Consigli per chi naviga in Internet

- **Installare** un **antivirus** e **sistemi di sicurezza**.
- **Aggiornare** regolarmente il **sistema operativo** installando le *patch* (aggiornamenti per eliminazione di errori) rilasciate periodicamente dal produttore.
- Non cliccare su ***link*** che non siano **sicuri**.
- Prestare **attenzione all'indirizzo** del sito che si visita (è possibile essere condotti a siti fittizi).
- **Aggiungere tra i preferiti gli indirizzi utilizzati frequentemente**, per evitare di commettere errori e garantirsi di essere sempre nella giusta home page.
- Accedendo a ***blog*** e ***social network*** servirsi di ***username*** che **non contengano dati personali** (ad esempio "Giovanni Roma", "Lucia Firenze", ecc.), ed evitare di pubblicare informazioni riservate.

Social network

- Selezionare i propri **contatti**.
- Rendere accessibili **foto** e **dati personali** solo a **contatti fidati**.
- Aprire un ***account e-mail*** **separato**, che non contenga il proprio vero nome, da utilizzare per inviare e ricevere comunicazioni dai siti web.
- Utilizzare ***password*** **sicure e complesse**.

A chi rivolgersi

Per saperne di più consultare il sito: www.furtoidentita.com

Se si è caduti vittime di un furto d'identità, **bloccare immediatamente i propri conti** e rivolgersi all'**Adiconsum**.

MEMO

www.adiconsum.it

Un click e sei in Adiconsum!

- Per **iscriverti** e **abbonarti**
- Per conoscere i **recapiti** delle sedi
- Per l'**informazione**, i **servizi**, l'**attività** dell'associazione

Iscriversi all'Adiconsum conviene:

- Per l'**aggiornamento sui tuoi diritti**
- Per l'**assistenza** nei 300 sportelli territoriali
- Per la **consulenza online** (servizionline@adiconsum.it)

5 x mille? All'Adiconsum.

Codice fiscale: 96107650580

ADICONSUM
associazione difesa consumatori e ambiente

Furto d'identità

Okkio a...

Test noi consumatori · Periodico settimanale di informazione e studi su consumi, servizi, ambiente · Anno XXI · Supplemento al n. 12 · 6 marzo 2009
Sped. in abb. post. D.L. 353/2003 (conv. in L.46/2004) art.1, comma 2 · DCV Roma

...La prevenzione del furto d'identità

Cos'è il "furto d'identità?
Come avviene? Come prevenirlo?

Adiconsum,
dalla parte del consumatore.

Cos'è il "furto di identità"?

Si ha un **furto di identità** quando un'informazione individuale, relativa ad una persona fisica o ad un'azienda è ottenuta in modo fraudolento da un criminale con l'intento di assumerne l'identità per compiere atti illeciti.

Come avviene?

Ecco **alcuni dei modi più comuni** attraverso cui i criminali recuperano le informazioni necessarie per il furto di identità:

- **Bin-raiding**. Vecchie bollette, estratti conto e persino lettere personali e le buste in cui sono contenute, forniscono informazioni preziose che possono essere raccolte semplicemente rovistando nell'immondizia.
- **Cambiamento di indirizzo**. I truffatori possono ricevere un'ingente quantità di informazioni se, a seguito di un cambio di residenza, ci si dimentica di comunicare la variazione di indirizzo alle poste, alla banca, ecc.
- **Contatti indesiderati**. I truffatori spesso contattano la vittima dichiarandosi incaricati di una banca e chiedendo di aggiornare i dati personali. Altre volte si presentano come ricercatori di mercato e richiedono informazioni personali.
- **Furto o smarrimento del portafoglio**. I portafogli contengono bancomat, carte di credito, documenti di identità, tessere personali, ecc.
- **Skimming**. Consiste generalmente nella clonazione di una carta di credito attraverso l'apparecchiatura elettronica utilizzata negli esercizi commerciali per pagare i beni acquistati. I dati che vengono raccolti, vengono poi trasmessi a organizzazioni criminali.
- **Furto dell'identità di un deceduto**. Alcuni malviventi svolgono attività criminali utilizzando l'identità di persone decedute, ottenendo informazioni attraverso necrologi e pubblicazioni funebri.
- **Cellulare**. Mediante l'invio di messaggi, con il falso pretesto della notifica di una vincita o altro, la vittima viene indotta a prendere contatti (link, numeri da chiamare, ecc.) che hanno come scopo ultimo l'estorsione di dati personali.
- **Phishing**: questo termine identifica il furto via posta elettronica. Il malvivente invia un'e-mail dichiarando di essere un incaricato di una banca o di una compagnia di carte di credito o di appartenere ad altre organizzazioni con cui si possono avere rapporti, inducendo a fornire informazioni personali con le più svariate motivazioni.
- **Web**. A tutti coloro che usano internet viene chiesto regolarmente di fornire informazioni personali per poter accedere a determinati siti o per poter acquistare beni e servizi. Spesso queste informazioni viaggiano sulla rete in chiaro e non in modalità protetta. Un crescente numero di utenti, inoltre, sta fornendo un'elevata quantità di dati personali a *blog*, siti *chat*, *social networks* come *MySpace* e *Facebook*.

Come difendersi?

- Fare attenzione quando si ricevono **inaspettate richieste di informazioni** personali da chi si qualifica come incaricato della banca, della polizia o di qualsiasi altra organizzazione. È sempre consigliabile non rispondere subito, ma recarsi di persona nella sede dell'organizzazione stessa, per essere certi di non cadere nelle mani dei criminali.
- Non perdere mai di vista **carte di credito e bancomat**. Se si richiede una nuova carta ed essa non arriva in tempi ragionevoli, avvertire l'emittente. Quando la si riceve, è bene firmarla con inchiostro indelebile e attivarla immediatamente. Tenerla costantemente sotto controllo durante i pagamenti. In caso di smarrimento contattare subito il servizio clienti.
- Se una **bolletta** non arriva, contattare immediatamente la società di servizio. Se la bolletta mancante risulta regolarmente spedita, potrebbe essere stata intercettata da un truffatore per ricavarne dati personali.
- Prima di gettarli nella spazzatura, distruggere i **documenti contenenti dati personali**. È consigliabile anche gettare i pezzetti di carta in contenitori diversi o in giorni diversi.
- È importante controllare periodicamente la propria **situazione creditizia** per assicurarsi che non vi siano posizioni aperte illegalmente a proprio nome.
- Conservare al sicuro tutto ciò che contiene **dati personali** (passaporto, patente, bollette, estratti conto, ecc.). Limitare inoltre il numero di documenti da portare con sé ed evitare di lasciarli in auto).
- Quando viene richiesta la **copia di un documento**, insistere oer comunicarne soltanto gli estremi.
- Assicurarsi che la propria **posta** sia al sicuro finché non la si ritiri, scegliendo una cassetta adeguata. Per spedire documenti che contengono informazioni personali, chiedere consiglio all'ufficio postale.
- In caso di **trasferimento**, comunicare al più presto la variazione alla banca, al fornitore della carta di credito e a tutte le organizzazioni con cui si intrattengono rapporti. È consigliabile anche chiedere alle poste di attivare un servizio di inoltro. Se si ha intenzione di stare fuori casa per un lungo periodo di tempo, si può chiedere di usufruire di servizi di affidamento della propria corrispondenza all'ente postale fino al proprio ritorno.

- Prima di firmare una **ricevuta di una carta di credito** controllarla attentamente: se compaiono tutte le informazioni della carta stessa (numero, scadenza, ecc.), cancellare qualche cifra. Se l'esercente non lo consente è meglio cambiare negozio.
- Quando si **opera con il bancomat**, osservare lo sportello e fare attenzione ad eventuali anomalie, alla presenza di qualcosa di diverso dal solito (ad es. una tasca laterale che prima non c'era contenente avvisi pubblicitari; un filo che esce o una sporgenza dalla fessura in cui si inserisce la carta, ecc.). Inoltre, mentre si digita il pin, coprire la tastiera con l'altra mano.