

Rete europea di prevenzione della criminalità

EUCPN Toolbox Series

N. 13

Prevenzione delle frodi individuali

Riassunto esecutivo

Il 13° toolkit della serie pubblicata dal Segretariato dell'EUCPN si concentra sulla prevenzione delle *frodi individuali*. La presidenza bulgara (prima metà del 2018) ha deciso di concentrarsi su:

"[...] questioni relative alle frodi e, in particolare, sulle truffe telefoniche. Negli ultimi anni, questo tipo di reato è diventato un'attività criminale redditizia, che sta prendendo piede sia a livello nazionale che transfrontaliero. I gruppi criminali specializzati in questa attività si stanno sviluppando in modo dinamico e colpiscono una gamma più ampia di vittime. Data la partecipazione attiva delle vittime e il loro coinvolgimento in scenari criminali e considerato l'effetto traumatizzante sulla mente delle vittime stesse, è necessario compiere seri sforzi di prevenzione, tenendo conto delle specificità a livello locale, nazionale e transfrontaliero".

La frode individuale è un tipo di frode in cui i criminali prendono di mira i singoli cittadini. Le vittime vengono persuase ad adottare una mentalità cooperativa e in seguito raggirate. La nostra attuale comprensione di questo tipo di frode è legata principalmente alle sue forme contemporanee, con il phishing quale esempio più probabile. Tuttavia, è importante riconoscere che la frode individuale esiste da secoli. Le evoluzioni tecnologiche degli ultimi decenni hanno permesso di industrializzare queste truffe solo su una scala più ampia di quanto mai ritenuto possibile. Chi non ha mai ricevuto un'e-mail di phishing in vita sua?

Come si evince dalla *logica* illustrata dalla presidenza bulgara, le vittime partecipano attivamente alla loro vittimizzazione. L'autore del reato mette gli occhi sul denaro della vittima, ma può avervi accesso solo convincendo quest'ultima a concederglielo. La tattica

essenziale adottata per spingere la vittima in questa relazione compiacente prende il nome di **ingegneria sociale**. Questa consente al truffatore di ottenere dalla vittima la fiducia fondamentale perché il reato vada a buon fine. La psicologia sociale ci offre una migliore comprensione di tale fenomeno. Facendo appello ai principi sociali quotidiani e sfruttando questa "debolezza umana", i truffatori sono in grado di attivare la cosiddetta "seconda via persuasiva": se la prima via richiede un grande sforzo di pensiero e cognitivo, la seconda, invece, non ha bisogno di una vera e propria elaborazione e reagisce quasi inconsciamente. Ad esempio, fingendo di essere una persona autorevole come un ufficiale di polizia, gli autori del reato possono facilmente ottenere un certo livello di obbedienza dalle loro vittime. Queste regole empiriche sociali e cognitive hanno i loro impieghi quotidiani, ma consentono ai criminali di sfruttarle a proprio vantaggio.

Tali tattiche ingannevoli sono utilizzate in una grande **varietà di truffe**. *Truffe alla nigeriana (419 scam), truffe agli anziani, truffe sentimentali, truffe del falso CEO...* le possibilità sono infinite tanto quanto la creatività dei truffatori. Questa gamma di tattiche ingannevoli permette ai criminali di prendere di mira un pubblico molto vasto in una sola volta o di adottare un approccio più personalizzato. Sempre più spesso, l'evenienza più comune sembra essere proprio quest'ultima. I truffatori si sono resi conto che, rivolgendosi in modo mirato e intelligente alle vittime prescelte, il loro "ritorno sull'investimento" è più elevato. Le e-mail di phishing stanno diventando sempre più sofisticate e si rivolgono a un target (gruppo) predeterminato. L'ultimo sorprendente passo di questa evoluzione riguarda la combinazione di una tecnologia nuova e vecchia allo stesso tempo: il telefono. Il vishing o il voice phishing offre la possibilità di combinare i vantaggi di Internet e del telefono. Effettuare una telefonata online non ha quasi alcun costo, è più difficile da rintracciare ed è un'azione che può essere automatizzata. L'uso del telefono ha ulteriori vantaggi: le persone si fidano maggiormente e, grazie alla creazione di un contesto più intimo, le vittime vengono convinte con maggiore efficacia. Un esempio indicativo del crescente livello di sofisticazione è il seguente: i truffatori sono arrivati ad assumere persino persone madrelingua per far sembrare le telefonate il più autentiche possibile.

La nostra attuale comprensione delle frodi individuali è tuttavia limitata. La portata del fenomeno è quantificabile come un enorme **numero oscuro**, poiché buona parte dei reati non viene denunciata. Le vittime non sanno di essere state vittimizzate, non percepiscono la reale gravità del reato, non ritengono che la denuncia porterà a qualche esito o, semplicemente, non sanno a chi rivolgere la propria denuncia in primo luogo. Inoltre, a causa del ruolo attivo che

la vittima svolge nella sua stessa vittimizzazione, i sentimenti di autocolpevolizzazione e di imbarazzo la trattengono dal raccontare la propria storia. Alcune truffe prevedono persino dei meccanismi di antidenuncia "integrati" in virtù dei quali le vittime devono intraprendere azioni illegali incriminando se stesse nel processo. Denunciare la truffa equivarrebbe, dunque, a costituirsi.

Da tale numero oscuro è nato anche il **mito** secondo cui gli anziani sarebbero le principali vittime di questo reato in quanto facili prede. Sebbene questo mito sia stato sfatato da alcuni studi, dovremmo rimanere cauti al riguardo considerato il numero limitato di ricerche disponibili in materia. Ciononostante, la popolazione più giovane e la fascia di mezza età vengono segnalate come i gruppi più sensibili alle truffe. Un altro mito esistente è quello secondo cui le vittime solitamente sono ritratte come persone prive di istruzione o analfabete, eppure sembra vero il contrario. Una possibile spiegazione è data dalla "lacuna della conoscenza", per cui le persone sono in grado di riconoscere i segnali di una truffa, ma non riescono ad applicare questa conoscenza alla propria situazione.

Purtroppo, l'esistenza delle cosiddette "**liste di babbei**" non è un mito. I truffatori telefonici possono contattare le loro vittime a caso o consultando i registri pubblici, ma condividono fra loro anche liste di persone già vittime di frodi. L'uso di tali elenchi è indicativo dell'alto livello di reiterazione della vittimizzazione. Alcuni truffatori, ad esempio, cercheranno di "aiutare" le vittime a recuperare i beni perduti...

Poiché il controllo di questo reato è estremamente difficile, la necessità di prevenzione è elevata. Tuttavia, sebbene siano state condotte poche ricerche accademiche e di valutazione sulle frodi individuali, possiamo ipotizzare alcune constatazioni di carattere generale. La tattica di prevenzione più comune consiste nell'educazione del pubblico. Questa può avvenire mediante una campagna di sensibilizzazione generale e, soprattutto quando viene impartita sotto forma di corso di formazione, è accompagnata da alcuni effetti positivi degni di nota. In sostanza, questi corsi di formazione cercano di colmare la lacuna del "saper fare" di cui dicevamo. Un'altra tattica chiave è quella di lavorare con le vittime. A causa del loro ruolo attivo e del rischio di essere raggirati più volte, le vittime dovrebbero essere sostenute e sensibilizzate rispetto alla loro particolare posizione.

Durante la Presidenza bulgara, il Segretariato ha raccolto una serie di **buone pratiche** incentrate su questo tema, che possono essere classificate in base al loro gruppo target. Una

prima categoria si concentra sull'intera popolazione: si tratta di campagne di sensibilizzazione, come gli esempi provenienti da Bulgaria, Svezia, Belgio o Europol. Queste comprendono, fra l'altro, spot radiofonici, manifesti, volantini e gadget che forniscono informazioni utili al pubblico e mostrano come proteggersi da eventuali rischi. Una seconda serie di attività è rivolta agli anziani: in questo caso vengono impiegati metodi più interattivi, come nella Repubblica Ceca. Gli anziani partecipano a un'opera teatrale educativa interattiva in cui imparano a conoscere i tipi di truffe più comuni e come reagire ad esse. Tale "esperienza vissuta" dovrebbe consentire loro di reagire adeguatamente in scenari di vita reale. La valutazione del progetto ha confermato la validità di questa ipotesi, in quanto il gruppo ha rifiutato delle offerte false due volte e mezzo in più rispetto a un gruppo di controllo che non aveva assistito allo spettacolo. L'ultima categoria di attività di prevenzione si è incentrata sulle vittime. Esempi provenienti dall'Australia, dal Regno Unito e dal Canada hanno dimostrato la necessità di questo tipo di prevenzione. Ciononostante, anche a livello globale, esistono pochi servizi di assistenza alle vittime di frodi individuali.

Infine, il Segretariato dell'EUCPN ha organizzato un workshop con diversi esperti per formulare alcune **raccomandazioni** su come prevenire le truffe telefoniche. Queste sono state strutturate secondo le cinque strategie di prevenzione della criminalità situazionale. La prima strategia possibile è quella di aumentare lo sforzo che un criminale deve compiere perché la truffa abbia successo. Limitare la pubblicazione e l'accesso ai numeri di telefono può già raggiungere questo obiettivo. Un'altra tecnica potrebbe essere quella di limitare i numeri di telefono che una persona può avere o almeno di collegarli a un conto bancario o a un numero identificativo.

Una seconda strategia consiste nell'aumentare i rischi. In questo caso è di fondamentale importanza condividere le informazioni. Tale condivisione non deve fermarsi ai confini del settore pubblico o privato, né a livello nazionale. Tutti i partner hanno un ruolo da svolgere nel completamento del puzzle informativo. Sapere con cosa si ha a che fare aumenta le possibilità di evitare che ciò accada. Inutile dire che le segnalazioni dovrebbero essere rese più semplici e accessibili. Le informazioni devono essere raccolte prima di poter essere condivise. Altre raccomandazioni sono state elaborate per ridurre l'anonimato del chiamante, rendendo quasi impossibile la falsificazione della propria posizione. Anche in questo caso potrebbe essere interessante utilizzare software di riconoscimento vocale.

Ridurre le ricompense che si possono ottenere commettendo questo reato è una terza strategia per prevenire le truffe telefoniche. In questo caso la raccomandazione principale è quella di procedere al sequestro dei beni ottenuti illegalmente. A tale scopo, per individuare le transazioni sospette, è fondamentale monitorare il flusso di denaro. Per agevolare questa operazione, i nostri esperti hanno raccomandato un'iniziativa a livello europeo.

Un'altra strategia è quella di ridurre le provocazioni. A questo proposito, è importante non condividere troppe informazioni sulle effettive modalità di esecuzione della truffa, così da evitare possibili emulazioni. Ciò, inoltre, potrebbe contribuire a prevenire alcune forme di vittimizzazione ripetuta. L'ultima strategia è stata quella di eliminare le scuse. L'obiettivo principale consiste nella sensibilizzazione dell'opinione pubblica sulle truffe telefoniche e su come proteggersi. Le buone pratiche di cui sopra sono qui illustrate come esempi chiave. Le campagne di sensibilizzazione dovrebbero diffondere lo stesso messaggio. Pertanto, i partenariati fra il settore pubblico e privato e la cooperazione internazionale devono essere stabiliti in modo da essere il più coerenti possibile: *basta dire di no*.