

## Consigli per i cittadini

Quando vi viene recapitata a casa, per posta, la carta di credito o il bancomat e il successivo codice Pin controllate che le buste siano integre e che siano della vostra banca (o di chi emette la carta di credito). Verificate che all'interno non vi siano alterazioni o rotture del cartoncino che contiene la carta e diffidate di buste bianche inviate con posta prioritaria o con francobolli (di solito sono buste con la tassa già pagata). Oltre a ricordarvi di non cedere mai la vostra carta e il vostro PIN ad altre persone (neanche al commerciante che afferma di non avere l'apparecchio P.O.S. con sé) Vi suggeriamo:

Con il bancomat

- **Allo sportello:** osservare l'apparecchiatura alla ricerca di anomalie e modifiche. Sulla verticale o diagonale della tastiera può esserci per esempio una microtelecamera.
- **Bocca della fessura:** controllare se la fessura dove si inserisce la tessera Bancomat è ben fissa. Se si muove o si stacca potrebbe significare che è stata coperta con uno "skimmer"
- **Tastiera:** verificare se anche la tastiera è ben fissa. Spesso i malfattori sovrappongono una loro tastiera per catturare il codice Pin. In questo caso c'è un gradino di un paio di millimetri
- **Pin:** digitare il codice nascondendo con il palmo dell'altra mano l'operazione
- **In caso di dubbio:** non introdurre la tessera e non inserire il Pin. Allontanarsi e se è orario di apertura chiamare il personale della banca per una verifica dell'Istituto bancario. In caso di orario di chiusura avvisare le Forze dell'Ordine che provvederanno ad accertare l'integrità dello sportello bancomat

Con le carte di credito

- **La tessera:** non perdetela mai di vista durante il pagamento
- **Estratto conto:** controllarlo ogni mese poiché è l'unico modo per accorgersi di eventuali spese mai effettuate
- **Attivare il servizio di alert (SMS) che vi avvisa immediatamente di operazioni sul vostro conto**
- **Addebiti impropri:** se vi arriva un estratto conto con addebiti impropri denunciate alle Forze dell'Ordine la clonazione della carta, disconoscendo le spese addebitate
- **Internet:** nel caso di acquisti sul web verificare se la pagina del sito è sicura (contrassegnata cioè da un lucchetto posto sulla parte inferiore dello schermo). Se così non è si corre il rischio di vedersi rubare i dati
- **Per acquisti online alla vostra banca è possibile richiedere e attivare una carta di credito prepagata sulla quale caricare importi minimi**
- **E-mail e Phishing:** se vi arrivano messaggi di posta elettronica dove vi si chiedono dati sensibili relativi alla vostra carta di credito o al conto corrente non bisogna rispondere ad alcuna richiesta. Con tutta probabilità vogliono carpire i vostri dati per farne un uso fraudolento. Il fenomeno del phishing interessa ogni giorno milioni di indirizzi e-mail. Potete filtrarli attivando il servizio Spam sulla vostra casella di posta elettronica

English

06/08/2013