30 luglio 2010 8:43

Furti di identità elettronica. Attenzione! Le vacanze estive favoriscono il fenomeno

di Deborah Bianchi*

Aerei da prenotare, caparre di soggiorni turistici da versare, macchine a noleggio da fissare per tempo. Come pagare? On line naturalmente. Attenzione pero' ai furti di identita'! L'identity theft o furto d'identità digitale è un crimine che si sta diffondendo in modo esponenziale in Italia e in tutto il mondo. L'Italia è al secondo posto in Europa per numero di frodi commesso attraverso l'uso di dati rubati.

Disciplina normativa

Il nostro ordinamento punisce questo crimine individuandolo nella disposizione normativa del **reato di sostituzione di persona**, disciplinato dall'art. 494 del Codice Penale, o nel più grave reato di **frode informatica** ex art 640 ter del Codice Penale.

Occorre poi tenere presente la previsione di cui al d.lgs. 196/03, **codice in materia di protezione dati personali**, che all'art. 169 prevede un illecito penale nel caso di omissione **nell'adozione delle misure di sicurezza** o, nel caso, della successiva mancata regolarizzazione delle stesse.

Le varie tecniche di furto

Dall'aprile 2006 viene pubblicato il rapporto ABI CIPA CNIPA sul furto di identità elettronica tramite internet con l'obbiettivo di analizzare le varie modalità di perfezione dell'illecito al fine di individuare tecniche di prevenzione. Di solito quando si vuole compiere un furto di identità si attaccano, tramite software eseguito da remoto, infrastrutture informatiche delle banche, del cliente o della rete telematica che li connette, allo scopo di carpire le credenziali digitali dell'utente dei servizi on-line. I metodi più usati sono i seguenti.

Social engineering

Si sfrutta la buona fede del destinatario della mail spia per fare in modo che l'utente dia spontaneamente le proprie credenziali elettroniche. E' una tecnica fondata sull'elemento psicologico.

Phishing

E' una forma particolare di *social engineering*, che consiste nella creazione e nell'uso di *e-mail* e siti web ideati in modo da ingenerare confusione con quelli di istituzioni finanziarie e/o governative, con lo scopo di raggirare gli utenti e carpire loro informazioni personali (*account* e *password*) per accedere a servizi di *home banking* o al proprio numero di carta di credito. Queste informazioni vengono catturate dal *phishers per poi essere* riutilizzate per frodi finanziarie e/o furti di identità.

Virus, worm, trojan horse, mass mailing, mixed mmc (malicious mobile code)

Si tratta di diffondere dei particolari virus nel computer del malcapitato tramite auto installazione fraudolenta atta a esportare dati e a prendere il controllo del sistema operativo del pc. Tra questi virus possiamo ricordare i seguenti.

Spyware: programmi spia che raccolgono informazioni dal pc infettato e le inviano al destinatario fraudolento;

Key-logging: programmi che si attivano quando l'utente si connette al sito di una banca o instaura una connessione protetta e carpiscono le credenziali informatiche quando l'utente li digita sulla tastiera.

Redirector: codice malevolo scritto in modo da reindirizzare il traffico Internet del computer infetto verso indirizzi IP differenti da quelli che si intendevano raggiungere;

Screen grabbing: programmi simili al *key-logger* che eseguono foto istantanee dello schermo dell'utente in modo che quando egli scrive le informazioni sensibili sui siti di *homebanking* queste vengono dirottate al criminale.

Spoofing

E' una tecnica complementare a quelle finora analizzate che consiste nel falsificare l'origine della connessione in modo da far credere all'utente di essere un soggetto diverso da quello reale. Per esempio l'utente crede di connettersi a un sito di una banca e invece viene reindirizzato al server del malvivente.

Connection hijacking

Si realizza mediante l'intercettazione di flussi di dati in transito; l'intruso, dopo averne analizzato il flusso, si inserisce nella transazione alterandone il contenuto e opera con le credenziali di chi legittimamente aveva iniziato la sessione.

Sniffing

Consiste in un'operazione di intercettazione delle comunicazioni mediante cattura di dati (password, posta elettronica, ecc.); questi strumenti di intercettazione sono gli **sniffers** sono, in sostanza, hardware, software, analizzatori legali in grado di intercettare, selezionare per protocollo, tradurre, visualizzare e memorizzare tutti i tipi di pacchetti in transito sulla rete.

Come proteggersi

Nonostante che le previsioni sulle misure di sicurezza obbligatorie del Codice Privacy tentino di arginare queste tecniche invasive è sempre e solo l'utente che deve stare in guardia e diffidare dalle mail strane.

Molte per esempio arrivano con testi non ortograficamente perfetti perché frutto di traduzioni automatiche.

Altre invitano a cliccare su dei link e sono accuratamente da cestinare.

Altre ancora contengono allegati che non devono assolutamente essere aperti.

Le mail che sembra possano arrivare dalla propria banca o dalle poste sono sempre inverosimili in quanto la banca o le poste se intrattengiamo rapporti con loro comunicano sui loro canali dedicati che sono le aree riservate di cui ci hanno fornito le credenziali.

Nel caso vi sia invece un furto di credenziali mentre ci colleghiamo al sito della banca allora occorre verificare il proprio conto on line ogni giorno in modo da denunciare subito la perdita e bloccare le credenziali e il conto.

***Deborah Bianchi,** avvocato specializzato in diritto applicato alle nuove tecnologie, esercita nel Foro di Pistoia e Firenze in materia civile e amministrativa*
avv.deborahgiribaldibianchi.it