

## **PANEL "INFORMAZIONE E PREVENZIONE DELLE FRODI NEI PAGAMENTI ELETTRONICI: IL RUOLO DELLE AZIENDE"**

Il seminario si è concluso con il Panel "Informazione e prevenzione delle frodi nei pagamenti elettronici: il ruolo delle aziende": **ABI, Unicredit, Poste Italiane e ICCREA Banca Spa** hanno parlato delle loro esperienze e di come stanno fronteggiando il problema delle frodi creditizie e delle truffe on line.

**Alessandro Zollo, responsabile settore Sistemi e Servizi di pagamento Retail di ABI** "Gli strumenti di pagamento diversi dal contante sono in forte crescita in Europa, anche se in Italia il cashless è ancora in netto ritardo nonostante si registri un incremento delle carte di pagamento trascinate dalla diffusione delle carte di debito e delle carte BANCOMAT. Per fortuna, il numero di frodi, a partire dal 2007, è in notevole diminuzione anche grazie allo sviluppo di azioni di contrasto e prevenzione delle frodi con carte di pagamento. Per quanto ci riguarda, ABI e il Consorzio BANCOMAT hanno collaborato con il MEF – UCAMP – Ufficio Centrale Antifrode Mezzi di Pagamento per la creazione dell'Archivio informatico SIPAF, che ha coinvolto oltre 700 banche/emittenti carte. Anche per l'Internet Banking, le iniziative del sistema bancario per la sicurezza del canale sono aumentate, in primis sul fronte dell'educazione della clientela ad un impiego sicuro del canale. Dal 2007 il ricorso a log-in e password come metodo di autenticazione viene progressivamente accantonato a favore di sistemi in grado di tutelare maggiormente privacy e sicurezza. Sempre maggiore è il ricorso alle password dispositive che vengono introdotte in modo stabile sull'operatività affiancate da sistemi a maggiore complessità quali la One Time Password viene offerta da circa il 46% delle banche campione, contro il 36% del 2006 e il 20% nel 2005. Cresce l'attenzione rispetto all'introduzione di policy interne e la creazione di vere e proprie "task force" per far fronte a eventuali emergenze attivando sistemi di monitoraggio per una tempestiva individuazione delle frodi".

**Luigi Altavilla, Head of Information Security Retail Italy Network Division di Unicredit** "La sicurezza online deve essere un problema della Banca, che deve dare al cliente la serenità di operare senza alcun rischio. Le principali strategie di UniCredit Banca per combattere le frodi online sono prima di tutto l'educazione della clientela: parlare e informare i clienti sulle minacce online, insegnare cosa fare (e non fare) e come difendersi. Abbiamo puntato anche sulla collaborazione con le FF.OO. e con le altre istituzioni finanziarie per condividere le informazioni sulla sicurezza online e sviluppato una partnership con Symantec. Dal punto di vista tecnologico, puntiamo ad aggiornare e perfezionare gli strumenti di protezione, integrare nuove tecnologie per migliorare la sicurezza online e sviluppare sistemi di monitoraggio preventivi e un processo di gestione degli incidenti".

**Raffaele Panico, fraud management di Poste Italiane** "Il nostro sito è sicuramente tra i più attaccati dal phishing, soprattutto perché

abbiamo uno strumento molto diffuso nel mondo come Carta Poste Pay, che purtroppo, essendo utilizzato via Internet, è molto appetibile ai truffatori. Sulla comunicazione al cliente già dal 2005 abbiamo iniziato a mandare avvertimenti e comunicazioni a casa. Monitoriamo continuamente le transazioni dei nostri clienti: nel caso di una transazione fatta da un indirizzo IP straniero, quando normalmente l'operatività del cliente è su indirizzi IP italiani, blocchiamo la transazione e chiediamo conferma al cliente dell'effettività dell'operazione. Dal 1° marzo 2009, inoltre, partirà il Progetto Oracolo, che ci consentirà di verificare la veridicità dei documenti che vengono presentati allo sportello collegandoci con il Ministero dell'Interno che ha l'archivio di tutti i documenti smarriti o rubati. Oggi riusciamo a chiudere gli attacchi di phishing in 12 ore e abbiamo realizzato una grande centrale di sicurezza".

**Antonio Galiano, responsabile E-Bank di ICCREA Banca S.p.A**

"La crescita globale dell'e-commerce è molto sostenuta ed è strettamente legata alla disponibilità di strumenti di pagamento elettronici (credit cards, paypal, ecc.), che stanno continuando a sostituirsi sempre di più al cash. Di conseguenza, anche le frodi seguono questi trend e si stanno spostando dalle 'Card Present' (principalmente clonazioni) alle card non present' (on-line e furto d'identità). Per evitare le frodi, è necessario tra l'altro l'uso della Tecnologia 3D Secure per generare password 'usa e getta' per acquisti online su siti abilitati al servizio (Verified By Visa e Secure Code di MasterCard) e puntare sulla Customer Education".