Non sempre in caso di phishing la banca è tenuta a risarcire il cliente

Autore: De Luca Maria Teresa
In: Diritto civile e commerciale

Sono sempre più numerosi i casi di c.d.
phishing,
una truffa on-line attuata da soggetti, indicati come phisher, che non sono altro che truffatori e ladri di informazioni personali dotati di competenze tecniche. Utilizzano lo spamming, siti Web ingannevoli, e-mail e messaggi istantanei per indurre le persone a divulgare informazioni riservate, quali ad esempio dettagli sul conto corrente e sulle carte di credito.

Con la sentenza n. 3028 depositata il 10 novembre 2015 il Giudice di Pace di Messina, dott.ssa Anna Aricò, ha rigettato la domanda di un cliente, titolare di un conto corrente
su cui era stato attivato il servizio di home banking, che pretendeva di essere risarcito dalla banca per il danno subito per una truffa informatica subita.

L'attore, infatti, esponeva che nell'accedere al proprio indirizzo di posta elettronica apriva una e-mail (apparentemente) proveniente dalla banca, con la quale veniva invitato ad inserire i suoi codici di sicurezza, a causa di una presunta “manutenzione per misure di sicurezza”.

Attraverso questo espediente i phishers effettuavano una ricarica internet di una carta prepagata con addebito sul conto corrente dell'attore.

L'interrogativo che si è posto il Giudice di Pace di Messina è il seguente: appurato
e non contestato che si sia in presenza di un caso di phishing

Diritto & Diritti ISSN 1127-8579

è configurabile nella fattispecie una responsabilità della banca per l'abusiva utilizzazione delle credenziali informatiche del correntista nell'ambito del servizio di home banking?

Per rispondere a tale domanda, il giudice, preliminarmente, ha operato una distinzione tra il phishing meno evoluto, dove l'aggiramento dei presidi di sicurezza ha luogo attraverso metodi che il cliente, usando un minimo di diligenza, è oggettivamente in grado di riconoscere, per cui l'eventuale sua credulità non risulta scusabile, e le versioni più sofisticate della stessa tecnica, che, sebbene conosciute dai cultori della scienza informatica, non permettono all'utente medio di prendere alcuna contromisura e che escludono la ravvisabilità di una colpa grave in capo allo stesso.

Nel caso in esame il correntista, dopo aver ricevuto una e-mail cd. “spam”, scritta
in un italiano scorretto e sgrammaticato,
ha inserito le proprie credenziali di accesso all'home banking sul sito indicato dai phishers.

Appare evidente, secondo il giudice, che la condotta tenuta dall'attore sia stata poco accorta o ingenua, e che, nel caso de quo, era facile per il cliente
accorgersi di trovarsi dinanzi ad una e-mail fraudolenta, come tale neutralizzabile dall'utente medio del servizio di home banking.

Ebbene, il Giudice di Pace di Messina ha ravvisato una colpa grave nella condotta dell’attore-correntista, ai sensi degli degli artt. 7 e 12 del D. LGS. n. 11 del 27.10.2010, in vigore dal 1°.3.2010 che ha dato attuazione in Italia alla direttiva comunitaria n. 2007/64 Ce relativa ai servizi di pagamento nel mercato interno e che regola, tra l'altro, anche il servizio di home banking.

Per il giudice dall'esame degli atti di causa
è emerso che l'attore ha dato seguito ad una e-mail oggettivamente di immediata riconoscibilità truffaldina, comunicando a terzi le proprie credenziali di accesso al conto on-line e ciò nonostante a pag.

Diritto & Diritti ISSN 1127-8579

18 della Guida ai Servizi della Banca è dato leggere testualmente “le politiche di sicurezza del nostro sito non prevedono in nessun caso la richiesta di inserire i codici di accesso via mail o telefonicamente; nel caso dovesse ricevere richieste di questo tipo la invitiamo a contattare prontamente il nostro Servizio Clienti”.

In questo modo, secondo il giudice, il cliente ha creato una situazione di fatto idonea a sfuggire a qualsiasi controllo della Banca, poiché lo stesso, negligentemente, ha consentito a terzi di venire a conoscenza delle proprie credenziali di accesso al conto on-line, e pertanto, l'Istituto, a seguito della sua condotta,
non ha avuto modo alcuno di impedire che i phishers operassero nell'immediatezza e con le modalità utilizzate nel caso de quo, ossia attraverso una operazione isolata di ricarica di carta prepagata, di importo non eccessivamente elevato che, per le sue caratteristiche, era inidonea a generare sospetti nel prestatore di servizi.

La domanda attrice è stata, pertanto, rigettata.

https://www.diritto.it/non-sempre-in-caso-di-phishing-la-banca-e-tenuta-a-risarcire-il-cliente/

Diritto & Diritti ISSN 1127-8579