CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

IL PHISHING BANCARIO, LA RESPONSABILITÀ DELL´ENTE CREDITIZIO E I SUOI LIMITI

L'articolo si propone di analizzare i profili del cd. "phishing" in ambito bancario, per tale intendendosi la captazione dei dati di accesso ai conti correnti degli utenti e la sottrazione di liquidità dagli stessi, ponendo l´accento in particolare sui profili di responsabilità della banca alla luce dei recentissimi arresti giurisprudenziali in materia.

di **Giulia Faillaci**
IUS/04 - DIRITTO COMMERCIALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Martedì 5 Gennaio 2021

CamminoDiritto.it
ISSN 2421-7123

Sommario: 1. Introduzione: cosa si intende per phishing; 2. Riferimenti normativi; 3. La responsabilità penale del phisher; 4. La responsabilità civile: le risposte della giurisprudenza in materia di risarcimento del danno; 5. L'attualità del problema ai tempi del Covid-19.

1. Introduzione: cosa si intende per phishing.

L'utilizzo sempre più frequente da parte degli enti bancari di sistemi tecnologici per la fruizione dei servizi di credito ha visto, come logica conseguenza, il proliferare di fenomeni di "truffe informatiche" assai sofisticate.

Tra queste, indubbia rilevanza ha assunto nel corso degli ultimi anni il cosiddetto "phishing", espressione mediante cui vengono individuati tutti quei comportamenti illeciti finalizzati all'intromissione indebita da parte di terzi nelle piattaforme di home banking allo scopo di sottrarre liquidità dai conti correnti dei utenti delle banche.

Si tratta di un tipo di truffa informatica che consiste generalmente nell'invio da parte di un hacker di e-mail o sms con cui si invita la vittima ad accedere al proprio account bancario, attraverso un sito molto simile a quello reale dell'istituto di credito, di modo da carpirne i dati riservati.

Mediante tale "maschera fake", quindi, la vittima, convinta di essere stata contattata dall'istituto bancario, cede, in modo inconsapevole, le credenziali per l'accesso al proprio conto corrente, vedendosi successivamente sottrarre somme di denaro anche molto consistenti.

2. Riferimenti normativi

L'utilizzo di sempre nuove tecnologie ha reso assai difficoltosa la creazione da parte del legislatore di un apparato normativo idoneo a fronteggiare tutti i problemi astrattamente ipotizzabili in materia.

Un riferimento legislativo è comunque rinvenibile all'interno del Codice sulla Privacy, introdotto con il d.lgs. 196/2003, il quale offre una serie di disposizioni utili a guidare l'interprete sia sotto il profilo della responsabilità civile che sotto quello della responsabilità penale. Da quest'ultimo punto di vista, inoltre, risultano certamente applicabili diverse norme contenute nel Codice penale.

CamminoDiritto.it
ISSN 2421-7123

3. La responsabilità penale del phisher

Per ciò che riguarda la responsabilità penale viene in considerazione, innanzitutto, l'art. 167 del Codice sulla Privacy.

Tale norma, infatti, punisce con la reclusione da sei a diciotto mesi chiunque, al fine di trarre per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione della normativa di riferimento e arrecando un nocumento all'interessato; la pena è aumentata nel caso in cui il fatto consista nella comunicazione o diffusione dei dati.

Sempre dal punto di vista penale, la condotta del cd. phisher potrebbe essere idonea ad integrare gli estremi del più grave reato di truffa ex art. 640, primo comma del Codice penale, che punisce con la reclusione da 6 mesi a 3 anni e la multa da 51 a 1032 euro «chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno», ovvero quello di truffa aggravata, di cui al secondo comma dell'art. 640 c.p., qualora il fatto sia commesso ingenerando nella persona offesa il timore di un pericolo o l'erroneo convincimento di dover eseguire l'ordine di un'autorità. Il phishing integra, inoltre, una serie di fattispecie delittuose, tra cui: il reato di frode informatica di cui all'640-ter c.p.[1], che presuppone l'alterazione di un sistema informatico o l'introduzione illecita sullo stesso o sui dati in esso contenuti, al fine di determinare un ingiusto profitto per il soggetto attivo e un danno per il soggetto passivo; il reato di cui all'art. 615-ter, co. 1 c.p., dedicato all'accesso abusivo ad un sistema informatico o telematico; il delitto di utilizzo indebito di carte di credito e di pagamento, disciplinato dall'art. 12 del d.l. n. 143/1991[2].

4. La responsabilità civile. Le risposte della giurisprudenza in materia di risarcimento del danno

Sotto il profilo della responsabilità civile, viene in considerazione ancora una volta il Codice sulla Privacy, il cui articolo 15 sancisce la responsabilità di chiunque cagioni un danno ad altri per effetto del trattamento di dati personali, obbligandolo a risarcire sia il danno patrimoniale che il danno non patrimoniale che dall'illecito deriva.

Tuttavia, numerose sono state le criticità riscontrate dalla dottrina e dalla giurisprudenza nell'applicazione della norma all'interno del settore delle truffe informatiche bancarie e, soprattutto, nell'individuazione in concreto del soggetto attivo punito dalla norma.

Ci si è chiesti, in particolare, se in casi siffatti dovesse ravvisarsi una responsabilità della

CamminoDiritto.it
ISSN 2421-7123

banca per non aver approntato tutti i sistemi di sicurezza necessari e idonei a scongiurare un possibile attacco informatico o se la responsabilità dovesse essere riversarsi solamente nella figura phisher o, ancora, se tale responsabilità fosse ravvisabile solo in capo al cliente che, in modo ingenuo, è caduto nella trappola predisposta dai cyber-criminali.

Sul punto, la giurisprudenza di merito non ha sempre dimostrato univocità di indirizzo.

Secondo un orientamento tradizionale, ormai superato, l'adozione da parte dell'istituto bancario di un sistema di crittografia dei dati del cliente era di per sé sufficiente ad escludere la possibilità che l'accesso ai conti personali degli utenti fosse consentito a terzi estranei.

Per tale motivo, quindi, la responsabilità per la captazione dei dati informatici ricadeva unicamente in capo al cliente, colpevole di aver adottato un comportamento incauto o negligente nell'esecuzione delle operazioni bancarie o nella custodia delle chiavi di accesso[3].

Le possibilità per gli utenti di vedersi riconosciuta una tutela a seguito di sottrazione illecita di liquidità da parte di hacker erano, quindi, assai remote.

Tale indirizzo, reputato eccessivamente gravoso nei confronti del cliente, ha subito un arresto per merito della sentenza n. 2950 del 2017 della Suprema Corte di Cassazione, che ha ribaltato l'impostazione sino a quel momento seguita, prendendo le mosse dalle coordinate fissate dal nostro ordinamento in tema di responsabilità contrattuale e facendo leva sul rapporto negoziale che intercorre tra il cliente e la banca.

Secondo questa impostazione, quindi, non solo la banca, qualora ne ricorrano i requisiti, deve essere chiamata a rispondere del danno patito dal suo utente, ma la stessa è gravata dell'onere di provare il corretto funzionamento del sistema adottato e la sua adeguatezza a fronteggiare ogni possibile attacco informatico.

Secondo i principi fondamentali del nostro ordinamento, infatti, il creditore che agisce per il risarcimento del danno, per la risoluzione del contratto o per l'adempimento, deve provare la fonte del suo diritto e il relativo termine di scadenza semplicemente allegando l'inadempimento della controparte; al contrario, sul debitore convenuto grava l'onere di provare che il fatto lamentato dall'attore sia dovuto a una circostanza a lui non imputabile, secondo quanto previsto dall'art. 1218 del codice civile.

Secondo la giurisprudenza ormai consolidata, quindi, spetta all'ente creditizio l'onere di

CamminoDiritto.it
ISSN 2421-7123

provare il corretto funzionamento del proprio sistema e la riconducibilità delle operazioni effettuate tramite le proprie piattaforme alla volontà di colui che le ha realizzate, pena l'obbligo di risarcire il danno patito dal cliente.

Sulla Banca sorge allora una diligenza qualificata ex art. 1176, c. 2 c.c., esercitando la stessa un'attività di natura tecnica e professionale, che richiede una valutazione comprensiva dei rischi tipici della professione e parametrata alla figura del "banchiere accorto".

Se ne deduce, quindi, che la corretta operatività della piattaforma di gestione del conto corrente online rientra pienamente nella sfera del rischio dell'impresa, gravando in tal modo sulla Banca una responsabilità di tipo oggettivo o semi oggettivo, che può essere confutata dalla stessa solo provando, anche in via presuntiva, che le operazioni oggetto di contestazione sono riconducibili al comportamento del cliente[4].

Si tratta di una conclusione che, peraltro, è funzionale a garantire la fiducia degli utenti nella sicurezza del sistema bancario, tutelando così lo stesso interesse degli operatori economici, e che è suffragata dalla normativa in materia di servizi di pagamento nel mercato interno, in virtù della quale è onere del prestatore di servizi fornire la prova della frode, del dolo o della colpa grave dell'utente che intenda disconoscere le operazioni di pagamento[5].

Invero, a rafforzare tale impostazione, il 14 settembre 2019 è entrata in vigore la Direttiva UE 2015/2366, nota come Payment Service Directive 2 (PSD2), con lo scopo di promuovere lo sviluppo di un mercato dei pagamenti sicuro ed efficiente e di rafforzare la tutela degli utenti dei servizi di pagamento elettronici.

Tale Direttiva si colloca nel solco già delineato con la Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007 (cd. Payment Service Directive o PSD), implementando le tecniche di tutela in relazione all'evoluzione delle tecnologie e dei sistemi di circolazione del denaro.

L'unica possibilità per la Banca di essere esente da responsabilità consiste, in definitiva, nella prova del comportamento doloso o eccessivamente incauto, tanto da non poter essere fronteggiato in anticipo, del cliente.

Va comunque esclusa, infatti, la responsabilità della Banca ogni qualvolta sia individuabile una colpa grave del cliente, configurabile, ad esempio, nel caso di protratto mancato controllo circa l'estratto conto[6].

CamminoDiritto.it
ISSN 2421-7123

Al contrario, non è ravvisabile un'ipotesi di colpa grave nel comportamento dell'utente che ometta di attivare i servizi di alert via sms o via e-mail delle disposizioni effettuate sul conto corrente online, come ormai pacificamente riconosciuto dalla giurisprudenza.

Tale servizio, infatti, pur essendo finalizzato a consentire un controllo aggiuntivo da parte del cliente, non può in alcun modo tradursi in un'esenzione della Banca dall'obbligo di accertamento e tutela dei dati della sua utenza.

L'adozione da parte dell'ente creditizio di sistemi di protezione rafforzati non vale, quindi, ad escludere la responsabilità dello stesso per gli attacchi informatici compiuti sui conti dei clienti.

Peraltro, la linea di pensiero ormai consolidata nella giurisprudenza appare molto più elastica e benevola nei confronti del cliente rispetto all'indirizzo interpretativo affermatosi in seno all'Arbitro Bancario Finanziario, il quale, in una recente decisione in tema di phishing, ha affermato che «mentre non può ravvisarsi un comportamento colposo del cliente qualora egli, a causa di un virus (malware, trojan, man in the browser), si veda sottrarre le proprie credenziali di accesso, è invece senz'altro connotato dall'elemento soggettivo della colpa grave il comportamento di chi "abbocchi" ad una tradizionale mail di phishing. Nello specifico il Collegio di coordinamento, con la decisione n. {https/URL}: colpevole in quanto egli è portato a comunicare le proprie credenziali di autenticazione al di fuori del circuito operativo dell'intermediario e tanto più colpevole si rivela quell'atto di ingenuità quanto più si consideri che tali forme di "accalappiamento" possono dirsi ormai note al pur non espertissimo navigatore di internet.»[7]

È evidente la distanza che intercorre tra tale orientamento e quello seguito invece dai Tribunali ordinari e dalla stessa Corte di Cassazione, teso ad abbracciare una visione maggiormente garantistica nei confronti del cliente.

5. L'attualità del problema ai tempi del Covid-19

La tematica in esame assume profili di grande attualità all'interno del periodo storico che stiamo attraversando, il quale di certo si propone come terreno fertile per il proliferare di episodi di phishing e di truffe informatiche.

Ciò per un duplice ordine di ragioni.

Da un lato, è evidente che l'emergenza pandemica che incoraggia, e certe volte obbliga, a

CamminoDiritto.it
ISSN 2421-7123

rimanere in casa e a servirsi sempre più frequentemente dei servizi di pagamento online, aumenta le possibilità di essere vittime di truffe informatiche, spingendo peraltro gli hacker ad aumentare la loro attività criminale.

Dall'altro, la crescente attenzione rivolta al Covid-19 è stata utilizzata dai phisher per diffondere malware e rubare le credenziali degli utenti mediante e-mail ed sms che promuovono finte campagne di beneficienza o che promettono benefici finanziari.

Lo stesso CNAIPIC, il Centro Nazionale Protezione Infrastrutture Critiche incardinato presso la Polizia Postale, ha messo in guardia gli utenti circa una nuova campagna di phishing legata al tema dell'epidemia Covid-19[8].

Sempre maggiore si rivela allora lo sforzo richiesto agli operatori economici al fine di prevedere e fronteggiare le operazioni fraudolente da parte di terzi e garantire la sicurezza dei dati dei propri utenti, ai quali, comunque, come testimoniato dai recenti interventi giurisprudenziali, viene riconosciuta una tutela pressoché assoluta, superabile solo nel caso in cui la loro condotta sia inficiata da colpa grave.

CamminoDiritto.it
ISSN 2421-7123

Note e riferimenti bibliografici

[1] Articolo introdotto con la legge 23 dicembre 1993 n. 547.

[2] Così come affermato in Cass. Pen. n. 37115/2002.

[3] Ex multis: Corte d'Appello di Trento, n. 68/2011.

[4] Tribunale di Parma, n. 1268/2018.

[5] Tale impostazione, nata in ambito europeo e fatta propria dal legislatore nazionale, è ormai da tempo recepita anche dalla giurisprudenza maggioritaria; in proposito, vd. Tribunale di Milano n. 7644/2018.

[6] Cass. Civ. n. 18045/2019.

[7] ABF 396/2020, Collegio di Roma su phishing, rimborso e risarcimento banca.

[8] {https/URL}

* Il simbolo {https/URL} sostituisce i link visualizzabili sulla pagina: https://rivista.camminodiritto.it/articolo.asp?id=6228