Verbraucherzentrale Südtirol
Centro Tutela Consumatori Utenti
Die Stimme der VerbraucherInnen
La voce dei consumatori

Centro Tutela Consumatori Utenti

Via Dodiciville 2
39100 Bolzano
Tel. 0471 975597
info@verbraucherzentrale.it

Furto dati su Facebook: a cosa devono fare attenzione consumatori coinvolti

Mer 14/04/2021 - 09:08

Diffusi anche i numeri di cellulare – Tenere d'occhio conti e carte di pagamento!

Aggiornamento del 16.04.2021:
Alcuni consumatori ci chiedono perché facciamo riferimento a un sito straniero per il controllo dei dati in questione. Il sito italiano analogo che offriva questo servizio, ha dovuto sospendere il servizio secondo le richieste del Garante italiano della privacy; la decisione del Garante non sembra davvero comprensibile.

I dati di 533 milioni di persone, fra i quali 35 milioni di italiani e italiane, offerti in vendita sul web. Il furto risalirebbe già al 2019 e la fuga di dati sarebbe stata tempestivamente bloccata, almeno così afferma Facebook, ma è presto per dare il "cessato allarme".

Quali dati risultano divulgati?
Risulterebbe che nomi, date di nascita, indirizzi e-mail, informazioni delle biografie su Facebook, come anche numeri telefonici siano stati oggetto di sottrazione (anche quelli inseriti nel social-network come "privati"). Particolarmente insidiosa è la questione dei numeri telefonici, in quanto molte richieste di autenticazione per pagamenti online e servizi bancari online vengono inviate per SMS e i numeri telefonici sottratti potrebbero quindi essere utilizzati per truffe telefoniche e smishing.

Sono rimasto anch'io vittima?
Alla pagina internet https://haveibeenpwned.com/ si può controllare, se i propri dati personali siano fra quelli sottratti. Basta inserire il proprio indirizzo e-mail oppure il proprio numero di cellulare completo di prefisso internazionale, senza però i due zeri (quindi 39 seguito dai canonici 10 numeri del vostro

cellulare, senza spazi).

Cosa posso fare per proteggermi?
A prescindere dal furto dati di cui si discute, è bene seguire le seguenti regole: controllare periodicamente i propri estratti di carte e di conti di pagamento, in maniera da poter intervenire tempestivamente in caso di necessità. Nel caso in cui fossero stati sottratti vostri dati personali, questi sono da considerare come "non sicuri" e quindi sarebbe meglio non utilizzarli quali elementi nella procedura di cd. identificazione a doppio-fattore (detta anche "strong-autentication"). Meglio utilizzare, in alternativa, le apps, anche se vi è da dire che anche nel caso di molte di queste apps relative a servizi bancari online sono presenti parti di codice che dal punto di vista della privacy non sono certo la migliore delle soluzioni – si rischia – quasi – di finire dalla padella alla brace.

Se trovate movimenti anomali …
Nel caso in cui vi fosse stato già sottratto denaro dal conto o dalla carta, non perdete tempo: chiudete e bloccate tutto, presentate subito denuncia e chiedete indietro i soldi all'intermediario bancario. Per i dettagli, potete chiedere aiuto e consiglio al servizio di consulenza dedicato del CTCU.

"Dall'introduzione della seconda direttiva sui servizi di pagamento vige l'obbligo di "autenticazione forte" nei pagamenti online. Molti prestatori di servizi hanno scelto – probabilmente per motivi economici o di marketing – di utilizzare lo smartphone dei loro clienti quale secondo fattore. Non solo chi tutela i consumatori, ma anche l'Autorità Bancaria Europea EBA non sono molto felici della scelta di inviare le password mono-uso tramite SMS, in quanto sono molto esposti al rischio intercettazione. Da parte nostra, non possiamo dare un "nulla osta" illimitato all'utilizzo delle app che si sostituiscono agli SMS per la generazione delle password "one time", in quanto molte di loro sembrano collezionare parecchi dati personali dei loro utilizzatori. La soluzione migliore sarebbe un "token" volto a generare solo le password, senza altri modi di comunicazione con il mondo esterno, come già offerto da alcune banche locali" riassume la Direttrice del Centro Tutela Consumatori Utenti, Gunde Bauhofer.

Nulla si sa poi riguardo alle conseguenze legali che il data breach potrà avere per Facebook: dai commenti dell'azienda, volti solo a tranquillizzare, non pare trapelare propensione ad assumersi alcuna responsabilità al riguardo.

Gli unici dati sicuri restano, pertanto, quelli mai pubblicati.