

## La nuova truffa che chiede di aggiornare lo Spid: come funziona e perché è pericolosa

Segnalata una nuova campagna di phishing. Le email fraudolente rimandano a una pagina su Google Sites che imita un portale ufficiale e ruba dati personali e bancari  
(Fonte: <https://www.corriere.it/> 26 gennaio 2026)



Dopo la truffa del rinnovo della [tessera sanitaria](#), ora tocca allo Spid. Il [Cert-AgID](#) (Agenzia per l'Italia Digitale) ha segnalato una nuova campagna di phishing particolarmente insidiosa, che sfrutta Google Sites per ingannare gli utenti.

### Come funziona l'attacco

Tutto inizia con un'email che chiede di verificare la propria identità digitale o confermare i dati Spid. Il link porta a una pagina ospitata su Google Sites – un dettaglio che rende la truffa più credibile, perché il dominio google.com appare affidabile.

La pagina replica l'aspetto di un portale Spid legittimo, con i loghi di AgID e del Dipartimento per la Trasformazione Digitale. L'utente viene invitato a compilare un modulo – e senza saperlo consegna i propri dati ai truffatori.

The screenshot shows the SPID registration interface. At the top, there's a navigation bar with links for Cittadini, Aziende, Pubbliche Amministrazioni, social media integration (Seguici su Facebook), a search bar (Cerca), and information about SPID. The main area is a form titled "Registrazione" (Registration) with fields for "Nome e cognome completo" (Full name), "Data di nascita" (Birth date), "Indirizzo" (Address), "CAP" (ZIP code), "Email" (Email), and "Il tuo numero di telefono" (Your phone number). There's also a note at the bottom left: "Salvo il vostro consenso, i vostri dati saranno trattati in base alle norme sulla Privacy".

## Quali dati vengono rubati

La pagina chiede generalità, indirizzo di residenza, email, numero di telefono, Iban e istituto bancario. Con queste informazioni in mano, i criminali possono fare danni seri: creare un secondo Spid a nome della vittima, accedere a servizi pubblici, dirottare rimborsi e stipendi, compiere acquisti fraudolenti. Il furto di identità digitale apre scenari preoccupanti, dalla sottoscrizione di contratti alla richiesta di finanziamenti.

## Come proteggersi

Le regole sono sempre le stesse, ma vale la pena ripeterle. **Mai cliccare sui link nelle email che chiedono di verificare credenziali:** meglio digitare direttamente l'indirizzo del proprio provider nella barra del browser. **Controllare sempre l'Url della pagina:** anche se appare "google.com", non significa che il contenuto sia sicuro. E ricordare che nessun gestore Spid chiede mai conferma dei dati via email.

Il Cert-AgID ha già avviato le procedure per chiudere la pagina malevola, ma campagne simili possono ricomparire in qualsiasi momento.