¡Cuidado! Hay estafas informáticas con las criptomonedas

La cadena de bloques ha crecido rápidamente en los últimos años, pero no es inmune a los ataques de seguridad. En este artículo señalo las principales preocupaciones de **seguridad informática** a las que se enfrentan las empresas y los inversores.

Algunas criptodivisas han sido víctimas de ataques por parte de ciberdelincuentes. ZenCash y Ethereum Classic perdieron millones de dólares debido a problemas de seguridad de blockchain. **Pero la piratería no es el único riesgo de seguridad para las criptomonedas, también pueden ocurrir estafas de tipo multinivel.**

Principales amenazas de seguridad informática a las criptomonedas

El problema de seguridad surge del uso de claves y transacciones en la cadena de bloques, debido a que son datos potencialmente visibles para todos los usuarios. Las adquisiciones de cuentas pueden permitir a las personas robar tu clave privada, que es la principal forma en que pueden tomar tu dinero.

La naturaleza imposible de rastrear de algunos activos de Bitcoin o criptomonedas significa que es un objetivo ideal para piratas informáticos y estafadores. Grandes grupos de piratas informáticos pueden trabajar para eliminar cuentas individuales, así como plataformas criptográficas completas.

Ciberseguridad en el uso de criptomonedas y tipos de estafas

El usuario que se está preparando para utilizar criptomonedas no solo debe ser consciente de cómo realizar una transacción a nivel práctico, sino que debe preocuparse por la custodia segura de sus credenciales criptográficas.

El sistema de criptomonedas, del cual Bitcoin es el ejemplo más significativo, se basa en registros públicos descentralizados en varios nodos participantes y cuyas "páginas" están formadas por bloques.

Cómo manipular mensajes de WhatsApp

Cada bloque que se agrega gradualmente a la cadena contiene un número variable de transacciones realizadas por los usuarios y para ser válida debe estar firmada con la clave privada del usuario que la realiza, única prueba válida y necesaria para la atribución de un determinado activo a un tema.

Cada uno de los nodos que participan en la cadena de bloques guarda una copia del registro completo y se encarga de crear nuevos bloques resolviendo problemas criptográficos cada vez más complejos. La finalidad es crear un nuevo bloque que, según un criterio de diseño específico, integre la impronta del anterior y de las transacciones contenidas en el mismo, volviendo paulatinamente inmutable el propio registro.

Tipos de estafas

Entre las estafas más comunes se incluyen:

Estafas de obsequios en las redes sociales

Debes tener cuidado con los grupos y usuarios de las redes sociales (en Facebook, Telegram y Twitter), que a veces se hacen pasar por figuras notables en el espacio criptográfico ofreciendo obsequios.

Sitios web clonados

Siempre recomiendo verificar dos veces la URL y marcar los sitios web visitados con frecuencia. Los sitios web clonados usarán letras similares en la URL para que se vea como la real de un vistazo rápido.

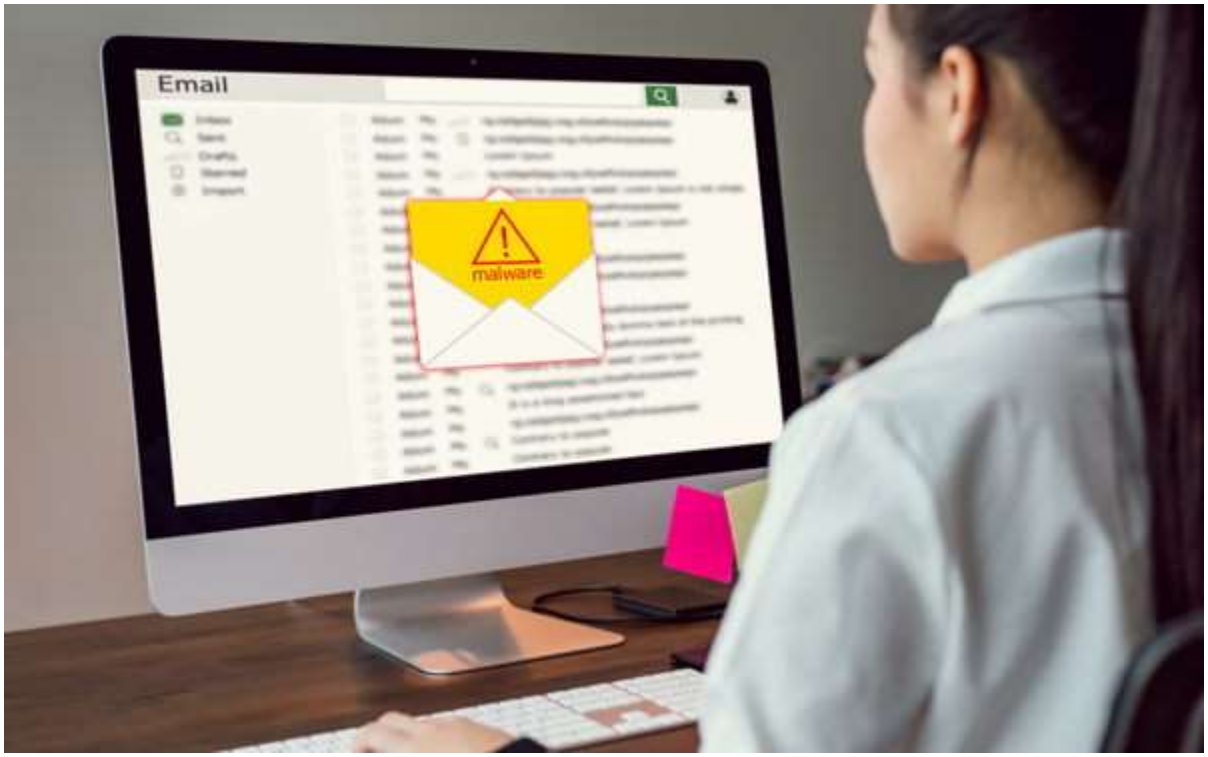
La Importancia del Informe Pericial Informática WhatsApp

Estafas publicitarias

Algunos anuncios publicitarios conducen a sitios de phishing. Los principales navegadores (Google Chrome, Mozilla Firefox, Microsoft Edge) permiten la instalación de extensiones especiales de bloqueador de anuncios y bloqueador de scripts (por ejemplo, AdBlock Plus, no-Script, uBlock).

Hacks de DNS

Un pirateo de DNS ocurre cuando el tráfico se redirige desde el sitio web legítimo al sitio fraudulento mediante la modificación de los registros DNS del sitio legítimo. **Esto significa que un usuario visita la URL correcta, pero sin saberlo es redirigido a un sitio fraudulento.** Una excelente manera de evitar los ataques al DNS es verificar el certificado SSL del sitio web que estás visitando.



Estafas por correo electrónico

Se trata de correos electrónicos falsos que mediante un enlace pueden redirigir a los usuarios a sitios web clonados para robar información personal y posteriormente robar los fondos. Estos a menudo surgen durante las ventas colectivas de ICO. Los estafadores han obtenido bases de datos de correos electrónicos y otra información personal de ICO anteriores en un esfuerzo por desplumar a los futuros inversores de sus fondos.

¡Cuidado con las estafas de whatsapp!

Aplicaciones e intercambios falsos

Cuando se trata de intercambios, apégate a los conocidos como Binance, Kraken, Bitfinex, Kucoin, Huobi, Bibox, Coinbase y Gemini. **Además, ten cuidado con la legitimidad de las aplicaciones que descargas en tu teléfono o navegador.**

Minería de malware y criptografía

El malware en cripto se presenta en dos formas; lo más común ocurre cuando se instala un software malicioso, en un dispositivo móvil o en una computadora, generalmente con el consentimiento ingenuo del usuario.

El malware de minería criptográfica es la segunda forma. En este caso, el malware utiliza en secreto los recursos de la computadora infectada para extraer criptomonedas, creando efectivamente una red de minería descentralizada.

Cómo evitar estas estafas informáticas

Si recibes un correo electrónico que habla sobre el aumento del saldo de criptomonedas o la necesidad de restablecer tus datos, asegúrate de verificar su identidad.

Tu clave privada es sagrada. La forma en que funcionan Bitcoin y otras criptomonedas significa que tu clave es algún tipo de vulnerabilidad si cae en manos de otra persona.

Por eso, la creación, uso y custodia de la clave privada de la billetera son esenciales para mantener el control sobre los activos. Recuerda que cada transacción es irrevocable y los fondos a disposición, aunque registrados de manera segura e inmutable en la cadena de bloques no están directamente en un medio tangiblemente disponible.

En la cadena de bloques no existe un sistema de "restablecimiento de contraseña" como en los servicios centralizados más comunes.

Cómo falsificar una conversación de WhatsApp

Consejos para evitar este tipo de amenaza

- Usar contraseñas complejas, un sistema operativo actualizado, protegido por un antivirus actualizado y software específico anti-malware y anti-ransomware, junto con recomendaciones generales de seguridad, como no visitar categorías de sitios notoriamente inseguros.
- Instalar en los navegadores extensiones especiales de bloqueador de anuncios y bloqueador de scripts que se encargan de reconocer e interceptar los banners, publicidad y código de máquina dinámico que no sea el utilizado para representar la estructura de la página web original.
- No abrir a la ligera los enlaces recibidos por correo electrónico, comprobar siempre en la vista previa que el enlace realmente apunta a la URL indicada. Además, desconfiar de cualquier comunicación con adjuntos o enlaces que sean de carácter urgente, injustificado como para inducirnos a actuar por impulso, sin reflexionar sobre el funcionamiento real y sobre los posibles riesgos.
- Usar VPN, Red Privada Virtual, que es un túnel encriptado, que garantiza el anonimato parcial, pero sobre todo refuerza la seguridad de la conexión, enrutándola en un canal seguro.

- También recomiendo aislar por completo la máquina que se utiliza para las operaciones, utilizando una máquina dedicada físicamente a tal uso o, más prácticamente, utilizando una denominada "máquina virtual".

Finalmente, si bien existen numerosas estafas, esquemas y perpetradores de diversas actividades fraudulentas en todo el cifrado, el mejor enfoque es proceder con un grado razonable de escepticismo y cuidado. A pesar de la cantidad de proyectos fraudulentos, existen innumerables proyectos y grupos de buena reputación y bien administrados que hacen que la inversión en criptomonedas valga la pena.

Recuerda que si necesitas asesoría respecto a la seguridad informática de tus datos o requieres un informe pericial me puedes contactar personalmente a través de: lluis@peritinformatic.com www.peritinformatic.com. Mi nombre es José Luis Martir Millán, perito informático con amplia experiencia en la investigación forense digital y en https://peritowhatsapp.com te podemos ayudar.