

## **PRESI IN TRAPPOLA**

*di Andrea Maselli*

Le cose non sono sempre così come sembrano. Soprattutto su Internet. Lo sanno bene i truffatori, che hanno imparato ad assumere le "sembianze" di aziende rispettabili per raggirarne i clienti. Un'e-mail contraffatta, un sito falso ma identico all'originale, un po' di distrazione e la vittima è presa all'amo. Signore e signori...il "phishing" è servito!

Immaginatevi un uomo "travestito da bancomat". Immaginatevelo mentre approfitta del suo particolare punto di osservazione per annotare i codici digitati dai clienti e copiare i dati contenuti nella banda magnetica delle tessere. Anche se potrebbe suonare un po' come una scena tratta da "Totòtruffa" è già successo davvero. E anche più di una volta. Su Internet accade addirittura migliaia di volte ogni giorno. È il "phishing", un fenomeno criminoso che sta assumendo proporzioni planetarie, con ritmi di crescita al di là di ogni immaginazione. Gli osservatori ritengono che questo genere di truffa si trovi ancora a uno stadio sperimentale, in una sorta di incubazione, ma è evidente a tutti che il suo livello di raffinatezza e di efficacia cresce di giorno in giorno. Al punto che secondo le autorità di Pubblica Sicurezza, questa diverrà presto "LA" truffa via Internet per antonomasia.

Ma in cosa consiste esattamente? Il phishing mira a sottrarre agli utenti Internet il loro dati personali e tutte le informazioni utili per accedere illecitamente ai servizi finanziari di cui le vittime sono titolari.

In sostanza i phisher (i truffatori) cercano di impossessarsi delle password e delle **username** dei clienti dei principali istituti bancari (e similari) che operano on-line.

E naturalmente non disdegnano i numeri di carta di credito...

### **Ma come fanno?**

Per raggiungere i loro obiettivi, i truffatori utilizzano due approcci diversi, molto spesso combinati tra loro.

Il primo, il più noto al grande pubblico, è quello cosiddetto del **social engineering**. I criminali in questo caso realizzano delle e-mail civetta che mirano a condurre i destinatari su siti Web contraffatti, spingendoli a fornire in quella sede i propri dati riservati.

I phisher cercano cioè di apparire agli occhi della loro vittima come i veri fornitori del servizio bancario, che si mettono in contatto con il proprio cliente per avere una conferma sui suoi dati personali. Le e-mail in questo caso sono progettate con tanto di loghi e intestazioni contraffatte, in modo da apparire le più verosimili ed "ufficiali" possibili, mentre i siti Web cui i messaggi di posta elettronica rimandano sono cloni perfetti di quelli originali. La seconda modalità per sottrarre informazioni alle vittime potenziali è quella di ricorrere a dei trucchetti tecnologici. Si tratta in questo caso di installare sul PC del bersaglio uno o più **troJan** in grado di raccogliere dati sensibili. Molto spesso si tratta di keylogger, software che si mimetizzano tra registro e hard disk per poi leggere, memorizzare e trasmettere all'esterno quanto digitato dall'utente durante la compilazione dei moduli elettronici sul Web (ivi compreso il contenuto delle classiche caselle per l'accesso sicuro ai servizi). Altre volte il trojan si limita a raccogliere dal computer infetto tutte le informazioni riconducibili a numeri di carte di credito, codici o password, sfruttando algoritmi che gli consentono di discernere tra una parola e l'altra.

Ancora, tra il software finalizzato al phishing e quindi a delinquere, vanno annoverati anche i cosiddetti hijacker che, una volta penetrarti nel sistema, dirottano il browser su siti che ospitano altri trojan e che sono in grado di inocularli nel PC del visitatore attraverso faUe dello stesso browser.

## Una truffa globalizzata

Anche se il phishing nasce come fenomeno planetario, fino a un anno fa era praticamente circoscritto ai grandi istituti finanziari nordamericani e alle principali aziende internazionali operanti sul Web. Ciò faceva sì che le vittime predestinate fossero quasi esclusivamente di lingua inglese. Tuttavia, la natura "generica e massificata" degli attacchi phishing ha fatto sì che per mesi e mesi (ma ancora oggi) anche milioni di utenti italiani ricevessero e-mail civetta in qualità di ipotetici clienti di istituti stranieri, come CityBank o Paribas: va da sé che difficilmente questo genere di messaggi potevano sortire nel nostro Paese l'effetto criminoso voluto dai loro mittenti. Oggi le cose sono cambiate, ed e-mail progettate specificamente per colpire i clienti di istituti italiani giungono con quotidiana regolarità

nelle nostre caselle di posta elettronica. Il fattore che ancora limita l'efficacia di questi messaggi è proprio la pedestre traduzione in lingua italiana, frutto di software automatici che rivelano l'origine extra-italiana dell'inganno. Sarebbe però pericoloso interpretare la correttezza del linguaggio dei messaggi di phishing come un metodo valido per smascherarli. È infatti oramai ovvio che il passo successivo sarà proprio quello di curare la forma grammaticale e sintattica delle e-mail, proprio con l'intento di sorprendere anche i destinatari più diffidenti. In realtà l'unico modo di difendersi dal phishing è quello di diffidare sempre, prescindendo dalle caratteristiche dei messaggi e persino da quelle dei siti Web a cui gli stessi messaggi rimandano. È infatti proprio di questi giorni l'avvento di quello che è stato ironicamente definito "secured phishing", ossia "phishing sicuro", una novità che è destinata ad incrinare molte... sicurezze.

**Galeotto fu il lucchetto** Con il secured phishing i truffatori si sono attrezzati per sfruttare la naturale fiducia che i navigatori sono propensi a riporre nelle cosiddette "connessioni sicure", ossia nei protocolli SSL, segnalati nella barra di stato del browser dall'oramai mitico "lucchetto", e nella barra di navigazione dalla dicitura "https". È infatti possibile simulare una connessione protetta utilizzando la cosiddetta certificazione digitale. Si tratta di una sorta di firma elettronica che molte aziende usano al proprio interno per validare i documenti in formato elettronico, e garantire quindi la provenienza. Quando il browser tenta di aprire un documento firmato elettronicamente si comporta esattamente come se accedesse a un sito protetto da un protocollo SSL: si accorge della presenza di una certificazione, e ne controlla la validità.

Quindi, mentre fa comparire il lucchetto nella barra di stato, il browser mostra a video anche una finestra dove avverte il navigatore di aver incontrato una certificazione, ma che questa risulta "auto-firmata" (non è cioè rilasciata da un ente certificatore terzo, ma è una sorta di firma personale). Starebbe all'utente a questo punto rinunciare alla connessione facendo clic su "No", Tuttavia l'esperienza insegna che il navigatore medio non è né così attento né così esperto da cogliere il senso dell'avvertimento e continua comunque la navigazione (o la transazione) rassicurato dall'idea che una qualche forma di "certificato" lo sta proteggendo.

Al di là del caso di specie, andrebbe ricordato che, comunque, anche una vera connessione protetta SSL garantisce soltanto che i dati vengono trasmessi in forma criptata e che, pertanto, non sono intercettabili da terzi. Il "lucchetto" quindi, può garantire semplicemente la connessione, ma non dice assolutamente nulla su chi si trovi effettivamente all'altro capo del collegamento. Neppure questi indicatori possono dunque essere considerati come un discrimine valido tra siti Web originali e i loro doni truffaldini.

**Vorrei spezzare una... fiocina** Qualche tempo fa IBM ha segnalato che si sta affermando un modalità di phishing rivoluzionaria e potenzialmente letale per le vittime. Si tratta del cosiddetto "spear phishing", letteralmente "pesca con la fiocina". Come già il nome lascia intuire, si tratta di una truffa mirata, ossia costruita su misura per colpire utenti di cui siano già noti alcuni tratti o addirittura le generalità complete.

Come già detto infatti, il phisher di regola spara le sue "e-mail esca" nel mucchio, contando di riuscire a colpire soprattutto le persone più impressionabili e, in particolare, quelle che, per combinazione, siano proprio titolari del servizio contraffatto. Lo spear phishing invece fa il salto di qualità. Viene condotto dall'interno dell'istituto bersaglio, a volte dagli stessi dipendenti del fornitore del servizio originale, in particolare da quelli che possono accedere alle generalità di un alto numero di potenziali vittime. In questo modo è possibile progettare e-mail civetta ad hoc, citando alloro interno il nome e il cognome del destinatario, o magari perfino il suo numero di codice cliente, di conto corrente o quant'altro di cui la "talpa" possa disporre. La vittima tende a fidarsi istintivamente di un messaggio che paia indirizzato proprio a lei e che dimostri implicitamente che il mittente è già in possesso di una gran quantità di informazioni sul suo conto.

## Uragani e intermediari

A volte il phisher, anziché costruire un sito Web contraffatto, donando l'originale, può tentare di coprire la propria attività (e ritardare il momento in cui la vittima si renderà conto dell'inganno) proponendosi come "intermediario" tra la vittima predestinata e illegittimo servizio. È capitato per esempio negli Stati Uniti in occasione dell'uragano Katrina, quando centinaia di e-mail hanno invitato altrettanti utenti del Web a venire in aiuto della Croce Rossa, contribuendo con la propria carta di credito. L'e-mail rimandava effettivamente al vero sito della Croce Rossa, ma sopra di esso apriva soltanto una finestrella pop-up da compilarsi.

Una volta eseguita l'operazione, la finestrella spariva, lasciando credere alla vittima di turno di aver realmente contattato la nota associazione umanitaria. Da qui il ritardo (o la mancanza) della denuncia alle Autorità competenti. In occasione dell'uragano Katrina sono comunque stati creati quasi 200 siti Web "falsi" per intercettare le donazioni dirette alle principali organizzazioni umanitarie realmente coinvolte nella raccolta di fondi; accadde esattamente la stessa cosa con il drammatico tsunami del Sud Est asiatico del dicembre scorso, quando nel giro di pochi giorni vennero venduti a destra e a manca centinaia di domini che suonavano come "helptsunami", "tsunamirelief", "tsunamidonation", e via di questo passo.

Inutile dire che da quei domini ai sopravvissuti indonesiani è arrivato ben poco...

## Quel messaggio non passerà!

Al momento ci sono ben poche difese tecniche contro

il phishing. La lotta tecnologica opera comunque su due fronti: da una parte si stanno sviluppando strumenti per filtrare la posta elettronica, con l'intento di individuare all'origine le ..e-mail truffa"; dall'altra si cerca di dotare i browser di una sorta di "intelligenza" che consenta loro di individuare la natura truffaldina dei siti clone in tempo reale durante la navigazione, avvisando opportunamente l'utente e bloccando ogni possibile interazione.

Per quanto riguarda la posta elettronica, i filtri hanno

il compito di capire se un determinato messaggio provenga realmente dall'indirizzo da cui "sostiene" di essere stato spedito. Infatti il campo "Da:/From:" di una e-mail può essere facilmente falsificato per indurre il destinatario a ritenere che il mittente sia diverso da quello che in realtà appare. Perché però il software possa effettuare questo tipo di verifica è necessario che il mittente partecipi a uno "schema di verifica", che prenda cioè parte a un programma internazionale contro le frodi via e-mail.

Tra i più noti c'è, per esempio "Sender Policy Framework" (SPF), il meccanismo con cui operano questi schemi di verifica è più o meno questo... Prendiamo il caso di eBay: nel momento in cui si è associato al circuito SPF ha dovuto fornire un certificato dove vengono specificati tutti i server che sono autorizzati ad inviare e-mail con il dominio eBay.com. Ora supponiamo che un utente di Fastweb riceva un'e-mail da eBay. Fastweb; anch'esso partecipante a SPF, va a verificare automaticamente che il server di provenienza del messaggio sia uno di quelli inclusi nel certificato depositato da eBay. Se il server si trova nella lista, allora il programma di posta elettronica dell'utente (o il software antispam a esso collegato), ove supporti lo standard SPF, bollerà il messaggio come "genuino". Se, viceversa il server di provenienza non è elencato nel certificato, il messaggio verrà marchiato come "sospetto". Se uno dei due domini (mittente o destinatario) non partecipa al programma SPF, ovviamente sul messaggio non potrà essere eseguita alcuna analisi.

Con la Service Pack 2 per Office 2003, anche Microsoft ha inserito un sistema di filtraggio contro le e-mail fraudolente nel proprio client di posta elettronica Outlook.

## Abbassate la barra

Al secondo "fronte di guerra" appartengono le cosiddette "barre anti-phishing" che operano in simbiosi con il browser. il meccanismo di funzionamento di tutti questi strumenti è analogo: una centrale elabora continuamente una "lista nera" di siti ritenuti fraudolenti e la invia a ciascun delle barre installate.

Queste, così aggiornate, intervengono sul browser per impedire l'accesso ai siti segnalati. Si tratta in sostanza di meccanismi di allerta preventivo, del tutto simili a quelli che presiedono al meccanismo di aggiornamento in tempo reale degli antivirus.

I più grandi produttori di browser stanno comunque cominciando a integrare queste tecnologie direttamente all'interno dei loro prodotti. Netscape ha inserito nella versione 8.0 del suo browser un sistema per bloccare l'accesso i siti che sono sospettati di ospitare programmi spyware o di dar luogo ad attività di phishing; anche questo meccanismo opera sulla base di una "lista nera" , inviata al browser che, poi, si occupa di impostare il livello di sicurezza adeguato ogni qual volta dovesse entrare in contatto con i siti "proscritti", rendendoli così inoffensivi per l'utente. La stessa Microsoft ha annunciato che la versione 7.0 di Internet Explorer includerà funzionalità anti-phishing, mentre una tecnologia analoga (Microsoft Phishing Fitter) sarà inserita anche neUa barra di ricerca di MSN. Già oggi può essere scaricata gratuitamente la versione beta di un add-on per la barra di MSN che le conferisce queste capacità "antifrode" (<http://addins.msn.com/phishingfilter>).

Molto interessante anche l'esperimento di NetCraft che ha sviluppato una barra anti-phishing gratuita di tipo "coUaborativo" (scaricabile al sito <http://toolbar.netcraft.com>). In sostanza, non appena un utente segnala l'indirizzo di un sito che esercita il phishing, a tutti coloro che hanno installato la barra di Netcraft - previo controUo deUa

veridicità deUa segnalazione viene impedito di accedervi. Se il sito su cui l'utente sta navigando è sconosciuto aU'archivio di Netcraft, la barra ne analizza comunque alcuni parametri ed esprime un giudizio suU'affidabilità del sito tramite una sorta di termometro presente neU'interfaccia: più l'indicatore si colora di rosso, maggior è la probabilità che il sito costituisca un rischio per il navigatore.

La barra di Netcraft controUa anche l'**IP address** cui corrisponde l'indirizzo di ogni sito, evidenziando la località geografica'neUa quale si trova il server che lo ospita: così facendo il navigatore può facilmente rendersi conto di una eventuale frode, dal momento che è altamente improbabile, tanto per esemplificare, che il server di Fineco possa trovarsi in Romania. Tutti i maggiori produttori di antivirus, stanno comunque dandosi da fare per arricchire i propri software con specifiche protezioni anti-truffa. Symantec ha addirittura acquisito la società WholeSecurity, specializzata in prodotti per contrastare le frodi basate sul furto d'identità. Questa società è titolare del "Phish Report Network", una tra le più grosse centrali di raccolta di indirizzi di siti che praticano il phishing nel mondo, ed è lo stesso circuito informativo cui fanno riferimento, per esempio, gli strumenti di sicurezza di Microsoft.

In pratica il PRN sta al phishing, come una centrale che individua e raccoglie le tracce virali sta ai virus informatici. C'è da credere che presto vedremo gli effetti di questa acquisizione all'interno dei prodotti Symantec.

## Attenti al Lupo

Volete approfondire l'argomento"phishing"?  
Avete domande da farei o curiosità da soddisfare sull'argomento?  
Discutetene con il nostro direttore Andrea Maselli,sul blog"Attenti al Lupo";un punto di incontro per essere sempre informati su truffe, bufale e virus.  
Il blog "Attenti al Lupo" è sul nostro sito  
[www.computer-idea.it](http://www.computer-idea.it).  
Vi aspettiamo!

## Che fare se ci si casca

Se rimanete vittima di una e-mail o di un sito fraudolento, non fatevi prendere dal panico. Nulla è perduto, anche perché, ad onore del vero,solo una minima percentuale di coloro che cadono nel tranello del phisher si ritrovano poi ammanchi sul proprio conto corrente. A ogni modo è fondamentale agire in fretta per minimizzare ulteriormente il rischio che il truffatore possa trarre vantaggio dai dati di cui è entrato in possesso con l'inganno. Agite così:

Informate tempestivamente l'azienda coinvolta utilizzando gli appositi numeri verdi.

Non limitatevi a inviare un' e-mail, ma telefonate subito!

Se il furto di dati riguarda un bancomat o una carta di credito, bloccateli immediatamente.

Se il furto riguarda i dati del vostro account eBay e potete ancora accedervi, cambiate subito la vostra password.

Se vi accorgete che è già stato sequestrato, segnalatelo a eBay con l'apposita procedura guidata: l'azienda provvederà alla sospensione dell'accountfino al completa mento delle indagini necessarie.

Se il furto riguarda il vostro account Paypal e potete ancora accedervi, analogamente a quanto indicato al punto precedente, modificate immediatamente la vostra password e verificate che non siano già state effettuate operazioni di pagamento o prelievo.

Sporgete formale denuncia presso un posto di Pubblica Sicurezza

## Prevenire è meglio che...

Non limitatevi a fronteggiare i singoli attacchi di phishing: adottate piuttosto uno "stile di vita informatico" utile a prevenire le truffe, proteggere chi vi sta a cuore e contribuire al perseguimento di questi delinquenti.

Assicuratevi che in famiglia tutti coloro che utilizzano la Rete siano adeguatamente consapevoli dei rischi legati al phishing e conoscano le metodiche con cui viene esercitato. Installate antivirus, antispyware, antispam e fire.wall e mantenetele costantemente aggiornati. Può apparire ridicolo dover ricorrere a una simile parata di protezioni, ma questi strumenti possono ridurre il rischio in maniera drastica. Ricordate che il phishing viene esercitato anche attraverso strumenti tecnici subdoli come trojan e keylogger. Mantenete sempre aggiornati il vostro sistema operativo e il vostro browser (soprattutto se si tratta di Internet Explorer).

Se avete degli account aperti presso società finanziarie, banche, intermediari di pagamento (per esempio PayPal) o aste (eBay) che operano on-line, controllateli di tanto in tanto. Non lasciate trascorrere mesi senza accedervi: così facendo rischiate di accorgervi di eventuali ammanchi quando oramai è troppo tardi per intervenire.

È buona norma cambiare con regolarità le proprie password e user-id. È importante anche scegliere password di una certa complessità, inserendovi caratteri particolari e alternando maiuscole, minuscole e numeri.

Non pensate soltanto a voi! Se avete ricevuto un' e-mail truffaldina inoltratela per conoscenza alla società coinvolta, oppure segnalategliela telefonicamente chiamando l'apposito numero verde. Segnalate il phishing anche alle Autorità di PS: potete per esempio inoltrare il messaggio alla Polizia Postale all'indirizzo [poltel.rm@poliziadistato.it](mailto:poltel.rm@poliziadistato.it).

Un altro indirizzo al quale sarebbe utile inoltrare un messaggio di phishing è [reportphishing@antiphishing.com](mailto:reportphishing@antiphishing.com) che fa capo alla principale organizzazione antiphishing mondiale.

## Siate cauti

Il modo migliore per difendersi dal phishing è la consapevolezza, arricchita dal tradizionale buon senso e rafforzata da una doppia dose di diffidenza. Affidarsi ciecamente alle sole difese elettroniche è il modo migliore per andare in contro a grossi guai. Ecco qualche consiglio, anche un po' controcorrente, per non farsi sorprendere con la guardia abbassata.

Se non ne riconoscete il mittente (anche in termini di i contenuti e stile di scrittura) considerate ogni e-mail che vi arriva come una potenziale truffa.

Se qualcuno vi chiede i vostri dati personali, i vostri estremi finanziari, password o altre informazioni riservate, non abbiate dubbi: stanno cercando di truffarvi. Partite dal presupposto che nessun istituzione finanziaria seria (o assimila bili) si sognerebbe mai di chiedervi simili informazioni via e-mail. Non raggiungete mai un sito Web utilizzando il link inserito

in un' e-mail; soprattutto se questa proviene da un sedicente istituto finanziario o da altre entità collegate, anche in modo remoto, con attività di "pagamento"; "riscossione" o "vendita": Se avete dei dubbi, piuttosto accedete al sito in questione

digitando manualmente l'indirizzo (che dovrete voi stessi conoscere) nell'apposita barra di navigazione del browser.

In linea generale non bisognerebbe mai utilizzare un link contenuto in un'E1.-mail.

## Pronto?

### Mi vogliono... pescare!

Ecco i numeri da contattare per segnalare tempestivamente casi di phishing agli istituti finanziari. Questi numeri possono essere utilizzati anche per il bocca di carte e account.

Società	per segnalazioni	
Numero verde	e-mail	
American Express	800-864046	
Banca Carim	800-018871	
Banca Intesa	800-020202	
Banca Sella	800-822056	info@sella.it
Banco di Sicilia	800-830088	
Banco Posta (Poste Italiane)	803-160	info@poste.it
BPN	800-080060	
Carige	800-778877	
Carime	800-665588	
Credem	800-273336	
Diner's	800-864064	
eBay		spooof@ebay.com
Fineco	800-525252	
PayPal		spooof@paypal.com
San Paolo	800-303302	
Servizi Interbancari	800-151616	
Top Card	800-900910	