VerbanoNews

Le news del Lago Maggiore

“È stato effettuato un pagamento su PayPal, clicca qui…”. Tentativi di truffe online e come evitarli

Tommaso Guidotti · Sunday, November 12th, 2023

*“È stato effettuato un pagamento di 438,38 euro con la carta ****, se non riconosci questo pagamento clicca qui”*. È questo il nuovo messaggio che sta arrivando, con diversi importi e diversi link da cliccare, a numerosissimi utenti.

La potremmo chiamare la “nuova frontiera” del phishing, che prova a colpire questa volta gli utilizzatori di **PayPal, arcinota società statunitense che offre servizi di pagamento digitale e di trasferimento di denaro** tramite Internet fondata nel 1999 da Confinity, poi passata sotto l’ala di Elon Musk e infine comprata da eBay nel 2002 che ne ha fatto una società indipendente nel 2015.

Il messaggio che arriva via sms ha come mittente proprio “PayPal”, cosa che potrebbe indurre in errore molti, magari disattenti o colti in un momento di scarsa lucidità. Lo stesso metodo usato dai truffatori in tante altre circostanze, con messaggi inviati da banche, app, siti e così via, tutti verosimili o somiglianti a quelli veri, creati apposta per ingannare e far cadere nella trappola ignari e sbadati utenti.

È proprio dal sito della società americana che però ci sono le spiegazioni di come evitare di cadere in questo tipo di trappole. Tra le FAQ, utilissime, che si trovano nella sezione Aiuto o Sicurezza della app o appunto sul sito internet, viene spiegato come si muove la vera PayPal e come segnalare eventuali tentativi di truffa come quello nella foto sotto.

Come faccio a riconoscere un sito, un messaggio o un’email PayPal falso, fraudolento o di phishing?

Se ricevi un messaggio e non hai la certezza che provenga da PayPal, controlla se rientra in una delle seguenti casistiche.
Usa saluti impersonali, generici, come "Gentile utente" o "Gentile [indirizzo di email]". Nelle sue email, PayPal si rivolge sempre a te usando il tuo nome e cognome o il nome della tua azienda. Non diciamo mai cose come "Gentile utente" o "Salve, utente PayPal".

Ti chiede di cliccare link che portano a siti fasulli. Controlla sempre i link contenuti nelle email prima di aprirli. Un link potrebbe sembrare perfettamente sicuro, ad esempio www.paypal.com/OfferteSpeciali. Assicurati di portare il puntatore del mouse sul link per vedere la destinazione reale. Se non ne hai la certezza, non cliccare il link.

Contiene allegati sconosciuti. Apri un allegato solo se hai la certezza che sia legittimo e sicuro. Presta particolare attenzione alle fatture provenienti da aziende e fornitori che non ti sembrano familiari. Alcuni allegati contengono virus che si installano quando vengono aperti.

Instilla un falso senso di urgenza. Le email di phishing sono spesso allarmiste e ti avvisano che devi aggiornare subito il tuo conto. La speranza dei criminali è che tu creda a questo senso di urgenza e ignori i segnali di allarme che l'email è falsa. Se sul tuo conto è richiesto un tuo intervento urgente, puoi trovare le relative informazioni accedendo a PayPal.

Di seguito sono riportate le frodi più frequenti in cui i truffatori usano email contraffatte.
· *"Il tuo conto sta per essere sospeso."*
Molti truffatori ti inviano email contraffatte per avvisarti che il tuo conto sta per essere sospeso. Nel messaggio ti chiederanno di immettere la password in una pagina web (contraffatta). Noi ti chiediamo di immettere la password solo nella nostra pagina di accesso. In caso di dubbi, accedi sempre a PayPal e cerca eventuali notifiche nel Centro risoluzioni.

· *"Hai ricevuto un pagamento."?Alcuni truffatori cercano di convincerti di aver ricevuto un pagamento per un ordine. Vogliono i tuoi prodotti gratuitamente. Prima di spedire qualcosa, accedi a PayPal e verifica di aver effettivamente ricevuto un pagamento. Noi non ti chiederemo mai di fornire un codice di tracciamento via email. Se hai ricevuto un pagamento, potrai sempre vederlo nella tua cronologia PayPal.*

· *"Hai ricevuto un pagamento eccessivo."?I truffatori possono cercare di convincerti che hanno pagato troppo un articolo. Ad esempio, ti invieranno un'email per dirti che hanno pagato 500,00 EUR per una fotocamera che vendi a 300,00 EUR. Il mittente ti chiede di spedire la fotocamera insieme ai 200,00 EUR aggiuntivi che avrebbe "pagato" per sbaglio. Il truffatore vuole la tua fotocamera E i tuoi soldi, ma in realtà non ti ha ancora pagato. Prima di spedire qualcosa, accedi a PayPal e verifica di aver ricevuto un pagamento.*

Per segnalare un'email o un sito sospetto, inoltrali all'indirizzo phishing@paypal.com, li esamineremo per te. Dopo che avrai inviato l'email, eliminala dalla tua casella di posta.

This entry was posted on Sunday, November 12th, 2023 at 10:05 am and is filed under Scienza e Tecnologia
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.