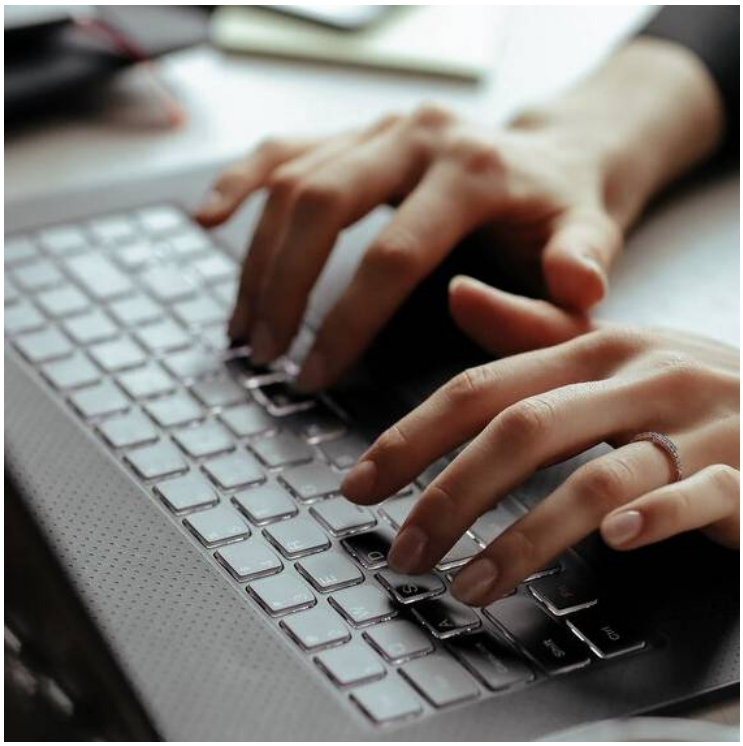
28/05/2025

Crece la ola de estafas digitales en Colombia, ¿cómo protegerse?

Circulan disfrazadas en mensajes de texto, chat, correo o publicidad en redes sociales. Sepa cómo identificarlas.



El panorama de la seguridad digital en Colombia experimenta una transformación inquietante, marcada por un incremento sofisticado y constante de las estafas en línea. Estas industrias del crimen digital han venido perfeccionado sus tácticas. Incluso en forma de 'noticias' falsas, que redes sociales como Instagram y Facebook permiten que circulen patrocinadas, en forma de publicidad, sin que ninguna autoridad las llame al orden por recibir dinero de bandas para permitirles promocionar sus engaños.

Según el portal especializado en ciberseguridad MuchoHacker, todas las semanas se detectan engaños que suplantan a los portales de EL TIEMPO y El Espectador, con supuestas 'entrevistas' a personalidades como Vicky Dávila o Gustavo Bolívar, para promocionar evidentes fraudes con inversiones en criptomonedas y para robar a los usuarios.

Precisamente la suplantación de identidad y la usurpación de marcas se han vuelto las herramientas predilectas de estos estafadores. La sofisticación de sus técnicas dificulta distinguir una comunicación genuina de un intento de fraude.

Un informe reciente de TransUnion revela que las llamadas telefónicas fraudulentas, conocidas como vishing, son hoy una de las principales vías de engaño. El estudio dice que cerca de un tercio de los colombianos que fueron blanco de intentos de fraude digital entre agosto y diciembre de 2024 reportaron que estos se produjeron con esa modalidad.

Pero el espectro de las estafas va más allá de las llamadas. El mismo informe señala que un significativo porcentaje de colombianos fue víctima de engaños a través de correos electrónicos y mensajes de texto. Esta diversificación de métodos subraya la adaptabilidad de los ciberdelincuentes para explotar las vulnerabilidades en el entorno digital.

Un dato alarmante del estudio es que solo una minoría de los colombianos que se enfrentaron a intentos de fraude lograron identificar la amenaza y evitar caer en la trampa. Esto deja ver la necesidad de fortalecer la educación digital y la conciencia sobre los riesgos inherentes al mundo en línea.

Nuevos riesgos

El informe de TransUnion advierte sobre la emergencia de nuevos objetivos para los estafadores. Las comunidades en línea y los videojuegos se han vuelto espacios donde la actividad fraudulenta ha aumentado. Los ciberdelincuentes emplean diversas tácticas

en estas plataformas, desde solicitudes engañosas hasta ofertas falsas, aprovechando la interacción y confianza que se da en estos entornos.

Appdome, empresa especializada en seguridad para aplicaciones móviles, señaló que la creación de videos falsos, que suplantan a personas, será la nueva arma de robo y estafa digital en el mundo. Ya en China, dice la empresa, lograron engañar a un CEO de una empresa para hacer una transferencia de 20 millones de dólares.

La Secretaría Distrital de Seguridad de Bogotá ha emitido alertas sobre el incremento de estafas digitales que utilizan correos electrónicos fraudulentos. Estos mensajes, diseñados para parecer legítimos mediante el uso de logotipos de instituciones judiciales y dominios aparentemente oficiales, buscan generar confianza en los destinatarios. En muchos casos, los correos tienen archivos adjuntos que, al ser descargados, infectan los dispositivos con software malicioso, permitiendo a los atacantes acceder a información personal y financiera de forma remota.

El secretario de Seguridad, César Restrepo, ha insistido en la importancia de la verificación como primera línea de defensa. Confirmar la procedencia de los mensajes antes de interactuar con ellos es fundamental. Lo mismo que desconfiar ante comunicaciones no solicitadas y validar la autenticidad de remitentes.

La proliferación de técnicas como el deepfake y el uso de inteligencia artificial para crear engaños más convincentes añade una capa de complejidad al tema. La capacidad de crear imitaciones muy realistas de voz y video plantea nuevos desafíos para la detección del fraude y exige una vigilancia constante y una actualización de las medidas de seguridad por parte de los usuarios.

Durante el 2020 fueron denunciados en Colombia 5.440 casos de suplantación de sitios web, con un crecimiento del 303 % frente a la cifra del 2019.

¿Cómo protegerse?

- No dé clic en enlaces desconocidos: evite enlaces que lleguen a través de mensajes o correos electrónicos sospechosos.
- Verifique todo: intente comprobar la identidad del remitente a través de números de teléfono oficiales o páginas web.
- Desconfíe de la urgencia y las amenazas: los mensajes que intentan generar un sentido de urgencia o que advierten sobre supuestos riesgos financieros suelen ser señales de alerta.
- No comparta información personal sensible: nunca revele claves bancarias, números de identificación o cualquier otro dato personal a través de correos electrónicos, mensajes de texto o llamadas telefónicas no solicitadas.
- Sospeche de ofertas: las promesas de dinero fácil, precios excesivamente bajos o premios son tácticas comunes de estafa.
- Confirme los correos electrónicos: revise que el correo provengan de dominios legítimos (por ejemplo @policia.gov.co, @bogota.gov.co).
- No descargue nada: los archivos adjuntos en correos de remitentes desconocidos pueden contener software malicioso.

Fuente: https://www.eltiempo.com/

LINK DE LA NOTICIA