

Trento, 21 aprile 2021

Comunicato stampa

**Furto dati su Facebook: a cosa devono fare attenzione
consumatori coinvolti
Diffusi anche i numeri di cellulare – Tenere d’occhio conti e
carte di pagamento!**

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?

Considerate che se avete inserito nella piattaforma numeri telefonici o email per il suo utilizzo, è altamente probabile che il furto abbia riguardato anche voi (circa 1 su 2). Scrivete direttamente a Facebook e al Garante della Privacy chiedendone conferma e segnalando la violazione.

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 perdetevi 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 CRTCU.

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.