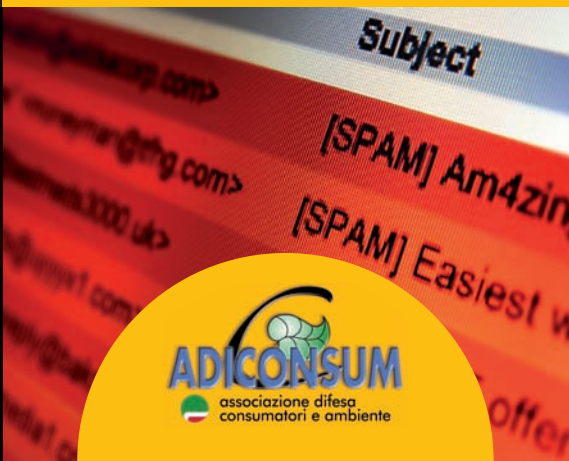
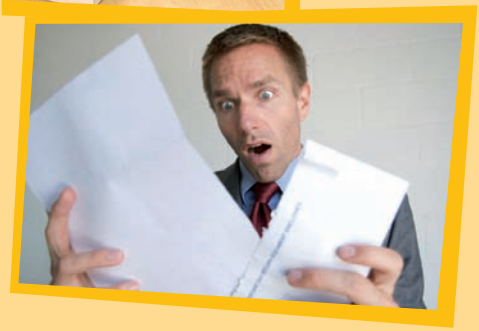
DIFENDI LA TUA IDENTITÀ

Guida pratica alla prevenzione del furto d'identità.



ADICONSUM
associazione difesa consumatori e ambiente

SOMMARIO



PREMESSA pag. 1

COSA È IL FURTO DI IDENTITÀ? pag. 2

COME PUÒ ESSERE RUBATA LA VOSTRA IDENTITÀ? pag. 3

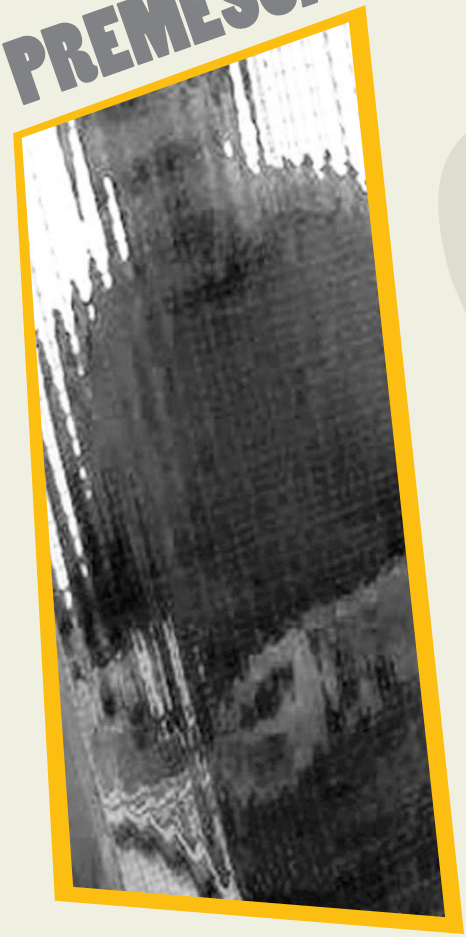
COSA PUÒ ESSERE FATTO CON LA VOSTRA IDENTITÀ pag. 4

COME PREVENIRE LE FRODI D'IDENTITÀ: SUGGERIMENTI UTILI pag. 5

SEMPLICI PASSI PER PROTEGGERE LA VOSTRA AZIENDA pag. 8

COSA FARE QUANDO SI DIVENTA UNA VITTIMA pag. 9

PREMESSA



Questa guida pratica realizzata per il secondo anno da **Adiconsum** *in collaborazione con* **Fellowes Leonardi** *vi sarà utile per comprendere cos'è il furto di identità, come può essere perpetrato e quali tipi di frodi possono essere commesse usando il vostro nome. Inoltre, contiene dei semplici suggerimenti su come proteggere voi stessi e il vostro business e sulle azioni da intraprendere nel caso in cui le informazioni personali o della vostra azienda vengano utilizzate in modo fraudolento.*

COSA È IL FURTO DI IDENTITÀ?

Si ha un furto di identità ogni qualvolta **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.** Tali comportamenti sono da annoverare giuridicamente sotto il nome di "frode". La frode di identità comprende reati quali l'apertura di conti correnti bancari, la richiesta di una nuova carta di credito o l'utilizzo dei dettagli personali della vittima per l'acquisto di beni, servizi o altri vantaggi finanziari. Il malvivente può addirittura giungere ad ottenere un passaporto a nome di terzi.

FURTO DI IDENTITÀ AZIENDALE: include il furto di identità di un'azienda e il commercio sotto falso nome.

COME PUÒ ESSERE RUBATA LA VOSTRA IDENTITÀ?

Ci sono diversi metodi per acquisire le informazioni necessarie a rubare l'identità di un soggetto. Sicuramente negli ultimi anni si sono moltiplicate le occasioni in cui è possibile il reperimento, l'archiviazione e la condivisione delle informazioni personali in seguito al cambiamento di abitudini e stili di vita. Diventa quindi, più facile essere soggetti ad un furto.

DI SEGUITO TROVATE L'ELENCO DI ALCUNI DEI POSSIBILI MODI IN CUI LA VOSTRA IDENTITÀ PUÒ ESSERE RUBATA:

- **Bin raiding:** i malviventi rovistano nella vostra immondizia, cercando estratti conto bancari o delle carte di credito e informazioni fiscali. Ogni giorno, i dettagli che voi pensate non siano importanti, come vecchie bollette del gas, dell'elettricità e del telefono, documenti sulle assicurazioni stipulate, lettere personali, nonché l'involucro con cui sono inviati giornali e depliant, contengono, in realtà, informazioni personali di notevole importanza.
- **Mancato inoltro della posta:** i malviventi possono reperire informazioni anche nel caso in cui, successivamente ad un trasferimento di residenza, dimenticate di comunicare la variazione dell'indirizzo alle Poste Italiane.
- **Skimming:** esso consiste nella clonazione di una carta di credito durante il prelievo, attraverso un'apparecchiatura elettronica (skimmer) che i malviventi appongono in maniera fraudolenta sullo sportello bancomat; può essere sufficiente per reperire i dati necessari ad utilizzare la carta senza rubare interamente l'identità della vittima.
- **Furto della borsa o del portafoglio:** generalmente i portafogli e le borse contengono bancomat, carte di credito e documenti di identità come la patente di guida e le tessere di iscrizione a varie associazioni. Le vittime si accorgono relativamente presto di essere state derubate, ma sovente realizzano troppo tardi il valore effettivo delle informazioni contenute nell'oggetto sottratto.
- **Contatti indesiderati:** spesso i malviventi effettuano chiamate telefoniche, presentandosi in nome della banca o dell'azienda con cui intrattenete rapporti commerciali. Siate molto cauti nel dare le vostre informazioni personali, cercando di capire sempre con chi state parlando. Se possibile, recatevi di persona nella sede dell'organizzazione da cui ricevete la comunicazione, per essere certi di non cadere nelle mani dei criminali.
- **Telefono cellulare:** mediante la ricezione di messaggi (SMS, Email) che comunicano la vincita di un telefonino di ultima generazione, seguite un link che porta ad una azione di phishing finalizzata ad acquisire i dati personali.
- **Siamo noi stessi o chi ci conosce a fornire informazioni:** altre fonti possono essere il portinaio, la domestica, o voi stessi che, inconsciamente, raccontate in pubblico fatti che vi riguardano. Per esempio, in un ambulatorio, raccontate cosa vi è successo o fate considerazioni che, non sapendo, possono risultare utili a chi vi ascolta. Intanto, il criminale, raccoglie il nome del vostro cane e quanti anni ha! Cosa ci fa? Può far credere a qualcuno della vostra famiglia che lui è un vostro caro amico o collega ed ottenere così qualche ulteriore informazione utile per portare a termine la frode. Inoltre può telefonare - per citare altri esempi - al call center di un'azienda per farsi dare la vostra password di accesso ad un servizio, facendo credere di non ricordarla più oppure per comunicare il vostro presunto cambio di residenza in modo da ricevere ***al suo indirizzo*** i documenti a voi destinati.

I PERICOLI DEL WEB

L'informatica e le nuove tecnologie hanno creato rischi fino a ieri impensabili e poco conosciuti dai consumatori; in particolare, l'uso ormai quotidiano di Internet ci espone a pericoli sottovalutati o spesso sconosciuti.

- **La navigazione in Rete:** a tutti coloro che navigano viene regolarmente richiesto di fornire informazioni personali per poter accedere a determinati siti e per poter acquistare beni; molto spesso queste informazioni viaggiano sulla rete in chiaro e non in modalità protetta.
- **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 (per riscuotere premi in denaro, beni tecnologici, ripristinare password scadute, etc…). Generalmente l'e-mail chiede di utilizzare un link per accedere ai dettagli del conto della vittima presso il sito della compagnia, adducendo motivazioni di sicurezza. Cliccando su quel link, tuttavia, l'ignaro malcapitato sarà condotto in un sito web solo all'apparenza originale. I criminali potranno poi utilizzare i dati inseriti in questo sito fittizio per prelevare denaro dai conti correnti delle vittime, fare acquisti o transazioni a loro nome.
- **Sniffing:** Si definisce ***sniffing*** l'attività di intercettazione passiva dei dati che transitano in una ***rete telematica***. Tale attività permette l'intercettazione fraudolenta di ***password*** o altre informazioni sensibili.
- **La diffusione di social network (ad es. Facebook, Twitter) e chat** ha attratto l'attenzione di hacker e malintenzionati. Infatti, il principale pericolo che deriva dall'uso di questi siti web è proprio l'eccessiva esposizione di informazioni personali.

CHE COSA PUÒ ESSERE FATTO CON LA VOSTRA IDENTITÀ

NEL CASO IN CUI VENGA RUBATA L'IDENTITÀ DI UNA PERSONA FISICA, UN LADRO PUÒ REALIZZARE VARIE TIPOLOGIE DI FRODI:

- aprire un conto corrente bancario;
- emettere assegni contraffatti e prosciugare il vostro conto corrente bancario;
- acquistare auto, elettrodomestici ed altri beni di consumo a rate;
- scrivere alla filiale di banca e modificare l'indirizzo di spedizione delle comunicazioni. Gli estratti conto saranno inviati al nuovo indirizzo, rendendo difficile scoprire il reato che si sta perpetrando a vostro nome.
- richiedere carte di credito;
- aprire un conto telefonico.

QUANDO, INVECE, LA VITTIMA DEL FURTO È UN'AZIENDA
è possibile che i malviventi accedano ai pubblici registri e cambino i nomi dei titolari dell'azienda e i loro indirizzi, ottenendo così beni e servizi senza adempiere a nessun pagamento e screditando il buon nome dell'azienda. Purtroppo questo non è l'unico rischio. Le coordinate bancarie dell'azienda possono essere di dominio pubblico, in modo da spingere i propri clienti ad effettuare i pagamenti direttamente sul conto corrente della compagnia.

Infine, sempre accedendo ai pubblici registri, i criminali possono procurarsi le firme degli intestatari del conto ed utilizzarle per compiere furti di identità e di denaro, a discapito dell'azienda.

COME PREVENIRE LE FRODI D'IDENTITÀ: SUGGERIMENTI UTILI

Gestendo le vostre informazioni personali attentamente, potrete ridurre le probabilità di cadere nelle mani dei malviventi!

COME DIFENDERSI DAL FURTO DI DOCUMENTI

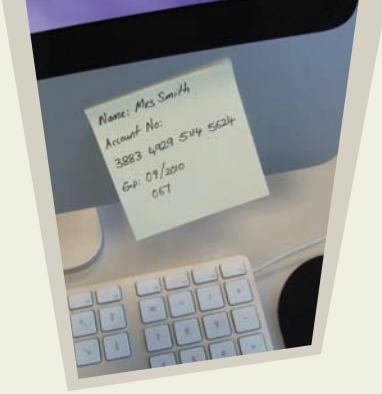
- **Conservate a casa, o, comunque, in luogo sicuro una fotocopia di tutti i documenti** come il passaporto, la patente di guida, il porto d'armi, il tesserino professionale, ecc.
- **Non conservare tutti i documenti di identità nello stesso posto**, specialmente se siete in viaggio.
- **Limitate il numero di documenti che portate con voi** e, se possibile, non lasciateli all'interno della vostra automobile.
- **Non lasciate mai incustoditi la giacca o la borsa** contenenti il portafoglio: il ladro è veloce e può essere anche una persona insospettabile, quella che lavora nella stanza accanto alla vostra: normalmente tutti ritengono che sia impossibile e, invece, ci sono tanti episodi che dimostrano il contrario.
- **Prestate attenzione a tutti coloro che vi contattano inaspettatamente** (tramite telefono, fax, faccia a faccia, ecc.) e che richiedono informazioni personali, anche se affermano di essere incaricati dalla vostra banca, dalla polizia o da qualsiasi altra organizzazione. Infatti, di solito, le banche, come le altre organizzazioni, non richiedono mai informazioni al telefono, ma sempre tramite comunicazione scritta. ***Non comunicate i vostri dati se non siete sicuri di darli alla persona giusta.*** Qualora vi vengano richiesti, ad esempio, dalla società emittente la carta di credito o da un fornitore, verificate l'attendibilità della fonte contattando telefonicamente la società, prendendo il numero di telefono dall'elenco o da documenti in vostro possesso di cui siete certi.

Dovete cercare di capire se la richiesta è accettabile e, quindi, inviare i dati ad un numero di fax della società stessa evitando di darli per telefono, anche se è più comodo.

- **Prestate attenzione alle bollette delle utenze:** se non ricevete la vostra bolletta, contattate le società di servizio immediatamente. Una bolletta mancante può significare che un frodatore è venuto a conoscenza del conto della vostra carta di credito e ha modificato la vostra residenza.
- **Rendete sicura la vostra posta:** assicuratevi che la posta sia al sicuro, finché non la ritirate. Scegliete una cassetta chiusa con un lucchetto.
- **Se dovete spedire documenti che contengono dettagli personali**, chiedete all'ufficio postale locale di consigliarvi il metodo più sicuro. Sarebbe bene utilizzare posta tracciabile es. raccomandate o assicurate. Visitate, comunque, il sito www.posteitaliane.it per ulteriori informazioni.
- **Distruggete tutti i vecchi documenti:** è la soluzione migliore per assicurarsi che i criminali non possano ricostruire il vostro profilo basandosi su quanto contenuto nei documenti che gettate nella spazzatura. Prima di gettare i documenti, distruggete tutto e, se potete, utilizzate sia al lavoro che a casa un distruggi documenti.

COME TENERE SOTTO CONTROLLO E PROTEGGERE DOCUMENTI BANCARI, BANCOMAT E CARTE DI CREDITO

- **Annotate le date di arrivo degli estratti conto** (ad esempio: metà gennaio, aprile, luglio, ottobre) ed interrogate la banca se per una di quelle date non vi sono pervenuti (tenendo a mente che potrebbe essere in ritardo, ma è sempre meglio prevenire i pericoli!).
- **Quando decidete di buttare via gli estratti conto ed altri documenti bancari**, incluse le ricevute della carta di credito, ***strappateli a pezzetti***, e se possibile, utilizzate un distruggidocumenti. In mancanza del distruggidocumenti buttate i pezzetti di carta in contenitori diversi o giorni diversi: la raccolta differenziata agevola i possibili malfattori.
- **Quando ricevete un estratto conto, controllatelo subito ed attentamente.** Informatevi presso la banca o la Società emittente la carta di credito quando un prelevamento o una spesa non vi è nota. ***E' molto utile attivare servizi che consentono di monitorare la situazione economica*** o semplicemente fornirci una maggiore protezione: ad esempio, chiedete alla vostra banca ed alla Società di aderire al servizio gratuito di SMS sul vostro cellulare quando viene eseguita una spesa oppure di ottenere un consuntivo via mail degli utilizzi effettuati nella giornata precedente.
- **Quando ritirate un carnet di assegni, controllate che ci siano tutti** e fate questo controllo periodicamente, soprattutto se lasciate il carnet a casa incustodito o lo tenete nel portafoglio;
- **Controllate le carte di credito:** è consigliabile ridurre al minimo il numero di quelle contenute nel portafoglio.
- **Prima di firmare una ricevuta di una carta di credito, controllare la ricevuta.** In alcuni casi compaiono completamente tutte le informazioni della carta di credito (numero, scadenza ecc.); quindi cancellate qualche cifra del numero della carta riportato sopra la ricevuta prima di firmarla. Se il negoziante non lo consente, meglio cambiare negozio.
- **Password e PIN:** evitate di usare informazioni facilmente reperibili o una serie di numeri consecutivi. Non usare lo stesso PIN per tutte le carte e per tutti i conti. Memorizzate le vostre password e i vostri PIN piuttosto che scriverli e non comunicateli mai a nessuno.
- **In caso di smarrimento o furto di bancomat/ carta di credito**, contattate il servizio clienti del vostro istituto di credito e richiedete di bloccarle immediatamente per essere sicuri che non siano utilizzate da persone non autorizzate.
- **Se richiedete una nuova carta ed essa non arriva entro un tempo ragionevole, avvertite la filiale.** Quando ricevete una nuova carta, firmatela con inchiostro permanente e attivatela immediatamente.
- **Cercate di prelevare sempre allo stesso sportello ATM**; quando vi recate a prelevare, osservate lo sportello e fate attenzione ad eventuali "segnali" anomali. Ad esempio, potreste trovare una tasca laterale, che prima non c'era, contenente avvisi pubblicitari; oppure nella fessura in cui inserite la carta, potrebbe essere stato apposto uno skimmer, ovvero un dispositivo che consente ai truffatori di entrare in possesso delle informazioni necessarie a clonare la carta.
- **Mentre digitate il codice segreto con una mano, coprite la tastiera** sulla quale state digitando il codice con l'altra mano o con fogli posti a pochi centimetri nella parte superiore.
- Fate attenzione a persone solerti che vogliono aiutarvi a prelevare: possono essere ladri!
- **Aggiornate i vostri contatti:** se vi trasferite o cambiate numero telefonico, comunicate al più presto il cambiamento alla vostra banca, al fornitore della carta di credito e, ovviamente, a tutte le organizzazioni con cui intrattenete rapporti. Potete informarvi presso Poste Italiane per l'attivazione del servizio di inoltro: è un buon modo per esser certi che tutta la posta vi sarà inviata al nuovo indirizzo e per ridurre il rischio che le vostre informazioni personali cadano nelle mani sbagliate.



ALCUNI CONSIGLI PER UN USO SICURO DEL WEB

- **Aggiornate regolarmente il sistema operativo** del vostro computer installando le "patch" (aggiornamenti per eliminazione di errori) rilasciate periodicamente dal produttore (generalmente Microsoft).
- **Tutelatevi quando siete on-line: utilizzate un buon antivirus, un firewall, un anti-spam e un anti-dialer** che proteggano il computer contro software che possono essere utilizzati per ottenere informazioni utili.
- **Evitate di utilizzare i software predisposti per il completamento automatico delle password.** Il software in sé non è rischioso, ma può essere facile per i criminali accedere alle vostre informazioni personali se riescono ad accedere al vostro PC.
- **Verificate il vostro URL:** quando siete in Rete, prestate molta attenzione all'indirizzo del sito che state visitando e verificate che sia scritto correttamente dato che è possibile essere condotti a siti fittizi. Aggiungete tra i preferiti gli indirizzi che utilizzate frequentemente, evitando così di commettere errori e garantendovi di essere sempre nella giusta home page.
- **Non cliccate su link** che ricevete via email ***se non siete sicuri***.
- **Usate password sicure e complesse** e non usate mai informazioni personali, come il codice fiscale o la data di nascita.

COMPORTAMENTI DA EVITARE QUANDO SI DECIDE DI ENTRARE A FAR PARTE DI SOCIAL NETWORK (TWITTER, FACEBOOK, MY SPACE ecc.)

- **Evitare di accettare amicizia da parte di sconosciuti:** fare finta di essere un'altra persona su social network è molto facile; basta inserire nome e cognome e magari aggiungere una foto falsa.

  Con questa tecnica ci si può fare molti amici (una buona percentuale degli utenti accetta l'amicizia pure da persone sconosciute) e poi diffondere link pericolosi.

- **Non date informazioni di carattere personale:** evitate di fornire nome, cognome, indirizzo, data di nascita, numero di telefono.

  Meglio usare nomi di fantasia (nickname).

- **Richieste di denaro** Un esempio di come si possono perpetrare truffe tramite i social network è costituito dai messaggi di richiesta di denaro provenienti da amici in situazioni d'emergenza, di cui bisogna diffidare.

- **100$ per un profilo** Di natura opposta invece la truffa congegnata dal sito Hack Facebook online, che fa leva sulla gola dei tanti ficcanaso e vandali della Rete. Il servizio - in cambio di cento dollari, pagabili tramite Western Union, quindi difficilmente tracciabili e senza alcuna possibilità di restituzione - promette di entrare in qualunque profilo di Facebook, leggerne il contenuto e prenderne eventualmente il controllo. Nonostante il sito offra una dimostrazione gratuita, per altro fornendo dati che non richiedono alcuna intrusione per essere acquisiti, per conoscere la password dell'utente-bersaglio naturalmente bisogna pagare. Va da sé che non verrà fornito nessun accesso, ma difficilmente qualcuno oserà contestare in sede legale che il sito non offre quanto promesso.

  Ricordatevi che è una pratica illegale quella di accedere a profili altrui senza il consenso!

- **Iscrizione a gruppi** Le amicizie nei social network rivelano molto di più di quanto si possa immaginare: addirittura ***il fatto stesso di pubblicare la lista dei propri amici permette di sapere cose che magari non si avrebbe intenzione di divulgare***.

  Il principio di fondo è abbastanza semplice: nella vita reale si cerca la compagnia dei propri simili e lo stesso vale su Internet.

  La differenza è che mentre nella vita reale raccogliere questi dati sulle conoscenze è impraticabile, farlo su Internet è facilissimo.

  Anche non rivelando intenzionalmente delle informazioni personali, l'affiliazione a determinati gruppi d'interesse può quindi rivelare informazioni sensibili oppure spingere la gente a fare deduzioni sbagliate sulle persone.

SEMPLICI PASSI PER PROTEGGERE LA VOSTRA AZIENDA

Come tutelarsi?
Quali gli obblighi a carico delle aziende?

Le aziende per legge hanno il dovere di conservare e proteggere le informazioni dei propri clienti e dei propri dipendenti oltre che l'obbligo. Infatti in Italia è vigente il ***Decreto Legislativo 196/2003 o " Codice in materia di protezione dei dati personali"***. Chiunque per motivi professionali conserva o tratta dati sensibili altrui (e quindi, tutte le organizzazioni, le aziende, gli enti pubblici, i professionisti…) è soggetto alle cautele e agli obblighi previsti dalla legge in quanto ***responsabile civilmente e penalmente*** anche in modo oggettivo di ogni danno cagionato al titolare o a terzi da un trattamento non corretto:

- √ La legge elenca ***17 possibili operazioni di trattamento dei dati***. In particolare, ***i dati su supporti cartacei o multimediali devono essere distrutti una volta cessato il trattamento (art. 16, c. 1-a)***. Distruggere i supporti, cartacei e non, è infatti il modo migliore per evitare che i criminali possano avere accesso ai dati sensibili.
- √ Il trattamento dei dati è considerato un'attività pericolosa, e come tale gode dell'inversione dell'onere della prova (art. 2050 Codice Civile): è il responsabile del trattamento dei dati che ha l'onere di dimostrare il corretto utilizzo per evitare di incorrere in sanzioni civili e penali.
- √ L'ufficio del ***Garante della Privacy*** può richiedere alle autorità di polizia di effettuare ***controlli*** e le ***sanzioni*** per il mancato rispetto della legge possono arrivare a 80.000 euro (articoli da 161 a 172 del decreto).

Anche le aziende possono essere obiettivo di criminali senza scrupoli. Il truffatore cerca di entrare in possesso o rubare quanto segue:

a) Il nome dell'organizzazione
b) Numero di iscrizione al Registro delle Imprese
c) Informazioni riguardanti i direttori, gli impiegati e/o i clienti
d) Particolari sui conti correnti

Queste informazioni servono per acquisire prodotti finanziari (ad esempio prestiti e carte di credito sociale), ordinare merci e servizi a credito dai fornitori, ingannare i clienti rovinando il buon nome della vostra azienda. Questa, tuttavia, non è la sola area in pericolo. I frodatori possono addirittura arrivare ad ottenere la firma nei pubblici registri e ad utilizzare i conti bancari presentandosi come i firmatari del conto. In alternativa, un truffatore può semplicemente metter su una falsa società per comprare beni e servizi a credito da una organizzazione e sparire prima di pagare.

Ecco alcuni **semplici passi e suggerimenti** per tutelare i propri dipendenti, clienti e fornitori:

- Fate in modo che i dipendenti siano cauti nel fornire le informazioni dell'azienda, on-line o via telefono, verificando con chi effettivamente hanno a che fare. Mettere i dipendenti a conoscenza dei rischi di frode di identità aziendale può garantirvi che rimarranno vigili.

- Predisporre ***un'accurata politica di gestione e archiviazione dei documenti*** partendo da una classificazione delle informazioni in possesso. Ci sono informazioni generali (di accesso a tutti), informazioni sensibili (ad es. quelle di contatto del cliente o dell'impiegato) e informazioni confidenziali (ad es. dettagli di conti bancari o altre informazioni riguardanti la gestione, i prodotti e la conduzione della vostra azienda).
  - Controllate chi ha accesso ai vari tipi di informazione e limitatela solo a quelli che hanno bisogno di averla;
  - I file, le cartelle e i documenti dovrebbero essere etichettati con cura in modo che sia più facile per il dipendente e il datore di lavoro sapere chi dovrebbe avere accesso a che cosa, dove custodirli quando non in uso e come distruggerli quando non servono più;
  - Controllate dove le informazioni sensibili e quelle confidenziali vengono conservate e assicuratevi che questo sia un posto sicuro e a norma di legge;
  - Assicurarsi che la procedura sia comunicata e correttamente eseguita da tutti i dipendenti e che la responsabilità di controllare che il sistema venga migliorato e seguito da tutti sia affidata a una persona qualificata.

- ***Distruggete tutti i documenti "confidenziali" quando non servono più, usando per esempio degli appositi distruggidocumenti.***
  - Assicuratevi sempre di distruggere le informazioni prima di lasciare l'ufficio. Impostate una linea di condotta che richieda anche la distruzione dei file elettronici non più essenziali e che i file trasferiti su apparecchi portatili siano cancellati non appena usati;
  - Assicuratevi anche che gli hard disk e i media portatili siano cancellati usando software specializzati o che tali dispositivi vengano distrutti una volta obsoleti;
  - Se vi servite di terze parti, assicuratevi che tutti i membri dello staff siano a conoscenza e aderiscano a questa direttiva.

- Assicuratevi che il ***sistema IT sia costantemente aggiornato e protetto*** con ***antivirus*** e ***firewall***. Infatti, è assolutamente indispensabile mettere tutte le informazioni critiche e sensibili al sicuro da potenziali spyware, malware e minacce di spam. Ma altrettanto importante è prevedere una soluzione di backup e recupero dei dati in caso di perdita accidentale o attacco.

COSA FARE QUANDO SI DIVENTA UNA VITTIMA

√ Immediatamente dopo aver subito un furto o uno scippo, denunciate l'accaduto al Pronto Intervento **112 per i Carabinieri, 113 per la Polizia di Stato** o direttamente sul web all'indirizzo **www.commissariatodips.it** Recatevi poi negli uffici dell'Autorità di Polizia Giudiziaria e presentate la denuncia, fornendo gli estremi dei documenti che vi sono stati sottratti.

√ Se sospettate che qualcuno abbia usato il vostro nome (o quello dell'azienda) o altre informazioni per effettuare un acquisto a credito o richiedere un prestito, vi suggeriamo di **Contattare la vostra banca** per segnalare l'accaduto e valutare se è necessario bloccare tutte le carte di credito e di debito.

√ Contattare il creditore, la banca, la compagnia telefonica e l'azienda di servizi pubblici e **congelate immediatamente i relativi conti**.

√ Rivolgersi alle associazioni di difesa dei consumatori come **ADICONSUM**, per ottenere consigli e consulenza, per verificare la propria situazione ed eventualmente per riconfermare la propria affidabilità creditizia. Le associazioni dei consumatori potranno fornire informazioni, suggerimenti e offrire tutela legale.

√ Dato che recuperare la propria identità rubata può essere un processo lungo e complicato, è importante **prendere nota di tutte le comunicazioni** e **tenerne una copia**. Se pensate che il vostro caso può condurre ad un processo civile, annotate anche quanto tempo utilizzate per risolvere il problema.

Per ulteriori informazioni consultare il sito:

www.furtoidentita.com

ADICONSUM
associazione difesa consumatori e ambiente

www.adiconsum.it
email: adiconsum@adiconsum.it

in collaborazione con Fellowes leonardi