AUDITORÍA CORPORATIVA

Una Entrevista de Trabajo Falsa Abrió el Camino al Robo de Binance

El 3 de noviembre, Binance explicó cómo se preparó el robo de criptoactivos que sufrió el 29 de octubre, que la empresa calcula en unos 6.340 millones de dólares (algunos medios redondean la cifra a 6.300 millones). Según el relato de Binance que publicaron BleepingComputer y CriptoNoticias, en septiembre contactaron a un ingeniero a través de un portal de empleo legítimo. Hubo una videollamada con alguien que se presentó como de recursos humanos y luego una entrevista con un supuesto CEO.

En esa segunda conversación le pidieron descargar una prueba técnica de programación. CriptoNoticias precisa que la descargó en su computadora de trabajo. El código instaló un programa malicioso que no se conocía y que el antivirus no detectó. Desde ese equipo, y con ayuda de una herramienta interna de inteligencia artificial, los atacantes llegaron a dos ingenieros más y obtuvieron credenciales. El 29 de octubre las usaron para entrar al servicio de firma de sus billeteras. El FBI atribuyó el ataque a hackers de Corea del Norte, según reportaron ambos medios. CriptoNoticias menciona además un intento anterior, en junio, que el equipo de seguridad detectó casi de inmediato.

La secuencia, con sus fechas, está resumida en la nota de CriptoNoticias del 3 de noviembre de 2026.
https://www.criptonoticias.com/seguridad-bitcoin/videollamada-robo-trampa-infiltro-binance/

Binance Ya Ensayaba Esta Trampa con Su Propio Personal

En julio, el director de seguridad de Binance contó a Cointelegraph que la empresa lanza cada mes ataques de phishing simulados contra sus empleados, que lo hace desde hace tres o cuatro años y que en uno de los escenarios su equipo rojo se hace pasar por reclutador. En septiembre empezó un engaño con esa misma forma, y funcionó. La formación sigue haciendo falta, pero no puede ser la única barrera. Una persona entrenada puede detectar cien correos falsos y aun así confiar en un proceso de selección con varias entrevistas, una videollamada y fotos personales. Por eso la pregunta de diseño es hasta dónde llega un equipo comprometido. En este caso, según el relato de Binance, una computadora de trabajo condujo a otras personas y, a través de ellas, a la firma de transacciones.

Las declaraciones sobre esas simulaciones fueron publicadas por Cointelegraph el 26 de julio de 2026.

https://cointelegraph.com/news/binance-red-teams-own-staff-every-month-to-keep-hackers-out

Por Qué una Empresa en Venezuela También Está Expuesta

Reuters informó el 19 de octubre que empresas de servicios petroleros como Weatherford, Baker Hughes, Halliburton y SLB anuncian decenas de vacantes en Venezuela. SLB tenía 35 en su sitio web para Anaco, Maturín y Caracas. Cuando circulan ofertas reales, el mensaje de un reclutador desconocido parece normal, y uno falso se confunde más fácil con los demás.

La nota de Reuters puede leerse en la copia publicada por BOE Report el 19 de octubre de 2026.
https://boereport.com/2026/10/19/venezuela-oilfield-hiring-picks-up-as-first-wave-of-investment-builds/amp/

El CICPC ya había hecho una advertencia en esa línea. En junio, su División de Delitos Informáticos recomendó desconfiar de propuestas económicas desproporcionadas en el mercado laboral y restringir las videollamadas y mensajes de números extranjeros no identificados. Lo que describimos aquí es una exposición, no un caso venezolano documentado: personal calificado que recibe ofertas, perfiles públicos que dicen dónde trabaja cada quien (el del ingeniero de Binance mencionaba su experiencia en la empresa, según BleepingComputer) y computadoras de trabajo que se usan para todo.

Las recomendaciones del CICPC fueron recogidas en la nota de El Diario del 10 de junio de 2026.
https://eldiario.com/2026/06/10/cicpc-delitos-informaticos-ia/

Reglas para Separar la Búsqueda de Empleo de los Sistemas de la Empresa

- Prohíbe abrir en equipos de la empresa cualquier prueba técnica, archivo o repositorio que llegue por un proceso de selección, y escríbelo sin tono de sospecha: buscar trabajo es legítimo y la regla habla de equipos, no de lealtad.
- Abre las pruebas y archivos desconocidos solo en una máquina aislada, como un equipo aparte o una máquina virtual, sin sesiones abiertas, claves guardadas ni acceso a la red interna.
- Haz una lista corta de los equipos y cuentas que pueden llegar a pagos, firma de transacciones, portales bancarios o consolas de administración, y saca de ella todo lo que no lo necesite.
- Da a cada persona los permisos mínimos para su trabajo y separa la cuenta de administración de la que usa para correo, chat y navegación.
- Exige doble aprobación para pagos y para cambios de cuentas de destino, y llaves de seguridad físicas para quienes administran los sistemas críticos.
- Asigna un responsable a cada alerta, con horario y suplente, y acuerda que quien ya ejecutó una prueba en un equipo de la empresa avise ese mismo día, sin castigo, para poder aislarlo.

Cómo lo Trabajamos en Auditoría y Pentesting Corporativo

Empezamos con un alcance y una autorización por escrito firmados por la dirección: qué personas, equipos y sistemas entran, qué pruebas se permiten y qué queda fuera. Dentro de ese marco preparamos un ejercicio de ingeniería social autorizado, por ejemplo un contacto de reclutamiento simulado dirigido a quienes tienen accesos privilegiados, con un archivo inofensivo que solo registra si se abrió y en qué equipo. Los resultados se reportan por proceso, nunca para sancionar a una persona. En paralelo revisamos las rutas desde un equipo de empleado hasta los sistemas críticos: permisos de administrador local, sesiones abiertas, herramientas internas conectadas a pagos o firmas, alertas y quién las atiende. Cada hallazgo lleva su evidencia. El informe ejecutivo ordena los riesgos, el plan de remediación dice qué cerrar primero y, cuando los cambios están hechos, verificamos que funcionen.

> *Una auditoría describe lo encontrado dentro de un alcance y en una fecha. No garantiza detectar programas maliciosos desconocidos ni que ningún engaño vaya a funcionar. Las reglas sobre equipos personales y la supervisión del personal tienen implicaciones laborales y de privacidad que conviene revisar con un abogado. Este artículo no es asesoría de inversión ni sobre criptoactivos.*

Una Comprobación Concreta

Abre la lista de roles de administración de tu plataforma de correo e identidad: en Microsoft 365 está en Roles y administradores del centro de administración de Microsoft Entra, y otras plataformas tienen una lista equivalente. Anota quién tiene el rol más alto y si cada una de esas cuentas usa autenticación multifactor; Microsoft recomienda menos de cinco administradores globales, todos protegidos con ella. Para cada nombre, indica si la misma cuenta se usa para el correo y la navegación de todos los días, y desde qué equipo. Repite la lista con las personas que pueden aprobar pagos en el portal de tu banco. No cambies nada durante la revisión: la lista es la base para decidir después.

Documentación de apoyo: Buenas prácticas de Microsoft para los roles de Microsoft Entra.
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices

Para seguir leyendo: El Fraude Puede Empezar con un Mensaje Creíble.
https://systems.kavaliero.com/blog/el-fraude-casi-nunca-empieza-con-un-hackeo

Si necesitas ayuda con este trabajo, consulta el alcance de Auditoría y Pentesting Corporativo.
https://systems.kavaliero.com/soluciones/auditoria-pentesting