OVATION
AMERICAS

Boletín Marzo 2022

Privacidad y Seguridad de las CRIPTOMONEDAS Proteja sus activos (Parte1)

Los ingresos de la estafa criptográfica en 2021 superaron los $ 7.7 mil millones, un 81 por ciento más que en 2020, según la plataforma de datos blockchain Chainalysis.

La privacidad y seguridad de su billetera criptográfica es una parte crucial de qué tan

exitosamente invertirá en criptografía. Una vez que mantenga su criptomoneda en billeteras, debe tener en cuenta que todos los tipos de billeteras criptográficas, incluso las billeteras de disco duro más seguras, están expuestas a cierto riesgo de ser pirateadas y drenadas. Aunque la tecnología blockchain está diseñada para ser extremadamente segura y una base de datos blockchain es casi imposible de hackear, los errores humanos y los riesgos físicos aún existen. Los riesgos pueden variar y cambiar constantemente, pero estas son algunas de las formas más vistas de perder todas sus criptomonedas de la noche a la mañana.

Malware de robo de claves

El malware que roba claves escanea el disco duro de su computadora o dispositivo móvil en busca de sus claves privadas criptográficas. El malware que roba claves puede irrumpir en su dispositivo cuando visita sitios web dudosos, sigue los enlaces de los estafadores, abre archivos adjuntos inseguros o descarga software de fuentes no confiables. Una vez que descarga malware que roba claves a su computadora o dispositivo móvil, escanea instantáneamente los discos duros en busca de sus claves privadas criptográficas y las pasa a un hacker. Si no protege sus billeteras criptográficas con autenticación de dos factores además de la clave, la persona que controla el malware ahora tendrá acceso a su cuenta y podrá transferir sus activos en unos segundos.

Troyano

Un troyano o caballo de Troya es otro tipo de malware de robo de criptomonedas. Los troyanos en realidad no "roban" sus criptomonedas, sino que escanean sus discos duros en busca de la cantidad exacta de criptos que posee. Luego cifran maliciosamente sus discos duros y le envían correos electrónicos y muestran mensajes para exigir rescates. Incluso los intercambios bien protegidos pueden encontrar dicho ransomware, y a veces los usuarios no tienen otra forma de lidiar con el dilema cuando el ransomware amenaza con formatear discos duros si los usuarios no pagan el rescate dentro de un cierto período de tiempo.

Estafa de salida

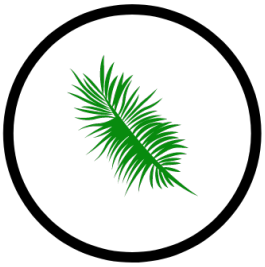
Una estafa de salida se refiere al momento en que los intercambios, intermediarios o administradores desaparecen con el dinero de los inversores. Es una versión criptográfica de un viejo truco de confianza que ha existido durante siglos. En el pasado, los administradores de fondos o los fundadores de startups podían huir con el dinero de los inversores. En la industria de las criptomonedas, los intercambios pueden desaparecer con los depósitos de sus usuarios; Los gerentes o propietarios de proyectos criptográficos podrían huir con los fondos recaudados durante una oferta inicial de monedas (ICO). Debido a la naturaleza descentralizada y anónima del mundo criptográfico y los marcos regulatorios limitados, puede ser más difícil rastrear a los estafadores y recuperarse fondos en

comparación con las estafas tradicionales. Las estafas de salida ocurren con frecuencia, los usuarios deben aprender a detectar posibles estafas antes de realizar inversiones en criptomonedas.

Phishing

Un ataque de phishing generalmente se lleva a cabo a través de correos electrónicos, mensajes o redes sociales. Es posible que reciba un correo electrónico o un mensaje pidiéndole que tome medidas, incluido el envío de su código de autenticación, contraseña, número de tarjeta de crédito u otras credenciales. Sin embargo, el correo electrónico no es legítimo o no intenta hacerse pasar por otra persona. Si responde a estos correos electrónicos de phishing y les da información, sus activos criptográficos pueden ser robados. No confíes en nadie que te pida tus credenciales y contraseñas.

Pérdida de dispositivos



Después de todo, existe la forma anticuada de perder sus pertenencias: literalmente perder sus dispositivos móviles (o computadoras portátiles). Cualquier persona que encuentre su dispositivo o lo robe físicamente también puede intentar desbloquearlo. Si logran desbloquear su dispositivo, pueden acceder a sus tenencias criptográficas almacenadas en las billeteras de ese dispositivo, así como a sus cuentas bancarias, correos electrónicos, contraseñas, cuentas de redes sociales y cualquier otra cosa de valor conectada a su dispositivo.

Cómo proteger y asegurar sus activos

1. Tome medidas básicas de seguridad en Internet. Utilice contraseñas seguras y actualizadas. No visite sitios sospechosos ni haga clic en enlaces sospechosos. No utilice "WiFi gratuito". Utilice herramientas de seguridad de Internet como programas antivirus y VPN. Habilite la autenticación de 2 factores para todas sus cuentas.

2. Recuerda que tú eres el eslabón débil. De hecho, hackear el código de una cadena de bloques o pasar por el sistema de seguridad de un sitio web es muy difícil y requiere habilidades especializadas que la mayoría de los delincuentes no poseen. Es mucho más fácil para un ladrón hacerse pasar por una parte de confianza o enviarle enlaces comprometidos con la esperanza de que haga clic en ellos.

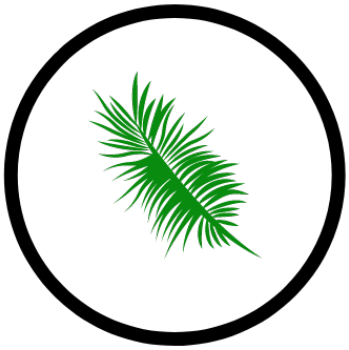
3. Siempre tenga cuidado y verifique cada notificación que reciba. La precaución lo mantiene alejado de promotores criptográficos dudosos, intercambios sospechosos que pueden desaparecer en cualquier momento, correos electrónicos y mensajes de phishing, etc. Elija sus fuentes de descarga de software y aplicaciones sabiamente: los sitios web oficiales y las tiendas como la App Store de Apple pueden ser una buena opción (aunque Google Play Store se ha identificado como una fuente importante de malware para Android). Si aparece un recordatorio cuando intentas acceder o descargar algo, lee el recordatorio y piensa si aún quieres

acceder y descargar lo que has planeado.

4. Teniendo en cuenta todos los riesgos y estafas mencionados anteriormente, es mejor controlar su propia billetera almacenada localmente con una aplicación de software de código abierto que almacena, acepta y transmite monedas virtuales directamente desde su computadora, una de las opciones más seguras para proteger sus activos de criptomonedas. Cuando su billetera se desconecta de Internet, ningún hacker puede verla y atacarla directamente. La seguridad criptográfica es una cuestión de buenos hábitos personales.

   Se estima que el 23% de todas las criptomonedas se han perdido debido a billeteras inaccesibles, si elimina el archivo o pierde el acceso, ha perdido su dinero en su interior. Por favor, no seas parte de esta estadística. Consideramos las monedas virtuales como una herramienta entre otras para proteger la privacidad o el anonimato en línea y nunca una inversión. En general, la mayoría de nuestros clientes no tienen ningún uso para ello.

Sigamos aprendiendo y manteniéndonos al día sobre temas de ciberseguridad para darnos la mejor oportunidad de evitar hackeos y estafas costosas.



OVATION
AMERICAS