bankinter

¿Cómo protegerse de los ciberdelincuentes?

Conocer las estafas virtuales más comunes es el primer paso.

Se las contamos

Los ciberdelincuentes intentarán contactar con usted **mediante cualquier canal** de **comunicación**, normalmente suplantando a una entidad que le resulte conocida, como su propio banco.

Copiarán los logotipos y el estilo de comunicación para que crea que es real, y le pedirán realizar alguna acción en concreto, en la mayoría de los casos de forma urgente para que no tenga tiempo de verificar la información.

Estos son algunos de los **canales más frecuentes:**

bankinter

Phishing

Consiste en el **envío de un correo electrónico a una persona simulando ser una empresa pública o privada** para que comparta su información personal, profesional o financiera.

Copian los logotipos, el estilo de los mensajes reales y le piden que realicen alguna acción, normalmente de forma urgente.

¿Cómo actuar?

- **Desconfíe si le piden** contraseñas o datos bancarios.
- **Preste atención al remitente** del email, y si ve algo raro, no lo abra.
- Si nota algo sospechoso, **no responda al correo**.
- **No haga clic** en ningún enlace ni descargue archivos adjuntos si le piden una acción que no ha solicitado.

bankinter

Smishing

Es el intento de **fraude a través de un mensaje de texto en el teléfono móvil (SMS)**, para obtener información personal, profesional o financiera. Normalmente **le pedirán hacer clic en algún enlace web o llamar a un teléfono** para "verificar", "actualizar" o "reactivar" algún servicio.

¿Cómo actuar?

- No se apresure, **no haga clic** en enlaces, archivos adjuntos o imágenes sin verificar el remitente y la dirección web.
- **No responda a un SMS** que solicite su PIN, la contraseña de su banco u otras credenciales de seguridad.
- **Bankinter nunca le solicitará** sus credenciales a través de un SMS.

bankinter

QRishing

El ciberataque se produce cuando **escanea un código QR** desde su teléfono móvil **que le dirige a un sitio web falso**, allí le pedirán las credenciales o información confidencial.

¿Cómo actuar?

- **Desactive** en su móvil la opción de abrir automáticamente los enlaces al escanear un código QR.
- **Use aplicaciones de escaneo** que permitan ver a qué URL dirige ese código antes de abrirlo.
- **Preste atención** por si el código QR hubiese sido manipulado.

bankinter

Vishing

Los atacantes **llaman por teléfono** para conseguir su dinero o el de su empresa, información sensible o acceso a su ordenador. Para convencerle, **usarán información básica sobre usted que habrán encontrado en Internet** para que crea que es una entidad legítima.

¿Cómo actuar?

- **Sospeche** si alguien le llama creando una sensación de urgencia o presión.
- **No facilite ningún tipo de información** sensible por teléfono.
- Si la persona que llama le pide descargar un software, hacer clic en algún enlace o abrir algún archivo, **no lo haga.**
- Bankinter **nunca contactará con usted para solicitarle información confidencial.**

bankinter

Baiting

Es un ciberataque en el que se utiliza un **dispositivo extraíble, por ejemplo un USB, para infectar su ordenador** con un programa malicioso que les permita obtener su información confidencial.

¿Cómo actuar?

- **Desconfíe** de los dispositivos extraíbles que no sepa de dónde provienen.
- **Mantenga siempre actualizado** el antivirus de su ordenador.
- **No conecte** dispositivos externos que no le pertenezcan.

bankinter

A través de redes WiFi públicas

Las redes WiFi públicas son **inseguras**, pues son más vulnerables frente a ataques, tengan o no contraseña.

Los ciberdelincuentes suelen poner nombres a las WiFi públicas parecidas a las reales en lugares transitados, como un aeropuerto.

¿Cómo actuar?

- No acceda a su banca online ni a su información confidencial **desde WiFi públicas o sin contraseña**.
- No entre en redes WiFi **abiertas sin credenciales** de inicio de sesión.
- Mantenga el navegador y el sistema operativo **actualizados a la última versión** disponible. Además de contar con un antivirus correctamente instalado.

bankinter

En compras online

Las compras en Internet pueden ser seguras, pero a veces aparecen ofertas que no son reales y puede tratarse de un fraude.

¿Cómo actuar?

- **Vigile que la URL** comience por “https”.
- **Verifique si la tienda** online dispone de certificado digital. **Busque información y opiniones** de la empresa.
- **Observe que el diseño** de la página no sea extraño o tenga errores.

bankinter

A través de Bizum

Bizum se usa para enviar dinero necesitando únicamente el número de móvil del destinatario. Es una función que está incluida en la propia app del banco, pero también puede dar lugar a fraude.

Algunos ciberdelincuentes envían **solicitudes de dinero a través de Bizum** a clientes del servicio, y sin darse cuenta, estos aceptan el envío de dinero.

¿Cómo actuar?

- Recuerde **verificar** el perfil del usuario con el que está interactuando.
- Cuando utilice Bizum, asegúrese de **leer** todo correctamente antes de realizar cualquier gestión.
- Cuando reciba un Bizum, el importe aparecerá instantáneamente en su cuenta bancaria y recibirá una **notificación** de su entidad para informarle.

bankinter

Fraude del CEO

Consiste en **suplantar la identidad de una persona con autoridad** sobre otras que tienen acceso a bienes económicos, con el objetivo de realizar movimientos de dinero a las cuentas del ciberdelincuente. Suelen usar el correo electrónico o llamadas.

¿Cómo actuar?

- **Sospeche** de este tipo de peticiones, sobre todo si no son habituales, o involucran a cuentas en el extranjero.
- **Examine** con detenimiento el remitente del mensaje y los fallos gramaticales.
- En caso de duda, compruebe que la persona que le contacta **es quien dice ser.**

Fake news

Se trata de **noticias falsas que se difunden** para escandalizar a la opinión pública y poder manipularla; el objetivo suele ser político, económico o social.

¿Cómo actuar?

- **Analice el medio** que ha publicado la noticia y contrástela.
- **Observe con atención** la URL, por si la encuentra sospechosa.
- **Compruebe las fechas** en las que fue publicada.
- **Verifique** que no existan errores ortográficos o gramaticales.
- **Observe** si las imágenes han sido manipuladas.

bankinter

A través de tarjetas

Los fraudes con tarjeta se producen cuando alguien accede a su tarjeta (o a sus datos) y utiliza dicho servicio de pago para efectuar compras, retirada o extracción de dinero en efectivo que no ha autorizado.

¿Cómo actuar?

- **Nunca facilite los datos de su tarjeta**, a menos que esté realizando una compra en un sitio legítimo.
- **Verifique** el importe de la compra antes de realizar cualquier transacción.
- **Utiliza siempre el doble factor de autenticación**, aunque las compras sean importes menores.

Y recuerde:

- Bankinter nunca le pedirá información confidencial por correo electrónico.
- No solicitará sus credenciales a través de un SMS.
- Y nunca contactará con otra persona para solicitarle en su nombre esta información.

Si ya ha caído en un fraude puede llamar al **Servicio de Atención al Fraude (900 81 00 62)**, o acercarse a la oficina más cercana, para recibir ayuda.

El conocimiento es la mejor protección.