ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

IL PHISHING

David D'Agostini, Antonio Piva

1. Introduzione

Con il termine "*phishing*" (dal verbo inglese "fish", a indicare il fatto che le vittime vengono prese all'amo lanciando delle esche nel mare di utenti di internet) si fa riferimento a un'attività truffaldina che, sfruttando il *social engineering*[1], mira a ottenere l'accesso al conto corrente del malcapitato, dal quale vengono prelevate somme di denaro generalmente trasferite all'estero.
Il phishing è un vero e proprio attacco, condotto soprattutto per mezzo della posta elettronica (Figura 1), che si realizza per esempio nel seguente modo:
1. il truffatore (*phisher*) invia un'e-mail che simula nella grafica e nel contenuto quella di un soggetto noto al destinatario (per esempio il suo istituto di credito);
2. l'e-mail contiene quasi sempre avvisi di problemi verificatesi con il proprio conto corrente o richieste di verifiche dell'account medesimo;
3. il messaggio invita la vittima a seguire un collegamento ipertestuale che, tuttavia, non porta al sito web ufficiale, bensì a una copia apparentemente simile al medesimo messa on line dal phisher;
4. quest'ultimo, pertanto, carpisce le credenziali di autenticazione[2] del correntista e le utilizza per acquistare beni ovvero per bonificare somme di denaro;
5. spesso tale denaro transita sul conto di un terzo che (a conoscenza o meno della provenienza illecita) si presta a trasferirlo all'estero, dietro compenso in percentuale.
Ciò che contraddistingue questo fenomeno sono, inoltre, le modalità con le quali si compie la fase successiva e necessaria del reimpiego del denaro, dei profitti e dei proventi anche grazie all'interposizione di società fittizie intestate a prestanome utilizzate nel "lavaggio" del denaro.

2. Le fasi del PHISHING

In assenza di una fattispecie unitaria a cui ricondurre il phishing e di una definizione universale, risulta comunque possibile individuare il *modus operandi* dei truffatori che agiscono attraverso fasi successive.
❑ ***La preparazione dell'attacco***: gli ideatori determinano le modalità con cui propagare l'attacco in rete, si avvalgono dei supporti tecnologici registrando domini e predisponendo i server su cui convogliare le informazioni riservate fraudolentemente carpite e da cui trasmettere richieste o interferire nelle comunicazioni tra i soggetti coinvolti.
❑ ***La propagazione dell'attacco***: a seconda delle modalità decise, vengono innescate le procedure rivolte a stabilire un contatto diretto o indiretto con la vittima, al fine di rubarne l'identità ottenendo le credenziali d'autenticazione. In questa

[1] Descrive l'insieme delle tecniche di persuasione e/o di inganno messe in campo per accedere a un sistema informatico; la tematica è stata trattata nella presente rubrica nel numero di giugno 2004 di Mondo Digitale.

[2] costituite per esempio da Username e Password.

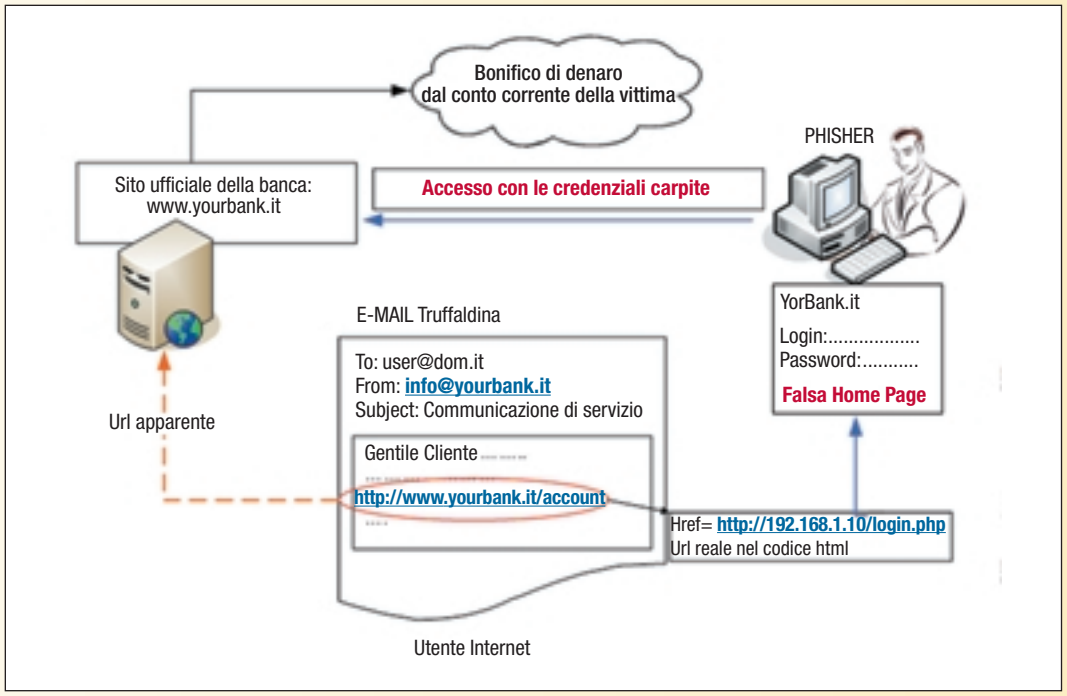

FIGURA 1
L'attacco condotto dal PHISHER

fase il phisher invia un'e-mail, qualificandosi come una banca, una società finanziaria, un ente, o più generalmente, nel caso in cui il phisher abbia scelto in modo mirato le proprie vittime, un soggetto che, a seconda della natura dei rapporti tipicamente intrattenuti dalla vittima, appaia a quest'ultima legittimata a procedere a richieste inerenti dati e chiavi di accesso. Il phisher può operare un invio casuale delle mail/esche a una svariata moltitudine di soggetti oppure decidere il target di identità utile ai propri fini. Nel primo caso lo strumento della posta elettronica è usualmente utilizzato dai truffatori con la logica dello spamming, attraverso l'invio di messaggi[3]. La mail inviata a un utente distratto e a volte ingenuo, chiede allo stesso di compiere un'attività che determinerà la rivelazione delle informazioni riservate attinenti a user id, password e altre chiavi necessarie all'accesso o all'utilizzo a opera del phisher. L'azione della vittima viene pertanto provocata attraverso il riferimento a situazioni che catturano l'attenzione dello stesso e si caratterizzano per la necessità e/o l'urgenza: notifica di problemi e disguidi inerenti i rapporti intrattenuti dal soggetto medesimo con l'ente o l'istituto finanziario, necessità di procedere a modifiche della password o aggiornamento dei dati, in risposta addirittura a possibili frodi e attacchi informatici denunciati dalla banca o istituto di credito; l'offerta di affari ovvero di nuovi servizi a termine validi solo in caso di immediata attivazione dell'utente.

❑ ***L'azione della vittima***: la vittima, convinta o semplicemente distratta, risponde all'attacco seguendo il link fornito dal phisher. Conscio della caratteristica del client di posta elettronica, di visualizzazione dei messaggi creati in HTML, il phisher ha inserito nel corpo dell'e-mail un link che, anche se esteriormente riporta un indirizzo web autentico, nascosto nel codice html (nel tag href), è stato impostato un collegamento ipertestuale che punta al falso sito web o a del codice da scaricare. In tal modo la vittima viene diretta al sito ufficiale dell'intermediario a cui vengono abilmente apposte delle finestre di pop up oppure a siti creati dal phisher che possono rappresentare il clone di quello ufficiale attraverso l'adozione di tecniche, sempre più sofisticate, rivolte all'occultamento dell'indirizzo IP (cosiddetto *IP spoofing*). Non da ultimo, la richiesta dei dati può essere contestuale e insita alla mail.

❑ ***Il furto d'identità***: il furto d'identità si compie nel momento in cui l'utente fornisce i propri dati al phisher digitandoli in un messaggio di risposta o nel sito internet clone oppure per mezzo dei programmi infetti attivati inconsapevolmente dal soggetto all'interno del proprio

[3] Tanto più efficaci quanto più credibili, circostanziati e affidabili.

computer; può infatti accadere che le informazioni vengano prelevate con l'ausilio di keylogger e web trojan[4], precedentemente scaricati e installati dall'ignaro utente.

❑ ***La consumazione della frode e della truffa***: il momento in cui si consuma il reato è quello in cui avviene da un lato l'indebita percezione del profitto (vale a dire l'incasso del denaro) e dall'altro lato la realizzazione del danno per l'utente internet: ciò si realizza nel momento in cui il phisher utilizza le credenziali fraudolentemente o abusivamente carpite e ottiene il trasferimento del capitale a mezzo dell'istituto di credito con conseguente sottrazione e impoverimento del patrimonio del correntista.

❑ ***La dispersione e il reimpiego dei profitti del reato***: la condotta fraudolenta del phisher non si esaurisce nel momento consistente nella violazione del patrimonio del correntista; subentra infatti una fase di reclutamento di soggetti compiacenti e non, che si rendono disponibili al transito di capitali attraverso i propri conti correnti. Si parla di transito, in quanto, i proventi convogliati su conti correnti bancari e postali vengono immediatamente ritirati attraverso prelievi in contanti e trasferiti per il mezzo di agenzie di money transfer o bonifici on line a conti intestati a società fittizie oppure a persone residenti all'estero. Minimo comune denominatore delle modalità scelte per il riciclaggio dei proventi del phishing è costituito dalla combinazione di internet e della transnazionalità delle operazioni, dalla creazione di società intestate a prestanome, dallo sfruttamento di regimi tipici dei cosiddetti paradisi fiscali[5].

3. Quali reati?

Sotto il profilo giuridico, l'assenza di una norma *ad hoc* rende difficoltoso ricondurre le condotte che costituiscono il phishing a una singola ipotesi di reato; tuttavia, sulla scorta dell'analisi delle fasi del fenomeno, si possono determinare le violazioni configurabili secondo l'ordinamento giuridico penale.

3.1. Il trattamento illecito di dati

Nel momento in cui il phisher ottiene abusivamente le credenziali di autenticazione dell'utente, senza il legittimo consenso di quest'ultimo, è configurabile l'ipotesi di reato di trattamento illecito di dati personali, prevista dall'art 167 del Codice in materia di protezione dei dati personali, approvato con il d.lgs. 30 giugno 2003, n. 196.

L'acquisizione fraudolenta dei dati personali, la raccolta delle informazioni inviate ai server dei siti web compromessi dal phisher e il loro successivo utilizzo per accedere attraverso l'identità violata del titolare dei dati, integra una serie di trattamenti dei dati personali[6]. La norma dell'art 167 punisce, tra gli altri, il trattamento dei dati personali posto in essere in violazione del consenso da parte dell'interessato. Infatti il phishing determina un accesso ai dati della vittima, senza che la stessa dia un consenso espresso e libero: Il phisher deliberatamente acquisisce dati che verranno trasmessi, raccolti, registrati, organizzati e utilizzati, al fine di trarre un illegittimo profitto con danno per la vittima, consistente per lo più nell'impoverimento patrimoniale.

3.2. La truffa

La disposizione dell'art. 640 c.p., nel prevedere il reato di truffa, punisce chi con artifizi e raggiri induca qualcuno in errore e procura a sé o ad altri un ingiusto profitto con altrui danno.

Il modello della truffa è quello che meglio si attaglia alla fase in cui il phisher procede a "lanciare l'esca/mail" all'utente. Infatti, salvo il caso di spamming, molto spesso il target delle vittime viene scelto ed in questo caso, per aumentare la credibilità, la mail sarà tanto più circostanziata e convincente quanto più il phisher conoscerà il soggetto vittima della propria offensiva.

L'utente che riceve l'e-mail fraudolenta viene indotto in errore e l'errore consiste nel ritenere di intrattenere dei rapporti con un determinato soggetto, di cui l'autore del reato ha assunto le sembianze, ragione per cui le azioni della per-

[4] Il keylogher è uno strumento in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio computer. Spesso i keylogger sono trasportati ed installati nel computer da virus denominati worm o trojan ricevuti tramite Internet ed hanno in genere lo scopo di intercettare password, credenziali di accesso e/o numeri di carte di credito.

[5] Caratterizzati dalle difficoltà inerenti alla cooperazione di polizia e giudiziaria al fine della repressione delle frodi.

[6] Intesi come qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la collezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

sona offesa non sono volontariamente e consapevolmente determinate.
Perché possa ritenersi avverata l'ipotesi di reato di cui all'art 640 c.p., è necessario che si verifichi l'induzione in errore della vittima. Colui che sporge denuncia per questi fatti è spesso proprio l'utente internet comune che, nonostante tema i pericoli della rete, essendo inesperto spesso non valuta in concreto le potenzialità che lo strumento informatico offre e non conosce i reali rischi. Pertanto anche condotte poco raffinate di artificio e raggiro[7] possono indurre in errore l'utente medio e il phisher ne tiene conto nella scelta delle proprie vittime. Nel caso del phishing l'artificio avviene, per esempio, attraverso l'indirizzamento dell'utente al sito internet dell'istituto bancario su cui vengono scientemente applicate finestre di pop up, nelle quali la vittima fornisce le credenziali richieste; oppure cliccando su un collegamento ipertestuale (link) indicato nell'e-mail, l'utente viene mandato verso il sito web clonato o offuscato attraverso il mascheramento dell'indirizzo IP.
Il raggiro, in base alla casistica illustrata, risiede nella fase della "*call in action*" dell'utente attraverso il messaggio e-mail in cui vengono usate le argomentazioni che permettono la prosecuzione della violazione nel momento successivo dell'artificio. Il raggiro può essere contestuale all'artificio qualora vengano riprodotte nel messaggio i caratteri tipici e dei segni distintivi del soggetto di cui è simulata l'identità.

3.3. La frode informatica

Un'analisi del fenomeno del phishing negli ordinamenti stranieri permette di riscontrare che lo stesso è definito internazionalmente come "*identity theft*" o " *fraud*"; la sostanza del fenomeno, al di là dei tentativi di ricondurlo a qualche fattispecie giuridica dell'ordinamento italiano, è proprio questa: la frode susseguente a un furto di identità, momento centrale dell'intera vicenda. Per questi motivi, risulta calzante il riferimento al "ciclo di vita del phishing", raffigurabile graficamente con un'immagine circolare a spirale, per cui il fenomeno si autoalimenta, segue un circolo, ma il cerchio non si chiude e passa attraverso le fasi della captazione illecita di informazioni riservate e l'utilizzo delle stesse[8].
Quale illecito è configurabile nel momento in cui i dati carpiti con l'inganno o in modo abusivo vengono utilizzati in un altro sistema informatico (quello della banca)?
In questo caso non si può fare riferimento alla truffa, in quanto il sistema informatico non può essere né raggirato, né verso lo stesso può avvenire un artificio: infatti tali concetti sono riferibili alle persone fisiche, non alle macchine.
Si può, allora, richiamare la norma di cui all'art. 640 ter c.p. la quale sanziona chi, 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, procura a sé o ad altri un ingiusto profitto.
Si precisa che per sistemi informatici il legislatore intende i "*sistemi di scrittura o di tale automazione d'ufficio ad uso individuale o particolare, nonché quelli di elaborazione dati*"; i sistemi telematici invece sono costituiti da "*reti di telecomunicazione sia pubbliche che private, locali o geografiche, nazionali o internazionali, operanti da e per il nostro Paese, e ogni altra loro componente (software, dati, informazioni, flussi di comunicazione, messaggi); il software, sia esso di base, di supporto, generalizzato o applicativo, inglobando nel concetto qualunque programma informatico realizzato dal costruttore dell'hardware, da strutture di produzione ad hoc, da singoli utenti*".
Tale norma punisce l'alterazione del sistema informatico e telematico e l'intervento sul dato informatico, avvenuta in qualsiasi modo, pertanto la frode informatica a differenza della truffa, si applica a quelle condotte del phisher che, sebbene fraudolente, non comportano artifici o raggiri.
Con riferimento a quest'ultimo aspetto, nel caso di frode informatica lo stesso legislatore assimila alle condotte dell'artificio e del raggiro, l'alterazione del sistema informatico e ritiene per ciò

[7] Da un punto di vista giuridico l'artificio consiste nella manipolazione, trasfigurazione della realtà esterna, provocata mediante la simulazione di circostanze inesistenti o la dissimulazione di circostanze esistenti; mentre il raggiro è un'attività simulatrice sostenuta da parole o argomentazioni atte a far scambiare il falso per il vero.

[8] In sostanza il fenomeno appare continuativo: può avvenire un accesso abusivo tramite la diffusione di virus; viene portato a compimento il furto dell'identità attraverso modalità fraudolente, le credenziali offerte vengono utilizzate attraverso lo stesso soggetto di cui il phisher ha assunto le vesti, un ulteriore accesso abusivo e un ulteriore sistema di frode.

integrata la fattispecie illecita, senza che sia necessario dimostrare l'induzione in errore.
In particolare, l'art. 640 ter c.p. disciplina queste due possibilità:

- l'alterazione, in qualsiasi modo, del funzionamento del sistema informatico e telematico: risulta violata l'integrità del sistema di informazione;
- l'intervento, senza diritto e con qualsiasi modalità su dati, informazioni, programmi contenuti in un sistema informatico o telematico: risulta violata la sicurezza del dato informatico.

Il Legislatore ha voluto determinare una distinzione tra le due ipotesi delle quali la prima presuppone un intervento più incisivo, che coinvolge tutto il sistema determinandone un'alterazione significativa[9]; la seconda invece fa pensare a casi in cui viene isolato un elemento del sistema, un dato informatico, un determinato programma, senza coinvolgere necessariamente tutto il sistema.

4. Conclusioni

Come più volte sottolineato, non esiste un'unica tipologia di *phishing* in quanto vengono continuamente sviluppate nuove e più subdole forme di inganno *on line*.
Per tutelarsi contro questi rischi, possono essere utilizzati appositi programmi[10] che bloccano email o collegamenti sospetti, confrontando gli indirizzi reali dei mittenti con le black list[11] presenti in internet. Tali sistemi, in taluni casi, possono essere comunque elusi e le black list non sempre sono perfettamente aggiornate, quindi gli esperti di sicurezza informatica consigliano in particolare di non rispondere a richieste di informazioni personali ricevute tramite posta elettronica, nonché di visitare i siti internet digitando l'indirizzo direttamente nella barra degli indirizzi e con l'accortezza di verificare che il sito utilizzi sistemi di crittografia (per cifrare la password)[12] Risulta, inoltre, prudente esaminare con regolarità gli estratti conto bancari e i report della carta di credito al fine di riscontrare eventuali anomalie e denunciare prontamente i sospetti movimenti illeciti.
In definitiva, considerate le difficoltà di natura investigativa e di ordine pratico, mai come per contrastare questo fenomeno la prevenzione risulta l'arma migliore. Di ciò ne sono consapevoli anche gli intermediari finanziari direttamente coinvolti, *in primis* le banche, che negli ultimi tempi hanno attivato numerose campagne d'informazione e servizi tecnologici (come gli sms che avvisano il cliente in caso di bonifici) volti ad arginare le frodi telematiche.

Bibliografia

[1] Phishing Dhs Report: *Online Identity Theft: Phishing Tecnology, Chokepoints and Countermeasures*. Aaron Emigh, Radix Labs, 3 ottobre 2005 reperibile su www.antiphishing.org/Phishing-dhs-report.pdf

[2] Call in action Report, a publication from the national consumer League, marzo 2006, www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf

Antonio Piva laureato in Scienze dell'Informazione, Vice Presidente dell' ALSI (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica.
Docente a contratto di diritto dell'informatica all'Università di Udine.
Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA ECDL.
E-mail: antonio@piva.mobi

David D'Agostini avvocato, ha conseguito il master in informatica giuridica e diritto delle nuove tecnologie, fornisce consulenza e assistenza giudiziale e stragiudiziale in materia di *software, privacy* e sicurezza, contratti informatici, *e-commerce*, nomi a dominio, computer crimes, firma digitale. Ha rapporti di partnership con società del settore ITC nel Triveneto.
Collabora all'attività di ricerca scientifica dell'Università di Udine e di associazioni culturali.
E-mail: david.dagostini@adriacom.it

[9] Si pensi ai casi di attacchi di phishing verificatesi nella pratica, per cui l'attacco, raggiunge l'apice in un ristretto lasso temporale determinando il blocco del sistema della banca o dell'istituto finanziario con conseguente paralisi dell'attività.

[10] Si pensi a Netcraft o per utenti di outlook: Delphish: programmi che avvisano l'utente quando arrivano email sospette (inoltre a volte tali email vengono fermate a monte già dall'e-mail server, tramite i filtri appositi, che utilizzano le black list presenti su internet).

[11] Le black list sono elenchi di indirizzi di posta elettronica, siti o domini, utilizzati solitamente per lo spam o diffusione di virus o phishing; tali elenchi sono pubblicati su internet e liberamente consultabili, vengono normalmente utilizzati dai server che li consultano ogniqualvolta ricevono una email verificando la presenza o meno del mittente in tali elenchi; se la verifica è positiva viene segnata come email spam o potenzialmente pericolosa.

[12] Di solito per tali collegamenti viene utilizzato il protocollo l'SSL: l'utente si accorge di ciò in quanto l'indirizzo riportato sulla barra del browser, inizia con https://.. al posto del solito http://..; in genere tale situazione è anche visualizzabile dalla lucchetto chiuso, in basso a destra, nel browser stesso.