

1 - Phishing: caratteri generali

L'espressione secondo alcuni deriva dalla storpiatura del verbo inglese to fish che significa pescare. L'idea è quella di pescare utenti in rete per farli cadere all'interno di trappole tese da incalliti e navigati truffatori.

Così nel mare di internet, vi sono soggetti che cercano di carpire dati ed informazioni relative agli utenti che si imbattono nel phishing.

Ma lo scopo dei phisher sono i soldi.

La letteratura recente descrive casi di phishing che hanno una ben precisa vittima sacrificale delle loro azioni: l'home banking, ovvero le carte di credito, i conti correnti on-line, i codici relativi a depositi effettuati in noti istituti di credito.

Ma come è possibile riuscire a rubare denaro attraverso il phishing?

Il fenomeno è allo stesso tempo criminale e sarcastico, ingegnoso e infantile.

Si cerca di estorcere denaro agli utenti della rete con un metodo semplicissimo: prendendoli in giro.

La tecnica utilizzata per colpire gli utenti italiani attraverso il phishing è stata, quella di inviare un'e-mail apparentemente proveniente dal proprio istituto di credito (in particolare Banca Intesa, Unicredit e Banca di Credito Cooperativo i casi più frequentemente riscontrati) con cui si informava l'utenza che, a causa di un trasferimento del sito (o per altre ragioni tecniche non meglio precisate) era necessario collegarsi al nuovo sito, entrare nella sezione riservata al proprio conto e compilare un apposito formulario.

Apparentemente non c'è nulla di strano. Solo che il sito verso cui ci si indirizza non è il sito della nostra banca ma è un altro sito utilizzato come esca per far abboccare gli ignari pesciolini. In seguito i dati e le informazioni carpite vengono utilizzate nei modi più svariati, e una non tempestiva segnalazione alla propria banca potrebbe condurre verso amare sorprese nel successivo estratto conto.

Il phishing è subdolo e sarcastico perché sfrutta l'ingenuità e l'ignoranza degli utenti. Il messaggio di posta elettronica del phisher è generalmente scritto in un italiano improbabile (il che lascia supporre che il fenomeno non abbia ancora preso piede presso i criminali del nostro paese), con gli accenti sbagliati, con verbi coniugati male, con improbabili espressioni idiomatiche.

Pertanto, un utente accorto avrebbe buon gioco a notare la differenza fra un e-mail scritta con i piedi e le comunicazioni usualmente provenienti dagli istituti di credito, formulate sempre in un italiano piuttosto forbito.

Sarebbe sufficiente una maggiore familiarità con la lingua italiana per accorgersi che una banca non si sognerebbe mai di mandare una comunicazione così delicata ad un cliente, invitandolo ad aprire il proprio conto on-line digitando password e quant'altro, attraverso un'e-mail zeppa di "orrori" ortografici.

Sotto il profilo tecnico è opportuno adottare ulteriori accorgimenti, e seguire questi brevi suggerimenti per non cadere in trappola.

Nel momento in cui giunge l'e-mail phishing occorre sapere che lo scopo del truffatore è quello di indurci in errore facendoci credere che il link presente nell'e-mail conduca verso la nostra banca.

Per smascherare il trucco è sufficiente posizionare il mouse sull'indirizzo della

banca verso cui il messaggio ci invita a recarci. Posizionandoci sull'indirizzo, senza cliccare, potremmo osservare sulla barra di navigazione (presente su ogni browser) il nome dell'indirizzo verso il quale ci condurrà il link. Leggendo attentamente quell'indirizzo ci accorgeremo come non corrisponda affatto a quello della nostra banca e quindi riusciremo a smascherare il phishing, evitando di cadere nella sua rete.

Tuttavia occorre segnalare come dalle recenti notizie di cronaca si evinca una certa evoluzione delle tecniche di phishing: nel caso di Unicredit bank, c'era una sola "s" di differenza fra il sito effettivo della banca e quello clonato dal phisher. Inoltre il sito civetta era in tutto e per tutto simile a quello originale. In questi casi una telefonata alla nostra banca non guasterebbe di certo, in fondo si spenderebbe qualche centesimo per risparmiarne migliaia e migliaia.

2 - Metodologia d'attacco

Il processo standard delle metodologie di attacco di phishing può riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (*phisher*) spedisce al malcapitato ed ignaro utente un messaggio e-mail che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. l'e-mail contiene quasi sempre avvisi di *particolari situazioni o problemi* verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account ecc.).
3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione.
4. il link fornito, tuttavia, *non* porta in realtà al sito web ufficiale, ma ad una *copia fittizia* apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere ed ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Talora, l'e-mail contiene l'invito a cogliere una nuova "opportunità di lavoro", a dare le coordinate bancarie del proprio conto on line per ricevere l'accredito di somme che vanno poi trasferite ad altri conti, trattenendo una percentuale dell'importo, che può arrivare a cifre molto alte. Solitamente, il trasferimento avviene con bonifici gratuiti, sempre via Internet, verso un altro conto on line. Si tratta del denaro rubato con il phishing, per il quale il titolare del conto on line, spesso in buona fede, commette il reato di riciclaggio di denaro sporco. Quest'attività comporta per il phisher la perdita di una certa percentuale di quanto è riuscito a sottrarre, ma esiste comunque un interesse a disperdere il

denaro in molti conti correnti e a farlo girare in differenti Paesi, perchè diviene più difficile risalire al suo conto e dati identificativi.

2.1 - Tecniche principali dei phisher

Vediamo in dettaglio quali sono le principali tecniche utilizzate dai phisher:

- **copie autentiche:**

il primo scopo del phishing è quello di colpire il lato psicologico del malcapitato utente utilizzando testi, immagini ed in molti casi veri e propri cloni dei siti originali in modo da convincere l'utente dell'effettiva autenticità del messaggio



Caso reale di phishing contro eBay– E-mail inviata in data 18 aprile 2005

- **utilizzo di indirizzi web (URL) autentici**

Essendo basato sull'inganno è assolutamente necessario per il phisher mascherare il falso URL verso il quale l'ignaro utente verrà indirizzato con il vero indirizzo del sito clonato. Per risolvere questo problema i phisher adottano prevalentemente due soluzioni: sfruttare le vulnerabilità dei vari browser o registrare nomi a dominio simili a quelli originali come nel caso della Unicredit Banca (www.unicreditbanca.com) la quale ha visto recapitare ai propri clienti un e-mail contenente un falso indirizzo www.unicreditsbanca.com simile ma assolutamente estraneo alla banca in questione.

- **indirizzo web mascherato**

Per camuffare l'URL, soprattutto nelle e-mail, il phisher è solito utilizzare una delle seguenti tecniche:

1. Conversione del nome a dominio in indirizzo IP.

Questo sistema consente di mascherare il nome del falso sito con il suo equivalente indirizzo IP; così il legittimo indirizzo:

<http://www.ebay.com/signin.ebay.com/ws/eBayISAPI.dll?SignIn&>

può trasformarsi in

<http://218.154.123.224/signin.ebay.com/ws/eBayISAPI.dll?SignIn&>.

2. Il carattere @.

Utilizzato nei primi casi di phishing, fa la sua prima apparizione l'11 novembre 2003 in un e-mail contro gli utenti di Amazon.com, il simbolo @ viene utilizzato per instradare l'utente verso il sito truffa. Infatti

modificando l'URL in questo modo <https://www.paypal.com/it/cgi-bin/webscr@www.microsoft.com> tutto quello che si trova a sinistra del simbolo @ viene ignorato mentre si è indirizzati verso il sito microsoft.com. A rendere questa tecnica ancora più subdola ci ha pensato il *dotless decimale* il quale consente di convertire un indirizzo IP in un numero decimale a 32-bit senza punti. In questo modo ad esempio l'indirizzo IP di www.microsoft.com 207.46.250.119 viene convertito in 3475962487 ed aggiunto all'URL modificato produce: <https://www.paypal.com/it/cgi-bin/webscr@3475962487>.

La tecnica del simbolo @ non è più sfruttabile in quanto Microsoft ha provveduto ad arginare il problema attraverso il rilascio di un apposita patch.

3. URL codificato.

La codifica dell'URL o parte di esso nell'equivalente ASCII esadecimale è una tecnica ancora molto usata dai phisher. Il meccanismo è semplice infatti tramite un apposito convertitore o anche manualmente è possibile trasformare www.anti-phishing.it nella sua versione meno comprensibile <http://www%2E%61%6E%74%69%2D%70%68%69%73%68%69%6E%67%2E%69%74>.

4. URL di elevate dimensioni.

Utilizzare un indirizzo web di dimensioni superiori a quelle della barra degli indirizzi è una tecnica molto usata. Ecco che URL si sono visti recapitare i clienti di Bank of America nell'ultimo caso di phishing : http://62.193.218.82/daokewqoekwqoekwqoekwqoekwqepwqkeopwkdpwsajdaoidjsaoidjsaoidjaoidjsaoidjsaoidjsaoidjsaoidsajdoisajdoi sajdoisadjsaoidjsaoidjsaoidjsaoidwqewqjepwqiekpwqkeopwk/card_activation.htm.

5. Reindirizzamento.

Per depistare l'utente sulla reale connessione in atto, molto spesso i phisher ricorrono al reindirizzamento. In questo modo l'utente crede di essere diretto verso il sito reale mentre in realtà viene trascinato nel sito truffa così come è avvenuto per i casi di phishing contro Banca Intesa.

- **spoofing nella barra degli indirizzi**

Nei casi in cui non è possibile registrare o impadronirsi di un URL simile al sito originale il phisher ricorre alle vulnerabilità dei browser e ad astuti trucchi per convincere il malcapitato utente della reale autenticità del sito trappola. A favorire il lavoro dei phisher negli ultimi mesi ci ha pensato Internet Explorer con una serie di bugs facilmente sfruttabili che hanno agevolato la contraffazione ed il proliferare del fenomeno phishing; tuttavia in diversi casi i phisher hanno favorito il metodo della sostituzione della barra degli indirizzi. Questa tecnica consente in maniera molto semplice e senza particolari conoscenze tecniche di sostituire la reale barra degli indirizzi con una falsa immagine della stessa contenente un falso URL.



Nella barra degli indirizzi viene riportato <http://it.yahoo.it> ma in realtà siamo all'interno del sito <http://www.anti-phishing.it>

Questa tecnica risulta particolarmente insidiosa in quanto lo stesso meccanismo può essere usato anche per modificare la barra di stato; soprattutto per visualizzare il lucchetto, tipico delle connessioni protette facendo così credere all'utente di essere realmente in una sessione sicura tipica dei servizi di home banking.

- **sostituzione dell'indirizzo web**

In molti casi i phisher ricorrono ad un ingegnoso trucco, infatti se la sostituzione della barra degli indirizzi può destare sospetti anche nell'utente più distratto, la sostituzione dell'indirizzo web continua ad essere ancora oggi una delle scelte preferite. Così come avveniva nel caso precedente, questa volta ad essere sostituito da un immagine contraffatta è solo l'URL contenuto nella barra degli indirizzi. Per smascherare il trucco è sufficiente aprire una qualsiasi finestra o semplicemente la finestra delle proprietà per vedere come il falso URL si sovrappone su queste ultime.

- **finestre popup**

Basata fondamentalmente sullo sfruttamento delle vulnerabilità dei browser, la tecnica delle finestre di popup è senza dubbio la scelta che garantisce il migliore rendimento per il phisher; infatti mentre in background è presente il vero sito una finestra priva di barra degli indirizzi, degli strumenti ed in alcuni casi anche con il tasto destro disabilitato richiede informazioni riservate al malcapitato utente. Tuttavia è possibile sfruttare questa tecnica anche attraverso il semplice linguaggio di programmazione HTML infatti attraverso il seguente codice:

```
<html>
<head>
<title>Anti-Phishing Italia </title>
</head>
<body topmargin="0" leftmargin="0" rightmargin="0" bottommargin="0">
<iframe src="http://www.yahoo.com" width="100%" height="650"
frameborder="0"></iframe>
<iframe src="http://www.hotmail.com" width="0%" height="350"
frameborder="0"></iframe>
```

```
</body>  
</html>
```

è possibile visualizzare nel primo frame il sito originale, mentre nel secondo frame è possibile eseguire un apposita finestra popup oppure in alcuni casi programmi keylogger.

- **Cross Site Scripting (CSS o XSS)**

Questa tecnica consiste nell'esecuzione ed inserimento di codice arbitrario, normalmente form, all'interno di un sito vittima e nella rispettiva visualizzazione di tale codice nel browser dell'ignaro utente come se facesse parte del sito vittima. La sua pericolosità sta di fatto nell'incapacità del sito reale di convalidare l'input prima di ritornare nel sistema dell'utente.

- **Trojan, Worms e Spywere**

Come già detto a favorire i casi di phishing ci ha pensato Internet Explorer, tuttavia un particolare contributo è arrivato anche da Microsoft Windows grazie ad una vulnerabilità riscontrata in tutte le sue versioni sulla gestione del file HOSTS. Quando digitiamo il nome di un dominio nel nostro browser il protocollo IP interroga il DNS per conoscere il corrispondente indirizzo IP; ma prima di far questo controlla il file HOSTS per verificare la presenza di tale indirizzo, se è presente, si collega automaticamente. A sfruttare questa vulnerabilità per rubare i numeri dei conti correnti on-line ci ha pensato il worm PWS-Banker.y e le sue varianti prendendo di mira importanti servizi di home banking tra cui Banca Intesa, Banca Lombarda, Csebanking, BYBank di BancaAntonveneta, Credito Cooperativo e Banca Sella. Inoltre un ulteriore alleato dei phisher è keylogger, il quale è in grado di registrare in maniera subdola e silenziosa tutto quello che viene digitato all'interno del nostro sistema: username e password, indirizzi e-mail, numeri di carta di credito, conto correnti, informazioni riservate.

2.2 - Un esempio di phishing sicuro

23/09/2005. A lanciare l'allarme su una nuova generazione di phishing è la SurfControl azienda che opera nel settore della sicurezza informatica dal 1997, la quale ha rilevato l'utilizzo di certificati SSL auto-rilasciati all'interno di siti clone. Il nuovo phishing si basa sugli elementi tradizionali, tuttavia nel momento in cui l'utente accede al falso sito per inserire i propri codici personali, viene attivata una falsa connessione protetta certificata dal lucchetto nella barra di stato del browser, facendo così cadere ogni sospetto all'utente il quale ora è realmente convinto di trovarsi all'interno del vero sito della propria banca on-line.

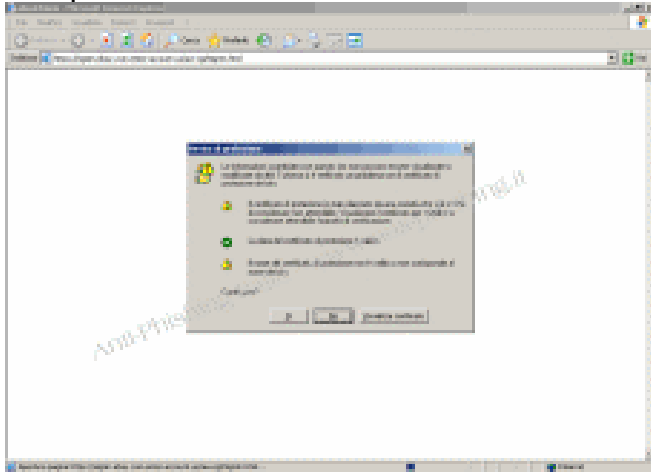
I certificati SSL auto-rilasciati rappresentano una realtà all'interno delle strutture aziendali, dove vengono utilizzati per autenticare i documenti interni ed hanno la caratteristica fondamentale di avere come "certificate authority" lo stesso creatore.

Tuttavia i browser nel momento in cui incontrano un certificato SSL di questo tipo, dopo aver controllato la sua validità, visualizzano un messaggio di pericolo, che nella maggior parte dei casi viene ignorato dagli utenti.

In tale data (23/09/2005) viene segnalato il primo caso di phishing sicuro, con il quale l'ingegnoso phisher era in grado di visualizzare all'interno del sito clone appositamente realizzato per sottrarre dati personali e bancari ad ignare vittime, l'icona tipica di una connessione sicura.

Vediamo, con un esempio, tecnicamente che cosa succede analizzando un caso reale di phishing "sicuro" ai danni di eBay:

- cliccando sull'apposito link proposto nell'e-mail truffa l'utente viene trasportato all'interno del sito clone



Un messaggio di avviso informa l'utente che durante l'accesso alla connessione sicura, si sono verificati dei problemi con il certificato SSL, nello specifico:

- Il certificato di protezione è stato rilasciato da una società che si è scelto di considerare non attendibile. Visualizzare il certificato per stabilire se considerare attendibile l'autorità di certificazione.
- Il nome del certificato di protezione non è valido o non corrisponde al nome del sito.

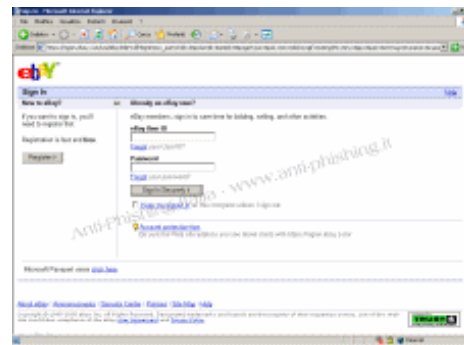
Questo avviene in quanto tali certificati di sicurezza vengono rilasciati da apposite Certificate Authority riconosciute legalmente mentre nel nostro caso il browser non è in grado di verificarne l'attendibilità in quanto siamo di fronte ad una versione auto-rilasciata dallo stesso phisher.

La comparsa di tale avviso dovrebbe mettere subito in allarme anche un utente meno esperto il quale avrebbe l'obbligo di capire che qualcosa non va, visto che collegandosi al vero sito eBay tale messaggio non è mai apparso; tuttavia poiché molti utenti non conoscono il vero significato di tale messaggio ed a volte sono proprio infastiditi da simili interruzioni, il tasto "Sì" rappresenta la scelta più diffusa.

A questo punto la vittima accede al sito clone:



il sito clone eBay



il vero sito eBay

Adesso la truffa è piazzata è l'unica possibilità per l'utente di distinguere il sito clone è riuscire a riconoscere eventuali errori nell'indirizzo web, il quale in questo caso risulta ben realizzato grazie all'utilizzo dei sottodomini. Ciò nonostante un'ulteriore soluzione è data dal controllo del certificato, cliccando sull'apposita icona, che mostra l'inattendibilità di esso. Tuttavia malgrado le varie discrepanze tecniche la truffa svolge il suo lavoro, infatti, per il phisher l'unico scopo è quello di illudere l'utente sull'autenticità del sito, pertanto consigliamo a tutti gli utenti soprattutto quelli poco esperti di prestare la massima attenzione ai vari messaggi di avviso segnalati dal browser il quale in questo caso avrebbe potuto salvare le tasche della malcapitata vittima se solo avesse prestato un po' più di attenzione.

3 - Spear Phishing

Lo spear phishing impiega una strategia di phishing molto più mirata. Gli autori di questo tipo di frode inviano messaggi di posta elettronica che sembrano attendibili a tutti gli impiegati o i membri di una determinata società, ente statale, organizzazione o gruppo.

La struttura del messaggio lascia intendere che il mittente è il datore di lavoro o un altro dipendente o collega (ad esempio, il responsabile delle risorse umane o la persona che gestisce i sistemi informatici) e può includere richieste di nomi utente e password.

In realtà le informazioni sul mittente vengono falsificate o ricavate tramite "spoofing". Mentre il phishing tradizionale si propone lo scopo di sottrarre informazioni da singoli utenti, le frodi che si basano sullo spear phishing hanno come obiettivo quello di penetrare all'interno dell'intero sistema informatico di una società.

Se fornisci il nome utente o la password oppure selezioni dei collegamenti o apri gli allegati in un messaggio di posta elettronica, in una finestra a comparsa o in un sito Web di spear phishing, diventi vittima di un furto d'identità ed esponi a rischi gli altri dipendenti o membri del tuo gruppo di lavoro.

Le frodi tramite lo spear phishing sono rivolte anche agli utenti che utilizzano un determinato prodotto o sito Web. Gli autori di tali frodi utilizzano qualsiasi informazione a disposizione per personalizzare un messaggio di phishing, in modo da restringere il più possibile il gruppo di utenti a cui è rivolto.

Per evitare le frodi di spear phishing si utilizzano le stesse tecniche adottate per il phishing tradizionale.

4 – Difesa dal phishing

4.1 – Metodologie di difesa

Una preoccupazione frequente degli utenti che subiscono il phishing è capire come ha fatto il perpetratore a sapere che hanno un conto presso la banca o servizio online indicato nel messaggio-esca. In realtà, normalmente il phisher non sa se la sua vittima ha un account presso il servizio preso di mira dalla sua azione: si limita ad inviare lo stesso messaggio-esca a un numero molto elevato di indirizzi di e-mail, facendo spamming, nella speranza di raggiungere per caso qualche utente che ha effettivamente un account presso il servizio citato. Pertanto non è necessaria alcuna azione difensiva a parte il riconoscimento e la cancellazione dell'e-mail che contiene il tentativo di phishing.

Nel caso del problema correlato noto come pharming, invece, non esiste una vera e propria soluzione a posteriori ed è necessaria un'azione preventiva. Un primo controllo per difendersi dai siti di phishing che tentano di sottrarre i dati della carta di credito, è quello di visualizzare l'icona (a forma di lucchetto in tutti i browser) che segnala che si è stabilita una connessione sicura (ad esempio una connessione SSL). La pagina di autenticazione è facilmente imitabile, copiando il relativo codice HTML, mentre la presenza di una connessione sicura richiede dei certificati che identificano univocamente un sito Internet.

Esistono programmi specifici che consentono di avvisare l'utente quando visita un sito probabilmente non autentico. Gli utenti di Microsoft Outlook / Outlook Express possono proteggersi anche attraverso il programma gratuito Delphish, un toolbar inserito nel MS Outlook / MS Outlook Express con il quale si può trovare i link sospetti in un'e-mail. Questi programmi e i più comuni browser non si avvalgono di whitelist contenenti gli indirizzi logici e IP delle pagine di autenticazione di tutti gli istituti di credito, che sarebbe un filtro anti-phishing sicuramente utile.

Se l'utente non è titolare di un conto corrente on-line e riceve gli estratti conto periodici per posta ordinaria (non via e-mail), può impostare il filtro anti-spam sull'indirizzo dell'istituto di credito. In questo modo, le e-mail contenenti un indirizzo del mittente o un link nel testo alla banca, saranno inserite nella cartella dello spam, rendendo più facilmente identificabili quelle sospette. Gli utenti di Internet Explorer possono utilizzare un filtro anti-phishing che utilizza una blacklist, e confronta gli indirizzi di una pagina web sospetta con

quelli presenti in una banca dati mondiale e centralizzata, gestita da Microsoft e alimentata dalle segnalazioni anonime degli utenti stessi.

Mancano invece banche dati di questo tipo condivise dai vari produttori di browser, pubbliche o istituite presso autorità che hanno la competenza sulle tematiche di Internet e del web (in Italia, la Polizia Postale).

L'oscuramento di un sito di phishing non è un'operazione semplice, se questo è ospitato come sottodominio di un altro indirizzo web. In quel caso, è necessario l'oscuramento del dominio ospitante, poiché la "falsa" pagina di autenticazione non è presente nell'elenco ICANN, ma in locale sul server. Il sito oscurato può essere comunque velocemente associato ad un altro indirizzo web.

E' possibile associare ad una pagina di un sito di phishing un indirizzo simile, ma non identico a quello del sito "copiato". Due pagine web, infatti, non possono avere lo stesso indirizzo IP né lo stesso indirizzo logico, che è associato ad un solo indirizzo IP.

All'utente medio resta comunque difficile distinguere un sito di phishing da quello dell'istituto di credito preso di mira. La barra degli indirizzi può contenere un indirizzo del tipo "Nome della

Banca.autethicationPage.php@indirizzo del dominio ospitante", l'indirizzo del dominio ospitante nel corrispondente indirizzo IP, il simbolo "@" nella codifica ASCII, o nell'equivalente binario o esadecimale, rendendo l'indirizzo della risorsa di "phishing" simile e poco più lungo di quello che è stato falsificato.

Tre semplici regole per evitare di cadere nella trappola dei phisher sono:

1. Non fornire dati personali tramite e-mail.

Importanti aziende come Ebay, PayPal e Microsoft ma soprattutto la vostra banca, non vi chiederanno mai di fornirgli tramite e-mail i dati dei vostri account, password o numeri di carta di credito.

2. Aggiornare il Pc.

3. Siate sempre sospettosi e cauti

Se ritenete di aver ricevuto un e-mail sospetta è consigliato innanzitutto verificare la sua eventuale presenza all'interno dei vari archivi. A questo punto il passo successivo è quello di denunciare immediatamente la frode all'azienda contraffatta stando attenti a NON utilizzare i collegamenti presenti all'interno dell'e-mail ricevuta.

Cosa fare se si è risposto a un messaggio di phishing

Se sospetti di avere risposto a un messaggio di phishing fornendo informazioni personali o finanziarie, per posta elettronica o immettendole in un sito Web falsificato, puoi comunque limitare i danni.

Passo1 - informare le seguenti organizzazioni:

- La società di emissione della carta di credito, se hai rivelato informazioni relative alla carta di credito. Questa è la prima segnalazione da effettuare perché consente alla società di emissione della carta di adottare le misure necessarie per ridurre al minimo i danni.

- L'azienda la cui identità è stata falsificata dagli autori della frode. Ricorda di contattare l'azienda direttamente e non rispondendo al messaggio di posta elettronica che ti è stato inviato.
- La Federal Trade Commission (FTC). Denuncia l'accaduto al National Resource for Identity Theft FTC (Federal Trade Commission).

Passo2 – cambiare le password di tutti i conti on-line.

Passo3 – controllare regolarmente gli estratti conto bancari e della carta di credito.

Passo4 - utilizza prodotti e servizi aggiornati in grado di assicurare la protezione dalle frodi online.

4.2 - Filtri anti-phishing

Nel filtro anti-phishing è integrata una nuova tecnologia di tipo dinamico che protegge gli utenti dalle frodi e dai rischi di furti di dati personali sul Web.

Tramite esso si possono avere tre tipi di protezione:

- Un filtro incorporato nel browser che esamina gli indirizzi Web e le pagine Web aperte alla ricerca delle caratteristiche associate a frodi o furti perpetrati con il phishing e già noti sul Web. L'utente viene avvisato se i siti visitati sono sospetti.
- Un servizio online che impedisce all'utente di accedere ai siti fraudolenti confermati con informazioni dell'ultima ora sui siti Web dediti al phishing e già segnalati. I siti di phishing spesso appaiono e scompaiono nel giro di 24-48 ore, quindi, ai fini della protezione, è necessario disporre di informazioni aggiornatissime.
- Una funzionalità incorporata che consente all'utente di segnalare siti sospetti o frodi. Con il filtro anti-phishing, l'utente può fornire informazioni utili su qualsiasi sito Web che si ritiene in grado di sferrare attacchi di phishing potenzialmente fraudolenti. L'utente invia le informazioni a Microsoft e Microsoft le valuta. Se i sospetti vengono confermati, il servizio online aggiunge le informazioni al database per proteggere la comunità di utenti di Internet Explorer e Windows Live Toolbar.

5 - Spoofing

Lo spoofing è una tecnica utilizzata per camuffare files in rete in rete e aggirare ignari ed impotenti utenti. La parola deriva dal verbo inglese to spoof che significa imbrogliare, truffare. Come è possibile prendersi una fregatura attraverso tecniche di spoofing e in cosa consiste in particolare? Come abbiamo detto in precedenza lo spoofing è una tecnica finalizzata a vincere le resistenze, anche psicologiche, dell'utente e consentire allo spoofer di entrare all'interno di un sistema, o di collocarci alcuni suoi software maliziosi.

Potremmo paragonare lo spoofer al vampiro descritto da Bram Stoker nel suo celebre "Dracula": per entrare in una casa nottetempo, il nosferatu aveva bisogno che qualcuno lo invitasse. Così lo spoofer cerca di danneggiare i malcapitati bersagli delle sue fregature attraverso la posta elettronica, per evitare le difese degli antivirus e dell'utente. Una volta entrato nel sistema il file mascherato dallo spoofing è libero di fare quello che vuole, e spesso la formattazione immediata della macchina diventa l'unico disperato rimedio per evitare danni peggiori.

Dicevamo che lo spoofing è una tecnica maliziosa, infatti spesso si caratterizza nell'invio di e-mail contenenti allegati apparentemente innocui, tipo archivi zip, o immagini, o anche documenti di testo con estensioni rispettivamente .zip, .jpg o .txt.

La tecnica dello spoofing consiste nel mascherare l'effettiva estensione del files allegato facendo credere all'utente (e spesso anche all'antivirus) che il files allegato sia qualcosa che in realtà non è. L'e-mail spoofing probabilmente non avrebbe avuto tutto il successo che ha avuto senza Windows. Le vecchie versioni di windows, in particolare 95/98/ME gestivano male le estensioni associate a diversi tipi di files, per cui di fronte a files con estensioni plurime (come ad esempio truffa.zip.exe) windows tratta il file come un eseguibile (e gli consente di agganciarsi all'interno) mentre lo visualizza senza l'estensione (nell'esempio di prima la visualizzazione del nome del file sarebbe truffa.zip). Ma cos'è l'estensione di un file? Potremmo definire, intuitivamente, estensione di un file come quell'appendice al nome del file, preceduto da un punto, che ne indica la natura (file di testo, di immagini, di suoni, programma eseguibile, internet files etc.). Così ad esempio un file salvato con word avrà un'estensione .doc, o .rtf etc. Ebbene lo spoofer rinomina il file dandogli una doppia estensione, una reale (generalmente .exe o .hta perché si tratta di eseguibili)

ed una fittiziamente innocua tipo .gif o .txt per far abbassare le difese dell'utente che vedendosi allegata alla propria mail un ipotetico file di immagini o di testo è più propenso a scaricarlo per vedere di cosa si tratta, piuttosto che se trovasse in allegato un programma eseguibile di cui non conosce bene gli effetti. In questo modo credendo di scaricare una foto in realtà, magari, installa sul proprio computer un dialer che gli farà inoltrare a sua insaputa chiamate verso numeri a tariffazione altissima.

Come fare per evitare lo spoofing? Per evitare di subire e-mail spoofing sarebbe buona regola avere sempre antivirus e firewall aggiornati, dal momento che queste sono le uniche difese nel momento in cui si gestisce la posta elettronica ricevuta attraverso un apposito software del tipo outlook, eleutera, etc. Questi tipi di programmi al momento della prima connessione scaricano sul nostro pc la posta ricevuta in modo che possa poi venire letta con comodo anche sconnessi. Tuttavia se abbiamo ricevuto qualche virus via mail, le uniche difese sarà un antivirus buono e soprattutto aggiornato. Se il nostro antivirus non è aggiornato rischiamo di ricevere direttamente allegati all'interno del nostro computer senza poter più intervenire se non a cose fatte. Viceversa non correremo questi rischi nel momento in cui visualizzeremo la posta elettronica direttamente da internet, come consentono di fare numerosi provider. In questo modo potremo scegliere se scaricare gli allegati oppure no. Buona norma sarebbe quella di evitare sempre di scaricare allegati provenienti da sconosciuti.

6 - Pharming (manipolazione di indirizzi web)

Il pharming è una ulteriore tecnica fraudolenta che sempre più spesso si sta accompagnando al phishing.

Mentre il phisher, generalmente, carpisce la buona fede degli utenti di internet attraverso falsi messaggi confidenziali, con il Pharming l'inganno è ancora più occulto.

La truffa consiste nel realizzare pagine web identiche ai siti già esistenti (banche, assicurazioni, softwarehouses etc.) in modo che l'utente sia convinto di trovarsi, ad esempio, nel sito della propria banca e sia indotto a compiere le normali transazioni sul proprio conto on-line. Una volta digitate le credenziali (password e user ID) del proprio conto, sarà semplice recuperarle, tramite keylogger o troiani, per utilizzarle a fini fraudolenti.

Come potrei imbartermi in un sito clonato? Ad esempio a seguito di una segnalazione proveniente attraverso un e-mail fraudolenta (phishing) in cui mi si invita a recarmi presso il sito della mia banca per ragioni di servizio o di sicurezza (utilizzando espressioni tipo "il suo conto deve essere confermato", oppure "per ragioni di sicurezza dovrebbe controllare se le sue password sono ancora attive", "per motivi di sicurezza deve compilare il seguente form", etc.). Una volta selezionato il collegamento verrei instradato su un sito identico a quello della mia banca ma in realtà diverso.

Esistono anche altri modi con cui è possibile clonare siti, ovvero servendosi

attraverso il pharming.

Ma in cosa consiste il pharming? Esso consiste in un intervento di manipolazione delle direzioni verso le quali viaggiano le informazioni relative agli indirizzi web verso i quali ci si dirige. In parole povere: l'utente digita l'indirizzo di un sito, ad es. www.banca&banche.it. A questo nome a dominio corrisponde un indirizzo IP composto da un codice numerico formato da dodici cifre, ad es 000.000.000.000.

Nel momento in cui noi digitiamo il nome di un sito nella barra degli URL, dopo aver digitato su "cerca" inviamo l'informazione relativa al sito che vogliamo visitare ad un server, per l'appunto quello in cui è ospitato il sito. Il server decodifica l'indirizzo web da noi digitato con l'indirizzo IP numerico appartenente al sito.

Con il pharming accade invece che questa corrispondenza fra nome a dominio del sito e suo indirizzo IP venga interrotta; al nome a dominio indicato viene associato un nuovo indirizzo IP relativo al sito creato dal Pharmer.

In sostanza il Pharming si concretizza in un attacco al server che gestisce le direzioni DNS (domain name system), in modo da far instradare la connessione verso il sito voluto, indipendentemente dalla volontà dell'utente ed evitando ogni contatto con il sito effettivamente clonato.

Il pharming è una tecnica d'attacco che riguarda soltanto i gestori di server? No, affatto. Esiste un altro tipo di pharming che si verifica a livello locale, all'interno del computer dell'utente, sfruttando una vulnerabilità del sistema di Windows.

All'interno del pc che gira su una piattaforma Windows esiste una cartella chiamata "host" ove sono contenuti gli indirizzi di server e gli indirizzi IP che maggiormente utilizza l'utente. Sarà sufficiente modificare gli indirizzi IP presenti in quella cartella perché il nostro motore di ricerca ci indirizzi verso un sito che non corrisponde a quello reale. Esistono infatti alcuni tipi di virus, chiamati troyani, che sono in grado di modificare automaticamente gli indirizzi IP presenti nella cartella "host".

7 - Spamming

Lo spamming è una parola che descrive un fenomeno molto noto a tutti coloro che utilizzano la posta elettronica: l'invio di materiale pubblicitario non richiesto e, spesso, non desiderato. Dunque, nell'accezione comune, la parola sta ad intendere la spazzatura che periodicamente ci riempie la casella di posta elettronica, costringendoci a ripulirla periodicamente per evitare che la intasi del tutto impedendoci di ricevere le comunicazioni che effettivamente aspettiamo.

Ma chi ha interesse a fare spamming? Lo spamming ha prevalentemente una natura commerciale. Inviare sistematicamente e-mail per reclamizzare un nuovo prodotto, informare sull'apertura di un nuovo esercizio commerciale, proporre offerte lancio per determinati prodotti non costa praticamente nulla. Esistono software in grado di rastrellare indirizzi sul web prelevandoli da siti, forum, newsgroup ed immagazzinarli in banche dati private per poi utilizzarli ai fini dell'invio di materiale pubblicitario.

Ma quanto costa ad un'azienda inviare migliaia di e-mail? Praticamente nulla.

Provate a pensare quanto dovrebbero spendere le imprese se volessero promuoversi con i sistemi promozionali. Realizzare i volantini, stamparli, spedirli per posta o recapitarli tramite incaricati del volantinaggio sono attività che invece hanno un costo non indifferente. Con lo spamming, invece, è sufficiente un semplice click e migliaia di persone sanno che il negozio all'angolo vende software con il 50 % di sconto.

Inoltre lo spamming, rispetto alle tecniche pubblicitarie tradizionali, riesce ad essere maggiormente capillare: è molto più semplice rilevare un indirizzo e-mail su internet che un indirizzo civico nel mondo reale, specialmente perché molti soggetti non compaiono in elenchi pubblici accessibili a chiunque come gli elenchi telefonici o le pagine gialle.

Lo spamming è l'avamposto di una nuova forma di commercializzazione di beni e servizio chiamata "direct marketing", ovvero, come ci suggerisce la traduzione maccheronica della locuzione, una forma di commercio diretto verso l'utente, piuttosto che orientato in forma seriale e con strumenti di comunicazione generalizzati.

Inoltre le statistiche dimostrano che qualche utente lo si riesce comunque ad interessare attraverso il direct marketing, ed è facile che un soggetto curioso si tramuti in cliente. Eppoi a fronte di investimenti praticamente irrisori, questa forma di pubblicità garantisce ritorni remunerativi.

Ma tutto questo è lecito? Una adeguata risposta a questa domanda necessita di alcune precisazioni. Se ci riferiamo all'ordinamento dell'Unione europea la risposta è sicuramente no. O meglio, non è possibile fare spamming senza il consenso del soggetto destinatario del messaggio pubblicitario. Lo ha previsto espressamente la direttiva 58/2002/CE, poi recepita in Italia nel testo unico sulla privacy, Decreto Legislativo n. 196/2003.

Per quanto riguarda il diritto degli USA invece si tratta di una prassi perfettamente legale.

Lo spamming, nella maggior parte dei casi proviene, dagli States inibendo così l'uso dei rimedi previsti dalla direttiva 58/2002/CE agli utenti del vecchio continente. Se invece lo spammer è europeo, o meglio tricolore, allora il discorso si fa più semplice.

Come si può fare per non ricevere più spamming? Il primo passo è individuare chi sta effettuando lo spamming: se si tratta di un mittente USA converrà lasciar perdere. Se invece il mittente è italiano bisognerà reperire un suo recapito fisico (ad esempio visitando il sito internet cui solitamente rimanda l'e-mail dello spammer) e comunicargli la propria opposizione al trattamento dei propri dati di posta elettronica, e la cancellazione dei propri dati dagli archivi del soggetto che sta effettuando il trattamento, come prevedono gli articoli 7 e 8 del D. Lgs. n. 196/2003.

Se a fronte dell'avvenuta comunicazione dell'opposizione e della richiesta di cancellazione lo spammer continua ad inviarci e-mail non richieste potremo agire presso il Garante per la protezione dei dati personali che potrà ordinarci di cancellare i nostri dati personali dai suoi archivi elettronici o cartacei.

8 – Aspetti legali

8.1 - Il phishing come illecito civile

È bene tenere in considerazione la circostanza che il phishing sarebbe quasi impossibile da realizzare al di fuori di internet. All'interno della rete avviene l'iniziale truffaldino invio dell'e-mail con cui si invita il destinatario a recarsi presso il sito del proprio istituto di credito; si consiglia di recarsi all'interno dell'area del sito dedicata al proprio conto corrente, e quindi compilare, eventualmente, ulteriori form. Sempre attraverso la rete avviene la successiva raccolta delle informazioni da parte del phisher e quindi la sottrazione del denaro dell'utente.

Appare utile ricordare come l'art. 122 del D.Lgs. n. 196/2003 (Codice privacy) inibisca a chiunque la possibilità di utilizzare *«una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente»*, al contrario di quanto pratica il phisher nel compimento del proprio comportamento illecito.

Ricordando che per *«abbonato»* il codice intende *«qualunque persona fisica o giuridica, ente od associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico»* appare di tutta evidenza come il disposto normativo dell'art. 122 del D.Lgs. n. 196/2003 riguardi senz'altro anche i dati contenuti nei server degli istituti di credito. Tali dati vengono utilizzati dal phisher –una volta che li abbia ottenuti ingannevolmente dai legittimi titolari- per sottrarre il denaro dell'utente o dell'abbonato e per trasferirlo presso altri beneficiari.

Una volta individuato il responsabile dell'illecito, questi sarà senz'altro tenuto al risarcimento dei danni patrimoniali e non patrimoniali che abbia eventualmente cagionato alla propria vittima.

Sempre restando in ambito civilistico, l'intera attività del phisher si configura come un illecito trattamento di dati personali dei soggetti colpiti dalla propria attività: i dati vengono carpiri senza che vi sia un effettivo consenso dell'interessato, anzi quest'ultimo non può sapere che in realtà le informazioni che riceve dal phisher per convincerlo a recarsi presso il proprio account sono assolutamente false.

In base al disposto dell'art. 15 del codice privacy, *«chiunque cagioni un danno per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile»*. La formulazione della norma tuttavia si presta a considerazioni ed a conclusioni ulteriori, e per certi versi sorprendenti.

Se il fine della norma è quello di punire *«chiunque»* cagioni un danno nell'ambito del trattamento, c'è da chiedersi se una parte di responsabilità non sia attribuibile anche agli stessi istituti di credito, vista l'ampia gamma semantica della nozione di *«trattamento»* che il codice prevede.

All'interno del procedimento che consente al phisher di danneggiare le proprie vittime, un ruolo importante viene, infatti, rivestito anche dalle banche che consentono (o meglio non impediscono) a terzi estranei di accedere alle informazioni relative a propri clienti.

Non è superfluo ricordare che, a mente dell'art. 31 del codice, ogni titolare di un trattamento di dati personali (qual è per l'appunto l'istituto di credito riguardo i dati dei propri clienti) deve custodire e controllare i dati personali trattati in modo da ridurre al minimo il rischio di accessi non autorizzati agli stessi.

In particolare, prescrive il codice privacy, tale custodia e tale controllo devono essere commisurati alla conoscenze acquisite in base all'evoluzione del progresso tecnico, oltre che del tipo di trattamento effettuato. Dunque, la gestione di conti correnti on-line, piuttosto che off-line, prevede per il titolare l'obbligo di predisporre misure ulteriori ed "evolute" per cautelarsi dal rischio di accessi non consentiti o non autorizzati. Ciò con particolare riguardo ad un rischio "nuovo" per l'istituto di credito, legato all'evoluzione del progresso tecnico in materia di software per la realizzazione di pagine web, ovvero quello di subire il pharming (ovvero una illecita "clonazione") del sito da cui vengono gestiti gli account dei propri clienti.

Anche questa omissione -ovvero la mancata vigilanza circa l'esistenza di attività di pharming nei confronti del proprio sito, ove esso sia possibile- potrebbe riverberarsi sul proprio cliente come un'attività idonea ad arrecargli un danno. Quindi, nell'ottica della dialettica prevista dal testo unico sui dati personali, il danno deriverebbe per effetto del trattamento effettuato dal titolare - banca, nei confronti dell'interessato-cliente. In tal caso potrebbe rivelarsi decisamente arduo per il titolare fornire in giudizio la dimostrazione di aver posto in essere ogni attività idonea ad evitare il verificarsi del danno, come prescrive l'art. 2050 c.c., quando in realtà non è stata posta in essere alcuna misura per evitare che il proprio sito venisse clonato.

Tuttavia gli aspetti di natura civilistica passano senz'altro in secondo piano rispetto ai profili di natura penale legati al fenomeno.

8.2 - Il phishing come truffa

La natura "ontologica" del phishing, al di fuori dei profili legati alle violazioni del codice privacy, è senz'altro connessa alla truffa, figura di reato descritta dall'art. 640 del codice penale.

Recita la norma penale relativamente alla truffa *«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 milletrecentadue euro»* (art. 640, comma 1).

Indubbiamente la tecnica del phishing costituisce un raggirio artificioso del destinatario dell'e-mail-phishing, dal momento che lo induce a credere che essa provenga effettivamente dal proprio istituto di credito e lo porta a collegarsi, tramite un link, ad un sito in tutto e per tutto identico a quello col quale il destinatario si aspetterebbe di essere collegato.

Alcuni dubbi potrebbero essere sollevati in considerazione delle seguenti circostanze: ovvero che spesso le e-mail inviate dai phisher non sono scritte in un italiano impeccabile, e che il nome al dominio relativo al sito "clone" dell'istituto di credito non ha in realtà nulla a che vedere con la propria banca e spesso ha un'estensione riconducibile a paesi extra UE.

Tuttavia queste obiezioni, pur valide, non tolgono nulla al carattere truffaldino del phishing, né inficiano la sua natura antiggiuridica dal momento che spesso gli utenti leggono le proprie e-mail frettolosamente, sono ormai abituati alle traduzioni in un italiano stentato effettuate in automatico dai software forniti dai motori di ricerca e non prestano attenzione agli indirizzi dei nomi a dominio dei siti che visitano. Inoltre la cronaca giudiziaria ci descrive fenomeni di phishing sempre più raffinati ed "evoluiti", spesso i nomi a dominio dei supposti istituti bancari differiscono dagli originali soltanto relativamente ad alcune, od una sola lettera.

Resta da chiedersi se il reato di truffa, previsto dal comma 1 dell'art. 640 sia effettivamente «*più grave*» rispetto a quello di trattamento illecito di dati personali di cui all'art. 167 del D.Lgs. n. 167/2003, al fine di valutare quale delle due ipotesi delittuose possa dirsi operante nei casi di phishing, e la risposta non può che essere positiva.

La truffa "semplice", ovvero quella descritta dal primo comma dell'art. 640 c.p. prevede, oltre alla pena detentiva identica nel massimo alla sanzione prevista per l'art. 167 del codice privacy, anche la pena pecuniaria della multa fino a 1032 euro. Di conseguenza, in caso di phishing, si dovrebbe ritenere applicabile il reato di truffa, e si dovrebbe escludere il concorso di reati con il delitto di illecito trattamento di dati personali, previsto dalla legge speciale. Per quanto riguarda la truffa "semplice" possiamo richiamare le considerazioni di natura processuale già espresse per l'illecito trattamento, circa i termini di prescrizione, i limiti alle intercettazioni, e l'impossibilità di richiedere ed applicare misure cautelari coercitive od interdittive.

Tuttavia una differenza rilevante attiene alla condizione di procedibilità per l'accertamento e la repressione dei due reati: mentre il reato previsto dal codice privacy è procedibile d'ufficio, la truffa "semplice" è procedibile su querela della persona offesa.

Il problema diventa allora individuare nel phishing chi possa considerarsi come persona offesa: in particolare può essere considerata persona offesa soltanto il soggetto che ha subito il phishing o anche l'istituto di credito? In caso di inerzia dell'utente, può la banca validamente esercitare poteri di impulso di natura processuale? Per rispondere positivamente al quesito è opportuno verificare se la truffa perpetrata dal phisher sia o meno suscettibile di arrecare un danno di natura patrimoniale anche alla banca, e la risposta non può che essere positiva. L'istituto di credito, nella maggior parte dei casi, non appena è al corrente del fatto che alcuni suoi clienti sono stati vittime di phishing è costretta ad adottare delle procedure straordinarie per informare la propria clientela e per invitarla a non divulgare i propri codici riservati. Inoltre tale tipo di informativa viene generalmente rilasciata in via riservata e non tramite pubblici annunci, per ovvi motivi legati alla pubblicità negativa che subirebbe la banca, ma con l'inevitabile aggravio di spesa che la comunicazione riservata comporta. Molte banche hanno attivato, inoltre, degli appositi call-center ove i clienti possano rivolgersi in caso ricevano e-mail di dubbia provenienza. Difficile non vedere come tutte queste attività comportino un costo in termini di tempo e denaro per la banca e che costituiscano un indubbio danno che essa subisce a causa della truffa del phisher, e che pertanto la legittimerebbe alla proposizione della querela.

Oltre alla truffa "semplice", procedibile a querela, l'art. 640 c.p. prevede anche delle ipotesi di truffa "aggravata", procedibile d'ufficio.

Particolarmente interessante, appare l'ipotesi di truffa aggravata prevista al n. 2) del comma 2 dell'art. 640 c.p., che si verifica quando il fatto sia stato commesso «*ingenerando nella persona offesa il timore di un pericolo immaginario*». Molto spesso capita che il phisher nel proprio messaggio inviato al suo destinatario, lo inviti a recarsi repentinamente presso il sito della propria banca, paventando proprio rischi di truffe o altri accessi non consentiti ai propri dati.

Pertanto così facendo, il phisher ingenera nella persona offesa un rischio che in realtà non potrebbe sussistere senza la fattiva collaborazione di quest'ultimo, un rischio che non esisterebbe se la persona offesa decidesse di restare inerte. Ad ogni modo, quando il messaggio inviato dal phisher non si limita sic et simpliciter a collegarsi verso il sito linkato dallo stesso messaggio, ma sollecita tale attività adombrando eventuali rischi collegati alla sicurezza della rete, allora il phishing effettuato ricadrà nell'ambito della truffa aggravata piuttosto che in quello della truffa semplice.

La sanzione prevista per la truffa aggravata è decisamente più grave: reclusione da uno a cinque anni e multa da trecentonove euro a millecinquecentoquarantanove euro. Nel caso della truffa aggravata pertanto, gli inquirenti potranno, come detto, procedere anche d'ufficio alla repressione dell'illecito, chiedere l'applicazione di misure cautelari coercitive od interdittive ed effettuare intercettazioni ambientali, telefoniche o telematiche.

8.3 - Il phishing come accesso abusivo ad un sistema informatico

Il comportamento del phisher è idoneo ad integrare gli elementi di un ulteriore reato: l'accesso abusivo ad un sistema informatico, previsto dall'art. 615 ter c.p. ed anch'esso introdotto, come il reato di frode informatica, dalla legge n. 547/93 (legge istitutiva dei cosiddetti reati informatici o computer crimes). Anche questa figura delittuosa prevede una ipotesi semplice ed una aggravata. Il reato di accesso abusivo ad un sistema informatico è punito, nell'ipotesi non aggravata, con la reclusione da uno fino a 3 anni ed è procedibile a querela. Viceversa nell'ipotesi aggravata (ovvero qualora il fatto sia stato commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema, oppure se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato, od ancora se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti) la pena è la reclusione da uno a cinque anni.

Quindi se l'azione di phishing abbia causato il blocco, anche momentaneo dell'accessibilità dell'account dell'utente presso il suo istituto creditizio, ricorreranno gli elementi dell'ipotesi aggravata dell'accesso abusivo, sanzionata più duramente, con le relative conseguenze di natura processuale già

richiamate in precedenza.

Esiste una ulteriore ipotesi aggravata di accesso abusivo a sistema informatico, la quale si potrebbe verificare qualora l'accesso abusivo, sia nell'ipotesi semplice che in quella aggravata, abbia avuto ad oggetto sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. In tal caso la pena prevista dalla norma è, rispettivamente, la reclusione da uno a cinque anni se relativa ad un accesso abusivo semplice, mentre da tre a otto anni se ha avuto ad oggetto un'ipotesi aggravata.

La Corte di Cassazione ha più volte espresso il proprio convincimento circa la possibilità di un concorso di reati fra l'accesso abusivo a un sistema informatico e la frode informatica. La condotta di accesso, infatti, non possiede tutti gli elementi puniti dal reato di frode informatica. La condotta punita da quest'ultimo è necessariamente caratterizzata dalla manipolazione dei dati presenti nel sistema (*«intervenendo senza diritto con qualsiasi modalità su, dati, informazioni o programmi»*, secondo la formula utilizzata dalla norma). Tale manipolazione non è prevista nè richiesta per il reato di accesso abusivo, il quale si configura nel momento in cui un soggetto *«abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo»*. Soffermandosi sulla prima parte delle due condotte contemplate dalla norma pocanzi richiamata appare evidente l'"abusività" del phisher il quale accede all'account della propria "vittima" senza averne alcun titolo eludendo le procedure di autenticazione e di identificazione predisposte dal sistema per tutelare i dati ivi custoditi da accessi non consentiti, quindi abusivi.

Pertanto pare non irragionevole ipotizzare che nel caso del phishing possa esservi anche un accesso abusivo, accompagnato ad una frode informatica. Appare invece da escludere l'eventualità del concorso formale fra i due reati: ovvero la violazione di più norme penali con la commissione di una sola azione od omissione. L'esclusione del concorso formale appare è dovuta all'esistenza di due momenti concettualmente slegati nell'attività del phisher: in primo luogo v'è l'introduzione all'interno del sistema (che realizza il reato di accesso abusivo), successivamente la manipolazione dei dati contenuti nell'account dell'utente (che realizza invece la frode informatica).

Appare preferibile descrivere l'intera gamma degli illeciti compiuti dal phisher nell'ambito del reato continuato, poiché il phisher commette una molteplicità di reati collegati fra loro (truffa, illecito trattamento dei dati personali, accesso abusivo, frode informatica ed eventualmente ulteriori reati fiscali) nell'esecuzione di un medesimo disegno criminoso. Anche se, in fin dei conti, il trattamento sanzionatorio previsto per il concorso formale è identico a quello previsto per il reato continuato, ovvero l'applicazione della pena prevista per il reato più grave moltiplicato per tre. Nella migliore delle ipotesi al phisher, ove gli venga riconosciuto il reato continuato, non gli si potrà infliggere una pena inferiore a nove anni.

Riferimenti:

- <http://www.anti-phishing.it>
- <http://www.microsoft.com>
- <http://www.poste.it>
- <http://it.wikipedia.org>

Sommario:

- 1 – Phishing: caratteri generali
- 2 – Metodologia d'attacco
 - 2.1 – Tecniche principali dei phisher
 - 2.2 – Un esempio di phishing sicuro
- 3 – Spear phishing
- 4 – Difesa dal phishing
 - 4.1 – Metodologie di difesa
 - 4.2 – Filtri anti-phishing
- 5 – Spoofing
- 6 – Pharming
- 7 – Spamming
- 8 – Aspetti legali
 - 8.1 – Il phishing come illecito civile
 - 8.2 – Il phishing come truffa
 - 8.3 - Il phishing come accesso abusivo ad un sistema informatico