Banche, chiavette e sicurezza: la rivoluzione del 14 settembre

Molti clienti lo sanno da tempo, messi in allerta da lettere e email dalle proprie banche: nel mondo dei pagamenti digitali sta per cambiare qualcosa e la data è molto vicina: il 14 settembre entrerà infatti in vigore una novità prevista dalla direttiva europea PSD2. E un altro tassello della direttiva, che sarebbe dovuta entrare in vigore sempre il 14, è stato prorogato a data da destinarsi ma solo per quegli istituti bancari che si sono fatti cogliere di sorpresa, nonostante il provvedimento Ue risalga al 2015.

Servizi bancari sempre più fluidi

Partiamo dalla novità che entrerà subito in vigore. Dal 14 settembre le banche saranno obbligate a condividere con terze parti tutte le informazioni che hanno sui propri correntisti. A patto, naturalmente, che il cliente autorizzi il proprio istituto di credito a farlo: sarà una sua libera scelta.

Queste “terze parti” hanno dei nomi da filastrocca: Pisp, Aisp e Cisp ma a ogni sigla corrisponde qualcosa di preciso e, potenzialmente, di grande utilità per il consumatore. Vediamo cosa sono:

- I Pisp (Payment Initiation Service Providers) sono società intermediarie tra il pagatore (consumatori o aziende) e la propria banca che hanno lo scopo di versare denaro a un terzo soggetto. Grazie ai Pisp sarà possibile effettuare un pagamento su un sito di ecommerce (impossibile non pensare ad Amazon) senza inserire i dati della propria carta di credito o bancomat, perché sarà il venditore ad accedere direttamente al nostro conto (previa una nostra prima autorizzazione, che in seguito verrà ricordata) e prelevare. Altri giganti del panorama digitale, come Google e Facebook, potranno beneficiare di questa nuova opportunità addebitando i clienti senza passare per il tramite di alcuna carta. Per accedere al conto del cliente i Pisp devono comunque usare procedure di autenticazione e devono mettere a disposizione del cliente tutte le informazioni relative a quell'operazione;
- Gli Aisp (Account Information Service Provider) sono servizi che "spiano" (sempre dietro consenso)i nostri conti correnti e le nostre carte, analizzano e aggregano questi dati per fornirci un quadro complessivo delle nostre finanze in un'unica schermata. Ad esempio un report sul nostro patrimonio complessivo, le entrate e le uscite del mese. E in base a questi dati possono fornire consigli su come investire i nostri soldi o proporre strumenti "salvadanaio". Cosa non possono fare: operare sul conto corrente o detenere i soldi del cliente;
- I Cisp (Card Issuer Service Providers) sono invece soggetti che emettono carte di pagamento. Solo che, a differenza delle prepagate (che il cliente può ricaricare di volta in volta prelevando denaro dal proprio conto corrente), queste sono direttamente collegate al conto corrente, anche se è stato aperto in una banca differente. I Cisp forniscono la carta ma non detengono il denaro del cliente, hanno però un canale

privilegiato per accedervi.

Pagamenti più sicuri (con qualche disservizio)

E poi c'è il grande tema degli strumenti di sicurezza per pagare online. La direttiva rafforza le misure a tutela dei risparmiatori, per prevenire frodi e furti di identità. La sicurezza dei clienti, secondo il testo, si basa su tre principi:

- Conoscenza: cioè una password o un codice pin che conosce solo l'utente;
- Possesso: uno strumento che possiede solo l'utente (uno smartphone o un token);
- Inerenza: cioè qualcosa che l'utente è, ad esempio un'impronta digitale o il riconoscimento facciale.

Le procedure di autenticazione delle banche devono prevedere almeno due di questi principi. Ad esempio: una password generata su smartphone, un pin generato da un token o un'impronta digitale impressa sul telefonino. Questi nuovi standard hanno portato diverse banche italiane a mettere in soffitta il caro vecchio token, provocando in alcuni casi qualche malumore tra i clienti (sulle nostre pagine abbiamo parlato del caso di Banca Intesa).

Queste nuove procedure sarebbero dovute entrare in vigore il 14 settembre ma Banca d'Italia ha fatto sapere lo scorso primo agosto che "in considerazione della complessità degli adeguamenti" e per "ridurre fortemente i rischi di disservizi nei pagamenti online con carta", ha deciso di concedere una proroga per un periodo limitato agli operatori che ne facciano richiesta e a patto che spieghino, nel dettaglio, in che modo intendono procedere. Quanto tempo durerà la proroga? Banca d'Italia spiega che questo verrà definito dall'Eba (l'autorità bancaria europea) che nello scorso giugno aveva autorizzato le banche centrali nazionali a concedere più tempo in casi limitati.

Addio al token? Non è detto

Il problema dei token attuali è che generano un codice (l'Otp, one time password) che pura pochi secondi ma non esclude la possibilità che un truffatore informatico possa utilizzarlo per compiere una seconda operazione-lampo, drenando soldi dal conto del cliente. Con le nuove regole, invece, il codice "restituito" al cliente è valido solo e soltanto per quella operazione.

Attenzione, però: anche se le banche dovranno togliere di mezzo gli attuali token, non è detto che questi strumenti scompariranno del tutto: alcuni istituti di credito semplicemente li sostituiranno con alcuni di nuova generazione (ad esempio Deutsche Bank consentirà ai propri clienti di scegliere tra uno virtuale, gratis, e uno fisico col tastierino, a pagamento). Il problema che diversi consumatori lamentano è che le banche, costrette dalla nuova direttiva, punteranno tutto sulle app per smartphone (come in effetti sta accadendo) discriminando chi possiede un telefono di vecchia generazione. In realtà diverse banche – tra le quasi Intesa Sanpaolo – prevedono, proprio per casi simili, l'invio del codice via sms, spesso a pagamento.

Non mancano, comunque, le critiche a questo aspetto della direttiva: "Per la mia esperienza, non ho mai avuto notizia di utenti che siano stati truffati o abbiano subito furti di identità usando gli attuali token. Le nuove misure di sicurezza servono piuttosto ad armonizzare le procedure di pagamento a livello europeo, ma non è vero che fino ad ora pagavamo in modo poco sicuro" dice **Giuseppe Mermati**, referente del settore bancario per l'Unione Nazionale Consumatori.

Mentre **Carlo Piarulli**, responsabile del settore credito per Adiconsum, si sofferma soprattutto sulla parte della direttiva dedicata alle "terze parti": "Dal 14 settembre sarà ancora più importante prestare la massima attenzione ai consensi che forniamo alla nostra banca. Perché è vero che i nuovi servizi

potrebbero essere utili a molti consumatori, ma è anche vero che si tratta di condividere informazioni preziose, e questo non può essere fatto a cuor leggero”.

Piarulli, come diversi altri osservatori, vede in questa direttiva un possibile “cavallo di Troia” per le banche tradizionali. “Giganti come Google, Facebook e Amazon avranno la possibilità di instaurare un rapporto sempre più diretto con i propri clienti e, con il tempo, potranno intercettare la clientela delle banche per portarli a sé. Non è un caso che queste società abbiano chiesto la licenza da operatori bancari in alcuni Paesi Ue.

www.repubblica,it