FURTO DELL' IDENTITÀ COMMERCIALE

PIÙ INFORMATI PIÙ PROTETTI

PER INFORMAZIONI

Settore Sanzioni e Regolazione del mercato della Camera di commercio di Torino • Via San Francesco da Paola 24
Tel. +39 011 5716970 • tutela.consum@to.camcom.it •
www.to.camcom.it/guidadiritti

stctipografico.it

FSC MISTO Carta FSC® C107186

CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
DI TORINO

FURTO DELL' IDENTITÀ COMMERCIALE

CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
DI TORINO

COS'È IL FURTO DELL'IDENTITÀ COMMERCIALE?

Il d.lgs. 64/2011 definisce il furto di identità come una "impersonificazione" grazie alla quale il "ladro" utilizza l'identità di un'altra impresa o persona, dietro cui si nasconde totalmente od opera con un'identità fittizia che combina dati propri e altrui.

Il furto d'identità è un fenomeno in forte ascesa che rappresenta un serio pericolo per l'impresa attraverso il quale è possibile, ad esempio:

- prosciugare il c/c o il credito telefonico di chi ne è vittima
- stipulare contratti o commettere reati ai suoi danni
- ottenere beni, servizi, crediti o pagamenti dilazionati
- screditare un'impresa concorrente
- carpire informazioni riservate su dipendenti e/o clienti
- appropriarsi di invenzioni e opere d'ingegno.

COME SI ATTUA?

Per perseguire i propri intenti criminosi il malvivente può usare indebitamente il nome della ditta, la sede, l'oggetto, il numero di iscrizione al registro delle imprese, il nome di chi ne ha la rappresentanza o tutti questi dati insieme.

Come proteggersi?

- Controllate costantemente estratti conto, ordini e fatture
- portate a conoscenza dei terzi l'elenco dei soggetti che possono concludere contratti a nome della vostra impresa e ripetete periodicamente questa comunicazione
- segnalate tempestivamente ogni modifica o revoca (ad esempio, con una telefonata seguita da una lettera e/o con annunci su giornali o in rete)
- tenete aggiornati i vostri strumenti di pubblicità, soprattutto quelli on line (siti web, blog, pagine facebook/twitter, ecc...) e affidatene la gestione a soggetti competenti
- controllate con regolarità tramite motori di ricerca la vostra presenza nel web, in modo da avere immediata notizia di eventuali siti impostori (c.d. fake) o di indebite intrusioni sul vostro
- avvaletevi della tutela di legge su marchi, brevetti e diritto d'autore: ricordate che, in ogni caso, è vietato ogni atto di concorrenza sleale, come diffondere notizie e apprezzamenti sui prodotti e sull'attività di impresa altrui, tali da determinarne il discredito.

QUALI INFORMAZIONI SONO PIÙ A RISCHIO?

L'impresa può essere bersaglio di furto proprio perché detentrice di una grande quantità di informazioni. Fra queste, le più appetibili sono i progetti e le invenzioni industriali e, dall'altro lato, i dati dei clienti, come coordinate bancarie, informazioni personali, preferenze d'acquisto. Il ladro può sottrarre fisicamente i supporti cartacei ove sono contenuti, oppure aggredire il sistema informatico o aggirarne la protezione utilizzando le credenziali d'accesso sottratte al dipendente.

Come proteggersi?

- Adottate una seria politica di gestione e archiviazione dati e predisponete misure di sicurezza idonee a ridurre i rischi di accesso non autorizzato e di sottrazione
- tenete presente che il trattamento dati è qualificato dalla legge come attività pericolosa, quindi sorge a carico dell'impresa una responsabilità per danni particolarmente rigorosa.

COME FARE QUANDO I DATI SONO IN FORMATO CARTACEO?

- Catalogate i documenti e conservateli in luoghi sicuri ad accesso limitato
- distruggete periodicamente quelli che non servono più.

COME FARE QUANDO I DATI SONO IN FORMATO DIGITALE?

- Adottate misure di verifica e di convalida dell'identità di chi accede al sistema (ad esempio id personalizzati e password sicure)
- usate procedure di autorizzazione che consentano solo le attività predefinite
- dotate il vostro sistema informatico di firewall, antivirus e antispam aggiornati
- se le dimensioni della vostra impresa lo consentono, dotatevi di un sistema di server di rete e di posta elettronica interna
- smaltite in maniera adeguata le apparecchiature elettroniche (computer, chiavi di memoria, dischetti, telefoni cellulari, tablet e smartphone), ad esempio utilizzando software specifici che procedono alla cancellazione sicura dei dati ivi contenuti
- formate adeguatamente i dipendenti sul tema della sicurezza e della protezione dati, se possibile destinandone uno o più a questa specifica mansione
- predisponete copie di backup per far fronte alle situazioni di crisi.