VADEMECUM

redatto dalla Prefettura di Varese con il supporto delle Forze dell'Ordine e della Polizia Postale

CASI RICORRENTI DI TRUFFE AD ANZIANI

Truffa del "sedicente avvocato". Il truffatore contatta il malcapitato spacciandosi per avvocato, poi gli riferisce di un possibile arresto (per esempio a causa di incidente stradale) che potrebbe avvenire ai danni di un suo congiunto (che si trova in stato di fermo presso la Questura o una Caserma dei Carabinieri) e prospetta una pronta risoluzione del caso, evitando conseguenze di tipo penale, qualora venga tempestivamente versata una cauzione.

Truffa del "finto tecnico del Comune" incaricato della verifica della rete idrica. Il truffatore, presentatosi presso l'abitazione dei malcapitati, solitamente anziani, riferisce di una contaminazione dell'acqua con rischio di un immediato pericolo di esplosione delle tubature dell'acqua, riuscendo a convincere l'anziano a riporre i monili in oro in frigorifero e, approfittando di un momento di distrazione, se ne impossessa dandosi poi ad immediata fuga. In alcuni casi si è registrato l'utilizzo dello spray al peperoncino da parte dei malviventi per convincere gli anziani proprietari dell'abitazione dell'effettiva contaminazione dell'acqua.

Truffa della "polizza assicurativa". Il truffatore si spaccia per un intermediario assicurativo e propone prodotti assicurativi a prezzi molto vantaggiosi. Una volta ottenuto il pagamento, emette una falsa polizza RC.

Truffa del "finto operatore di banca". Il truffatore contatta telefonicamente o via sms la vittima spacciandosi per un impiegato di banca. Si fa poi consegnare gli estremi delle carte di credito e dei conti correnti per poi effettuare dei bonifici.

Truffa del "fornitore di energia elettrica". Il truffatore contatta telefonicamente la vittima prescelta spacciandosi per un incaricato di un'azienda erogatrice di energia elettrica. Propone dei contratti a prezzi molto vantaggiosi e si fa consegnare un anticipo in denaro.

Truffa del "finto bisognoso". Il truffatore si finge indigente e bisognoso. Raggira il malcapitato facendosi elargire denaro tramite bonifico.

Truffa del "finto appartenente alle Forze dell'Ordine". Il truffatore, fingendosi Carabiniere o comunque appartenente alle Forze dell'Ordine, unitamente ad un complice che si finge addetto al controllo dell'impianto idrico, paventano alla vittima una possibile contaminazione dell'acqua. Una volta all'interno dell'abitazione, soggiogano il malcapitato, asportandogli oro e contanti.

Truffa del "caro nipote". Il truffatore contatta la vittima sulla sua utenza telefonica casalinga, generalmente acquisendo il nome da registri telefonici pubblici e concentrandosi su nomi non più in uso potenzialmente riferibili a persone anziane e, spacciandosi per un parente gravemente malato bisognoso di cure mediche costose (negli ultimi anni molto utilizzato il finto malato Covid ricoverato in struttura sanitaria e prossimo a intubazione), convince la vittima a raccogliere il denaro e oggetti preziosi da consegnare ad un incaricato del ritiro che si presenterà con una parola chiave, generalmente un nome proprio.

Truffa "dello specchietto". Il truffatore, con una macchina generalmente intestata ad un prestanome, parcheggia a lato strada e attende il passaggio della vittima a bordo di altra macchina. Quando la vittima gli passa di fianco, il truffatore, con un piccolo sasso, o altro oggetto, colpisce il veicolo della vittima in modo da causare un rumore come se fra i due veicoli si fosse verificata una collisione. Nel momento in cui la vittima si ferma per verificare cosa sia successo, il truffatore riesce a fargli credere di essere stato colpito dalla sua macchina allo specchietto, chiedendo il pagamento della relativa riparazione, senza procedere a constatazione amichevole o segnalazioni all'assicurazione, in modo da non far salire le classi di merito, e chiedendo in genere una somma non molto elevata, comunque calibrata sulla percezione dei fatti che dimostra avere la vittima.

Truffa mediante "tecnica dell'abbraccio". Una donna aggancia l'anziano facendo complimenti, spesso lasciando intendere un approccio di tipo sessuale. Attraverso l'abbraccio riesce a sfilare abilmente l'orologio di ingente valore al polso della vittima. Acquisito l'orologio si allontana velocemente facendo perdere le sue tracce.

Truffa "della cassetta della frutta". L'anziano viene avvicinato da un uomo più giovane che inizia a salutarlo con confidenza stupendosi del fatto che non lo riconosca. Si spaccia per un figlio di un conoscente o di un parente. Dopo essere entrato in confidenza rivela di attraversare un periodo di difficoltà economica. A causa di ciò ha deciso di vendere al dettaglio la frutta. Apre il cofano della sua macchina e mostra una cassetta colma di frutta. La vittima, al fine di compensare adeguatamente il "povero" ragazzo, paga una cifra consistente, ben oltre il valore reale del bene. L'uomo carica la cassetta della frutta sull'automobile del malcapitato, ringrazia e lo saluta. La vittima scoprirà successivamente che, al di là della frutta posta in superficie, di buona qualità, all'interno della cassetta vi è soltanto frutta marcia da gettare.

CASI RICORRENTI DI TRUFFE COMMERCIALI

Truffa del "resto della spesa". Il malvivente raggira la cassiera di un esercizio commerciale durante il pagamento ottenendo il resto in denaro maggiore di quanto dovutogli.

Truffe con "assegni rubati". I contatti tra truffato e truffatore avvengono generalmente in maniera indiretta (telefono, mail, ecc.). Il malvivente paga il venditore raggirato con assegni rubati o falsificati. Le utenze utilizzate solitamente risultano appartenere a soggetti estranei alla vicenda.

CASI RICORRENTI DI TRUFFE TRAMITE SISTEMI INFORMATICI

Truffa del "trading online". E' un servizio che consente, attraverso piattaforme di broker appositamente autorizzati dalla CONSOB, l'acquisto e la vendita online di strumenti finanziari come azioni, obbligazioni, titoli di stato, ecc. Si tratta di una forma di investimento particolarmente diffusasi grazie ai minori costi di commissione richiesti dal broker all'investitore ed alla possibilità di potersi informare direttamente sull'andamento di un particolare titolo o della borsa in generale (la visualizzazione di grafici e informazioni utili sui titoli) per effettuare con maggiori dati le scelte di investimento. Si sono parallelamente diffuse false piattaforme i cui "gestori" hanno il solo fine di sottrarre il denaro che gli ignari risparmiatori credono di avere investito attraverso di esse. Solitamente i primi contatti con il presunto broker avvengono da call center e la vittima ha la possibilità di constatare che le piattaforme sono ben fatte e sono

supportate da assistenza telefonica. Seguono poi il contatto telefonico con il broker in persona, la formalizzazione di un contratto ed il versamento di piccole forme iniziali per lo più a mezzo bonifici su conti correnti di banche che hanno sede all'estero. Constatando l'apparente bontà dell'investimento, la vittima viene persuasa ad effettuare bonifici ben più consistenti fino a che, chiedendo di rientrare di tutto o parte dell'investimento, non vi riesce capendo di essere stata truffata.

Truffa del "cryptolocker". Questa frode viene realizzata attraverso l'inoculazione dei c.d. "*Ransomware*", un'evoluzione dei classici virus informatici, progettati con lo scopo finale di estorcere denaro alle ignare vittime che si vedono inibito l'accesso al proprio sistema a causa della cifratura di intere cartelle di documenti.

Truffa sul portale subito.it o similari: l'utente mette in vendita un oggetto ed in breve tempo è contattato da persona che si mostra interessata all'acquisto, spesso invia anche copia del proprio documento di identità, naturalmente falso, e chiede al venditore di recarsi presso uno sportello bancomat per accreditare la somma pattuita per la vendita, l'ignaro venditore in pochi minuti si accorge che la somma non è stata accreditata ma addebitata; altro modus operandi è quello di chiedere una somma di denaro per pagare le tasse di trasporto all'estero in quanto l'acquirente sostiene di risiedere ad esempio in Francia.

Vendite di oggetti su siti internet: spesso i siti vengono creati molto simili a quelli dei marchi ufficiali, proponendo il materiale a prezzi molto vantaggiosi; importante scorrere la pagina sino al termine, notare se vengono riportati dati fondamentali quali la partita IVA, la sede legale della ditta, nonché controllare le recensioni lasciate da altri utenti, dovendo diffidare di costo decisamente inferiore a quello proposto nei negozi fisici o sui siti ufficiali.

Pagamento paypal: non eseguire mai un pagamento paypal con la dicitura "invia pagamento ad amici e familiari", se lo si fa non si avrà più diritto al rimborso in caso di truffa ed è una pratica molto in voga tra i truffatori.

Truffa romantica: le persone vengono contattate sui social (facebook, instragram, telegrametc) da una persona che inizia una conoscenza discreta, le conversazioni avvengono in chat (telegram, hangoutetc) e l'interlocutore con il trascorrere dei giorni si mostra sempre più attento ai bisogni dei malcapitati, sino a confessare il proprio amore, utilizza foto di persone di piacevole aspetto e di buon livello sociale (medico, militare, agente di commercio di prodotti di lusso) tratte da profili facebook o instagram i cui legittimi titolare ne sono ignari. Non spostano mai la conversazione sul sesso e quasi mai effettuano chiamate o videochiamate, lo scopo è quello di chiedere soldi per difficoltà economiche o altre scuse simili.

Sex extorsion: le vittime vengono contattate sui social da avvenenti donne o uomini e dopo una serie di convenevoli, propongono una video chiamata finalizzata a consumare un rapporto sessuale online; all'avvio della video chiamata la persona vedrà una donna/uomo che inizia a spogliarsi ed invita a fare lo stesso, quando il o la malcapitata si accorge che si tratta di un video registrato è troppo tardi perché si è già inquadrato completamente nudo e il truffatore ha effettuato degli screenshot. Successivamente iniziano a chiedere soldi con la minaccia di divulgare le immagini a tutti gli amici preventivamente individuati sui social.

Phishing. Si tratta di una frode informatica che mira alla sottrazione di dati personali attraverso l'azione inconsapevole dell'utente, generalmente tramite l'invio di e-mail o sms fittizi contenenti l'avviso di un'anomala attività riscontrata sul conto corrente. E' sempre presente un link che

rimanda a un sito clone di quello della banca. Una volta aperto il link, l'utente viene indotto ad inserire il codice utente ed il pin di accesso al conto corrente. Dopo pochi istanti, la vittima riceve una telefonata nel corso della quale l'interlocutore chiede che gli vengano forniti gli ulteriori codici ricevuti via sms e in tal modo il truffatore ha piena disponibilità del conto corrente del malcapitato.

Vishing: tecnica di truffa in cui i dati personali della vittima vengono recuperati a seguito di contatto telefonico; di fatto il malfattore effettua una chiamata, che sembra provenire dal servizio clienti della banca, informando la vittima di un possibile tentativo di prelievo di denaro dalle sue carte di credito; pertanto l'ignara persona riferisce ai truffatori i pin d'accesso nella convinzione che siano utilizzati per bloccarle temporaneamente al fine di sventare l'addebito non autorizzato, naturalmente il pin viene utilizzato per prelevare da casse ATM.

Smishing: Similare al phishing, per la truffa dello smishing vengono utilizzati messaggi SMS che giungono al malcapitato che, per esempio, viene informato dell'esistenza di movimenti sospetti nel proprio conto corrente, quindi viene inviato a entrare all'interno di una pagina web, grazie a un link presente nel messaggio, creata appositamente dai malfattori con design uguale a quello dell'istituto di credito; all'interno di questa pagina web la vittima inserisce i propri dati personali d'accesso, che vengono carpiti così dai malfattori.

Trojan: come è ben facile intuire dal nome, con il termine di Trojan vengono racchiusi tutti i *virus* che vengono inoculati con varie metodologie all'interno di device fornendo la possibilità ai malfattori di interfacciarsi con il dispositivo stesso e permettendo di carpire i dati sensibili rinchiusi all'interno dei device. Il metodo più comune di inoculare i detti virus trojan da parte dei malfattori è quello di inviare al malcapitato una e-mail avente come oggetto ad esempio il pagamento di una fattura di un abbonamento, tutto ciò induce la vittima ad aprire il file allegato che conterrà il virus trojan.

Ultime analisi di sicurezza informatica hanno individuato anche codici di virus Trojan all'interno di file di tipologia PDF.

Come sotto categoria degli attacchi Trojan esistono gli attacchi ransomware: i dati del computer del malcapitato vengono criptati e solo al pagamento di una riscatto di un codice di decriptazione potranno essere recuperati.

Digital Extortion: Campagne digitali massicce di estorsione che minacciano l'immagine di un soggetto, le relazioni sociali e nei casi estremi perfino la vita stessa del malcapitato; fanno parte di questa categoria ad esempio le varie mail dove si sostiene che la vittima abbia visitato sito web pornografici; inoltre il truffatore sostiene di aver preso il controllo del computer del malcapitato avendo avuto così il tempo di raccogliere i dati dei suoi contatti, minacciandolo di inviare a quest'ultimi i video che avrebbe raccolto durante la visione di siti compromettenti.

Evoluzione della DIGITAL EXTORTION è l'invio da parte dei truffatori di un e-mail in cui si spacciano per un'organizzazione governativa alla lotta contro la pedo-pornografia richiedendo di pagare una sanzione per aver visitato dei siti a carattere pedo-pornografico.

Non è mai da escludere che chi effettua questa tipologia di attacco informatico non possa effettuare una metodologia di doppio attacco, per esempio un attacco Trojan all'interno di un messaggio di DIGITAL EXTORTION.

Fake Crowdfunding: simile alla truffa romantica tranne per il fatto che al posto di far leva sul sentimento di affetto o amore si basa sulla dedizione all'aiuto del prossimo.

Man In The Middle: in italiano "uomo di mezzo", è una terminologia informatica in cui qualcuno ritrasmette o altera le comunicazioni tra due parti; in questo caso la truffa è composta da tre soggetti, due passivi, i malcapitati, ed un soggetto attivo, il malfattore. Scopo del malfattore è di avere un vantaggio economico e nello specifico dirottare dei fondi verso un proprio conto corrente creato appositamente.

Nella stragrande maggioranza dei casi il malvivente, una volta riuscito ad intercettare le comunicazioni tra i due soggetti, che il più delle volte risultano essere aziende, attende l'emissione di una o più fatture di pagamento; quindi, quando reputa che il momento sia propizio, di solito, va ad alterare in tutto o in parte la comunicazione per il pagamento inserendo le proprie coordinate bancarie, di un conto creato appositamente, il più delle volte aperto presso istituti di credito residenti all'estero.

Questa tipologia di truffa è spesso preceduta da attacchi trojan o phishing da parte dei malviventi.