



## Scontrini: i rischi per chi li abbandona per strada

**Autore :** Alessandro Curioni

**Data:** 20/02/2017

*Una gesto distratto, come buttare via una ricevuta può mettere a rischio la nostra privacy.*

Tutti i piccoli foglietti di carta dei quali periodicamente ci liberiamo contengono, in quantità diverse, dati personali che ci riguardano. Per questa ragione la “pulizia” di borse e portafogli richiede l'accortezza di un'attenta **distruzione di scontrini e ricevute** che, se abbandonati integri al loro destino, potrebbe permettere a chiunque di scoprire molto più di quanto probabilmente vorremmo fare sapere a un estraneo.

Da molti anni si parla dei rischi di **clonazione di carte di credito e bancomat** recuperando i dati presenti sulle ricevute delle operazioni effettuate. Per quanto gli operatori finanziari abbiano progressivamente limitato la quantità di informazioni, i codici presenti permettono facilmente di scoprire i seguenti dati: la vostra **banca**, il **tipo di carta** di cui siete in possesso e almeno una parte dei **numeri della carta stessa**.

### Scontrini di farmacia

Immaginiamo che oltre a una ricevuta di un pagamento con carta vi liberiate anche di uno **scontrino parlante** rilasciato da una **farmacia**. In primo luogo potrebbe contenere il nostro codice fiscale: per sua natura è un dato identificativo, in molti casi



utilizzato nelle procedure di recupero password e utenze di siti di commercio elettronico e di gestione delle carte di credito. Esistono dei software on line che consentono di ricavare dal codice fiscale i dati utilizzati per comporlo (nome, cognome, data e luogo di nascita). Così sarà facilissimo risalire dal codice che identifica il farmaco a quanto vi è stato prescritto. Sul sito **Federfarma** è disponibile un servizio attraverso il quale, imputando il codice prodotto, fornisce il nome, il principio attivo, il produttore e se richiede la ricetta per la prescrizione.

## Scontrini di ricariche telefoniche e supermercati

Un'altra ricevuta che potrebbe essere cestinata è quella di una vecchia **ricarica telefonica** sulla quale, ovviamente comparirà il vostro numero di cellulare.

Alla lista potremmo aggiungere anche quella del **supermercato** che, se avete pagato con carta di credito, aggiungerà altri dati finanziari, oltre a quelli del bancomat e, nel caso possediate una **carta fedeltà**, renderà noti anche quelli. In questo modo avete fornito un piccolo tesoro ai truffatori che così hanno abbastanza strumenti per mettere in atto la versione moderna delle truffe telefoniche che oggi sono chiamate **vishing** (contrazione dell'espressione voice phishing).

## Il vishing: la nuova truffa sulla carta di credito

Con i dati in suo possesso, il delinquente potrebbe telefonarvi al vostro numero di cellulare spacciandosi per un operatore della società emittitrice della vostra **carta di credito**. Potrebbe annunciarvi che risultano delle attività anomale che hanno portato al **blocco provvisorio della carta di credito**. Ma prima di fornirvi i dettagli deve verificare la vostra identità, quindi vi chiede di confermare una serie di dati. Vi dice il vostro nome, cognome, luogo e data di nascita, codice fiscale, le prime sei e le ultime quattro cifre della carta di credito (tutti dati estratti dagli scontrini), oltre alla data di scadenza. Chiede a voi di completare il numero della carta e di fornirgli quello del codice di controllo che si trova su retro. Se esitate aggiunge qualche dettaglio su vostri acquisti (sempre quelli degli scontrini di cui è in possesso). A questo punto potrebbe essere molto difficile dubitare del vostro interlocutore. Certo potreste ricordarvi di avere buttato in un cestino delle ricevute, ma non è detto, di conseguenza è preferibile non avere dubbi e distruggere con cura i "foglietti chiacchieroni".