CORPORATE AUDIT

A Fake Job Interview Opened the Way to the Binance Theft

On 3 November Binance described how the theft it suffered on 29 October was prepared. The company puts the loss at about USD 6.34 billion in digital assets (some outlets round it to USD 6.3 billion). According to Binance's account, as reported by BleepingComputer, in September an engineer was approached on a legitimate job-hunting platform by someone posing as a project director at a fictitious company. A live video call with a supposed HR representative followed, then an interview with someone claiming to be the CEO.

In that second interview he was told to download a coding assignment. CriptoNoticias says it went onto his work computer. The code installed previously unseen custom malware that antivirus software did not detect. From that machine, and with an internal AI tool, the attackers reached two more employees who worked on the wallet infrastructure and obtained credentials. On 29 October they used them to get into the wallet signing service. The FBI attributed the attack to North Korean state-sponsored hackers known as TraderTraitor, BleepingComputer reported. CriptoNoticias also describes an earlier attempt in June, which Binance's security team spotted almost at once.

The full sequence, with dates, was reported by BleepingComputer on 3 November 2026.
https://www.bleepingcomputer.com/news/security/binance-says-fake-job-interview-led-to-63-billion-crypto-heist/

Binance Already Rehearsed This Trap with Its Own Staff

In July, Binance's chief security officer told Cointelegraph that the company runs simulated phishing attacks on its own employees every month, has done so for three to four years, and that in one scenario its red team poses as job recruiters. In September a lure of that same shape began, and it worked. Training still matters, but it cannot be the only barrier. A trained person can spot a hundred fake emails and still trust a selection process with several interviews, a live video call and personal photos. So the design question is how far a compromised work device can reach. Here, by Binance's account, one work computer led to other people and, through them, to transaction signing.

The interview about those simulations was published by Cointelegraph on 26 July 2026.
https://cointelegraph.com/news/binance-red-teams-own-staff-every-month-to-keep-hackers-out

Why a Company in Venezuela Is Exposed Too

Reuters reported on 19 October that oilfield service companies including Weatherford, Baker

Hughes, Halliburton and SLB are advertising dozens of jobs in Venezuela. SLB had 35 vacancies on its website for Anaco, Maturín and Caracas. When real offers circulate, a message from an unknown recruiter looks normal, and a fake one blends in more easily.

The Reuters story can be read in the copy published by BOE Report on 19 October 2026.
https://boereport.com/2026/10/19/venezuela-oilfield-hiring-picks-up-as-first-wave-of-investment-builds/amp/

The CICPC had already given a warning along these lines. In June its computer crime division advised people to distrust disproportionate job offers and to restrict video calls and messages from unidentified foreign numbers. What we describe here is exposure, not a documented Venezuelan case: skilled staff receiving offers, public profiles that say where each person works (the Binance engineer's profile mentioned his experience there, according to BleepingComputer) and work computers used for everything.

The CICPC's recommendations were reported in El Diario on 10 June 2026.
https://eldiario.com/2026/06/10/cicpc-delitos-informaticos-ia/

Rules That Keep Job Hunting Away from Company Systems

- Ban opening, on company devices, any coding test, file or repository that arrives through a hiring process, and word it without suspicion: looking for a job is legitimate, and the rule is about devices, not loyalty.
- Open unknown tests and files only on an isolated machine, such as a spare computer or a virtual machine, with no open sessions, saved passwords or access to the internal network.
- Write a short list of the devices and accounts that can reach payments, transaction signing, bank portals or admin consoles, and remove everything that does not need to be on it.
- Give each person the least privilege their work needs, and keep administrator accounts separate from the accounts used for email, chat and browsing.
- Require two approvals for payments and for changes to destination accounts, and hardware security keys for whoever administers critical systems.
- Give every alert an owner, with hours and a deputy, and agree that anyone who has already run a test on a company device reports it the same day, without penalty, so it can be isolated.

How Security Audits & Penetration Testing Approaches It

We start with a written scope and an authorisation signed by management: which people, devices and systems are included, which tests are allowed and what stays out. Within that frame we prepare an authorised social engineering exercise, for example a simulated recruiter approach aimed at staff

with privileged access, using a harmless file that only records whether it was opened and on which device. Results are reported by process, never to penalise an individual. Alongside it we review the paths from an employee device to critical systems: local administrator rights, open sessions, internal tools connected to payments or signing, alerts and who responds to them. Every finding comes with its evidence. The executive report ranks the risks, the remediation plan says what to close first and, once the changes are made, we verify that they work.

> *An audit describes what was found within a scope at a particular date. It cannot guarantee that unknown malware will be detected or that no deception will work. Rules about personal devices and staff monitoring have employment and privacy implications worth reviewing with a lawyer. This article is not investment or crypto-asset advice.*

A Check You Can Run

Open the list of administrator roles in your email and identity platform: in Microsoft 365 it is Roles and administrators in the Microsoft Entra admin centre, and other platforms have an equivalent list. Write down who holds the highest role and whether each of those accounts uses multifactor authentication; Microsoft recommends fewer than five Global Administrators, all protected with it. For each name, note whether the same account is used for everyday email and browsing, and on which device. Repeat the list with everyone who can approve payments in your bank’s online portal. Change nothing during the check: the list is what you decide from afterwards.

Supporting guidance: Microsoft’s best practices for Microsoft Entra roles.
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices

Continue with: Fraud Can Start with a Believable Message.
https://systems.kavaliero.com/en/blog/fraud-almost-never-starts-with-a-hack

For help with this work, see the scope of Security Audits & Penetration Testing.
https://systems.kavaliero.com/en/services/security-audits