Gentile utente,

ti informiamo che stanno aumentando le truffe online che usano il nome dell'INPS per rubare dati personali e finanziari. Queste truffe avvengono principalmente attraverso SMS o e-mail false (chiamate phishing o smishing), che sembrano inviate dall'INPS.

Questi messaggi invitano a cliccare su link non ufficiali per verificare, confermare o integrare i propri dati per continuare a percepire prestazioni INPS, ottenere presunti rimborsi o altre motivazioni simili.

Non farlo! È una trappola per rubare le tue informazioni personali.

Se fornisci i tuoi dati su tali siti, i truffatori possono:

- richiedere prestiti a tuo nome;
- aprire conti correnti fraudolenti;
- dirottare i pagamenti delle tue prestazioni;
- attivare, a tua insaputa, credenziali SPID a tuo nome;
- accedere ai servizi della Pubblica Amministrazione fingendo di essere te.

Fai quindi attenzione a qualsiasi messaggio SMS o e-mail, apparentemente inviato a nome di INPS, che ti invita a cliccare su link in essi riportati, e ricorda che:

- l'INPS non invia mai e-mail o SMS con link per confermare dati o ricevere rimborsi ma invitiamo sempre gli utenti ad accedere sempre e solo al sito istituzionale www.inps.it;
- le uniche e-mail con link che INPS invia sono quelle per le indagini sulla soddisfazione degli utenti, ma non ti chiederanno mai dati bancari o documenti;
- l'unico sito ufficiale dell'INPS è www.inps.it. Controlla sempre che l'indirizzo del sito che stai visitando termini con ".inps.it", perché possono venire creati domini con denominazioni simili e ingannevoli (es. insp, ipns, inpis e simili);
- se hai dubbi, consulta il vademecum anti-truffe sul sito INPS, dove trovi esempi di messaggi falsi e consigli su come difenderti.

Se ricevi un messaggio sospetto, non cliccare sul link e segnalalo subito!