Phishing fiscale e previdenziale: falsi rimborsi IRPEF, furto delle credenziali CIE e PEC contraffatte. Come riconoscere le comunicazioni fraudolente

Le nuove segnalazioni dell'Agenzia delle entrate e dell'Agenzia delle entrate-Riscossione. Dall'Inps le indicazioni per riconoscere le truffe e proteggere i propri dati personali, bancari e le credenziali di accesso ai servizi digitali della Pubblica Amministrazione.

False comunicazioni relative a rimborsi IRPEF, pagine web che riproducono il sistema di autenticazione mediante Carta di Identità Elettronica (CIE), messaggi di posta elettronica certificata apparentemente provenienti dall'Agente della riscossione e applicazioni contraffatte dell'Inps. Sono solo alcune delle modalità utilizzate nelle campagne fraudolente recentemente segnalate dalle amministrazioni fiscali e previdenziali.

Con gli avvisi del **26** e del **27 novembre 2026**, l'Agenzia delle Entrate ha richiamato l'attenzione dei contribuenti su due nuove campagne di *phishing* finalizzate, rispettivamente, alla sottrazione di informazioni finanziarie e delle credenziali dell'identità digitale. A queste segnalazioni si aggiungono quella **dell'Agenzia delle entrate-Riscossione del 10 novembre 2026**, riguardante l'invio di false PEC, e le indicazioni diffuse dall'Inps sulle attività di contrasto

alle truffe *online*.

Il tratto comune delle diverse iniziative fraudolente è l'utilizzo indebito del nome, dei loghi e dell'identità grafica degli enti pubblici per indurre i destinatari a ritenere attendibili richieste di informazioni riservate o di pagamento.

Agenzia delle Entrate: false richieste di rimborso IRPEF

Con l'**avviso del 26 novembre 2026**, l'Agenzia delle entrate ha reso nota l'individuazione di una campagna di *phishing* realizzata attraverso e-mail, SMS e altri messaggi contenenti collegamenti a pagine web fraudolente, estranee ai domini istituzionali dell'Amministrazione finanziaria.

La truffa fa leva sulla prospettiva di ottenere un rimborso IRPEF. Il contribuente viene indirizzato verso pagine che simulano una procedura di verifica e liquidazione del rimborso, fino alla richiesta di informazioni personali e finanziarie.

Le schermate riprodotte nell'avviso dell'Agenzia mostrano come l'impiego di elementi grafici istituzionali e di informazioni apparentemente riconducibili a una pratica fiscale possa rendere credibile una procedura del tutto inesistente.

L'obiettivo della campagna è acquisire informazioni utilizzabili per effettuare operazioni fraudolente e pagamenti non autorizzati.

L'Agenzia raccomanda di verificare l'indirizzo delle pagine web prima di inserire qualsiasi informazione, di accedere ai servizi fiscali esclusivamente attraverso i canali

istituzionali e di diffidare delle comunicazioni che sollecitano adempimenti urgenti, prospettando la perdita del diritto al rimborso in caso di mancata risposta.

Falso accesso tramite CIE: a rischio le credenziali dell'identità digitale

Con il successivo **avviso del 27 novembre 2026,** l'Agenzia delle entrate ha segnalato una campagna fraudolenta che sfrutta il sistema di autenticazione mediante Carta di Identità Elettronica.

La pagina contraffatta riproduce l'interfaccia di autenticazione CIE di livello 2 e utilizza indebitamente i loghi del Ministero dell'Interno e della Carta di Identità Elettronica, allo scopo di indurre l'utente a comunicare le proprie credenziali.

In questo caso, il rischio non è circoscritto all'accesso ai servizi dell'Amministrazione finanziaria. La sottrazione delle credenziali dell'identità digitale può infatti consentire a soggetti non autorizzati di accedere anche ad altri servizi telematici della Pubblica Amministrazione e dei soggetti privati convenzionati, acquisire informazioni personali e fiscali riservate e compiere ulteriori attività fraudolente.

L'Agenzia delle Entrate, dichiarandosi estranea a entrambe le campagne, invita i contribuenti a verificare l'autenticità delle comunicazioni ricevute consultando la sezione dedicata al phishing del proprio sito istituzionale o rivolgendosi ai recapiti ufficiali e agli uffici territorialmente competenti.

Agenzia delle entrate-Riscossione: attenzione anche alle false PEC

I tentativi di *phishing* interessano anche la posta elettronica certificata.

Con l'**avviso del 10 novembre 2026**, l'Agenzia delle entrate-Riscossione ha segnalato a cittadini e imprese l'invio di messaggi PEC provenienti da indirizzi simili a quelli ufficiali, diretti a ottenere informazioni personali o a richiedere pagamenti non dovuti.

L'Agente della riscossione ricorda che l'unico dominio di posta elettronica certificata ufficialmente utilizzato per l'invio delle proprie comunicazioni è:

@pec.agenziariscossione.gov.it

La ricezione di un messaggio tramite PEC non costituisce, di per sé, garanzia della sua effettiva provenienza dall'ente indicato nel messaggio.

Anche in presenza di comunicazioni ricevute mediante posta elettronica certificata, occorre pertanto verificare l'indirizzo del mittente prima di aprire allegati, utilizzare collegamenti ipertestuali o fornire informazioni riservate.

In caso di dubbio, l'Agenzia delle entrate-Riscossione invita a non dare seguito alle richieste sospette e a rivolgersi esclusivamente ai propri canali istituzionali.

Inps: dalle false applicazioni alle truffe

mediante intelligenza artificiale

Con una **notizia pubblicata il 26 novembre 2026**, l'Inps ha illustrato le attività svolte per individuare e contrastare le frodi digitali che utilizzano indebitamente il nome e il logo dell'Istituto.

Tra i casi segnalati figura quello di una falsa pagina per il *download* dell'applicazione Inps Mobile, individuata l'11 novembre 2026 grazie alla collaborazione tra l'Istituto e il CERT-AgID.

L'Inps richiama inoltre una campagna di *smishing* (*phishing* realizzato mediante SMS), individuata nell'agosto 2026, nella quale venivano impiegati sistemi di intelligenza artificiale per esaminare i documenti acquisiti dalle vittime. Attraverso una falsa procedura di identificazione, agli utenti veniva richiesto di trasmettere documenti d'identità, buste paga e immagini personali.

L'utilizzo di tali tecnologie può contribuire a rendere più verosimili le procedure fraudolente, simulando le ordinarie operazioni di verifica dell'identità.

L'attività di contrasto dell'Inps comprende il monitoraggio dei domini sospetti, dei siti contraffatti e dei profili social che utilizzano impropriamente i riferimenti all'Istituto, nonché l'attivazione delle procedure per la loro rimozione, in collaborazione con il **CERT-AgID** e l'Agenzia per la Cybersicurezza Nazionale (ACN).

Il ***vademecum* antitruffe dell'Inps**: come riconoscere una comunicazione autentica

Per consentire agli utenti di distinguere le comunicazioni istituzionali da quelle fraudolente, l'Inps ha predisposto un apposito vademecum, periodicamente aggiornato, nel quale

vengono illustrate le diverse tipologie di truffa e le modalità per difendersi.

In particolare, l'Istituto previdenziale precisa che:

- non invia e-mail o SMS contenenti collegamenti attraverso i quali ottenere rimborsi;
- non richiede documenti tramite e-mail o telefono;
- non invia propri incaricati presso le abitazioni degli utenti per effettuare accertamenti;
- non richiede dati bancari mediante e-mail o SMS;
- può inviare e-mail nell'ambito di indagini sulla soddisfazione degli utenti (*Customer Experience*), senza richiedere dati personali.

Il ***vademecum*** mette inoltre in guardia dalle telefonate di falsi operatori, dalle visite di presunti funzionari e dalle offerte di finanziamenti o agevolazioni provenienti da soggetti che si dichiarano, senza esserlo, convenzionati con l'Inps.

La sottrazione dei dati personali e dei documenti identificativi può essere funzionale non soltanto all'accesso abusivo ai servizi telematici, ma anche all'attivazione fraudolenta di identità SPID, all'apertura di conti correnti e alla richiesta di prestiti o finanziamenti a nome delle vittime.

Le precauzioni da adottare, anche negli studi professionali

Le segnalazioni delle amministrazioni fiscali e previdenziali suggeriscono l'adozione di alcune cautele anche nell'organizzazione degli studi professionali, che gestiscono quotidianamente comunicazioni telematiche,

documentazione fiscale e informazioni riservate dei propri assistiti.

In particolare, è opportuno:

- **verificare l’effettivo indirizzo del mittente**, senza limitarsi alla denominazione visualizzata nel messaggio;
- **controllare il dominio del sito web** prima di inserire dati personali o credenziali;
- **accedere direttamente ai portali istituzionali**, evitando di utilizzare i collegamenti presenti nelle comunicazioni sospette;
- **non aprire allegati inattesi e non installare applicazioni attraverso collegamenti ricevuti via SMS o e-mail**;
- non comunicare *password,* dati delle carte di pagamento o altre informazioni riservate in risposta a richieste non verificate;
- **verificare l’esistenza di eventuali rimborsi, debiti o richieste di adempimento attraverso le aree riservate dei portali istituzionali**;
- segnalare tempestivamente le comunicazioni sospette attraverso i canali ufficiali degli enti interessati.

È inoltre opportuno sensibilizzare collaboratori, dipendenti e clienti dello studio sulle campagne fraudolente in corso, affinché le richieste apparentemente provenienti dalle amministrazioni pubbliche siano sottoposte a verifica prima di procedere alla trasmissione di informazioni o all’esecuzione di pagamenti.

Link **agli avvisi ufficiali**

Le amministrazioni interessate mettono a disposizione

apposite sezioni dei propri siti istituzionali, nelle quali vengono pubblicate le segnalazioni delle campagne fraudolente e le indicazioni per riconoscerle:

- **Agenzia delle Entrate** – ***Focus sul phishing***.
- **Agenzia delle entrate-Riscossione** – ***Phishing* – Segnalazioni e approfondimenti**.
- **Inps** – ***Vademecum* antitruffe**.
- **Inps** – **Come l'Istituto contrasta le truffe online – Notizia del 26 novembre 2026**.