



January 5, 2026

Matias Sequeira  

Security Engineer

Alejo Sequeira 

Software Developer

Wallets

Based on a security evaluation of 77 crypto wallets across iOS, Android, and browser extensions, and a total of 2,233 individual security checks, we released the third edition of [Coinspect's Wallet Security Ranking](#).

Since our [last update](#), we've:

SKIP TO CONTENT

- Re-evaluated every previously ranked wallet to capture fixes and feature changes since the previous edition.

- Added NuFi and Elytro browser extension wallets to the evaluation pool, as part of a commitment to [share testing results with the WalletBeat initiative](#).

Our mission remains unchanged: to provide **transparent, objective security benchmarks** that empower users to choose safer crypto wallets while motivating developers to raise Web3 security standards.

If you're new here, check out our [methodology deep-dive](#) to understand how we evaluate wallets.

"Methodology criteria"

- *We count a feature as supported only if it is enabled by default.*
- *All tests were performed on public, production releases.*
- *Experimental or opt-in features (e.g. EIP-7702) were out of scope, but may be considered in future testing rounds.*

Highlights

At a glance:

- **Movement:** 39 wallets moved up, 22 moved down, and 16 maintained their position.

SKIP TO CONTENT: **Phishing detection** saw the fastest growth across all platforms.

- **The Gap:** Advanced protections remain fragmented; **mobile lags significantly behind extensions.**

- **Transparency: Transaction simulation** is becoming standard on extensions but remains rare on mobile.
-

Trending Features

1. Phishing address detection

Phishing protection is no longer a differentiator on extensions — it's becoming table stakes.

On browser extensions, adoption increased due to OKX and Ctrl adding support, reinforced by new entrants like **Binance**, **NuFi**, and **Zerion**.

On mobile platforms, adoption remains limited and driven by a small subset of wallets: **Phantom**, **OKX**, and **Coinbase Wallet** on Android, and **OKX** and **Uniswap** on iOS.

2. Malicious dApp detection

Mobile wallets continue to rely on user vigilance rather than preventative controls.

On iOS, adoption increased due to **imToken** and **Trust Wallet** adding support, **SKIP TO CONTENT** adoption remains limited.

On Android, changes were driven by a small number of wallets, with no broad adoption across the ecosystem.

3. Transaction simulation

Transaction simulation adoption surged on browser extensions, driven by wallets such as **OneKey**, **Coin98**, **Ctrl**, and **Exodus** adding support.

On mobile platforms, changes were limited to a small number of wallets, resulting in more modest overall movement.

4. eth_sign support

Disabling eth_sign remains one of the clearest indicators of a wallet's security posture.

While most wallets disable eth_sign, a minority of wallets (10 out of 77) still allow it across Android, iOS, and browser extensions.

Top Gainers / Losers

- **MetaMask** once again secured the #1 position across all three platforms.
- **OKX Extension** jumped 10 positions to #2, driven by a major security overhaul.

SKIP TO CONTENT

- **Phantom for Android** made a massive leap, climbing 10 positions to #3.

- **Unstoppable Wallet for Android** experienced the largest drop in ranking position, falling 7 places.
 - **Gem for iOS** was the top mover on Apple devices, climbing 10 positions to enter the top 20.
-

Why Phantom and OKX Led the Pack

Both **Phantom (Android)** and **OKX (Extension)** recorded the largest ranking gains this edition, each climbing 10 positions. Notable additions include:

- **Phishing protection**, with both wallets implementing alerts for known malicious blockchain addresses. Phantom additionally introduced phishing dApp detection.
 - **Access control**, implementing automatic wallet locking for idle sessions. Phantom additionally improved seed phrase authentication.
 - **Improved intent verification (OKX)**, with full EIP-712 object parsing, clearer display of signing data, and invalid address checksum detection.
-

Cross-Platform Feature Changes Since the Previous Edition

SKIP TO CONTENT

The table below summarizes **security features** that were added by wallets already present in the previous edition.

Newly added wallets are intentionally excluded to avoid mixing baseline feature support with post-entry improvements.

Feature	Extensions	Android	iOS
Transaction Simulation	OneKey, Coin98, Ctrl, Exodus	Bitget, Zerion	—
Malicious Address Detection	OKX, Ctrl	Phantom, OKX, Coinbase Wallet	OKX, Uniswap
Malicious DApp Detection	Phantom	Phantom	imToken, Trust Wallet
Disabled eth_sign	—	Bitget, Zerion	Tomo

Baseline Security Features at Entry (New Wallets)

The table below reflects security features supported by wallets newly added in this edition at the time they entered the ranking.

These entries represent baseline feature availability, not improvements.

Feature	Extensions	Android	iOS
Transaction Simulation	Binance, NuFi, Zerion	Ctrl Wallet	—
Malicious Address Detection	Binance, NuFi, Zerion	—	—
Malicious DApp Detection	NuFi	—	—

SKIP TO CONTENT

Feature	Extensions	Android	iOS
Disabled eth_sign	Binance, Elytro, NuFi, Uniswap, Zerion	Ctrl Wallet, Zengo	—

Wallets Not Evaluated in This Testing Round

In this round, we evaluated **23 extension wallets**, **26 iOS wallets**, and **all 28 Android wallets**. Wallets that hadn't released new versions or presented exceptional difficulties (geofenced downloads, unstable backends, or broken onboarding) were excluded from this cycle.

- **Ambire (iOS):** The iOS application is currently not available for public download.
- **AlphaWallet (Mobile):** The mobile application is no longer available for download via standard app stores.
- **Taho (Extension):** The extension was last updated on April 18, 2025. Given the wallet ranking baseline of March 26, 2025, the lack of recent development falls outside our freshness threshold.
- **BlockWallet:** The project has ceased operations.

SKIP TO CONTENT **aways**

- Security maturity is improving, but remains uneven across platforms.

- Browser extensions continue to lead in proactive security protections.
- Mobile wallets still lag in transaction transparency and dApp risk mitigation.
- A small set of wallets are setting the pace; most remain reactive.

"Rankings reflect security feature availability, not historical exploit data or overall code quality."

Looking Ahead

Based on current trends, we expect:

- Wider adoption of transaction simulation on mobile platforms
- Continued deprecation of eth_sign
- Increased convergence between extension and mobile security models

Explore the full [ranking](#), share it with your community, and collaborate with us to strengthen the Web3 ecosystem.

SKIP TO CONTENT

[See the Updated Ranking](#)

The Wallet Security Ranking Changelog

We publish Wallet Security Rankings through structured testing rounds conducted at least twice per year. Each round evaluates selected wallet versions against thousands of security checks, followed by a rigorous pair-review process to verify results.

Ahead of the third edition, we chose to release preliminary results prior to Devcon, before all double-checks were fully finalized. This highlighted the need for a public Changelog to clearly document subsequent adjustments. The Changelog provides a transparent record explaining why rankings may change even when wallet versions do not.

[Explore the full changelog](#)

Related Posts

[SKIP TO CONTENT](#)

More articles you might enjoy.

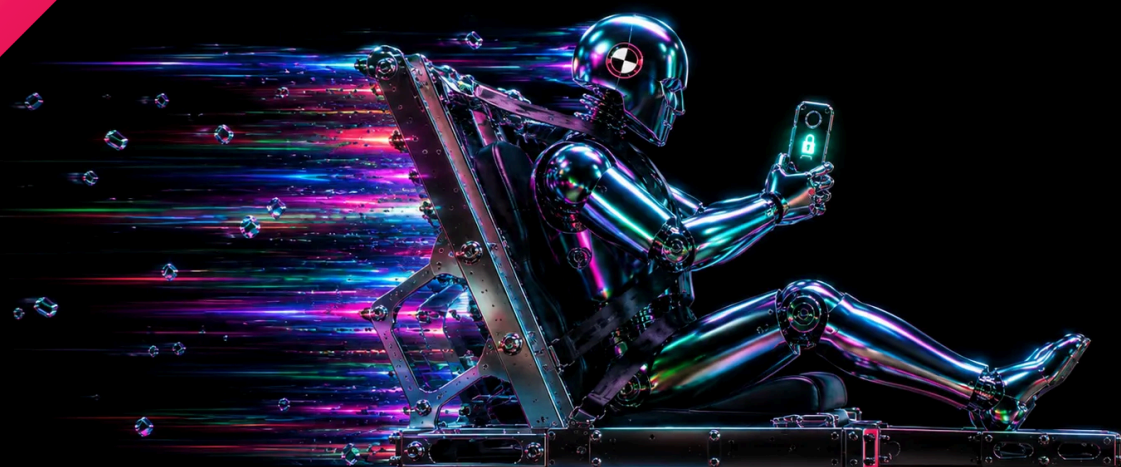
NEW

III Bloom: Investigating a Wallet Generation Vulnerability During Active Exploitation

August 5, 2026

How Coinspect traced a wallet-drain investigation back to a twelve-year-old insecure randomness flaw, searched for exposed addresses at scale, and disclosed the findings in stages while attackers were still active.

SKIP TO CONTENT

NEW

Introducing the Wallet Security Framework

July 16, 2026

Coinspect expands the Wallet Security Verification Standard into the Wallet Security Framework, an open-source resource that now combines white-box controls with black-box benchmark tests.

SKIP TO CONTENT

NEW

Why Weak Seed Generation Can Put Crypto Wallets at Risk for Years

June 24, 2026

Weak randomness in wallet generation turns impossible-to-brute-force recovery phrases into realistic attacker targets. Updating apps or re-importing seeds does not fix the risk.

Home

Services

Blog

SKIP TO CONTENT

Wallet Ranking

Contact

© 2026 Coinspect Security [Privacy](#)

