



 Finanzas
  Para Todos

Estafas y fraudes financieros

Protege tu dinero y tus inversiones

Fraude financiero

Acción engañosa



Con ánimo de lucro



Que causa perjuicio económico a terceros



Chiringuitos financieros

- ✓ Ofrecen servicios de inversión o financiación sin estar autorizados.
- ✓ ¡Estafadores muy peligrosos!
- ✓ Actúan al margen de la ley.
- ✓ Sus víctimas carecen de protección.

¡Confiar en un chiringuito financiero es una forma segura de perder tu dinero!





Evita ser víctima de un chiringuito

- ✓ Comprueba siempre que la entidad está autorizada para prestar los servicios financieros que ofrece.
- ✓ Pide información a la CNMV o al Banco de España.
- ✓ Consulta información adicional de la [CNMV](#) y del [Banco de España](#).





Phishing

Smishing

Vishing



Objetivo: conseguir nuestros claves personales de acceso o datos de la tarjeta de crédito, con el fin de suplantar nuestra identidad, operar con nuestras cuentas y disponer de nuestros fondos.





Precauciones – phishing, smishing y vishing

- ✓ Nunca respondas a solicitudes de confirmar datos confidenciales.
- ✓ No descargues ni ejecutes ficheros adjuntos.
- ✓ No pinches en enlaces sin verificar la URL.
- ✓ Utiliza contraseñas seguras y cámbialas con regularidad.



Desconfía siempre de cualquier correo, mensaje de texto o llamada telefónica que solicita que confirmes claves de acceso a tus cuentas bancarias o datos de tus tarjetas.

Ninguna entidad autorizada pedirá jamás a sus clientes estos datos.



Pharming

- ✓ Parecido al phishing.
- ✓ Un malware redirige a sitios web falsos parecidos a los auténticos.
- ✓ Permite el robo de datos personales.
- ✓ Difícil de detectar.





Precauciones – pharming

- ✓ Instala programas reconocidos antivirus y antimalware y actualiza tus dispositivos.
- ✓ Utiliza un gestor de contraseñas.
- ✓ Evita sitios web sospechosos.
- ✓ Verifica que tienes una conexión segura.



Fraudes con criptoactivos

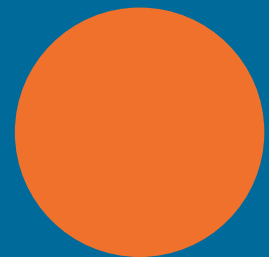
- ✓ Publicidad agresiva en muchos canales (RRSS, anuncios en páginas web, etc.).
- ✓ Promesas de grandes rentabilidades.
- ✓ Presión para tomar decisiones.
- ✓ Información poco clara y llena de tecnicismos.



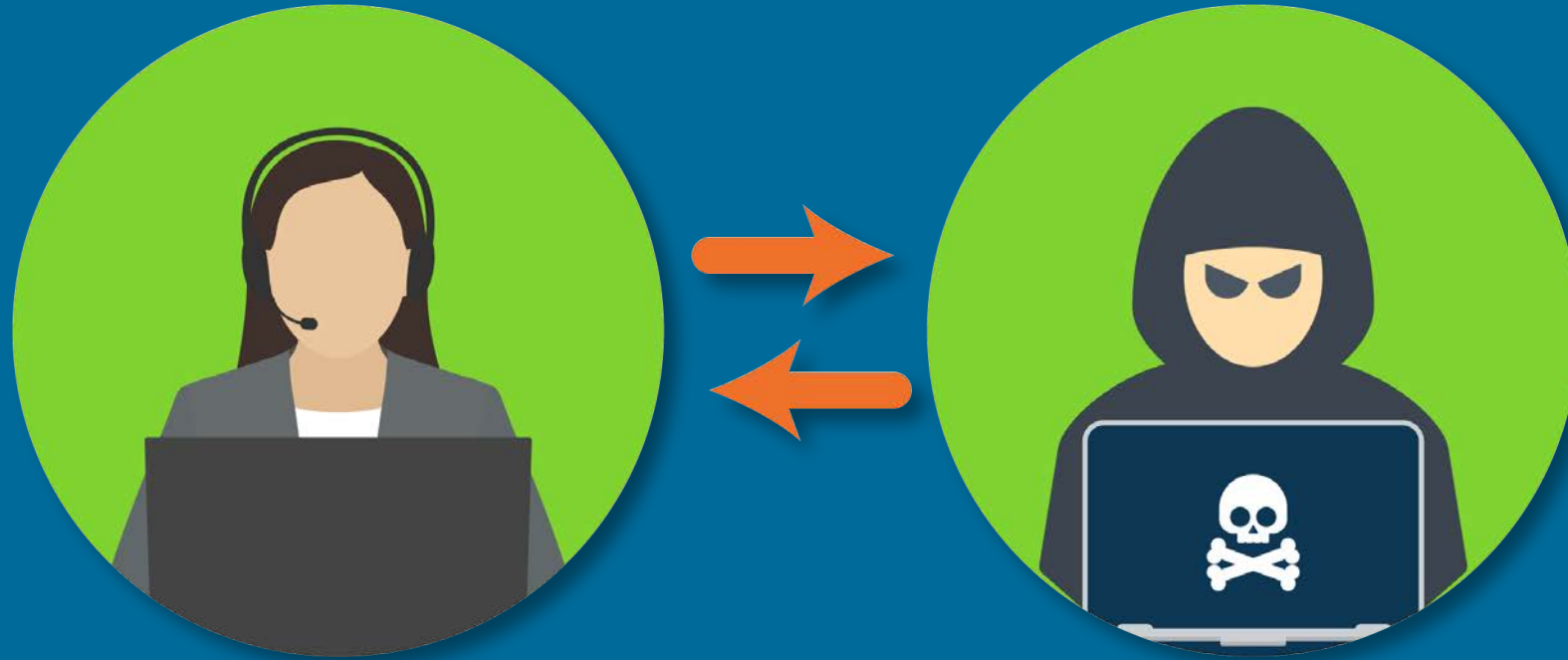


Precauciones – criptoactivos

- ✓ Desconfía de promesas de grandes ganancias en poco tiempo.
- ✓ Comprueba si la empresa figura en la lista negra de advertencias.
- ✓ Nunca inviertas en algo que no entiendes.
- ✓ Recuerda: los criptoactivos quedan fuera de la protección que ofrecen las normas vigentes sobre servicios financieros.



Estafa del técnico informático



- ✓ Se hacen pasar por soporte técnico.
- ✓ Utilizan un programa o una *app* para conectarse a tu equipo remotamente.
- ✓ Acceden a tus cuentas, roban tus datos personales o hacen compras con tu tarjeta de crédito.

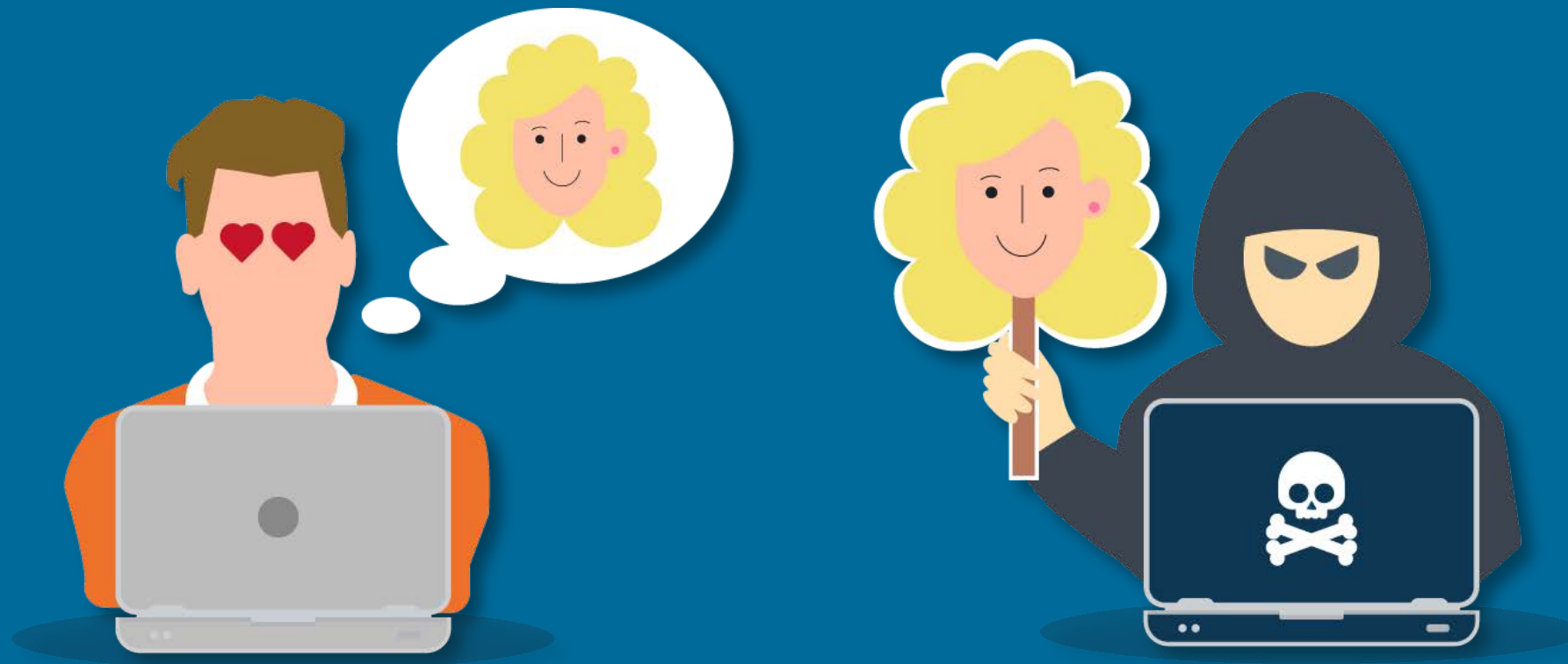


Precauciones

- No compartas con terceros claves de acceso a tus cuentas bancarias y de valores.
- No permitas el acceso remoto a tus dispositivos.
- No inicies una sesión con tus cuentas bancarias y de valores con un tercero conectado.



Catfishing



Estafas
financieras

Extorsión

Robo de datos

Precauciones – Catfishing

- No envíes dinero a alguien que no conoces personalmente.
- Nunca compartas tu número de tarjeta de crédito ni datos de acceso a cuentas online.
- No compartas online información, fotos o vídeos comprometedores.
- Cuidado con los enlaces enviados en redes sociales y chats.





Cuentas de trading financiadas ligadas a cursos de formación



- ✓ Exigen pagar por adelantado un curso para aprender a operar.
- ✓ Suele ser una estafa.



Advertencias – cuentas de trading financiadas ligadas a cursos de formación

- Antes de entregar dinero, ten en cuenta que puede tratarse de un fraude.
- Estos cursos y la apertura de las citadas cuentas no entran dentro del ámbito de actuación/supervisión de la CNMV .



Estafa de “recovery room”



Ofrecen gestionar la recuperación de pérdidas por estafas anteriores.

Pueden intentar que vuelvas a invertir dinero.





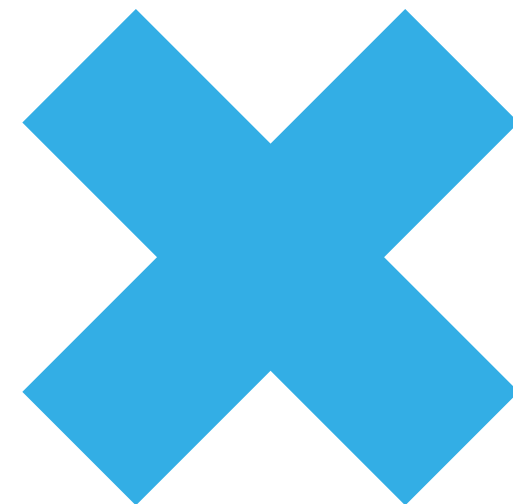
Precauciones – “recovery room”

- Nunca hagas un pago adelantado para este servicio.
- Puedes volver a ser víctima de fraude.
- Desconfía si te contactan en nombre de la CNMV. Es señal de estafa.



Resumen

- ✓ Comprueba que la entidad figura en los registros de la CNMV o del Banco de España.
- ✓ Desconfía de entidades:
 - con datos de contacto incompletos.
 - o con números de móvil cuyo prefijo no es español.



BANCO DE **ESPAÑA**
Eurosistema

Resumen

- ✓ Desconfía siempre de propuestas que no hayas solicitado, a través de cualquier canal.
- ✓ Los intermediarios financieros autorizados no se dirijan a personas que no son clientes con ofertas de inversión.



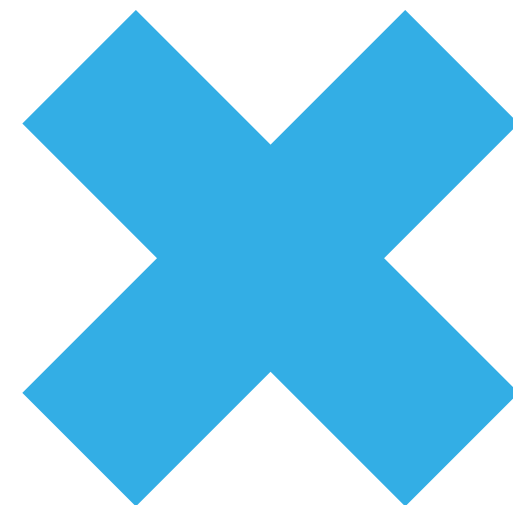
Resumen

- ✓ Desconfía siempre de promesas de grandes rentabilidades, sin riesgo.
- ✓ La inversión siempre tiene riesgo.



Resumen

- ✓ Desconfía de ofertas de entidades en países remotos.



Resumen

- ✓ ¡Protege tus datos personales!
- ✓ Desconfía siempre de los correos electrónicos, mensajes de texto o llamadas telefónicas que solicitan estos datos.
- ✓ No sigas enlaces sin haber verificado su procedencia.



Resumen

- ✓ Desconfía siempre de personas o empresas que intentan hacerse pasar por la CNMV, haciendo recomendaciones o vendiendo productos de inversión.
- ✓ La CNMV nunca recomienda inversiones.





Finanzas Para Todos

 <p>CNMV COMISIÓN NACIONAL DEL MERCADO DE VALORES</p>	 <p>BANCO DE ESPAÑA Eurosistema</p>	 <p> GOBIERNO DE ESPAÑA</p>	 <p>VICEPRESIDENCIA PRIMERA DEL GOBIERNO MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL</p>
<p>plan de educación financiera</p>			