Vademecum antitruffe

(Fonte: https://www.inps.it/ 15 aprile 2025)

Viviamo in un'epoca in cui la nostra identità digitale è diventata una risorsa preziosa e, purtroppo, un obiettivo per truffatori sempre più organizzati.
Attraverso email, SMS, telefonate, siti web falsi o persino visite a domicilio, i tentativi di **furto d'identità e di dati sensibili** si moltiplicano. L'INPS, da sempre al fianco dei cittadini, ha attivato un sistema di monitoraggio e segnalazione costante, in collaborazione con il **CERT-AGID**, per combattere le frodi digitali che sfruttano il nome dell'Istituto.
Le finalità di queste truffe sono molteplici: sottrarre **dati anagrafici, bancari, documenti d'identità** (spesso associati a selfie), **accedere illecitamente allo SPID** o ai servizi digitali della pubblica amministrazione. Nei casi peggiori, i dati vengono rivenduti sul **dark web** o usati per frodi finanziarie.
Di seguito **le principali truffe**: è importante riconoscerle per difendersi.

Phishing (via email)
Una delle tecniche più diffuse è il phishing. Il truffatore invia una **email** che **sembra provenire dall'INPS** e chiede all'utente di cliccare su un link per:

- aggiornare i dati personali o bancari;
- ricevere un rimborso;
- evitare la sospensione di una prestazione.

Il link conduce a una **pagina falsa**, simile al portale INPS, che registra i dati inseriti.
Nella pagina "Truffe online: il phishing" è possibile vedere le tipologie più recenti di email di phishing.

Smishing (tramite SMS)
Simile al phishing, ma con messaggi via cellulare, è lo **smishing**. Lo schema è lo stesso:

- invito a cliccare su un link;
- comunicazioni urgenti (es. bonus da incassare, errori nei dati, aggiornamenti richiesti).

Alcuni SMS contengono anche link per installare **app dannose**.
Nella pagina "Truffe tramite sms: lo smishing" è possibile vedere le tipologie più recenti di SMS truffaldini.

Truffe telefoniche
I truffatori si spacciano per operatori INPS e chiedono:

- dati personali o bancari;
- informazioni su prestazioni in corso;

- verifiche sulla propria posizione.

L’INPS non richiede mai queste informazioni per telefono.

Falsi funzionari a domicilio

Sono stati segnalati casi di individui che si presentano **a casa degli utenti**, spacciandosi per incaricati INPS. Possono chiedere di:

- visionare documenti;
- raccogliere firme o informazioni.

L’INPS non manda mai personale presso le abitazioni.

Pubblicità ingannevoli e prestiti truffa

Esistono siti o società che si presentano come “partner INPS” o “convenzionati INPS” per offrire **prestiti o agevolazioni**. Usano indebitamente la sigla "INPS" nel nome o nell’indirizzo web. Bisogna controllare sempre sul sito ufficiale l’elenco delle banche e delle società realmente accreditate.

Cosa si rischia se si cade nella trappola

Fornendo i propri dati, i truffatori possono:

- attivare SPID con il nome dell’utente truffato;
- accedere ai suoi servizi pubblici online;
- richiedere prestiti o finanziamenti;
- aprire conti correnti fraudolenti;
- rubare l’identità digitale per venderla.

Come riconoscere una comunicazione autentica

Per non confondere le comunicazioni autentiche dell’INPS con quelle fraudolente, è importante ricordare che l’Istituto:

- **non invia** SMS o email con link su cui cliccare per ricevere rimborsi;
- **non chiede** documenti via email o telefono;
- **non invia** personale a casa per accertamenti;
- **non chiede** dati bancari via email o SMS;
- può inviare email per indagini di soddisfazione (Customer Experience) ma **non chiede dati personali**.

Tipologia comunicazione	
Azione	**L'INPS lo fa?**
Inviare SMS o email con link su cui cliccare per ricevere rimborsi	No
Chiedere documenti via email o telefono	No
Inviare personale a casa per accertamenti	No
Chiedere dati bancari via email o SMS	No
Inviare email per indagini di soddisfazione	Sì, **ma non chiede dati personali**

Cosa fare per proteggersi

Verificare sempre:

- il mittente dell'email o SMS;
- la correttezza dell'indirizzo del sito (deve terminare con **inps.it**);
- se ci sono errori grammaticali o richieste insolite.

Non bisogna mai:

- cliccare su link sospetti;
- scaricare file **.exe** o allegati non richiesti;

- inviare documenti personali su richiesta.

In caso di dubbio:

- consultare questo vademecum;
- contattare il Contact center ai numeri **803.164** (da fisso) o **06.164.164** (da cellulare);
- rivolgersi ai **profili social ufficiali** dell'INPS.

In caso di ricezione di un messaggio sospetto:

- non cliccare sul link;
- non inserire dati personali;
- fare una segnalazione immediata attraverso i canali ufficiali INPS.

Materiali utili

Sito AgID – Smishing a tema INPS: come comportarsi in caso di furto dei dati

Sito AgID – Smishing a tema INPS: in vendita online i documenti trafugati