«Abbiamo deciso di eliminare definitivamente il tuo account Facebook», occhio al phishing!

In questi giorni una massiccia campagna sta cercando di sottrarre gli account di Facebook e Instagram di lingua italiana. Ecco a cosa fare attenzione.

(Fonte: https://www.corriere.it/ 26 maggio 2025)

«Abbiamo deciso di eliminare definitivamente il tuo account Facebook». Esordisce così, nei messaggi privati, quella che in realtà è una massiccia campagna phishing che prende di mira gli account Facebook e Instagram. Il messaggio viene recapitato da account che si spacciano per i profili ufficiali di Meta che, per risultare più credibili, aggiungono nella foto profilo **la spunta blu** in modo da sembrare account ufficiali. Il messaggio fa leva su un senso di urgenza: viene informato l'utente di **una prossima chiusura del proprio account** per via delle segnalazioni di altri utenti. Ma c'è un modo per salvarsi dalla (finta) chiusura. Ovvero visitare un sito in cui inserire i propri dati personali. **Si tratta ovviamente di un escamotage per sottrarre all'utente il proprio account.**

Lo scopo è quello di suscitare una pressione tale per cui gli utenti che ricevono il messaggio clicchino in breve tempo su un link presente nel messaggio e che cedano dati sensibili, come e-mail, password, etc. Inutile dire che **Meta non inoltra mai messaggi privati per quanto riguarda la sicurezza dell'account**. Ma cosa succede se si clicca sul link?

Meta IA

Meta IA

You're friends on Facebook
Lives in Bologna, Italy
Works at Libero professionista

View profile

End-to-end encrypted
Messages and calls are secured with end-to-end encryption. Only people in this chat can read, listen to, or share them. Learn more

11:04 AM

Il messaggio di phishing

Cliccando sul link si accede ad un sito Web gestito da criminali informatici. Da qui questi potranno accedere ad una serie di informazioni personali di varia natura. Dal proprio indirizzo IP, fino alle credenziali di Facebook, se cedute compilando un form. Una volta eseguiti questi passaggi, è un attimo perdere il controllo del proprio profilo, se non si dispone di un metodo di autenticazione a due fattori (o se si cedono pure i codici univoci).

Cosa succede agli account sottratti

Se i criminali informatici riescono a sottrarre l'account, questo probabilmente verrà utilizzato per contattare gli amici del profilo rubato e utilizzare tattiche di ingegneria sociale, per perpetrare truffe o diffondere malware, oppure ancora rubare altri account. Una volta preso il controllo del profilo, contatteranno gli amici del medesimo. In questo modo i malintenzionati cercheranno di guadagnarsi la fiducia di chi contatteranno, spacciandosi per la persona una volta proprietaria dell'account. Potranno chiedere qualunque cosa: dati, soldi, informazioni.

Cosa fare se ti hanno sottratto l'account

Se un account Instagram o Facebook è stato violato, è bene contattare subito Meta e segnalare l'accaduto, per trovare una soluzione. Basterà collegarsi alle rispettive pagine dedicate alle segnalazioni di **Instagram** e **Facebook** e seguire le indicazioni suggerite. Inoltre è bene segnalare alla Polizia Postale la violazione e le modalità di contatto con cui è stato sferrato l'attacco. Bene anche avvisare anche i propri contatti che vi è la possibilità che l'account sia stato utilizzando contro la propria volontà. Infine, meglio cambiare password e attivare l'autenticazione a due fattori.