

Massimo Melica
Presidente Centro Studi di Informatica Giuridica

Le nuove insidie per il cyber utente: Phishing e il riciclaggio

1. Premessa 2. Il *modus operandi* del phishing 3. Il phishing come truffa e/o frode informatica 4. Il riciclaggio e la responsabilità dell'utente

1. Premessa. L'espressione phishing deriva dalla deformazione lessicale del verbo inglese *to fish* che significa pescare. L'uso della parola è strettamente connesso con l'immagine che essa evoca, ovvero la "pesca" di utenti nella rete, pronti ad abboccare alle insidie disseminate dai malintenzionati.

Una società di ricerca ha stimato che le perdite dirette per frode negli Stati Uniti attribuibili al phishing, hanno raggiunto nel 2004 i 137 milioni di dollari. Tuttavia occorre ammettere che, proprio nel 2005, questo fenomeno ha smesso di essere trattato e descritto soltanto dalla cronaca giudiziaria e dalla letteratura giuridica d'oltre oceano, ed è entrato di prepotenza nella vita e nella storia del nostro Paese. Ciò ha portato anche noi giuristi italiani a doverci confrontare con questa nuova insidia telematica, che presenta aspetti decisamente nuovi da descrivere alla luce dei principi e delle norme del nostro ordinamento.

Il fenomeno phishing riguarda da vicino anche noi avvocati, sia perché, come detto, siamo chiamati ad interpretare tali fenomeni giuridici alla luce degli istituti già conosciuti e codificati, ma anche perché il phishing interessa da vicino due realtà ben note al legale: l'internet e l'e-banking.

Le carte di credito, i conti correnti on-line, i codici relativi a depositi effettuati in banca, i pin dei bancomat. Tutte queste informazioni costituiscono l'obiettivo del phisher (ovvero l'autore degli atti di phishing), il quale, per riuscire a snidare il danaro sottratto dai legittimi titolari, si serve anche della incauta collaborazione degli stessi utenti. La compartecipazione degli utenti a questa truffa telematica, come vedremo, è indispensabile per consentire ai phishers di ricondurre il danaro sottratto nella propria disponibilità attraverso complesse operazioni bancarie.

Nell'esecuzione dei propri disegni, il phisher si avvale dell'imprudente attivismo di molti utenti, i quali, senza saperlo, si trovano poi coinvolti in indagini penali relative a riciclaggio.

È bene premettere, tuttavia, che, contrariamente a quanto potrebbe credersi, le principali armi del phisher non sono le sue risorse tecnologiche, che pure non gli mancano, bensì la sua *vis* persuasiva, ovvero le sue tecniche di ingegneria sociale.

2. Il *modus operandi* del phishing. Il phishing consiste nell'invio massiccio di messaggi di posta elettronica, o comunque telematici (spamming), apparentemente provenienti da società affidabili, come banche e/o imprese che comunque si muovono nell'ambito creditizio. Messaggi che in realtà sono assolutamente falsi, oltre che ingannevoli. Chi invia tali messaggi spera di carpire l'attenzione del destinatario, inducendolo a recarsi presso un sito, indicato in link all'interno del messaggio. Nel testo del capzioso messaggio inviato, i truffatori generalmente rappresentano talune improcrastinabili esigenze di sicurezza che si traducono nell'invito perentorio a recarsi presso il sito indicato nel link al fine di inserire e/o modificare i codici d'accesso personali relativi ai propri conti on line. Non appena viene visualizzato il sito relativo al link inserito nel messaggio, nel computer dell'utente viene visualizzata una pagina web in tutto e per tutto identica a quella del proprio istituto di credito. Il fenomeno della "clonazione" di pagine web viene chiamato "pharming". Non appena vengono inseriti i codici relativi al proprio *account* on line, i phishers sono in grado di recuperare quelle informazioni per accedere al reale conto bancario o postale dell'utente e sottrarre illecitamente il denaro in esso contenuto.

Dopo aver sottratto il denaro dal conto del truffato, l'ulteriore obiettivo del phisher è quello di far perdere le tracce informatiche dei propri accessi e soprattutto del denaro sottratto. Tali fraudolenti obiettivi vengono generalmente perseguiti attraverso una complessa serie di trasferimenti bancari, avvalendosi della complicità di ignari utenti. Gli autori del phishing inviano nuovamente messaggi elettronici (oppure si camuffano da imprese in cerca di collaboratori) promettendo opportunità di guadagno e/o di lavoro. La collaborazione che essi chiedono agli aspiranti

lavoratori consiste nel chiedere loro la disponibilità del proprio conto corrente, ove dovranno essere “ospitate” per qualche tempo determinate somme di denaro, per poi trasferirle, tramite bonifici, presso altri conti correnti o a favore di determinati soggetti fiduciari. Il tutto verso il corrispettivo di una percentuale del valore delle somme depositate e poi trasferite. In tal modo le somme illecitamente trafugate tramite il phishing vengono fatte circolare attraverso molteplici conti correnti (rendendo difficile il lavoro degli investigatori che dovranno ricostruire tutti i relativi tragitti telematici) finché non vengono inviati verso l'estero, o presso i fiduciari dei truffatori.

Anche in Italia la tecnica utilizzata per colpire gli utenti italiani attraverso il phishing è stata, innanzitutto lo spamming. False un'e-mail apparentemente proveniente dal proprio istituto di credito (in particolare Banca Intesa, Unicredit, Bancoposta, Fineco i casi più frequentemente riscontrati) sono state inviate a milioni di utenti presso i rispettivi indirizzi di posta elettronica. Nei messaggi si informavano i destinatari che, a causa di un non meglio precisate esigenze di sicurezza, risultava necessario collegarsi presso il sito linkato nell'e-mail, entrare nella sezione riservata al proprio conto e compilare un apposito formulario. Secondo stime prudenziali effettuate da alcuni studiosi, circa il 10 % dei messaggi di phishing è andato comunque a buon fine, nel senso che ha indotto effettivamente gli utenti a rilasciare i propri codici d'accesso all'interno dei siti “clone”. Emblematico è stato il caso di un'inchiesta conclusasi durante il mese d'agosto a Milano, quando gli inquirenti sono stati in grado di bloccare circa 1,4 milioni di euro, trafugati tramite tecniche di phishing, pronti per essere trasferiti all'estero dove probabilmente sarebbe stato difficilissimo recuperarli.

Com'è evidente, il phishing sfrutta l'ingenuità, l'ignoranza ma anche la disattenzione degli utenti. Il messaggio di posta elettronica del phisher è generalmente scritto in un italiano non sempre inappuntabile (anche se gli ultimi casi hanno messo in luce un notevole affinamento del lessico utilizzato). Un utente accorto avrebbe, infatti, buon gioco a notare le imperfezioni linguistiche utilizzate dal phisher nel suo messaggio capzioso. Talvolta basterebbe una maggiore

attenzione nella lettura dei messaggi ricevuti per rendersi conto che non potrebbero mai provenire dalla propria banca.

Dal punto di vista giuridico il phishing si presenta come un fenomeno decisamente complesso e si caratterizza come un illecito che presenta profili sia di natura sia civile che penale. Sponderemo alcune considerazioni su questi ultimi.

Sappiamo che nell'ordinamento giuridico italiano non esiste alcuna legge che preveda una definizione del fenomeno sopra descritto come phishing, il quale si configura come una concatenazione di azioni finalizzate all'esecuzione di un unico disegno criminoso. Da un punto di vista penale le attività relative al *modus operandi* del phishing risultano idonee ad integrare gli estremi di svariate ipotesi di reato previste dal codice penale: dall'art. 640 (truffa), 640 *ter* (frode informatica), al 648 bis (riciclaggio.)

È interessante osservare in che modo l'utente possa trovarsi coinvolto, con un ruolo di inconsapevole complicità, all'interno dell'attività criminosa compiuta dal phisher. Risulta parimenti interessante sottolineare come la compartecipazione - generalmente involontaria - dell'utente al disegno criminoso del malfattore costituisce anche un disdicevole intralcio all'attività investigativa degli inquirenti.

3. Il phishing come truffa e/o frode informatica. La natura "ontologica" del phishing è senz'altro connessa alla truffa, figura di reato descritta dall'art. 640 del codice penale. Recita la norma penale a tal proposito: «*chiunque, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a milletrentadue euro*».

Oltre all'ipotesi delittuosa della truffa, il phishing integra gli estremi di un altro concomitante reato: la frode informatica, di cui all'art. 640 *ter* del codice penale: «*chiunque alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico, o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da cinquantuno euro a trentadue euro*».

Il reato di frode informatica, come ha ricordato più volte la giurisprudenza della Cassazione (v., in particolare Cass. sez. IV, 4 ottobre 1999, n. 3056) ha la medesima struttura, e quindi i medesimi elementi costitutivi, della truffa, dalla quale si distingue solamente perché l'attività fraudolenta dell'agente investe non la persona, bensì il sistema informatico (significativa è la mancanza del requisito della "induzione in errore" nello schema legale della frode informatica, presente invece nella truffa). Di talché il phishing da un lato, induce in errore la persona che fornisce inconsapevolmente i propri dati al phisher, dall'altro lato la sua azione investe il sistema informatico dell'istituto creditizio poiché interviene *sine titulo* all'interno dello stesso.

La norma istitutiva del reato di frode informatica, di cui all'art. 640 c.p., punisce, infatti, chiunque «*interuenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno*». Quindi il phisher, carpendo i dati di utenti di istituti di credito ed accedendo nei rispettivi account, interviene all'interno del sistema informatico dell'istituto di credito senza averne alcun titolo, e, ove sottragga, o comunque manometta, i valori rinvenuti all'interno realizza gli estremi del reato previsto dall'art. 640 *ter* c.p..

Il reato di frode informatica presenta numerose analogie con quello di truffa: identico trattamento sanzionatorio (da sei mesi a tre anni unitamente alla multa da 51 a 1032 euro), e analoga suddivisione fra un'ipotesi delittuosa semplice ed una aggravata dagli stessi elementi previsti dal secondo comma dell'art. 640, e analogo simmetrico richiamo alla procedibilità a querela nell'ipotesi semplice legato procedibilità officiosa nell'ipotesi aggravata.

4. Il riciclaggio e la responsabilità dell'utente. Dopo aver sottratto illecitamente il denaro dai conti correnti delle vittime del phishing, gli autori dei reati hanno la necessità di far transitare all'interno di conti correnti non agevolmente individuabili dagli inquirenti il denaro trafugato, prima di incassarlo.

Per realizzare tali criminosi intendimenti, i phishers non lesinano artifici fantasiosi e maliziosi, come ci testimonia la cronaca giudiziaria di questi ultimi giorni. Sono presenti su internet numerose società che promettono facili guadagni in cambio di

posti lavoro da “cassiere” atipico. Il lavoro richiesto presuppone che l’aspirante lavoratore debba mettere a disposizione della società committente il proprio conto corrente. Il lavoro, in realtà, consiste nel ricevere del denaro e quindi inviarlo presso ulteriori conti correnti indicati dalla società, in cambio, generalmente, di una provvigione percentuale sul danaro transitato.

L’attività degli inquirenti ha portato ad individuare diverse pseudo società (come Platin Way, Sateny, Silvestry Enterprise, e numerose altre, come segnalato in diversi siti che si occupano della lotta al phishing, come ad esempio l’americano Anti-phishing.org, o l’italiano Anti-phishing.it) che promettono guadagni facili, ma che in realtà prevedono un sostanziale coinvolgimento dell’utente nelle attività di riciclaggio del denaro sottratto.

Recita infatti l’art. 648 bis c.p. *«chiunque sostituisce o trasferisce denaro, beni o altre utilità provenienti da delitto non colposo; ovvero copie in relazione ad essi altre operazioni, in modo da ostacolare l’identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da milletrentadue euro a quindicimilaquattrocenonovantatre euro».*

Il delitto di riciclaggio, introdotto nel codice penale dalla legge 9 agosto 1993, n. 328, fa quindi riferimento al compimento di specifiche operazioni consistenti nella sostituzione o nel trasferimento del denaro di illecita provenienza. Tali operazioni, in ogni caso, ostacolano il lavoro degli inquirenti volto all’identificazione della provenienza delittuosa di denaro, realizzando gli estremi della norma incriminatrice. Non è richiesta dalla norma la circostanza che la condotta dell’agente sia finalizzata al rientro del bene nella disponibilità dell’autore del reato presupposto. Pertanto, la posizione di chi abbia inteso collaborare con società di servizi presenti su internet, al fine di guadagnare grazie alla concessione della disponibilità del proprio conto, è indubbiamente delicata, per non dire compromettente. Accettando le offerte di lavoro on line rispondenti ai requisiti sopra descritti, il rischio di vedersi coinvolti in un processo per riciclaggio è altissimo, per certi versi inevitabile (perlomeno limitatamente al coinvolgimento nelle indagini preliminari, ove dovrà essere appurato l’effettivo coinvolgimento dell’utente nel reato sotto il profilo della verifica della sussistenza dell’elemento soggettivo dello stesso). Il ruolo dei giuristi, in questa fase, è cruciale: ogni avvocato dovrebbe contribuire a mettere in guardia i propri

clienti dal cedere alle lusinghe presenti nella rete che prospettano agevoli introiti con minimi costi, poiché probabilmente egli soltanto ha i mezzi per poter individuare i profili di responsabilità penale connessi a tali pratiche.

Per non cadere nelle trappole del phishing e per non vedersi coinvolti, nostro malgrado, in procedimenti penali relativi al riciclaggio, come ricordano gli inquirenti, i consigli da seguire sono prettamente due.

Il primo è non credere e non dar seguito a messaggi elettronici che richiedono informazioni personali riservate o peggio ancora codici d'accesso a conti correnti, poiché tali informazioni non possono essere richieste, né tantomeno rilasciate, con modalità insicure come e-mail non certificata, o comunicazioni sprovviste di adeguate autenticazioni.

Il secondo è quello di non credere a chi promette facili profitti chiedendo in contropartita la disponibilità del proprio conto corrente.