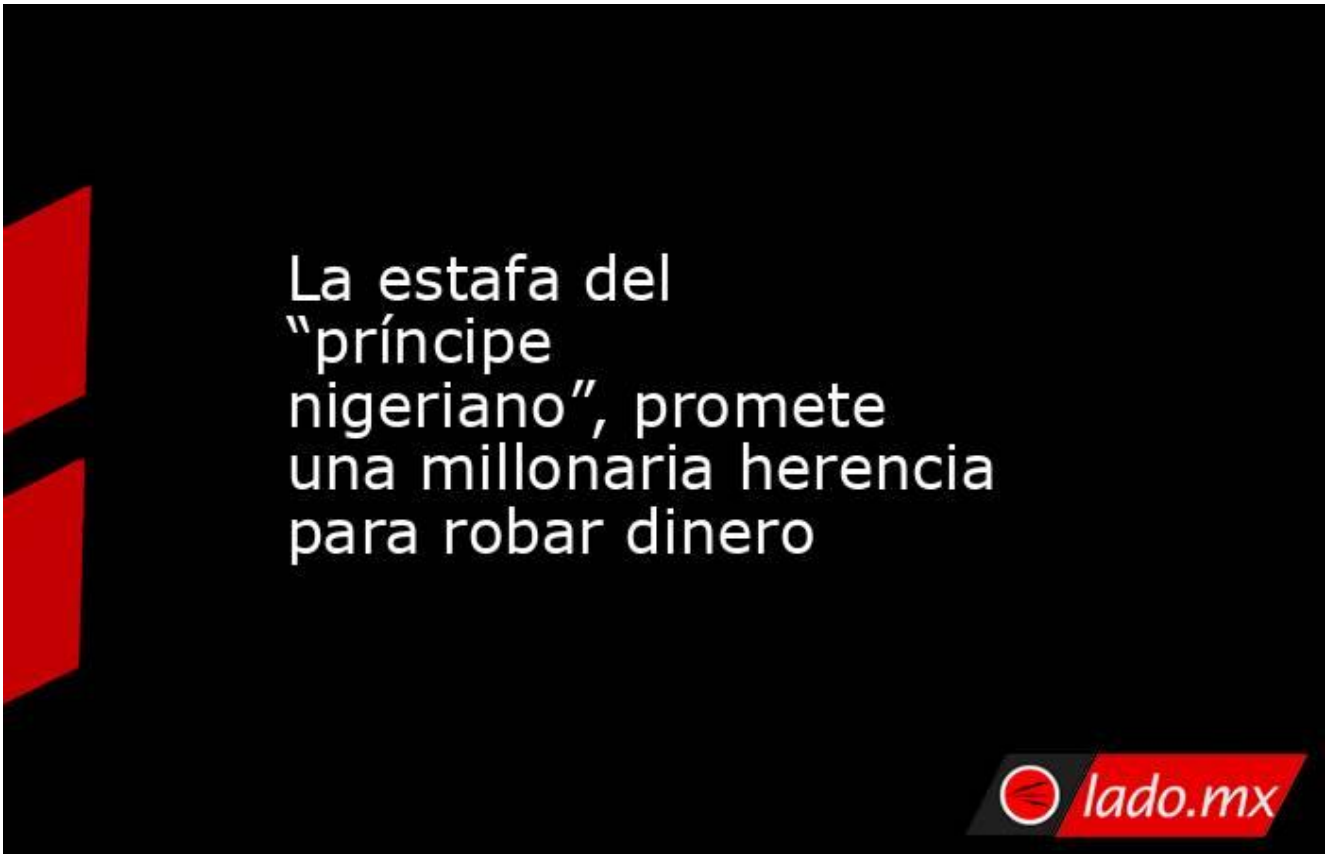
La estafa del “príncipe nigeriano”, promete una millonaria herencia para robar dinero

18/04/2023



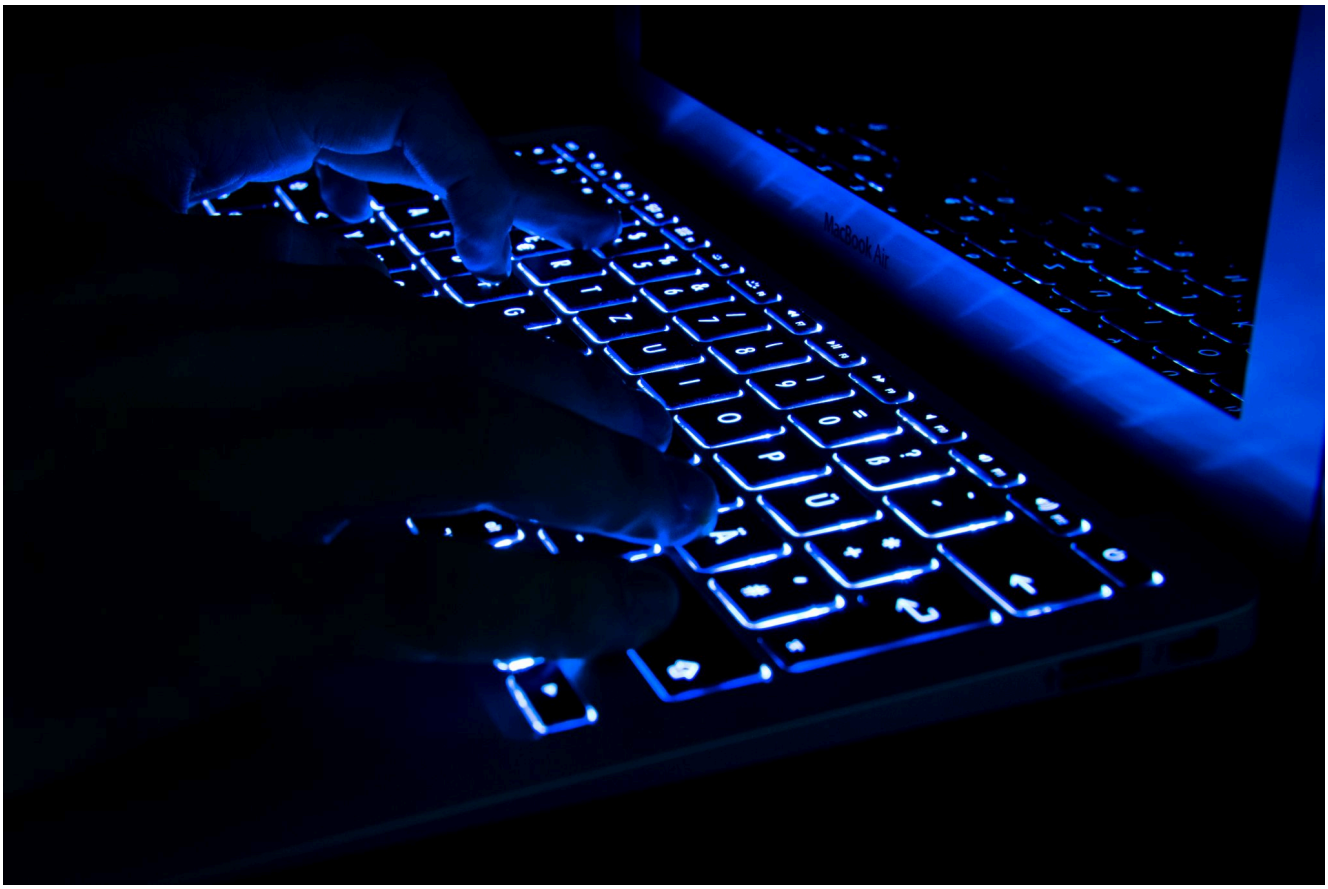
Durante los últimos 20 años la “estafa del **príncipe nigeriano**” se convirtió en la más famosa y poderosa en la historia de internet al usar un correo electrónico o un mensaje directo en alguna **red social para robar.**

Existieron varias adaptaciones dependiendo del país, pero el mensaje que enviaban los estafadores consistía en una breve presentación en la que se hacían pasar por un “príncipe” o “millonario” de **Nigeria** que necesitaba ayuda, ya sea para enviar su dinero al extranjero o para dejar una herencia.

El criminal detrás del mensaje aseguraba que se tenía que

compartir **información financiera** para realizar el movimiento o, en todo caso, solicitaba “un poco de dinero” con la promesa de devolver un monto superior. De esta forma, se buscaba recaudar fondos provenientes de múltiples víctimas o directamente robar el dinero de sus **cuentas bancarias**.

Sin embargo, los “micro pagos” no se realizaban en una sola operación, sino que una vez que la víctima aceptaba realizar al menos una, el estafador solicitaba cantidades cada vez más altas con mayor frecuencia hasta que el afectado decidiera no caer más en el engaño o se quedaba sin dinero.



La estafa del «príncipe nigeriano» tenía la intención de robar dinero directamente de las cuentas de las víctimas. (Franziska Gabbert/dpa)

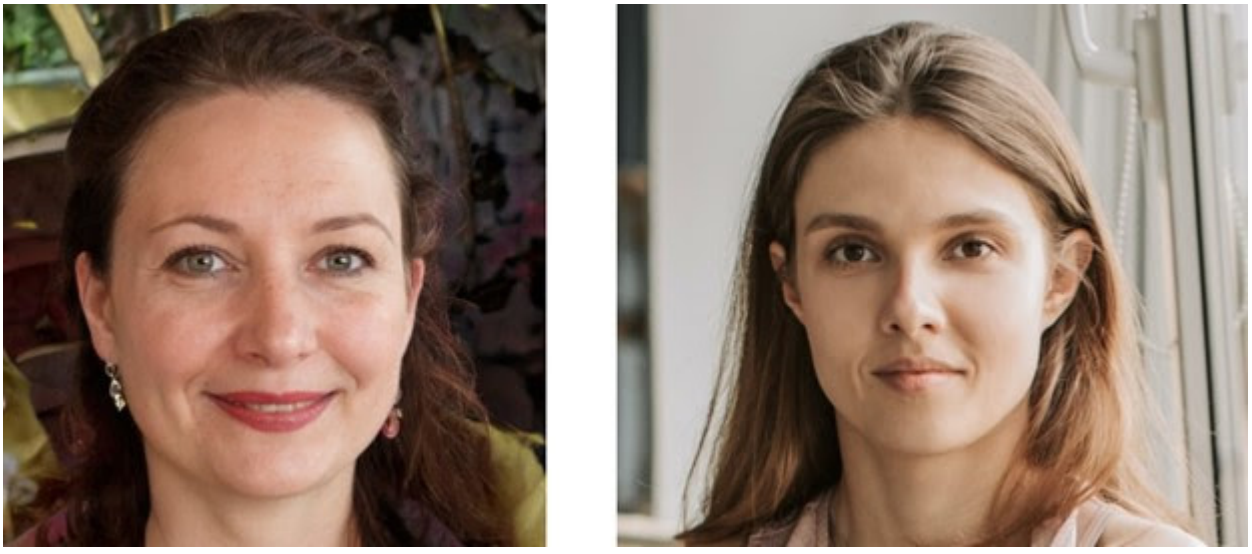
La “oportunidad” que presentaba el mensaje o correo de multiplicar el dinero sin necesidad de **trabajar** o de hacer algo más que “prestar” cierta cantidad a un “millonario”, es lo que finalmente seducía a las víctimas, quienes llegan a darse cuenta demasiado tarde del error que cometieron al

confiar en este “príncipe”.

Una de las formas con las que se puede evitar caer en esta **estafa** es que la víctima se detenga a pensar en cómo un príncipe nigeriano llegó a dar con su correo electrónico o perfil en **redes sociales**, por qué necesitaría ayuda para movilizar su **dinero**, por qué pide un “préstamo” y qué garantía se tiene de que todo lo que diga sea real.

Aunque esta modalidad de **estafa** sea utilizada hasta la actualidad y pueda ser relativamente sencilla de detectar y prevenir, existen otras formas aún más sofisticadas y difíciles de detectar para las potenciales víctimas. Estos métodos pueden recurrir a tecnología más avanzada como la **inteligencia artificial** y mejorar en cuanto al uso de las redes sociales como plataforma para maximizar el alcance del engaño.

Por ejemplo, los **“rostros GAN”** son imágenes extremadamente realistas generadas por computadora con ayuda de inteligencia artificial y que cuesta mucho trabajo diferenciar de una fotografía real. Con esta herramienta, los cibercriminales también pueden abrir perfiles en **redes sociales** o aplicaciones de citas para empezar con el proceso de **estafas online**.



Un rostro GAN (a la izquierda) es generado por una inteligencia artificial. (ESET)

Debido al realismo de la simulación, el método usado por los **cibercriminales** puede incluir “la estafa del amor” en la que se busca entablar conversaciones íntimas con la víctima, expresar intenciones románticas lo más pronto posible para luego solicitar “ayudas económicas” o animar a tomar “oportunidades de inversión”, usualmente en criptomonedas o en otro tipo de negocios que en realidad buscarán robar el dinero de las **cuentas bancarias** de sus víctimas.

En este tipo de casos es preferible mantenerse alertas ante las expresiones repentinas de afecto, menciones a posibles inversiones o criptomonedas. También es recomendable no permitir que la conversación se realice fuera de la plataforma de citas pues estas tienen métodos de moderación para evitar casos de **estafas** o robos online.

Fuente: Infobae