

POSTE ITALIANE: I CONSIGLI PER LA SICUREZZA INFORMATICA E PER CONTRASTARE LE TRUFFE ONLINE

30 Settembre 2022



PESCARA - Poste Italiane, in linea con la campagna "Cyber Security Month" istituita dall'Unione Europea per promuovere e sensibilizzare durante l'intero mese di ottobre aziende e cittadini sull'importanza della sicurezza informatica, coglie l'occasione per offrire anche ai cittadini abruzzesi una serie di suggerimenti e consigli utili per non cadere vittima delle truffe online.

Collegandosi al sito www.poste.it, infatti, si può accedere alla sezione dedicata alla sicurezza dove sono disponibili una serie di video che spiegano come avvengono le principali tipologie di truffe online, sulle App e sui canali social e analizzando occasioni più pratiche come quando si finalizza un acquisto e-commerce o nei casi in cui si compiono operazioni di pagamento.

La prima regola per evitare di cadere nella rete di malintenzionati è quella di diffidare sempre di richieste più o meno urgenti di dati personali e ovviamente di non comunicarli in nessuna modalità e per nessun motivo.

Altra indicazione fondamentale è che Poste Italiane S.p.A. e PostePay S.p.A. non richiedono mai di fornire dati riservati come il "nome utente", le password, i codici di sicurezza per eseguire una transazione, come ad esempio il codice OTP-One Time Password ricevuto via sms, in nessuna modalità (e-mail, sms, chat di social network, operatori di call center) e per nessuna finalità. Se qualcuno, anche presentandosi come un operatore di Poste Italiane S.p.A. o PostePay S.p.A., dovesse chiedere tali informazioni, si tratta certamente di un tentativo di frode.

Più in generale, per evitare il rischio di essere colpiti da episodi di truffe online, occorre mettere in pratica i seguenti semplici accorgimenti:

Non rispondere mai a e-mail, sms, chiamate o chat da call center in cui ti vengono chiesti i tuoi codici personali (utenza, password, codici di sicurezza, dati delle carte di pagamento);

Controllare sempre l'attendibilità di una e-mail prima di aprirla: verificare che il mittente sia realmente chi dice di essere e non qualcuno che si finge qualcun altro (ad esempio controllando come è scritto l'indirizzo e-mail del mittente);

Non scaricare gli allegati delle e-mail sospette prima di aver verificato che il mittente sia noto o ufficiale;

Non cliccare sul link contenuto nelle e-mail sospette; se per errore dovesse accadere, non autenticarti sul sito falso, chiudi subito il web browser;

Segnalare a Poste Italiane eventuali e-mail di phishing inoltrandole all'indirizzo antiphishing@posteitaliane.it. Immediatamente dopo cestinare e cancellare anche dal cestino;

Digita direttamente l'indirizzo Internet <https://www.poste.it/> nella barra degli indirizzi del web browser per visitare il sito di Poste Italiane;

Utilizza l'App per usufruire anche del servizio gratuito di push notification ed essere informato in tempo reale sulle operazioni di pagamento effettuate con il tuo conto corrente e le tue carte di pagamento. In alternativa attiva il servizio di notifica tramite SMS sul tuo telefono cellulare, gratuito per i pagamenti su siti internet e su app. Per ulteriori informazioni sul servizio consulta i fogli informativi nella sezione Trasparenza Bancaria del sito [poste.it](https://www.poste.it).

Le informazioni messe a disposizione da Poste Italiane hanno l'obiettivo di promuovere la cultura della sicurezza e contribuire alla prevenzione dei fenomeni di microcriminalità, in linea con il tradizionale ruolo sociale di Poste Italiane e con i valori di inclusione e vicinanza ai cittadini abruzzesi che da sempre ne ispirano l'azione.