Google ha informado que actores maliciosos están utilizando técnicas como el “cloaking” en páginas de aterrizaje para llevar a cabo estafas en las que fingen ser sitios legítimos.

> *“El cloaking está diseñado específicamente para eludir los sistemas y equipos de moderación que revisan el contenido que infringe políticas, permitiendo que el fraude llegue directamente a los usuarios”,* comentó Laurie Richardson, vicepresidenta y directora de Confianza y Seguridad de Google.
>
> *“Las páginas de aterrizaje suelen imitar sitios populares y generan una sensación de urgencia para manipular a los usuarios, incentivándolos a adquirir productos falsificados o engañosos”.*

El cloaking es una práctica en la que se muestra contenido distinto a los motores de búsqueda como Google y a los usuarios, con la intención de manipular los resultados de búsqueda y engañar a las personas.

El gigante tecnológico también observó una tendencia de cloaking en la que los usuarios que hacen clic en anuncios son redirigidos mediante plantillas de seguimiento a sitios de scareware que informan que sus dispositivos están infectados con malware, llevándolos a otras páginas falsas de soporte al cliente que los engañan para que revelen información confidencial.

Otras tácticas recientes adoptadas por estafadores y ciberdelincuentes incluyen:

- El uso indebido de herramientas de inteligencia artificial (IA) para crear deepfakes de figuras públicas, aprovechando su credibilidad y alcance para cometer fraudes de inversión.
- El uso de imitaciones hiperrealistas para estafas de inversión en criptomonedas fraudulentas.
- Estafas de clonación de aplicaciones y páginas de destino, que engañan a los usuarios

para que visiten páginas casi idénticas a las originales, lo que conduce al robo de datos de acceso, descargas de malware y compras fraudulentas.
- Aprovechar eventos importantes y combinarlos con IA para defraudar a personas o promover productos y servicios inexistentes.

Google informó que planea publicar advertencias sobre fraudes y estafas en línea cada seis meses, como parte de sus esfuerzos para educar al público sobre los riesgos.

Muchos de los fraudes relacionados con criptomonedas, como el "pig butchering" (fraude de «cebo y estafa»), provienen del sudeste asiático y son gestionados por organizaciones criminales de China, que atraen a personas con ofertas de empleos bien remunerados solo para confinarlas en fábricas de fraude ubicadas en Birmania, Camboya, Laos, Malasia y Filipinas.

Un informe publicado el mes pasado por las Naciones Unidas señaló que las organizaciones criminales en la región están evolucionando rápidamente, integrando *"nuevos modelos de negocio basados en servicios y tecnologías como malware, IA generativa y deepfakes en sus operaciones, además de abrir nuevos mercados clandestinos y soluciones en criptomonedas para sus necesidades de lavado de dinero".*

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) describió la integración de IA generativa y otros avances tecnológicos en el fraude cibernético como un "multiplicador de fuerza", que no solo aumenta la eficiencia, sino que también reduce la barrera de entrada para delincuentes con menos conocimientos técnicos.

En abril, Google demandó a dos desarrolladores de aplicaciones en Hong Kong y Shenzhen por distribuir aplicaciones falsas de Android utilizadas en fraudes de inversión. A fines del mes pasado, Google, junto con Amazon, presentó una demanda contra el sitio web Bigboostup.com por vender y publicar reseñas falsas en Amazon y Google Maps.

> *"El sitio vendía reseñas falsas de productos a estafadores para publicarlas en sus*

> *páginas de productos en la tienda de Amazon y reseñas falsas de negocios en la Búsqueda de Google y Google Maps"*, dijo Amazon.

Esta situación ocurre poco más de un mes después de que Google anunciara una colaboración con la Alianza Global contra las Estafas (GASA) y la Federación de Investigación de DNS (DNS RF) para combatir las estafas en línea.

Además, Google informó que ha bloqueado o eliminado más de 5.5 mil millones de anuncios que violan sus políticas en lo que va de 2023 y que está lanzando una función de detección de estafas en vivo en su aplicación de Teléfono para Android para proteger a los usuarios de posibles fraudes, aprovechando su modelo de IA Gemini Nano en el dispositivo.

> *"Por ejemplo, si alguien llama afirmando ser de su banco y le solicita que transfiera fondos de forma urgente debido a una supuesta brecha de seguridad en su cuenta, la Detección de Estafas procesará la llamada para determinar si probablemente es spam y, de ser así, puede proporcionar una alerta auditiva, táctil y una advertencia visual de que la llamada podría ser una estafa"*, explicó.

Otra nueva característica de seguridad es la introducción de alertas en tiempo real en Google Play Protect para notificar a los usuarios sobre aplicaciones potencialmente maliciosas, como el stalkerware, que estén instaladas en sus dispositivos.

> *"Al analizar los patrones de actividad reales de las aplicaciones, la detección de amenazas en vivo ahora puede identificar aplicaciones maliciosas que intentan ocultar su comportamiento o permanecer inactivas durante un tiempo antes de involucrarse en actividades sospechosas"*, señaló Google.