Digeat N.6 - 19 Giugno 2025

Doppio SPID: tra truffa e realtà l’inganno è una fake news

Di Claudio Anastasio

Abstract

Autorevoli divulgatori ed esperti di cybersecurity ci spiegano i rischi di truffa portati dal fenomeno del “doppio SPID a tua insaputa”. In questo articolo andremo ad analizzare nella pratica come questo tipo di truffa sia altamente improbabile, se non impossibile, da attuare. Ciò mette in luce il costante pericolo della disinformazione che non risparmia nemmeno gli addetti ai lavori, coloro di cui ci fidiamo e a cui ci affidiamo per “navigare” in sicurezza con gli strumenti digitali, con il rischio anche per essi di venire travolti da una superficiale analisi tecnica (tecnicamente possibile), ma che diventa, a ben guardare, impossibile nella pratica. Il concetto di “sicurezza” non può limitarsi solo ad evidenze tecniche, ma deve permeare in tutti gli aspetti d’uso del processo sottostante, altrimenti si ottiene l’effetto contrario di un allarmismo generalizzato e ingiustificato che in astratto porterebbe, come unica soluzione, tecnicamente vera ed efficace, a “staccare” la spina per non connettersi mai più in rete. Non può essere questo l’approccio metodico corretto per la mitigazione e prevenzione dei rischi nel mondo digitale senza aver analizzato quanto il rischio teorico emergente sia poi impraticabile nella realtà.

Indice

- Allarme “doppio spid”: verità, falsità e necessaria chiarezza per i cittadini
- Il minuzioso processo di identificazione: un baluardo contro le frodi
- L’inefficacia economica e logistica di un attacco massivo
- La “fake news” come mistificazione della realtà

Allarme “doppio spid”: verità, falsità e necessaria chiarezza per i cittadini

Nelle scorse settimane, un’eco di preoccupazione si è diffusa in rete tra gli utenti del Sistema Pubblico per l’Identità Digitale (**SPID**). La notizia di una presunta falla nel sistema, che teoricamente consentirebbe l’attivazione di un “doppio SPID” da parte di individui con intenti malevoli, ha sollevato timori riguardo alla sicurezza della propria identità digitale di Stato.
L’ipotesi, seppur remota, di una **clonazione dell’identità** per accedere a servizi esclusivi e personalissimi come l’accesso all’**Agenzia delle Entrate** per manipolare i dati bancari nei rimborsi tributari, ha generato un comprensibile **senso di allarme**.
Il primo allarme diffuso in rete è stato proposto dall’ottimo divulgatore **Marco Camisani Calzolari**, esperto in materia e ripreso dalla trasmissione “**Striscia la Notizia**”, finendo anche lui per primo vittima della “**fake news**” con questo video del 3 aprile 2025. In ultimo, l’allarme diffuso dal Prof. **Matteo Flora**, anche lui vittima della “fake news”, con questo ulteriore video del 9 giugno 2025.

Ciò che sorprende in questa vicenda è che la diffusione di tale scenario, per fortuna altamente improbabile, sia avvenuta anche ad opera di professionisti che, in quanto esperti del settore,

posseggono una conoscenza approfondita dei meccanismi che regolano l'attivazione e la gestione delle identità **SPID**.

Proprio la loro familiarità con i processi sottostanti dovrebbe far comprendere quanto sia arduo, se non impossibile, replicare un'identità digitale in modo fraudolento.

La radice della preoccupazione sembra risiedere, piuttosto, nella reale e concreta minaccia rappresentata dalla circolazione nel "dark web" di ingenti quantità di dati personali e copie di documenti d'identità di cittadini italiani, frutto di attacchi informatici e "data breach" pregressi.

> È dunque impellente **fare chiarezza sul funzionamento** intrinseco del processo di attivazione di **SPID** e **valutare con obiettività** quanto il sistema sia effettivamente sicuro e resistente a tentativi di clonazione.

Sia che un cittadino scelga la via dell'attivazione autonoma, avvalendosi di una firma elettronica qualificata già in suo possesso, sia che opti per l'assistenza di un operatore, entrambi **i percorsi sono caratterizzati da un passaggio fondamentale e imprescindibile: la verifica rigorosa dell'identità del richiedente da parte di un funzionario**. Questa fase non si limita a una semplice formalità burocratica, ma implica un investimento significativo in termini di tempo e un costo stimato per il richiedente di identità digitale intorno ai 20 euro per ogni singola attivazione, ovvero duplicazione di **SPID**.

Il minuzioso processo di identificazione: un baluardo contro le frodi

La procedura di identificazione prevede la presentazione fisica (o tramite sistemi proprietari di video identificazione con elevati standard di sicurezza e brevetti industriali) di un documento d'identità valido (carta d'identità, passaporto o patente di guida) e della tessera sanitaria. A ciò si aggiunge un riscontro visivo e, in molti casi, una registrazione video del volto della persona che sta richiedendo l'attivazione, al fine di confrontarlo con la fotografia presente sul documento.

> Il mero possesso di dati anagrafici e scansioni di documenti rubati, sebbene rappresenti un rischio per la privacy e possa essere utilizzato per altre forme di truffa online, non è di per sé sufficiente per superare queste barriere di sicurezza e ottenere un nuovo **SPID** a nome di un'altra persona.
> Il potenziale truffatore si troverebbe di fronte a una serie di sfide operative di notevole complessità.

In primo luogo, dovrebbe produrre una replica fisica del documento d'identità della vittima, un'operazione che richiede competenze tecniche avanzate e l'accesso ad attrezzature specifiche per la stampa e la laminazione di documenti con caratteristiche di sicurezza sofisticate. **Non basterebbe una semplice fotocopia modificata**; la contraffazione dovrebbe essere sufficientemente convincente da superare un controllo visivo da parte di un operatore addestrato.

Parallelamente, **la creazione di una tessera sanitaria falsa rappresenterebbe un ulteriore ostacolo.** Questo documento, apparentemente semplice, presenta codici di controllo sul retro la cui generazione e riproduzione fedele sono estremamente complesse e richiedono una conoscenza approfondita degli algoritmi utilizzati. **Tali codici sono pensati proprio come un ulteriore livello di verifica per la convalida dell'autenticità del documento** e sono praticamente impossibili da dissimulare senza le informazioni e gli strumenti appropriati.

Oltre alla produzione fisica di documenti falsificati, **il malintenzionato dovrebbe anche superare la fase di prenotazione dell'appuntamento con l'operatore incaricato dell'identificazione**. Questo

processo, che normalmente richiede alcuni giorni di attesa (dai 2 ai 4 giorni), introduce un ulteriore elemento di rischio e di esposizione per il truffatore. Infine, **non va dimenticato il costo di circa 20 euro per ogni tentativo di attivazione**, una spesa che, come vedremo, rende l'operazione su larga scala economicamente insostenibile.

L'inefficacia economica e logistica di un attacco massivo

Considerando lo scenario ipotizzato, in cui **l'obiettivo finale della truffa sarebbe l'accesso al portale** dell'**Agenzia delle Entrate** per modificare l'IBAN associato a eventuali rimborsi IRPEF, è cruciale analizzare la sua potenziale efficacia in termini di costi e benefici.

> Statisticamente, solo una porzione residuale della popolazione italiana ha diritto a ricevere rimborsi IRPEF ogni anno. Pertanto, per ottenere un guadagno significativo, la truffa dovrebbe essere condotta su un numero estremamente elevato di identità false o duplicate, seguendo un principio di "attacco massivo": colpire un gran numero di bersagli per ottenere un piccolissimo risultato da ciascuno.

Tuttavia, se si considerano i costi diretti (circa 20 euro per ogni tentativo di attivazione di SPID) e il tempo necessario per ogni singola operazione (in media, considerando la prenotazione e l'appuntamento, almeno 3 giorni), anche immaginando un attacco mirato su un campione di 1.000 persone, i numeri diventano scoraggianti per il potenziale truffatore. Si parlerebbe di un investimento di 3.000 giorni di "lavoro" e una spesa di 20.000 euro, con l'incognita tutt'altro che trascurabile che tra queste 1.000 persone non vi sia alcun soggetto beneficiario di un rimborso IRPEF, che peraltro, nella maggior parte dei casi, è di importo inferiore ai 1.000 euro.

> Estendendo l'analisi a un campione di 10.000 persone, la situazione diventa ancora più proibitiva: sarebbero necessari circa 82 anni di "lavoro/uomo" e un esborso di 200.000 euro per il malintenzionato, il tutto con la flebile speranza di ottenere un profitto marginale attraverso i rimborsi IRPEF. È evidente come, da una prospettiva di analisi del rischio/beneficio, un'operazione di tale portata si configuri come impraticabile e antieconomica.

Anche ipotizzando uno scenario in cui il processo di produzione dei documenti falsi e di accesso ai sistemi venisse automatizzato con investimenti significativi in attrezzature e software sofisticati, **il fattore umano rappresentato dalla verifica dell'operatore rimane un collo di bottiglia insormontabile**.

Inoltre, un'operazione di "clonazione" su vasta scala richiederebbe la complicità di un numero considerevole di migliaia di persone disposte a prestare il proprio volto per sostituire quello presente sui documenti contraffatti, mantenendo una coerenza credibile con il sesso e l'età dei dati anagrafici originali. Reclutare e coordinare un tale numero di complici rappresenterebbe un'ulteriore sfida logistica e un aumento esponenziale del rischio di essere scoperti, altamente inverosimile di impegno, considerando anche che i fornitori di **SPID** possono verificare lo stesso volto su più identità in rilascio ed in maniera automatizzata, vanificando lo scopo di "doppio SPID" simulato dal truffatore.

La "fake news" come mistificazione della realtà

Autorevoli esperti in sociologia e comunicazione digitale, tra tutti il Professore Ordinario Dott.ssa **Nicoletta Vittadini** dell'Università Cattolica del Sacro Cuore di Milano o il Professore Associato

Toscano Emanuele dell'Università Guglielmo Marconi di Roma, hanno contribuito a chiarire il significato della definizione di "**fake news**" che non si limita alla sola e semplice diffusione di informazioni completamente false. Rientrano in questa categoria anche notizie che, pur contenendo elementi di verità tecnica (come la teorica possibilità di una duplicazione), vengono presentate in modo da generare allarmismo e preoccupazione ingiustificati, omettendo o mistificando la reale praticabilità e la probabilità di tali scenari.

In questo contesto, la notizia "allarmistica" relativa alla truffa del "doppio SPID" si configura come un esempio emblematico di come anche una potenziale vulnerabilità teorica, se analizzata nel contesto dei reali processi operativi e dei costi-benefici per i criminali, si riveli di fatto una "**fake news**" nel senso più ampio del termine. Essa genera un'ansia immotivata tra i cittadini, basandosi su una possibilità remota e su una profonda sottovalutazione dei meccanismi di sicurezza implementati nel sistema **SPID**.

> È fondamentale che i cittadini ricevano informazioni chiare e accurate riguardo alla sicurezza dei propri strumenti digitali offerti dallo Stato. Sensibilizzare sui reali rischi legati alla circolazione dei dati personali online è cruciale, ma è altrettanto importante evitare la diffusione di allarmismi infondati che minano la fiducia in sistemi sicuri ed efficienti come lo **SPID**, ormai pilastro fondamentale per l'accesso ai servizi della Pubblica Amministrazione.

La vera sfida è educare all'utilizzo consapevole degli strumenti digitali e alla protezione dei propri dati personali, contrastando efficacemente le vere minacce informatiche senza cadere nella trappola di "**fake news**" che distorcono la realtà e generano paure ingiustificate.