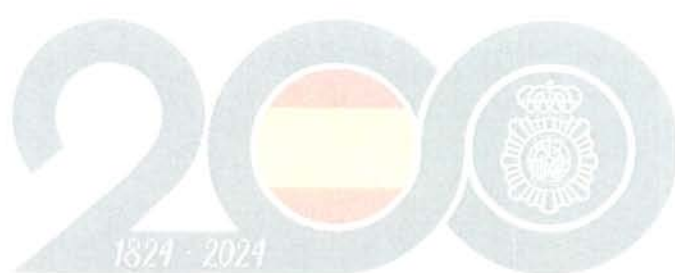


Estafas y Fraudes. Modalidades, Ejecución y Consejos de Prevención



Guía dirigida a los miembros de CEIM – Confederación Empresarial de Madrid-CEOE, con el objetivo de informar sobre las principales modalidades delictivas que afectan a empresarios, con detalle de su ejecución y recomendaciones de prevención basadas en alertas de la **Policía Nacional**.

Man in the Middle

Fraude basado en suplantar las comunicaciones entre proveedor y cliente, con la finalidad de desviar un pago legítimo hacia una cuenta bancaria controlada por el estafador.

Ejecución

1 Correo del proveedor

Una empresa recibe un correo electrónico de un proveedor, solicitando el pago de una factura por la prestación de un servicio.

2 Interceptación y manipulación

A través de una brecha, en la seguridad informática, el estafador intercepta y manipula dicho correo electrónico, cambiando el IBAN (Cuenta destinataria del pago).

3 Suplantación del proveedor

El ciberdelincuente se hace pasar por el proveedor, enviando el mensaje desde una dirección de correo electrónico casi idéntica a la original, pero con una ligera alteración, apenas perceptible.

4 Transferencia fraudulenta

La empresa receptora, confiando en la autenticidad del mensaje, realiza la transferencia a la cuenta fraudulenta, perdiendo el control total de los fondos.

Cuando la empresa ordenante advierte la estafa e intenta bloquear los fondos transferidos, con el banco destinatario, estos ya han sido transferidos a otra entidad o retirados, perdiendo el control sobre ellos.

- 📄 Desde el **9 de octubre de 2025**, los proveedores de servicios de pago estarán legalmente obligados a comprobar que el nombre del beneficiario coincide con el titular del IBAN, alertando al ordenante en caso de discrepancias. **Reglamento (UE) 2024/886 el Parlamento europeo y del Consejo.**

🎧 PODCAST POLICÍA NACIONAL

🎧 Escucha el podcast de Policía Nacional sobre esta modalidad de estafa en Spotify:
https://open.spotify.com/episode/3RLSENqDN6Iyu6nGBfrdZ1?si=q2D3e5XtRymoA_fRZ12NUg



Tips de Prevención



Verificación de destinatarios

Verificación de la autenticidad de los destinatarios, en mayor medida en solicitudes de pago urgentes.



Señales de alerta

Tomar en consideración las señales de alerta o advertencia tipo: "No existe coincidencia entre el destinatario y el titular de esa cuenta"



Cambios inesperados

Sospechar de cambios inesperados en los datos de facturación.



Enlaces sospechosos

Evitar enlaces de correos procedentes de fuentes desconocidas.

Medidas adicionales de seguridad

- Acceder a sitios web seguros con certificado
- Proteger la red wifi de la empresa. Contraseñas robustas y no adivinables. En el caso de que los clientes se conecten a una red en la empresa, habilitar una red de invitados con acceso restringido a la red corporativa y servicios de la empresa.
- Tener actualizado el software, especialmente el sistema operativo y el navegador.
- En el caso de conectarnos a redes públicas, evitaremos difundir información personal.
- Evitar enlaces de correo procedentes de fuentes desconocidas.
- Limpieza del equipo antes de transmitir cualquier información sensible.

Pagarés sin Fondos

Los miembros de un entramado criminal simulan ser empresarios solventes ante empleados de establecimientos comerciales para la obtención de objetos que posteriormente comercializan.

Ejecución de la estafa

Estas personas se presentan ante establecimientos comerciales como empresarios solventes y con capacidad económica, construyendo una apariencia de legitimidad cuidadosamente planificada. Para ello, y aprovechando su amplio conocimiento en materia de falsedad documental y de la operativa mercantil y bancaria, adquieren sociedades inactivas o carentes de actividad real.

La titularidad de estas empresas les permite operar formalmente en el tráfico jurídico y obtener de las entidades bancarias instrumentos de pago, como pagarés, que refuerzan su imagen de solvencia. Con dichos pagarés adquieren bienes y mercancías en distintos establecimientos, generando en los vendedores la confianza necesaria para cerrar las operaciones.

Posteriormente, los artículos obtenidos son comercializados a través de portales de compraventa de segunda mano en internet, convirtiéndolos rápidamente en liquidez. En otros casos, determinados bienes, como piezas de alta relojería o prendas de marcas exclusivas, son utilizados para reforzar su puesta en escena, exhibiéndolos como signos externos de éxito empresarial y solvencia económica, lo que facilita la comisión de nuevas operaciones fraudulentas.

Tips

Verificar identidad

Verificar la identidad de la persona y empresa que dice ser propietario.

Desconfiar de propuestas ventajosas

Desconfiar de propuestas rápidas o demasiado ventajosas.

Exigir transferencias

Exigir transferencias inmediatas en vez de pagarés.

La Siembra

Se trata de un tipo de estafa en el que intervienen varias personas con una estructura organizada y con un claro reparto de funciones: un conductor y dos personas más que serían las encargadas de seleccionar a la víctima para realizar el engaño, particularmente personas de edad avanzada.

Ejecución de la estafa

Los estafadores se desplazan en vehículo hasta las inmediaciones de un cajero automático previamente seleccionado, valorando especialmente que se encuentre situado en el exterior de la sucursal bancaria, circunstancia que facilita una actuación rápida, discreta y con menor riesgo de identificación durante la ejecución de la estafa.

01	02	03
Observación del PIN	Engaño en la pantalla	Retirada de efectivo
Estas personas aprovechan el momento en el que una persona se dispone a extraer dinero en efectivo del cajero para colocarse tras ella simulando ser otro cliente más que necesita hacer una transacción, pero lo que realmente hacen es situarse suficientemente cerca de la víctima como para observar el número pin en el teclado.	En el momento en el que la víctima ha finalizado su operación bancaria, uno de los autores le hace creer que hay un error en la pantalla y por eso no puede utilizar el cajero, para lo cual le convence de que, para desbloquear la pantalla debe de colocar su tarjeta bancaria sobre el contactless del teclado.	Una vez que la víctima ha colocado su tarjeta bancaria en el contactless y se ha ido del lugar, el/la autora introduce el número pin que previamente ha visto y realiza la retirada de efectivo.

Variante en Parkings y Tips de Prevención

Variante en parkings de centros comerciales

Una variante de este tipo de delitos se está llevando a cabo actualmente en los parking de centros comerciales y establecimientos de alimentación. En este caso, el autor selecciona a la víctima que está distraída introduciendo la compra u otros objetos en los asientos o maletero de su propio vehículo, se acerca a esta y deja en el suelo cualquier tipo de objeto o incluso dinero con la finalidad de entretenerla el tiempo suficiente para que un segundo autor (compinche), sustraiga las pertenencias que la víctima previamente ha dejado depositadas en el interior del vehículo.

Tips

Cajeros automáticos

En cuanto a cajeros automáticos, desconfiar de personas desconocidas que se aproximen innecesariamente con la sola intención de poder visualizar nuestro número pin de tarjeta, y sobre todo, desconfiar de cualquier tipo de ayuda que pueda repercutir en la adquisición de nuestros datos bancarios.

Parkings

En el apartado de los parking, desconfiar de personas desconocidas que ofrezcan su ayuda o cualquier tipo de argucia de distracción.

Modalidad de estafa

Vishing y Smishing

A través de mensajes de texto alertan a las víctimas de un supuesto intento de fraude bancario, llegando incluso a incorporar en el texto un teléfono fijo al que deben de llamar en caso de no reconocer la operación.

Ejecución de la estafa

Este entramado cuenta con los medios técnicos necesarios para que los mensajes remitidos a los teléfonos móviles de las víctimas no sean identificados por los sistemas de seguridad como "posible fraude", evitando así generar sospechas iniciales. Asimismo, con el fin de reforzar la apariencia de legitimidad y credibilidad, los mensajes incluyen un número de teléfono fijo al que las víctimas pueden llamar en caso de duda, siendo dicha línea atendida por los propios estafadores para afianzar el engaño.

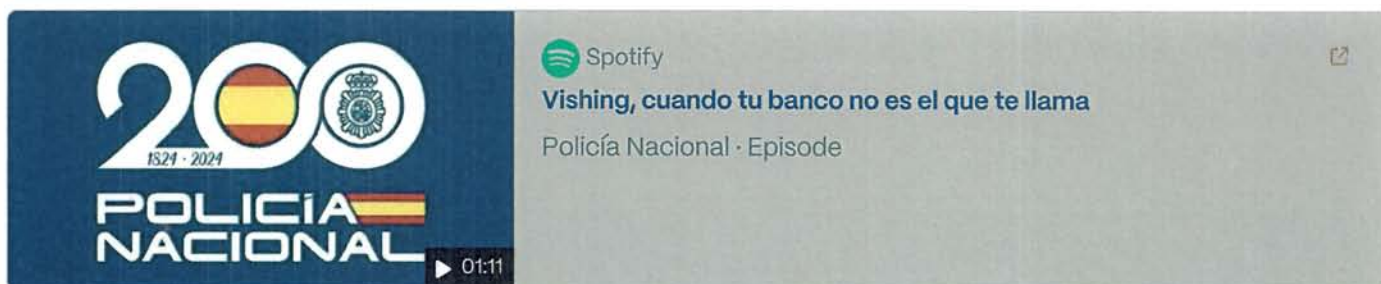
Cuando la víctima realiza la llamada para verificar que efectivamente es su banco, una persona se hace pasar por agente del departamento antifraude del banco, y gracias a la ingeniería social, los autores consiguen que la víctima le proporcione información sensible en cuanto a sus datos bancarios, y una vez ganada la confianza, llegan a dar directrices a los perjudicados para ayudarles en cuanto a los supuestos cargos fraudulentos.



El proceso de engaño se basa en la confianza generada por la apariencia de legitimidad del mensaje y la llamada telefónica.

🎧 PODCAST POLICÍA NACIONAL

🎧 Escucha el podcast de Policía Nacional sobre esta modalidad de estafa en Spotify:
<https://open.spotify.com/episode/1vskLVEDAyUwPdItsRLWeN?si=BSSmuq58RLa1DDumsNg2tg>



Tips de Prevención



Eliminar mensajes sospechosos

Omitir o eliminar este tipo de mensajes o notificaciones, y en ningún caso acceder al enlace ni descargar ningún tipo de aplicación que nos indiquen, así como tampoco responder a los mismos.



Cambiar contraseñas

En el caso de haber accedido al enlace y haber introducido las credenciales de acceso a la cuenta bancaria, se deberán de modificar o cambiar las contraseñas de acceso a banca online, así como informar a la entidad bancaria.



Revisar la URL

Revisar la URL de la página web. Si no contiene un certificado de seguridad o no corresponde con el sitio web, nunca facilites ningún tipo de información personal o bancaria.

Modalidad de estafa

"Mulas" Financieras

Se trata de un fraude que consiste en abrir cuentas bancarias aportando nóminas falsas para dar apariencia de solvencia económica, y de cuyas cuentas obtenían tarjetas bancarias para realizar compras y apuestas en casinos.

Ejecución de la estafa: El entramado criminal contacta con personas, principalmente a través de redes sociales, y les ofrecen ganar dinero de forma sencilla y rápida.

Estas personas que se denominan "mulas financieras", son piezas claves en la estafa porque gracias a su identidad y a la creación de nóminas falsas que aportan a la entidad bancaria, se abren cuentas que llevan aparejadas tarjetas de crédito que van a parar a los estafadores y con las que realizan compras y apuestas en casinos.

Tips – "Mulas" Financieras

No abrir cuentas innecesarias

No abrir cuentas bancarias que "realmente no necesitamos", y menos a cambio de una cantidad económica.

Claves intransferibles

Nunca entregar las claves de acceso y de operativa, que son intransferibles, a terceras personas.

Responsabilidad del titular

La apertura de una cuenta bancaria, lleva aparejada la responsabilidad del uso que se haga de la misma. La cesión del uso y control de la cuenta bancaria, no exime de responsabilidad penal al titular.

¡SOSPECHA!

Si nos ofrecen una cantidad económica a cambio de la apertura y las claves de una cuenta bancaria "SOSPECHA", pueden estar convirtiéndote en parte de un delito.

