ALTRO CASO DI TRUFFA utilizzando i vostri dati personali.

Dopo aver pubblicato un annuncio sul sito di annunci economici, riceverete un messaggio di contatto da parte di una persona interessata all'acquisto, ma che Vi invita a controllare i dati del vostro annuncio perchè incompleti. Il vostro annuncio è indicato con un link http://autoblu.com/sk/bat/aut.php?..... *chiaramente falso.*

Il link contenuto nel messaggio porta a una pagina fasulla, identica alla home page dell'azienda ove avete inserito l'annuncio nell'apposito form, inserite i vostri dati personali di accesso e così, i codici di identificazione personale vengono acquisiti dal malfattore che accede nella vostra area personale modificando i vostri annunci pubblicati.

IN PARTICOLARE: Il malfattore in possesso dei vostri dati (user-id e password), entra nella vostra area personale, modifica l'indirizzo email di contatto nel vostro annuncio di vendita e vende qualcosa al posto vostro intascando il denaro e senza inviare la merce.

UN SUGGERIMENTO:

SE PONETE IL MOUSE SU UN LINK, GUARDATE IN BASSO A SINISTRA SULLA BARRA DI STATO CHE SI TROVA SOTTO IL VOSTRO BROWSER E VISUALIZZERETE L'INDIRIZZO A CUI FA CAPO QUEL LINK.

(se non visualizzate la barra di stato, è sufficiente spuntarlo andando su Visualizza-Barra di stato).

UN SISTEMA DECISAMENTE NUOVO PER EVITARE TRUFFE.

Il "Deposito a garanzia ESCROW"
E' possibile utilizzare anche il sistema di deposito a garanzia con il quale un intermediario si inserisce nel rapporto tra venditore ed acquirente in qualità di fiduciario.
Ad es. www.escrow-europa.com

Il servizio funziona così:

1. Il compratore versa il prezzo su un conto fiduciario;
2. Il fiduciario avvisa il compratore del deposito dei soldi.
3. Il fiduciario consegna i soldi al venditore solo nel momento in cui la merce giunge al compratore senza vizi. Ciò aumenta la sicurezza per il compratore.
4. Il servizio di amministrazione fiduciaria tutela contemporaneamente anche la sicurezza del venditore, il quale sa già prima di inviare la merce che il prezzo è già stato pagato ed è nelle mani del fiduciario. Attraverso questa forma di pagamento si ha la possibilità di proteggersi da eventuali truffe o da consegne errate, poiché l'importo pagato per la merce rimane in custodia fino all'arrivo della merce ed è prevista l'ulteriore possibilità di verificare se la merce giunta presenta dei vizi e solo successivamente consentire il trasferimento dei soldi al venditore.
5. Costa qualcosa in più per il servizio ma garantisce di evitare truffe.

* presidente IPA , sovr. c. della P. di S.

INTERNATIONAL POLICE ASSOCIATION
Sezione Italiana — XV Delegazione Marche
Comitato Esecutivo Locale Macerata-Fermo

Via Saragat c/o Centro civico Fontespina
62012 Civitanova Marche

Comitato Locale

Macerata-Fermo

Truffe via web?

«Cose da sapere e...»

di Tommaso Galeone *

www.ipa-macerata.it

Truffa via web? «Cose da sapere e ...»

Il PHISHING

- **spillaggio** di dati sensibili -

vietato dalla legge, ha lo scopo principale di ottenere l'accesso a informazioni personali o riservate (user-id e password).

Il furto d'identità avviene mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.

Grazie a messaggi che imitano grafica e logo dei siti tipo poste e banche, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc..

Metodologia di attacco.

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

1. *il phisher* spedisce al malcapitato e ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il provider web 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, oppure un'offerta di denaro o premi).
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.
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 e 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 sue mani.
5. il phisher utilizza questi dati per acquistare beni o trasferire somme di denaro.

Nessuna azienda chiede al proprio cliente i codici perchè la stessa azienda può azzerare gli account e fornirne uno nuovo.

NON CONSIDERATE e-mail nelle quali vi viene chiesto di effettuare il login utilizzando un link contenuto nel messaggio.

Per le pagine personali importanti, accedete sempre direttamente utilizzando l'indirizzo web che avete salvato nei preferiti oppure digitatelo direttamente.

Nel caso aveste fornito i vostri dati personali con la procedura sopra descritta, accedete subito al vostro account direttamente dal sito originale, modificate la password e comunicate l'accaduto all'azienda coinvolta.