La truffa dello Spid: con un falso Sms dell'Inps i cybercriminali riescono a duplicare la tua identità digitale

I criminali informatici sottraggono i documenti delle proprie vittime per creare uno spid alternativo in modo da ottenere rimborsi, bonus e altro

(Fonte: https://www.corriere.it/tecnologia/ 10 aprile 2025)

I cybercriminali ora prendono di mira anche lo **Spid**, il Sistema Pubblico di Identità Digitale. Ovvero quel sistema di autenticazione che permette di accedere ai servizi online della pubblica amministrazione. Lo Spid, però, **non è la refurtiva ma la «chiave»** delle truffe che hanno poi l'obiettivo di sottrarre (al solito) soldi e dati sensibili alle proprie vittime. La **vulnerabilità** - se così possiamo chiamarla - che viene sfruttata è la possibilità di poter **creare più Spid legati alla stessa persona fisica**. Una possibilità ammessa alla normativa vigente.

L'sms «dell'Inps»

Tutto inizia con un Sms o da una mail. Attraverso la tecnica dello «spoofing» i criminali informatici sono in grado di inviare questi messaggi fraudolenti facendoli apparire come ufficiali: appare, come mittente, un nome ben noto all'utente, nonostante questo sia invece un inganno. **Nel caso di questa truffa, appare come mittente l'Inps.** Il falso Sms invita gli utenti a collegarsi ad un sito falso, che replica esattamente le fattezze del sito originale dell'Inps, come riporta il sito della Polizia Postale. Solo nel mese di marzo, Il **CERT-AGID** (Agenzia per l'Italia Digitale) ha individuato **33 falsi domini Inps**. Nel sito falso viene infatti richiesto di inserire una serie di informazioni personali per aggiornare il proprio profilo: **dati anagrafici, Iban, buste paga**, a volte

anche un **selfie**. E viene anche chiesto di caricare una copia digitale dei propri **documenti personali**.
Sono tutte informazioni utili a creare un nuovo o un secondo Spid. Compreso il selfie, o il breve video, a volte richiesto dagli Identiy Provider - le società incaricate dallo stato per creare i profili di identità digitale - per verificare se la persona che sta richiedendo la nuova utenza sia la stessa che compare nei documenti. Per quanto riguarda l'Iban o le buste paga, questi servono **più semplicemente per risalire ai dati di pagamento o delle carte di credito o ancora della propria banca per sottrarre denaro**.

Cosa può fare un malintenzionato con uno Spid
Le operazioni che si possono portare a termine dopo aver effettuato l'accesso ai vari servizi con lo Spid sono diverse e anche dannose. Ad esempio **è possibile accedere al Cassetto Fiscale dell'Agenzia delle Entrate e cambiare Iban**. In questo modo il truffatore può così appropriarsi di rimborsi e altro che spetta al legittimo proprietario dell'identità creata. Ma potrebbero anche venir richiesti bonus, sussidi, pensioni anticipate o **NASpI** a nome della vittima.

Come proteggersi
Le modalità per proteggersi non sono molte, ma sono semplici da ricordare. Bisogna infatti attivare **l'autenticazione a due fattori** sui vari servizi, in modo da ricevere un Sms o dalle app **Authenticator** un codice utile ad accedere ai propri spazi digitali personali in sicurezza. Inoltre, è bene verificare di aver attivato un servizio di notifica ogni qualvolta avviene un'operazione bancaria. Se si scopre di essere vittima di una truffa simile, bisogna **sporgere denuncia alla Polizia Postale e richiedere un nuovo documento.** Per proteggersi bisogna ricordarsi che **l'Inps non invia Sms**, ad ogni modo, nel caso, bisogna accertarsi che in qualsiasi caso, per dirigersi sul sito dell'Inps, bisogna collegarsi in autonomia sul sito www.inps.it digitando l'indirizzo esatto nella barra degli indirizzi del proprio browser.