

Internet, email, sms, app e social network: oggi più che mai disponiamo di strumenti e canali che offrono molteplici opportunità, ma che possono esporci anche a qualche rischio.

L'INPS è perciò in prima linea nel mettere in allerta gli utenti e segnalare i **tentativi di frode** che si verificano con diverse modalità, ma tutti finalizzati al **furto di dati personali e sensibili**.

Ecco un breve **vademecum** che raccoglie informazioni e consigli utili per difendersi dalle truffe.

Truffe online: il phishing

Tra le truffe più diffuse e insidiose, il **phishing** è un tipo di frode informatica che mira al furto dei dati sensibili.

Numerose le segnalazioni dell'INPS agli utenti su questo fronte: una delle modalità riscontrate, in particolare, è l'invio di **false email** che invitano ad aggiornare i propri dati personali o le proprie coordinate bancarie, tramite un link cliccabile, per ricevere l'accredito di fantomatici **pagamenti e rimborsi** da parte dell'Istituto. In alcuni casi il link apre una **falsa pagina** dei **servizi INPS**.

I tentativi fraudolenti si sono verificati anche durante l'**emergenza Covid-19**, un'ulteriore occasione per provare a truffare gli utenti interessati alle prestazioni e ai servizi erogati dall'Istituto per fronteggiare la crisi dovuta alla pandemia.

Ne è un esempio il caso delle email di phishing finalizzate a sottrarre i dati della carta di credito con la falsa motivazione del pagamento del **Bonus 600 euro** o di altre **indennità Covid-19**.

Non solo email. È necessario fare attenzione anche agli **SMS** che inducono ad aprire un link per aggiornare la propria **domanda Covid-19** e a installare un'app malevola. Questi SMS non sono inviati dall'INPS.

E sempre a proposito di emergenza Coronavirus e bonus INPS, l'Istituto ha smentito la notizia circolata recentemente su un fantomatico **nuovo bonus**, chiarendo che gli unici benefici attualmente concessi sono quelli già previsti dalle norme.

Truffe telefoniche

Gli utenti possono anche ricevere una **telefonata** nel corso della quale un finto operatore telefonico INPS chiede di conoscere i dati relativi alla propria posizione nell'ambito di soggetti di diritto privato, come società o associazioni.

Falsi funzionari

I tentativi di raggio avvengono, inoltre, da parte di **falsi funzionari INPS** che possono presentarsi anche presso la propria abitazione. L'Istituto non invia incaricati presso il domicilio degli utenti e assistiti.

Prestiti e pubblicità ingannevole

Esistono **società**, non correlate e non riconducibili all'Istituto, che fanno riferimento nel proprio nome, in tutto o in parte, a "INPS" e che offrono **servizi** in termini equivoci o ingannevoli.

Si tratta di **società d'intermediazione finanziaria** che pubblicizzano, tramite SMS, **prestiti** sponsorizzati come "convenzionati" con l'Istituto, i cui siti non rimandano affatto ai benefici erogati istituzionalmente dall'INPS ai propri iscritti e pensionati.

Consigli utili

È importante ricordare che l'INPS non acquisisce in alcun caso, telefonicamente o via email ordinaria, le coordinate bancarie o altri dati che permettano di risalire a informazioni finanziarie. Inoltre, tutte le **informazioni sulle prestazioni** sono consultabili **esclusivamente accedendo al sito istituzionale**.

È, quindi, necessario:

- non dare seguito a richieste che arrivino per email non certificata, telefono o tramite il porta a porta;
- diffidare di qualsiasi persona dichiara di essere un incaricato o funzionario INPS e sostenga di dover effettuare accertamenti di varia natura;
- prestare la massima attenzione alle comunicazioni che si ricevono, non cliccare sui link di email di origine dubbia e verificare sempre l'indirizzo di provenienza.