osi.es

Detectadas distintas modalidades de fraude a través de plataformas de

7-9 minutos

Están proliferando en la Red distintas modalidades de fraudes, que tienen como objetivo común engañar al usuario para que invierta por Internet en alguna plataforma fraudulenta de inversiones, y quedarse así con su dinero. Los ciberdelincuentes suelen contactar con su víctima a través de redes sociales, foros u otras plataformas online, como pueden ser Facebook, Telegram o Instagram, aunque también hay usuarios que reciben llamadas telefónicas tras haber facilitado sus datos durante el registro en alguna de estas páginas fraudulentas. En cualquier caso, para que las posibles víctimas realicen la inversión les indican que obtendrán rentabilidades muy altas de manera muy sencilla y en poco tiempo.

Recursos afectados

Todo aquel usuario que caiga en el engaño y siga las instrucciones del ciberdelincuente para invertir en las

plataformas online que se le indiquen.

Solución

Si has resultado ser víctima de un fraude de estas características, recopila todas las evidencias que dispongas e interpón una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado.

Además, si para crear la cuenta en la plataforma fraudulenta, reutilizaste una contraseña que uses para acceder a otros servicios online, actualízala lo antes posible para que no accedan a tus cuentas personales. Acuérdate de cambiar también la clave de tu monedero o *wallet*, en caso de que se lo facilitaras a alguien guiado por el engaño.

De manera adicional, si llegaste a descargar alguna aplicación o herramienta bajo sugerencia del "asesor", "amigo" o supuesto "experto inversor", procede a desinstalarla lo antes posible.

También es importante que analices el dispositivo con alguna herramienta antivirus para descartar posibles infecciones o amenazas que pudieran haberse colado en tu equipo a raíz de la instalación de la herramienta anterior.

Finalmente, ponte en alerta y usa el sentido común si contactan contigo o encuentras informaciones en la Red sobre inversiones online, con las siguientes pistas:

1. **Prometen ganancias de forma rápida** y una rentabilidad

más alta que otro tipo de inversiones.

2. La **inversión inicial es baja** en comparación con los posibles beneficios a corto plazo.
3. Se trata de una **oferta disponible solo por tiempo limitado o para nosotros.** Presionan para que actuemos precipitadamente.
4. Ponen mucho énfasis en que se trata de una **operación sin riesgos**.
5. **Intentan que invitemos a familiares, amigos o personas de confianza** a que inviertan en el mismo producto o servicio a cambio de comisiones.
6. Se dirigen a nosotros porque **no tenemos conocimientos en el tema o buscan personas que nunca hayan invertido como público objetivo**.
7. Utilizan **términos complejos y no disponen de información adicional** para comprobar estudios sobre el mercado o proyecto para demostrar sus palabras.
8. Utilizan la **imagen de personajes famosos y medios de comunicación reconocidos** para dotar de mayor credibilidad al fraude.

Detalles

Se está identificando un elevado número de fraudes en los que los ciberdelincuentes engañan a sus víctimas ofreciéndoles unas rentabilidades muy altas por una inversión baja de dinero. Para no caer en esta trampa y

perder todo nuestro dinero hay que informarse bien y contrastar la información antes de proceder a invertir en cualquier plataforma online. Frecuentemente, las víctimas potenciales son contactadas a través de perfiles fraudulentos de redes sociales, aunque los fraudes también se difunden por foros, grupos o canales de chat, de servicios como Telegram, Facebook o Instagram, o incluso a través de anuncios publicitarios fraudulentos, de forma que un usuario puede caer en las redes de los estafadores simplemente por el mero hecho de buscar información sobre inversiones en webs, foros o grupos no contrastados.

En muchos de los casos identificados, independientemente del medio por el cual los usuarios llegan hasta el fraude, se les convence para que inviertan dinero principalmente en criptoactivos, por ejemplo, 250€. Para dotar de mayor credibilidad al fraude, y que el trámite parezca lógico y habitual para este tipo de gestiones, se les piden datos personales, como DNI, número de cuenta bancaria, etc. Tras realizar la supuesta inversión, es posible que durante varios días los ciberdelincuentes llamen a sus víctimas para informarles de cómo van sus inversiones, hasta que en una de estas comunicaciones les notifican que la cantidad invertida es un importe muy bajo y que tendrían que invertir más cantidad de dinero para aumentar la rentabilidad, por ejemplo, otros 2.000€. Los usuarios, al no interesarles la propuesta al ser una cantidad de dinero más elevada,

intentarán recuperar su inversión inicial de 250€, pero se encontrarán con que la web tiene bloqueado sus accesos y, por tanto, no podrán recuperarlo.

Se han identificado otros casos, cuyo *modus operandi* es el siguiente: el usuario, tras ser engañado para invertir, se crea una cuenta en una plataforma fraudulenta. Al principio solo invierte una pequeña cantidad de dinero, pero en la web puede ver cómo las acciones suben rápidamente su valor. En este punto es importante indicar que como se trata de una falsa plataforma, las acciones/activos suben de manera ficticia para hacer creer a la víctima que está obteniendo grandes beneficios. Se le incita a invertir más cantidad de dinero para obtener una supuesta recompensa. Si el usuario accede y coloca más dinero, seguirá viendo en la plataforma cómo sus beneficios van aumentando. Sin embargo, en algún momento, cuando el usuario quiera recuperar su dinero verá cómo está “bloqueado” o que no se puede retirar por alguna cuestión técnica. Obviamente, será la excusa que utilicen los estafadores, ya que desde el principio todo se trata de un engaño.

Otras casuísticas identificadas también:

- El usuario invierte dinero en una plataforma falsa, y pasados unos días, cuando intenta retirar sus beneficios, le piden una comisión y otros pagos en conceptos varios, como por ejemplo, un certificado.
- Tras invertir, se le indica al usuario que como sus

ganancias son elevadas, debe crearse una cuenta prémium de pago. De no acceder a las peticiones, no podrá retirar su dinero.

- A través de una canal de Telegram el usuario hace una consulta técnica sobre una plataforma legítima en la que ha invertido en criptomonedas. Le contacta una persona que se hace pasar por el soporte y le remite a otra página web. Bajo engaño le facilita la llave del monedero, motivo por el cual ha perdido todo el dinero que tenía en el balance.
- El usuario ha invertido dinero en una plataforma falsa, y para retirarlo le piden que haga más ingresos, pero además, le intentan convencer para instalarse una herramienta de acceso remoto, que realmente copiará toda la información de su cartera a la de los ciberdelincuentes.

  Como podemos ver en todos los casos mencionados, el objetivo final siempre será hacerse con el dinero del usuario, y para ello, le harán creer que invirtiendo en la plataforma que se le indique ganará mucho dinero en poco tiempo, pero la realidad es que el usuario se verá envuelto en una espiral en la que perderá dinero y difícilmente podrá recuperarlo.

  ¿Te gustaría estar a la última con la información de nuestros avisos? Anímate y suscríbete a nuestros boletines o al perfil de Twitter @osiseguridad y Facebook. Serás el primero en enterarte de los últimos avisos de

seguridad dirigidos a ciudadanos. También ponemos a tu disposición la Línea gratuita de Ayuda en Ciberseguridad de INCIBE: 017, y nuestros canales de mensajería instantánea de WhatsApp (900116117) y Telegram (@INCIBE017).