

Truffe INFORMATICHE

PHISHING

COS'E'?

Il termine **Phishing** deriva da *fishing*, cioè "pescare" e richiama volutamente il riferimento al pesce che abbocca all'amo. È un tipo di **truffa** diffuso in tutto il mondo, tanto da aver originato anche un'associazione che si preoccupa di combatterlo www.antiphishing.it . Anche in Italia si segnalano già numerosi casi, con gli attacchi più importanti registrati ai danni delle Poste e di alcune banche.

Il meccanismo è molto semplice: **tutto si basa su un messaggio email** che riprende nell'aspetto, nella grafica e anche nel logo quello dell'azienda presa come bersaglio: servizi di banche on line o società di carte di credito come Visa, società di servizi di pagamento online (.eBay, PayPal). Il messaggio **chiede di aggiornare, modificare o comunque inserire i propri dati personali** (spesso password o numeri di carta di credito) **clickando su un link apposito** oppure (a volte) compilando un modulo all'interno dello stesso messaggio email. **Il sito a cui fa riferimento il link** oppure il modulo stesso non hanno naturalmente **niente a che vedere con l'azienda citata nella mail** e così i dati incautamente forniti finiscono nella banca dati del truffatore che ha inviato la finta e-mail.

Questi messaggi (le "phishing e-mail") vengono inviati in gran numero ma è sufficiente che ne vadano a segno pochi per provocare notevoli danni e ottenere consistenti guadagni.

La contraffazione dei dati del mittente (banca, società emittente carte, servizi di pagamento online) viene effettuata accuratamente in modo da indurre il destinatario ad abboccare alla proposta fraudolenta e ad effettuare le azioni richieste.

Truffe di questo tipo possono essere smascherate semplicemente analizzando la richiesta che può fare riferimento a strumenti (conto online, carta , etc.) che non rientrano nella operatività del cliente. Ad es. il cliente potrebbe non aver mai effettuato pagamenti tramite eBay o PayPal dai quali proviene la richiesta fraudolenta per la fornitura dei dati personali.

COSA FARE ?

I **CONSIGLI** da seguire sono semplici ed allo stesso tempo efficaci:

- **Non utilizzare mai link riportati su messaggi email** che sembrano puntare a servizi protetti da password in precedenza sottoscritti (banche, account di posta, qualsiasi collegamento necessiti di autenticazione). Le banche, le società emittente le carte, le società che gestiscono sistemi di pagamento online non richiedono mai informazioni personali in un messaggio di posta elettronica. In caso di dubbio, prima di rispondere conviene contattare telefonicamente l'azienda che l'ha inviata.
- **Non inserire dati significativi in moduli o siti che non sono crittografati in SSL.** Questo è verificabile controllando l'indirizzo del sito: gli indirizzi SSL iniziano con https:// invece di http:// e dalla presenza del lucchetto "giallo" sulla barra in basso dello schermo.
- **Accedere al sito** in cui vanno immessi i dati **inserendo direttamente il percorso e caricandolo dai preferiti/segnalibri della propria rubrica.**
- **Tenere aggiornato il proprio browser.** A volte questi attacchi sfruttano anche delle debolezze dei browser usati dagli utenti. Le versioni aggiornate dei browser più diffusi (Internet Explorer, Firefox, Opera) sono dotate di sistemi in grado di identificare e limitare l'impatto di queste truffe.

- **Controllare regolarmente gli estratti conto** della banca e delle carte di credito.
- **Segnalare immediatamente** eventuali casi sospetti alla propria Banca ed alle autorità.

RICORDA: la Banca non richiede mai i dati personali del cliente per l'accesso ai servizi di home banking che, sono e devono essere noti solamente all'utente.

Per Saperne di più

[Polizia di Stato](#) (italiano)

[Consigli da Microsoft](#) (italiano)

www.antiphishing.org