Scritto da Administrator
Mercoledì 22 Febbraio 2023 19:35

L'autenticazione a due fattori (2FA) è una misura di sicurezza essenziale per proteggere i vostri account
online. Tuttavia, l'
utilizzo del numero di telefono
come metodo di autenticazione può
mettere a rischio la vostra sicurezza
.

{loadposition user7}

Esistono molti modi per utilizzare l'autenticazione a due fattori, dall'utilizzo dell'app Google Authenticator
al classico SMS, ma non tutti sono ugualmente sicuri.

Il punto debole delle password è che chiunque può conoscere le vostre e le fughe di password stanno diventando sempre più comuni. L'autenticazione a 2 fattori risolve questo problema richiedendo sia la vostra password che l'accesso a un dispositivo affidabile per autenticare la propria identità. A seconda del metodo 2FA impostato, il sistema invierà un codice tramite SMS, vi chiederà di recuperare il codice da un'app di autenticazione o vi chiederà di inserire una chiave di sicurezza per confermare la vostra identità.

Per quanto qualsiasi sistema di autenticazione sia meglio di niente, gli SMS sono il metodo più debole, poiché i numeri di telefono non sono una forma di identificazione sicura. I malintenzionati possono indurre gli operatori di rete a trasferire il vostro numero di telefono sulla loro scheda SIM, in un attacco noto come di SIM Swapping o pagare un altro operatore per

reindirizzare i vostri messaggi di testo al loro numero. In entrambi gli scenari, riceveranno i vostri codici 2FA e potranno accedere ai vostri account senza problemi.

Anche l'utilizzo del proprio numero di telefono come nome utente per i vostri account comporta dei rischi, poiché sono in circolazione molti numeri di telefono riciclati. C'è la possibilità che il numero che avete apparteneva a qualcun altro e se quella persona lo ha utilizzato anche per un account senza modificarlo, l'accesso con quei numeri potrebbe non garantirvi l'accesso al proprio account.

Ecco perché si consiglia di utilizzare metodi di autenticazione più sicuri, come app di autenticazione o chiavi di sicurezza. Le app di autenticazione, come il già citato Google Authenticator, generano un codice univoco ogni 30 secondi associato al vostro account. Le chiavi di sicurezza fisiche agiscono come un'app di autenticazione in forma fisica e richiedono la connessione del dispositivo alla chiave di sicurezza per autenticare la vostra identità.

{jcomments on}

{loadposition user6}