# Consejos contra estafas de phishing

BANCOS NUNCA PIDEN ESO .com

**Cada día, personas como tú pierden su dinero con estafas de phishing en línea. No caigas por lo falso — aprende a identificar mensajes de texto, correos electrónicos y llamadas telefónicas sospechosas, sabiendo qué cosas nunca te preguntaría tu banco.**

## Estafas por correo electrónico

Las estafas por correo electrónico representan el 96 por ciento de todos los ataques de phishing, convirtiendo al correo electrónico en la herramienta más frecuente de los delincuentes.

**CORREO ELECTRÓNICO**
LLAMADAS TELEFÓNICAS
MENSAJES DE TEXTO
APLICACIONES DE PAGO MÓVIL

### Evita hacer clic en enlaces sospechosos

Si un correo electrónico te presiona para hacer clic en un enlace, ya sea para verificar tus credenciales de inicio de sesión o hacer un pago, puedes estar seguro de que es una estafa. Los bancos nunca te piden que hagas eso. Lo mejor es evitar hacer clic en enlaces de correo electrónico

### Estate Alerta a tácticas de intimidación

Los bancos nunca recurren a tácticas de intimidación, amenazas o lenguaje de alta presión para que actúes rápidamente, pero los estafadores sí lo hacen. Cualquier demanda que pide acción urgente debería  ponerte en máxima alerta. No importa cuán auténtico parezca un correo electrónico, nunca respondas.

### Estate atento a los adjuntos y a los errores

Tu banco nunca enviará adjuntos como un PDF en un correo electrónico inesperado. Los errores ortográficos y la mala gramática también son señales de advertencia de una estafa de phishing.

### Ten cuidado con todos los correos electrónicos

Tratar siempre el correo electrónico entrante como un riesgo potencial te protegerá de las estafas. Los correos electrónicos fraudulentos pueden parecer muy convincentes, utilizando lenguaje y logotipos oficiales, e incluso URL similares. Esté siempre alerta.

## Qué hacer si caes en una estafa por correo electrónico

1. Cambia tu contraseña si hiciste clic en un enlace y proporcionaste cualquier información personal, como tu nombre de usuario y contraseña, en un sitio falso.
2. Ponte en contacto con tu banco.
3. Si perdiste dinero, presenta un informe policial.
4. Presenta una queja ante la Comisión Federal de Comercio o llama al 1-877-FTC-HELP (382-4357)

American Bankers Association®

# Consejos contra estafas de phishing

**Cada día, personas como tú pierden su dinero con estafas de phishing en línea. No caigas por lo falso — aprende a identificar mensajes de texto, correos electrónicos y llamadas telefónicas sospechosas, sabiendo qué cosas nunca te preguntaría tu banco.**

BANCOS NUNCA PIDEN ESO .com

## Estafas por llamadas telefónicas

A veces, los estafadores intentan engañarte y robarte dinero fingiendo ser tu banco por teléfono. En algunas estafas, son amables y serviciales. En otras, te amenazan o intentan asustarte. Frecuentemente, los estafadores te pedirán tu información personal o tratarán de convencerte para que les envíes dinero. Los bancos nunca harían esto.



### Ten cuidado con un falso sentido de urgencia

Los estafadores cuentan con que actúes sin pensar, generalmente incluyendo una amenaza. Los bancos nunca harían esto. Un estafador podría decir “actúa ahora o cerraremos tu cuenta” o incluso “hemos detectado actividad sospechosa en tu cuenta.”

### Nunca proporciones información sensible

Nunca compartas información sensible como tu contraseña bancaria, PIN o un código único con alguien que te llame inesperadamente, incluso si dicen ser de tu banco. Puede ser que los bancos necesiten verificar información personal si tú los llamas, pero nunca al revés.

### No confíes en la identificación de llamadas

Los estafadores pueden hacer que aparezca cualquier número o nombre en la identificación de llamadas. Incluso si tu teléfono muestra que es tu banco quien llama, podría ser cualquier persona. Siempre desconfía de las llamadas entrantes.

### Cuelga, incluso si parece legítimo

Ya sea que sea un estafador fingiendo ser tu banco o una llamada real, puedes quedar seguro finalizando las llamadas inesperadas y marcando el número en la parte posterior de tu tarjeta bancaria en su lugar.

## Qué hacer si caes en una estafa por llamada

1. Si divulgaste información personal como tu número de seguro social o número de cuenta bancaria a un estafador, ve a RoboDeIdentidad.gov para ver qué pasos debes seguir, incluyendo cómo monitorear tu crédito.
2. Cambia tu contraseña si compartiste cualquier tipo de nombre de usuario o contraseña.
3. Ponte en contacto con tu banco.
4. Si perdiste dinero, presenta un informe policial.
5. Presenta una queja ante la Comisión Federal de Comercio o llama al 1-877-FTC-HELP (382-4357).

American Bankers Association®

# Consejos contra estafas de phishing

**Cada día, personas como tú pierden su dinero con estafas de phishing en línea. No caigas por lo falso — aprende a identificar mensajes de texto, correos electrónicos y llamadas telefónicas sospechosas, sabiendo qué cosas nunca te preguntaría tu banco.**

BANCOS NUNCA PIDEN ESO .com

## Estafas por Mensajes de Texto

Los mensajes de texto de phishing intentan engañarte para que compartas información personal como tu contraseña, PIN o número de seguridad social con el objetivo de acceder a tu cuenta bancaria. Tu información estará segura mientras no respondas a estos mensajes y los borres.



### Tómate tu tiempo, piensa antes de actuar

Si actuas demasiado rápido cuando recibes mensajes de texto de phishing puede resultar en dar acceso involuntariamente a los estafadores a tu cuenta bancaria, y por ende, a tu dinero. Los estafadores quieren que te sientas confundido y apresurado, lo cual siempre es una señal de alerta

### No hagas clic en enlaces

Nunca hagas clic en un enlace enviado por mensaje de texto, especialmente si te pide iniciar sesión en tu cuenta bancaria. Los estafadores usan esta técnica para robar tu nombre de usuario y contraseña.

### Nunca envíes información personal

Tu banco nunca te pedirá tu PIN, contraseña o código de inicio de sesión único en un mensaje de texto. Si recibes un mensaje de texto solicitando información personal, es una estafa.

### Elimina el mensaje

No arriesgues responder accidentalmente o guardar un mensaje de texto fraudulento en tu teléfono. Si estás reportando el mensaje, toma una captura de pantalla para compartir y luego elimínalo.

## Qué hacer si caes en un mensaje de texto de phishing

1. Cambia tu contraseña si hiciste clic en un enlace y diste tu nombre de usuario y contraseña en un sitio falso.
2. Ponte en contacto con tu banco.
3. Si perdiste dinero, presenta un informe policial.
4. Llama a la Comisión Federal de Comercio al 1-877-FTC-HELP (382-4357).

American Bankers Association®

# Consejos contra estafas de phishing

BANCOS NUNCA PIDEN ESO .com

**Cada día, personas como tú pierden su dinero con estafas de phishing en línea. No caigas por lo falso — aprende a identificar mensajes de texto, correos electrónicos y llamadas telefónicas sospechosas, sabiendo qué cosas nunca te preguntaría tu banco.**

## Estafas con Aplicaciones de Pago Móvil

Las estafas que utilizan aplicaciones de pago como Cash App, PayPal, Venmo o Zelle® están volviéndose cada vez más comunes a medida que estas plataformas se vuelven cada vez más populares. Una vez que caes en la trampa, solo se necesitan segundos para que un estafador acceda a tu dinero ganado con esfuerzo.

CORREO ELECTRÓNICO
LLAMADAS TELEFÓNICAS
MENSAJES DE TEXTO
**APLICACIONES DE PAGO MÓVIL**

### Ojo a los mensajes o llamadas sobre aplicaciones de pago

Las estafas con aplicaciones de pago a menudo comienzan con una llamada o un mensaje. Si recibes una llamada inesperada, simplemente cuelga. Si recibes un mensaje de texto inesperado, elimínalo. Incluso cuando parezcan legítimos, verifica llamando a tu banco o a la aplicación de pago.

### Solo utiliza las aplicaciones de pago con amigos y familiares

No envíes dinero a alguien que no conoces o nunca has conocido en persona. Esta acción por aplicaciones de pago es igual a entregar efectivo a alguien.

### Alerta ante solicitudes urgentes de pago

Los estafadores confían en crear una sensación de urgencia para que actúes sin pensar. Podrían afirmar que tu cuenta corre peligro de ser cerrada o amenazarte con acciones legales. Estas tácticas son señales de advertencia de una estafa. Un banco nunca las utilizaría.

### Evita métodos de pago inusuales

Los bancos nunca te pedirán que pagues facturas con una aplicación de pago, ni te pedirán que te envíes dinero a ti mismo. Los estafadores pueden “falsificar” direcciones de correo electrónico y números de teléfono para que parezca que son de tu banco. Si tienes dudas, comunícate directamente con tu banco.

## Qué hacer si caes víctima de una estafa en una aplicación de pago

1. Notifica a la plataforma de la aplicación de pago y pide que reviertan el cargo.
2. Si vinculaste una tarjeta de crédito o débito a la aplicación de pago, informa al banco o a la compañía de tarjetas de crédito sobre el fraude. Pide que reviertan el cargo
3. Presenta un informe policial
4. Llama al FTC al 1-877-FTC-HELP (382-4357)

American Bankers Association®