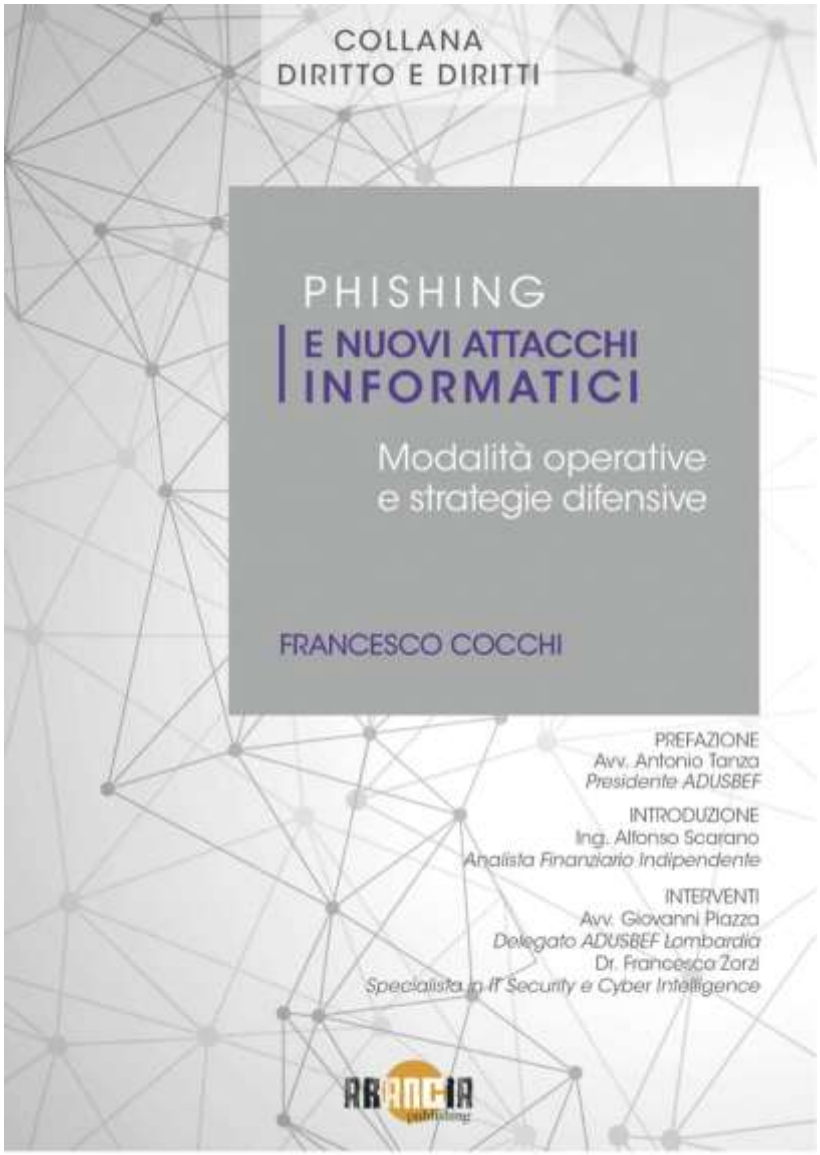
RISPARMIO & FUTURO



Sede Nazionale ADUSBEF, via Bachelet n. 12, p. 1° - 00185 - ROMA

Mensile anno XXXIV– N°8- 1° Agosto 2022

Sped. in abb. Postale DL 353/2003 (Conv. in L. 27/02/2004 n° 46) art. 1 comma 1 DCB Roma

La rivista è finanziata con i contributi pubblici all'editoria e con altri finanziamenti pubblici.

RISPARMIO & FUTURO prodotto e distribuito da ADUSBEF APS

TRASPARENZA INFORMAZIONE CERTEZZA DEL DIRITTO NELLA CONTRATTAZIONE

Anno XXXIV – N° 8 - AGOSTO 2022

Periodico d'informazione
Direttore Responsabile Sen. Dott. Elio Lannutti, Presidente Onorario di ADUSBEF ETS
Amministrazione, Redazione: Via Bachelet n. 12, 00185 ROMA
Stampa: Corso porta Luce n. 20, 73013, Galatina (LE)
Autorizzazione del Tribunale di Roma N° 299 del 18 maggio 1988
Abbonamenti: Ordinario € 23 euro; Sostenitore € 100 e oltre.
Versamenti su **conto corrente postale** IBAN: IT74S0760103200000070043005 oppure su **conto corrente bancario** presso Monte dei Paschi di Siena IBAN: IT35Q 01030 03204 000001471949, sempre intestato ad Adusbef.
Redazione: Antonio Tanza - Fabio Massimo Blasi - Mauro Novelli – Federico Novelli - Rosalba Di Placido - Donato Surano - Salvatore Ruberti - Mario Fasano - - Giuseppe Palamà - Tania Saracino - Patrizia Rossetti - Luisa Frassanito - Filomena Cosentino - Daniele Imbò - Olga Tanza - Vincenzo Laudadio.
Corrispondenti: Giuseppe Angiuli (BA); Orazio Isidoro Scuro (BA); Angela Dell'Aquila (BR); Paola Licia Follieri (FG); Raffaele Rutigliano (FG); Giuseppe Sbriglio (AO); Lucia Monacis (TO); Anna Patisso; (TO) Daniele Folino (VB); Andrea Sella (BI); Giovanni Piazza (MI); Caterina La Sala (MI);Fulvio Cavallari (PD); Sveva Rossi (PD);Manuela Spada (RO); Monica Spada (Vi);Emanuela Marsan (VI); Camilla Cusumano (VR); Emanuela Bellini (VR); Paola Formica (MC); Daniela Rossi (AP); Paolo Polato (TN); Federico Capalozza (UD); Patrizia Monferrino (GE); Anna Maria Patisso (GE); Grazia Angelucci (BO); Alberto Basaglia (RA); Giulio Caselli (FI); **Lorenzo De Cesaris (GR);** Fabrizio Mirko (LU); Andrea Frosini (PO); Floro Bisello (PU); Silvia Surano (PG); Riccardo Falocco (TR); Alessandra Di Sarno (RM); Fiammetta Fiammeri (RM); Massimo Campanella (RM); Giuliano Forlani (RM); Maria Elena Catelli (FR); Carlo delle Site (RM); Angelo Turriziani (RM); Antonio Serafini (Rm); Veronica Mattei (RM); Maria Rita Di Giambattista (PE); Doriana Pescara (CB); Monica Cirillo (NA); Ivan Lambiasi (SA) Maria Teresa De Bottis (CE); Vittoria Marzioni (PZ); Felice Belisario (PZ); Elena Mancuso (CZ); Lucia Cittadino (CZ); Fernando Scarpelli (CS); Angela Blando (PA)**;** Giorgio Panzeca (PA); Elisabetta Freni (CT); Marianna Orlando (ME); Nicola Marchese (ME); Serena Lazzaro (SR); Guenda Pili (CA); Alberto Marongiu (OR); Antonino Siffu (SS); Elisabetta Cristiani (MI); Cristiano Aretusi (TE); Antonio Stagnaro (GE) Jessica Cosseta (CU);

Sommario del n° 8 – AGOSTO 2022

Estratto dall'ultima pubblicazione Studi ADUSBEF:

"PHISHING
E NUOVI ATTACCHI INFORMATICI"

dell'Avv. Francesco COCCHI, Delegato Adusbef di Firenze

Acquistabile su AMAZON:
https://www.amazon.it/Phishing-informatici-operative-strategie-difensive/dp/8894863069/ref=sr_1_3?crid=2VK8EADATSII2&keywords=phishing+cocchi&qid=1657274750&sprefix=cocchi+p%2Caps%2C122&sr=8-3

3.3 Il successo del nuovo spear phishing: il fattore umano

Il contesto operativo del nuovo spear phishing mostra uno scenario di attacco estremamente complesso, legato in parte alla sua impercettibilità dovuta all'impiego di tecniche di spoofing ed in parte all'impiego di tecniche di hacking capaci di sfruttare sia tecniche di comunicazione avanzate che di manipolazione psicologica. Un aspetto che si manifesta nella fase dell'attacco relativa al contatto telefonico, utile a indurre la vittima a compiere l'azione richiesta con il precedente invio dell'sms.

Non vi è dubbio, infatti, che proprio il contatto telefonico abbia la capacità di superare le ultime resistenze dell'interlocutore dinanzi alla falsa notizia di una violazione nella sicurezza del suo conto corrente, conferendo all'attacco una maggiore credibilità.

Pare proficuo, quindi, indagare i meccanismi emotivi in base ai quali il contributo di tali tecniche di comunicazione sia capace di conferire maggiore possibilità di successo alla frode informatica in esame.

Diversamente dai precedenti schemi di phishing attacks, in quello che abbiamo definito nuovo spear phishing vi è la combinazione di diverse tecniche di hacking che si avvalgono anche di un colloquio strutturato con la vittima, grazie ad una preventiva raccolta di dati su di essa proprio secondo il classico paradigma dello spear phishing.

Sebbene la conoscenza di informazioni, come il numero di utenza cellulare ed il suo collegamento ad un account bancario, unitamente all'impiego di tecniche di spoofing, siano elementi in grado di indurre nella vittima un fondato timore verso la falsa notizia di un attacco informatico che può danneggiare le proprie finanze, è pur vero che sarebbe riduttivo attribuire la capacità di successo registrata dal nuovo attacco in esame soltanto a tali elementi.

Non vi è dubbio, infatti, che anche il colloquio che l'hacker inscena fingendosi un (falso) operatore dell'intermediario rivesta un notevole rilievo nella frode poichè capace di innescare nella vittima la volontà di seguire le istruzioni ricevute per la soluzione del falso problema.

Gli elementi che, pertanto, devono essere indagati sono meccanismi psicologici sfruttati da queste nuove tecniche di hacking anche al fine di comprendere se vi possano essere potenziali controffensive che la vittima può opporre ad essi.

Comprendere tali dinamiche potrebbe, inoltre, fornire anche una chiave di lettura del nuovo attacco spear phishing utile soprattutto a disinnescare eventuali comportamenti automatici che la vittima pone in essere dinanzi ad una situazione di pericolo. Come già accennato, infatti, il buon esito di un attacco informatico è

determinato dalla risposta della vittima a stimoli ben calibrati e veicolati dall'hacker, che si prefigge come unico obiettivo quello di convincere la vittima a compiere le azioni da lui richieste. Per raggiungere tale obiettivo e carpire dati e informazioni riservate l'attaccante deve prima di tutto conquistare la fiducia del suo interlocutore affinchè vi sia un naturale abbassamento della soglia attentiva nella vittima cui farà seguito, poi, il compimento di una serie di azioni di impulso dinanzi agli stimoli dell'hacker. Un risultato che può essere raggiunto con l'impiego di tecniche comunicative capaci di fare leva proprio sulla volontà della vittima.

Ne discende che l'analisi deve essere indirizzata soprattutto al processo decisionale che ogni individuo innesca nel momento in cui interagisce con gli altri individui e l'eventualità che in un simile contesto vi sia la possibilità di controllare e guidare la volontà del nostro interlocutore.

Il contesto nel quale tali dinamiche operano è quello della comunicazione, all'interno della quale due soggetti si scambiano informazioni in un determinato intreccio comunicativo. Comunicare, infatti, "significa, letteralmente, mettere in comune. Si può mettere in comune informazione quando sono presenti almeno due entità: una fonte e un destinatario".

I soggetti coinvolti nello sketch comunicativo risentiranno anche del contesto nel quale la comunicazione si svolge, che potrà influenzare la comunicazione stessa, unitamente ad altri fattori.

All'interno di un processo comunicativo vi sono, inoltre, ulteriori elementi in grado di influenzare le nostre decisioni durante l'interazione con l'altro, che non sempre sono frutto di lunghe elucubrazioni ma che anzi, spesso, si affidano a risposte e comportamenti stereotipati, più semplici da attuare. Sarebbe, infatti, estremamente faticoso per la nostra mente innescare lunghi processi decisionali nella vita di ogni giorno nel tentativo di controllare tutti gli elementi di una questione ed assumere decisioni a riguardo dopo lunghe riflessioni.

Al contrario, come autorevolmente affermato da Robert B. Cialdini, nell'assumere delle scelte spesso la nostra mente si affida a "scorciatoie" utili ad assumere decisioni in un minore tempo all'interno di un contesto complesso e ricco di continui stimoli. Questo dettaglio diviene determinante se lo si pone in relazione con gli obiettivi che l'hacker si prefigge nel compimento di un attacco: ottenere la fiducia della vittima ed indurla il più possibile a non riflettere affinché assuma decisioni di impeto. Tale considerazione sembra tracciare il perimetro del problema in esame e cioè il perché un attacco informatico può essere portato a termine con successo. Se, infatti, la nostra mente non sempre compie lunghi processi decisionali ma anzi si affida comportamenti stereotipati per assumere decisioni più efficienti secondo schemi predefiniti, proprio in tali processi mentali può risiedere una possibile vulnerabilità del nostro comportamento che può essere abilmente sfruttata dall'hacker che, da profondo conoscitore e osservatore della natura umana, è certamente capace di utilizzare le reazioni spontanee del suo interlocutore a proprio vantaggio.

I comportamenti stereotipati o automatici sono condotte che si rivelano certamente utili nella vita poiché capaci di risparmiare all'individuo l'esame di ogni fattore che influenza una determinata situazione all'interno della quale assumere decisioni. I copioni con cui, invece, stereotipiamo le nostre risposte davanti a determinate situazioni ci permettono di avere una reattività maggiore nel processo decisionale e nella interazione con gli altri, sebbene, possano nascondersi in essi più di una insidia. Può infatti accadere che la scelta così assunta non sia la migliore, sebbene in ogni caso ne accettiamo gli esiti.

Sono questi i fattori che, quindi, possono indurci a reagire assumendo un contegno del tutto prevedibile per il nostro interlocutore al quale basterà stimolare tali reazioni per ottenere una risposta già ipotizzabile e quindi innescare con semplicità un processo di persuasione.

Tali reazioni stereotipate, definite da Robert B. Cialdini come "armi di persuasione automatica", hanno dei comuni elementi che consistono in un automatismo meccanico di attivazione che rende possibile il loro sfruttamento da parte di chi le utilizza con semplicità e senza sforzi poiché sarà sufficiente "far scattare le molle potenti che già sono contenute nella situazione".

Queste risposte automatiche, quindi, potranno essere sfruttate dal nostro interlocutore con il minimo sforzo per manipolarci.

I principali fattori che dominano la persuasione sono individuati da Robert B. Cialdini nei seguenti elementi: la reciprocità, coerenza, riprova sociale, simpatia, autorità e scarsità. Questi fattori, quindi, dominano quei meccanismi in grado di innescare in noi una propensione ad accondiscendere le richieste del nostro interlocutore automaticamente.

Una propensione che certamente può essere sfruttata dall'hacker all'interno di un attacco.

Esaminandoli brevemente vediamo che il fattore della reciprocità fa riferimento a quel sentimento di innata gratitudine che dimostriamo dinanzi ad una cortesia inattesa e non richiesta usataci da una persona. Questo dono inatteso e, soprattutto, apparentemente privo di ragioni evidenti è capace di liberare in chi lo riceve un meccanismo di "debito" che lo induce a contraccambiare il dono. Un meccanismo che agevola la contrazione di "debiti non richiesti", ma che ci sentiamo in obbligo di soddisfare.

Sentirsi in debito con qualcuno per una cortesia ricevuta può quindi indurci a compiere azioni senza valutare che le stesse ci siano state imposte.

Altro principio che ben si coordina con il principio di reciprocità è quello della coerenza, secondo il quale gli individui tendono a rimanere (automaticamente) coerenti con un'azione compiuta o con gli impegni assunti verso altri.

Rimanere coerenti evita di dover riflettere costantemente sulle decisioni, aprendo facili scorciatoie di pensiero che evitano così di ragionare approfonditamente sulle situazioni che si configurano volta per volta. Se, quindi, in noi vi sono meccanismi che agevolano la possibile abitudine a rimanere coerente con impegni assunti, sarà sufficiente far assumere

un impegno al nostro interlocutore per sfruttare la sua naturale tendenza a rimanervi coerente. Al manipolatore sarà, pertanto, sufficiente farci impegnare al compimento di un atto da lui desiderato per ottenere il risultato voluto, poiché più assumiamo atteggiamenti incoerenti nelle nostre condotte e maggiore fatica farà il manipolatore a guidarci verso scelte a noi indesiderate.

Non deve, poi, essere sottovalutata la capacità di tali fattori di legarsi tra loro. Reciprocità e coerenza, infatti, possono interagire tra loro aumentando la risposta persuasiva nel soggetto che le subisce, poiché ricevuta una cortesia o un dono inaspettato saremo propensi a restituire quanto ricevuto sentendoci in debito. Accettato questo schema e scelto di "ripagare il debito contratto", saremo ulteriormente propensi a rimanere coerenti alla scelta assunta di ripagarlo.

In questo contesto entra in gioco anche l'ulteriore elemento dell'autorità, che si lega alla naturale deferenza che ogni individuo mostra verso l'autorità.

Se riconosciamo come autorevole il nostro interlocutore, sarà altamente probabile che si inneschi in noi il meccanismo automatico della accondiscendenza quale scelta utile nel processo comunicativo.

Evidenze empiriche hanno dimostrato che "obbediamo ciecamente alle richieste di una persona che riteniamo legittimamente abilitata a formularle", senza però interrogarci realmente sulle qualifiche della stessa.

Ancora una volta un automatismo che affidandosi a stereotipi non porta ad una approfondita riflessione sulle vere qualità del nostro interlocutore.

Proseguendo nell'analisi svolta da Cialdini troviamo la simpatia. E' infatti estremamente facile comprendere come si è più propensi ad essere accondiscendenti con una persona che ci è simpatica. Un interlocutore che ci appare gentile, che ha un buon eloquio, che è capace di mostrarsi sorridente ed in grado di evocare emozioni come l'allegria e la serenità, sarà in grado di farci cedere più facilmente alle sue richieste per una naturale inclinazione che manifestiamo verso le persone che identifichiamo come brillanti.

Vi è poi la riprova sociale, un ulteriore elemento che sfrutta la necessità di sentirci parte di un gruppo e di essere accettati dallo stesso. Ciò potrà condurci a non riflettere sulla correttezza o meno di un pensiero poiché seguire un gruppo renderà certamente più facile la scelta da assumere. Così come la naturale tendenza ad essere attratti da ciò che è raro (rarità), l'ultimo fattore in grado di influenzare le nostre scelte, poiché la scarsa disponibilità di un bene può far nascere in noi la sensazione di perdere una occasione dinanzi all'offerta di poterlo avere.

L'influenza che questi fattori possono esercitare sulle nostre scelte e sui nostri comportamenti mostra la vulnerabilità cui siamo esposti davanti a soggetti in grado di sfruttare tali strumenti per i propri fini.

E' possibile, infatti, rinvenire nel nuovo attacco spear phishing qui in esame la presenza di alcuni elementi descritti quali la reciprocità, la coerenza, l'autorevolezza ed anche la simpatia, intesa in termini di gentilezza.

Riepilogando brevemente il paradigma di attacco, ricordiamo che il nuovo spear phishing si compone di un attacco con sms spoofing al suo inizio, rinforzato poi da un contatto telefonico sempre sull'utenza cellulare collegata al servizio di home banking.

Lo schema esecutivo dell'attacco mette in luce la centralità del colloquio telefonico e l'impiego in esso di tecniche manipolative al fine di indurre la vittima a cedere dati riservati.

Tornando alle tecniche di persuasione descritte possiamo rinvenire proprio nella fase iniziale di tale contatto telefonico l'impiego del fattore della reciprocità. Infatti, subito dopo aver allarmato con un sms la propria vittima, l'attaccante fingendosi un operatore del servizio clienti o di altro servizio dell'intermediario, offrirà un aiuto tempestivo alla soluzione del problema.

L'aiuto, tempestivo e non richiesto, che verrà offerto dal falso operatore apparirà alla vittima certamente come una cortesia capace al contempo di rendere più credibile la falsa allerta creata dall'sms ricevuto, e innescare in quest'ultima un "debito" contratto per l'aiuto ricevuto.

Non può essere sottovalutata in un simile scenario la sensazione di ansia che le due comunicazioni via sms e telefonica faranno sorgere nella vittima.

Tali contatti sono capaci di far sorgere timore e disagio nel soggetto attaccato e generare in lui uno stato emotivo ansioso che come autorevolmente affermato può essere così definito: "ciò che definiamo ansia è un insieme di reazione cognitive, emotive, fisiologiche e comportamentali che costituiscono una forma importante di adattamento dell'organismo all'ambiente" .

L'ansia può quindi essere una risorsa per l'hacker poiché davanti ad un pericolo la componente cognitiva del soggetto attaccato valuterà le possibili minacce e gli opportuni correttivi.

Se, quindi, la comunicazione tramite un sms camuffato e quindi credibile, innesca una sensazione di timore in chi lo riceve, l'offerta di un aiuto inatteso e tempestivo, quale quello che viene offerto dal falso operatore, innescherà una "molla" reattiva di gratitudine, tipica del meccanismo della reciprocità. Proprio la sensazione di aver contratto un "debito di gratitudine" da "ripagare" (secondo il principio di reciprocità), innescherà nella vittima, una volta percepita tale reazione emotiva, la successiva ulteriore "molla automatica" della coerenza, con l'effetto che la vittima seguirà le istruzioni ricevute dal sedicente operatore avendone accettato il ruolo ed essendo grata per l'aiuto.

Un'ulteriore influenza sarà esercitata, poi, dal fattore della autorevelezza, agevolata dalla presentazione dell'hacker durante il colloquio telefonico come un operatore del servizio clienti e del servizio antifrode. Innescati i meccanismi di reciprocità e coerenza, sarà probabile che l'esigenza di verificare la concreta autorevolezza e le professate qualità dell'interlocutore sfumi del tutto nella mente del soggetto attaccato. Ciò sempre per l'ulteriore "pensiero automatico" di non mettere in discussione l'autorità di un interlocutore che si presenta come tale.

Infine, ma non per ordine di importanza, un dialogo ben strutturato con all'interno termini tecnici e privo di accenti, se posto con modalità cortesi e toni simpatici farà definitivamente abbassare ogni difesa alla vittima, confermando anche la presunta autorevolezza già automaticamente conferita al falso operatore.

Non dobbiamo dimenticare che il contatto telefonico che tipizza il nuovo spear phishing ha solitamente una numerazione apparentemente coerente con il servizio clienti dell'intermediario impersonificato dall'hacker, elemento che conferisce ancor più autorità al falso operatore.

Dalla ricostruzione sin qui formulata è possibile concludere come la struttura di contatto vishing con la vittima, impiegata dal nuovo attacco di spear phishing, sfrutti tecniche persuasive in grado di manipolare la volontà dell'interlocutore.

Abbandonate, quindi, le classiche tecniche di inganno tipiche del deceptive phishing che mirano a ingannare grossolanamente la vittima, il nuovo spear phishing si avvale di efficaci tecniche human hacking soprattutto capaci di sfruttare quei comportamenti automatici posti in essere dalla nostra mente dinanzi a determinati stimoli o contesti. Con il chiaro effetto, così, di aumentare la propensione ad automatismi di pensiero e decisioni di impulso, poiché la paura o l'ansia legata alla notizia di violazione dei servizi di pagamento ricevuta indurrà la vittima a decisioni rapide necessarie ad allontanare la sgradevole sensazione prodotta da simili emozioni negative.

E' importante, in ogni caso, avere presente come le tecniche di ingegneria sociale che danno inizio ad un attacco complesso come quello in esame, sfruttano quei comportamenti stereotipati che, però, possono essere anche controllati qualora l'interlocutore sia in grado di riconoscere gli stimoli che li fanno "scattare".

Una prima importante difesa verso un attacco manipolativo o persuasivo può essere ricondotto alla ritrosia verso gentilezze o aiuti che non abbiamo richiesto.

Una difesa che però appare difficilmente attuabile nell'attacco informatico qui in esame che, diversamente dal classico phishing e dalle sue varianti, non impiega semplici messaggi di allarme, ma una struttura di attacco capace di instillare timore e paura con molteplici tecniche di social engineering tra loro coordinate unitamente a tecniche di human hacking.

La diade avviso di pericolo con sms spoofing e conferma del problema con contatto telefonico di vishing, non solo sarà capace di sfruttare questi comportamenti stereotipati e automatici descritti, ma anche di generare nel soggetto colpito una elevata percezione del problema comunicato come vero. Circostanza che poi lo indurrà ad accondiscendere anche alle ulteriori richieste che l'attaccante gli formulerà durante l'attacco. Tale ultimo aspetto conferma la capacità del nuovo spear phishing di massimizzare il profitto generato dalla previa conoscenza da parte dell'hacker di dati della vittima (come ad esempio il numero di utenza cellulare), anche grazie all'impiego di tecnologie come lo

spoofing. L'ulteriore determinante punto di forza del suo successo è il "fattore umano" e la capacità di manipolazione della volontà della vittima resa possibile attraverso l'impiego delle tecniche di comunicazioni descritte all'interno di un contesto di timore per la vittima accuratamente costruito e sfruttato.

3.4. Il fattore umano nel cybercrime: tecniche di persuasioni e induzione all'azione richiesta dall'hacker

Dall'esame dei fattori che possono influenzare i nostri comportamenti abbiamo potuto constatare come non sempre sia necessario costruire articolati schemi comunicativi per indurre una persona ad un determinato comportamento in quanto, davanti a determinati stimoli, è semplicemente sufficiente sfruttare la situazione che abbiamo davanti e le reazioni "automatiche" del nostro interlocutore agli stessi; reazioni che possono essere controllate dal manipolatore poiché la manipolazione consiste "nell'esercitare "con delicatezza" un dominio su un'altra persona".

Non vi è, dunque, la necessità di forzare la volontà altrui per ottenere la risposta desiderata, in quanto sarà sufficiente accompagnare il nostro interlocutore verso il nostro obiettivo non solo sfruttando le sue "strutture automatiche di pensiero", ma anche e soprattutto influenzandolo mediante l'esercizio di pressioni per così dire "leggere". L'interlocutore, infatti, non dovrà mai avere la percezione di obbedire ad un comando del manipolare, ma anzi dovrà sentire in sé che le azioni che andrà a compiere siano frutto di una propria ed autonoma decisione.

Per giungere ad un simile risultato il manipolatore non solo dovrà sfruttare precise tecniche di comunicazione, ma dovrà soprattutto sfruttare il fattore umano, cioè l'insieme di reazioni emotive e sensazioni che si manifesteranno come reazione alle sollecitazioni inviate all'interlocutore.

Sarà quindi necessario calibrare e prevedere le reazioni dell'interlocutore preservando la sensazione in lui di stare agendo in piena libertà secondo la propria intenzione.

In tale tessuto comunicativo avranno infatti maggiore successo quegli schemi argomentativi che permetteranno di mantenere viva tale percezione nel destinatario della comunicazione.

E' opportuno esaminare, pertanto, se vi siano precise tecniche manipolative in grado di sfruttare tale falsa percezione del manipolato. Può essere infatti creata nel nostro interlocutore la percezione di voler compiere un'azione e di essere libero di effettuarla chiedendogli semplicemente quando la farà, con la conseguenza di dare già per scontato che quanto richiestogli sarà certamente da lui eseguito. La domanda contenuta in una simile tecnica argomentativa, infatti, non mette mai in discussione che una certa azione sarà compiuta o che un evento avrà luogo, in quando semplicemente pone una falsa alternativa all'interlocutore che ha come oggetto soltanto il momento che da lui sarà scelto per porla in essere.

È possibile, poi, cercare di ottenere una determinata cosa da un'altra persona attraverso la tecnica della

"richiesta minima" che sfrutta la generosità altrui stimolata proprio da una piccola richiesta iniziale che indurrà il manipolato a concedere via via sempre di più. Ed infatti, dinanzi ad una piccola ed iniqua richiesta, come ad esempio il dono di una minima somma di denaro, si è propensi a donarne una maggiore poiché viene stimolata la naturale propensione dell'individuo alla generosità. Diversamente, può invece essere impiegato l'opposto schema di richieste incessanti e continue, partendo prima da richieste minime per poi accrescerle col tempo.

Tale meccanismo sfrutta, invece, la concessione iniziale che l'interlocutore accorda al manipolatore per poi farlo rimanere fedele alla decisione iniziale assunta ed ottenere da lui molto di più.

Infine, è possibile muovere da tutt'altro presupposto e formulare richieste iniziali assurde e sproporzionate, col rischio di far saltare una negoziazione, per poi procedere con richieste più ragionevoli in seguito, che però saranno percepite dal manipolato come un risultato, positivo, alle proprie iniziali resistenze.

Gli stratagemmi comunicativi descritti hanno il pregio di conservare intatta nel soggetto che ne cade vittima la percezione di tenere una condotta frutto di una propria scelta.

Un'abilità, quella descritta, che senza dubbio risulta capace di ingannare l'attenzione del manipolato impedendogli di rendersi tempestivamente conto di quanto sta accadendo.

Tale aspetto deve, quindi, essere valorizzato anche all'interno dei nuovi attacchi informatici e soprattutto all'interno di quello che abbiamo definito il nuovo spear phishing, in quanto capace di sommare all'interno di esso un nuovo determinante fattore di successo: l'human hacking.

Questo nuova modalità di hacking risulta, come detto, capace di sfruttare l'insieme delle reazioni umane, consapevoli o meno, con la conseguente fuoriuscita dei colloqui costruiti attraverso di esso dallo schema classico del vishing verso una diversa e più pervasiva forma di induzione verbale della vittima, capace di manipolare la sua volontà con maggiore facilità.

Una caratteristica, quella descritta, che deve quindi essere esaminata proprio nella sua maggiore efficacia decettiva. In particolare, l'aspetto che deve maggiormente essere considerato è quello della costruzione del colloquio attraverso tecniche comunicative che, come descritto, risultano altamente efficaci nello sfruttare reazioni automatiche e "scorciatoie" decisionali dinanzi ad una scelta da assumere.

Non vi è dubbio, infatti, che tali tecniche siano presenti nel nuovo attacco in esame e che siano combinate con tecniche di hacking di tipo informatico capaci di trarre in inganno la vittima con maggiore efficacia, quali ad esempio lo spoofing.

Ciò porta a concludere che l'human hacking unitamente alle tecniche di hacking di tipo informatico, sono in grado di dare vita ad una nuova e diversa forma di social engineering capace di indurre in errore la vittima con maggiore efficacia all'interno di scenari di attacco sempre più credibili. Tale considerazione porta la riflessione verso un possibile parallelismo tra nuove tecniche di human hacking e software malevoli al fine di poter

stabilire una pari efficacia sotto il profilo della loro assoluta impercettibilità per la vittima.

Come già accennato, infatti, l'elemento della impercettibilità è stato valutato dalla giurisprudenza dell'Arbitro Bancario che, chiamato a valutare la presenza di profili di colpa grave nella condotta della vittima di attacco informatico, ha rilevato come in alcuni casi gli elementi che lo caratterizzavano erano da tali da rendere assolutamente impercettibile la truffa grazie all'impiego di malware sofisticati in grado di ingannare anche l'utente più accorto.

L'aspetto della impercettibilità è, pertanto, valutato secondo l'aspetto della materiale impossibilità per la vittima di avvedersi tempestivamente dell'inganno. Un'impossibilità agevolata anche dall'impiego di software malevoli in grado di rappresentare una falsa realtà informatica alla vittima talmente efficace da non far sorgere in lei alcun dubbio sulla autenticità di quanto le viene richiesto.

Muovendo da tale presupposto è forse possibile tentare di mettere in correlazione artifici informatici ed artifici comunicativi-manipolativi quali quelli esaminati, propri del nuovo spear phishing.

Se, infatti, l'impercettibilità può essere una qualità riferibile ad un inganno informatico particolarmente efficace, frutto ad esempio di un malware capace di creare un contesto di frode credibile, tale qualità può essere riferita anche alle tecniche di human hacking esaminate. Emerge, anzi, una loro maggiore efficacia in termini di reazione da parte di chi le subisce poiché, ricordiamolo, sfruttano le c.d. "molle automatiche" del nostro pensiero.

Il concetto di impercettibilità può quindi essere ricostruito come un fattore capace di ingannare l'ideazione del soggetto attaccato attraverso una efficace alterazione della realtà che non permette la tempestiva analisi del quadro di insieme degli elementi presenti in essa e dell'inganno sottostante. Tali caratteristiche possono quindi essere rinvenute, in tesi, sia in uno scenario creato da un malware che in altro creato da un fattore psicologico-persuasivo tipico delle tecniche di human hacking esaminate.

La vicinanza di questi fattori induce ad esaminare un nuovo aspetto della impercettibilità della truffa informatica, che deve essere approfondito in relazione ai singoli scenari di frode costruiti volta per volta dall'hacker e nei quali l'utente di servizi di pagamento cade vittima. Con la ulteriore conseguenza di porre in essere un avvicinamento sul piano pratico delle tecniche di hacking informatico e di human hacking proprio sotto il profilo della impercettibilità, valorizzato proprio nella giurisprudenza dell'Arbitro Bancario Finanziario.

Avv. Francesco COCCHI
Delegato Firenze

FOREX - TRADING ON LINE: il Tribunale di Padova accoglie la richiesta di chiamare nel processo penale la banca depositaria.

Con una recente decisione significativa, il Tribunale di Padova conferma la decisione in accoglimento della richiesta della parti civili costituitesi con l'**avv. Marilena Bertocco** del Foro di Padova e **delegata Adusbef,** di mantenere la presenza della banca depositaria nel processo penale pendente a carico di un ex consulente finanziario, imputato per abusivismo e truffa e radiato dalla Consob dall'albo unico dei consulenti finanziari per tali fatti nel 2017, a seguito del reclamo presentato nell'interesse delle persone offese, dall'**avv. Anna Lorenzi** del Foro di Padova e **delegata Adusbef Padova**.

I fatti risalgono al 2012 e si sono protratti sino al 2015, quando, la persona offesa scopriva che, a sua insaputa, il predetto consulente offriva fuori sede servizi di investimento cd Forex, di una società svizzera non autorizzata sul territorio italiano, gestendo così i suoi risparmi attraverso la piattaforma di trading on line della banca depositaria Saxo Bank sa con succursale a Milano.

Ed ecco quindi che il Tribunale di Padova, a fronte della opposizione del legale della Banca, ha invece imposto la presenza di Saxo Bank in qualità di terzo responsabile, a seguito di accoglimento della richiesta del difensore delle parti civili, avv. Marilena Bertocco perchè possa rispondere a titolo di responsabilità oggettiva e solidale per dei danni causati anche dalla perdita dei risparmi investiti.

ll Giudice patavino apre perciò la via in ambito penale a questo nuovo filone: detta decisione costituisce infatti una possibilità per gli investitori, vittime di truffe nel settore forex e trading on line, di chiamare a rispondere per il volatilizzarsi delle somme investite nella eventuale "mala gestio" su tale, tanto dinamico quanto rischioso, mercato anche gli operatori professionali cd "Forex broker", attraverso le cui piattaforme di trading on line permettono di effettuare le operazioni forex .

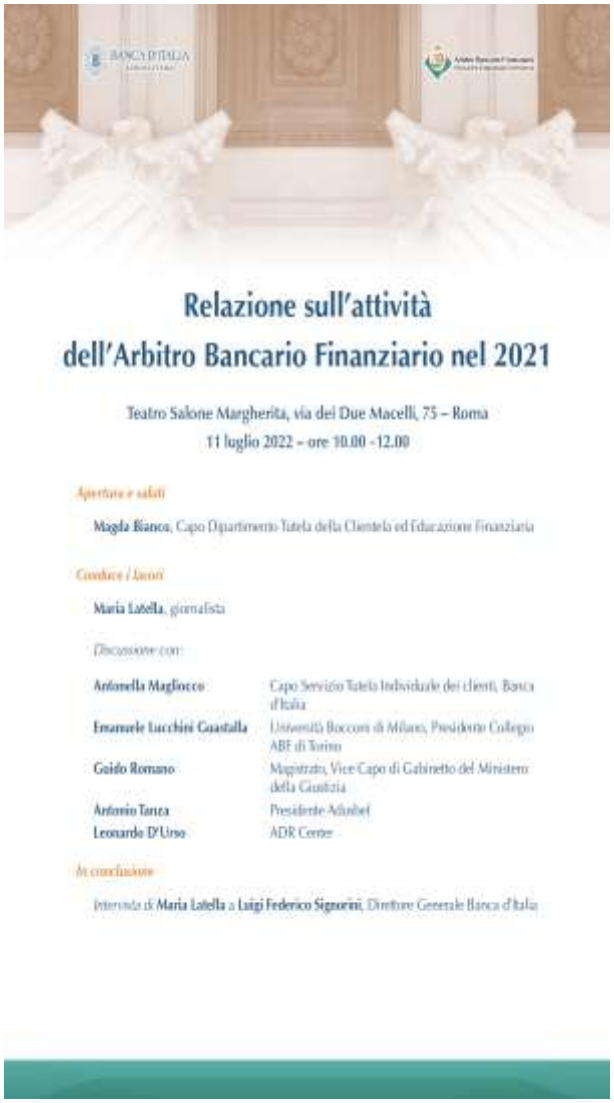
avv. Marilena BERTOCCO
Delegata Vicenza

avv. Anna LORENZI
delegata Padova

ATTIVITA' ADUSBEF del MESE di Luglio

11 luglio 2022

Relazione sull'attività dell'Arbitro Bancario Finanziario nel 2021



Relazione sull'attività
dell'Arbitro Bancario Finanziario nel 2021

Teatro Salone Margherita, via dei Due Macelli, 75 – Roma
11 luglio 2022 – ore 10.00 - 12.00

Apertura e saluti

Magda Bianco, Capo Dipartimento Tutela della Clientela ed Educazione Finanziaria

Conduce / Introduce

Maria Latella, giornalista

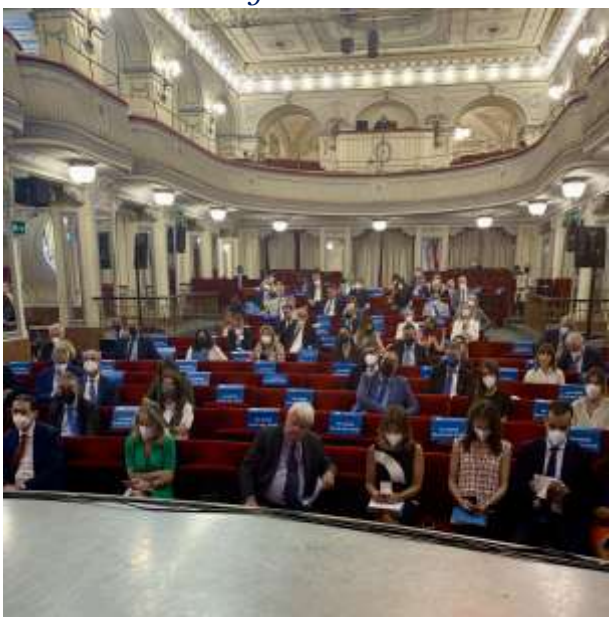
Discussione con:

Antonella Magliocco	Capo Servizio Tutela Individuale dei clienti, Banca d'Italia
Emanuele Lucchini Guastalla	Università Bocconi di Milano, Presidente Collegio ABF di Torino
Guido Romano	Magistrato, Vice Capo di Gabinetto del Ministero della Giustizia
Antonio Tanza	Presidente Adusbef
Leonardo D'Urso	ADR Center

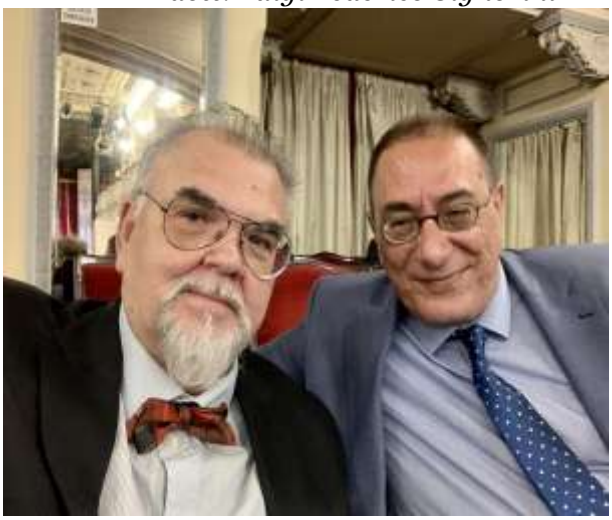
In conclusione

Intervista di Maria Latella a Luigi Federico Signorini, Direttore Generale Banca d'Italia

Leonardo D'Urso, Antonio Tanza, Guido Romano, Emanuele Lucchini Guastalla, Antonella Magliocco. Maria Latella.

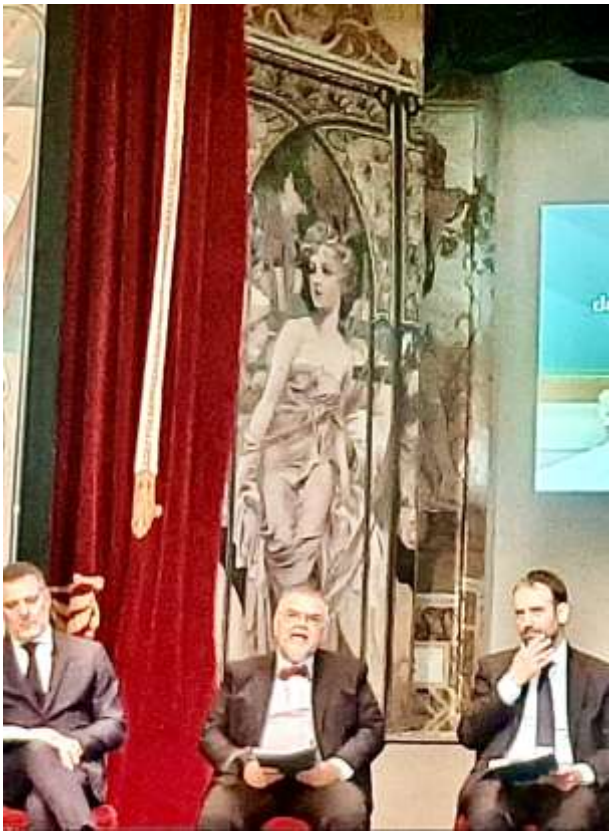


Prima fila al centro:
dott. Luigi Federico Signorini



Antonio Tanza e Massimo Campanella

Intervento di Magda Bianco



Intervento Presidente ADUSBEF

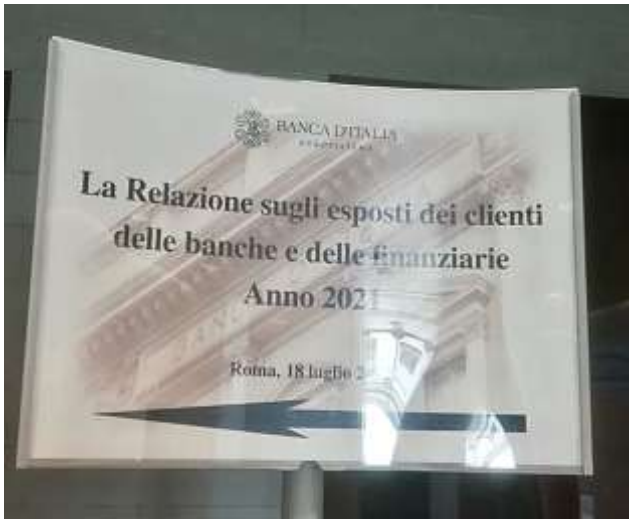
14 luglio 2022

Anteprima presentazione volume:
"PHISHING
E NUOVI ATTACCHI
INFORMATICI"

L'Avv. Francesco COCCHI,
Delegato Adusbef di Firenze

18 luglio 2022

Relazione sugli esposti dei clienti delle banche e delle finanziarie nel 2021



Per ADUSBEF presente
l'Avv. Massimo Campanella

Sostieni i consumatori, sostieni ADUSBEF!

Puoi sostenere ADUSBEF anche attraverso il 5 per 1000: in fase di dichiarazione, indica il **codice fiscale 03638881007**

*Per difendere meglio i tuoi diritti destina il **5 per mille** delle tue imposte a sostegno di **Adusbef**. Indica il codice fiscale della nostra associazione **0 3 6 3 8 8 8 1 0 0 7** sul modulo della denuncia dei redditi ed apponi la tua firma come sotto indicato:*

730 Agenzia Entrate

SOSTEGNO DEL VOLONTARIATO E DELLE ALTRE ORGANIZZAZIONI NON LUCRATIVE DI UTILITA' SOCIALE, DELLE ASSOCIAZIONI DI PROMOZIONE SOCIALE E DELLE ASSOCIAZIONI E FONDAZIONI RICONOSCIUTE CHE OPERANO NEI SETTORI DI CUI ALL'ART. 10, C. 1, LETT A), DEL D.LGS. N. 460 DEL 1997

FIRMA X .....

Codice fiscale del beneficiario (eventuale) | 0 | 3 | 6 | 3 | 8 | 8 | 8 | 1 | 0 | 0 | 7 |

TRAPARENZA, INFORMAZIONE e CERTEZZA DEL DIRITTO NELLA CONTRATTAZIONE

ASSOCIAZIONE DI PROMOZIONE SOCIALE (APS) -ENTE DEL TERZO SETTORE (ETS)

DAL MAGGIO 1987, ADUSBEF APS ETS COMBATTE ASPRE BATTAGLIE IN DIFESA DEI DIRITTI DEI CITTADINI IN OGNI SETTORE CONSUMERISTA ED È PARTICOLARMENTE SPECIALIZZATO IN CREDITO, FINANZA E ASSICURAZIONI.

FINALITA' DELL'ASSOCIAZIONE: in termini culturali e di bagaglio tecnico, Adusbef Aps Ets è attrezzata per operare con peculiare incisività nei settori: bancario, finanziario, assicurativo, postale, delle telecomunicazioni, della giustizia

RAPPORTO CON GLI ASSOCIATI: le nostre iniziative sono elaborate partendo sempre dalla realtà dei fatti, e diffuse tramite il periodico "Risparmio & Futuro" e attraverso comunicati stampa. Gli Associati coinvolgono l'Adusbef informando su argomenti dallo sviluppo manifestatamente non corretto o sospetto, richiedendo direttamente consulenze o semplici risposte a quesiti, coinvolgendo l'associazione su problemi di utenza e di consumo.

STRUTTURA. SEDI: Oltre la sede nazionale romana di via Vittorio Bachelet n. 12 Adusbef Aps Ets conta oggi più di 190 sedi locali ed è presente in tutte le Regioni d'Italia.

I professionisti responsabili delle delegazioni in cui si articola l'Associazione, sono in maggioranza avvocati. Tutti hanno sottoscritto il codice etico, elaborato originariamente nel dicembre 2000, il cui testo si può reperire sul nostro sito (www.adusbef.it) dove sono presenti tutte le sedi ufficiali Adusbef.

SE VUOI AIUTARCI A CONTINUARE LE NOSTRE BATTAGLIE IN DIFESA DEI TUOI DIRITTI.....
..... ISCRIVITI ALL'ADUSBEF Aps

- **Socio ordinario + Rivista 12 numeri (validità biennale + abb. 12 num rivista R&F): - €. 25,00 (1,00 euro per anno quota associativa – 23,00 euro per 12 numeri rivista R&F)**
- **Socio ordinario + Rivista 6 numeri (validità annuale + abb. 6 num. rivista R&F): - €. 12,50 (1,00 euro per anno quota associativa – 11,50 euro per 6 numeri rivista R&F)**
- **Socio ordinario (validità biennale): - €.2,00 (1,00 euro per anno)**
- **Socio ordinario (validità annuale): - €. 1,0**
- **Socio ordinario sostenitore: - €. 100,00**

- VERSAMENTI SU CONTO CORRENTE **POSTE ITALIANE**
  IBAN: IT74S0760103200000070043005 INTESTATO ADUSBEF;
- OPPURE SU CONTO CORRENTE BANCARIO PRESSO **MONTE DEI PASCHI DI SIENA SPA**
  IBAN: IT35Q0103003204000001471949 INTESTATO ADUSBEF;
- OPPURE ISCRIVITI **ONLINE:** https://web.adusbef.it/iscrizione_socio.asp
- OPPURE ISCRIVITI PRESSO LA DELEGAZIONE ADUSBEF (https://www.adusbef.it/sedi);

CI DARAI UNA MANO A BATTERE LA PREPOTENZA DI UN POTERE POLITICO FINANZIARIO SEMPRE PIÙ SUPPONENTE ED ARROGANTE CHE MORTIFICA PERFINO QUEI DIRITTI ACQUISITI ED INALIENABILI DEI CITTADINI E DEI CONSUMATORI IN TUTTI I CAMPI. GRAZIE DELL'ATTENZIONE.

Finanziamenti pubblici ricevuti da Adusbef nel 2021 ed anni precedenti: Presidenza Del Consiglio dei Ministri Mef CONTRIBUTOASSOC.CONSUMATORI D.LGS 70.2017 Editoria; MISE – Ministero dello Sviluppo Economico; Regione Lazio; Regione Calabria; MEF – Cinque per Mille – Ministero del Lavoro e delle Politiche Sociali; CSEA.

*"Per difendere meglio i tuoi diritti destina il **5 per mille** delle tue imposte a sostegno di **Adusbef**. Indica il codice fiscale della nostra associazione **0 3 6 3 8 8 8 1 0 0 7** sul modulo della denuncia dei redditi ed apponi la tua firma."*