Cómo proteger tus cryptos con un hardware wallet

Mantener un secreto digital, sin dejar de tener acceso a él, es sorprendentemente difícil. Pero, existe la posibilidad de saber **cómo proteger tus cryptos con un hardware wallet**.

Hay varias formas de lidiar con el desafío de asegurar tus fondos: una es subcontratar toda la seguridad dejando tus fondos en un intercambio.

Otra manera, es un pequeño dispositivo de seguridad dedicado, es la mejor opción para los usuarios habituales, ya que proporciona una administración segura de claves mientras mantiene tus fondos accesibles y utilizables. A continuación conoce todo sobre el resguardo que debes hacerle a tus cryptos.

Cómo proteger tus cryptos con un hardware wallet de la forma más segura

Las amenazas no son solo abstractas o teóricas; siguen apareciendo nuevas estafas y las viejas están latentes. Ya sea que se trate de una billetera falsa configurada para engañar a los usuarios, un intento de phishing para robar claves privadas o incluso un plan de criptomonedas falso, debes tenerlo en cuenta en todo momento.

Sin embargo, tomando unos simples pasos, los defensores de las criptomonedas (ya sea Bitcoin, o cualquier otro medio) pueden protegerse de muchos ataques comunes.

Mantener el control de tu criptodivisa merece la pena, al igual que mantener tu dinero en efectivo fuera de la vista en una caja fuerte.

Pero primero aclaremos qué se entiende por "billetera Bitcoin". Una billetera Bitcoin es una billetera digital donde se almacenan Bitcoins. Obviamente, no se trata de almacenarlos en cualquier lugar, ya que contienen una clave privada o un número secreto para cada dirección de Bitcoin registrada en la billetera.

Hay varios tipos de billeteras Bitcoin: billetera de escritorio, móvil, en línea (o web), de hardware o de papel. Pero en este caso hablaremos de cómo proteger tus Cryptos con un hardware Wallet o billetera de hardware.

Los bienes digitales deben estar protegidos en “almacenamiento en Frío”

Un paso importante para proteger tus cripto es almacenar cualquier cosa de valor significativo en una cartera de hardware.

Los expertos advierten que no se debe almacenar grandes cantidades de monedas a través de los intercambios de criptodivisas, ni guardarlas en aplicaciones de algún monedero digital en el Android o el ordenador.

Ya que en la Internet pública, hay demasiadas maneras en que los atacantes o malware pueden tratar de hackear tu cartera o engañarte para que les des acceso.

Te gustará leer: Tesla invierte 1.500 millones de dólares en Bitcoin y dispara su valor

Selecciona carteras de hardware seguras

El precio para comprar carteras de hardware seguras como Trezor o Ledger Nano S es alrededor de $100 o menos, y es fácil de configurar.

Simplemente eliges un código PIN y una "semilla" de recuperación compatible (generalmente es un conjunto de palabras y números) en caso de que olvides tu PIN, o tu billetera funcione incorrectamente.

Esta es una seguridad muy confiable, así que asegúrate de guardar una copia del PIN y la semilla donde puedas acceder a ella, pero que los intrusos domésticos no puedan acceder.

Emin Gun Sirer, un investigador de criptografía y sistemas distribuidos de la Universidad de Cornell, incluso recomienda que "guardes una copia security de la clave semilla en una caja fuerte a prueba de fuego".

Poca cantidad para facilitar seguridad en las transacciones

La desventaja de una billetera de hardware es que hace que aprobar transacciones sea un poco engorroso. Si deseas un acceso más fluido a las criptomonedas, los expertos recomiendan almacenar una pequeña cantidad en la App de la billetera para facilitar las transacciones de bajo valor.

La clave aquí: solo guarda la cantidad que estás dispuesto a perder en la aplicación y nunca le des ninguna clave privada a nadie.

Aplicaciones como Mycelium Wallets, que pueden interactuar con carteras de hardware populares, pueden hacer que tu configuración sea más fluida.

Las opciones basadas en aplicaciones, como Samourai Wallet, están trabajando arduamente para ver priorizar funciones sólidas de encriptación y privacidad. **Sin embargo, no confíes en ninguna aplicación donde tengas que guardar demasiado dinero en efectivo, por ahora.**

Te puede gustar: Elon Musk dispara el DogeCoin tras su reaparición en twitter

Considera dónde almacenar la clave privada

Esta es la parte secreta del conjunto de claves pública y privada que te permite autorizar la revisión de la cadena de bloques. Cífralos siempre, y trata de evitar colocarlos en dispositivos que uses a menudo para realizar muchas tareas diferentes, como por ejemplo tu PC personal.

También considera cuidadosamente tu transacción por la pantalla. Hay miles de instituciones maduras y confiables, pero siempre surgen nuevas y sofisticadas criptomonedas, y hay dudosas emisiones iniciales de tokens, que pueden no tener nada detrás, pero aún se están moviendo.

Te puede interesar: Bitcoin imparable: sobrepasa los $50.000 y alcanza máximos históricos

Para proteger tu vida digital en general, también ayuda a proteger tu criptomoneda

Philip Martin, director de seguridad de Coinbase, dijo: "Alentamos a todos los clientes a que realicen algunas acciones básicas gratuitas para colocarlos sobre una base más estable y segura".

Esto quiere decir, que usa un administrador de contraseñas y emplea identidades duales. Verifica y utiliza protocolos de seguridad mejorados para proteger tu dirección de correo electrónico.

Martin incluso, sugiere activar las nuevas funciones de protección avanzadas de Gmail y / o agregar medidas defensivas como un PIN o contraseña a tu número de teléfono. Para que le sea más difícil al atacante controlar tu cuenta transfiriendo la SIM a tu propio dispositivo.

Todas estas técnicas pueden mejorar tu nivel de seguridad y salud digital en general. Pero son especialmente útiles para reducir tu exposición a estafas de criptomonedas más simples.

Algunos consejos para seguir minimizando los riesgos

Ten cuidado con los sitios de phishing. Ya sea que inicies sesión en un intercambio o en una billetera en línea, asegúrate de que sea en la dirección correcta.

Muchos sitios web falsos imitan los intercambios con el único propósito de robar tus datos de inicio de sesión. **Siempre verifica si funciona la dirección del sitio.**

Conéctate solo a términos web seguros con certificados HTTPS

La mayoría de los sitios legítimos tienen uno. Para mayor seguridad, prueba los complementos del navegador como "HTTPS Everywhere".

Utiliza una conexión Wi-Fi segura

Nunca inicies la sesión en tu billetera en línea, cuenta de intercambio u otro punto de seguridad crítico a través de WiFi público. Incluso cuando te encuentres en un lugar seguro, verifica que tu punto de acceso WiFi utiliza un cifrado sólido, como el protocolo WPA-2.

Separa tus fondos por seguridad

No guardes todos tus activos criptográficos en un solo lugar. **La mejor manera de administrarlos es utilizar uno o más almacenes fríos para las tenencias a largo plazo, y al menos una billetera caliente para el comercio.**

Autenticación de dos factores

Asegura siempre tus cuentas con 2FA. Si es posible, utiliza software o hardware 2FA en lugar de SMS.

Lista blanca de direcciones IP y retiros

Si tienes una dirección IP estática, úsala por tu seguridad. Cerciórate de que solo tú puedas acceder a tus cuentas y fondos.

Verifica las direcciones criptográficas

Algunos programas maliciosos de la web pueden editar y pegar una dirección de transacción incorrecta cada vez que realizas una avenencia. Por lo general, la nueva dirección es propiedad de un atacante. ¡Es mejor prevenir que lamentar!

Utiliza medidas de seguridad que puedas administrar

Algunas personas nunca se sienten seguras y hacen todo lo que está a su alcance para dogmatizar su criptomoneda.

Sin embargo, olvidan que también pueden perder el acceso a sus cuentas y a sus fondos. No compliques demasiado tu resguardo si ese no es el objetivo. **Busca un equilibrio adecuado entre complejidad y seguridad.**

Ventajosamente, no necesitas ser un experto en cifrado para saber cómo proteger tus cryptos con un hardware wallet, y así prevenir la mayoría de los posibles ataques que te hagan.