FURTO D'IDENTITÀ

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 D'IDENTITÀ

CAMERA DI COMMERCIO
INDUSTRIA ARTIGIANATO E AGRICOLTURA
DI TORINO

COS'È IL FURTO D'IDENTITÀ?

È l'appropriazione e l'utilizzo indebiti del nome o dei dati identificativi di un'altra persona per accedere ai più svariati servizi (ad es. l'username e la password per l'accesso all'e-mail, o al c/c tramite il servizio di home banking, o ai profili Facebook e Twitter, o i codici di utilizzo del bancomat o dello smart phone), allo scopo di servirsene, ad esempio per prosciugare il conto corrente o il credito telefonico, o al fine di stipulare contratti o commettere dei reati.

Spesso si realizza attraverso:

- il furto e l'alterazione dei documenti d'identità (passaporto, C.I., patente, ecc...)
- il furto e l'alterazione di bancomat e carte di credito
- la clonazione delle carte di pagamento, di solito per manomissione o sostituzione del dispositivo che memorizza i contenuti delle bande magnetiche delle carte di pagamento (c.d. skimming).

Come proteggersi?

- Non perdete di vista le vostre carte di credito quando le consegnate per effettuare pagamenti
- schermate la tastiera quando digitate codici e PIN
- conservate in luoghi sicuri e diversificati i documenti, quelli di identità ma anche quelli che contengono altri dati (ad es. la dichiarazione dei redditi, il curriculum, gli estratti conto bancari, le bollette delle utenze)
- monitorate i movimenti di dare e avere dei vostri conti correnti
- distruggete con cura (meglio sminuzzarli) i documenti di cui vi volete liberare
- controllate la regolarità della ricezione delle bollette e comunicate immediatamente eventuali cambi di residenza a tutti i contatti abituali.

COS'È IL FURTO PER ABBOCCAMENTO?

Si tratta del cosiddetto "phishing". Il raggiro parte da una e-mail o un sms che sembrano provenire da siti web familiari alla vittima (ad es. quello di home banking o eBay) e che invitano a reinserire le proprie credenziali di accesso, spesso dirottando su siti web quasi identici agli originali, allo scopo di appropriarsene.

Come proteggersi?

- Navigate solo su siti sicuri e non cliccate su link a siti che non conoscete
- verificate gli indirizzi (URL) dei siti che visitate. È il metodo più efficace per sventare tentativi di phishing: potete infatti accorgervi che l'URL del sito camuffato non corrisponde a quello dell'originale
- diversificate le password e modificatele periodicamente; non le costruite usando dati che si possono indovinare facilmente, come il vostro codice fiscale o il nome e la data di nascita dei vostri figli/amici/animali.

  Se pensate di non poterle ricordare a memoria, appuntatele su carta.

COS'È L'INTERCETTAZIONE INFORMATICA?

Si tratta di una particolare forma di furto, altrimenti detta "keylogging", resa possibile da specifici software che captano ciò che viene digitato sul computer o sullo smart phone.

Come proteggersi?

- Installate e aggiornate periodicamente antivirus, firewall e filtri antispam e controllate la reputazione delle Apps prima di installarle, perché i software malevoli possono provenire dalla rete o da applicazioni telefoniche
- se vendete il vostro telefono o ne comprate uno usato, resettate tutte le informazioni in esso contenute e riconfiguratelo.

COME AVVIENE IL FURTO D'IDENTITÀ NEI SOCIAL NETWORK?

Viene aperto un falso profilo su cui pubblicare contenuti non autorizzati (foto, dichiarazioni, annunci, ecc...), anche a scopo diffamatorio o persecutorio, o comunque lesivo della reputazione o della personalità della vittima. Noto anche come "fake accounting", "cyberbullying", "cyberstalking".

Come proteggersi?

- Imparate a usare le restrizioni a tutela della privacy del sito di social network cui siete iscritti e selezionate con attenzione chi aggiungere ai vostri contatti
- non lasciate visibili a tutti informazioni quali il numero di cellulare o la data di nascita per intero
- limitate l'accesso alle foto
- non pubblicate foto o commenti imbarazzanti, né vostri né di altri.

E PER ESSERE DAVVERO SICURI?

Siate cauti nel raccontare in pubblico notizie su voi stessi o sulle vostre abitudini e verificate preventivamente le qualifiche e l'affidabilità di chi vi chiede informazioni personali: la prudenza è sempre la migliore arma di difesa!