Diritto del Risparmio

L'ATTACCO INFORMATICO "*MAN IN THE BROWSER*" NELLA GIURISPRUDENZA DELL'ARBITRO BANCARIO.

di Francesco COCCHI*.

Man in the browser attack is such as more sophisticated computer fraud by hacker through which by using an intrusive element based upon a malware, he takes victim's PC control including banking transactions.
In the case the malware acts like a well-placed, hidden spy in the PC recording all the traffic entered into the browser through the infected computer and acting when the user log into their banking services account.
When logging in is done, through a fake page, the hacker captures credentials to access the online account by driving out the target person from browsing.
Precisely the construction of false home banking environments through fake pages that faithfully reproduce the stylistic features of the intermediary will lead the victim to believe that they are operating in the protected environment of their own bank, while in reality they are handing over data to the cybercriminal.
The purpose of this contribution is to examine the main phases of the M.I.T.B. attack by comparing it to the most ancient Phishing attacks and the new "hybrid" forms of phishing, also giving an account of the analysis of this computer fraud in the jurisprudence of the banking Arbitrator and in the ordinary one.

fascicolo 1/2024

ISSN 2785-3004

* Avvocato.

Rivista di Diritto del Risparmio

L'attacco informatico **"man in the browser"** *nella giurisprudenza dell'Arbitro Bancario* *

di Francesco COCCHI**

Man in the browser attack is such as more sophisticated computer fraud by hacker through which by using an intrusive element based upon a malware, he takes victim's PC control including banking transactions.
In the case the malware acts like a well-placed, hidden spy in the PC recording all the traffic entered into the browser through the infected computer and acting when the user log into their banking services account.
When logging in is done, through a fake page, the hacker captures credentials to access the online account by driving out the target person from browsing.
Precisely the construction of false home banking environments through fake pages that faithfully reproduce the stylistic features of the intermediary will lead the victim to believe that they are operating in the protected environment of their own bank, while in reality they are handing over data to the cybercriminal.
The purpose of this contribution is to examine the main phases of the M.I.T.B. attack by comparing it to the most ancient Phishing attacks and the new "hybrid" forms of phishing, also giving an account of the analysis of this computer fraud in the jurisprudence of the banking Arbitrator and in the ordinary one.

Aprile

Fascicolo 1/2024

---

* Contributo approvato dai *referee*.
** Avvocato.

Abstract

Man in the browser attack is such as more sophisticated computer fraud by hacker through which by using an intrusive element based upon a malware, he takes victim's PC control including banking transactions.
In the case the malware acts like a well-placed, hidden spy in the PC recording all the traffic entered into the browser through the infected computer and acting when the user log into their banking services account.
When logging in is done, through a fake page, the hacker captures credentials to access the online account by driving out the target person from browsing.
Precisely the construction of false home banking environments through fake pages that faithfully reproduce the stylistic features of the intermediary will lead the victim to believe that they are operating in the protected environment of their own bank, while in reality they are handing over data to the cybercriminal.
The purpose of this contribution is to examine the main phases of the M.I.T.B. attack by comparing it to the most ancient Phishing attacks and the new "hybrid" forms of phishing, also giving an account of the analysis of this computer fraud in the jurisprudence of the banking Arbitrator and in the ordinary one.

****

L'attacco "man in the browser" è una frode informatica particolarmente sofisticata nella quale l'hacker sfruttando un principio intrusivo basato su di un malware riesce a prendere il controllo del PC e delle transazioni bancarie della propria vittima.

In pratica il malware, come una spia silente si anniderà nel PC registrando tutto il traffico che dalla macchina infettata sarà immesso nel browser di navigazione, attivandosi nel momento in cui l'utente si dirigerà verso i propri servizi bancari. In quel momento, attraverso una fake page l'attaccante otterrà le credenziali per poter accedere la conto on line estromettendo così dalla navigazione il soggetto target.

Proprio la costruzione di falsi ambienti di home banking tramite pagine civetta che riproducono fedelmente gli stilemi dell'intermediario, indurranno la vittima a ritenere di stare operando nell'ambiente protetto della propria banca, mentre invece sta cedendo dati al malfattore.

Il presente contributo si prefigge lo scopo di esaminare le principali fasi dell'attacco M.I.T.B. ponendo in raffronto con i più risalenti attacchi Phishing e le nuove forme "ibride" di phishing, dando conto anche dell'analisi di tale frode informatica nella giurisprudenza dell'Arbitro bancario e ed in quella ordinaria.

L'attacco informatico "*man in the browser*" nella giurisprudenza dell'Arbitro Bancario.

SOMMARIO: 1. Il "*man in the browser*" (c.d. M.I.T.B.): caratteristiche operative e fasi dell'attacco. – 2. Aspetti caratteristici del M.I.T.B. e differenze rispetto al *deceptive phishing*. – 3. Un elemento distonico dell'attacco M.I.T.B.: la convalida dell'operazione da parte del cliente. – 4. La responsabilità dell'utilizzatore di servizi di pagamento: l'assenza di colpa grave o dolo nella condotta dell'utente vittima della truffa informativa "*man in the browser*".

1. Il "*man in the browser*" (c.d. M.I.T.B.): caratteristiche operative e fasi dell'attacco.

L'attacco informatico *Man in the browser* (M.I.T.B.) è una tipologia di *phishing* particolarmente aggressiva capace di interferire nelle transazioni finanziarie della vittima modificandole e permettendo all'attaccante di assumerne il controllo a sua insaputa. Il principio intrusivo utilizzato nell' attacco informatico è un *malware* denominato Zeus, appartenente alla famiglia dei *"trojan horse",* in grado di captare le transazioni finanziarie sfruttando la vulnerabilità del browser web. Il *malware* solitamente viene scaricato dalla vittima nel proprio PC sotto forma di allegato mail o come aggiornamento e/o elementi di miglioramento delle funzioni del browser stesso e, una volta infettata la macchina, agisce come una spia silenziosa rimanendo dormiente e registrando tutte le informazioni che la persona immette nel proprio browser senza creare alcun malfunzionamento[1].

Il programma, una volta infettato il pc resterà in uno stato di quiescenza registrando come detto tutto il traffico di navigazione dell'utente attraverso il browser, senza alterare il funzionamento della macchina e senza essere rilevato da programmi antivirus, fintanto che

[1] Si veda in argomento: https://www.entrust.com/wp-content/uploads/2014/03/WP_Entrust-MITB_March2014.pdf; *Man in the Browser Attacks* di Ayyagari, Krishna Sai Anudeep, *"Man in the Browser Attacks"* (2017). Culminating Projects in Information Assurance. 42, in repository.stcloudstate.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1054&context=msia_etds; https://www.cyber-security-libro.it/articoli/man-in-the-browser/; https://www.cybersecurity360.it/nuove-minacce/man-in-the-browser-il-malware-che-spia-le-connessioni-internet-come-proteggersi/; https://en.wikipedia.org/wiki/Man-in-the-browser; https://it.qwe.wiki/wiki/Man-in-the-browser; https://owasp.org/www-community/attacks/Man-in-the-browser_attack.

non registrerà l'inizio di una operazione finanziaria. In quel momento il programma malevolo si attiverà iniziando a generare falsi problemi di login all'account bancario o rallentamenti nel caricamento della pagina di home, deviando l'utente colpito dall'attacco su di una *fake* page all'interno della quale verranno carpite le credenziali ed i codici utili alla esecuzione di operazioni di pagamento fraudolente. Una nota decisione del Collegio di Coordinamento dell'ABF, nel ricostruire per la prima volta le fasi dell'attacco in esame ha evidenziato come, una volta infettata la macchina, «*il malware resta completamente "in sonno" attivandosi solo nel momento in cui l'utente si colleghi ad un sito finanziario compreso fra quelli dei programmi a abbia posto nel mirino (target banks). In quel preciso istante il malware "si risveglia" ed entra in azione captando il collegamento dell'utente e propinandogli una pagina-video esattamente identica a quella che l'utente è abituato a riconoscere in sede di accesso regolare al sito del proprio intermediario. L'unica differenza, obiettivamente impercettibile ad un pur scrupoloso utente, è la stringa di descrizione della pagina che, a differenza di quello originale, reca un prefisso di accesso (c.d. protocollo di trasferimento ipertestuale, Hyper Text Transfer Protocol) "http" e non "https" (dove la "S" finale sta per secured, protetto).*»[2].

La falsa pagina web ha, quindi, un ruolo determinante nell'attacco *Man in the Browser* in quanto sarà proprio all'interno di essa che avverrà la captazione delle credenziali e le password temporanee utili alla esecuzione di operazioni in danno al soggetto colpito attraverso l'attenta costruzione di *form* nei quali verranno richiesti dati. Proprio il rilievo posto in essere dalla decisione del Collegio di Coordinamento ricorda come l'unica differenza tra la pagina "sicura" dell'intermediario e quella invece artefatta risiede nel protocollo della stessa che è un semplice "http" anziché un "https". Un dettaglio che sfuggirebbe anche ad un accorto utente. Di fatto la vittima non percependo di stare operando su di una "*fake-page*", ma anzi sicura di essere nell'ambiente di home banking del proprio istituto di credito, inserirà i predetti dati nella certezza di risolvere l'iniziale (falso) problema di accesso al servizio mentre, invece, verranno utilizzati dall'hacker per eseguire operazioni in suo danno. Ottenute le credenziali, infatti, l'attaccante potrà accedere al conto on line e procedere alla esecuzione di numerose operazioni, che saranno autorizzate grazie alla captazione anche dei necessari codici OTP

[2] Cfr. ABF, Collegio di Coordinamento, decisione n. 3498/2012. Conforme: Collegio di Napoli decisione n.8206/2016, ABF Collegio Roma decisione n.1362/2019, ABF Collegio Roma decisione n.1363/2014, ABF Collegio Roma decisione n. 511/2015, ABF Collegio di Milano decisione n. 822/2014, ABF Collegio di Napoli, n.8206/2016, ABF Collegio Milano decisione n.3119/2019.

che saranno richiesti alla vittima grazie alla «*schermata di cattura formulata con illusionismo informatico (che) induce il cliente a comunicare i propri dati e il codice monouso generato dall'OTP*»[3].

È ormai noto, infatti, che a seguito della introduzione del presidio di sicurezza dell'autenticazione forte, introdotta dalla Direttiva n. 2015/2366 EU (PSD2) secondo le specifiche tecniche cui essa fa rinvio, dettate dal Regolamento delegato (UE) n. 2018/389 della Commissione Europea del 27 novembre 2017 che ha integrato la predetta direttiva, si pone oggi per l'hacker ha necessità non solo di captare le c.d. credenziali statiche ma anche quelle dinamiche e più precisamente le *One Time Password* (indicate con l'acronimo OTP) generate appunto con processi di strong Customer Authentication. L'attacco in esame, quindi, non colpisce direttamente la sicurezza della fase di autenticazione e accesso al servizio di home banking ma la aggira, con un vero e proprio artificio informatico reso possibile dalla interposizione dell'attaccante tra il pc dell'utente ed il suo servizio di on line banking all'interno del browser di navigazione. Il *malware*, infatti, sarà capace di modificare tutte le transazioni poste in essere dalla vittima nel momento in cui sono formate nel browser, in quanto riuscirà a frapporsi tra essa ed i meccanismi a presidio della sicurezza del browser web stesso.[4]

La struttura dell'attacco in esame deriva dalla figura del "*Man In The Middle*" (c.d. M.I.T.M.), (traducibile come "*uomo nel mezzo* ") altra tipologia di frode informatica attraverso la quale l'attaccante «*si posiziona tra l'utente e sito legittimo*»[5] allo scopo di acquisire informazioni intercettando e manipolando le comunicazioni via Internet.[6] Nel "*Man In The Middle*" (c.d. M.I.T.M.) il soggetto attaccante però crea connessioni indipendenti tra vittima e destinatario del messaggio generando in loro la parvenza di stare comunicando direttamente, mentre invece si frappone tra i soggetti controllando la loro sessione.[7] Ciò potrà avvenire con successo soltanto nell'ipotesi in cui nessuna delle due parti in comunicazione si avveda che il loro collegamento è stato compromesso dall'attacco. Il *Man In The Browser*, invece, sfruttando

[3] Cfr. ABF Collegio Napoli, decisione n. 8400/2019.
[4] Gühring, Philipp (27 January 2007). "*Concepts against Man-in-the-Browser Attacks*" (PDF). Retrieved 2008-07-30, cit. in https://en.wikipedia.org/wiki/Man-in-the-browser.
[5] F. Tajani, G. Costabile, G. Mazzaraco, "*Phishing e furto d'identità digitale*", Milano 2008,29.
[6] Cfr. "*Attacco Man in the middle, tutti i modi possibili e come difenderci*", in www. Cyber security 360.it.
[7] Si veda in argomento: "*Attacco man in the middle*" in wikipedia in cui si richiama *What is man-in-the-middle attack (MitM) – definition from Whatls.com,* su IoT Agenda; T. Pantage, How to defend yourself against MITM attack to the HTTPS protoc in IEEE Security Privacy, Vol. 7, n.1.2009, pag. 78-81; *V. Lavecchia, caratteristiche-e-differenza-tra-man-in-the-middle-e-man-in-the-browser-attack in https://vitolavecchia.altervista.org/caratteristiche-e-differenza-tra-man-in-the-middle-e-man-in-the-browser-attack/*.

il medesimo principio intrusivo, si frappone tra la vittima ed il browser, controllando cosi le transazioni finanziarie che tramite esso disporrà.

A differenza del M.I.T.M., quindi, il *Man In The Browser* (c.d. M.I.T.B.) non solo si interpone tra soggetto e sito finanziario ma per farlo sfrutta unicamente la vulnerabilità del browser ottenendo il controllo di tutte le informazioni che passeranno dalla macchina della vittima al browser stesso. Le caratteristiche descritte portano a definire il *Man In The Browser* come una evoluzione del M.I.T.M, molto più aggressiva in quanto il portatore dell'attacco risulterà capace non solo di frapporsi in una comunicazione digitale ma anche di assumerne il controllo in maniera silente e varcare l'accesso all'account bancario della vittima (con conseguente autenticazione) insieme al soggetto colpito operando, in seguito, in completa autonomia.

Nella prassi si registrano alcune variazioni nello schema di attacco M.I.T.B., attraverso l'impiego di diverse tecniche di *social engineering*. Una prima ipotesi è quella in cui l'attaccante dirotta la vittima su di una "*fake page*" del tutto simile, come detto, a quella originale del suo istituto di credito. Tale "pagina" avrà la duplice funzione di far credere all'utente di stare operando nel reale ambiente di home banking e permettere al cybercriminale di ottenere attraverso essa tutti i dati riservati che la inconsapevole vittima vi inserirà per tentare di eseguire il login di accesso e disporre in seguito un pagamento in totale autonomia.

Altra ipotesi, maggiormente utilizzata nella prassi, è quella in cui l'attaccante genera rallentamenti nella sessione bancaria simulando mal funzionamenti e problemi di accesso/login al conto e sempre attraverso una *fake page* verrà proposta al malcapitato, come soluzione alle difficoltà di login rilevate, l'inserimento di codici ricevuti sul cellulare che verranno presentati alla vittima come "codici di sblocco" del (falso) problema. In realtà tali codici saranno *One Time Password* (OTP), cioè password temporanee inviate *out of band* dalla banca al cliente o per il login o per l'esecuzione di operazioni, che verranno invece captate dall'hacker e utilizzate poi sulla vera pagina web dell'intermediario per finalizzare l'attacco. Altra ipotesi, infine, è quella di proporre pagine, sempre artefatte e del tutto simili a quelle originali dell'intermediario, con molti campi di richiesta dati da riempire al fine di risolvere un falso problema di blocco del conto corrente on line o di servizi propinato alla vittima. I molteplici "*form*" contenuti nella pagina web di contatto, renderanno l'interfaccia più credibile e saranno utili a distrarre la vittima facilitando così la cessione di codici e dati insieme ad altri

dati personali meno importanti. Una volta perfezionato l'accesso al conto del soggetto attaccato, l'hacker cercherà di massimizzare l'attacco ponendo in essere il maggior numero di operazioni, spesso anche attraverso l'impiego di appositi software che permettono una rapida interazione con il servizio di on line banking facilitando così la creazione e conseguente ricezione di codici OTP utili ad autorizzare le operazioni di pagamento fraudolente.

2. Aspetti caratteristici del M.I.T.B. e differenze rispetto al *deceptive phishing*.

La principale caratteristica del *Man In The Browser attack* risiede nella capacità del *malware* di attivarsi unicamente nel momento in cui la navigazione internet della vittima si dirige su siti finanziari, per poi assumere il controllo della transazione a completa insaputa della vittima grazie all'interposizione del portatore dell'attacco tra il computer dell'utente ed il browser utilizzato per la navigazione. Da tali elementi emerge con chiarezza la notevole pericolosità dell'attacco poiché capace di sorprendere la vittima senza permettergli di assumere tempestive controffensive alla minaccia nella quale è incorsa.

Come abbiamo avuto modo di vedere nella fase iniziale dell'attacco, le metodiche di acquisizione dei dati riservati possono variare dal rallentamento della sessione all'impossibilità di accedere al proprio account bancario, mentre invece il portatore dell'attacco vi sta già operando, sino a giungere all'immediato re-indirizzamento su finte pagine del sito bancario, del tutto uguali, la cui differenza unica con quella reale è il protocollo (HTTP anziché HTTPS).

Superata, quindi, la fase iniziale dell'attacco, occorre approfondire anche le successive fasi nelle quali il soggetto target dell'attacco è condotto dal malfattore alla cessione dei dati.

E' indubbio, infatti, che anche nel M.I.T.B. lo scopo ultimo della truffa sia quello di acquisire dati riservati che si trovano nella unica disponibilità della vittima (codice utente, password statica e password dinamica) attraverso la loro cessione all'interno della suddetta *fake page*.

Tale ultima circostanza porterebbe a ritenere che anche nel caso del M.I.T.B. si verifichi di una cessione colposa di credenziali da parte dell'utilizzatore di servizi di pagamento con l'effetto di avvicinare tale ipotesi di truffa informatica al diverso caso del *deceptive phishing*. In

vero la tesi non appare sostenibile già solo ove si consideri il diverso e più complesso scenario informatico in cui l'intero attacco M.I.T.B. si svolge.

Occorre nel merito precisare come il M.I.T.B. si presenti come una aggressione informatica complessa e altamente "informatizzata" in cui il portatore opera attraverso il PC della vittima, previamente "infettato", utilizzando il suo "indirizzo IP" per operare all'interno del conto della vittima, frapponendosi tra la macchina ed il browser web utilizzato per la navigazione, senza necessità di violare gli apparati di sicurezza predisposti dagli istituti di credito.

Le considerazioni che precedono sono già di per sé sufficienti ad allontanare la fattispecie in esame da quella del c.d. *deceptive phishing*, nella quale invece una volta carpite le credenziali per operare con tecniche di *social engineering* legate al c.d. fattore umano, l'attaccante eseguirà login e operazioni fraudolente dal proprio PC (utilizzando il proprio indirizzo IP) e non da quello della vittima.

La complessità dell'attacco M.I.T.B. emerge, quindi, non solo dalla capacità di tale attacco di generare falsi problemi informatici durante l'accesso all'home banking del cliente, ma soprattutto nella costruzione di perfette false pagine web del tutto simili a quelle autentiche dell'intermediario su cui l'hacker dirotta l'utente per poter poi carpire le credenziali. Contrariamente a quanto sin d'ora detto, invece, nel caso del *deceptive phishing* la captazione di dati e credenziali avviene al di fuori dell'ambiente di home banking, in quanto la vittima fornisce spontaneamente le informazioni riservate ed i codici di accesso al servizio bancario rispondendo a una mail civetta o cliccando sul link ivi contenuto o compilando un *form* inserito nella mail. L'invio di e-mail civetta non è l'unico strumento utilizzato dai truffatori per ottenere i dati riservati in quanto nuove forme di phishing vengono poste in essere anche con sms (c.d. *smishing*) o contatto telefonico (c.d. vishing).

Appare pertanto evidente la netta distinzione attacco phishing e M.I.T.B., in quanto mentre nel primo vi è una colpevole cessione di dati da parte dell'utente caduto vittima di una negligente credulità, nell'attacco M.I.T.B. si è in presenza di un sofisticato metodo di intrusione nel sistema informatico del cliente capace di creare una parvenza di ambiente protetto in cui il medesimo opera in completa tranquillità, mentre invece l'intera transazione è guidata dal portatore dell'attacco informatico. L'acquisizione di dati riservati attraverso tecniche di *deceptive phishing*, infatti, è resa possibile da una interazione dell'utente che

spontaneamente cade nella rete del *phisher*. Interazione da ritenersi colpevole data la ormai notorietà di tale truffa e le numerose raccomandazioni degli istituti di credito di non rispondere mai a messaggi che chiedono l'inserimento di dati personali.

Solitamente un attacco phishing ha inizio con un invio massivo di mail o sms tramite tecniche di *spammig* che raggiungono un numero imprecisato di utenti allo scopo di convincerli a esaminare il problema rappresentato mediante attraverso il link evidenziato per la soluzione. Anche in tale ipotesi vengono predisposti appositi *format* che si attivano cliccando su *link* postati all'interno della comunicazione fraudolenta o ad esse allegati. Dopo aver predisposto tutti i *tools* utili a carpire informazioni riservate il *phisher* ha infatti bisogno di instaurare un contatto con la vittima per indurre il bersaglio a compiere tutte quelle azioni utili alla cessione di credenziali di accesso e dispositivi al proprio conto on-line.

Vi sono poi ipotesi come nel caso dello "*spear phishing*" in cui l'attacco non è diffuso con tecniche di spamming ma anzi l'attaccante seleziona attentamente la vittima (da qui l'impiego del termine "*spear*"- fiocina) studiandola preventivamente ed acquisendo dati su di essa per poterla poi "agganciare" con comunicazioni mail maggiormente credibili perché più dettagliate.[8] L'attacco, poi, si completa con la determinazione della vittima, poco avveduta, di ritenere vero il messaggio ricevuto e quindi procedere alle azioni di soluzione al problema che le vengono proposte.

In conclusione, quindi, un attacco di *deceptive phishing* ha successo unicamente se la vittima cade nell'inganno predisposto dall'attaccante e quindi si determina a cedere dati e informazioni all'interno dello scenario di frode che le viene propinato. Infatti, l'allarme procurato dalla finta comunicazione e-mail o dal messaggio sms o dal contatto telefonico, a seconda dello strumento di comunicazione scelto, induce il soggetto target a tentare di risolvere il falso alert ponendo in essere proprio quel comportamento che il *phisher* si aspetta e che ha pianificato attentamente con la predisposizione di *link, format* e *tools* utili a rendere credibile l'interazione ed il contesto in cui la frode si svolge.

Dalla disamina che prede emerge il netto tratto distintivo tra i due attacchi in esame in quanto nell'attacco M.I.T.B. non si è in presenza di comunicazioni *randomizzate* bensì di un malware capace di infettare la macchina in uso alla vittima e spiare le comunicazioni da questa inserite

[8] G. Sbraglia, *Op. Cit.*, cap 6.3.

nel browser per poi prendere il comando delle operazioni di pagamento una volta avviata una sessione con la propria banca, senza che sia necessaria alcuna interazione diretta con la vittima.

Sebbene entrambe le ipotesi in esame giungano al fine ultimo di carpire dati riservati e credenziali bancarie al soggetto colpito, non sfugge la maggiore complessità dell'attacco M.I.T.B., in quanto capace di operare in tempo reale nella sessione bancaria volontariamente aperta dall'utente con il proprio istituto di credito. Valutando infatti le ordinarie fasi preparatorie di un attacco informatico vediamo che al M.I.T.B. non è richiesto di intrattenere contatti preliminari con la vittima, né indurla ad una cessione volontaria dei dati, ma anzi richiede un minore impiego di tecniche di *social engineering* le quali operano unicamente nella fase iniziale con cui viene infettata la macchina dal *malware*.

Occorre, però, dare atto anche di una trasformazione delle ipotesi *classiche* di phishing, che col tempo hanno generato forme più aggressive di tale attacco. Forme che potremo definire "ibride" poiché sommano a sé caratteristiche di diverse tipologie di attacchi phishing. L'attenzione può essere posta verso le tipologie di phishing che impiegano l'utenza telefonica per la veicolazione del messaggio quali lo *smishing* ed il *vishing*.

Il tratto distintivo dello *smishing* (*sms-phishing*) risiede nell'uso di sms per l'invio di messaggi in grado di indurre le vittime a chiamare un numero telefonico o accedere ad un sito, al fine sempre di risolvere un problema. Anche tali tecniche di *social engineering* sono unicamente funzionali a carpire dati riservati alla vittima con risponditori automatici o format del tutto simili agli originali cui fanno riferimento.[9] Il *vishing* (*phishing-vocale*) si verifica, invece, «*quando un truffatore crea un sistema vocale automatizzato (o manuale) per fare chiamate vocali verso utenti telefonici e chiedere loro informazioni private*». «*L'intento è lo stesso del phishing di e-mail o dell'SMS phishing (smishing): la chiamata vocale crea un senso di urgenza per l'utente che per questo motivo fornisce informazioni riservate*».[10]

Ciò che rileva è, soprattutto, l'impatto psicologico e la conseguente sensazione di sorpresa e spiazzamento che un simile tentativo di truffa può generare. Pensiamo infatti, alla circostanza

[9] Sul punto P. Tarsitano, *Smishing: cos'è e come funziona il phishing che usa gli SMS come esca*, in www.cybersecurity360.it.
[10] W. Rocchi, *Il vishing e la truffa del "consenso rubato": cos'è e come difendersi dal phishing vocale*, in www.cybersecurity360.it.

in cui in un primo momento ci giunge dall'Hacker un messaggio sul cellulare (*smishing*) che ci richiede una azione, magari artefatto con tecniche di spoofing che lo rendono ancor più credibile, generando così una sensazione di allarme alla quale, poco dopo, si somma un contatto telefonico (*vishing*) che crea un rafforzamento psicologico nella ipotetica veridicità del problema.

Se a quanto descritto viene aggiunto l'impiego di tecniche di falsificazione dell'identificativo del numero chiamante o del numero mittente i messaggi sms (c.d. *spoofing – caller ID spofing*) [11] possiamo concludere come la vittima sia maggiormente indotta a compiere tutte le azioni che le vengono richieste con una conseguente riduzione della propria soglia di vigilanza.

In tale ottica assume assoluto rilievo soprattutto il contenuto stesso del messaggio, veicolato anche attraverso la conversazione telefonica (*vishing*), reso sempre più efficace da scelte terminologiche appropriate, linguaggio tecnico e chiaro idoneo a far credere alla vittima di stare parlando con un vero operatore dell'intermediario bancario. Certezza che, infine, può essere ulteriormente rafforzata anche dalla conoscenza da parte del truffatore di alcuni dati personali della vittima, elemento quest'ultimo idonea a scardinare ogni resistenza verso il *phisher*.

Sebbene tali nuove forme "ibride" di phishing siano caratterizzate da una maggiore complessità del paradigma di attacco portata dall'impiego sinergico di più tecniche di ingegneria sociale nonché l'impiego di maggiori fattori informatici, occorre ulteriormente confermare come in esse resti sempre centrale la interlocuzione dell'attaccante con la vittima, volta a porre in essere una cooperazione che, invece, nell'attacco M.I.T.B. è del tutto assente in quanto l'attaccante ottiene credenziali e codici all'interno di uno schema di attacco più complesso e privo di prodromici contatti con il target. Nel M.I.T.B., infatti, l'attacco ha una matrice prettamente informatica tranne un primo iniziale momento in cui la vittima viene indotta a scaricare il *malware* solitamente nascosto in una utilità di sistema o un allegato ad una mail. Da lì in poi l'hacker sarà totalmente indipendente nelle azioni, ingannando l'internauta con falsi ambienti informatici e problemi tecnici.

[11]Sul tema, voce "spoofing" in wikipedia.

Un tratto distintivo che quindi permane rispetto non solo ai più classici attacchi di *deceptive phishing* ma anche rispetto alle nuove c.d. nuove forme "ibride" di *phishing* certamente più aggressive rispetto all'archetipo classico.

3. Un elemento distonico dell'attacco M.I.T.B.: la convalida dell'operazione da parte del cliente.

L'utente al fine di porre in essere una operazione con modalità telematiche sul proprio conto on line deve seguire una serie di passaggi. Il primo di essi è quello della autenticazione presso il proprio account bancario. Autenticarsi significa provare la propria identità a livello digitale e di conseguenza confermare la nostra identità attraverso l'inserimento di codici riservati in nostro possesso e che soltanto noi conosciamo[12]. Si procede così a trasformare l'identità fisica del soggetto in una identità digitale rappresentata attraverso l'inserimento di codici riservati e, pertanto, esposta al rischio di "furto di identità." Sarà, infatti, sufficiente entrare in possesso dei fattori utili alla autenticazione per rappresentarsi falsamente al sistema di home banking come il soggetto a ciò legittimato.

Altro passaggio determinante è quello dell'autorizzazione dell'operazione dispositiva, posto in essere con l'inserimento di un fattore "dinamico" generato e legato temporalmente all'operazione stessa. Gli attacchi informatici operano a diverso livello proprio su tali fasi generando distonie in segmenti specifici di essi ed essendo, così in grado di bypassare i presidi di sicurezza predisposti dal gestore di servizi.

Al fine di contenere tale rischio, che appare purtroppo fisiologico all'uso di strumenti di pagamento, prima la Direttiva 2007/64/CE del 13 novembre 2007 relativa ai servizi di pagamento nel mercato interno (Payment Services Directive – PSD)[13] e, successivamente, la Direttiva (UE) 2015/2366 del 25 novembre 2015 (Payment Services Directive – PSD 2)[14] , con la connessa normativa attuativa, hanno tra l'altro rafforzato proprio il sistema di sicurezza delle transazioni on line.

---

[12] G. Sbaraglia, *Autenticazione a due fattori: cos'è, come e perché usarla, anche alla luce della PSD2*, in https://www.cybersecurity360.it/soluzioni-aziendali/autenticazione-a-due-fattori-cose-come-e-perche-usarla-per-google-facebook-instagram-e-altri/.

[13] In eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32007L0064.

[14] In eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32015L2366.

Viene infatti individuato nella Strong Customer Authentication (SCA), una nuova modalità di autenticazione che rispetto alle precedenti, di tipo statico e monofattoriale, si basa invece sulla verifica di almeno due fattori di diversa natura per il riconoscimento dell'utente sia al momento dell'accesso al conto on line che per la riferibilità al medesimo di un'operazione di pagamento. La direttiva Europea PSD 2 infatti ne prescrive l'obbligo quando il cliente esegue l'accesso al proprio conto, dispone pagamenti o effettua qualsiasi altra azione tramite canale telematico o a distanza soggetto a rischio di frodi.[15]

Il rafforzamento della sicurezza di questa forma di autenticazione quindi risiede proprio nella multifattorialità che la caratterizza e, soprattutto, nella indipendenza dei fattori in essa coinvolti.

Le specifiche tecniche del processo di autenticazione forte sono state disciplinate a livello europeo, ad integrazione della Direttiva UE n.2015/2366, dal Regolamento delegato UE n.2018/389 del 27 novembre 2017 che ha opportunamente disciplinato le metodiche tecniche di formazione dei fattori che la compongono. Affinché, quindi, si possa essere in presenza di autenticazione forte occorre che siano coinvolti almeno due o più fattori classificabili nelle categorie della conoscenza, del possessore dell'inerenza.

Per conoscenza si intende qualcosa che solo l'utente conoscente come ad esempio una password; per possesso qualcosa che solo l'utente possiede come ad esempio un token o uno smartphone e per inerenza riferita a qualcosa che caratterizza l'utente come ad esempio l'impronta digitale[16].

All'interno di tale processo è determinante l'indipendenza di ognuno di tali fattori, affinché la violazione di uno di essi non infici la validità degli altri soprattutto quando impiegati su dispositivi multifunzionali quali cellulari e tablet. L'impiego di tali fattori comporta la generazione di un codice di autenticazione accettato una sola volta dal prestatore di servizi nel momento in cui l'utente accede al proprio conto on line o dispone su di esso una operazione.

---

15 Cfr. art 97 Direttiva 2015/2366 U.E.

16 G. Sbaraglia, *Autenticazione a due fattori: cos'è, come e perché usarla, anche alla luce della PSD2*, *Cit.*; si veda altresì Considerando 6 e ss. Regolamento delegato UE 2018/389.

A presidio della sicurezza di tale processo vi è l'ulteriore prescrizione che il codice di autenticazione così generato si riferisca specificatamente all'importo dell'operazione disposta ed al suo beneficiario con la conseguenza che qualsiasi modifica dell'operazione invaliderà il codice generato per essa.

L'autenticazione forte, quindi, rappresenta uno strumento in grado di garantire la sicurezza delle transazioni telematiche nei termini descritti. Da un punto di vista operativo nell'ipotesi di autenticazione a due fattori dopo aver inserito il primo dei due fattori l'altro, generato dinamicamente, sarà ricevuto nella maggior parte dei casi sulla utenza telefonica cellulare collegata al proprio account bancario via sms o all'interno di token/app. La *One time Password* così generata avrà una durata temprale limitata e, soprattutto, sarà generata nel momento in cui l'utente richiede l'accesso al proprio servizio o una operazione di pagamento. In tale secondo caso la O.T.P. conterrà, come detto, anche gli estremi dell'operazione cui fa riferimento e che la stessa andrà a convalidare.

L'elevato livello di sicurezza garantito dal processo in esame ha portato a ritenere la sua sostanziale invulnerabilità della strong customer authentication alle aggressioni di tipo informatico. Tale opinione ha trovato una iniziale conferma in un risalente orientamento dell'Arbitro Bancario che, ritenuto invulnerabile tale sistema di sicurezza rispetto a quello di tipo statico impiegato in precedenza, presumeva l'ascrizione automatica di colpa grave del cliente nella causazione di truffe telematiche. Tesi successivamente superata dall'importante intervento del Collegio di Coordinamento ABF che, esaminando le richiamate distinzione tra attacchi phishing e attacchi *Man In The Browser*, ha in particolar modo valorizzato il continuo progresso informatico dei nuovi cyberattacchi[17]. Ed infatti la decisione ha il pregio giuridico di muovere proprio dalla valutazione della maggiore aggressività dei nuovi attacchi informatici esaminati dalla prassi giurisprudenziale dell'Arbitro che, pur confermando la sicurezza dell'autenticazione a più fattori, non permette più l'automatismo deduttivo della ascrizione di colpa grave all'utente in caso di operazioni fraudolente. Ciò proprio alla luce dell'evoluzione sul piano tecnico ed informatico di tali nuove aggressioni e della loro capacità offensiva, ritenuta centrale dal Collegio di Coordinamento nella valutazione della condotta della vittima.

[17] Cfr. ABF, Collegio Milano, decisione nn. 2658/2011, 2103/2013, 1462/2012; ABF, Collegio di Coordinamento, decisione n. 3498/2012.

I nuovi attacchi informatici come ad esempio il *Man In The Browser* presentano, infatti, un maggiore grado di complessità, tale da non permettere all'utente di percepire tempestivamente la frode in atto a suo danno grazie ad un vero e proprio *illusionismo informatico* [18] in grado di rendere l'attacco del tutto impercettibile. Con evidenti ricadute anche sulla valutazione della condotta tenuta dalla vittima in occasione della frode stessa. Più correttamente, infatti, nel caso del *Man In The Browser* non siamo in presenza di un *cyber attack* caratterizzato da una violazione della sicurezza sistema di autenticazione, ma di un attacco che invece aggira tale presidio attraverso l'impiego di tecniche di *social engineering* complesse ed evolute.

Tornando quindi ad esaminare questa forma di attacco informatico notiamo come l'operazione di pagamento fraudolenta viene predisposta ed eseguita interamente dall'hacker che, avuto accesso al conto della vittima con modalità intrusive impercettibili grazie a malware spia, porterà a termine la stessa con il corretto inserimento anche delle password monouso (OTP) generate in piena conformità alla normativa di settore sulla sicurezza delle operazioni telematiche.

In tale ultimo passaggio, l'inserimento da parte della ignara vittima, del codice OTP all'interno della *fake page* predisposta dall'attaccante potrebbe essere letto come una cessione colpevole di dati e quindi come un contegno gravemente negligente dell'utente, con conseguente impossibilità per quest'ultimo di ottenere il rimborso delle operazioni disconosciute.

Una simile valutazione, però, però non terrebbe conto della complessiva capacità dell'attacco M.I.T.B. di indurre l'utente di servizi di pagamento a ritenere di essere all'interno del proprio ambiente di home banking e di stare operando in totale sicurezza. Occorre infatti ricordare che la pagina civetta su cui l'hacker carpisce credenziali e codici differisce da quella genuina dell'intermediario unicamente per il suo protocollo che, come osservato dal Collegio di Coordinamento ABF, è indicato come un semplice HTTP anziché HTTS (cioè sicuro/protetto). Un dettaglio che potrebbe essere ignorato anche dal più scrupoloso degli utenti. La realtà che quindi deve essere valutata è quella che viene rappresentata *a video* dall'attaccante alla vittima durante le varie fasi della frode in esame.

[18] Cfr. ABF Collegio di Napoli decisione n. 8400/2019.

Soccorre in tale ricostruzione il Considerando n. 72 alla Direttiva PSD 2 il quale afferma che al fine di valutare la eventuale negligenza o grave negligenza dell'utente di servizi di pagamento in occasione della frode subita, dovrebbero essere prese in considerazione tutte le circostanze che hanno caratterizzato l'attacco.

Da ciò discendono le perplessità circa il possibile avvicinamento del *Man In The Browser attack* alle ipotesi di cessione colpevole di codici tipiche del c.d. phishing classico, proprio in considerazione della diversa metodica con la quale gli stessi vengono acquisti dall'attaccante.

La cessione nell'attacco in oggetto non avviene attraverso una richiesta alla vittima con falsi *form*, bensì con tecniche informatiche aggressive ed impercettibili anche per il più attendo utente. Depone a favore di tale tesi un ulteriore importante elemento: le modalità di disposizione dell'operazione fraudolenta.

Nei casi di attacco M.I.T.B., infatti, le operazioni sono portate a termine attraverso istruzioni impartite dall'hacker direttamente dal PC della vittima. Ciò grazie al sistema intrusivo impiegato che, infettando il computer dell'utente, permette all'hacker come detto di assumerne il controllo. Le operazioni saranno, pertanto, disposte dall'indirizzo IP della vittima e non da altro indirizzo come nel caso del phishing classico. Questo elemento fa emergere ancor più la irrilevanza della corretta conclusione di operazioni autorizzate con OTP-password quale elemento di colpa grave della vittima, in quanto è del tutto evidente che nel *Man In The Browser* non è l'utente ad inserirle nel reale ambiente di home banking. Difetta, pertanto, quel contegno gravemente colposo dell'utente che incautamente cede volontariamente i codici all'attaccante in quanto nell'attacco in esame gli stessi vengono carpiti con un inganno informatico del tutto impercettibile e le successive operazioni sono disposte direttamente dal truffatore sul PC della vittima stessa.

Le considerazioni sin qui svolte inducono a ritenere come la esecuzione dell'operazione da parte della vittima di attacco M.I.T.B. non sia un elemento distonico dal quale far discendere contegni negligenti o colposi della vittima, ma anzi rappresenti il tratto caratteristico di tale attacco dal quale discenderebbe semmai l'incolpevole affidamento che l'utente ha riposto nella pagina web civetta con la quale ha interagito.

E grazie a tale artificio informatico ed al finto ambiente di home banking che lo stesso è capace di riprodurre, che l'hacker otterrà non solo il controllo del PC ma anche del conto

della vittima, disponendo le operazioni dall'indirizzo IP e dal computer della stessa. Circostanza che ove correttamente esaminata non permetterà di attribuire l'esecuzione e autenticazione delle operazioni all'utente colpito da attacco M.I.T.B., anche se presidiata da autenticazione forte.

Ed Infatti l'elevato livello di complessità informatica dell'attacco *Man In The Browser* anziché violare tali fattori li aggira agendo sulla captazione sia delle credenziali statiche che di quelle dinamiche, senza che l'inserimento di esse nella *fake page* integri cessione volontaria o colposa di codici da parte della vittima. Elemento quest'ultimo che di fatto allontana il caso in questione dalle ipotesi di phishing.

4. La responsabilità dell'utilizzatore di servizi di pagamento: l'assenza di colpa grave o dolo nella condotta dell'utente vittima della truffa informativa "*man in the browser*".

Un elemento di fondamentale importanza nell'analisi della responsabilità della vittima nella causazione del danno da frode informatiche è certamente la complessità dell'attacco da essa subito. Nel caso del *Man In The Browser* occorre nuovamente evidenziare la complessità del paradigma di attacco e delle modalità intrusive in esso impiegate. Modalità che come detto sfruttano un *malware* spia capace di rendere impercettibile la consumazione della truffa in danno alla vittima creando anzi delle illusioni informatiche capaci di impedirle pronte controffensive.

Posta tale premessa occorre dare atto un diverso approccio rilevabile nella giurisprudenza di merito e di legittimità rispetto a quello invece formatosi nelle decisioni dell'Arbitro Bancario.

Mentre infatti la giurisprudenza ordinaria ha ritenuto approcciare l'esame della responsabilità legata al verificarsi di truffe informatiche soprattutto dal lato dell'intermediario, esaminando gli obblighi di condotta delle parti coinvolte in un operazione di pagamento e gli obblighi di sicurezza imposti sul prestatore di tali servizi affermando come corretta l'allocazione di questi ultimi sull'intermediario, l'Arbitro Bancario ha invece incentrato la propria analisi, visto anche il più ampio numero di casi giudicati, sulla ricostruzione dei singoli casi di attacco, individuandone i caratteri tipici di ognuno e soprattutto valutando all'interno delle singole fattispecie gli obblighi di condotta cui l'utente è tenuto. Obblighi che da un lato fanno

riferimento alla corretta custodia dei codici di accesso al sistema e dall'altro al loro corretto utilizzo. Muovendo dall'esame della Giurisprudenza ordinaria si osserva come la Suprema Corte abbia di fatto espresso un *favor* verso l'utilizzatore di pagamenti elettronici. Trova conferma tale impostazione nell'affermazione del principio, ormai consolidato, che pone a carico dell'istituto di credito il rischio legato ad operazioni poste in essere con collegamenti telematici, poiché rientrante nell'area del rischio professionale del prestatore di servizi di pagamento. Il pericolo cui si fa riferimento è quello legato alla possibilità di utilizzazione di codici di accesso al sistema da parte di terzi non autorizzati, che ben potrà essere contenuto, secondo la Suprema Corte, dalla predisposizione di preventive misure che permetteranno di ricondurre le operazioni alla effettiva volontà del cliente. Diviene pertanto centrale per l'intermediario, in caso di operazioni non autorizzate dal cliente, l'obbligo di provare la riconducibilità delle operazioni al correntista.[19] A tali premesse fa seguito l'affermazione dell'obbligo sempre per il prestatore di servizi di pagamento di una diligenza di natura tecnica che prende a parametro la figura dell' "accorto banchiere".[20] Nella prestazione di servizi di pagamento è indubbio, infatti, che l'intermediario nella sua qualità di contraente professionale sia tenuto alla esatta conoscenza degli attacchi informatici che possono rappresentare delle criticità per tale sistema e quindi porre in essere quanto necessario al fine di garantire sempre una sicurezza adeguata alla evoluzione di tali frodi.[21]

Emerge pertanto un rafforzamento della tutela dell'utilizzatore di tali servizi, del tutto in linea con la normativa dettata dal D. lgs. n.11/2010 in recepimento delle direttive europee PSD e PSD 2, motivata anche nell'orientamento della Corte di Cassazione dalla necessità di garantire proprio la fiducia della clientela nella sicurezza del sistema stesso data.

Diversamente dall'approccio della Giurisprudenza di legittimità, quella dell'Arbitro Bancario ha invece incentrato la propria analisi sulla ricostruzione delle singole ipotesi di truffa, tracciandone i caratteri distintivi e peculiari di ognuna e, come detto, ponendo l'attenzione

[19] Cass. Civ. sez. VI Ord. del 12.04.2018 n.9158 in Ridare.it; Conforme: Cass. Civ. Sez.I, Sent. del 03.02.2017 n.2950 in Giust. Civ. Mass. 2017, Cass. Civ. Sez.I Sent. del 23.05.2016 in Resp. Civ. e Prev. 2017,3,850, Cass. Civ. Sez.I Sent. del 19.01.2016 n. 806 in Foro I. 2016,2,I,455.

[20] Cass. Civ. Sez. I Sent. del 12.06.2007 n.13777 in Giust. Civ. 2008,12,2933, conforme Cass. Civ. Sez. I Sent. del 19.01.2016 n.806 in Responsabilita' Civile e Previdenza 2017, 1, 216, Trib. di Roma Sez. X Sent. del31.08.2016 n.16221 in Resp. Civ. e Prev 2017,3,852.

[21] R. Frau, *Responsabilità civile della banca per operazioni di home banking disconosciute dal cliente*, in Resp.Civ e Prev. F.3,2017, pag. 853B.

non solo agli obblighi di condotta e sicurezza dell'intermediario ma anche su quelli dovuti dall'utente e sulle concrete condotte tenute da quest'ultimo in occasione della frode.

Per quanto attiene all'attacco *Man In The Browser*, occorre dare atto come un importante decisione del Collegio di Coordinamento ABF sia intervenuta a comporre un contrasto formatosi all'interno dei propri Collegi in merito a tale attacco, tracciandone per la prima volta i tratti distintivi con importanti ricadute anche sul tema della responsabilità della vittima nella causazione dell'evento.

Il citato contrasto muove da un risalente orientamento formatosi nel Collegio Milanese che, risaltando la sicurezza dell'autenticazione a più fattori ("*Strong Care Authentication*"), deduceva in presenza di fattore di sicurezza una automatica colpa grave dell'utente nel caso di captazione dei codici dispositivi dell'operazione. Il fondamento di tale presunzione risiedeva nella ritenuta invulnerabilità di tale sistema di sicurezza anche in presenza dei più recenti attacchi informatici poiché strumento capace di garantire la massima sicurezza informatica al momento.[22] In vero una simile impostazione non teneva conto delle concrete modalità operative delle nuove forme di attacco informatico che, come nel caso del *Man In The Browser*, lontane da cessioni colpevoli di dati basate sulla colpevole credulità dell'utente, risultano in grado di captare codici riservati senza violare i parametri di sicurezza del sistema che li ha generati e trasmessi e senza generare allerta nella vittima. Come detto l'operatività dell'attacco in esame risulta estremamente sofisticata in quanto in grado di ricostruire un ambiente di Home banking del tutto simile a quello cui l'utente è visivamente "abituato", del tutto indistinguibile rispetto all'originale, utile alla inconsapevole captazione dei codici necessari ad operare sul conto. Occorre inoltre tenere conto anche delle modalità intrusive del *malware* utilizzato da questo attacco informatico che di fatto permette l'accesso dell'hacker al conto corrente della vittima permettendogli di operare in totale autonomia.[23]

Le descritte caratteristiche dell'attacco in esame sono state valorizzate da alcune decisioni dell'autorità bancaria suddetta, che si sono allontanate dall'orientamento che valorizzava l'impiego di sistemi di autenticazione "forte" (S.C.A.), ha affermato l'esistenza di nuove

[22] Cfr. ABF Collegio Milano decisione n. 2658/2011, n.2103/2013, n.1462/2012.
[23] Sulle caratteristiche tecniche si veda ABF Collegio di Coord. decisione n.3498/2012 Cit , ABF Collegio di Bari decisione n. 37/2019, ABF Collegio di Milano decisione n. 822 /2014, ABF Collegio di Roma decisione n.2156/2015, ABF Collegio di Napoli decisione n.8400/2019, ABF Collegio di Napoli decisione n. 8206/2016.

forme di rischio per tali sistemi di protezione, dando vita ad un contrasto interpretativo che ha richiesto un intervento compositivo del Collegio di Coordinamento. Muovendo dalla conferma della capacità protettiva dell'autenticazione "forte" il Collegio ha posto la propria attenzione sulla continua evoluzione delle aggressioni informatiche, valorizzando anche il contesto nel quale l'attacco informatico si svolge superando così di fatto l'automatica ascrizione di colpa grave all'utente. La decisione, in tale ottica, traccia per la prima volta la distinzione tra le ormai classiche ipotesi di phishing e la figura del *Man In The Browser*, ricostruendone dettagliatamente differenze e caratteristiche operative ed affermando come tale ultime attacco <<*ha luogo attraverso un sofisticato metodo di intrusione caratterizzato da un effetto sorpresa capace di spiazzare l'utilizzatore, grazie alla perfetta inserzione nell'ambiente informatico originale e nella correlata simulazione di un messaggio che a chiunque non potrebbe apparire che genuino, posto che l'unica " differenza" consta, come si è detto, nell'acronimo del protocollo di trasferimento, individuato come un normale "http" e non già come un "https" protetto*>>.[24] Elemento, quest'ultimo del tutto ininfluente secondo la decisione in esame in quanto capace di sfuggire all'attenzione di chiunque.

Proprio l'elemento della impercettibilità, unito alla capacità di spiazzamento dell'utente tipica di questa sofisticata forma di attacco induce il Collegio ad escludere qualunque grado di colpa nella vittima, sia di grado grave che lieve, giungendo ad affermare che anche la messa a disposizione di ulteriori fattori di sicurezza quali sistemi di SMS alert, non possa condurre alla deduzione di colpa grave nei riguardi del cliente che non se ne sia avvalso.

Ritenuto ininfluente anche l'aspetto della presenza di programmi malevoli nel sistema operativo della vittima poiché non valutabile di per sé come indice di negligenza nella custodia del medesimo, la decisione valorizza nuovamente la complessa natura del *malware* impiegato nell'attacco M.I.T.B. e la sua capacità di rimanere inerte sfuggendo a firewall e antivirus installati nel PC.

Si giunge, quindi, ad affermare la totale assenza di colpa nella condotta del soggetto caduto vittima di tale attacco, poiché vittima di una "illusione informatica" in grado di spiazzarlo ed impedirgli tempestivamente di opporre adeguate reazioni.

[24] ABF Collegio di Coord. dec. Cit., Conformi: ABF Collegio Roma decisione n. 1362/2019, ABF Collegio di Bologna decisione n. 778/2019.

La decisione del Collegio di Coordinamento, poi, evidenza anche un importante punto di contatto con i principi espressi dalla Suprema Corte, affermando anch'essa l'obbligo del prestatore di servizi di introdurre tutte le cautele necessarie a prevenire accessi non autorizzati ai servizi di pagamento ricordando inoltre l'obbligo per l'intermediario di verifiche periodiche sulla vulnerabilità dei presidi di sicurezza.

Un ulteriore punto di contatto con la Giurisprudenza di legittimità è poi rilevabile nel principio espresso sempre dal Collegio secondo il quale lo squilibrio di responsabilità nascente dal dettato normativo del D. lgs. n. 11/2010 si fondi sulla maggiore capacità economica del prestatore di servizi di sostenere il rischio connesso all'impieghi di strumenti di pagamento, vista l'impossibilità di una sicurezza assoluta dei medesimi. Una affermazione che recuperando il tema del rischio legato alle operazioni concluse con canali telematici già espresso dalla Suprema Corte, ne amplia la portata legandolo anche ad un ulteriore importante elemento: la continua promozione di servizi di pagamento. Viene affermato infatti dal Collegio che «*l'addossamento del rischio all'intermediario appare vieppiù giustificato dalla forte incessante promozione all'uso di tali strumenti posta in essere dal mondo bancario, in ciò aiutato anche da un sistema legislativo che sempre più ne impone l'adozione.*»[25]

Da quanto esposto emerge come le caratteristiche che sono proprie dell'attacco *Man In The Browser* non permettono di ritenere colposa la condotta della vittima caduta in un impercettibile "tranello", reso possibile da un "illusionismo informatico"[26] attraverso il quale la vittima sarà condotta a tentare un'operazione che in realtà non avrà seguito in quanto la pagina su cui opera avrà come conseguenza quella di comunicare i suoi dati riservati al portatore dell'attacco a sua totale insaputa.[27] La valorizzazione anche dell'aspetto emotivo in cui l'intera operazione fraudolenta si svolge permette di comprendere proprio l'impatto che tale tipologia di attacco crea sulla vittima. Ed infatti, come già detto, la circostanza che nel *Man In The Browser attack* la comunicazione dei dati da parte della vittima è dovuta al fatto che la stessa sia realmente persuasa o del problema di sicurezza incontrato al momento dell'accesso all'account bancario oppure di stare operando nel reale ambiente di home banking anziché su di una *fake page*. In vero proprio l'elemento psicologico descritto porta

[25] V. ABF, Coll. Coord. dec. *Cit.*
[26] V. ABF Collegio di Napoli, decisione n.8400/2019.
[27] V. ABF Collegio di Milano, decisione n. 822/2014 *Cit*.., Conforme ABF Collegio di Roma n. 2156/2015.

l'utente ad un affidamento incolpevole verso la schermata video cui si trova davanti e nella quale ripone fiducia. Si tratta di quell'effetto di spiazzamento, enunciato proprio dalla richiamata decisione e recepito anche in recenti decisioni dei singoli Collegi dell'Arbitro Bancario, che non permette alcuna razionale valutazione alla vittima ma anzi la induce all'inserimento dei dati nella sicurezza e operando in totale sicurezza sul proprio ambiente informatico bancario. Resta in ogni caso la valorizzazione anche nella giurisprudenza dell'Arbitro bancario dell'obbligo per l'intermediario di fornire la prova della colpa grave del cliente e l'insussistenza di malfunzionamenti nelle fasi di autenticazione e corretta registrazione dell'operazione contestata secondo la disciplina di settore con riferimento agli artt. 10 e 10 bis del Decreto citato. Colpa che come detto non può essere ravvisata neanche in grado lieve nell'ipotesi dell'attacco *Man In The Browser*.[28]

[28] Cfr. ABF Collegio di Roma decisione n. 1363/2014, ABF Collegio di Milano decisione n. 577/2019. Conforme ABF Collegio di Milano n.3857/2013, ABF Collegio di Roma decisione n. 511/2015, ABF Collegio Napoli decisione n.8206/2016, ABF Collegio di Milano decisione n.3119/2019, ABF Collegio di Bologna decisione n. 2772/2020.