CENNI INTRODUTTIVI

In questi ultimi anni, a seguito dello sviluppo impetuoso del settore informatico e dell'utilizzo di massa delle nuove tecnologie da parte di soggetti meno avvezzi o "ingenui", si evidenzia uno sviluppo notevole e preoccupante di condotte fraudolente atte a impossessarsi in maniera illecita di dati sensibili quali *password* e/o informazioni strettamente personali al fine di poter accedere in modo illecito a settori vulnerabili della vita privata.

Tale problema si evidenzia, soprattutto, nell'eventualità di accesso alle *password* riguardanti la gestione dei conti correnti bancari, di carte di credito, di bancomat o, comunque, ogni genere di carta o servizio in materia bancaria[1].

Il sistema per carpire tali dati è tanto semplice quanto spesso, purtroppo, molto efficace.

Un c.d."*phisher*", in genere soggetto esperto nell'utilizzo della tecnologia informatica, riproduce una pagina *web* similare a quella dell'istituto di credito o al soggetto istituzionale (es. Poste) che offre un determinato servizio di gestione di denaro e poi inoltra tramite posta elettronica un falso avviso richiedendo con urgenza all'utente *password* e codici sensibili.

L'utente, ricevuta la *mail*, con ingenuità, cerca di entrare subito sul *link* indicato dalla posta elettronica, contenente la pagina *web* "falsa", e fornisce i propri dati.

[1] Nella provincia di Milano si contavano circa 7.000 casi di truffa telematica nel solo anno 2003 (articolo di Alberto Berticelli, "*Reati ed arresti in aumento. Record delle truffe online*", Il Corriere della sera, 23 dicembre 2003); nel settembre 2012 quasi un terzo dei casi affrontati dall'Arbitro Bancario Finanziario in tema di problemi utenti / istituto di credito riguardano questo annoso problema (articolo di Manlio Torquato, " *Quando scatta il phishing il cliente può «salvarsi»*", "Il Sole 24 ore", 29.09.2012).

Ottenuto così quanto richiesto il "*phisher*",spesso residente all'estero o, comunque, che utilizza più server per non farsi identificare, preleva il denaro contenuto nel conto corrente del soggetto che ha riscontrato la falsa richiesta e lo reindirizza in diversi conti correnti di altri soggetti.

Il "*phisher"*, a questo punto, ha due possibilità.

Nel primo caso lo reindirizza subito ad un conto corrente di un soggetto compiacente, magari residente all'estero, contando sulla distanza e le lentezze burocratiche degli istituti di credito, per poi impossessarsi dell'intera somma.

In un secondo caso i "*phishers* " più "cauti" reindirizzano il prelievo illecito presso un conto corrente di un soggetto terzo (c.d."*financial manager*") il quale, successivamente, ritirate prontamente le somme, le inoltrerà al "*phisher"* tramite sistemi diversi quali *money trasfert*, trattenendosi una quota a compenso della propria prestazione illecita.

Fatte tali premesse, occorre ora verificare quali rimedi possono essere esperiti per poter ricevere una tutela e comprendere per quali reati il "*phisher"* ed il *"financial manager"* possono essere perseguiti.

Come già espresso in precedente articolo dell'autore[2], per quanto attiene alla posizione delle vittima del reato sarebbe opportuno, a fini riparatori, prediligere maggiormente una eventuale azione civile avverso il proprio intermediario bancario (sempre che ve ne sia effettivamente la possibilità!) ma, nell'eventualità la colpa di ciò sia da attribuirsi solo ad una condotta poco diligente del danneggiato, l'unica strada giuridica da percorrere è l'eventuale azione di

[2] B. Ravagnan,"*Frode telematica: il c.d. "phishing". Problematiche generali e strategie processuali in ambito civile per la restituzione della somma indebitamente sottratta e il ristoro del danno non patrimoniale*", sito internet "www.borsa – banca.it"

risarcimento danni derivante da un accertamento della responsabilità degli imputati in sede penale.

PRINCIPI BASILARI DI TUTELA IN CASO DI LESIONE DA "PHISHING"

Verranno esposti ora alcuni principi basilari da seguire in ogni caso nell'eventualità in cui si sia vittime di *phishing*.

Constatata la violazione, sia essa di natura patrimoniale o meno, occorre attivarsi prontamente contattando l'istituto che gestisce il servizio al fine di ottenerne l'immediato blocco e limitare, per quanto possibile, i danni.

Successivamente dovrà essere proposta una apposita denuncia – querela entro e non oltre tre mesi dalla scoperta del danno.

Si precisa che la denuncia – querela può essere presentata già in forma scritta, magari con documenti allegati, oppure può essere formulata oralmente.

In quest'ultimo caso l'Autorità rilascerà copia del verbale di cui darà conto di quanto esposto.

Ciò, anche se difficilmente porterà alla precisa individuazione del reo od al recupero di quanto illegittimamente sottratto, avrà l'effetto di indurre l'Autorità Giudiziaria ad indagare sull'evento.

In prospettiva futura, comunque, la denuncia – querela potrebbe esser prodotta come prova documentale in sede di procedimento civile (o nell'azione civile a risarcimento del danno all'interno del procedimento penale) dimostrando che il soggetto si è fatto parte diligente, attivandosi subito appena resosi conto dell'evento lesivo.

Quest'atto formale, altresì, potrebbe fornire ulteriori prove a favore del danneggiato: le indagini, infatti, pur senza giungere all'individuazione del reo, potrebbero fornire elementi interessanti

quali l'indirizzo IP da cui ha avuto origine la violazione, se ha colpito serialmente, in che modo eventualmente è riuscito ad aggirare i sistemi di sicurezza dell'istituto che doveva custodire i dati.

Appare opportuno coltivare la denuncia recandosi periodicamente ad assumere informazioni presso l'Autorità e facendo presente (col suggerimento di farlo verbalizzare) sin dal primo momento che si vuole essere informati in caso di archiviazione della *notitia criminis* [3], così, in futuro, quando sarà comunicato il provvedimento del P.M., valutare se sia il caso di opporsi a tale richiesta (entro dieci giorni dalla ricezione dell'atto!) oppure rinunciare definitivamente alla prosecuzione.

Si suggerisce, in questi casi, di eleggere domicilio presso il proprio effettivo domicilio e comunicarne eventuali variazioni così da consentire una notifica precisa e tempestiva.

Un eventuale errore, infatti, se da un lato impedirebbe al soggetto di esserne adeguatamente informato, comporterebbe altresì l'impossibilità di opporsi all'archiviazione stante lo spirare dei termini che, si badi, sono perentori.

In questo modo, a prescindere dai risultati finali delle indagini, si potranno raccogliere preziose informazioni per il tramite di un canale ufficiale e sicuro, qual è quello delle forze di polizia.

BREVE PANORAMICA SULLE IPOTESI DI REATO ATTRIBUIBILI AL C.D. "PHISHER" ED AL "FINANCIAL MANAGER"

Seppur la denuncia – querela sia già completa ed idonea a cagionare l'effetto di attivare l'Autorità Giudiziaria anche senza la specifica indicazione di quali fattispecie di reato si vadano

[3] Ci si richiama, in questo caso, alla disciplina ex art. 408 – 410 c.p.p

a contestare, può apparire opportuno comunque indicare, magari anche per sommi capi, i reati principali di cui il soggetto leso sia stato vittima.

Il nostro ordinamento penale, infatti, non prevede un reato specifico sotto cui sussumere la condotta rimproverata ma, piuttosto, un concorso di reati di "natura" informatica.

Valutiamo i principali in ordine crescente, dal meno grave al più grave.

Dapprima sicuramente il "*phisher"* sarà perseguibile per il reato di "sostituzione di persona" *ex* art. 494 c.p.

Il reato sanziona chiunque, al fine di procurare a sé od altri un ingiusto vantaggio, induce qualcuno in errore sostituendosi ad un diverso soggetto.

Nel caso di specie il "*phisher"*, simulando di essere un ente od un soggetto diverso, ha pienamente integrato tale condotta poiché ha agito inducendo in errore la vittima con il precipuo fine di ottenere un guadagno quindi con un dolo c.d. specifico poiché motivato al fine di ottenere un guadagno (differenziandosi per questo dal dolo c.d. "generico" che richiede solamente la coscienza e volontà dell'azione, senza un precipuo scopo).

Secondo alcuni correnti giurisprudenziali, è possibile perseguire da tale condotta anche il reato di "falsificazione di corrispondenza informatica" *ex* art. 617 *sexies* c.p. poiché il reo, agendo come sopra illustrato, avrebbe inoltrato, appunto, una comunicazione informatica creando un testo assolutamente falso e cagionando un errore in capo alla vittima.

Occorre ora concentrarsi sulle due fattispecie criminose di maggior interesse.

STUDIO LEGALE POLATO
30174 Venezia – Mestre, Via C. Battisti n. 7
Tel. 041 98 53 77 Fax 041 95 20 53
31100 Treviso, Strada Comunale Corti n. 56 int. 2
Tel. 0422 42 33 50 Fax 0422 31 60 98
studiolegalepolato@tiscali.it
www.banca-borsa.it

Sicuramente il "*phisher"* integra il reato di accesso abusivo ad un sistema informatico *ex* art. 615 *ter* c.p. che sanziona chiunque si introduca in un sistema informatico in maniera abusiva[4].

La giurisprudenza, dopo lunghe esitazioni, ritiene oggi che il reato sia perseguibile nell'eventualità in cui il soggetto acceda in qualsiasi modo ad un sistema contro la volontà del soggetto a prescindere dalle finalità che l'abbiano spinto a farlo[5].

Appare evidente che anche l'inoltro di una mail con scopo fraudolento possa integrare tale fattispecie.

Ultimo punto da prendere in considerazione è il reato di frode informatica *ex* art. 640 *ter* c.p. che estende la disciplina della truffa *ex* art. 640 c.p. anche ai raggiri informatici.

Per integrare l'art. 640 *ter* c.p. si richiede, quindi, l'accesso abusivo ad un sistema informatico tramite raggiro e l'ingiusto profitto derivante da ciò (cioè il prelievo dal conto)[6].

Nell'eventualità il "*phisher*" abbia accesso ad un sistema di un ente statale o di interesse nazionale (es. Poste) scatterà immediatamente anche l'aggravio (quindi il reato di frode informatica aggravata)[7].

In conclusione occorre ora affrontare i reati attinenti alla posizione del "*financial manager*".

Quest'ultimo, infatti, in genere è più facile da reperire poiché risulta colui il quale ha ricevuto direttamente il prelievo fraudolento.

[4] Di recente Cass. Sez. Pen. 27.09.2013 n. 40303 ha ritenuto che, in tema di accesso abusivo a sistema informatico o telematico, la competenza territoriale sia del giudice del luogo ove è collocato il server violato.

[5] In tal senso, dirimente la sentenza Cass. Sez. Pen. Sez. Unite 07.02.2012 n. 4694

[6] La sentenza più importante in tale tema è Corte d'Appello Milano 07.10.2011

[7] In tale senso Cassazione Penale, Sez. II, 24.02/11.03.2011 n° 9891, la quale conferma, altresì, il concorso fra i reati di frode informatica ex art. 640 ter c.p. e di accesso abusivo a sistema informatico ex art. 615 ter c.p.

Nell'eventualità sia dimostrata una connivenza il problema non si pone poiché egli andrà soggetto ad imputazione penale per i medesimi reati del "*phisher"* risultando quindi un concorso di persone nel reato *ex* art. 110 c.p. (detto in modo gergale il c.d. "complice").

Più complesso sarà l'eventualità che il soggetto fosse all'oscuro di tutto o convinto in buona fede di operare nella legalità (alla luce però di precisi elementi oggettivi e fattuali che la difesa dello stesso dovrà dimostrare).

In questo caso, venuto meno l'elemento soggettivo del reato (cioè la colpevolezza, intesa come un comportamento rimproverabile), sarà improbabile che l'Autorità ritenga di sanzionarlo per i reati sopra meglio inquadrati.

Ad ogni modo la giurisprudenza ritiene comunque sanzionabile tale condotta per i reati di ricettazione (art. 648 c.p.) o di riciclaggio (art. 648 *bis* c.p.), a seconda che l'agente si sia limitato a ricevere le somme di denaro con l'elemento soggettivo del dolo eventuale (cioè essendo consapevole della loro provenienza illecita ed accettando il rischio di procedere nell'azione delittuosa), oppure si sia limitato a trasferire le somme al "*phisher*" con modalità idonee ad ostacolare l'identificazione della loro provenienza.

In quest'ultimo punto si rammenti la sentenza Cass. pen., Sez. II, 17.06.2011 n. 25960 *"Il dolo di ricettazione o riciclaggio può dirsi sussistente in capo al financial manager solo quando, sulla base di precisi elementi di fatto, si possa affermare che questi si sia seriamente rappresentato l'eventualità della provenienza delittuosa del denaro e, nondimeno, si sia comunque determinato a riceverlo e trasferirlo all'estero con le modalità indicate dal phisher*".

Per completare quanto sinora esposto si rammenta nuovamente, in sede di proposizione di denuncia – querela, di aggiungere comunque alla fine una ampia riserva lasciando che sia

l'autorità ad identificare precisamente quali reati contestare, così da ovviare all'eventualità, sempre possibile, che qualche pubblico ministero ritenga di apprezzare ulteriori condotte a fini di rimproverabilità penale.

In tema di tribunale competente, infine, si ricordi come la legge 18.03.2008 n. 48, nel risistemare la disciplina sostanziale e processuale in materia di reati informatici, abbia ulteriormente ampliato il numero dei reati attribuiti alla competenza dei pubblico ministero presso il tribunale del capoluogo del distretto, indicato quindi come tribunale naturale per la perseguibilità di tali reati.

Si precisa che, in ogni caso, la denuncia – querela possa esser presentata presso qualsiasi ufficio o caserma delle forze di polizia, senza che venga a rilievo in alcun modo la competenza del tribunale penale, che assume valore solo per l'instaurazione del processo penale.

CONSIDERAZIONI FINALI

Come precedentemente rammentato, in tale ambito la decisione di agire penalmente, pur molto importante ed in ogni caso consigliata, potrebbe non portare agli effetti riparatori voluti dal soggetto leso, stante anche l'incapienza economica dei rei.

Ad ogni modo, un'indagine approfondita potrebbe portare al recupero almeno parziale della somma o, perlomeno, all'identificazione di qualche soggetto operante in ambito nazionale.

Nell'eventualità ciò accada, sarà opportuno valutare, per il tramite della consulenza di un legale, se valga la pena costituirsi parte civile in ambito di procedimento penale e chiedere in quella sede un risarcimento del danno sia per i danni di natura patrimoniale (la somma concretamente sottratta), sia non patrimoniale (danni morali, biologici etc.) che, però, sono da dimostrarsi.

STUDIO LEGALE POLATO
30174 Venezia – Mestre, Via C. Battisti n. 7
Tel. 041 98 53 77 Fax 041 95 20 53
31100 Treviso, Strada Comunale Corti n. 56 int. 2
Tel. 0422 42 33 50 Fax 0422 31 60 98
studiolegalepolato@tiscali.it
www.banca-borsa.it

L'alternativa (non cumulativa!) rispetto all'azione civile nel processo penale è adire direttamente le vie giudiziarie in ambito civile facendo valere una responsabilità cagionata da fatto illecito *ex* art. 2043 c.c.

(a cura di Bruno Ravagnan)

STUDIO LEGALE POLATO
30174 Venezia – Mestre, Via C. Battisti n. 7
Tel. 041 98 53 77 Fax 041 95 20 53
31100 Treviso, Strada Comunale Corti n. 56 int. 2
Tel. 0422 42 33 50 Fax 0422 31 60 98
studiolegalepolato@tiscali.it
www.banca-borsa.it