APPROFONDIMENTO
Generazioni Connesse
SAFER INTERNET CENTRE

IL FURTO D'IDENTITÀ

Il furto di identità è un reato penale, sanzionato anzitutto dall'articolo 494 del c.p. "*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, induce taluno in errore, sostituendo la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno*".
Anche il **Codice della privacy** (D.L.vo 196/2003) tutela l'identità personale.

Internet e in particolare i social network, anche utilizzati tramite smartphone, sono sempre più il terreno di queste truffe, in quanto favoriscono la circolazione poco protetta dei nostri dati personali . Vediamo i casi più frequenti:

- **Phishing**: utilizzo della posta elettronica per carpire dati di accesso con e-mail, falsamente provenienti da Istituzioni pubbliche (Agenzia delle entrate, ad esempio), Istituti di credito, Poste italiane, grandi aziende di servizi elettrici o telefonici con motivazioni accattivanti o minacciose (riscossione di premi, sblocco del conto corrente o della carta di credito, ripristino password etc).
- **Creare un account di posta elettronica** intestato ad un'altra persona, allo scopo di instaurare rapporti con altri utenti della Rete inducendoli, quindi, in errore sulla reale identità del mittente.
- **Creare un account di Facebook o altro social network (Impersonation)** a nome di un'altra persona ed utilizzarlo a suo danno, ovvero con lo scopo di attribuirle azioni e dichiarazioni, pubblicare sue immagini compromettenti o imbarazzanti o altro.
- **Skimming**: clonazione della carta di credito effettuata durante l'operazione di prelievo o di pagamento presso sportelli automatici e terminali POS.
- **Bin raiding**: recuperare informazioni fiscali, estratti conto, bollette o qualsiasi altra documentazione altrui, riportante informazioni personali, per farne uso illecito.
- **Attivazione di SIM per telefonia e connessione Internet intestate ad altre persone**: viene realizzata presentando dati reali di una persona (sottratti o intercettati con varie modalità) e documenti di identità falsificati. Il rischio è duplice, ovvero che siano addebitati all'ignara vittima i costi per traffico e abbonamenti goduti dai ladri di identità, o peggio che le siano imputate responsabilità per le eventuali attività illecite svolte utilizzando quelle sim (traffico di droga, terrorismo, rapine ed altro).
- **Apertura di credito, acquisti a rate o richiesta di prestiti presso banche e finanziarie, a nome della vittima, in modo da farle addebitare la restituzione**. La persona che subisce il furto di identità si vedrà recapitare bollettini o richieste di pagamento, o peggio atti giudiziari come decreti ingiuntivi, ai quali dovrà opporsi dimostrando di non aver mai acquistato i beni o richiesto i prestiti.

FURTO D'IDENTITÀ

Il furto di immagini e video

Anche l'immagine di una persona (o il logo di una impresa, di una associazione) deve essere considerata sicuramente "dato personale" e il titolare del trattamento dei dati ha l'obbligo di garantire all'interessato la possibilità di esercitare in qualsiasi momento i diritti di **aggiornamento, rettifica, integrazione o cancellazione dell'immagine/video. Pertanto non è lecito utilizzare le immagini altrui senza autorizzazione scritta.**

<u>Cosa fare se si sospetta di essere stati vittima di un furto di identità?</u>

- **Innanzitutto bloccare le carte di credito, i conti correnti o le SIM interessati dall'uso fraudolento,** telefonando ai gestori. Attenzione a conservare il codice della segnalazione fatta, che viene comunicato alla fine della telefonata**.**
- **In caso di prestiti ed acquisti rateali, disconoscere il contratto tramite lettera raccomandata A/R e non pagare quanto richiesto.**
- **Dare seguito** al disconoscimento con regolare **denuncia presentata presso le autorità di Pubblica Sicurezza** (da fare sempre, anche in via cautelativa contro eventuali usi illeciti dell'identità rubata non ancora noti)
- **Modificare le password di tutti gli account online,** a partire da quelli correlati a informazioni o istituti finanziari.
- **Se il furto di identità si realizza tramite un sito web o social media**, contattare immediatamente il relativo servizio di sicurezza o di assistenza per disconoscere l'account e per chiederne il blocco.

Cosa fare in caso di sottrazione e pubblicazione di foto/video

- Inoltrare una formale richiesta al sito in questione (anche a mezzo fax e/o posta elettronica) per ottenere la cancellazione, ai sensi del Codice della privacy. Se non la si ottiene, occorre rivolgersi al Garante della protezione dei dati personali mediante ricorso.
- Sotto il profilo penale, presentare denuncia presso il più vicino ufficio di Polizia.

Cosa fare in caso di furto di profili social (Facebook, Instagram,Twitter, Linkedin etc.) o dell'account di posta elettronica

- **Fare una denuncia ad un ufficio di Polizia**, per accesso telematico abusivo e sostituzione di persona.
- **Chiedere la rimozione del falso profilo** segnalandolo direttamente al centro assistenza del social.