GIRONA NOTICIES.COM
+ Periodisme

Las cinco criptoestafas en redes y apps más frecuentes, según Panda Security

Comunicados | 08/03/2022 | 00:00

El importante aumento que se ha producido en las inversiones en criptomonedas durante los últimos años, las ha puesto en el punto de mira de muchos cibercriminales y estafadores online. Así, duplicar las ganancias en cuestión de segundos es tan probable como perderlas. Sin ir más lejos, en los últimos meses se han multiplicado los casos de hackers que por medio de técnicas de phishing suplantan la identidad de famosos para timar a miles de personas con un phishing. Sin embargo, hay muchos más timos

/COMUNICAE/

El importante aumento que se ha producido en las inversiones en criptomonedas durante los últimos años, las ha puesto en el punto de mira de muchos cibercriminales y estafadores online. Así, duplicar las ganancias en cuestión de segundos es tan probable como perderlas. Sin ir más lejos, en los últimos meses se han multiplicado los casos de hackers que por medio de técnicas de phishing suplantan la identidad de famosos para timar a miles de personas con un phishing. Sin embargo, hay muchos más timos

Según un comunicado remitido por Panda Security "es importante conocer los riesgos del mundo de la criptografía". Internet y los procesos de digitalización van de la mano de increíbles mejoras. Pero, también de inmensos riesgos, entre los que las estafas son el una de las principales fuentes de ingresos para para los ciberdelincuentes. Hervé Lambert, Global Consumer Operations Manager de Panda Security, explica: “Los datos hablan de un volumen excelso del criptofraude. Y esto no es fruto de la casualidad, surgieron cuando el Bitcoin estaba en su valor máximo, algo que es muy atractivo para los criptoestafadores”.

1. Cuentas verificadas que en realidad son falsas

Es común que los hackers también falseen un perfil de Twitter o de Instagram e incluyan la marca de verificación azul en el lugar exacto donde ésta debería estar. Para no caer en la trampa, es tan fácil como situar el ratón y pulsar sobre ella. Si es real saldrá una ventana emergente con la información de la cuenta.

2. Sorteos y regalos en Instagram, Facebook o Twitter

Los estafadores se hacen pasar por promotores de una marca o por famosos para vender a los

usuarios la posibilidad de duplicar sus ganancias en Bitcoin y otras criptodivisas. Para que esto ocurra, piden a la víctima que deposite su dinero en una dirección de billetera que proporcionan. Una vez envíado, nunca volverá a su bolsillo.

Para evitar caer en estos engaños, primero hay que buscar el sorteo o la promoción en google e infórmate de si ha salido alguna noticia al respecto. Si no aparecen miles de resultados procedentes de fuentes autorizadas, hay motivos para desconfiar. Por último, será necesario consultar el sitio web oficial donde deberían estar colgadas las bases del sorteo. Es importante verificar también que se trata de en una URL auténtica.

3. Catfishing en Tinder

Últimamente se están consumiendo varios documentales sobre grandes estafas cometidas a través de la técnica catfishing. Nada más y nada menos que la técnica basada en usurpar la identidad de alguien para ligar con otras personas por interés y lograr un propósito, nunca bueno. Uno de los más sonados es la última producción de Netflix: El timador de Tinder. Pues bien, se está detectando en la app por excelencia para aquellos que se deciden a conocer gente por internet, varios casos de estafas sobre criptodivisas. Si al hacer match con alguien, intentase venderle la idea de invertir en una criptomoneda, habra que hacer saltar las alarmas y desconfiar.

4. “Vendehumos” en Youtube

Los famosos vídeos con personajes que se presentan como los nuevos gurús del éxito de las criptomonedas, pueden ser cibercriminales y hasta se exponen en directo. Cuentan las novedades, los balances y dicen en qué invertir, pero en la caja de comentarios dejan un enlace con algún tipo de promoción, que en realidad, es la puerta a su fraude. Para ello, hayq que verifica el canal de Youtube, mirar el número de vídeos y de seguidores y si cuenta con la insignia gris de autenticación propia de la plataforma. Eligen la modalidad del directo para no tener que pasar los filtros de revisión del contenido de la plataforma.

5. Cuidado con las respuestas en Twitter

Los cibercriminales están a todo y saben que Twitter es la red social donde más contenido se mueve. Mucha gente está pendiente a las respuestas de tweets de famosos y del hilo que de estos se generan. Los estafadores suplantan la identidad de cuentas verificadas en Twitter de perfiles no tan conocidos para responder según lo que les convenga a los perfiles de grandes celebridades.

En ocasiones, cambian la información del perfil haciéndose pasar por medios de comunicación o programas con notoriedad pública, como fue el caso del robo de cuenta de Troy Stecher para hacerse pasar por el Twitter oficial de “Saturday Night”.

La amenaza no solo está en las redes sociales, sino también en la mensajería SMS de toda la vida. Aunque progresivamente los gobiernos parecen poner el ojo en este mercado, “en el mundo de la criptografía todavía existe un vacío legal grande y la poca regulación al respecto hace que sea muy difícil que puedas recuperar tu dinero; a diferencia de los robos en cuentas bancarias a través de tarjetas de crédito que son más fáciles de rastrear. Por eso, el mejor mecanismo de defensa ante estos ataques es que refuerces tus sistemas de seguridad digital y estés ojo avizor con mensajes, notificaciones o promociones que suenen muy tentativas sobre maneras rápidas y eficaces de ganar grandes sumas de dinero, pero cuyo propósito sea únicamente desfalcarte”, apostilla Hervé Lambert.

Fuente Comunicae

Autor: Redacció

https://gironanoticies.com/comunicado/168665-las-cinco-criptoestafas-en-redes-y-apps-mas-frecuentes-segun-panda-security.htm