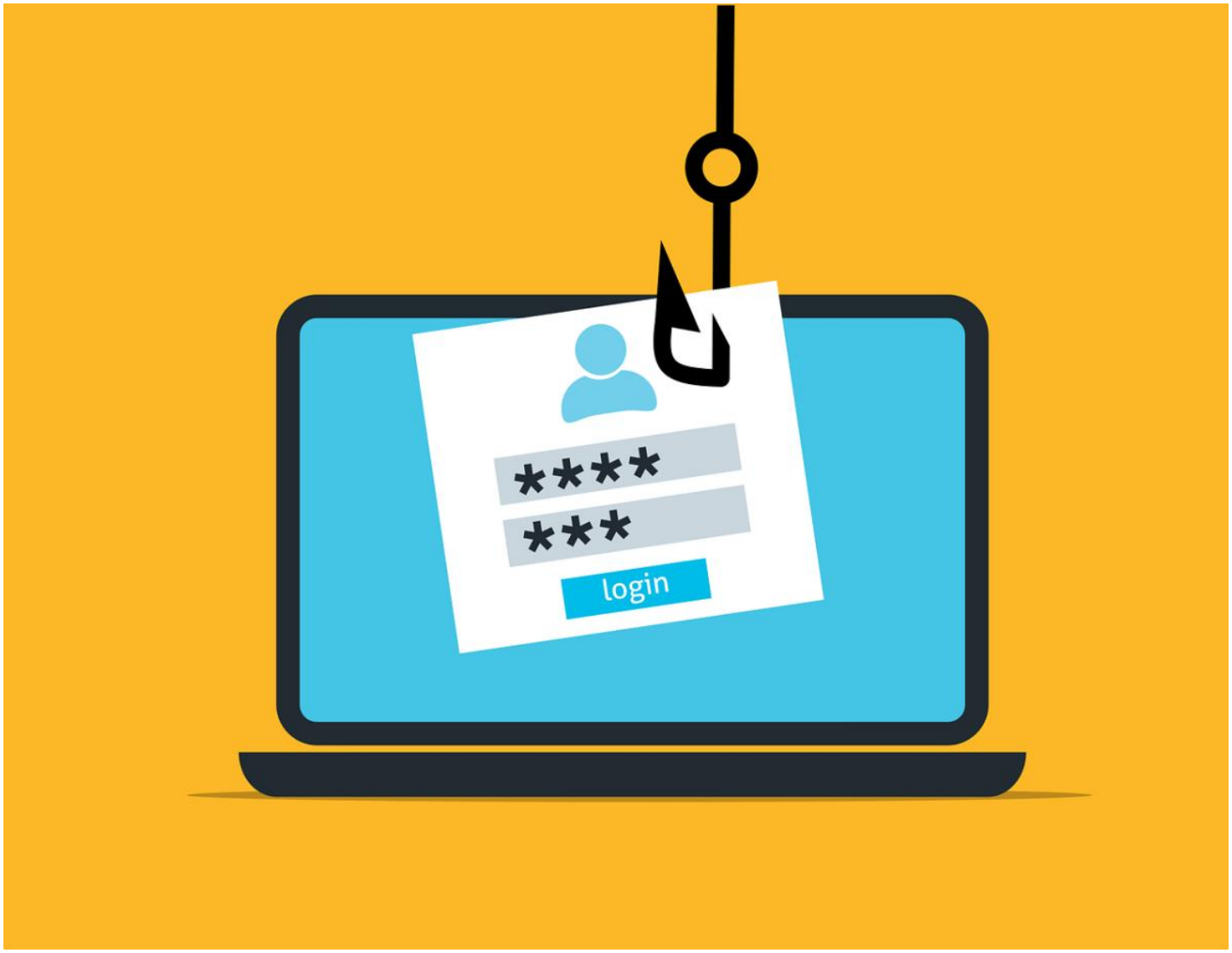
Occhio alla multa da pagare con PagoPa, è una truffa: ecco come riconoscerla

C'è una nuova truffa che sta circolando nel nostro Paese: si tratta dell'ennesimo tentativo di phishing (Fonte: https://www.ilgiornale.it/ 28 giugno 2025)



Attenzione alla nuova **truffa** che sfrutta il sistema di pagamenti **pagoPA** per ingannare le vittime e convincerle a versare denaro o a cedere informazioni sensibili credendo di stare comunicando con la pubblica amministrazione. Stavolta i cybercriminali inviano delle email fasulle rese del tutto simili alle comunicazioni di pagoPA per spingere le persone a pagare. Nelle mail compare il logo di pagoPA con tanto di numero di pratica e importo da pagare.

Chi riceve il messaggio spesso va nel panico, perché si fa riferimento a una multa per eccesso di velocità da pagare subito se non si vuole che questa raddoppi dopo 72 ore. Ecco quindi che la vittima viene invitata a cliccare su un link per accedere al portale ed effettuare il versamento.

Purtroppo si tratta dell'ennesimo tentativo di **phishing** ben studiato. PagoPA non ha nulla a che fare con questa vicenda.

Il **CERT-AgID** ha lasciato una comunicazione (qui) in cui mette in allerta i cittadini. Sono stati tanti, in questi mesi, i tentativi di ingannare le persone con comunicazioni apparentemente ufficiali. *"Le campagne, contenenti falsi solleciti di pagamento relativi a presunte sanzioni stradali, vengono veicolate principalmente tramite email. L'obiettivo è indurre gli utenti a effettuare pagamenti*

non dovuti attraverso link ingannevoli", si legge nel documento. *"La vittima viene reindirizzata a una pagina web che riproduce i loghi di PagoPA e si articola in due fasi: nella prima viene richiesto l'inserimento di dati personali come nome, cognome, email e numero di telefono; nella seconda, invece, viene sollecitata la compilazione dei campi relativi alla carta di credito, sempre con il pretesto di estinguere una presunta sanzione*".

I **messaggi fraudolenti** sono molto curati. La grammatica è corretta, i loghi sono molto simili, si fa riferimento a reali codici di violazione e c'è senso di urgenza. Come difendersi, dunque?

La prima cosa da fare è non lasciarsi prendere dal panico. L'urgenza del messaggio non deve allarmare, semmai deve essere considerato una spia del fatto che ci troviamo di fronte a una potenziale truffa. Non si deve mai cliccare sui **link**, né effettuare alcun tipo di operazione che viene indicata. Mai cedere le proprie coordinate bancarie, o i dati sensibili.

Bisogna sempre ricordare che nessun ente ufficiale, come pagoPA, richiede certe informazioni via email o messaggio. Altra cosa importante è controllare la presenza del certificato di sicurezza HTTPS (spesso, in caso di truffa) non è presente.