ABI Associazione Bancaria Italiana

COMUNICATO STAMPA

ABI: nelle banche attività di sensibilizzazione e formazione contro i crimini informatici

Aumenta l'impegno del mondo bancario nella lotta ai crimini informatici attraverso iniziative di formazione del personale, campagne di sensibilizzazione per la clientela e presidi tecnologici. Nel 2017 le banche italiane hanno investito oltre 300 milioni di euro per garantire alla clientela "operazioni" digitali ancora più sicure. I clienti retail vittime di frode sono stati solamente lo 0,0018% del totale di quelli che operano su home banking, pari ad uno su 55 mila.

Secondo lo studio ABI Lab sulla sicurezza on line, con l'affermarsi del digitale, sempre più rilevante nelle abitudini di cittadini e imprese, per le banche risulta fondamentale attuare attività di sensibilizzazione e formazione non solo per la clientela, ma anche per il personale bancario. In particolare, nel 2017 le azioni si sono concentrate maggiormente sulla formazione del personale specialistico addetto alla sicurezza (per il 75% delle banche intervistate), e del personale di filiale (per il 67,9%) per la relazione diretta con la clientela e la relativa assistenza offerta in caso di anomalie. Sul tema della sensibilizzazione verso la clientela sui rischi del *cybercrime* lo studio sottolinea che le banche italiane hanno sviluppato campagne attraverso il portale di Internet Banking (per il 96% delle banche rispondenti), attraverso le informative presso le filiali (per il 74,1%), le informative contrattualistiche (per il 59,3%), le informative sulle App dei dispositivi mobili (per il 37%) e quelle via e-mail (per il 33%) e si sono fatte promotrici di collaborazioni intersettoriali, come il CERTFin – CERT Finanziario Italiano (Computer Emergency Response Team).

La sicurezza informatica, tuttavia, passa anche attraverso la collaborazione dei clienti delle banche. Per operare on line in modo comodo e sicuro, infatti, è importante seguire alcune semplici regole: ignorare qualunque richiesta di dati relativi a carte di pagamento e conto on line, che la banca non chiederà mai alla propria clientela; connettersi al sito della banca scrivendo direttamente l'indirizzo nella barra di navigazione, ignorando eventuali link ricevuti via mail ed sms; verificare sempre l'autenticità della connessione con la banca; controllare regolarmente i movimenti del proprio conto per assicurarsi che le transazioni riportate siano quelle effettuate; diffidare di qualsiasi messaggio, anche se apparentemente autentico, ricevuto tramite e-mail, sms, social network, che inviti a scaricare documenti o programmi; installare e mantenere sempre aggiornato il sistema operativo e l'antivirus; fare attenzione a eventuali peggioramenti delle prestazioni generali (rallentamenti, apertura di finestre non richieste, ecc.) del proprio servizio di home banking o del proprio PC, che possono indicare infezioni sospette.

Roma, 23 giugno 2018