Cronaca - *Truffa del curriculum su WhatsApp, così i finti recruiter svuotano i conti: come riconoscere l'inganno e difendersi*

Roma - 02 lug 2026 (Prima Notizia 24) **Una telefonata con il pretesto di un'offerta di lavoro apre la strada a una sofisticata frode. I truffatori si spacciano per selezionatori del personale per rubare dati personali e denaro.**

Chi è alla ricerca di un impiego è diventato uno dei bersagli preferiti dei cybercriminali. L'ultima frode sfrutta infatti l'attesa di una risposta dopo l'invio del curriculum per convincere le vittime ad abbassare la guardia. Il raggiro inizia con una telefonata proveniente da un numero italiano, preceduto dal prefisso +39. Dall'altra parte risponde una voce preregistrata, ma realistica, che comunica: "Salve, abbiamo ricevuto il tuo curriculum, aggiungici su WhatsApp per parlare di lavoro". Un messaggio volutamente generico che può sembrare credibile a chi ha inviato numerose candidature e aspetta di essere ricontattato. Come funziona il raggiro Nella maggior parte dei casi i truffatori non hanno mai ricevuto il curriculum della persona contattata. I numeri di telefono vengono recuperati da vecchi database o raccolti attraverso canali illeciti, per poi essere utilizzati in campagne di chiamate automatiche. La richiesta di spostare immediatamente la conversazione su WhatsApp rappresenta il primo campanello d'allarme. Da quel momento entra in scena un presunto recruiter che cerca di instaurare un rapporto di fiducia con la vittima. Le quattro fasi della truffa Secondo gli esperti, il raggiro segue uno schema ormai consolidato. Il sedicente selezionatore si presenta con nome, cognome e ruolo, spesso mostrando il logo di un'azienda realmente esistente o condividendo link a siti internet per apparire affidabile. Successivamente propone un impiego semplice e immediato, spesso da svolgere online. Tra le attività richieste ci sono mettere "like" ai video, iscriversi a canali social oppure recensire contenuti sul web, promettendo guadagni elevati a fronte di uno sforzo minimo. Per rendere credibile il sistema, in alcuni casi i truffatori inviano piccole somme di denaro oppure mostrano estratti conto falsificati che sembrano dimostrare il buon funzionamento dell'attività. Quando la vittima si fida, arriva la vera trappola. Viene chiesto di compilare moduli con dati personali, documenti d'identità, coordinate bancarie oppure di effettuare un primo versamento con la promessa di ottenere compensi molto più elevati. Dietro l'offerta di lavoro, però, non esiste alcuna reale opportunità professionale. Quali sono gli obiettivi dei truffatori Lo scopo della frode può essere diverso a seconda dei casi. I criminali informatici cercano innanzitutto di impossessarsi dei dati personali delle vittime per commettere furti d'identità. In altri casi puntano a prendere il controllo dell'account WhatsApp oppure a sottrarre direttamente denaro convincendo le persone a investire su piattaforme finanziarie non autorizzate. Chi rischia di più La truffa viene diffusa in modo indiscriminato, ma alcune categorie risultano particolarmente vulnerabili. Tra queste figurano i neolaureati e i giovani alla ricerca del primo impiego, i disoccupati o chi ha

inviato decine di curriculum e fatica a ricordare tutte le candidature presentate. Più esposte anche le persone con minore familiarità con gli strumenti digitali, che possono avere maggiori difficoltà a riconoscere tentativi di phishing, link fraudolenti e numeri sospetti. Come riconoscere una vera selezione Camilla Cignarella, esperta di consulenza professionale, invita a prestare attenzione a pochi ma fondamentali dettagli. "Proteggersi dalla truffa telefonica del curriculum è possibile con un po' di attenzione: basta gestire con metodo le candidature e verificare ogni contatto prima di fidarsi. Piccoli accorgimenti, dall'usare canali ufficiali al tenere traccia delle risposte ricevute e diffidare delle offerte troppo allettanti, possono ridurre molto il rischio". In una selezione autentica il recruiter si identifica chiaramente con nome, cognome, ruolo e azienda, fa riferimento a una candidatura specifica e utilizza indirizzi e-mail aziendali o piattaforme professionali come LinkedIn. Soprattutto, non chiede mai denaro per proseguire il processo di selezione. Come difendersi Gli esperti consigliano di interrompere immediatamente la chiamata se una voce automatica invita a proseguire la conversazione su WhatsApp. È opportuno bloccare il numero senza seguire ulteriori istruzioni. Può essere utile anche tenere un elenco aggiornato delle candidature inviate. Se un'azienda che non compare nell'elenco contatta il candidato parlando del curriculum, è bene verificare con attenzione la sua identità prima di rispondere. Cosa fare se si è già caduti nella trappola Chi teme di essere stato vittima della truffa dovrebbe interrompere ogni contatto con i presunti recruiter, avvisare immediatamente la propria banca per bloccare eventuali carte o operazioni sospette e modificare le password degli account personali. È inoltre consigliabile presentare denuncia alla Polizia Postale, conservando screenshot delle conversazioni, ricevute di pagamento ed eventuali documenti condivisi, così da agevolare le indagini e limitare i danni.

(Prima Notizia 24) Giovedì 02 Luglio 2026