La truffa con il Bluetooth

Utilizzando la tecnologia del "Bluetooth" - un protocollo di comunicazione che consente di collegare tra loro senza fili apparecchiature digitali - è stata messa a punto una **nuova truffa** informatica.

Questa è la tecnica usata finora : i truffatori, forzando porte e finestre, accedono di notte in strutture commerciali come distributori di benzina e supermercati cercando di non lasciare traccia per non insospettire gli esercenti. Quindi **installano un microchip** all'interno del **Pos** (utilizzato dagli esercizi commerciali per i pagamenti con bancomat e carte di credito) e restano in attesa dell'apertura dei negozi, a poca distanza, con il pc portatile collegato attraverso Bluetooth alla trasmittente da loro inserita.

Il cliente che paga con bancomat o carta di credito, viene "**sniffato**" (come si dice in gergo informatico) ovvero i dati personali vengono istantaneamente acquisiti dal computer dei criminali. A questo punto con lo "skimmer" (l'apparecchio utilizzato per leggere e sovrascrivere la banda magnetica) inseriscono i dati acquisiti sulle carte vergini e iniziano a fare massicci acquisti.

17/11/2007