosesc telefonul pentru escrocherii îşi pot contacta victimele la întâmplare sau căutând în registrele publice, dar, de asemenea, fac schimb de liste între aceştia cu ţinte care au fost deja escrocate. Folosirea unor astfel de liste indică nivelul ridicat de victimizare repetată. De exemplu, unii escroci vor încerca să vă „ajute" să vă recuperaţi bunurile pierdute...

Deoarece controlul acestei infracţiuni este extrem de dificil, nevoia de prevenire este mare. Cu toate acestea, au fost efectuate puţine cercetări academice şi evaluative cu privire la frauda individuală. Totuşi, putem prezenta câteva concluzii generale. Cea mai frecventă tactică de prevenire este educarea publicului. Acest lucru se poate realiza într-o campanie generală de creştere a gradului de conştientizare, dar mai ales atunci când este oferit într-un anumit format de instruire, există anumite efecte pozitive care trebuie remarcate. În esenţă, aceste instruiri încearcă să reducă decalajul dintre „cunoaştere şi punere în aplicare" la care ne-am referit anterior. O altă tactică esenţială este colaborarea cu victimele. Datorită rolului activ al acestora şi a riscului existent de a cădea victime de mai multe ori, victimele ar trebui să fie susţinute şi informate cu privire la poziţia specifică a acestora.

În timpul Preşedenţiei bulgare, Secretariatul a adunat un număr de **bune practici** privind acest subiect. Acestea pot fi clasificate în funcţie de grupul ţintă. O primă categorie vizează întreaga populaţie. Este vorba despre campanii de creştere a gradului de conştientizare, precum exemplele din Bulgaria, Suedia, Belgia sau Europol. Acestea implică spoturi radio, afişe, pliante, dispozitive, ... care oferă informaţii utile publicului şi arată modul în care vă puteţi

proteja pentru a preveni prejudicierea. Un al doilea set de activităţi se adresează vârstnicilor. Aici, sunt implementate mai multe metode interactive, cum este cazul în Republica Cehă. Vârstnicii participă la o piesă educaţională interactivă, în care învaţă despre cele mai frecvente scheme înşelătoare şi cum să reacţioneze la acestea. Această „experienţă trăită" ar trebui să le permită să reacţioneze în mod adecvat în situaţiile din viaţa reală. Evaluarea acestui proiect a demonstrat că această presupunere este adevărată, deoarece grupul a refuzat de două ori şi jumătate mai multe oferte false decât un grup de control care nu a urmărit piesa. Ultima categorie de activităţi de prevenire centrate pe victime. Exemple din Australia, Regatul Unit şi Canada au arătat nevoia acestui tip de prevenire. Cu toate acestea, există, chiar şi la nivel mondial, puţine servicii de susţinere pentru victimele fraudelor individuale.

În cele din urmă, Secretariatul EUCPN a organizat un atelier cu diferiţi experţi pentru a elabora câteva **recomandări** cu privire la modul de prevenire a escrocheriilor telefonice. Acestea sunt structurate în funcţie de cele cinci strategii de prevenire a infracţiunilor situaţionale. Prima strategie posibilă este creşterea nivelului de efort pe care un infractor trebuie să-l depună pentru ca escrocheria să aibă succes. Prin intermediul restricţiei publicării şi a accesului la numere de telefon se poate deja obţine acest lucru. O altă tehnică ar putea fi limitarea cantităţii de numere de telefon pe care o persoană o poate avea, sau cel puţin, asocierea acestui lucru cu un cont bancar sau un număr de identificare.

O a două strategie este creşterea riscurilor. Este de o importanţă esenţială aici să facem schimb de informaţii. Acest schimb nu ar trebui să se oprească la graniţele sectorului public sau privat sau la nivel naţional. Toţi partenerii deţin o piesă importantă pentru a completa puzzle-ul cu informaţii. Ştiind cu ce aveţi de-a face creşte şansele de a preveni întâmplarea. Este de la sine înţeles că raportarea ar trebui să fie efectuată mai uşor şi ar trebui să fie mai abordabilă. Informaţiile trebuie adunate înainte de a putea fi trimise altor persoane. Alte recomandări au fost făcute pentru a reduce anonimatul apelantului, făcând aproape imposibilă depistarea locaţiei. Aici ar putea prezenta interes şi software-ul de recunoaştere vocală.

Reducere recompenselor care pot fi obţinute prin săvârşirea acestei infracţiuni este o a treia strategie pentru prevenirea escrocheriilor telefonice. Confiscare bunurilor obţinute ilegal este aici recomandarea principală. Pentru a face acest lucru, monitorizarea fluxului de bani este crucială pentru a detecta tranzacţii suspecte. Experţii noştri au recomandat o iniţiativă la nivelul U.E. cu sectorul bancar pentru a facilita acest lucru.

O altă strategie este reducerea provocărilor. În acest sens, este important să nu faceţi schimb de prea multe informaţii cu privire la modul în care escrocheria a fost efectiv executată, deoarece acest lucru va preveni imitatorii. Pe lângă aceasta, ar putea ajuta la prevenirea unor forme de victimizare repetată. Ultima strategie a fost eliminarea pretextelor. Acest lucru se axează în principal pe creşterea gradului de conştientizare cu privire la escrocheriile telefonice şi modul în care vă puteţi proteja. Bunele practici menţionate anterior sunt prezentate ca exemple cheie aici. Campania de creştere a gradului de conştientizare trebuie să răspândească acelaşi mesaj. Prin urmare, parteneriatele publice şi private şi cooperarea la nivel internaţional trebuie stabilite pentru a fi cât mai consecvente: *spuneţi nu.*