

Phishing: ciò che occorre sapere

Viene definito **phishing** la tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli, opportunamente creati per apparire autentici ed inviati con l'oramai classica tecnica dello Spam. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati sensibili, come numero di conto corrente, nome utente e password, numero di carta di credito ecc. In questi ultimi mesi, ad esempio, sono stati numerosi i casi di **phishing** ai danni dei clienti di banche italiane quali Fineco Unicredit e ultimamente Antonveneta.

Come funziona il phishing?

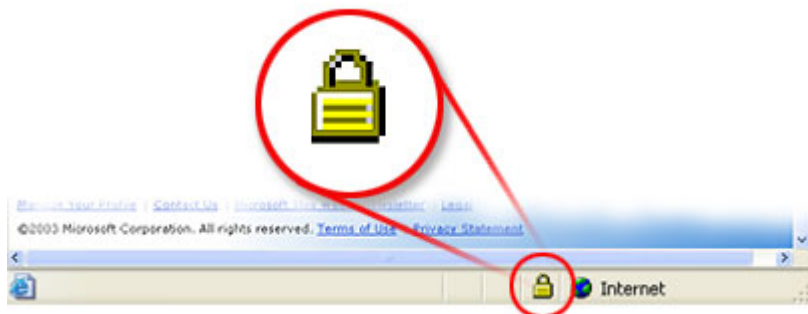
Il processo di queste metodologie di attacco può riassumersi nei seguenti passi:

1. Il phisher spedisce al malcapitato ed ignaro utente un messaggio e-mail che simuli nella grafica e nel contenuto quella di una istituzione nota al destinatario (ad es. la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. la e-mail contiene avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad es. un addebito enorme, la scadenza dell'account ecc.).
3. nella mail il destinatario è invitato 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 collegamento al sito web della banca fornito NON porta in realtà al sito web ufficiale, ma a pagine appositamente create per emulare il sito in oggetto e richiedere al 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 e quindi finiscono nelle mani del phisher.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Ecco cosa fare per proteggersi dal phishing

Gli esperti di phishing continueranno a sviluppare nuove e più subdole forme di inganno online, così come si può osservare dalle indagini svolte dal nostro GlobalTrust 911 Network alla pagina <http://www.globaltrust.it/news/phishing/index.aspx>. Tuttavia, seguendo questi passaggi è possibile proteggere le proprie informazioni.

1. Non rispondere mai a richieste di informazioni personali ricevute tramite posta elettronica. In caso di dubbio, rivolgetevi all'istituto che dichiara di avervi inviato l'e-mail.
2. Visitare i siti Web digitandone il rispettivo URL nella barra degli indirizzi..
3. Verificare che il sito Web utilizzi la crittografia e i relativi certificati digitali.



Icona del lucchetto su un sito protetto. Il lucchetto chiuso indica che il sito utilizza la crittografia.

4. Esaminare regolarmente i rendiconti bancari e della carta di credito.
5. Denunciare sospetti usi illeciti delle proprie informazioni personali alle autorità competenti.