LA NUOVA BUSSOLA QUOTIDIANA
DOMENICA
Direttore Riccardo Cascioli

hacker scatenati

Creare SPID falsi, ecco l'ennesima truffa online

POLITICA 04_04_2025

Ruben Razzante

Quella del doppio SPID è una truffa ormai nota da tempo, ma che in questi ultimi mesi ha ripreso vigore, complici alcune vulnerabilità strutturali del sistema di identità digitale italiano. Con l'inizio della stagione fiscale e l'apertura della dichiarazione dei redditi 730, milioni di cittadini utilizzano lo SPID per accedere ai portali della Pubblica Amministrazione, come l'INPS e l'Agenzia delle Entrate, per verificare la propria

posizione fiscale e ottenere eventuali rimborsi IRPEF.

Proprio questa dinamica viene sfruttata dai cybercriminali, i quali approfittano di un punto debole del sistema: la possibilità di attivare più identità digitali per lo stesso codice fiscale, utilizzando provider differenti e associando email e numeri di telefono diversi. Questo consente ai truffatori di creare un secondo SPID a nome della vittima e di utilizzarlo per compiere operazioni fraudolente. Il meccanismo della truffa si sviluppa in tre fasi. Innanzitutto, i criminali ottengono i dati anagrafici e i documenti di identità della vittima, spesso acquistandoli su marketplace illegali presenti su Telegram, dove carte d'identità e tessere sanitarie vengono vendute a poche decine di euro.

Con queste informazioni, riescono ad attivare un nuovo SPID presso un provider diverso da quello già in uso dalla vittima, utilizzando un'email e un numero di telefono sotto il loro controllo. Una volta ottenuta la seconda identità digitale, i truffatori accedono ai portali istituzionali e modificano l'Iban associato ai pagamenti della Pubblica Amministrazione, dirottando stipendi, pensioni e rimborsi fiscali verso conti correnti a loro riconducibili. La vittima si rende conto del raggiro solo quando il denaro atteso non arriva, ma a quel punto il danno è già stato fatto.

La radice del problema risiede nella struttura federata dello SPID, che permette la coesistenza di più identità digitali valide per lo stesso codice fiscale senza che ci siano controlli incrociati tra i vari provider. Non esiste infatti un sistema centralizzato che verifichi l'esistenza di più SPID associati a un'unica persona, né sono previsti *alert* automatici per segnalare attivazioni sospette. Questa mancanza di supervisione consente ai truffatori di agire indisturbati, sfruttando le falle del sistema per rubare identità digitali e sottrarre somme di denaro considerevoli.

Come detto, la stagione fiscale è il contesto ideale per questi attacchi, perché in questo periodo aumentano le operazioni legate ai rimborsi IRPEF e i criminali possono approfittare della disattenzione o dell'urgenza con cui i cittadini effettuano l'accesso ai servizi online. Inoltre, il mercato nero delle informazioni personali è in continua espansione: attraverso data breach o tecniche di *phishing* mirato, i truffatori riescono ad arricchire i propri database con dati biografici e credenziali di accesso, rendendo ancora più semplice la creazione di identità digitali fittizie. Nonostante il problema sia noto da anni, non sono ancora state implementate soluzioni strutturali per arginarlo.

Alcune possibili misure tecniche potrebbero includere l'obbligo di associare lo SPID a un'email certificata (PEC), la sincronizzazione in tempo reale tra i vari provider per verificare l'esistenza di identità digitali duplicate e l'introduzione di una verifica

biometrica aggiuntiva per le nuove attivazioni. Tuttavia, qualsiasi cambiamento richiede una revisione normativa dell'intera architettura dello SPID, un processo che fino ad oggi non è stato avviato. Nell'attesa di un intervento istituzionale, l'unica possibilità per i cittadini è quella di adottare misure preventive per ridurre il rischio di essere truffati.

L'associazione per la tutela dei consumatori *Codici* sta portando avanti una battaglia per sensibilizzare l'opinione pubblica e spingere le autorità a intervenire con urgenza. Secondo il segretario nazionale di *Codici*, Ivano Giacomelli, il problema principale è che il sistema attuale consente di richiedere più identità digitali con lo stesso codice fiscale rivolgendosi a diversi gestori. Questo apre la porta ai truffatori, che grazie al furto di documenti personali possono attivare SPID fasulli per accedere a servizi pubblici e compiere frodi finanziarie.

***Codici* sottolinea che con lo SPID** è possibile accedere a dati fiscali sensibili, modificare informazioni personali e persino aprire conti bancari o attività a nome della vittima, con conseguenze potenzialmente devastanti. L'associazione chiede ai gestori di identità digitale di rafforzare le misure di sicurezza, ma invita anche i cittadini a prestare maggiore attenzione e a mettere in atto alcuni accorgimenti per proteggersi. Tra le raccomandazioni di *Codici* c'è il controllo periodico sul sito dell'Agenzia per l'Italia Digitale, per verificare quanti SPID risultano attivi a proprio nome. Se si scopre l'esistenza di un'identità digitale non richiesta, è necessario segnalarlo immediatamente alle autorità competenti.

Inoltre, abilitare l'autenticazione a due fattori per accedere ai servizi online può aumentare il livello di sicurezza, rendendo più difficile l'accesso non autorizzato. È fondamentale anche prestare attenzione alla condivisione dei documenti personali: inviare copie di carte d'identità e tessere sanitarie via email o tramite app di messaggistica istantanea può esporre al rischio di furto di dati. Un altro consiglio utile è attivare le notifiche bancarie per monitorare in tempo reale i movimenti di conto e carta di credito, così da accorgersi subito di eventuali transazioni sospette.

La truffa del doppio SPID evidenzia una criticità importante del sistema di identità digitale in Italia: l'assenza di un meccanismo di controllo centralizzato che impedisca la creazione di identità parallele. Questa falla non solo mette a rischio i risparmi dei cittadini, ma mina la fiducia nell'intero ecosistema digitale della Pubblica Amministrazione. Fino a quando non verranno introdotte misure strutturali per prevenire il fenomeno, il rischio di clonazioni di identità continuerà a esistere, con conseguenze sempre più gravi per le vittime. La battaglia di Codici mira proprio a portare il problema all'attenzione delle istituzioni e a sollecitare un intervento concreto

per rendere il sistema SPID più sicuro. Tuttavia, fino a quando le normative non verranno aggiornate, spetta ai cittadini adottare strategie di autotutela per evitare di cadere vittime di questa truffa sempre più diffusa.