BANCHE: ABI PRESENTA DECALOGO PER DIFENDERSI DA TRUFFE WEB

(ANSA) - COURMAYEUR (AOSTA), 1 DIC - Dieci semplici regole destinate agli oltre 8 milioni di clienti dell'home banking per evitare le truffe via internet. Le ha presentate oggi a Courmayeur, l'Associazione bancaria italiana (Abi), nel corso della Conferenza Internazionale dell'Onu sul tema "La sfida crescente della frode identitaria: come combattere frode, abuso e falsificazione dell'identita", promossa dal Centro nazionale di prevenzione e difesa sociale (Cnpds), dalla Fondazione Courmayeur e dall'Ispac (International Scientific and Professional Advisory Council of the United Nations Crime Prevention and Criminal Justice Programme).

Il decalogo e' dunque una delle armi di informazione ai clienti con cui le banche italiane stanno cercando di arginare il problema sicurezza posto dal boom di internet e in particolare dell'home banking': l'85% dei navigatori italiani fanno acquisti on-line e oltre 2,5 milioni nel 2007 paga con carte di credito.

L'Abi ha ricordato oggi, tra l'altro, che "mai potranno essere richiesti dati riservati su codici e password via email" e che "le iniziative truffaldine non sono personalizzate, chiedono informazioni personali per motivi non specificati e fanno uso di toni intimidatori". I clienti pertanto - raccomanda l'Abi - non devono rispondere a email con richieste di questo tipo, ma informare subito la banca e non devono mai cliccare su link presenti in email sospette perche' questi collegamenti potrebbero condurre ad un sito contraffatto. (ANSA).

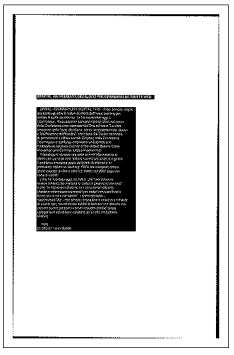
KWL
01-DIC-07 14:54 NNNN

BANCHE: ABI PRESENTA DECALOGO PER DIFENDERSI DA TRUFFE WEB (2)

(ANSA) - COURMAYEUR (AOSTA), 1 DIC - Questi, in sintesi, i contenuti del decalogo di suggerimenti per i clienti dell'home banking per difendersi dal phishing, presentato oggi dall'Abi, a Courmayeur:

- la banca non chiede dati riservati su codici e password via email;
- le email truffaldine non sono personalizzate, chiedono informazioni personali per motivi non specificati e fanno uso di toni intimidatori;
- non rispondere mai a email con richieste di questo tipo ma informare subito la banca;
- non cliccare su link presenti in email sospette perche' questi collegamenti potrebbero condurre ad un sito contraffatto;
- assicurarsi, quando si inseriscono dati riservati in una pagina web, che si tratti di una pagina protetta, riconoscibile in quanto l'indirizzo che compare nella barra del browser comincia con hppts:// e non con http:// e nella parte in basso a destra compare un lucchetto;
- diffidare se improvvisamente cambia la modalita' con la quale viene richiesto di inserire i codici di accesso personali all'home banking;
- controllare regolarmente gli estratti conti;
- controllare periodicamente l'aggiornamento del browser;
- aggiornare sempre il software antivirus perche' email truffaldine e siti di phishing tentano di installare sul computer della vittima un codice malevolo atto a carpire le informazioni personali in un secondo momento, attivandosi quando vengono digitate;
- non digitare dati riservati e personali se non si e' sicuri dell'identita' di chi lo sta chiedendo: in caso di dubbio rivolgetevi in banca.

Dal punto di vista tecnico - e' stato spiegato oggi - le email sono in formato html e contengono un collegamento nascosto al sito web contraffatto. I server sui quali sono installati i



siti di phishing sono posizionati in paesi con cui la collaborazione delle forze dell'ordine italiane e' difficoltosa: il 47% di essi e' infatti collocato in Corea, il 17% in Russia e il 4% in India. Attualmente la collaborazione fra banche e forze dell'ordine consente di reprimere entro 12 ore l'attivita' del sito di phishing. (ANSA).

KWL/FCO
01-DIC-07 16:41 NNNN