ABI Associazione Bancaria Italiana

IL FURTO DI IDENTITÀ

Un vademecum per saperne di più

CERTFin

OSSIF

Polizia di Stato

Le banche sono impegnate quotidianamente nel garantire la massima sicurezza per la clientela, anche riguardo ai tentativi di **frodi identitarie**, che prevedono l'**utilizzo illecito di dati identificativi e/o reddituali** della vittima.
Allo stesso tempo, è importante che la clientela collabori con la banca, mantenendo sempre alto il livello di attenzione alla protezione dei propri dati personali.

Cosa si intende per furto di identità?

Il furto d'identità consiste nell'appropriazione indebita dei dati di una terza persona allo scopo di sostituirsi ad essa. Può essere commesso in maniera totale o parziale:

- ***impersonificazione totale***: il furto di identità è commesso mediante la sottrazione di tutti i dati personali della vittima, sia quelli identificativi sia quelli reddituali. Questa tipologia può riguardare anche persone non più in vita.

- ***impersonificazione parziale:*** il furto di identità è commesso mediante l'utilizzo illecito dei dati identificativi o reddituali di un soggetto terzo (es. combinare la propria identità con la busta paga altrui per ottenere un finanziamento).

Perché rubare un'identità?

Un malvivente può rubare l'identità altrui per molteplici motivi che si possono riassumere in ragioni di natura personale[1] e motivazioni di tipo economico o per entrambi gli aspetti.

Come avviene il furto di identità?

Le tecniche utilizzate dai malviventi sono numerose. Per comodità, possiamo dividerle in due macrocategorie:

1. Le tecniche tradizionali consistono nel furto dei dati mediante la sottrazione fisica di documentazione cartacea (es. documenti smarriti o rubati, estratti conto, estremi delle utenze domestiche, richiesta illecita di informazioni).

2. Le tecniche informatiche (minacce) mirano ad acquisire digitalmente i dati della vittima. Le minacce utilizzate sono sempre più sofisticate e sono veicolate attraverso i canali Internet e di telefonia mobile.

1. In questa tipologia rientrano, ad esempio, motivazioni legate a ragioni razziali, stalking, bullismo.

Un tema molto caldo è anche quello del furto dell'Identità Digitale… Che cosa è?

L'identità digitale è l'insieme dei dati e delle informazioni che, all'interno di un determinato sistema informatico, definiscono una persona fisica.
Si tratta quindi della rappresentazione virtuale dell'identità reale che consente l'interazione elettronica con altri individui o sistemi informatici. Inoltre, l'identità digitale permette di accedere anche ai sistemi informativi e può essere utilizzata per la sottoscrizione di documenti digitali. Con l'identità digitale, è possibile stabilire che una data persona in un preciso momento ha avuto accesso a un sistema informatico e sta compiendo delle determinate azioni. L'accesso al sistema informatico avviene tramite delle credenziali che identificano univocamente la persona e di cui soltanto il soggetto dovrebbe essere in possesso.

Quali sono le conseguenze del furto di identità?

Le conseguenze del furto di identità possono essere per l'utente molto gravi dal punto di vista del rischio di coinvolgimento dei propri dati in attività illecite, sotto l'aspetto reputazionale nonché sotto quello finanziario.

Cosa dice la legge riguardo al furto di identità?

Manca una regolamentazione specifica del furto di identità. Frequentemente la fattispecie del furto d'identità si riconduce ad altre tipologie di reati, quali: diffamazione (art. 595 c.p.), falsità materiale in scrittura privata (art. 485 c.p.) o sostituzione di persona (art. 494 c.p.).

1 COME PROTEGGERE LA NOSTRA IDENTITÀ MEDIANTE SEMPLICI ACCORGIMENTI

1. In caso di **smarrimento o furto di documenti personali**, recarsi immediatamente dalle **Autorità di polizia** preposte per sporgere denuncia. In caso di **furto o smarrimento di carte di credito e/o di debito**, dopo averne ordinato il blocco chiamando il numero messo a disposizione, **la denuncia va comunicata anche alla propria banca.**

2. **Fare molta attenzione nello smaltimento della documentazione cartacea che contiene informazioni personali** (es. estratti conto, utenze domestiche): è opportuno rendere illeggibili i dati sensibili riportati nei documenti prima di cestinarli.

3. **Proteggere con cura le credenziali di accesso ai conti online e i codici delle carte di credito e/o di debito e tutti gli altri codici di accesso (es. lo SPID);** se si sceglie di salvare questi dati sui propri dispositivi (es. computer e/o cellulare) assicurarsi che siano adeguatamente protetti (es. cifrati). Allo stesso modo occorre tenere sempre attentamente custodite le credenziali e i codici utili a disporre della propria firma digitale.

4. **Salvaguardare le proprie carte di pagamento dotate di tecnologia cd. "contactless"** (ovvero quelle per cui non è richiesto l'inserimento nel POS per effettuare la transazione), **con custodie schermate** (rivestite in alluminio) per ridurre al minimo la possibilità di essere vittime di truffe che prevedano la lettura del chip [es. con comunicazione RFID (identificazione con la radiofrequenza) e NFC (identificazione attraverso comunicazione di prossimità)].

Occorre comunque ricordare che ci sono delle regole che limitano i rischi:
- il PIN è sempre richiesto per le operazioni al POS sopra i 50 euro;
- dopo 5 pagamenti consecutivi al POS senza digitare il PIN, il successivo, anche se di piccolo importo, necessita dell'autenticazione forte del cliente (c.d. SCA) e cioè dell'inserimento del codice segreto/PIN;
- analogamente se l'ammontare dei pagamenti disposti al POS "senza contatto" a partire dalla data dell'ultima applicazione della SCA supera complessivamente i 150 euro occorre inserire il codice segreto/PIN.

5. **Cambiare frequentemente le credenziali di accesso (le password) per entrare nei conti online ed evitare di utilizzare password che potrebbero essere facilmente individuate dai frodatori** (es. la data di nascita). In generale, una password, per avere un livello di sicurezza considerato adeguatamente tutelante, deve essere caratterizzata da lettere maiuscole e minuscole, numeri e caratteri speciali (es. come !, ?, %, $).

6. È importante imparare a riconoscere i messaggi autentici dai messaggi fraudolenti. **Le banche:**

- **non chiedono mai**, né tramite posta elettronica, né telefonicamente, né con messaggi sms, **le credenziali di accesso al conto e i codici delle carte del cliente.** Qualora si ricevano richieste di questo tipo, avvisare la propria banca per avere conferma della sua estraneità all'invio ed evitare di dare alcun riscontro alla richiesta ricevuta;

- **non inviano mai e-mail contenenti link se non nell'ambito di un processo avviato dall'utente** (es. modifica e-mail personale, aggiornamento documento di riconoscimento). Qualora il cliente ricevesse un messaggio con link dalla banca senza preventiva richiesta da parte sua, occorre avvisare la propria banca per avere conferma della sua estraneità all'invio ed evitare di dare alcun riscontro alla comunicazione ricevuta.

7. **Ogni volta che si usa un computer pubblico per accedere al proprio conto online, occorre poi ricordarsi di chiudere la sessione (logout)**. Inoltre, è sempre preferibile digitare personalmente l'indirizzo online della propria banca e non cliccare su indirizzi già memorizzati. Se la connessione è pubblica, è maggiore il rischio che possibili malintenzionati sfruttino la connessione precedentemente aperta per carpire informazioni.

8. **I messaggi fraudolenti contengono spesso link malevoli** (attraverso cui il computer e/o cellulare vengono violati) o collegamenti per reindirizzare l'utente su siti clone (utilizzati per carpire informazioni personali). Per questo motivo, **è fondamentale non cliccare mai su questi link** [2].

9. **Diffidare da presunti operatori che contattano le potenziali vittime affermando di aver bisogno di informazioni personali, bancarie o di credito,** per verificare l'identità o per sapere dove inviare pacchi, denaro, vincite fasulle o documenti legati alla giustizia.

2. Questa modalità di truffa viene identificata con il termine "adescamento" ("phishing") ed è realizzata tramite canali web, ingannando gli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli apparentemente provenienti da soggetti qualificati, utilizzati correntemente dagli utenti (banche o società emittenti di carte di credito) e da siti web che richiedono l'accesso previa registrazione (web-mail, e-commerce ecc.). Il messaggio invita, riferendo problemi di registrazione, consegna o di altra natura, a fornire i propri dati riservati di accesso al servizio.

10. **Nel caso il proprio cellulare non sia più in grado di effettuare/ricevere chiamate, verificarne i motivi contattando il proprio operatore telefonico:** si potrebbe essere vittima di una frode effettuata tramite scambio della tua scheda telefonica (ovvero una truffa denominata Sim Swap[3]).

11. **Utilizzare con attenzione e prudenza i canali social** e soprattutto non comunicare e non condividere mai attraverso questi canali dati personali o finanziari.

12. **Scegliere un programma antivirus e mantenerlo sempre aggiornato**, installare regolarmente gli aggiornamenti del sistema operativo utilizzato in modo da proteggere tutte le apparecchiature e i dispositivi in uso da infezioni da malware.

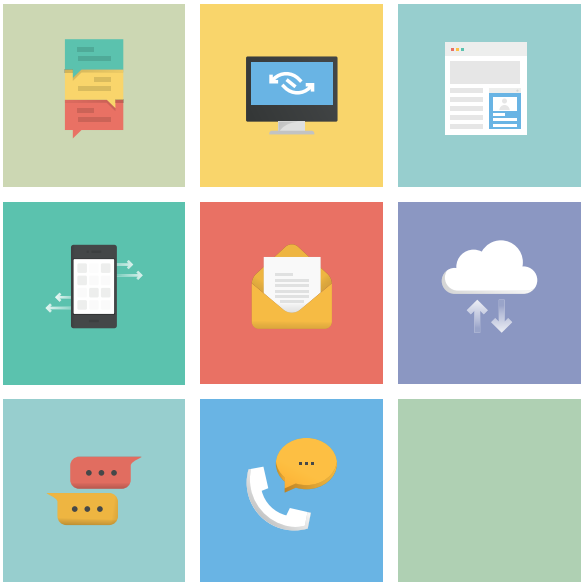
3. I truffatori riescono con raggiri a spostare il numero della vittima su una nuova scheda SIM controllata da loro. Sulla nuova sim, intercettano gli sms inviati dalla banca del malcapitato e li utilizzano per operare sul suo conto bancario.

2 COSA FARE IN CASO DI FURTO DI IDENTITÀ

Non appena ci si accorge di essere stati vittime di un furto di identità, qualsiasi sia il contesto in cui ciò possa essere avvenuto e a prescindere dai dati sottratti (es. furto dati biometrici, dati sensibili, dati sanitari, …), è importante **sporgere subito denuncia alle Forze di Polizia,** raccogliendo e fornendo tempestivamente quante più informazioni possibile, ricostruendo i fatti a supporto della denuncia [es. dati, modalità e tempi dell'avvenuta (errata) identificazione, documentazione inerente ai falsi contratti stipulati a proprio nome]. Ciò sarà utile, più in generale, anche per dimostrare quanto accaduto in tutte le altre sedi opportune.

In caso di pratiche di finanziamento portate a termine da sconosciuti, è utile raccogliere con particolare scrupolo sia le evidenze relative alle modalità con cui i criminali hanno assolto ai requisiti richiesti dalla finanziaria (es. hanno prodotto copia della busta paga), sia quelle che forniscano dettagli su come il finanziamento è stato erogato (sia in caso di assegno circolare sia in caso di bonifico, è possibile che i criminali abbiano aperto un conto corrente a nome della vittima, ovviamente a sua insaputa).

Nel caso in cui vi accorgiate che qualcuno ha concluso un contratto a vostro nome contestatelo il prima possibile. La collaborazione tra banca e cliente è fondamentale al fine di individuare situazioni che rientrano nel furto di identità. La tempestività ha anche un valore sociale, in quanto può consentire di bloccare ulteriori attività criminali a danno di altre persone.



3

ALCUNI ASPETTI SPECIFICI RELATIVI AL RIMBORSO DI OPERAZIONI DI PAGAMENTO NON AUTORIZZATE

È possibile che, nonostante il rispetto di tutte le buone prassi sopra ricordate, un furto di identità porti all'effettuazione di operazioni di pagamento elettronico non autorizzate a danno della vittima del furto di identità. In questo caso, **il cliente in buona fede viene sempre tutelato.**

- La normativa prevede, infatti, tempi e modalità per disconoscere pagamenti non autorizzati. In particolare, per il cliente che si è comportato con attenzione, seguendo le regole del proprio contratto relativo al conto o allo strumento di pagamento, è possibile ottenere il rimborso di operazioni non autorizzate, ad esempio a causa dello smarrimento o del furto di strumenti di pagamento, entro il giorno lavorativo successivo alla notifica, con una franchigia massima (cioè l'importo a carico dell'utente) pari a 50 euro.

- La contestazione dell'operazione deve essere effettuata prima possibile, e comunque entro 13 mesi dalla data del pagamento, secondo quanto indicato dal contratto con la banca. Anche se sono concessi 13 mesi di tempo per chiedere il rimborso, il cliente deve avvisare del furto, smarrimento o dell'operazione non autorizzata non appena ne viene a conoscenza.

4

IL FURTO DI IDENTITÀ: UN'IMPORTANTE INIZIATIVA DI PREVENZIONE

È bene sapere che tra i principali strumenti di prevenzione è operativo il Sistema **"SCIPAFI"**. In cosa consiste?

È il **Sistema Pubblico di prevenzione delle frodi**, con specifico riferimento al furto di identità. Si tratta di un s**uper archivio informatico nel quale confluiscono i dati contenuti nei database delle pubbliche amministrazioni** (per ora Ministero dell'Interno, dell'Agenzia delle Entrate, del Ministero dei Trasporti, dell'INPS e dell'INAIL), al quale le banche e altri soggetti accedono per verificare l'autenticità della documentazione della clientela prima di attivare un servizio finanziario. Il collegamento con ulteriori banche dati pubbliche e private è attualmente in fase di evoluzione. La consultazione dell'Archivio è prevista per l'attivazione di tutte le tipologie di servizi finanziari (decreto Legislativo 13 agosto 2010 n 141 e successive modifiche).

Pubblicata ad aprile 2022

ABI Associazione Bancaria Italiana

CERTFin

OSSIF

Polizia di Stato

In collaborazione con:

ACU Associazione Consumatori Utenti Organizzazione senza scopo di lucro

ADICONSUM Associazione Difesa Consumatori e Ambiente promossa dalla CISL

Adoc

ASSO-CONSUM

ASSOUTENTI

Casa del Consumatore

CITTADINANZATTIVA

Verbraucherzentrale Südtirol Centro Tutela Consumatori Utenti

CODACONS

CONFCONSUMATORI CONFEDERAZIONE GENERALE DEI CONSUMATORI

Federconsumatori

LEGA CONSUMATORI

Ente Terzo Settore MOVIMENTO DIFESA del Cittadino 35° 1967-2012

MOVIMENTO CONSUMATORI

U.Di.Con. UNIONE per la DIFESA dei CONSUMATORI

60° UNC 1955 | 2015