Servizio Comunicazione e informazione

UNIONE
SINDACALE
TERRITORIALE

Stefano Contu
Responsabile Ufficio Stampa
Tel 035 324 122
Cellulare 335 273189
E-mail: stefano.contu@cisl.it

COMUNICATO STAMPA

ADICONSUM invita all'attenzione. Numerosi i casi in provincia

Anno nuovo, truffe (quasi) nuove

"I nostri dati sono il vero tesoro"

Busi: "*PostePay, e-commerce e phishing i territori più colpiti*"

"Le truffe con cui ogni giorno gli utenti in possesso di una PostePay, carte debito e di credito, si devono misurare sono veramente tante, e il rischio, se non si presta la giusta attenzione, è di cadere in un vortice dal quale si uscirà con decurtazioni di denaro e con tutti i dati sensibili irrimediabilmente trafugati. Negli ultimi periodi ci siamo trovati diversi casi di persone che si sono viste prelevare dal conto i soldi senza aver disposto alcun pagamento".
Mina Busi, presidente di ADICONSUM Bergamo, alza ancora una volta il velo su un sistema fraudolento che si riversa sugli utenti e sui cittadini, anche nella provincia orobica.
Quello che è successo è che alcuni utenti, intestatari di una Postapay Evolution, si sono visti arrivare un messaggio nella propria casella di posta elettronica che altro non era che un tentativo di frode vera e propria. La mail in questione era stata impostata in modo da ricordare in tutto e per tutto una comunicazione ufficiale di Poste Italiane.
"*Nell'ultimo caso da noi seguito, addirittura l'email era compatibile con una richiesta di ricollegamento al numero telefonico fatta in Filiale, ma il prelievo di 900 € è stato dirottato su un conto a Malta!*".
Nella mail si richiedevano alcuni dati inerenti il conto, il tutto attraverso un link che avrebbe permesso di modificare quanto risultava dal sistema. Il problema, però, è che il link in questione riportava ad una pagina che assomigliava nella grafica al portale ufficiale di Poste Italiane ma che, di fatto, **era un sito fake gestito da truffatori** che, una volta ottenuti i dati richiesti, utilizzavano quanto in loro possesso per svuotare i conti e portare a termine la frode
"*Nei casi di phishing, ovvero di mail ed sms sospetti, l'unica cosa da fare per evitare brutte sorprese è non aprire link e pagine a cui le stesse rimandano, perché altro non sono che tentativi degli hacker di entrare nel sistema degli utenti.* ***Quando le stesse sono difficilmente distinguibili da quella che potrebbe essere una comunicazione ufficiale, nel dubbio, sempre meglio contattare l'Ente o l'Istituto che risulta essere il mittente,*** *si tratta di una truffa saranno i primi a mettere in guardia sull'accaduto.*
Il rischio è molto elevato e non deve assolutamente essere preso sotto gamba. Se ricevete messaggi di questo tipo, cancellateli immediatamente e non date assolutamente credito. Ricordate infatti che Poste Italiane, le Banche o gli Enti Statali non inviano mai email per la riattivazione di account o il cambio della password".

Le frodi online, ricorda ADICONSUM, sono però più frequenti di quanto si possa immaginare. Spesso si leggono notizie relative a truffe realizzate e sventate grazie all'uso delle nuove tecnologie. Insieme ai tentativi di phishing, una delle truffe più diffuse rimane sicuramente quella della clonazione della carta (ovvero quando gli hacker entrano in possesso di numero, scadenza, intestatario e cvv della Postpay). In questo caso, qualora dovessero riscontrarsi movimenti sospetti nel conto, **la prima cosa da fare è bloccare la carta e presentare immediatamente denuncia alle Autorità, reclamo all'Istituto di credito per il reintegro delle somme**, in caso di risposta negativa si può ricorrere all'Arbitro Bancario Finanziario.
"*Bisogna presentare denuncia a Carabinieri o Polizia anche quando si acquista un prodotto online e non si riceve nulla in cambio. Queste truffe sono ancora molto diffuse, nonostante gli e-commerce chiedano sempre più garanzie ai propri venditori. Potrebbe capitare, pertanto, di ritrovarsi nella spiacevole posizione di aver speso dei soldi inutilmente.*
Un'altra truffa che riguarda le compravendite online, è che si è diffusa a macchia d'olio recentemente, è quella relativa a ***vendite e acquisti presso un rivenditore straniero****. È capitato infatti che molti utenti venissero contattati da venditori che, adducendo scuse di varia natura, chiedessero loro gli estremi dalla carta, i documenti di identità e una somma da accreditare ad una fantomatica banca straniera per poter procedere con la compravendita*.
Una richiesta che, di fatto, altro non è che un tentativo di truffa, dal quale l'utente può difendersi solo evitando di fornire dati sensibili e procedendo con una denuncia. *In ogni caso bisogna ricordarsi che la prudenza non è mai troppa in questi casi. Agire con consapevolezza e tenere sempre gli occhi aperti, dunque, è alla base di tutto*".

Bergamo, 16 gennaio 2020