PrimaDaNoi.it
Il primo quotidiano on line per l'Abruzzo
Testata giornalistica registrata al tribunale di Chieti n.7 del 22 agosto 2005.
Direttore responsabile: Alessandro Biancardi

Il Carding: per sapere e prevenire

Argomento: INTERNET

SPECIALE. Il furto è di sicuro uno dei reati più perpetrati.
Benchè i metodi più utilizzati siano ancora quelli "tradizionali" come scippo e furti in appartamenti, la cronaca ha registrato un notevole incremento di furti "tecnologici" ed avanzati.
Insomma, il progresso applicato al furto ha generato trappole micidiali in grado di far mettere le mani a spregiudicati hacker direttamente nel proprio contocorrente.
Sono moltissime le trappole occorre, dunque, aprire gli occhi.
Di seguito pubblichiamo una dettagliatissima relazione dell'esperto informatico Alessandro Sigismondi che spiega cosa è il Carding (la clonazione della carta di credito) e come può avvenire.
Tutto ha inizio nel… 1730 quando Christopher Thomson mercante di mobili crea dei sistemi creditizi per dilazionare i pagamenti delle sue merci.
Non si cedono più immediatamente monete ma documenti sostitutivi che certifichino il credito.
Nel 1914 la società Western Union iniziò a fornire ai suoi clienti più importanti una carta di materiale metallico che poteva essere utilizzata per dilazionare i pagamenti dei suoi servizi. Nasce così la carta di credito.
Da allora di strada ne è stata fatta.
Il problema fondamentale allora è cercare di stare sempre un passo avanti rispetto ai nuovi ladri, dovere fondamentale delle forze dell'ordine.
Ma non sempre è possibile o è agevole scovare i malviventi.
Il furto molto spesso ha inizio con la sottrazione di dati essenziali che schiudono il fortino (il proprio conto corrente).

Come avviene tecnicamente il furto di dati?
«Quando vengono effettuati i pagamenti», spiega Sigismondi, «la carta viene "sniffata"attraverso il dispositivo e i dati sono inviati con bluetooth ad un ricevitore che può essere sia un palmare che un pc portatile da dove poi i dati vengono raccolti e inseguito le carte vengono clonate».
Esistono sul web degli "sniffer bluetooth", la nota società "Airmagnet" ha lanciato persino un tool free che riesce ad individuare se nelle vicinanze vi siano "device bluetooth".

Furti del genere ne sono stati perpetrati anche in Abruzzo che appare tra le regioni maggiormente a rischio.
«Finora le forze dello Stato», spiega ancora Sigismondi,«non sono riuscite a debellare il fenomeno, poichè per intercettare un individuo che sta prelevando codici da una transazione, si dovrebbe essere posizionati a circa metà distanza tra il pos (da cui avviene la transazione) e il pc (chi ruba i dati) utilizzando software free reperibile nel web è possibile vedere il passaggio».

06/12/2007 15.34