



Qué hacer si recibes mensajes sospechosos relacionados con tu banco

Recibir un mensaje que aparentemente proviene de tu banco puede generar preocupación, especialmente cuando afirma que existe un problema con tu cuenta, una transferencia pendiente, un cargo no reconocido o un intento de acceso no autorizado.

Los delincuentes aprovechan precisamente estas situaciones para generar urgencia y conseguir que las personas compartan información confidencial, hagan clic en enlaces falsos o descarguen archivos maliciosos.

Este tipo de engaño se conoce comúnmente como “phishing”, cuando ocurre mediante mensajes, correos electrónicos o sitios web falsos. También puede presentarse a través de llamadas telefónicas, una modalidad conocida como “vishing”.

La buena noticia es que existen algunas medidas sencillas que te pueden ayudar a identificar estos intentos y proteger tus cuentas bancarias.

¿Cómo identificar un mensaje sospechoso?

No todos los mensajes fraudulentos son fáciles de reconocer. Algunos utilizan logotipos, nombres e incluso diseños prácticamente iguales a los de las instituciones financieras. Sin embargo, existen algunas señales de alerta.

1. Te piden actuar inmediatamente. Frases como las siguientes buscan provocar miedo o urgencia para que actúes sin pensar: "Tu cuenta será bloqueada". "Tienes una transferencia pendiente". "Detectamos un acceso sospechoso". "Debes confirmar tu identidad ahora". "Tu tarjeta será cancelada". La urgencia es una de las principales herramientas de los fraudes digitales, por eso, antes de hacer cualquier cosa, detente y verifica la información.

2. Te solicitan datos confidenciales. Desconfía si el mensaje te pide proporcionar tu contraseña, NIP, CVV de tu tarjeta, número completo de tarjeta, códigos de seguridad o código de verificación enviado a tu celular. Los datos de acceso y códigos de autenticación son información confidencial y no deben compartirse por mensajes, llamadas o correos.

3. Incluye un enlace extraño. Un mensaje puede decir "Ingresa aquí para desbloquear tu cuenta" y llevarte a una página que parece idéntica a la de tu banco. Si recibes un mensaje inesperado de tu banco, evita entrar desde el enlace que contiene. En su lugar, abre directamente la aplicación oficial de tu banco, acude a una sucursal o comunícate al servicio de atención a clientes para verificar si la información es real.

4. Tiene errores o un tono poco habitual. Los mensajes fraudulentos pueden contener errores ortográficos, frases poco naturales, formatos extraños o solicitudes que normalmente tu banco no realiza. Pero aunque un mensaje esté bien escrito y parezca profesional, esto tampoco garantiza que sea legítimo, por eso siempre hay que confirmar antes de actuar.

¿Qué debes hacer si recibes un mensaje sospechoso?

La primera recomendación es sencilla: no abras enlaces ni archivos adjuntos si tienes dudas sobre el origen del mensaje. Un enlace puede dirigir a una página falsa diseñada para robar tus datos.

Aunque el mensaje te pida contestar con algún dato o confirmar una operación, evita hacerlo. Responder también puede confirmar a los delincuentes que tu número telefónico o correo electrónico está activo.

Si el mensaje afirma que existe un problema con tu cuenta, no utilices los datos de contacto incluidos en él. Abre la aplicación oficial de tu banco o busca el número de atención al cliente en tus documentos bancarios o en el sitio oficial de la institución. Pregunta directamente si existe alguna alerta o movimiento relacionado con tu cuenta.



bancodonde.com

Si el mensaje es sobre una operación no autorizada, primero revisa tus movimientos y los inicios de sesión o alertas de seguridad, si la plataforma ofrece esta función. Si realmente detectas una operación que no reconoces, comunícate inmediatamente con tu institución financiera.

¿Y si ya diste clic en el enlace? No entres en pánico, pero actúa rápidamente. Si únicamente abriste el enlace y no proporcionaste información, cierra la página y evita interactuar con ella.

Si ingresaste tu usuario, contraseña, NIP, datos de tarjeta o algún código de seguridad, contacta inmediatamente a tu banco a través de un canal oficial. También es recomendable cambiar las contraseñas comprometidas y, si utilizabas la misma contraseña en otros servicios, modificarla también.

Protege también tu teléfono

La seguridad bancaria no depende únicamente de reconocer mensajes fraudulentos. Por eso, mantén actualizado tu teléfono y las aplicaciones que utilizas, utiliza bloqueo de pantalla y evita instalar aplicaciones desde fuentes desconocidas.

También es recomendable activar las notificaciones de movimientos bancarios. De esta manera, podrás detectar rápidamente operaciones que no reconozcas.

Adicionalmente, puedes adoptar algunos hábitos de prevención, como el uso de contraseñas únicas y robustas, así como la autenticación de dos factores. Otra recomendación es evitar realizar operaciones financieras desde redes Wi-Fi públicas, además de no guardar datos bancarios en sitios desconocidos.

Los fraudes digitales utilizan cada vez más estrategias para parecer comunicaciones legítimas. Por eso, no basta con observar el logotipo o el nombre del banco, también es necesario prestar atención a lo que el mensaje solicita y, sobre todo, evitar actuar bajo presión. Unos segundos de pausa pueden ser suficientes para evitar una pérdida económica importante.



bancodonde.com