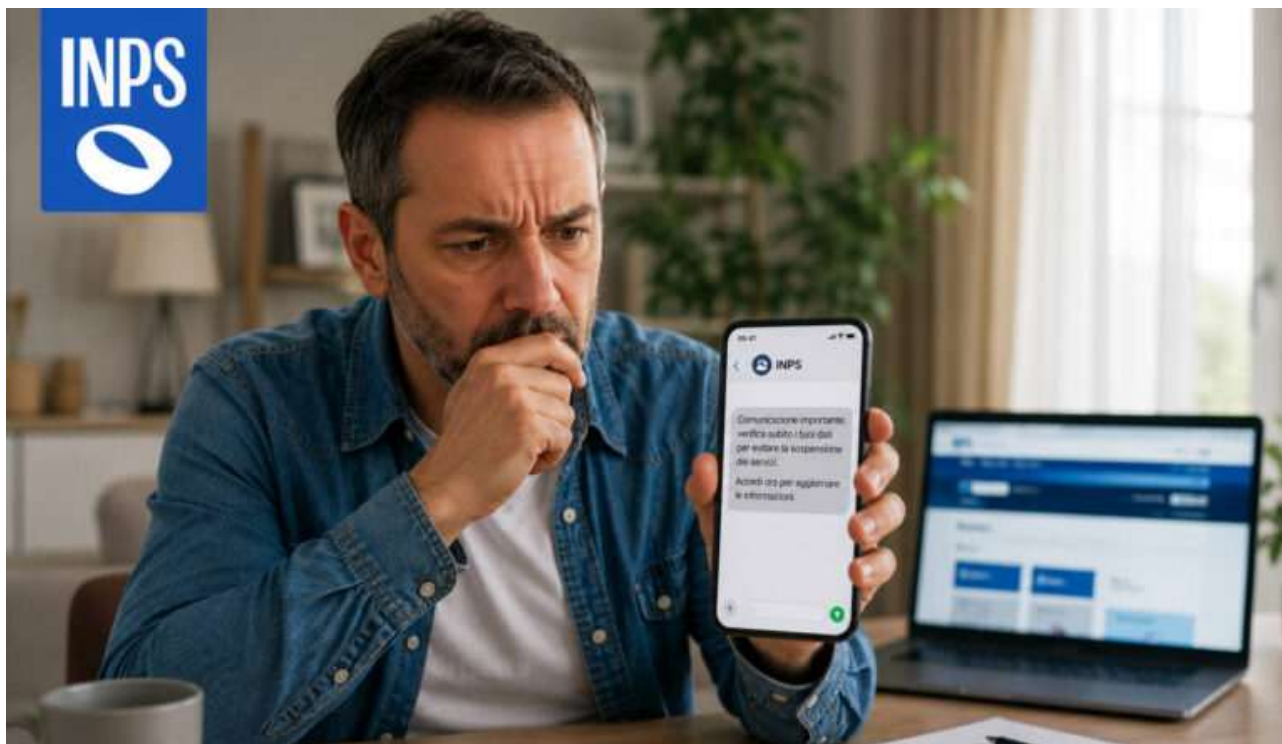


Hai ricevuto un SMS dall'INPS? Attenzione, la nuova truffa è più difficile da riconoscere

Nuova truffa INPS via SMS: lo smishing diventa più credibile grazie all'AI. Ecco come riconoscere i messaggi falsi e proteggere i propri dati.

(Fonte: <https://www.lavoroediritti.com/> 17 agosto 2026)



Negli ultimi giorni è stata segnalata una **nuova impennata delle truffe via SMS** che utilizzano il **nome dell'INPS** per convincere i cittadini a fornire dati personali e documenti. La novità, questa volta, è particolarmente insidiosa: i criminali informatici hanno introdotto anche **un sistema di verifica basato sull'intelligenza artificiale**, rendendo il percorso predisposto per la vittima più sofisticato e credibile.

A mettere in guardia i cittadini è lo stesso INPS, con una comunicazione pubblicata il 14 agosto 2026. La nuova campagna di **smishing a tema INPS** è stata osservata dal CERT-AgID l'11 agosto e riprende uno schema già utilizzato in precedenti tentativi di frode, ma con strumenti più evoluti. Il pericolo non riguarda soltanto password o coordinate bancarie: attraverso il falso sito possono essere richiesti **dati anagrafici, documenti di identità, buste paga, CUD e persino un selfie**. Informazioni che, una volta finite nelle mani dei truffatori, possono essere utilizzate per ulteriori frodi e tentativi di furto d'identità.

Cos'è lo smishing e perché bisogna fare attenzione agli SMS INPS

Con il termine **smishing** si indica sostanzialmente una forma di **phishing** realizzata attraverso gli SMS. Il meccanismo punta a sfruttare la fiducia che il destinatario ripone nel soggetto apparentemente indicato come mittente del messaggio.

Nel caso delle campagne segnalate dall'Istituto, i criminali utilizzano **nome, logo e identità grafica dell'INPS**, cercando quindi di far apparire la comunicazione come autentica.

Il messaggio invita generalmente il cittadino a compiere un'azione apparentemente urgente o necessaria: verificare i propri dati, controllare una posizione, confermare alcune informazioni oppure intervenire per evitare problemi nell'erogazione di un servizio.

L'obiettivo è però un altro: **convincere l'utente a premere sul link contenuto nell'SMS**.

Ed è proprio questo uno degli elementi che deve far scattare immediatamente il campanello d'allarme.

Come funziona la nuova truffa INPS segnalata ad agosto

La nuova campagna individuata dal CERT-AgID utilizza come pretesto la necessità di **verificare i dati personali per garantire la continuità nell'erogazione dei servizi**.

Il collegamento inserito nell'SMS porta a una pagina contraffatta costruita per assomigliare il più possibile al vero portale dell'INPS.

Una volta entrata nel sito falso, la vittima viene accompagnata attraverso **un percorso guidato composto da cinque fasi**. Durante la procedura vengono richieste progressivamente numerose informazioni personali.

Tra i dati e i documenti che possono essere richiesti figurano:

- dati anagrafici;
- documenti d'identità;
- buste paga;
- CUD;
- un selfie.

La presenza di una procedura articolata e apparentemente professionale può contribuire a dare alla vittima l'impressione di trovarsi realmente davanti a un servizio istituzionale.

La novità dell'intelligenza artificiale rende la truffa più credibile

L'elemento che distingue questa campagna dalle precedenti è proprio **l'introduzione, per la prima volta, di un sistema di verifica basato sull'intelligenza artificiale**.

Secondo quanto riportato dall'INPS, questa caratteristica contribuisce a rendere il tentativo di frode **ancora più credibile agli occhi delle potenziali vittime**.

È un passaggio importante anche dal punto di vista della sicurezza informatica: non bisogna più pensare alle truffe online soltanto come a pagine improvvisate, piene di errori grammaticali o palesemente diverse dai siti ufficiali.

Una procedura ben costruita, una grafica convincente o la presenza di sistemi tecnologicamente avanzati **non sono una garanzia di autenticità**.

Per questo diventa molto più efficace concentrarsi su una regola semplice: verificare **come siamo arrivati su quella pagina**, anziché giudicarne l'affidabilità soltanto dall'aspetto.

Non è la prima campagna di smishing (phishing) che sfrutta il nome dell'INPS

La nuova offensiva si inserisce in una serie di campagne già rilevate nei mesi precedenti.

A luglio, ricorda l'Istituto, il CERT-AgID aveva individuato altri SMS fraudolenti che utilizzavano nome, logo e grafica dell'INPS per sottrarre **dati personali e informazioni relative alle carte di pagamento**.

In uno dei casi il collegamento portava a un sito che imitava addirittura la sezione **“Visualizzazione indebiti”** del portale INPS, cioè il servizio attraverso il quale i cittadini possono verificare la propria posizione debitoria.

Cambiano quindi il messaggio, gli importi indicati o la motivazione utilizzata per attirare l'utente, ma il meccanismo rimane sostanzialmente lo stesso: **creare un senso di urgenza, portare il cittadino su un sito contraffatto e convincerlo a consegnare informazioni riservate**.

Come riconoscere un falso SMS dell'INPS

Su questo punto l'indicazione dell'Istituto è particolarmente chiara e può diventare la regola principale da ricordare.

L'INPS non invia e-mail o SMS contenenti link sui quali cliccare per confermare i propri dati o per ricevere rimborsi.

Se arriva quindi un SMS che chiede di aprire un collegamento per aggiornare informazioni personali, confermare un rimborso o completare procedure simili, bisogna considerarlo sospetto.

L'Istituto precisa che le uniche e-mail contenenti link inviate dall'INPS sono quelle relative alle **indagini sulla soddisfazione degli utenti**. Anche in questi casi, però, non vengono richiesti dati bancari o documenti.

Attenzione anche all'indirizzo del sito: INPS.it può essere imitato

Un'altra verifica fondamentale riguarda l'indirizzo visualizzato nel browser.

Il sito istituzionale dell'Istituto è www.inps.it e l'INPS raccomanda di controllare che l'indirizzo termini correttamente con **“.inps.it”**.

I criminali possono infatti registrare domini contenenti parole estremamente simili a INPS, approfittando magari di una semplice inversione delle lettere.

Nel documento l'Istituto cita, a titolo di esempio, denominazioni ingannevoli come **“insp”, “ipns” o “inpis”**.

A una lettura veloce, soprattutto sul piccolo schermo di uno smartphone, la differenza può facilmente sfuggire.

Cosa fare quando arriva un SMS INPS sospetto

La soluzione più sicura è anche la più semplice: **non utilizzare il link ricevuto nel messaggio**.

Se l'SMS sostiene che esiste una comunicazione, un pagamento, un rimborso o un problema relativo alla propria posizione, è preferibile chiudere il messaggio e raggiungere autonomamente il portale INPS, digitando l'indirizzo ufficiale nel browser o utilizzando i canali istituzionali.

L'INPS invita inoltre a confrontare le comunicazioni sospette con gli esempi contenuti nel proprio **vademecum antitruffa**.

Questa precauzione diventa ancora più importante perché il blocco di un sito fraudolento non mette definitivamente fine alla campagna.

L'Istituto segnala infatti tempestivamente SMS e domini malevoli affinché possano essere bloccati, ma i criminali possono **aprire nuovi domini, riattivare quelli utilizzati in precedenza e modificare contemporaneamente il testo dei messaggi**.

Ho cliccato sul link: cosa devo fare?

Cliccare accidentalmente sul collegamento non significa necessariamente aver già consegnato i propri dati ai truffatori. La situazione diventa più delicata quando sul sito contraffatto sono state inserite informazioni personali, credenziali, documenti oppure dati di pagamento.

In questo caso è prudente **interrompere immediatamente qualsiasi ulteriore operazione**, non inviare altri documenti e non effettuare eventuali pagamenti richiesti.

Se sono state comunicate credenziali utilizzate anche su altri servizi, è opportuno cambiarle rapidamente; se invece sono stati forniti dati di una carta o di un conto, è consigliabile contattare il proprio istituto di pagamento attraverso i canali ufficiali.

Particolare attenzione merita la consegna di **documento d'identità e selfie**, proprio perché la nuova campagna segnalata dall'INPS può richiedere entrambi. In presenza di una possibile sottrazione di dati e documenti personali è opportuno conservare SMS, indirizzo del sito e ogni altra prova disponibile e valutare una segnalazione alle autorità competenti.

La regola più semplice per evitare le truffe INPS

Con campagne sempre più sofisticate, distinguere un sito autentico da una copia può diventare difficile anche per chi ha una certa dimestichezza con Internet.

Per il cittadino medio è quindi molto più utile adottare una regola preventiva: **un SMS non deve diventare la porta d'ingresso al proprio profilo INPS**.

Quando si riceve una comunicazione che sembra provenire dall'Istituto, soprattutto se contiene richieste urgenti relative a dati personali, rimborsi, pagamenti o prestazioni, è meglio non seguire il collegamento proposto.

Si può invece aprire autonomamente il portale istituzionale e verificare da lì la propria posizione. La grafica di un sito si può copiare, il logo INPS può essere riprodotto e, come dimostra la nuova campagna, persino sistemi basati sull'intelligenza artificiale possono essere utilizzati per rendere più convincente una frode. **L'indirizzo ufficiale e l'accesso diretto ai servizi INPS restano quindi la verifica più importante da fare prima di fornire qualsiasi informazione personale.**