Polizia di Stato

Come proteggere la nostra carta di credito

Uno dei sistemi classici utilizzati dai truffatori per acquisire entrambi i codici è chiamato skimming. Consiste nella cattura dei dati della banda magnetica con la semplice "strisciata" della carta di credito su un apparecchio denominato, appunto, Skimmer. Lo Skimmer può essere grande quanto un pacchetto di sigarette e autoalimentato con batteria, ma anche più grande, per un utilizzo meno occulto, e può immagazzinare fino a diverse decine di bande magnetiche. I dati illecitamente carpiti vengono trascritti su un supporto plastico, con le caratteristiche di una carta di credito/bancomat, attraverso un comune PC e un programma di gestione per bande magnetiche. Lo skimmer, ovviamente, è un'apparecchiatura diversa dal normale P.O.S. fornito dalle società emittenti; per eseguire questo genere di frodi è necessario quindi che il malintenzionato entri in possesso per alcuni istanti della carta di credito del cliente lontano dalla sua vista. Ecco allora una lista di accortezze che l'utilizzatore di carta di credito dovrebbe adottare per ridurre le possibilità di clonazioni e di frodi: 1. non cedere la carta ad altre persone; 2. non perdere mai di vista la propria carta di credito al momento del pagamento; 3. diffidare di un qualsiasi esercizio che afferma di non avere l'apparecchiatura P.O.S. in prossimità della cassa; 4. controllare, al momento del recapito della carta di credito e del successivo codice PIN., che la busta sia integra, che sia della vostra banca, di chi emette la carta di credito oppure della società incaricata dei servizi di recapito postale.

06/08/2013