GUÍA PHISHING; Protégete y Actúa.

El phishing es una técnica de fraude en línea que se utiliza para engañar a las personas y obtener información personal y financiera.

Entendemos lo angustiante que puede ser haber sido víctima de una estafa de phishing y queremos transmitirte un **mensaje tranquilizador**. Como despacho, estamos aquí para ayudarte y queremos que sepas que haremos todo lo posible para que recuperes tu dinero.

Puede que te sientas culpable de la estafa, pero lo cierto es que **los Bancos** son los **responsables** de no protegerte debidamente delante de estas estafas y es por eso que los tribunales les obligan a pagar a sus clientes, el dinero que se les ha sustraído.

Aquí hay una guía práctica sobre cómo detectar y evitar las estafas de phishing:

¿Qué es el phishing? El phishing es una técnica de fraude en línea que se utiliza para engañar a las personas y obtener información personal y financiera con el fin de sustraer dinero de las víctimas.

¿Cómo detectar el phishing?

Los estafadores utilizan correos electrónicos y mensajes de texto para robar contraseñas, números de cuenta e información bancaria. Si obtienen esta información, podrían acceder a sus cuentas.

Actualizan sus tácticas para mantenerse al día, pero usan tácticas comunes en el phishing, como contar historias para engañar a las personas y hacer que hagan clic en enlaces o abran archivos adjuntos.

Ejemplos más comunes:

- **Pago sospechoso**: Recibes un SMS o una llamada de tu supuesto banco (BBVA, CaixaBank, Sabadell…). Te explican que hay un pago sospechoso en tu cuenta bancaria y te piden credenciales ya sea mediante llamada de un falso operador o a través de una página Web que simula ser la de tu banco.
  Para solucionar ese supuesto pago, das tu información (contraseñas o códigos) y con eso proceden a sustraerte el dinero de tu cuenta.

- **Paquete de Amazon/Correos**: En este caso recibes un mensaje informando que tu paquete está paralizado en aduanas, o que ya puedes pasar a recogerlo. Una vez accedes al enlace que te envían iniciarás sesión con tus credenciales, que robarán y utilizarán para cometer la estafa.

- Otros : Afirmar que hay un problema con su información de pago, pero no lo hay. Decir que usted tiene que confirmar algún dato personal o financiero, cuando no es así. Adjuntar una factura que no reconoce, porque es falsa. Pedirle que haga clic en un enlace para hacer un pago, pero el enlace tiene un programa malicioso. Decir que le pertenece un reembolso del gobierno, pero es una estafa. Ofrecerle un cupón para conseguir algo gratis, pero eso no es cierto…

¿Cómo protegerse de los ataques de phishing? Hay varias maneras de protegerse contra los ataques de phishing.

- **Tener precaución** al abrir correos electrónicos o mensajes de texto de remitentes desconocidos, así como los adjuntos que sean descargables.

- **Valida la Identidad del Remitente**: Verifica la identidad del remitente, especialmente si recibes correos electrónicos inesperados. Si se trata de tu entidad bancaria o una empresa conocida, contacta con ellos para verificar la fuente del mensaje/correo.

- **Sé Escéptico:** Mantén una actitud escéptica ante correos electrónicos, mensajes o sitios web inesperados o sospechosos.

- **Verifica la URL**: Antes de hacer clic en cualquier enlace, verifica la URL. Los sitios web legítimos utilizan direcciones web coherentes y seguras. No hagas clic en enlaces que parezcan sospechosos o que te redirijan a dominios desconocidos.

¿Qué hacer si sospecha un ataque de phishing? Si sospecha que ha sido víctima de un ataque de phishing, es importante tomar medidas inmediatas para proteger su información personal y financiera.

1) En primer lugar, **cambie todas sus contraseñas**

2) póngase en contacto con su banco o compañía de tarjeta de crédito para **informarles del incidente**.

3) Poner una **Denuncia a la policía**

4) Contactar con un **despacho especializado** en estafas Phishing

¿Cómo puedo recuperar mi dinero?

Si has sido víctima de una de estas estafas y tu banco te dice que has incurrido en negligencia y que no hay nada que hacer, **no te lo creas**.

Pero, aunque esto ocurra, el banco también puede ser responsable por **negligencia**.

El Tribunal Supremo ya ha manifestado que no solo los perjudicados podrían ser responsables, sino que es la entidad financiera o banco quien también tiene que adoptar las medidas de seguridad necesarias para que el comercio electrónico sea suficientemente seguro.

Documentos que debes guardar

Localiza y conserva estos documentos para poder reclamar ante una estafa de phishing:

– El mensaje, SMS o correo que ha servido de anzuelo para la estafa.
– La reclamación al banco y respuesta del banco, si existe.
– La denuncia ante la Policía.
– Extractos bancarios con los cargos objeto de la estafa.
– Contrato de la cuenta corriente y/o de la tarjeta.

¡Podemos ayudarte!

Si has sido víctima de una estafa Phishing, contacta con nosotros ahora mismo y estudiaremos tu caso de manera **gratuita** para asesorarte como recuperar tu dinero.

93 727 59 65

lluis@advocatsferrer.com