

Ecommerce e mobile banking, Abi lancia vademecum per acquisti sicuri online

mercoledì 20 dicembre 2017

Regole semplici per pagamenti sicuri”.

Da dove si parte?

Cambiare

regolarmente le password e non comunicarle ad altri, evitare il salvataggio automatico di password e chiavi d'accesso sul browser, installare e aggiornare sempre gli antivirus: sono i primi passi per pagamenti sicuri attraverso home banking, mobile banking e carte di pagamento. I consigli diventano poi più dettagliati. Ad esempio: non inviare immagini dei propri strumenti di pagamento ed evitare di spedire via email o cellulare la fotografia di un assegno, che potrebbe essere usato, se la controparte è in malafede, per costruire un “clone” da incassare al posto dell'originale.

I consigli

vengono da un vademecum realizzato dall'Associazione bancaria italiana (ABI) per acquisti sicuri in Rete, che ha l'obiettivo di promuovere l'uso responsabile della tecnologia e degli strumenti di pagamento e concludere senza rischi transazioni di commercio elettronico, usare con attenzione le carte e accedere in sicurezza da pc o cellulare ai canali digitali delle banche.

“Consapevolezza

e attenzione: queste le caratteristiche fondamentali richieste ai consumatori quando utilizzano i nuovi canali digitali per gestire operazioni di pagamento”, sottolinea l'Abi, che ha promosso la campagna di sensibilizzazione sull'uso responsabile della tecnologia e degli strumenti di pagamento, realizzata da Bancaria Editrice con il contributo di ABI Lab e di interlocutori quali Polizia di Stato, CERTFin e Fondazione per l'Educazione Finanziaria e al Risparmio (Feduf). I messaggi della campagna comunicazione sono veicolati attraverso la guida cartacea “Home banking, carte, e-commerce... Regole semplici per pagamenti sicuri”, compendio di consigli pratici e buone prassi per utilizzare senza rischi i servizi di e-commerce e le carte di pagamento, accedere in sicurezza all'home banking e al mobile banking ma anche usare consapevolmente il computer e i Social network. Prevista anche una versione digitale in forma di infografica destinata ai canali Social e ai siti Web.

Tra i messaggi

veicolati oltre a semplici suggerimenti – come la raccomandazione agli utenti dell'home banking a modificare periodicamente i codici di accesso alla propria area riservata, a non utilizzare computer condivisi per concludere transazioni online o, ancora, l'accortezza di non conservare mai il Pin assieme alle proprie carte di pagamento – anche consigli tecnici come l'indicazione di cliccare, una volta connessi al sito della propria banca, sull'icona a forma di lucchetto nella barra di navigazione per avere conferma sull'attendibilità del sito Web. Gli utenti di servizi bancari via smartphone sono tra l'altro invitati a utilizzare solo applicazioni ufficiali, mantenere sempre aggiornati antivirus e sistema operativo e attivare la crittografia del telefono e della scheda di memoria.