TRUFFE WEB Come difendersi? Decalogo dell'Abi

Per non abboccare...

COURMAYEUR

Dieci semplici regole destinate agli oltre 8 milioni di clienti dell'home banking per evitare le truffe via internet. Le ha presentate ieri 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'identità».

Questi, in sintesi, i contenuti del decalogo.

1) La banca non chiede dati riservati su codici e password via email; **2)** le email truffaldine non sono personalizzate, chiedono informazioni personali per motivi non specificati; **3)** non rispondere mai a email con richieste di questo tipo ma informare subito la banca; **4)** non cliccare su link presenti in email sospette perché questi collegamenti potrebbero condurre ad un sito contraffatto; **5)** 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; **6)** diffidare se improvvisamente cambia la modalità con la quale viene richiesto di inserire i codici di accesso personali all'home banking; **7)** controllare regolarmente gli estratti conto; **8)** controllare periodicamente l'aggiornamento del browser; **9)** aggiornare sempre il software antivirus perché 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; **10)** non digitare dati riservati e personali se non si è sicuri dell'identità di chi lo sta chiedendo: in caso di dubbio rivolgetevi in banca.

Dal punto di vista tecnico - è 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 è difficoltosa: il 47% di essi è 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'attività del sito di phishing.

Acquisti via web: attenzione