Alertan por amenazas de ciberseguridad para usuarios del metaverso

> El metaverso además de una evolución de internet también trae consigo riesgos, alertan expertos.

En la actualidad es difícil escapar a la vida digital, gran parte de las tareas que mucha gente realiza las hace en la red, más ahora que el llamado metaverso es una realidad donde cada vez más personas conviven.

Expertos en informática alertaron que si bien está evolucionando hacia la Web 3.0, impulsada por los avances en criptomonedas, la tecnología blockchain y el almacenamiento descentralizado de archivos, esto también trae consigo muchos riesgos de seguridad para los usuarios.

Un componente central de esta transición es la experiencia tridimensional conocida como metaverso. Sin embargo, este último trae consigo toda una serie de riesgos.

Especialistas, han analizado las principales ciberamenazas y estafas en este universo post-realidad, basadas tanto en técnicas de ingeniería social y phishing ya conocidas como en nuevos métodos de ataque.

Algunos riesgos de seguridad identificados en la Web 3.0 y el metaverso son:

Dominios ENS-DNS para carteras de criptomonedas. El nombre ENS (Ethereum Name Service) elegido podría eliminar el anonimato, revelando la identidad del propietario de la dirección del monedero virtual. Es bastante común ver nombres ENS como 'DebbieSmith.eth' o encontrarlos en los perfiles de Twitter, con lo que se puede averiguar el saldo de dicha persona y atraer a los ciber-delincuentes. El 3.8% de las direcciones .eth encontradas contenían más de 100,000 dólares en Ethereum, mientras el 9% de las direcciones contenían más de 30,000 dólares.

Ataques de ingeniería social. Principalmente realizados a través de redes sociales y destinados a clonación de carteras, estafas del soporte de Metamask y ataques a cuentas 'ballena' con gran cantidad de criptomonedas.

Contratos inteligentes maliciosos.
Los atacantes escriben su propio malware que se sitúa en la cadena de bloques en forma de código de contrato inteligente malicioso. Algunos ejemplos son 'sleepminting' (falsificación de la procedencia de NFT) y atacantes que engañan a los usuarios para que den acceso a sus monederos sin entregarles el activo digital.

Ataques activos a los seed phrase o frases semilla y filtración intencionada de frases semilla de carteras.

Aunque la tecnología de la Web 3.0 todavía no ha evolucionado para ofrecer un metaverso completo, hay algunos aspectos clave que deben tener en cuenta los usuarios al interactuar en este espacio virtual.

Practicar los fundamentos básicos de seguridad. Elige contraseñas sólidas, utiliza la autenticación multifactor, examina las direcciones de los dominios ENS y de las criptocarteras en busca de errores tipográficos astutamente ocultos y nunca hagas clic en enlaces no solicitados a través de redes sociales o correo electrónico.

Proteger la frase semilla. Cada vez más, las carteras de criptomonedas se utilizan para la identificación y personalización de los usuarios en el Metaverso. Nunca debe compartirse con nadie (especialmente en forma de código QR), pues al perder la frase semilla se pierde el control sobre la identidad y todas las pertenencias digitales personales.

Utilizar un monedero de hardware. El uso de un monedero de hardware añade otra capa de seguridad a las criptodivisas/NFTs, ya que se debe conectar el dispositivo, validar con PIN y aprobar/rechazar cualquier transacción que implique la dirección del monedero.

Investigar las compras. Antes de comprar/minar NFTs, busca la dirección del contrato inteligente y mira si el código fuente está publicado. Un código fuente no publicado es una bandera roja. También se recomienda utilizar una dirección de cartera recién generada que contenga sólo los fondos necesarios para la compra.

"A medida que la Web 3.0 y el metaverso maduran, atrayendo usuarios e inversiones adicionales, se espera que este espacio también implique un mayor interés por parte de los ciberdelincuentes, con ataques que se intensifican tanto en términos de volumen como de sofisticación", concluyó Schultz.

Fuente de información: forbes.com.mx