Todo lo que necesitas saber para evitar estafas

Hace poco, un amigo me compartió algo que le pasó y que te puede sonar muy familiar. Y puedo dar fe que él es una persona cuidadosa con la tecnología, pero un día recibió un mensaje de texto que le llamó la atención. Decía algo así:

«¡Alguien inició sesión en tu cuenta desde Bélgica! Si no fuiste vos, llamanos inmediatamente.»

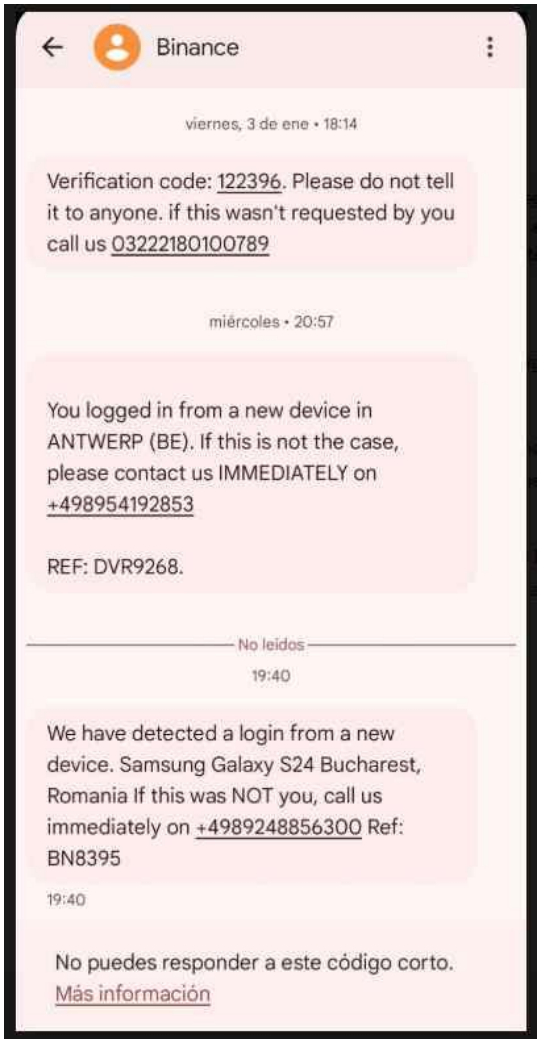
Marcelo se asustó, y obviamente pensó: *«¿Me hackearon? ¿Qué pasa con mi plata?»*. Sin pensarlo mucho agarró el teléfono y empezó a marcar el número del mensaje. Pero algo lo frenó. Antes de llamar, recordó que había leído algo sobre mensajes falsos y decidió revisar directamente el app de la plataforma. Ahí se dio cuenta de que no había ningún inicio de sesión sospechoso, y que el mensaje era, en realidad, un intento de estafa. («Piensa, luego actúa»)

Marcelo estuvo a un paso de caer en la trampa, y no porque sea descuidado, sino porque los ciberdelincuentes son cada vez más ingeniosos.

Esta experiencia no es únicamente de Marcelo. De hecho, **yo mismo recibí mensajes muy parecidos en los últimos 60 días**, desde (aparentemente) mi cuenta de **Binance**.

Esta es una captura de pantalla de mi propio móvil donde se pueden ver los distintos mensajes.

Por eso, quiero ayudarte para que aprendas a reconocer estas situaciones y te protejas.
Vamos a verlo paso a paso, con ejemplos concretos y claros.



¿Qué es esto del phishing?

Imagina que recibís un mensaje que dice algo como:
«Detectamos un inicio de sesión desde un dispositivo nuevo. Si no fuiste vos, llamanos urgente al número X.»

En ese momento, te agarra la paranoia y piensas: «¿Qué pasó con mi cuenta?». Sin embargo, el mensaje no viene de la empresa real. **Es un engaño**. Lo que buscan es que actúes rápido, sin pensar, y les des tu información personal o accedas a un link que les abre las puertas a tu cuenta.

¿Cómo detectar estos mensajes falsos?

A veces, puede ser difícil darse cuenta, pero hay señales claras de que algo no anda bien. Por ejemplo:

1. **El remitente parece confiable, pero no lo es.**
   Aunque diga «Binance» (como en mi caso), esto se puede falsificar con técnicas de suplantación.
   Ejemplo real: Recibís un mensaje que dice venir de Binance, pero el número que te piden llamar no está en su sitio web oficial.
2. **Tonos de urgencia.**
   Frases como «Llámanos inmediatamente» o «Tu cuenta será bloqueada» están creados para que tomes decisiones apuradas, sin pensar.
3. **Información extraña o irrelevante.**
   Mencionan inicios de sesión desde lugares donde nunca estuviste, como Bucarest, Bélgica, Argentina o la Antártida...

¿Por qué (con mi ejemplo) los mensajes se agrupan como si fueran de Binance?

Acá está el truco técnico: cuando recibís un SMS, tu teléfono agrupa todos los mensajes con el mismo

nombre de remitente, incluso si vienen de números diferentes. Los delincuentes aprovechan esto para que parezca que los mensajes son legítimos.

Si ya recibiste un mensaje real de Binance (u otra plataforma) con un código de verificación, el próximo mensaje falso también se va a guardar en el mismo grupo. Así, piensas: *«Debe ser de Binance, seguro.»*

¿Cómo te proteges?

Desconfía de cualquier mensaje urgente.
Si te dicen que llames «YA», espera un momento y pensá. Las empresas confiables no te presionan así.

Nunca llames a números en mensajes sospechosos.
Siempre busca el número oficial en el sitio web de la empresa.

Revisa directamente en la app o en el sitio oficial.
Por ejemplo, si usas Binance, entrá a la app y chequeá tus notificaciones. Lo mismo vale para otros servicios.

Activá la autenticación de dos pasos (2FA).
Esto hace que sea mucho más difícil que alguien acceda a tu cuenta.

¿Cómo responden las plataformas profesionales?

El problema es tan serio y causa pérdidas millonarias en el mundo que hoy recibí casualmente por email desde Binance información al respecto. Si te interesa puedes leer aquí:

https://www.binance.com/en/learn/sms-and-whatsapp-scams

Entonces, no tengas miedo, pero sí cuidado.

La idea no es que vivas paranoico con cada mensaje que te llega. La clave está en frenar, analizar y actuar con precaución. ¿No estás seguro si un mensaje es real? Consúltame o revisa en los canales oficiales.

Por favor, síguenos y danos «me gusta»: