VareseNews

“Posso chiederti un piccolo favore?”. Attenzione ai “furti social” che iniziano con un messaggino

Pubblicato: Martedì 22 Agosto 2023

“Ciao, posso chiederti un piccolo favore?”. Inizia così, con un messaggio diretto su Instagram dal profilo (finto) di uno del propri contatti, uno dei più **diffusi tentativi di furto di account social**. L’obiettivo di chi prova a metterlo in atto è quello di ottenere click su link o un codice, necessari per poi accedere al profilo in cui ci si vuole intrufolare.

In altri casi, la richiesta, pur mascherata da messaggio confidenziale, potrebbe essere più diretta e passare da altri canali di messaggistica, come WhatsApp: “Ciao, ti ho inviato un codice per sbaglio, potresti rimandarmelo?” è il testo di una delle chat più diffuse che arriva sul nostro cellulare da un contatto che sembra a tutti gli effetti quello della nostra rubrica. Molto spesso gli utenti, tratti in inganno dalla presunta conoscenza del mittente e non consapevoli della violazione del profilo, rispondono al messaggio, senza esitazione, inoltrando il codice richiesto. In questo modo, si consente ai cybercriminali di impadronirsi dell’account WhatsApp e di sfruttare il servizio di messaggistica istantanea per compiere ulteriori frodi utilizzando il numero di telefono della vittima, nonché di avere accesso ai contatti salvati nella rubrica, innescando una sorta di “catena di Sant’Antonio”.

I casi di furto di account social e di messaggistica istantanea segnalati dagli utenti sono in costante aumento secondo quanto dichiarato dalla polizia postale italiana.

Prevenire i furti con l’autenticazione multifattoriale

“Per prevenire questi furti – si ricorda – è necessario adottare adeguati sistemi di protezione capaci di innalzare i livelli di sicurezza delle nostre “App” (applicazioni) come l’autenticazione “multifattoriale” che si distingue in autenticazione a due fattori e verifica in due passaggi. L’autenticazione di base prevede l’inserimento di un solo fattore, generalmente una password. **L’autenticazione multifattoriale, invece, associa alla password un altro fattore di sicurezza che rende più difficile la violazione da parte di terzi**. I fattori di autenticazione sono di tre tipi: Dati già conosciuti dall’utente (es. password o pin); Codici temporanei di volta in volta generati e ricevuti dall’utente, ad esempio, su smartphone o token; Elementi che identificano l’utente (es. impronta digitale o dati biometrici). La verifica in due passaggi combina fattori appartenenti alla stessa categoria (es. password/pin). **L’autenticazione a due fattori combina, al contrario, fattori di tipologia diversa (es. password/impronta digitale)”.**

Non comunicare mai codici ricevuti via messaggio, mail o sms

La Polizia Postale e delle Comunicazioni ricorda inoltre che: i codici che arrivano per sms sono strettamente personali e non vanno mai condivisi, anche se richiesti da un nostro contatto o da amici e/o familiari; non si deve **mai cliccare su eventuali link presenti nei messaggi di testo;** nel caso di messaggi sospetti, è consigliabile contattare telefonicamente il mittente per accertarsi che il suo account non sia stato violato.

Cosa fare se l’account è stato rubato

In caso di violazione dell’ account è importante avvisare immediatamente i propri contatti su quanto è accaduto, per evitare che a loro volta possano diventare vittime della catena. È importante inoltre presentare formale denuncia presso un Ufficio di Polizia.

di mcc