
NOTA DE PRENSA

AVACU alerta de un nuevo intento de *phising*

Valencia, 27 de octubre de 2021. La Asociación Valenciana de Consumidores y Usuarios quiere advertir a los clientes de Bankia - CaixaBank de un nuevo intento de estafa a través de correos electrónicos que estarían recibiendo en sus cuentas, algo que ya ha ocurrido en otras ocasiones, especialmente en los últimos meses desde que se anunciara la fusión entre CaixaBank y Bankia.

Aprovechando el desconocimiento de algunos clientes, que pueden no tener claro en qué les va a afectar dicha fusión, y la próxima fecha del 12 de noviembre, en que dejará de funcionar la aplicación móvil de Bankia, los clientes han comenzado a recibir en sus cuentas de correo electrónico un mensaje en el que se les indica que deben activar su tarjeta para garantizar una mayor seguridad y, de no hacerlo, dejarán de poder utilizarla:

¡Atención este correo es privado!



Estimado cliente,

A partir del 26/10/2021, no podrá utilizar su tarjeta si no ha activado el nuevo sistema garantiza mayor seguridad en sus operaciones Activa ahora para leer :

<https://www.caixabank.es/particular>

Número de cliente: #100653212

Atentamente,
© 2021 Caixa
Muchas Gracias.

Como en otras ocasiones, estos intentos de fraude buscan conseguir datos personales y bancarios de los clientes, a través de enlaces a páginas web en las que se les indica que deben introducir o facilitar dichos datos para, por ejemplo, poder seguir accediendo a sus cuentas, utilizando sus tarjetas, realizando pagos por Bizum...

¿Qué debemos hacer si recibimos uno de estos correos?

- fijarnos en **QUIÉN envía el correo**: las cuentas desde las que recibimos este tipo de correos suelen incluir el nombre de la empresa a la que intentan suplantar con alguna pequeña modificación (incorporando mayúsculas o minúsculas, cambiando la extensión...)
- **QUÉ nos indican en el asunto**: suelen incluir conceptos como "urgente", que nuestra cuenta ha sido suspendida, que es necesario actualizar o activar algún dato... En ocasiones, pueden incluir caracteres, letras y números sin sentido o raros.
- **A QUIÉN se dirige**: estos correos no van personalizados, sino que se encabezan con "Estimado cliente", "Apreciado usuario"...
- **CÓMO está escrito el correo**: aunque cuando comenzaron a surgir estos correos maliciosos la redacción y ortografía de los mismos era bastante mala y se identificaban claramente, en los últimos tiempos este aspecto ha mejorado bastante. Aún así, suele tratarse de una redacción muy básica, con frases muy cortas y directas que, al pasar por motores de traducción, no emplean correctamente palabras, giros o frases
- **QUÉ aparece en el cuerpo del correo**: incluyen un enlace que nos va a llevar a una página no oficial de la compañía o entidad. Si tuviéramos que hacer alguna gestión con nuestra operadora, debemos acceder siempre a través de la zona de cliente de la web oficial, y revisar ahí si hubiera algún problema con alguna factura

De: CaixaBank [mailto:infos5115support@contact.unieuro.it]
Enviado el: martes, 26 de octubre de 2021 4:56

Asunto: ***SPAM***RE: Aplicar para reactivar su tarjeta de crédito #10095769 !

el correo electrónico desde el que nos lo envían no es el oficial de la entidad

caracteres raros

¡Atención este correo es privado!



correos generalizados, no personalizados

Estimado cliente,

A partir del 26/10/2021, no podrá utilizar su tarjeta si no ha activado el nuevo sistema garantiza mayor seguridad en sus operaciones Activa ahora para leer :
<https://www.caixabank.es/particular>

redacción básica, no escrito correctamente

Número de cliente: #100653212

Atentamente,
© 2021 Caixa
Muchas Gracias.

aunque pueda parecer que el enlace nos va a llevar a la página oficial de la entidad, si pasamos el cursor por encima veremos la dirección real a la que nos dirige y podemos comprobar que no es la de CaixaBank

Por todo ello, si recibiéramos un correo con estas características, es más que probable que nos encontremos ante un correo malicioso, que únicamente pretende hacerse con nuestras claves u otros datos personales, por lo que **NO DEBEMOS ACCEDER** al enlace que nos indiquen y borrarlo de nuestra bandeja de entrada. En caso de duda, siempre podemos contactar directamente con nuestra entidad bancaria para verificar la veracidad de esos correos.

No obstante, ante cualquier duda, pueden también ponerse en contacto con nosotros, a través de nuestra web www.avacu.es o correo electrónico avacu@avacu.es.