

PLAN MAYOR



SEGURIDAD

FICHA DIFUSIÓN EN CIBERDELINCUENCIA



Estafas en plataformas de inversión falsas (falso Broker)



COMANDANCIA DE MADRID
JEFATURA DE PERSONAL
NEGOCIADO DE FORMACIÓN
"PLAN MAYOR SEGURIDAD"

1.Finalidad:

En los últimos meses, se ha detectado un aumento significativo en las denuncias por una nueva modalidad de “ciberestafa”, consistente en engañar a personas, **principalmente a mayores de 65 años o con poca formación tecnológica**, para que inviertan en plataformas fraudulentas, prometiendo altas rentabilidades en poco tiempo y con aparente facilidad. Esta ficha busca informar y concienciar a la ciudadanía sobre este tipo de delitos, proporcionando recomendaciones clave para evitar caer en las trampas de los estafadores.

2. Breve descripción del modus operandi:

Los “ciberdelincuentes” emplean diversas técnicas para captar a sus víctimas, utilizando redes sociales o anuncios dirigidos en páginas relacionadas con inversiones en criptomonedas. El proceso de estafa suele seguir estos pasos:

- **Primer contacto:** atraen a los usuarios mediante publicidad engañosa o contactan con ellos directamente a través de redes sociales.
- **Generar confianza en la víctima:** proponen una primera inversión con una cantidad reducida de dinero y prometen beneficios inmediatos, que en muchas ocasiones llegan a producirse inicialmente, logrando de esa forma conseguir ganar la confianza de la víctima.
- **Inversión mayor:** una vez ganada la confianza, incentivan a la víctima a realizar nuevas inversiones y de mayor cuantía.
- **Bloqueo y nuevas exigencias:** cuando la víctima sospecha del fraude e intenta recuperar su dinero, los estafadores exigen pagos adicionales para poder liberar los fondos, ocasionando así mayores pérdidas a la víctima.

Recomendaciones:

- Nunca confíe en personas que le contacten por redes sociales o teléfono ofreciendo inversiones con altas rentabilidades y bajo riesgo.
- Antes de invertir, sea prudente, no tenga prisa y verifique la legitimidad de la plataforma o la agencia de inversión consultando a organismos oficiales, como la Comisión Nacional del Mercado de Valores (CNMV), o en su entidad bancaria.
- Los estafadores suelen usar tácticas de urgencia para evitar que analice las ofertas con detenimiento y pueda descubrir su carácter fraudulento. Tómese su tiempo antes de tomar decisiones financieras.
- Evite descargas sospechosas, puede estar instalando aplicaciones que permitan el acceso remoto a tu dispositivo, como Anydesk, TeamViewer o RustDesk, y que pueden ser utilizadas para el robo de información.





**COMANDANCIA DE MADRID
JEFATURA DE PERSONAL
NEGOCIADO DE FORMACIÓN
“PLAN MAYOR SEGURIDAD”**

Teléfono 918073900 ext: 0110438
m-cmd-madrid-planmayor@guardiacivil.org