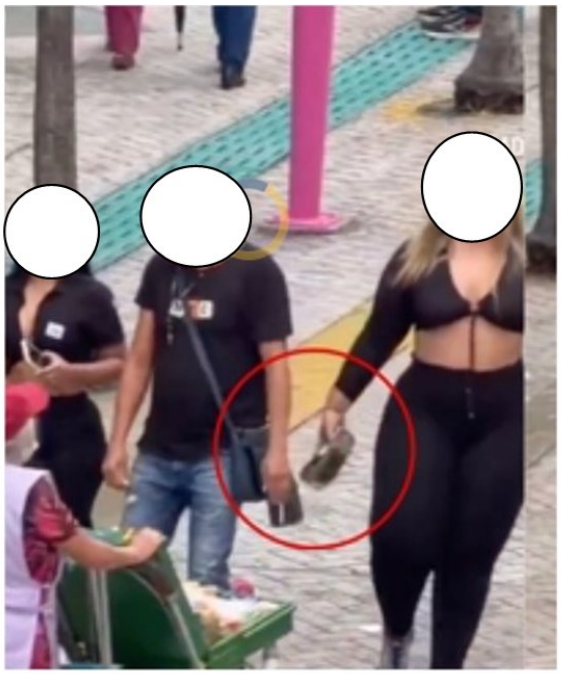
Anti-Borseggio Contactless



Il borseggio contactless avviene quando un malintenzionato utilizza un lettore portatile nascosto (spesso all'interno di una borsa o di un giornale) per "leggere" i dati della tua carta di pagamento (o badge identificativo) mentre si trova ancora nel tuo portafoglio o nella tua borsa, grazie alla tecnologia a radiofrequenza (RFID/NFC).

La Barriera Fisica: Protezione RFID:

La difesa più efficace contro questo tipo di furto è creare una barriera fisica che blocchi le onde radio. **Non tenere mai la carta contactless a diretto contatto con il lato esterno di una borsa o di un portafoglio non protetto.**

Portafogli e Custodie RFID Blocking: Acquista un portafoglio, un ferma soldi o un porta carte specificamente etichettato come **"RFID Blocking"** o **"Schermato"**. Questi prodotti sono rivestiti internamente con materiali metallici (come alluminio o fibre speciali) che creano una **gabbia di Faraday** bloccando le scansioni. Sono disponibili anche **card protettive** (solitamente chiamate *jammer card*) che, inserite nel portafoglio insieme alle altre carte, emettono un segnale che confonde i lettori esterni.

Utilizzo di Fogli di Alluminio (Metodo Fai-da-Te): Se non hai una custodia schermata, puoi avvolgere le tue carte contactless in un sottile **foglio di alluminio** (carta stagnola). L'alluminio funge da scudo di base (anche se meno efficace e comodo di una soluzione professionale).

Controlli e Gestione delle Carte:

Aumentare la sicurezza delle tue carte limita i potenziali danni.

Limita la Funzione Contactless: Se la tua banca lo consente, valuta la possibilità di disattivare completamente la funzione contactless (NFC/RFID) per gli acquisti con importo superiore a una certa soglia, oppure di disattivarla del tutto, lasciandola attiva solo per i prelievi con chip. Molte banche permettono di gestire questa funzione tramite l'app mobile.

Imposta Notifiche in Tempo Reale: Abilita le **notifiche SMS o push** sul tuo telefono per ogni transazione effettuata con la tua carta. In questo modo, se viene effettuato un addebito non autorizzato, lo saprai immediatamente e potrai agire subito.

Controlla Regolarmente gli Estratti Conto: Verifica il saldo e le transazioni della tua carta frequentemente, cercando addebiti insoliti o di piccole somme (che i borseggiatori usano spesso come test).

Precauzioni Comportamentali:

Anche se il furto è "invisibile", alcune precauzioni riducono il rischio di essere presi di mira.

Attenzione nei Luoghi Affollati: I borseggiatori elettronici lavorano in luoghi dove possono avvicinarsi inosservati: metropolitane, autobus, code, mercati affollati o ascensori. Se devi estrarre la carta per pagare, fai attenzione a chi ti guarda.

Riduci il Numero di Carte: Lascia a casa le carte che non userai. Meno carte hai con te, minore è il rischio.

Usa Google Wallet o Apple Pay:I pagamenti tramite smartphone (come Google Wallet o Apple Pay) sono generalmente **più sicuri** del contatto diretto della carta fisica. Questi sistemi non inviano il numero reale della tua carta, ma un "token" (numero virtuale) usa e getta, rendendo i dati rubati inutili per transazioni future.

Cosa Fare in Caso di Sospetto o Furto:

Blocco Immediato: Se noti un addebito non autorizzato o hai il sospetto di essere stato scansionato, chiama immediatamente il **numero verde della tua banca** per bloccare la carta. Il blocco è prioritario.

Sporgi Denuncia: Se sei certo di un furto di dati, sporgi denuncia alle Forze dell'Ordine. Questo è cruciale per la procedura di rimborso (il *chargeback*) da parte della banca.

Dispositivo mobile usato per le transazioni