SINDACATO AUTONOMO DI POLIZIA
FLASH
NELLA NOSTRA AUTONOMIA LA VOSTRA LIBERTA'
#34
2022
LUNEDI' 22 AGOSTO 2022

TRUFFE ON-LINE

EDITORIALE DEL SEGRETARIO GENERALE

Le frodi on-line sono la nuova frontiere delle truffe. Per chi cade nella rete non c'è scampo e il rischio è di rimetterci anche cospicue somme di denaro. Attenzione, perché è molto facile inciampare in queste truffe on-line. A volte per fretta e distrazione, si rischia di inserire dei dati importanti che poi vengono utilizzati per aggirare il malcapitato di turno. Per questo motivo pubblichiamo un'intervista effettuata ad un nostro collega specialista nella materia (che ringraziamo per il prezioso contributo), il quale in modo chiaro e preciso, descrive quelle che sono le possibili insidie. Ci auguriamo possa essere utile non solo ai colleghi, ma anche a tutti i nostri lettori

Stefano Paoloni

LA NUOVA FRONTIERA DELLE TRUFFE INFORMATICHE: TRADING-ONLINE, SMISHING, MAN IN THE MIDDLE

*di **Giusy Criscuolo** - Ufficio Stampa SAP*

Sono sicuramente più remunerative e non lasciano in dietro nessuno. Queste nuove truffe stanno dilagando e stanno diventando pericolose non solo per i semplici cittadini ma anche per professionisti e grandi multinazionali. Si va dalle migliaia di euro, un capitale per chi ha esigue disponibilità, fino ad arrivare a milioni di euro.
Uno dei nostri Dirigenti Sindacali, un poliziotto che si occupa proprio di questo specifico argomento ci dà delle delucidazioni importanti su quali siano le nuove truffe e su come evitarle.

Di che tipo di truffe si parla?

Un esempio potrebbe essere la casella di sms con il famoso messaggio di avviso della propria banca. Sono studiati perfettamente e sono in molti a cascarci. Ovvio se uno non ha la BNL cancellerà il messaggio, ma se il messaggio arriva dalla "propria banca" si tiene sicuramente in considerazione. Ma non sono assolutamente inviati dal proprio ente bancario. La gente deve capire che questo non è il metodo di comunicazione che le strutture utilizzano per potersi mettere in contatto con i propri clienti. In realtà questi sono dei servizi acquistati da aziende straniere e non ben identificate. Questi messaggi possono essere veicolati tramite email, sms, social network. In buona fede in molti (soprattutto anziani) cliccano sul link e indicano i propri dati personali e le proprie credenziali venendo truffati e derubati.

ORGANO UFFICIALE DELLA SEGRETERIA GENERALE SAP
Reg. Tribunale di Roma n° 98 del 21 febbraio 2000
Direttore Politico e Direttore Responsabile: Stefano Paoloni
I ♥ POLIZIA
www.sap-nazionale.org

Ma oltre allo spam di che truffe si parla?

Il primo metodo di truffa è quello del trading on-line che ha fatto grossissimi danni soprattutto durante il periodo del Covid e continua a farne. Con il trading on-line ad essere truffati non sono solo gli anziani, che hanno accesso a device o internet, ma anche soggetti che hanno grande dimestichezza con le nuove tecnologie è che catturati dall'idea di ottenere guadagni facili, decidono

di investire attraverso l'acquisto di Bitcoin, venendo fagocitati dal sistema per poi essere truffati. Per dare inizio alla truffa bisogna compilare un format al quale si accede attraverso un link, inserendo nome, cognome, data di nascita e numero di telefono. Il passo successivo è seguito da una chiamata del soggetto truffante che si spaccia per trader di Bitcoin. I soggetti sono altamente preparati quindi riescono a proporre il prodotto al meglio, carpendo la fiducia di chi ascolta. Questi truffatori sono specializzati, perché conoscono la materia in modo eccellente. La loro preparazione la loro capacità affabulatoria è riuscita a irretire persone come professori universitari, ingegneri e addirittura colleghi. Senza tralasciare persone anziane e giovani che hanno voglia di guadagnare immediatamente senza grande sforzo. Una volta irretiti vengono convinti a fare un piccolo investimento con la carta di credito sulla piattaforma loro indicata. L'investimento minimo è di €200.

Cosa succede dopo che le persone hanno investito?

I truffatori per far vedere che l'investimento è andato a buon fine rinviano ad un link tramite posta elettronica. A questo punto le persone vengono indotte a scaricare dei software che sono a gestione remota come Any Desk o TeamViewr. Ne segue che il soggetto controllerà il PC della persona da remoto e a tutti gli effetti sarà concretizzata la truffa. I mal capitati, indotti ad inserire i codici bancari, permetteranno di far acquisire tutti i dati necessari per effettuare tutte le transazioni di cui avranno bisogno fino a fine truffa

Ma come mai le persone non si accorgono della truffa?

Perché attraverso il software Any Desk che gli fanno scaricare sono in grado di fargli vedere che il loro investimento ha prodotto dei risultati e dei guadagni immediati, il tutto attraverso software di

borsa e trading. A questo punto i truffatori consigliano di fare un ulteriore investimento, superiore a quello precedente, partendo da una base media di €1000. Dopo l'investimento, la vittima ha bisogno di certezze per valutare se si tratta di una truffa, chiedendo così di poter ritirare o ricevere una quota di ciò che è stato versato. Perfettamente organizzata, la truffa prevede l'invio, al mal capitato, di €200/500, che serviranno a convincere il truffato della veridicità dell'affare. A questo punto la vittima è irretita perché crede che sia una cosa reale e comincia a fare investimenti grossi fino ad arrivare a migliaia di euro. Ma quando la truffa verrà scoperta, sarà troppo tardi, perché non potranno più avere indietro il denaro.
La cosa che, però, ci lascia un po' perplessi è che quando vengono a fare denuncia non sono ancora del tutto convinti che sia una reale truffa.

Come si può evitare che le persone possano cadere in tali tranelli?
Noi abbiamo una regola fondamentale: il trading on-line non si fa su piattaforme esterne ma solo attraverso la propria banca. Diffidare di tutto ciò che è esterno alla propria banca compresi i messaggi sms, email e/o telefonate. Chi vuole fare trading lo può fare solo recandosi in filiale con la specifica richiesta di voler provare questo investimento. In poche parole, bisogna recarsi fisicamente in banca aprendo un canale privato bancario collegabile soltanto al trading on-line. Solo a quel punto la banca fisicamente e de visu, darà delle credenziali per poter effettuare questo tipo di investimento. Ripetiamo, diffidare assolutamente di sms, email e chiamate telefoniche che provengono da sedicenti banche, perché la banca non chiede mai on-line o via email codici, così come il cambio password o reset account.

Ci sono altri tipi di truffe oltre al trading on-line?
Come accennavo precedentemente c'è lo "smishing". Questo consiste in quei messaggi soprattutto tramite SMS che sono mandati da sedicenti banche che appaiono con i nomi corretti delle banche di appartenenza dei soggetti a cui sono inviati. Il soggetto truffato vede che il messaggio arriva dalla "propria banca", la quale chiede di cambiare password, per i problemi più vari, tipo difficoltà di entrare nella home banking. Il soggetto per fare velocemente inserisce i propri dati. A quel punto gli hacker entrano nella pagina personale e chiamano telefonicamente il soggetto, dicendo in diretta:" Signor* tal dei tali stiamo aggiornando i dati. Le dovrebbe essere arrivato un codice sul telefonino, potrebbe darcelo per aggiornare i sistemi?".

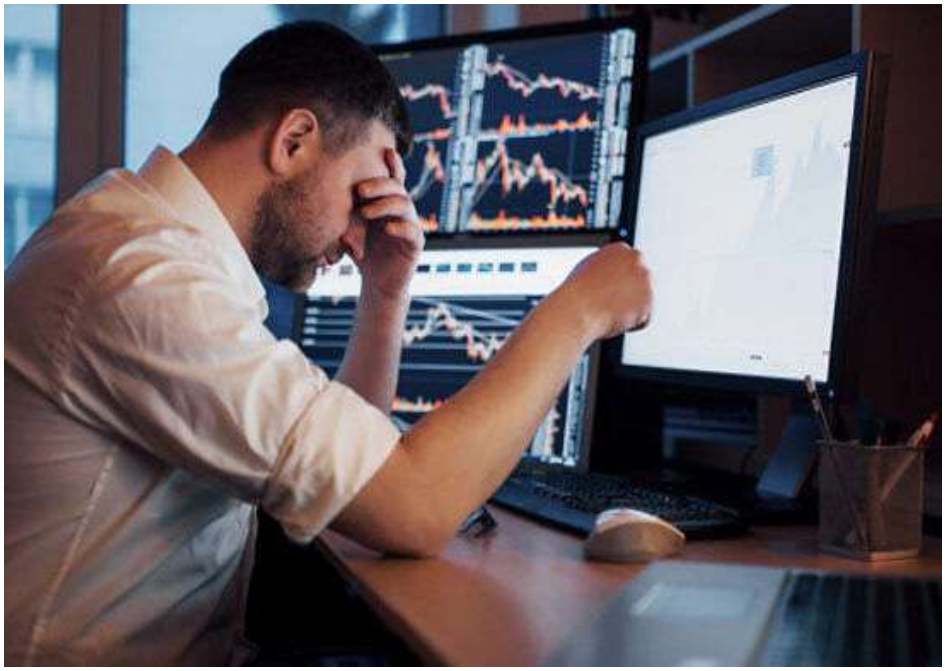
Quello che il soggetto truffato darà, equivale al codice dispositivo. Nel mentre i truffatori avranno

già impostato un bonifico da fare all'estero e con il codice datogli dal soggetto truffato, il passaggio di denaro verso filiale estera non individuabile sarà immediato. Il soggetto si accorgerà della truffa dopo diverse ore o giorni.

Cosa è lo smishing?

Lo "smishing" è un tipo di sistema che viene effettuato attraverso l'acquisto di software che camuffano il numero reale chiamante, facendolo apparire come un numero appartenente ad una grossa società o ad una banca. I software acquistati per questa truffa servono per cambiare sia l'intestazione che la residenza del chiamante.

Ma c'è una truffa che noi riteniamo la più pericolosa perché sta avvenendo su larga scala è che noi chiamiamo "men in the middle". Qui si parla di truffe veramente corpose, ci si aggira intorno ai milioni di euro. Prendiamo per esempio una grossissima azienda "X" che vende e una grossissima azienda "Y" che acquista, come potrebbe essere un grosso marchio automobilistico che compra un treno di gomme da un altrettanto grande azienda di pneumatici. I contatti possono avvenire attraverso dei Domini di posta privati, alcune volte pubblici o personali. Accade che chi deve acquistare il treno di gomme, comunica con la società fornitrice già da tempo con email. Arriverà uno specifico giorno in cui gli verrà effettuata una richiesta di 15milioni di euro di gomme entro tot giorni. Il tutto viene effettuato attraverso questi account di posta elettronica "non certificata", cioè account che non sono PEC e non sono criptati, ma semplici account di posta elettronica, dove serve semplicemente inserire nome utente e password



Cosa accade nel momento in cui l'azienda X fa una richiesta di un certo tipo all'azienda Y?

Accade quindi che queste email non criptate siano prese di mira da hacker che attraverso determinati software fanno girare la ricerca della password (a volte anche per giorni) fino a trovarla. A questo punto, avendo il nickname, la mail e la password riusciranno a comunicare da un qualsiasi luogo del globo spacciandosi per coloro che sono delegati alla vendita e/o alla parte economica e commerciale dell'azienda, controllando le mail che arrivano. E' così che iniziano lo studio di questi grossi personaggi che contrattano attraverso le email. Una volta inquadrati i soggetti, nel momento in cui arriva la richiesta dell'azienda "X" di voler comprare un treno di gomme per un valore di 15milioni di euro (ed è accaduto) la truffa si compie.

Nello specifico cosa accade?

L'azienda "X" chiede per il valore dell'importo un treno di gomme per l'Asia. A questo punto l'interlocutore principale rimanda ad un secondo interlocutore. Il truffatore che intercetta la mail in uscita, si appropria dell'account rispondendo a nome del secondo soggetto chiamato in causa. Il truffatore risponderà come fosse il soggetto addetto alla vendita, ma la sua mail differirà dall'originale per un semplice punto, un underscore, una lettera, una vocale, ma non desterà sospetto, convincendo chi acquista di essere in contatto con il soggetto deputato alla vendita. Durante lo scambio di email accade che il soggetto truffatore dica di non inviare l'importo del pagamento sul solito IBAN ma di inviarlo su un altro conto, spiegando che per problemi tecnici bancari ci si appoggia momentaneamente su un'altra banca, per esempio in Lituania. A quel punto, la truffa sarà compiuta, e quei 15 milioni di euro saranno spariti nel nulla.

Questo sistema serve per bucare non solo il sistema di compravendita delle grosse aziende ma anche a bucare il sistema interno dell'azienda stessa perché studiando i vari soggetti. Si possono inviare delle email all'interno dell'azienda stessa, dove il falso CEO scrive ad un suo sottoposto dicendo che c'è un acquisto in atto, di non parlarne con nessuno e di effettuare l'acquisto. Il soggetto che riceve la mail dal CEO non la mette in dubbio e quindi procede all'acquisto bucando anche internamente l'azienda e facendo perdere il capitale.

Che consigli possiamo dare?

Il consiglio che la Polizia postale lascia e di effettuare determinati tipi di comunicazione solo ed esclusivamente attraverso mail criptate con sistemi di sicurezza o pec. Inoltre sarebbe opportuno chiedere conferma attraverso altro canale precedentemente utilizzato, per qualsiasi cambiamento di IBAN o dati anagrafici ecc.

Ricapitolando le 3 truffe nuove sono: le fake trading on-line, lo smishing e il man in the middle.

Per il trading online i soggetti sono multipli soprattutto anziani o professionisti intenzionati ad investire per guadagnare qualcosa di più. Con lo smishing ci cascano tutti indifferentemente. Con la truffa man-in-the-middle invece i soggetti colpiti sono grossissime società multinazionali con portafogli che trattano centinaia di migliaia o milioni di euro.