24.01.2020

Fuga di dati da Microsoft

A dicembre sono stati pubblicamente accessibili 250 milioni di dati di supporto di Microsoft, che potrebbero essere sfruttati dai truffatori per inviare e-mail di phishing o effettuare truffe telefoniche. Proteggetevi!

Dal 5 al 31 dicembre 2019 250 milioni di record contenenti dati di supporto di clienti Microsoft sono stati disponibili pubblicamente senza protezione. Secondo un comunicato, Microsoft avrebbe reagito e risolto la fuga di dati entro 24 ore. I dati dei clienti risalirebbero fino al 2005 e comprenderebbero messaggi chat, indirizzi di posta elettronica e posizioni geografiche.

Si teme che i truffatori potrebbero usare illecitamente queste informazioni per preparare e-mail di spam o phishing credibili. Nel caso di Microsoft sarebbe immaginabile anche lo sfruttamento per commettere truffe telefoniche. Il supporto telefonico falso ad opera di presunti collaboratori dell'assistenza di Microsoft, infatti, è una prassi ricorrente da anni. Non è ancora noto se persone non autorizzate abbiano potuto accedere ai dati.

Proteggetevi così:

- Interrompete immediatamente le chiamate indesiderate di presunti collaboratori di Microsoft, società di assistenza informatica o istituti finanziari. Non date per scontato che il numero visualizzato sul display del telefono sia corretto.
- Se avete domande da rivolgere all'assistenza, componete sempre i numeri di telefono ufficiali di Microsoft, delle società di assistenza informatica o del vostro istituto finanziario, riportati p. es. sulle fatture o sugli estratti conto.
- Durante le telefonate non comunicate mai informazioni riservate come le password.
- Non utilizzate mai un link ricevuto via e-mail, SMS o servizio di messaggistica o scansionato tramite codice QR per accedere ai portali di Microsoft, una società di assistenza informatica o un istituto finanziario.
- Non compilate mai i moduli ricevuti via e-mail che chiedono di inserire i dati d'accesso.
- Inserite l'indirizzo della pagina di accesso del vostro fornitore di servizi online o istituto finanziario sempre manualmente, nella barra degli indirizzi del browser.
- Quando aprite la pagina di accesso, verificate che la connessione sia SSL (https://, icona a forma di lucchetto) e assicuratevi di trovarvi sulla pagina desiderata controllando l'indirizzo Internet nella barra degli indirizzi del browser.

Ulteriori informazioni sono disponibili nei nostri articoli sul phishing (https://www.ebas.ch/phishing) e sulle telefonate fraudolente dall'assistenza (https://www.ebas.ch/it/telefonate-fraudolente-dallassistenza/).

Imparate a proteggervi efficacemente dai truffatori di Internet frequentando uno dei nostri corsi (https://www.ebas.ch/course)!