Economy
IL BUSINESS MAGAZINE DI MONDADORI

SE LA BENEFICENZA È UNA TRUFFA

CARTE DI CREDITO L'ultimo tentativo di frode telematica arriva dalla Gran Bretagna e passa attraverso le pagine del social network Facebook. Ecco come non cadere nella rete. di Andrea Telara

L'ultima minaccia arriva dalla Gran Bretagna e si chiama *parcelling*, cioè un sofisticato tentativo di truffa via carta di credito, mascherato come un'operazione di beneficenza. Le vittime vengono di solito arruolate via internet, attraverso le pagine del social network **Facebook** o con dei messaggi di posta elettronica. Gli italiani per ora non sono caduti nella rete dei *cybertruffatori* grazie al lavoro dei militari del Gat, il nucleo antifrodi telematiche della Guardia di finanza, che hanno sventato per tempo il pericolo, ma non è detto che non arrivi un secondo attacco. Ecco perché rimangono sempre all'erta.

La ragione è che il rischio di frodi telematiche, in particolare sulle carte di credito, è una minaccia quotidiana molto variegata (*vedere anche il riquadro in basso con i reati più diffusi*). La vicenda di Albert Gonzalez, il ventinovenne di Miami arrestato il 17 agosto scorso per aver frodato 130 milioni di tessere magnetiche, è senz'altro la più grave della storia. Ma non è un episodio isolato.

VIOLAZIONI IN CRESCITA DEL 10%. E anche nel nostro Paese i numeri sono in crescita: nel 2008, in Italia, sono state denunciate 1.340 truffe elettroniche, in aumento di oltre il 10% rispetto al 2007. Secondo il Gat, i dati del primo semestre 2009 sono in linea con quelli del 2008 e dimostrano inequivocabilmente che la carta di credito è uno strumento di pagamento non ancora affidabile per effettuare acquisti su internet.

Oggi è il settore del commercio elettronico, cioè l'ecommerce, il maggior responsabile delle truffe telematiche perché molti venditori online dispongono di sistemi di sicurezza vulnerabili. Per questo i pirati informatici hanno vita facile nel compiere rapine via computer.

Per difendersi occorre adottare pochi e semplici rimedi. Per fare acquisti in rete, per esempio, è bene utilizzare il più possibile le carte prepagate, che hanno un meccanismo di funzionamento simile al credito dei telefonini: il titolare deposita sulla carta un determinato importo di denaro, anche di poche decine o centinaia di euro, che poi può spendere gradualmente nel tempo e ricaricare come vuole, man mano che il credito si esaurisce. Così il rischio di sottrazioni indebite è limitato soltanto all'importo di denaro depositato.

In alternativa, ci sono dei servizi avanzati di alert via sms: per ogni acquisto effettuato con la carta di credito, il titolare riceve un messaggio sul telefonino. In caso di un addebito non riconosciuto, si contatta il numero verde della società che ha emesso la carta per bloccare l'operazione, presentando una denuncia contro ignoti alle forze dell'ordine.

CORBIS

TUTTE LE TECNICHE PER RUBARE IL DENARO ELETTRONICO

PHISHING
Il titolare della carta di credito riceve un messaggio email in cui gli si chiede di collegarsi al sito internet della banca e di fornire i codici della propria carta. In realtà si tratta di un «sito civetta» gestito da pirati informatici, che poi rubano i codici.

VISHING
Arriva un messaggio sms in cui si invita il titolare della carta a chiamare un numero verde della banca per riceve comunicazioni urgenti. In realtà, all'altro capo del telefono c'è il truffatore che cerca di carpire gli estremi della carta di credito.

SPYWARE
È un software maligno che si insinua sul computer del titolare di una carta di credito di solito durante la navigazione in internet o durante l'installazione di un altro software. Poi spia l'utente e invia a un server esterno i dati sensibili, come gli estremi della carta di credito.

SKIMMING
Tramite un apparecchio chiamato skimmer, i truffatori entrano in possesso dei dati della carta di credito contenuti sulla banda magnetica, li riportano su un computer e li trascrivono poi su altre carte di credito falsificate.

PARCELLING
Il truffatore contatta via email un certo numero di persone, chiedendo di partecipare a un'iniziativa di beneficenza. Si richiede di ospitare a casa propria della merce, che la finta organizzazione benefica provvederà poi a ritirare per destinarla ai bisognosi, per esempio degli orfanotrofi in Africa. In realtà, la merce è frutto di acquisiti con carte di credito clonate che portano il nome e l'indirizzo dell'ignaro ospitante che rischia così 8 anni di carcere per ricettazione.