

CAPITOLO 4:

I PAGAMENTI INNOVATIVI



Come si stanno evolvendo i

PAGAMENTI

ELETTRONICI?





MESCOLIAMO LE IDEE



Quando effettuiamo pagamenti ricorrendo a strumenti come le Carte effettuiamo un **PAGAMENTO ELETTRONICO**.

- ▶ Le tecnologie associate a questo tipo di pagamenti **stanno cambiando molto rapidamente**: siamo passati dalla banda magnetica al pagamento con microchip, e oggi possiamo pagare anche solo avvicinando la Carta al POS.

Ciò è possibile grazie alla **tecnologia "CONTACTLESS"**, che già comincia ad essere utilizzata anche per effettuare pagamenti attraverso Smartphone abilitati.





- ▶ In futuro potremo lasciare a casa il portafoglio e uscire solamente con il nostro smartphone, in cui saranno rese virtuali le nostre Carte di Pagamento.

Così come potremo **“virtualizzare”** anche la nostra carta di identità, l’abbonamento dei mezzi pubblici, della palestra, le carte fedeltà... grazie ad **apposite App!**



Ma torniamo ai pagamenti... Con una App caricata sul nostro smartphone potremo "sostituire" il nostro portafoglio fisico, aggregando in un **Mobile Wallet** una o più Carte di Pagamento, con le quali potremo pagare da remoto (cioè indipendentemente dal luogo dove si trova il commerciante) oppure in prossimità (cioè presso il commerciante), sfruttando tecnologie quali **NFC, QR CODE, BLE**, etc.

GLOSSARIO

Anche Apple, Google e Samsung hanno già lanciato i propri **Wallet** in più Paesi e a breve arriveranno in Italia!



GLOSSARIO

[esci](#)[a](#) [b](#) [c](#)

NFC: l'acronimo indica la Near Field Communication, una tecnologia wireless basata sullo standard ISO/IEC 18092. La tecnologia consente la trasmissione di informazioni, ad una velocità massima di 424 kbit/s, tra dispositivi distanti, tra loro, non più di 4 centimetri.



In Italia esistono ancora molte **paure legate alla sicurezza dei pagamenti elettronici** e in particolare sulla tecnologia contactless...

Ci si chiede, per esempio:



“Se un malintenzionato tenesse attivo un proprio ricevitore vicino ai POS presso i quali vengono effettuati pagamenti contactless con Carte e smartphone, potrebbe impossessarsi di informazioni utili ad effettuare frodi?”

LA RISPOSTA E' NO!





Il **MICROCHIP** contenuto nella Carta **custodisce tutte le informazioni in modo assolutamente sicuro**. Il malintenzionato non potrebbe, quindi, acquisire informazioni sufficienti a replicare quelle necessarie a effettuare un ulteriore pagamento.

Per quanto riguarda lo **smartphone**, le informazioni sono scambiate con il POS utilizzando complesse tecniche di crittografia; inoltre, lo scambio avviene solo in seguito ad esplicita attivazione della APP di pagamento da parte del proprietario dello smartphone.



Tutti gli acquisti fatti su Internet attraverso il PC, il Tablet o anche lo Smartphone vengono definiti **E-COMMERCE**.



Nell'ultimo anno, in Italia, gli acquisti on line sono aumentati, ma il nostro Paese resta sempre indietro rispetto agli altri Stati, soprattutto per il timore di incorrere in frodi!



Le frodi esistono, ma i miglioramenti tecnologici aiutano sempre più ad impedirle.



Esistono delle **BUONE PRASSI** per evitare le frodi e per comprare in modo intelligente:



① **controlliamo sempre il dominio del sito** da cui acquistiamo; se ha qualcosa di strano, presenta apparenti errori di battitura o ricorda il nome di un sito famoso potrebbe non essere attendibile;

② **diffidiamo dalle offerte troppo vantaggiose** rispetto al prezzo di mercato, potrebbero essere relative a merci contraffatte o di dubbia provenienza (es. oggetti rubati);





3

valutiamo sempre le recensioni lasciate da altri utenti circa l'affidabilità del venditore; cerchiamole sul sito d'acquisto, sui blog o nei motori di ricerca;

4

verifichiamo che il sito abbia il simbolo del "lucchetto chiuso" nella barra dell'indirizzo, e, cliccando sul lucchetto, leggiamo le informazioni di dettaglio per assicurarci che non ci siano warning di sicurezza;

5

forniamo solo le informazioni essenziali per il pagamento.



COMPLIMENTI, questo capitolo è stato concluso.

