

20.06.2024

Il phishing con le catene di risposte

Praticamente tutti conosciamo le catene di risposte nelle e-mail: un messaggio viene inviato a una o più persone e poi si ricevono tante risposte. Non ci si aspetta che nella conversazione si intrufoli un'e-mail di phishing. Di solito, si pensa che un tentativo di phishing si presenti come messaggio nuovo, non all'interno di una catena di risposte.

In un attacco di phishing in stile «reply-chain», ossia come catena di risposte, i criminali utilizzano un indirizzo e-mail legittimo rubato in precedenza per inviare una risposta contenente un link dannoso o un codice QR. Questo indirizzo e-mail corrisponde a uno dei soggetti coinvolti in una conversazione via e-mail. In questo modo, l'hacker può scrivere da un indirizzo che gli altri destinatari conoscono e di cui si fidano. Inoltre, sfruttano il vantaggio di poter leggere tutta la catena di risposte per scrivere una risposta estremamente coerente. Questi punti rendono più credibile la loro risposta, con la conseguenza che chi la riceve pensa che provenga da un mittente fidato – e quindi è più incline a fare clic sul link o ad aprire l'allegato che i criminali fanno arrivare tramite l'account di posta elettronica rubato.

Le seguenti misure possono ridurre il rischio di un attacco di phishing «reply-chain»:

- Utilizzate password sicure e salvatele in un luogo sicuro, ad esempio in un gestore di password. Ciò complica l'accesso al vostro account di posta elettronica per i criminali.
- Utilizzate con grande prudenza un link ricevuto via e-mail o messaggio breve o scansionato tramite codice QR.
- Non comunicate mai i dati d'accesso per i vostri dispositivi, account di posta elettronica, ecc.

Ulteriori informazioni sul tema del phishing sono disponibili [qui \(https://www.ebas.ch/it/phishing/\)](https://www.ebas.ch/it/phishing/).