ABRUZZO SERA
www.abruzzosera.it

Aumentano le truffe in Abruzzo: i consigli di Poste Italiane

19 Aprile 2024



Anche in Abruzzo sono sempre più frequenti le truffe online. A tal proposito, tra le molteplici iniziative per contrastare il fenomeno, Poste Italiane ha realizzato un vademecum contenente poche e semplici regole per operare in sicurezza ed evitare spiacevoli sorprese quando si utilizza il conto online di Poste Italiane.

I consigli sono disponibili sul sito poste.it, nella sezione dedicata alla sicurezza, al seguente link: https://www.poste.it/come-difendersi-dalle-truffe.html?wt.ac=1473802358516.

Riassumiamo qui le principali regole da tenere a mente per difendersi dalle truffe online e sull'applicazione. Per prima cosa occorre ricordare che Poste Italiane e PostePay non chiedono mai i dati riservati (utenza, password, codici sicurezza) in nessuna modalità (e-mail, sms, chat social network, operatori call center) e per nessuna finalità. Se qualcuno, anche presentandosi come dipendente di Poste Italiane o rappresentante delle Forze dell'Ordinedovesse chiedere tali informazioni si tratta di un tentativo di frode, quindi non fornirle a nessuno.

Non è mai richiesto di disporre transazioni di alcun genere con il pretesto di problemi di sicurezza sul conto o sulla carta tantomeno attraverso indicazioni telefoniche di presunti dipendenti di Poste Italiane o rappresentanti delle Forze dell'Ordine, che inducono a recarsi in Ufficio Postale o allo

sportello ATM Postamat per effettuarle.

Ricordate di non rispondere a e-mail, sms, telefonate o chat, in cui vengono chiesti i codici personali (utenza, password, codici sicurezza, dati carte pagamento) o segnalati fantomatici problemi di sicurezza con imminenti blocchi di operatività. Anche se sembrano provenire da fonti attendibili o da indirizzi aziendali conosciuti, Poste Italiane non chiede mai tali informazioni e non cliccare su link eventualmente presenti.

Bisogna controllare l'attendibilità di una e-mail prima di aprirla: verificare che il mittente sia conosciuto e identificato.

Non scaricare gli allegati di una e-mail sospetta e non cliccare sul link contenuto prima di aver verificato che il mittente sia conosciuto e identificato; se per errore dovesse accadere, non autenticarti sul sito falso e chiudere subito il web browser.

Digitare direttamente l'indirizzo internet www.poste.it nella barra del web browser per accedere al sito di Poste Italiane.

Potete utilizzare l'applicazione mobile per usufruire del servizio gratuito di push notification ed essere informati in tempo reale sulle operazioni di pagamento effettuate con il conto corrente e le carte di pagamento. In alternativa attivare il servizio di notifica tramite sms sul telefono mobile.

Segnalare a Poste Italiane eventuali e-mail di phishing, inoltrandole a antiphishing@posteitaliane.it. Immediatamente dopo, le mail sospette vanno cestinate e cancellate definitivamente.